

A Logical Programming Language as an Instrument for Specifying and Verifying Dynamic Memory



René Haberland
Saint Petersburg Electrotechnical University "LETI"
Saint Petersburg, Russia

(original compatible with standard GOST R.7.0.11-2011)
(permission to air granted on 29th January 2021; self-translated into English)

2017

Contents		
I	Introduction	3
I-A	Hoare calculus	3
	I-A1 Hoare Triple	4
	I-A2 Logical Reasoning	6
	I-A3 Automated Reasoning	10
	I-A4 Alternative Approaches	14
I-B	Object Calculi	17
I-C	Dynamic Memory Models	23
	I-C1 Transformation into Stack	23
	I-C2 Shape Analysis	24
	I-C3 Pointer Rotation	24
	I-C4 File System	25
I-D	Further Areas	25
I-E	Existing Tools	27
II	Issues related to Dynamic Memory	29
II-A	Motivation	30
II-B	Issues related to correctness	32
II-C	Issues related to completeness	33
II-D	Issues related to optimisation	34
III	Expressibility of Heap Formulae	35
III-A	Heap Graph	37
III-B	Predicates	40
IV	Logical Programming and Proof	45
IV-A	Prolog as Logical Reasoner	45
IV-B	Reasoning as Proof Search	49
IV-C	Language Compatibility	56
IV-D	Knowledge Representation	57
IV-E	Verification System Architecture	59
IV-F	Class Objects	60
V	Strengthening Heap Expressibility	61
V-A	Motivation	61
V-B	Ambiguity of Spatial Operators	63
V-C	Strengthening Spatial Operators	65
V-D	Class Object as Heap	69
V-E	Partial Heap Specification	70
V-F	Discussion	71
VI	Automated Verification with Predicates	72
VI-A	Fold and Unfold	73
VI-B	Predicate Extension	73
VI-C	Predicates as Logical Rules	74
VI-D	Interpretation of Heap Predicates	77
VI-E	Translating Horn Rules	78
VI-F	Syntax Parsing as Heap Verification	79
VI-G	Properties	81
VI-H	Implementation	82
VI-I	Conclusions	92
VII	Conclusions	94
VIII	Original	99
	Nomenclature	183
	Glossary	184
	References	191
	List of theorems	199

Abstract—This work proposes a Prolog-dialect for the found and prioritised problems on expressibility and automation. Given some given C-like program, if dynamic memory is allocated, altered and freed on runtime, then a description of desired dynamic memory is a heap specification. The check of calculated memory state against a given specification is dynamic memory verification. This contribution only considers formal specification and verification in a Hoare calculus.

Issues found include: invalid assignment, (temporary) unavailable data in memory cells, excessive memory allocation, (accidental) heap alteration in unexpected regions and others. Excessive memory allocation is nowadays successfully resolved by memory analysers like Valgrind. Essentially, papers in those areas did not bring any big breakthrough. Possible reasons may also include the decrease of tension due to more available memory and parallel threads. However, starting with Apt, problems related to variable modes have not yet been resolved – neither entirely nor in an acceptable way. Research contributions over the last decades show again and again that heap issues remain and remain complex and still important. A significant contribution was reached in 2016 by Peter O’Hearn, who accepted the Gödel prize for his parallel approach on a spatial heap operation.

An essential issue of dynamic memory is when two languages are involved: one for describing and another for checking. Languages are often inhomogenous. Models that are supposed to correspond are tough to see are plausible. Languages include functional or other very special, which end up in limitations, e.g., both sides’ expressibility. Other issues regard variability and extensibility of languages involved as well as models. The results are bloated notations and complex checks, lack of expressibility or it may eventually require specific non-common conventions.

Restrictions include, e.g. the use of symbols (not variables in an imperative sense), expressibility of heap terms, logical conjuncts and less intuitive heap model and rules. Thus, a verification may become very hard to perform and debug, even with elementary examples due to the full context.

Furthermore, the input programming language and other involved languages, are often (artificially limited) by language-specific features present or absent and become the verification rules. Universal approaches seem to be hard to implement. Separation of concerns between all languages involved looks urgent and challenging. In real-life applications, the input language is inhomogenous and often represented by triads or the Polish-inverse notation, which bloats specification and verification rules.

Keywords. heap logic, points-to, heap specification and verification, heap conjunction, heap disjunction, Hoare calculus, partial heap specification, dynamic memory, variables mode, Pointer calculus, axiomatic semantics, Prolog, Horn-rules, attributed grammar, Warren’s abstract machine, semi-structured data, term transformation, spatial heap operation, operation ambiguity, memory models, object calculi, heap graph, verifier architecture, unification of processes, narrowing down languages, abstract predicates, completeness by incompleteness, fold and unfold, static analysis, multi-paradigmatic programming, parsing as proving.

Errors related to dynamic memory are one of the most expensive and intricate to locate for several decades. Often the program location where a problem arises, if any, does not correspond to the real. Consequently, development and approaches in improving error localisation and avoidance are up to date research objectives.

Expressibility of assertions, completeness of rules and automation define success for heap verification. Assertion expressibility refers to assertion formalism and verification rules. Recently, it is found descriptions of dynamic memory to be rather intricate and not intuitive. Logical reasoning improvements towards correctness and completeness often represent isolated implementations that not always cooperate in theory and practice with recent approaches. Due to an ever-growing number of conventions specification and verification languages, they do not grow in expressibility opportunities. Even the opposite is the case.

Verification often remains non-trivial and overwhelming. All the unique but different languages involved make it counter-intuitive and very challenging to handle in practice.

Research Objective

In this work, the expressibility level is increased for describing and checking dynamic memory by narrowing down heap specification and verification, excluding ambiguities and prototypical implementation.

Dedication

The work was funded by research grant no.2.136.2014/K from the Ministry of Science of the Russian Federation. I would like to thank I.L. Bratchikov, N.K. Kosovsky and A.N. Terekhov (Saint Petersburg) for the excellent preparation and motivation given prior to taking the big challenge. I would like to thank Andrew Pitts (Cambridge), Peter O’Hearn (London), Uday Reddy (Birmingham) and Graham Hutton (Nottingham) for their very motivating talks and valuable discussions. I would like to thank Paul Bowen-Hugget, Con Bradley, Rob Lougher (Bristol) and Andy Thomason (Oxford) for being excellent working colleagues. Special thank to Con for recommending never to give up. Thank you and forever in remembrance S.A. Ivanovskiy. Apart from the need to earn for a living, unfortunately, I had to fight with (inner-)German racism without which this works would not be.

Declaration

The research presented is the result of only my own initiative during the ‘spare time’ whilst working at the same time full-time on an unrelated job. This thesis is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text. It is not substantially the same as any that I have submitted for a degree, and does not exceed 250 pages.

Saint Petersburg, 2017

I. Introduction

This section introduces this dissertation's topic: "A Logical Programming Language as an Instrument for Specifying and Verifying Dynamic Memory". It introduces Hoare's calculus, basic definitions and existing approaches.

For comparison and discussion, the quality ladder from fig.1 is referred to, where the higher level includes the lower level. This ladder is the author's favourite clustering applying to any computer program. The more a program obeys the listed criteria, the higher is its quality. For example, if a program miscalculates a result, completeness and optimality may not be that important anymore. Though, an essential bit in that example would be correctness. If software obeys correctness only then, the reached level is "basically stable".

Once correctness proves to an acceptable level, additional features may be requested from a function then and only then, including a broader input variable domain. Once the basic set of input proves to work correctly, all other input variables follow for consideration – this is the second quality level named "completely stable". The second criterion includes the first and therefore is stricter. If the first two criteria hold, then the considered function is sound and complete from a computability's perspective. If so, then the third quality level asks for how good a function computes. Satisfying a given specification of the third level achieves "optimal stability". Completeness and correctness remain invariant to optimality. Optimally stable implementations may include visual effects and processing files but are not considered any further in this work.

Level	Criterion	Quality Predicate
3	Optimality	optimally stable
2	Completeness	completely stable
1	Correctness	basically stable

Figure 1: Prioritised quality ladder

Each of the proposed criteria may be resolved and accompanied accordingly by appropriate metrics to measure achievement. It appears pointless in practice to discuss, for instance, soundness and optimality when completeness violates. The reason may be an unsound implementation, which for an essential domain is just not visible and though working correctly, even when all other cases seem to work. A bad case may require a total rewriting of the considered program. Alternatively, as a compromise, the input domain may be bound, and the callers' arrangements may be required. Next, this quality ladder is applied numerous times as an orientation gadget in favour or against discussed features throughout the following techniques and sections.

This work considers imperative and hypothetical programming languages (PL) at a draft stage. For application purposes, object-orientation is the focus. Hence this

section also introduces object calculi (OC), particularly to the Theory of Objects. Next, theoretical as well as practical frontiers on dynamic memory are considered. Later representation models such as Shape Analysis (SA), Region Calculus (RC) and others are discussed. Separation Logic (SL) is considered essential for the theoretical model of dynamic memory w.r.t. dynamic memory because of the locality property. Afterwards, an overview is given on proof automation, and its restrictions are discussed. Hoare calculus is chosen to understand the proofs and their confluency better, and abstraction is introduced. A short agenda on these competing issues is found in [303]. Neighbouring disciplines like alias analysis (AA) (sec.I-D), garbage collection (GC) and code introspection (CI) are briefly introduced. Existing provers are briefly introduced at the end of this section.

A. Hoare calculus

The Hoare calculus is a formal verification method originating back to the computer scientist Charles Anthony Hoare, which allows checking correctness according to a given specification, namely, a formal description of a program's properties. Specifications denote calculation states by mathematical formulae since those are believed to be at most precise and where a conclusion is made according to a given set of rules and axioms within a defined course of discussion.

The objective of a program verification using Hoare's calculus is the formal check whether acclaimed properties are correct indeed or not. By doing so, claims towards quality may be confirmed or rejected. If a program obeys previously claimed properties, the program may be compared with other programs and other routines to perform a more complex task.

A rule in Hoare's calculus is a logical judgement of the kind $A \Rightarrow B$ reads as: "if "antecedent A is true, then the consequence can be derived". Let us consider fig.2.

$$\begin{array}{l}
 \text{(P1)} \frac{A}{B} \quad \text{(P2)} \frac{B \vee \neg B}{C} \quad \text{(P3)} \frac{\{P\}C\{Q\}}{\{P'\}C'\{Q'\}} \\
 \text{(P4)} \frac{\{P \wedge \Pi\}A\{Q\} \quad (P \wedge \neg \Pi) \Rightarrow Q}{\{P\} \text{ if } (\Pi) A \{Q\}}
 \end{array}$$

Figure 2: Logical rules in Hoare's calculus

Rule (P1) is an axiom. Let A locally be an empty antecedent. The main idea behind an axiomatic system is a check whether the finite application of rules ends in axioms or not. We do not distinguish between rules and axioms for simplicity from now on since the latter specialises earlier. Rule (P2) is an axiom if antecedent $B \vee \neg B$ can always be derived in analogy to propositional logic and can be replaced by "true" or just be dropped. However, initially, no artificial restrictions existed in the Hoare calculus, e.g. regarding judgements. Predicates

may replace assertions. A logical derivation becomes a judgement over predicates. Arbitrary methods may be applied as logical reasoning as first-order predicates, for instance, natural deduction [262], Robinson's resolution or the Tableaux method [79], [262]. The named methods are founded upon deduction. Besides deduction, abduction and induction may be used as a verification primitive. Induction proposes the introduction of not ultimately yet proven assertions that are hard to prove directly but make sense to assume are right in a context. An induced assertion can be considered as part of the verification rule set. An inductive rule added may appear strange on the first look but often may not be rejected due to a lack of contradiction, though it may be beneficial on a proof. A classic example of induction is Popper's method of falsification: Given the sentence: "All swans are white" may not always be falsifiable in practice because the number of entities to be checked may either be immense or (temporarily) unavailable (in that classic example only in Australia seem to habit black swans naturally). More general, the problem applied to logic states: occasionally, not all entities may be checked in order to decide a predicate is true or not. Therefore, an inductive statement may be chosen as a "right" rule until proven differently in the area of discourse. For example, if our discourse is about Europe only then, we are safe in asserting such an induction unless we extend our discourse to Australia — this would finally falsify our induction. Induction allows bypassing very hard or even unexplainable phenomena within a discourse by introducing a new rule or axiom, in which terms our model seems complete. So, induction allows us potentially infinite structures to be described and finally be checked by finite formulae. Whenever at least one counter-example is discovered, we either are required to reformulate our rule set or discard it entirely.

In contrast to that, abduction searches for necessary and sufficient conditions, s.t. the consequence is derivable from a fixed rule set.

A Hoare calculus may be characterised as a deductive series of judgements applied to an imperative program statement (as it was proposed by Hoare initially). The state of calculation describes each derivable judgment before and after executing that particular program statement (see section I-A1). Regarding confluency of proof (see later, sec.7), abduction and induction may be included as proof primitives for the sake of automation. Otherwise, a missing rule may disrupt a proof unfinished. Whenever the reasoned universe is generated by strict application of rules, and there is no interleaving of antecedents, the set of derivable consequences is closed (regarding the description). For example, the interpretations of possible logical statements from (P3) and (P4) from fig.2 is enclosed.

1) Hoare Triple: Hoare [116] introduces a triple for specifying the calculation states and the program state-

ment.

Definition 1.1 (Hoare Triple). A Hoare triple $\{P\}C\{Q\}$ consists of a precondition P before and a postcondition Q after invoking a program statement C .

Declarative PLs, e.g. functional, differ from imperative ones by varying calculation states depending on the variables' content. Unless said otherwise, it is agreed that by default, the evaluation order is non-strict. The declarative programming paradigm differs from the imperative paradigm, for instance, memory use, especially on symbols and variables. By default, this work considers imperative PLs only as input PLs. Initially, Hoare recommended an elementary imperative PL close to Pascal and the slightly different triple notation $P\{C\}Q$. Since superfluous parentheses became unpopular, the positions at which parentheses are put switched as introduced at the beginning around P and Q . Both P and Q denote the calculation state as assertions before and after the execution of C . C may be composed of an arbitrary number of imperative statements.

So it becomes clear why C change the calculation state stepwise. By (logical) random-access memory (RAM), we understand a CPU registers file, stack and dynamic memory as depicted in fig.25. A Hoare triple is interpreted as the following: Assuming a calculation state is denoted by P , and a program statement C is given, the corresponding computation is terminated and transits into Q . In other words, P and Q describe the calculation step before and after C . If the Hoare triple is sound, then the transition between memory states is sound. Otherwise, the following reasons may be given for unsound behaviour:

- 1) If C does not terminate, then the rule set is "incomplete", and state Q is unreachable. It can formally be described as $\vdash \{P\}C\{Q\} \rightarrow (\llbracket C \rrbracket \neq \perp) \wedge Q$, where $\llbracket \cdot \rrbracket$ is the denotational semantics for a given statement [9], [6], [276].
- 2) The axiomatic rules are incomplete. There is no such rule that applies for a given state P .
- 3) The obtained actual calculation state Q is not the expected state Q' .

Fig.3 shows essential axioms and rules for imperative PLs. Programs listed in an imperative paradigm may be rewritten in a declarative paradigm as long as both have the equivalent potency of computation model, e.g. by simulating a universal Turing machine. A control-flow graph (CFG) may abstract an imperative program. Subroutine calls can be performed on common stack architectures. Hoare's initial calculus [116] does not impose additional restrictions on the expressibility of specifications as this was primarily not addressed, nor is it a topic in his successors' work, e.g. by Apt [16]. Apt suggests a Hoare calculus for single- and multi-threaded application. Furthermore, he suggests a classification of assertions of input and output variables. Later we are going to assess

the advantages and disadvantages of such propositions in more detail.

$$\begin{array}{c}
\text{(SEQ)} \frac{\{P\}A_1\{Q\} \quad \{Q\}A_2\{R\}}{\{P\}A_1; A_2\{R\}} \\
\\
\text{(LOOP)} \frac{\{P \wedge B\}S\{P\}}{\{P\}\text{while } B \text{ do } S \{ \neg B \wedge P \}} \\
\\
\text{(ASN)} \frac{}{\{P[e/x]\}x := e\{P\}} \\
\\
\text{(CONSEQ)} \frac{P' \Rightarrow P \quad \{P\}C\{Q\} \quad Q \Rightarrow Q'}{\{P'\}C\{Q'\}} \\
\\
\text{(SP)} \frac{R \Rightarrow P \quad \{P\}A\{Q\}}{\{P\}A\{Q\}} \\
\\
\text{(WP)} \frac{\{P\}A\{Q\} \quad Q \Rightarrow R}{\{P\}A\{Q\}}
\end{array}$$

Figure 3: An incomplete rule set for verification

For example, the sequential rule (SEQ) from fig.3 requires if the compound statement $A_1; A_2$ is given with precondition P and postcondition R , then in order to prove correctness, the existence of an intermediate Q shall be shown, s.t., first, A_1 with precondition P , and, second, that Q serves as a precondition for the proof of A_2 . A sequence's correctness is proven after A_1 is proven, and A_2 is proven to have the postcondition R .

The rule of logical consequence (CONSEQ) serves for demonstration purposes as a second example. This rule is a generalisation of (SP) and (WP). Concretisation either strengthens a precondition or generalises a postcondition. If the predicate is "true" in general, then for some arbitrary well-defined (sub-)set V , the predicate is also true $\forall v \in V$. Assume, $V_1 \subseteq V$. V is a generalisation of V_1 . In this case, V_1 is a concretisation of V . It can easily be grasped the implication $V \Rightarrow V_1$ holds. However, $V_1 \Rightarrow V$ does, in general, not hold. W.l.o.g. the correctness of a predicate may be concluded for a concrete case. Therefore, rules (SP) and (WP) hold.

When unifying (SP) and (WP) (CONSEQ) may be obtained. However, renaming must be taken into consideration carefully.

As a third example, the loop rule (LOOP) can be considered a critical feature in any minimalistic and Turing-mighty PL. This rule states that if we have a loop as a program statement with P as precondition and Q as postcondition, then in order to prove correctness, it is sufficient to prove the correctness of the loop's body S accordingly with P as precondition and $\neg Q$ as postcondition, where \neg negates the postcondition.

It is worth noting that the loop from (LOOP) and the assignment rule both together allow expressing all other kinds of loops due to expressibility aspects (cf. fig.4).

$$\begin{array}{c}
\text{(REP)} \frac{\{P\}S\{P'\} \quad \{P'\}\text{while } B \text{ do } S \{Q \wedge \neg B\}}{\{P\}\text{do } S \text{ while } B\{Q \wedge \neg B\}} \\
\\
\text{(FOR)} \frac{\{P\}i := 1; \text{while } B \text{ do } (S; i := i + 1) \{Q\}}{\{P\}\text{for } i \text{ from } 1 \text{ to } n \text{ do } S \{Q\}}
\end{array}$$

Figure 4: Loop rules replacing while

For simplicity, let us agree upon (FOR) n denotes the number of iterations that is known before executing the loop, i denotes a new variable in P and Q . If i was not fresh, then another new variable name should be chosen according to all stacked variables' visibility scope. This issue is profoundly investigated to a full extent within the so-called "Numeral Logic in [204], [49]. So, (REP) may be transformed w.l.o.g. into (LOOP) and vice versa. However, in general, (FOR) should be transformed only unidirectional since for the opposite transformation, only a pre-calculated integer should bound the number of iterations which is often not the case, therefore (FOR) should then not be used. In the case of primitive recursion, it actually may not even be the case. An in-depth insight into generalised μ -recursions and termination issues with mutual recursion is best considered in [25].

A conditional branch operator is not considered separately because w.l.o.g. may entirely be replaced by (LOOP). Further reading on the minimalistic but complete PL "PCF" [209], [65] is recommended. The essential concept of simulating Turing-computable functions lies in a minimalistic set of program statements. The crucial difference between a simple statement and a loop is its body is repeated zero or more times, and assigned variables in the body change every time the body is entered. All variable dependencies need to be analysed to catch all modifications in a basic block (BB) until the loop exits. Often this requires a profound abstraction. Usually, this can be done manually only. Such an abstraction also requires auxiliary variables to be introduced to keep the invariant part of that body description smooth and straightforward. Therefore, the description approximates some general target function containing target variables (cf. fig.11), making up the loop invariant. The generation of an invariant often is not a trivial part and can often not be decided.

For this reason, a manual refinement of the invariant specification is vital. The postcondition of the loop considered represents an invariant. In analogy to a fixed mapping from projective geometry, when one point remains fixed, a loop invariant is an assertion that remains invariant regardless of how often the loop is iterated. The invariant formula Φ must obey $\Phi \circ Y = Y \circ \Phi \circ Y$, where Y is a fix-point combinator and \circ a binary function concatenation. Y is some syntactic notation simulating repetition. Its objective is to define some search minimum, widely used with λ -calculi (for more details, refer to [22]). Alternatively, but

equivalent w.r.t. expressibility, Kleene's μ -operator [79] may implicitly be applied to variables to be minimised, s.t. a predicate still holds.

Let us consider the example from fig.5.

```
a:=0; b:=x;
while b>=y do b:=b-y; a:=a+1; do
```

Figure 5: Code example for the remainder of two integers

Here, $a \cdot y + b = x^b \geq 0$ may be invariant since this equality describing the remainder on division by integer y does not alter. y is the divisor of $x \geq 0$, a an integer, and b is the remainder of x divided by y . The assignment rule (ASN) denotes: if a well-defined expression e is assigned to a compatible variable x , then before and after assignment, the state in P remains without changes. The state before assigning requires a variable binding extension, including x . In case of a name clashing, it is required to perform a renaming first in the specification.

Completeness depends on the completeness of Hoare triples of kind $\{P\}C\{Q\}$, which depends on complete coverage of C and all fully covered preconditions of P (cf. def.1.7). Postconditions like Q are logical consequences if met by P and C . Since verification rules may be applied in potentially any order they occur, the question arises: Can one rule accidentally or intentionally exclude or overlap any other rule? It can.

Nevertheless, the answer on how to decide to do this automatically does not seem too trivial. Naturally, if a given Q and given program statement C , different preconditions P_1 and P_2 are inferred, then this clearly shows the rule set is not sound. Besides correctness and completeness, according to the quality ladder from fig.1, optimality matters most. So, the question related to an effective rule set concerns compactness and simplicity as well. If the question is about automation, then the question of the chosen architecture is essential too. This section shows that the invariant generation may be tricky because an accurate and the most general conclusion requires all variables modified in the loop body and could include all referred variables in memory. Let us also pay attention to automatically allocated variables with a different scope than dynamically allocated variables. Moreover, it can be noticed the comparison between a given and expected specification may require some previously agreed formalisation, which enables us to decide equality.

2) Logical Reasoning: The rule ($P1$) from fig.2 represents the most general logical rule ever. Verification means a formalised process (see obs.4.8). A verification is either valid or not. For the latter, when execution is undetermined, it is the same as when the postcondition is not specified or a statement does not terminate. Otherwise,

verification is false. When applying rules, the antecedent may branch into several (sub-)verifications, which all need to be verified. Hence, any formal verification is tree-structured.

Definition 1.2 (Input Programming Language). A PL is a formal language whose words are programs consisting of statements. The execution of a program statement may alter memory (stack, heap). By default, a C-like imperative PL with object-oriented extensions is considered, though not C++ nor Peyton-Jones' C--.

An imperative language is selected for several reasons. C or Java are among the most popular PLs according to the TIOBE index, and why redefining apriori more and more new languages? If there is no need, then it would certainly be better not. However, the difficulty seems to decide whether this is the case or not. Second, in this work, a C-dialect is chosen to minimise primarily (re-)defining legacy syntax and semantics from a fragment of existing languages. Naturally, C is platform dependent – this seems to be a disadvantage. However, the dependency will be discussed further to get a qualitative judgement on this possible issue. The selected C-dialect is a subset of ISO C99 (cf. fig.73, see [306], [308]). As being PCF-compliant [209], it supports a basic while-loop, as discussed in fig.4. It supports object calculus type (1) according to fig.14

Definition 1.3 (Specification Language). Any specification language for dynamic memory considered here is formal. This language refers to variables and the input language's features, symbolic expressions, quantifiers and auxiliary program units for facilitating proofs. A specification language must follow apriori agreed formal logic. In contrast to an input PL, the specification language is of declarative paradigm, but indeed not of imperative paradigm (cf. sec.IV-A).

$$\frac{\frac{A_1 \quad \frac{\text{false (!)} \quad A_2}{A_3}}{B_1} \quad \frac{\text{true} \quad B_1}{B_2}}{B}$$

Figure 6: Example of a proof refutation

A specification language describes each BB of the associated CFG (cf. fig.11) the calculation state based on memory (see fig.25). Let us choose an arbitrary derivation tree from fig.6 with the assertions $\{A_1, A_2, A_3, B_1, B_2, B\}$. Initially, the Hoare triple B ought to be shown accordingly to def.1.1. Thus, the given rule is applied. The antecedent shall contain A_3 and B_2 , both of which need to be proven separately using respective replacements and strictly according to given rules, (e.g. local symbols), shall be generated using B as its consequent.

Furthermore, applying the rules, we show that B_1 is a precondition to B_2 and B_1 according to the rule is a

tautology, e.g. $\{n = 0 \wedge n \geq 0\}a = 5; \{n = 0\}$ whenever it becomes evident that a is not bound (but a free variable with n). Next, A_3 is proven. However, this would imply that A_2 contradicts itself. This condition is enough in order A_3 to derive to false and as such B to the same. So, we have just shown B is incorrect, and the reason for that lies in A_2 . In the example, there is no need to track further down the proof on A_1 , even if it is correct or not.

Definition 1.4 (Logical Consequence). A logical consequence $A \vdash B$ denotes an assertion A to which some given rule from a given axiom system is applied once. It leads to assertion B (according to Frége [263]). If B is obtained after rule application several times, including none at all, the consequence is noted as $A \vdash^* B$.

If we want to express that, a triple A is always valid under a given rule set Γ . Then we use $\models_\Gamma A$ if it is clear from the context that only Γ is considered or $\models_\Gamma A$.

Observation 1.5 (Proving as Searching). For a given rule set Γ a proof of some theorem B in Hoare calculus can be formulated as a search for axioms, so $\models_\Gamma B$.

First, we intentionally do so for the sake of a better understanding and approximation, not exclude possible inaccuracies in the rule set to be considered. For example, referring to Γ , we also refer to a formal logic, which consists of a closed set of dependencies regarding given rules and a carrier set and base logical constants. By default, we agree upon any arbitrary rule set used for logical reasoning. We insist on a well-defined and sound Hoare calculus with triples according to def.1.2 based on def.1.4. This observation is a precursor to syntax definition as proof (see thes.6.11).

Definition 1.6 (Soundness of a Hoare Calculus). A Hoare calculus is sound whenever cases are guaranteed to be excluded when a syntactical sound program C with a rule set Γ derives (semantically) different results.

If for one valid logical reasoning results in B_1 , and another valid reasoning results in B_2 , although neither of which may derive from the other, then Γ is not sound. This derivation is denoted as $\{P\}C\{Q\} \vdash^* \{P_1\}C_1\{Q_1\}$ and $\{P\}C\{Q\} \vdash^* \{P_1\}C_2\{Q_2\}$ where $\{P_1\}C_1\{Q_1\} \not\vdash^* \{P_2\}C_2\{Q_2\}$ and $\{P_2\}C_2\{Q_2\} \not\vdash^* \{P_1\}C_1\{Q_1\}$ (see fig.7).

The theorem just formulated upon a Hoare calculus is often called diamond-property due to its shape and originates back to rule-based rewriting systems and λ -calculi [22]. That theorem goes back to Church-Rosser, hence called CRT (see [203]). If at least one assertion whilst reasoning may result in ambiguity, then the entire rule set Γ is not sound (see def.1.7). Proof confluency — a severer restriction than soundness, is not always obeyed in practice, for instance, due to general non-decidability on the grounds of non-termination (see [247]). Soundness is a required precondition to confluency. If some

calculus is not sound, then at least one case exists, so two or more different results may be derived — and that is certainly not correct. According to Steinbach's [247] term rewriting system [19], decidability on termination strongly determines confluency. This outcome is a bold statement. He represents logical rules as term rewriting rules and uses bound partially sets to prove termination of his newly obtained rewriting system. However, that system does not work for all cases since termination is only semi-decidable due to foundational limitation. It can be noticed that the approximation of an upper bound for the reasoning is in general not bound due to self-application or to recursive symbolic terms [207]. The idea of a descending poset chain is strongly intertwined with Domain Theory's concept [236]. Steinbach applies poset chains for determining the least upper bounds on rule sets to decide termination, which is a precondition to soundness.

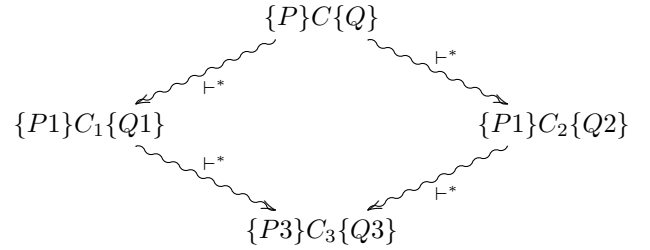


Figure 7: Church-Rosser theorem applied to Hoare triples

Cook [67] investigates both, soundness and completeness of Hoare calculi as competing quality measures. It is worth remarking that tiny changes towards one objective may heavily change the other objective, for example, in modifying variables in procedures. Cook's sense of completeness is the full coverage of some function's domain, so a total mapping of all input programs, including those earlier mentioned in [15]. "Soundness" is defined as an equivalence between observed and expected behaviour as recommended by [79], [189]. There it is defined by operational semantics over Hoare triples. Abstract automata then interpret calculations. A convenient solution by Cook means either a complete or a sound calculus. His propositions to overcome some imperative input PL restrictions are supposed to back the objective up, such as:

- Restriction 1 Global variables are allowed. However, it is strictly prohibited to pass them to procedures as actual parameters.
- Restriction 2 Parameters by call (or by reference) are forbidden.
- Restriction 3 No recursive procedures and no functionals (higher-order functions).

As some of those essential restrictions may come as a surprise (but they undoubtedly exist after all), how can disobedience of those lead to unsoundness or incompleteness, since those restrictions must be taken

into consideration when designing a PL most fit for a heap verification? A classic stack requires parameters by-reference to address where to return once a stack window is fully processed. As soon as a return is initiated, all existing local variables stop existing. A pass by reference allows altering a unique content at different places among the stack windows, but the pointer to an object may change during a subroutine call. If we permit parameters by call or recursive functions, then data may alter but not how the stack is processed on calls. For example, globals may alter almost everywhere. In such cases, "naïve" specifications may quickly become invalid in general. Invalidation may be excluded by restricting input and output parameters to a procedure. Hierarchical specifications [235], [37] may blow up specifications. Moreover, since those specifications may occur anywhere in a program, the use of finer-grained specifications might diminish quickly to nought, just because the program's location may dramatically change and expand even more level. Consequently, the depth of those nested specifications increases too. So, in the end, finer modularity may become useless in practice. For example, built-in procedures would need to be fully specified. Furthermore, objects may lose their identity and closure because passing a procedure as a parameter may finally lead to unpredictable behaviour towards a class-objects memory layout.

Clarke [62] outlines only limitations still a problem to date w.r.t. Hoare calculi. Rigid constraints refer to:

- Restriction 4 Expressibility and completeness of the input PL
- Restriction 5 Loop invariants (e.g. transformation)
- Restriction 6 Recursive procedures which do (not) use globals and static variables
- Restriction 7 Co-procedures as input and output parameter to a procedure
- Restriction 8 Dynamic allocation and deallocation (also see [215])

Both Cook and Clarke understand guarantees under soundness, s.t. all syntactical sound theorems derive correctly and all unsound theorems false. As any formal system, Hoare calculi underpin theoretical limitations. For example, one can always define different theories on integers which will eventually be sound but cannot be proven under the surrounding proof facilities if, e.g. certain axioms are modified or dropped. This phenomenon is better known under Gödel's incompleteness theorem. Clarke notices as Cook before him that if a Hoare calculus contains a non-terminating cycle, then there must be a (mutual) recursion in the rule set. He suggests banning aliasing pointers (see later), and for the sake of soundness to ban unbound recursion. Clarke's problem may be relaxed if substitution rules in the Hoare rules are applied from outermost to the innermost direction (this

corresponds to lazy evaluation). At the design level of a PL as an input language, exactly this evaluation order should be taken into account, ideally.

PLs with strict evaluation, like OCaml, in contrast to non-strict languages like Haskell, should ideally extend its parameter passing method and ABI. According to Clarke, expressibility always primarily refers to the assertion language, which can be noticed from his work effectively. Restriction 6 on recursive procedures may be excluded in two cases. (i) When recursion steadily terminates, so a descending chain always exists [247]. (ii) parameter passing ordering and parameter type checking [55] on a procedure call must always precisely match between caller and callee, and variables from the current stack window shall permanently be excluded, so non-global and non-static variables, for instance.

Kaufman [134] considers expressibility and practical need as the most critical problems that hinder a popular currently vital break-through of formal verification based on Hoare calculi, especially w.r.t. specification and PL. He sees in induction and abstraction the single most potent verification techniques. To distinguish better between a calculation error committed by an input program and an inaccurate specification, he urges a most generic method for constructing counter-examples automatically. His motivation is to automatically also derive a concrete example as a counter-example for better understanding and faster troubleshooting.

Gerhart [104] compares existing tools to that time, which today are still not resolved nor resolved satisfactorily. To name the most important open problems:

- 1) Lack of generalised approach in decidability of program termination
- 2) Support for distinct variable modes (like static, globals, cf.[62])
- 3) A handy usage and generalised IR of all components of a verification system

She notices inductive definitions are an exemplary apparatus to numerous issues simultaneously, e.g. with problems on expressibility. A further insight makes one agree with Gerhart's remark in practice. Gerhart insists on simple proofs must primarily refer to universal and global assertions. From [62] also follows that problems from (ii) are defying and of global nature, and it can hardly be believed that a tiny modification in a Hoare calculus will suddenly allow a solution.

Definition 1.7 (Completeness of a Hoare Calculus). According to its rules, a Hoare calculus is complete whenever syntactically well-defined program soundness can be shown, and unsoundness of not well-defined programs can be rejected.

In case of lack of at least one rule till termination, the calculation is considered incomplete and the verification in total undetermined. In practice, a tiny modification in an (input) program (or specification) may already

significantly change a program's behaviour [62], [67], [68]. Not surprisingly, this can happen and witnesses a high complexity of the verification has to take into consideration. Example 1: According to restriction 6, the absence of static variables and recursive procedures can still lead to a complete program, which depends on the program fragment is considered. Example 2: The completeness of program verification with internal procedures is violated whenever restriction 6 or restriction 7 is violated. Whenever two rules lead to two different results, state A implies $A \vdash B_1$ and $A \vdash B_2$, where B_1 and B_2 are syntactically different, but the diamond-property is obeyed from fig.7, then B_1 and B_2 denote just intermediate states and both states confluence. From a practical perspective, a full confluency check may, in general, become quite complicated due to the exponential rise of the number of sub-verifications to be performed. This problem may significantly be reduced by determining all rules. Clarke also advises imposing the following restriction in order to fight incompleteness:

- Restriction 9 Introduction of partially-computed data-structures.

For partially-computed (possibly infinite) data structures, all fields are calculated only on accessing those (this is a lazy evaluation). An example is taken from [255] in Haskell and deals with linear lists.

```
take 10 [ (i,j) | i <- [1..], let k = i*i, j <- [1..k] ]
```

, which computes

```
[(1,1),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(3,3),(3,4),(3,5)].
```

However, this linear list definition, as take's second argument, does not have an upper bound. The obtained data structure only has a lower bound (the integer 1). Thanks to the partially-computed data structure, a procedure's termination behaviour to be investigated on each occasion individually may finally terminate in case of non-strict evaluation. "strict" means a given procedure evaluates all incoming parameters first and only then starts to store to memory. Non-strict procedures mean incoming procedure parameters are evaluated partially and only if needed in the current algorithm (see [256], [255]). Thus, for instance, termination may be checked using a potentially infinite input data structure as a quick test.

Wand [265] understands under a complete function the same as Cook does. Namely, every sound input parameter corresponds to a sound output parameter, and that every unsound input parameter corresponds to an error. The transition function between input and output parameters must be total and non-termination apriori excluded (see def.1.6). Wand shows that when a program's specification is represented immediately by a CFG, then the specification may not be complete in general or just not always defined properly whenever higher-order predicates are used. Wand urges quantified

predicates used in specifications must give an intuitive explanation in the best way possible, s.t. a human reading that specification has a full understanding of the predicate and its dependencies immediately.

Cook [68] compares the SAT-problem of boolean functions with theoretical estimates on associated problems of formal verification. The paper gives an overview of the theoretical complexity involved. From a practical point of view, this paper, unfortunately, is futile for two reasons. First, the established levels are too coarse and, therefore, cannot be helpful in practice. Second, the paper's main objective seems to be epistemological rather than have concrete results that could be applied in practice, not even as a design recommendation for future projects.

Landin [152] suggests turning formal calculi elements in an expression containing λ -terms as it was proposed initially. A Hoare calculus is indeed a formal calculus. Landin demonstrates, by example, conditional branches and recursion are tractable and tractable elegantly. From a computability perspective, this is already sufficient. Moreover, he shows, functional programs [255], [35] may be represented in an imperative program with the help of "closures" which are well-founded on operational semantics. Generalised models of computation are presented that attract Hoare calculi as well.

The best practices in verification in Hoare calculi gained over past decades is carefully analysed by Apt [15] towards soundness and completeness of a C-like dialect and with nearly minimal modifications on all aspects considered, mainly procedures and variable modes. In addition to all reviewed papers, Apt sees general recursion as the central issue in divining the matching calculation state of an executed program w.r.t. specification. Hence, he suggests restricting ourselves to primitive recursion whenever possible to reduce the overall verification complexity. Also, Apt recommends restricting procedure calls to those in which actual and formal parameters match and in which so-called "incorrect" parameters are excluded because those can lead to a series of anomalies. Harmless looking program features were proven wrong and therefore are suggested for a ban: for example, uninitialised fields, functionals gained by undermined parameters can even totally change a function's semantic and syntax but at the same time does not extend expressibility in its foundation.

Cook [67] and authors already consider two problems as the most important:

- Completeness 1 Procedure Non-Termination.
- Completeness 2 Expressibility restrictions in the assertion language (for instance, predicates and invariants).

A sound and complete example is chosen in fig.8 to discuss modifications and their effect on completeness and soundness. A_j denotes program statements, D denotes a declaration block of local variables, σ denotes a variable

environment and \star denotes Kleene's star. σ is of type "*variable name* \rightarrow *value*".

$$\begin{array}{l}
\text{(VAR)} \frac{P \ y/x\{begin \ D^*; \ A^* \ end\} \ Q \ y/x}{P \ \{begin \ new \ x; \ D^*; \ A^* \ end\} \ Q} \\
\\
\text{(SEQ)} \frac{P > R, \ R\{A\}S, \ S > Q}{P\{A\}Q} \\
\\
\text{(ITE-1)} \frac{P\{A\}Q, \ Q\{begin \ A^* \ end\}R}{P\{begin \ A; \ A^* \ end\}R} \\
\\
\text{(ITE-2)} \frac{}{P\{begin \ end\}P} \\
\\
\text{(CON)} \frac{P \ \& R\{A_1\}Q, \ P \ \& \neg R\{A_2\}Q}{P\{if \ R \ then \ A_1 \ else \ A_2\} \ Q} \\
\\
\text{(ASN)} \frac{}{P \ e/x\{x := e\} \ P} \\
\\
\text{(CALL-2)} \frac{p(x : v) \ proc \ K, \ P\{K\}Q}{P\{call \ p(x : v)\}Q} \\
\\
\text{(LOOP)} \frac{P \ \& \ Q \ \{A\} \ P}{P\{while \ Q \ do \ A\} \ P \ \& \ \neg Q} \\
\\
\text{(PAR)} \frac{P\{call \ p(x : v')\}Q}{P \ u, e/x', v' \ \{call \ p(u : e)\} \ Q \ u, e/x', v'} \\
\\
\text{(CALL)} \frac{P\{call \ p(u : e)\}Q \quad \text{where } \sigma = z'/z}{P\sigma \ \{call \ p(u : e)\} \ Q\sigma} \\
\\
\text{(PROC)} \frac{D, \ P\{begin \ D^*; \ A^* \ end\}Q}{P\{begin \ D; \ D^*; \ A^* \ end\}Q}
\end{array}$$

Figure 8: Example of a complete and sound rule set taken from [67]

In addition to restriction 6, a further restriction remark shall be noted:

- Restriction 10 Non-automatically allocated variables

As mentioned earlier, the introduction of global, static and dynamic variables may invalidate rule sets in Hoare calculi. Moreover, locals in multi-threaded applications may also invalidate rule sets because parallel execution (thread-local variable mode) are not considered by Cook. This work is dedicated to single-threaded execution only.

For a fully-fledged industrial use, additional language features would be required not yet considered and not in the next future, namely, exceptions that seem to disintegrate with any Hoare calculus (Clarke mentioned). So there is no wonder why a sound and incomplete rule set integrating exceptions may be challenging since the stack would have to behave fundamentally different when invoking program statements inside a try-catch block,

for instance (see [84], [107]). Up to date, not a single proposition was made in terms of a Hoare calculus allowing a sound or/and complete stack rewinding that would include, for example, dynamic variables [107].

Hoare [116] considers abstraction the essential verification technique, especially for young engineers who are new to verification and would like to play with some simple examples for the beginning. From Hoare's original work, it can be implied that "goto" labels, unconditional jumps and passing parameters by name are hard to formalise. Hoare does not speak in favour or against higher-order logics. However, he sees a declarative assertion specification as a pivotal element to success for all kind of Hoare calculi in general.

3) Automated Reasoning: This section aims to introduce and briefly illustrate theoretical problems on proof automation. In this section, examples with the theorem prover Coq are considered. Coq [32] can prove previously specified assertions by theorems, different kind of inductively defined structures and commands based on the typed λ -expression calculus of second order. Assertions are specified in the functional PL "Gallina". Proofs are specified in the command language "Vernacular". Coq often cannot independently search for proofs automatically. It is a proof assistant that helps the user debug and record proofs. Coq has a core asset of theories, e.g. on integers or floating-point numbers, which may swiftly be loaded to the verifier core as modules. The proof assistant allows tracking and record-keeping proofs and finds out intermediate proof states.

The sequence of recorded proof commands may manually be enriched by tactical commands (short for "tactics"). Tactics try to apply several default proof steps, including normalisation and simplification, at once in order to reduce or even bring the current proof to the desired goal to be found. Coq is a rare, compelling and widely accepted proof assistant platform. Successful applications include compiler phase verifications [225], [157], [41], [42], [158], [159], [215].

Formulae based on predicate logic are specification expressions.

Definition 1.8 (Logical Formulae in the First-Order Predicate Logic). A formula Φ in first-order predicate logic is defined as

$$\Phi ::= true \mid false \mid x \mid REL(f(\vec{x})) \mid P(\vec{x}) \mid \neg\Phi \mid \Phi \circ \Phi \mid \forall x. \Phi[x] \mid \exists x. \Phi[x]$$

where x is a boolean variable, f is a functor, P an assertion predicate, REL a relation having term arguments (relation), and \circ is logical conjunction, or operator, or disjunction. Vector \vec{x} defines a term vector, which by default contains components regardless of which context they are. It is assumed formulae containing quantifiers bind free occurrences of x in Φ .

Coq makes use of normalised formulae on reduction.

These formulae may become undetermined or partially determined as the calculation proceeds. Coq's proof schemas are founded on lazy reduction equivalent to the second-order λ -calculus (see [55], [203], [179]). Because rules may be arbitrary at their definition, completeness is not guaranteed. Typing given λ -expressions in Coq, as is by default, avoids antinomies that would otherwise arise due to inductive definitions over Cantorian sets (cf.[22], [34]), e.g. self-applicable terms. The absence of typing leads to typing ambiguities related to paradox.

Definition 1.9 (Terms $T_{\lambda 2}$). The type $T_{\lambda 2}$ is a set in second-order λ -calculus types and is defined as

$$\begin{array}{ll} t \in T_{\lambda 2}, & t \in V \\ (t_1 \rightarrow t_2) \in T_{\lambda 2}, & t_1, t_2 \in T_{\lambda 2} \\ \forall a. t \in T_{\lambda 2}, & a \in V, t \in T_{\lambda 2} \end{array}$$

, where V denotes the set of variable symbols, \rightarrow denotes type application. Examples of sound $T_{\lambda 2}$ -types include, for example, $\forall a. a$ or $(\forall a_1. a_1 \rightarrow a_1) \rightarrow (\forall a_2. a_2 \rightarrow a_2)$.

Definition 1.10 (Set of $\Lambda_{T_{\lambda 2}}$ terms). $T_{\lambda 2}$ -terms $\Lambda_{T_{\lambda 2}}$ are defined as

$$\begin{array}{l} \Lambda_{T_{\lambda 2}} ::= V \mid \\ \Lambda_{T_{\lambda 2}} \Lambda_{T_{\lambda 2}} \mid \\ \lambda x : t \in T_{\lambda 2}. \Lambda_{T_{\lambda 2}} \mid \\ \Lambda x. \Lambda_{T_{\lambda 2}} \mid \\ \Lambda_{T_{\lambda 2}} t \in T_{\lambda 2} \end{array}$$

, where $\Lambda x. t$ denotes an abstraction of term t by some variable $x \in V$. Sound definitions may be $\Lambda_{T_{\lambda 2}}$ -types, such as $\Lambda a. \lambda x : a. x$ or $\lambda x : (\forall a. a \rightarrow a). x (\forall a. a \rightarrow a) x$. Reduction (β -reduction, see [22]) of λ -terms is an application of a possibly undefined term to a given λ -abstraction. For example,

$$(\Lambda a. \lambda x : a. x) \text{ Int } 3$$

can be reduced to $(\lambda x : \text{Int}. x) 3$, which finally reduces to "3", where Int denotes integers (equals V from def.1.10).

The objective of reducing $T_{\lambda 2}$ -terms is: (1) evaluate a final result and (2) type checking. Type checking differs from verification by the absence of the meaning of a state and expressibility limitations.

Definition 1.11 (Type Checking). Type checking (after Hindley-Milner [115]) of a term e having type t for a given rule set Γ is noted as $\Gamma \vdash e : t$.

The type of a term is checked by structural typing rules and further by reduction rules for a given formal theory (skipped here):

$$\begin{array}{l} (\forall\text{-Intro}) \frac{\Gamma \vdash e : t}{\Gamma \vdash \Lambda a. e : \forall a. t} \\ (\lambda\text{-Intro}) \frac{\Gamma, x : t_1 \vdash e : t_2}{\Gamma \vdash \lambda x : t_1. e : t_1 \rightarrow t_2} \\ (\forall\text{-Elem}) \frac{\Gamma \vdash e : \forall a. t}{\Gamma \vdash e \ t' : t[a := t']} \\ (\lambda\text{-Elem}) \frac{\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 \ e_2 : t_2} \end{array}$$

For the sake of simplicity, in the definition, base rules are skipped because universality allows them to define more generalised and in non-typed λ -calculi (see [22]). For instance, the axiom $\Gamma \vdash x : t$, the rule $(\exists\text{-Intro})$ or $(\exists\text{-Elim})$, can be defined in analogy to $(\forall\text{-Intro})$ or $(\forall\text{-Elem})$.

Since Coq bases on $T_{\lambda 2}$ and redex reduction goes from outermost to innermost, type checking becomes decidable. The checking complexity is linear. For reductions from innermost to the outmost, type checking is in general undecidable (cf. [203], [32]).

Let us recapitulate the previously said with fig.9. For example, the tautology $p \vee \neg p$ seems intuitively straightforward, but when the Tableaux method is absent and when implications only may be used to reason, any successful proof may become anything than trivial — so it is with an intuitionistic judgement attempt here. Depending on the rules chosen, Peirce's tautology may become impossible or hard to prove, as shown in fig.9 facilitating a Coq-proof.

Definition peirce := forall (p q: Prop), ((p->q)->p)->p.

Definition lem := forall p, p \vee \sim p.

Theorem peirce_equiv_lem: peirce <-> lem.

Proof.

unfold peirce, lem.

firstorder.

apply H with (q:= \sim (p \vee \sim p)).

firstorder.

destruct (H p).

assumption.

tauto.

Qed.

Figure 9: Peirce's theorem about the excluded third in Coq

We need to prove the first definition "peirce" can turn into the definition "lem", where "peirce" may not contain disjunction nor negation but may contain implications of a kind \rightarrow . Let us pay attention to both definitions contain quantified assertions. Any recorded proof would be a sequence of proof commands in Coq. Any sequence would start with the keyword "Proof" and

finish with the keyword "Qed" (short form of "quod erat demonstrandum", which translates into "what was to demonstrate"). Initially, there is only the equality of both theorems to be shown. Then both sides of the equality are unfolded. The latter "first-order"-keyword tries to replace \forall -quantified assertions into Skolemised normal-form. We need to show on the right-hand side of the definition "lem" for any true proposition " p ": $p \vee \neg p$ holds. In this case, the left-hand side is a provable hypothesis $H = \forall p, q. ((p \rightarrow q) \rightarrow p) \rightarrow q$, which must be shown for any propositions p and q . Now, $p \vee \neg p$ is replaced by p , and q is replaced by $p \vee \neg p$. Thus, we obtain $(p \vee \neg p \rightarrow \neg(p \vee \neg p)) \rightarrow p \vee \neg p$ as a hypothesis to be proven still under the condition that p holds. The consequence of "peirce" must be separated from its precondition in order to prove the hypothesis. It is required to abstract the hypothesis and then skolemize it to normal-form, s.t. q is no more quantified. Now we obtain another more comfortable hypothesis, $H_0 = (p \rightarrow q) \rightarrow p$, which can prove if we assume $H = \forall p. p \vee \neg p$, s.t. the right-hand side of the disjunction holds. So, we introduce a new hypothesis, $H_1 = \neg p$. Such a choice is arbitrary, and once applied $\neg p$ to H_0 , we immediately find p holds because the remaining implication always holds as soon as the left-hand side of the implication is false. Since we assumed p holds initially, we have just confirmed the theorem holds. The tactic's application helps them prove to accomplish since simple mechanical normalisations are sufficient to quit the proof successfully.

Although this example is intuitive and candid, proofs still require extra-ordinary resources and are not intuitive whatsoever, for example, the definition of intermediate normal-forms and hypotheses.

The application of tactics is no guarantee at all. Tactics do not recognise non-obvious abstractions. It is not hard to notice that automating this kind of non-standard transformation must eventually fail and most likely not even be recognised in the first place.

Definition 1.12 (Formal Proof). A proof is a sequence of applied equalities (rules and axioms) applied to a given theorem based only on valid axioms.

Remark: If Hoare rules (rules of some Hoare calculus) are complete and proof exists upon defined axioms, proof can be automated. If rules are complete, then any valid theorem may be proven within the considered context (w.r.t. exceptions related to Gödel's incompleteness theorem). Semiotics, syntax (e.g. see def.1.8), and semantics must be defined to express some formal theory. Whenever languages are meant, not only a formal theory is determined by expressions, but also the pragmatics of that language shall be defined. Semantics, e.g. axiomatic semantics, decide which meaning is derivable from a formal system or not, particularly by a Hoare calculus. Signs and the interconnection between formulae are abstractions of some tangible object representatives or physics. Hence,

for historical reasons, meta-physics often replace physics. An abstracted physics, or logics, whenever not a factual matter is meant, but properties about them indeed – as is the case with Hoare calculi describes program properties. It must be noted that any formal logic is also, by definition, formal algebra.

In analogy to modular programming, proofs may be composed to simplify and strengthen the essential thoughts from a designer's perspective. A more formal definition is given in the coming sections.

For analogy purposes, the units used in a proof are lemmas (are auxiliary theorems), theorems and inductive definitions. The simplest example of inductively defined sets are natural numbers (see fig.10).

Inductive nat : Set := O : nat | S : nat -> nat

Figure 10: Inductive Coq definition of Church's numbers

Since tactics are arbitrary sequences of verification commands, we will not consider these in more detail here. They are just like macros, just another modular unit.

In contrast to that, predicates' abstraction has a definite practical meaning: the more straightforward a proof is, the better. Symbols and predicates may be unfolded by need. Facing the current situation and accompanied rules leading to proof would be highly recommended to automate the quest. One essential question remains: When to fold and when to unfold an inductive definition, how often may this be required? Unfortunately, the practice taught us a lesson that may be challenging to decide and is almost impossible to predict on an automated schedule. Due to the reasons mentioned earlier, it is better to reduce terms lazily and in outermost-to-innermost order. Otherwise, the proof may suddenly stop unfinished even if `redex(es)` still exist.

Observation 1.13 (Verification Model of Computation). Verification units remind one unit (or modules) in programming. Lemmas correspond to procedures. The main theorem to be proven corresponds to the main-function of a program.

From fig.9, the following problems may be derived:

- 1) A description of a problem competes with its expressibility. This race can lead to severe expressibility limitations and bloated descriptions.
- 2) Often, a simplification of equalities of a related theory (e.g. integer theory) bloats the amount and complexity of the significant theory (e.g. theory on dynamic variables). Although, e.g. an arithmetic theory is not directly related to memory layout or any specific programming statements, this can also be considered a significant hinder to prove automation.
- 3) On proof refutation, a reasonable explanation desires better or is absent. Counter-examples as expla-

nations, if any, are not intuitive and not general enough.

Wos [280], [279] gives a more detailed explanation of automated theorem proving regardless of age. The problems Wos addresses can be categorised into three classes: (i) assertion model representation, (ii) logical rules representation, and (iii) choice of optimal proof strategy and tactics. Wos suggests parallelism, data/knowledge base indexation, and considering modified reasoning techniques to raise proof efficiency. A more in-depth analysis of articles related to Wos' remarks, the following can be summarised:

- Type checking is helpful to avoid static analysis errors at an earlier stage. However, its use beyond that stage tends to be, in fact, nearly zero.
- The actual formula notation is not essential as long as the program semantics (of an imperative program) is caught.
- Even if Robinson's resolution method is widely discussed in Wos' contributions, the Natural Deduction can be considered more important when it comes to verification in Hoare calculi, presumably due to the proximity to definitive proofs from classic math proofs and is therefore preferred.
- Competition can be witnessed in proof searches between local and global optimal values.

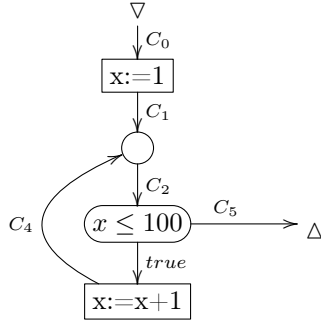
Wos [280] supersedes all others from all problems, namely the need to strip bloated formulae in specifications and repetitions from verification descriptions. Wos's motto is: "It is better to simplify assertions than to analyse all different variants". Nobody can disagree with such a position. Wos's heuristic suggests applying simplifications at most with a polynomial complexity in the worst case rather than risk an exponential rise in search space. Wos expects a reduction of approximately 90% on average. Preston [212] refers to Wos [279], expecting good research on all of Wos' raised issues will eventually fill a PhD thesis each, especially since not much work concentrated on those topics. Overbeek [191] refers to Wos too. He provides for each of Wos' issue at least one concise practical example. Mackock's [165] contribution may seem old, but the addressed issues are close to Wos' and are, nevertheless, still up to date. Gallier [102] is a more recent monography on automated theorem proving. The issues he raises are mostly congruent with Wos'. Leroy [160] questions the overall verification process altogether. He provides critical measures from a practical view. His remarks are heavily covered by the mentioned. He, Appel and Dockings [14] give the prover developers and researchers recommendations to obey common principles they suggest for prover development so that researchers can compare existing provers years later, mainly focusing on rule categorisation.

Abstract Interpretation. The Cousots [74], [73] suggest

for the first time a formal method (see def.1.12) a universal static code analysis based on approximation of stepwise interpretation calculations for a given program. The method analyses a CFG (cf.[189]). If the CFG cannot be normalised (e.g. no unique entry or exit), it is normalised, e.g. by adding auxiliary uniting nodes. The program statements are partially ordered in a non-strict way according to an algebraic lattice in the order of the operator's appearance. Abstraction helps to approximate the limit [6] by introducing new dependent parameters using bound intervals (narrowing down visibility interval) and by analysing the most common interval (widening visibility). Thus, uninitialised variables are assigned the interval $-\infty$ to ∞ . Stepwise approximation of interpretations terminates as soon as two consecutive steps yield the same result. Interpretations renew after each program statement. Due to the Halting problem, interpretations may have unpredictable, so arithmetically huge limits. Alternatively, limits might be tiny, for instance, when entering a loop with an apriori undetermined value. Static evaluation of allowed array bounds [189] is a classic application for it. The family of methods may be altered and applied to very different applications, for instance, in [252] for an optimised branching based on heuristics in compiled code. In order to compare two interpretations, an isomorphism over mappings can be defined. Two interpretations, I_1, I_2 , are considered isomorphic, iff two mappings α, α^{-1} exist that are injective, surjective and for which I_1 maps onto I_2 by using α , and I_2 maps back onto I_1 by α^{-1} . Even if Cousots' method is universal, it still lacks restrictions that would allow proof automation for many reasons. First, the approximation proposed mismatches the exact nature of Hoare's calculus and the exact symbolic values. One could consider Hoare calculus as a singularity of Cousots' method. However, their method focuses, after all, on arithmetic approximation. Second, within a Hoare calculus, verification bases on terms and assertions, a specification language, and so forth – this all is not the case with Cousots' method. A commented example for their application can be found in fig.11.

Steinbach [247] illustrates termination as a firm criterion, even a precondition for proof confluency (e.g. applying the Knuth-Bendix algorithm) and completeness. Termination may be decidable in some instances.

Apart from the mentioned restrictions, another theoretical restriction exists, dating back to Presburger's arithmetic. Presburger's arithmetic is a real subset of Peano's very popular arithmetic on natural numbers. Peano's arithmetic only knows "+" (or its inverse operation "-") as an operator [244]. This discrete structure leads to usual incoming programs containing a "+" that may be decided in a finite amount of time in first-order predicate logic (e.g. when calculating object offsets, see sec.III, sec.IV). However, this cannot be generalised for expressions under Peano's arithmetic or its extensions. No-



$$\begin{array}{ll}
C_0 = [,] & C_3 = C_2 \cap [-\infty, 100] \\
C_1 = [1, 1] & C_4 = C_3 + [1, 1] \\
C_2 = C_1 \cup C_4 & C_5 = C_2 \cap [101, +\infty]
\end{array}$$

The method assigning assertions to a CFGs was first proposed by Floyd [97].

Figure 11: CFG with assigned intervals

tably, this is of interest for automated proof resolvers [69], [61] (see obs.1.13). Expressions in Presburger's arithmetic are decidable with complexity $\Theta(m, n) = 2^{2^{n \cdot m}}$, where n denotes the minimal amount of search branches and $m \geq 1$ is some constant factor (see [95]). It can easily be noticed complexity raises fast for incrementing n . It is also important to notice that ignoring the expressibility of Presburger's arithmetics, e.g. including further operators, may cause in practice non-decidability in certain cases. However, obeying Presburger arithmetic axioms will dramatically reduce the upper bound for theorems to be proven.

Pommerell [210] evaluated theoretical complexity and finds ineffective implementations of related formal theories in theorem provers is the biggest hinder in an overall verification barrier. For example, he demonstrates encoding as huge matrices to be solved rather than ineffective, despite scarce matrix algorithms. The situation can be overcome when applied theories can be separated from the core verification rule set. It is recommended to use SMT-solvers instead, which ease tension w.r.t. completeness issues and further structural rules. Practice shows [188] solvers may significantly improve the resolution of related theories. A solver could be initiated whilst verification by need. Those solvers include "Why" [272], which is, in fact, a functional PL or its successor "Y-not" [187].

4) Alternative Approaches: As mentioned at the beginning, verification is a formal method that checks if a given program follows a given specification or not. Verification of Hoare triples is a static method that does not require the given input program to be run. It is worth noting that reducing the rule set may always happen

when rules are unified, generalised or both. Apart from verification presented earlier, other approaches like Static Analysis or Model Checking or localising problems based on stripping syntactic and environmental code. Other approaches exist, e.g. dynamic approaches like AT, bug-free development (hypothetical), and static approaches like some type checking.

Approach 1 — Testing. AT is a dynamic attempt in checking cases that used to be problematic or are suspected to be such. AT checks whether a specified scenario is calculated correctly by a program or not with an expected result. Scenarios are implemented as test cases by the test developer. Each scenario should be minimal and self-containing. One or more tests are associated with a function that all need to be successful to state anything about quality. As soon as at least one test fails, the overall testing fails. When a testing scenario is known, all input and output data is specified and then compared. If a test requires manual interaction, then the test is not automated. Automated tests significantly contribute to software development as they minimise risks on each stage of development since there is always one step back possible to find a potential code modification that broke the system. Automating Testing (AT) [24] yields significant advantages: high efficiency, so for a short period, a considerable amount of tests may be checked. So, errors based on incorrect or fuzzy input data may immediately be detected. If a scenario requires many objects involved, this could indeed happen but would require explicit specification. If tests are simple, then modules can easily be understood, and the risk for errors is lowered. Ideally, each test specification is simple. If not, this is always a reason to believe something is over-engineered or error-prone — this comes from practical experiences.

For a given program p and a test asset $\forall i. t_i(p)$, each test is launched for p , and results are observed. A disadvantage of AT is the manual test setting which can be pretty challenging, especially when the CFG is getting complex per p . The number n of needed tests p_1, p_2, \dots, p_n to cover all test branches rises exponentially. The more complicated a CFG gets, the more edges linking back to higher BBs it contains, the more tests are needed, and the more complex tests will get in general.

Approach 2 — Automated Model Checking. The main problem of approach 1 is the exponential rise in test cases needed, which is hard to automate to get a representable amount of tests. The idea behind Model Checking lies in a formula describing a given program using assertions and temporary expressions, which are checked stepwise. The problem is to find a solution for the discrete formula depending on multiple (logical) variables systematically. If the formula is probed too detailed, the AT will not even terminate within a long period. If, in contrast, the formula is analysed only superficially, then the result will be useless. The responsibility of certain constraints as

equalities is to direct Model Checking. If equalities are too much restricted, then results may be skipped. If equalities are too generous, then results may be skipped too. If there are too few restrictions, AT may take too long or find too many possible unimportant problems first. An ineffective search strategy might be equivalent to non-termination or an avoidable, very slow model checking [143]. Several modifications can be exploited for higher performance or expressibility, namely introducing formulae [63] or static methods deciding which part of the model formula to be tested in more detail next based on heuristics [148]. Implementations include VDM++ [271], [270].

So, effective alternatives to Hoare-based verification are AT [167], Model Checking as introduced first by Peled and Clarke [63] ([147] [270] give an actual review on recent tools). The advantage of testing in contrast to Model Checking is its simplicity and execution without explicit formulae, but the problem of a full test specification and execution every time whilst software development is required.

Approach 3 — Bug-free software development.

Naturally, bug-free software development has only advantages and resolves all other problems presented and, most importantly, does not require verification at all. After all, this is only a dream since humans make errors. However, model-based software development approaches try to exploit the minimal distance between a design blueprint and an actual reference implementation – this difference would be much easier to check, and patterns seem to have a single significant impact on this [136]. As long as the number of reported errors is tiny and (or) mainly related to minor issues, e.g. regarding performance in non-critical code areas only, then the overall number should approximate zero over time. Another crucial observation is that the shorter a program gets, the smaller the number of committed errors are on average during the development process. A program with zero lines has guaranteed zero errors – this natural law always holds independently from a concrete implementation and does not require further explanation: an empty program has a minimal number of errors, full-stop. Humans always introduce errors, and by the nature of programming – this will not be avoided regardless of how strong we try to. Even if a program was perfect, it might be the specification then which might be not accurate, and as a consequence, both parts require corrections. Humans do debugging and error localisation, and it cannot be fully automated. Abstract data types (ADT), algorithms and intuition, in general, are all human reasoning too. The software development process, module description and interfaces are all defined by humans. So, defining a brand-new, fully automated approach (even with a very high level of artificial intelligence involved) will still not be feasible by computer software only.

Software Development. The developer should think

about robust and at most error-free design and stability issues at an early stage supported by the modelling language UML and its extension OCL. The practice has shown on multiple occurrences that proper modelling can avoid crucial design flaws and keep expenses low when it comes to maintenance or new feature implementation. Unfortunately, not all issues can be resolved apriori, and this is why:

- Every developer is an individual, software development. After all, it requires creativity, and many skills computers currently cannot be done yet.
- It is hard to predict the area where an error may occur in the future. Apart from that, even bug localisation can be tricky sometimes.

Model transformation.

Graph transformation means a correct initial program is given and needs to be converted into another correct program. A graph transformation is just for this job, and the challenge is to keep the transformation process safe [87]. This approach is similar to the last approach presented earlier on approaches on dynamic memory verification. However, Dodds' approach is based on a term rewriting system only and therefore is beyond the scope of this work. Another term rewriting system, but with solid task priority queues, is Stratego XT, [125] and [294]. [132] suggests heuristics for applying rewrite rules for better confluency.

Approach 4 — Type Checking. Type checking excludes numerous mistakes in expressions at an early development stage due to incompatible types. For example, an assignment of a 32-bit integer to an 8-bit floating-point, in the best case, copies just that small value and causes no harm, if lucky. In a bad case, it may store any pseudo-random value.

If type checking succeeds, then the proceeding semantic analysis gets valid input. However, type checking cannot state, e.g. a loop is correctly implemented. To state just that, one would first specify what "correct" means. Second, check this specification then. Unfortunately, type checking is insufficient for verification purposes and can only be considered a required precondition. Type checking e.g. does not contain information about data dependencies. It also does not know which variables will be allocated. It also does not know how many objects might be in memory. The static analysis does this, which is an independent phase during software development:

Type checking may be formalised as $\Gamma \vdash e : t$, where Γ is a term environment containing an associative map onto types, e is a term expression to be checked, and t is an associated type to be checked against (see [22]). e requires decomposition to its base statements, and each statement requires a separate check to validate whether a given compound statement e is of type t in Γ .

No.	Phase	Input representation
0		command line
1	Syntax analysis	tokens, derivation tree
2	Semantic analysis	yes/no
3	Code Generation	derivation tree
4	Static Analysis	yes/no, any data structure
4*	Linking	Target file
5	Program Invocation	terminal text and errors

Figure 12: Phases until code generation

In contrast to Hoare triples, terms corresponding to statements are assigned a type. In contrast to Hoare's calculus, type checking only checks if expressions have a specific type that must match a declaration.

On type checking, program statements and expressions are checked against expected types for compatibility. Type checking does not know of a calculation state as verification does.

In analogy to Hoare calculi, type checking is a bottom-up approach, so the checking starts with a given expression e and terminates in case of success. Type checking, if considered as proof of program properties, is bound to a tiny check only. It is a single and mandatory check whilst semantic analysis (cf.[243]). It does not cover nor overlap with verifying dynamic memory since type checking is not extensible and has no easy way to represent the dynamic memory model (see later).

Observation 1.14 (Phase Type Checking). Type checking must be performed before all other semantic phases (especially before verification), which rely on correct typing available.

When type checking (after Hindley and Milner) [115], [203], [48] Hoare triples, then it must be noted that "true" is the most common precondition. Furthermore, type checking has fundamental restrictions equivalent to simplified Hoare triple checks (see sec.IV, cf. fig.13).

Extensions are made, which now allow checks on structs, type strengthening, properties of non-assignment, and static bounds of struct size [96]. Regrettably, dynamic memory properties may not be checked either. For example, let us consider

$$(\rightarrow\text{-elim}) \frac{\Gamma \vdash e_1 : (s \rightarrow t) \quad \Gamma \vdash e_2 : s}{\Gamma \vdash (e_1 e_2) : t}$$

The rule (\rightarrow -elim) demonstrates a type-specification (e.g. $s \rightarrow t$) may be used as a simple specification (see [58], [186]).

In [22], all crucial theorems and lemmas to the λ -calculus are introduced and their proofs. The paper [207] is dedicated to non-decidable problems with λ -terms in untyped calculi (e.g. in Curry's calculus, but not in Church's calculus). For instance, $\lambda x.xx$ cannot be typed and cannot generally be solved in applications. Let us assume that

Type checking (see [178]): $\vdash_{\Gamma} e : t$.	1
Type checking. Given Γ, e, t , show $\vdash_{\Gamma} e : t$.	2
Type inference. Given Γ, e , find t ?	3
Inhabitant problem. Given Γ, t , find e ?	4.

1	Hoare Calculus: $\vdash_{\Gamma} \{P\}C\{Q\} \equiv B$
2	Proof checking, where $\overline{A_{i,j}}$ is an axiom, $A_{i,j}$ is a rule: $B \vdash_{\Gamma} A_{n,0..} \vdash_{\Gamma} A_{n-1,..} \vdash_{\Gamma} \overline{A_{0,..}}$, given: everything.
3	Logical inference, given: B, Γ , wanted: $B \vdash_{\Gamma} A_{n,0..} \vdash_{\Gamma} A_{n-1,..} \vdash_{\Gamma} \overline{A_{0,..}}$
4	Inhabitant problem: $\{P\}, \{Q\}$, wanted: C

Figure 13: Comparison between type checking and Hoare calculus

$\lambda x.xx$ was typable, then x would have type t_2 , and the first x would be a functional type $t_0 \rightarrow t_1$. However, that does not apply to t_2 in the first-order typed λ -calculus, in which types are not further parameterised. Hence, $\lambda x.xx$ is a not typable term. However, if assuming infinite types [166], then an approximating limit may be found. This type corresponds to the recursively defined ADT, which has further (possibly again recursive) dependencies and may be resolved by a union type (a struct or record as in C or Pascal).

Observation 1.15 (Verification Non-Reducibility towards Typing). In general, type checking can be reduced to verification in a Hoare calculus. However, the opposite does not hold. Fig.21 clarifies this for the ALC from fig.19.

Approach 5 — Automated problem reduction.

An automated problem reduction tries to cut off fragments (e.g. lines) from a given program listing, s.t. a given error or any other specifiable program behaviour remains. Other specifiable function behaviour might be, e.g., "function test123 always returns 5". If a program calculates some mapping, but we are interested only in a single value from its domain, then all code may be replaced by a fixed constant except for that singleton. Often a program error is related to small program fragments due to modularity design. Unfortunately, bulky or unknown programs may dramatically increase error localisation efforts, which is often the reality.

Assume we build a software project by a single shell command. For the sake of simplicity, GNU make [100] is replaced by a primary project build tool, called "builder", which may be used for any software project to be built

[304]. The slicing tool "shriner" [305] is used to automate an incoming program reduction. The program works repeatedly: it builds the software project from sources, analyses it and launches it, then it compares observed with expected behaviour. If the program after reduction still builds, runs, and comparison succeeds, then reduction succeeds, and another reduction step is tried recursively. If the reduction fails, then another reduction is tried. If no other reduction is available, the overall reduction exits with the previous successful reduction as final. The program under investigation dumps all it would usually do to stdout and stderr. By default and w.l.o.g. it is agreed upon that any behaviour may be directed to stdout or stderr – this may, under the circumstances, may require tracing information issued directly by the program at that place that interest when analysing the problematic code regions (so-called symptom).

A symptom is specified behaviour of a program, either desired behaviour or undesired. If a symptom still appears after a reduction step, then behaviour remains invariant, and we continue with reduction until the invariant is violated. This behaviour is very close and related to how a while-loop is defined (see axiomatic semantic of (LOOP) in fig.3, cf. fig.4). This approach is best described in algo.1. The algorithm is naïve and not optimal as e.g. line selection *lineseq* is not determined and may contain any number of lines equals to at least one or more lines. It must be stated, the number of selected lines may fluctuate over time depending on if reduction succeeds or fails for several consecutive times. The default reduction strategy may also be tweaked.

Algorithm 1 Naïve line-based reduction attempt [305]

```

1: procedure naiveShrinker(prog, symptom)
2:   newProg  $\leftarrow \emptyset$ 
3:   oldProg  $\leftarrow prog$ 
4:   for all loc(newProg)  $\leq loc(oldProg)$  do
5:     (newProg, oldProg)  $\leftarrow$ 
      (REDUCE(oldProg, symptom), newProg)
6:   end for
7: end procedure
8: procedure reduce(prog, symptom)
9:    $\exists lines \leftarrow lineseq(prog)$ 
10:  if RUN(prog \ lines) == symptom then
11:    return prog \ lines
12:  else
13:    return prog
14:  end if
15: end procedure

```

B. Object Calculi

OCs are formal rules that impose how representations of and operation on objects such as type checking and assertion checks. OCs can be divided into two groups,

namely Abadi-Cardelli calculi (ACC) and Abadi-Leino calculi (ALC) (cf. fig.14).

Type	Calculus
(1)	Abadi-Cardelli [3], class object, Example: <pre> class MyClass{ int A; int B; MyClass C; }; MyClass o1 = new MyClass(); o1.A=1; o1.B=2; o1.C=NULL; MyClass o2= new MyClass(); o2.A=5; o2.B=3; o1.C=o2; </pre>
(2)	Abadi-Leino [155], [4], [2], non-class instance, Example: <pre> object o1 = [A=1; B=2; C=[A=5; B=3]]; </pre>

Figure 14: Object calculi

So, why do we need a formalisation of objects? Why can objects not just be replaced by bare variables instead? Second question first: yes, it could be replaced at the end. Nevertheless, as objects have fields and more interaction may happen, it is, after all, better to abstract more and therefore to use objects as an abstraction of some data container and operations over it. Algorithms and specification may greatly simplify, and in terms of verification, another indirection may be required — but there is no apparent reason that could outweigh the advantages. A class of an object is an (ADT) and not just a data container. ADT is also a carrier set of objects foreseen for complex problem modelling (see [156]). Operations over objects are closures. Thus, an object may not suddenly decompose itself while calling a method. Hence, a developer defines an object only with operations, which are characteristic and presumably affect only its inner state. Encapsulation is very close to a split-up as a modelling technique with union-types in pre-object-oriented time. Operations characteristic to objects are in practice class methods, where an object is a class instance. The object-oriented paradigm has undoubtedly been prevalent, as can be checked periodically with industry's TIOBE index. The ADT concept can be assessed at a notable single successful contribution – independently belief or personal preferences anyone may have gathered over the last years. ADT indeed supersedes all possible refinements, such as encapsulation, polymorphism, message sending, event handling.

So, one advantage of ADT is an improved modularisation concept which allows building even more reliable, flexible, more intuitive, more complex and faster software due to a well-understood set of modelling techniques ap-

plicable to objects, for instance, object-oriented modelling (OOM) [77], [229] or patterns [136]. Those best-practices are well accepted and wide-spread in the industry. The importance of patterns can hardly be overestimated. Positive effects include the decline in error probability compared to traditional development approaches due to a strict separation of concerns. Patterns are stereotypes. "Stereotypes" are idioms that allow humans to grasp particular objects and their dependencies on other objects faster. However, it is an essential precondition for a better understanding of software, including software maintenance and development – without thoroughly reading the code. Many philosophical concepts can be considered a precursor of object-orientation, as (logical) atomism, connectionism and many others. Without any claim of completeness, patterns could intuitively be interpreted as object comparison OOM with roles assigned to actors of a scene: each actor acts according to a global and well-understood written manuscript, a specification for a full shot. This picture is what a pattern makes a software pattern as we know it. When it is said, a software developer thinks in patterns, the developer thinks in pictures, which can be fully grasped within just a few seconds. It is no mystery nor magic at all. It is common human psychology – this also counts for how objects shall be structured and how many fields or methods shall be allowed, which entities or compartments shall be chosen better as long as each unit does not have more than seven everything seems fully compatible with the human mind. A pattern's pragmatism increases when a scenario (e.g. use-cases or tests) can be described as more comfortable and clearer.

The OC can be used for semantic analyses, e.g. for type checking or verification. Apart from that, it may be facilitated to analyse object field dependencies, e.g. by a compiler to ease the tension regarding spills on processor registers [181]. Occasionally it may be useful to merge object fields into a contiguous array block or split them into local variables if both array bound and object size are known apriori to be small (cf.[44]). The data dependency determines register candidates (may include general-purpose registers and stack cells) whilst register allocation. CPU registers are fast. However, they occur in a tiny amount and can usually accommodate only tiny words regardless of new architectures trying to lower the pressure. On the other side, CPU registers depending on a concrete platform may, under the ABI (application binary interface, see [252], [253], [160]), store only a few words. Words are restricted, and even so, an ABI usually does not split contiguous blocks of data chunks representing class objects because compilation makes it nearly impossible to predict which object fields will be used and how their memory layout finally looks. The C (and ISO C++, too) specifications state that objects shall be treated as contiguous memory lump and further details remain unspecified [243]. However, if there was an effective way to predict reliably, then the current, solely

conservative GCC approach could significantly improve the runtime and reduce memory consumption in the ABI on the caller's side. However, the reality keeps objects always contiguous, even if 99% of all fields may not even be touched. If memory would lead to a speed issue, then all memory access would add additional stack store and load operations, strictly speaking, which may not be necessary.

Ehrig's records in his "Record Calculus" [90] only differ by definition. They are not ADT but just data containers. His record is formalised as a tuple (related to Codd's relations) and applied to parallel executions.

Scott [236] considers data types (generalised as tuples) as algebraic lattice, which has initially often an uninitialised infimum, a final value as supremum, and specific Galois-joints defined upon set (tuple component) inclusion. All values a variable may be assigned to between those extremums, infimum at its lower bound and supremum at its upper bound, is encoded as a state tuple that obeys evaluation order. For more details for verification purposes with non-dynamic objects, refer to [58], [182]. For further discussion, refer to [23], where verification conditions are formulae of first-order predicate logic. Attributed fields are modelled separately and are allocated to dedicated memory regions. Alternatively, an object's field is fully embedded into another object – here, all fields and types must be known apriori. However, this work's main contribution are two predicates dealing with predicate definitions with an intuitive meaning. In analogy to [23], [58], dependent fields are highly recommended to be modelled as dependent objects instead. Both papers suggest input of new assertions for object invariants, which are always valid as long as an individual object lives. None of the approaches listed is related to pointers (see sec.II).

Class-based OCs are mentioned only briefly. This family of calculi dominates recent PLs, e.g. Java or C(++) [252], [243]. A class is used to instantiate objects on runtime. This section is not primarily interested in memory allocation yet, but "new", "malloc", and "calloc" will be used. After a short characterisation, we will decide in favour of the object-based OC. Both calculi, however, allow type checking and enable program specification and verification. Abadi and Cardelli motivate their calculus with subclasses, polymorphism and closure/recursion through objects. Both authors refer to typed λ -calculi as an example of second-order calculus. It is worth noting that λ -terms representing objects may be used as quantified types (so, polymorphic, a type class set implicitly bound to variables by \forall , see. [203], [48]) by using unbound symbols. Next, recursive and recursion-free classes require a denotational structure. In other words, types dependent on new parameters – represent an abstraction of λ -types of higher-order over object types in ACC.

For instance, w.l.o.g., the question of which region in RAM is used to store a specific object cannot directly be

answered since pointers are the only abstraction ACCs have. The same holds for the question where is an object stored relatively to some top-level object. x denotes an object in fig.15, which has one inner object with two content cells, abc and def , and some content ghi again. Apart from that, pointer y points to some object containing jkl , where x has some field (or any other subfields from a field), which points to the content of y , namely jkl .

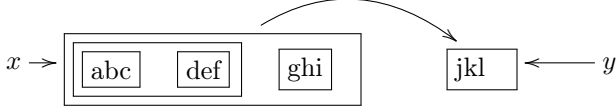


Figure 15: x points to an object which points to y

A class hierarchy by inheritance denotes a poset, whose infimum by default is an empty class, e.g. Object or []. Thus, any two classes in the hierarchy are comparable. Even two unrelated classes may be comparable, according to \sqsubseteq , $\not\sqsubseteq$.

ACL allows inheritance, as well as delegation, inner fields and objects. The use of keywords: "self" and "super" as defined in the C++ language [243] are permitted. However, their use is underlain by prior semantic checks in the context of the related class. This additional security measure and further measured required for life-cycle management quickly bloat in OCs. Cardelli notices that additional checks due to actual and pointed classes and just using the keyword "self" leads to compulsory checks of the whole class hierarchy. Extensive unneeded checks can easily be avoided if each variable is fully qualified at an early semantic analysis stage. Subclassing and reference checks do imply (full) searches on the class hierarchy, which has an acceptable bound of $\Theta(n) = \log(n)$. However, a severe restriction lurks regards late binding and virtual methods. Practical and theoretical implementation details on inheritance and class hierarchies for C++ can be found in Raman's paper [216].

Object methods contain code which by default, is visible only to the object itself. For simplicity reasons, we will model methods accessible only after new creates the object in contrast to static methods. There is no need to access the previously allocated memory region from a particular object in static classes because variables in the stack window are allocated independently from an object. By convention, every object has a unique method, a constructor, for initialising fields. Its code is generated to the assembly file's section .ctor in C++ [243]. For destruction, ".dctor" is used. Thus, the following object phases may be defined (see fig.16), which will serve us later in specification:

Points 1 and 2 have just been discussed. Point 3 relates to any state of a non-dead object. An object is non-dead iff it is life – this is after construction but before destruction.

1. Constructor (c-tor)
2. Destructor (d-tor)
3. Perpetual Presence
4. Precondition to a Class Method
5. Postcondition to a Class Method
6. Arbitrary Verification Condition

Figure 16: Specifiable life-cycle of an object

Points 4 and 5 imply specifications for procedures. For the sake of application, a forced specification of the whole program shall be avoided. That refers to the lightweight approach, which will not be considered further yet. It is agreed upon that any arbitrary assertion may be inserted between statements as we go, which are optional (see sec.VI), in order to increase flexibility and problem localisation by default. In both calculi, the methods are not artificially bound apriori. However, unbound methods may also include code modification, removal of existing and insertion of new methods. Obviously, in unbound calculi, specifications grow in complexity, and changes are complex and error-prone. Even worse, unbound calculi may become theoretically not decidable. Thus, maximum opportunities here lead to too harsh verification limitations.

As mentioned earlier, unbound methods provide neither do they extend Turing-computability. Hence, methods with mutable code are no more considered in this work by default. Object-based calculi have the logical judgement

$$E \vdash obj : A :: B$$

where E is an object environment containing all created objects.

The location obj is an object represent (a variable in calculus 1, and a whole object in the case of calculus 2). A is of type obj (so the class names obj). B is a specification of object obj . The specification may contain, for example, the object's internal state description. If $obj.m()$ is called instead of obj , then B has state obj before and after m is called, but B may also include assertions from fig.16. The assertions may not contradict the actual runtime state. Both the embedded auxiliary operators and the special-purpose register enable access to the results before and after statement execution. The register may either contain the whole object (in case 2) or an object field. To any considered OC, the judgement on objects, type and assertion, is essential.

Remarkably, on the one side, B may alter over time, but on the other side typing of A may not. That becomes a problem when a remote method alters its signature, but its state does not. For instance, a web-server or driver are loaded when its specification is fixed, but its behaviour is unknown.

Both ACC and ALC do not support pointers (see later). Pointers avoid copying redundant memory regions, which leads to performance increase unless genuine copies are

needed – this question may not always be obvious to answer in practice (see later).

A class type T is inductively defined as T type, integer or another class. The class object includes fields f_i and methods m_j , where all class components are unique, and each field is assigned some type T . Methods have

$$T_j \rightarrow T_{j+1} \rightarrow \dots \rightarrow T_k$$

as a type signature.

Next, calculus 2 is considered (ALC). The PL Baby Modula 3 [2] is introduced by Abadi and the company DEC as an experimental modular PL. A minimal feature set adopted from Modula-2 is very close to Pascal by its syntax and semantic, but with extensions as an OC. The language proposed is close to the languages suggested by Abadi, Cardelli and Leino. It contains all is needed for μ -recursive schemas, particularly assignment and unbound recursion. [111] contains a detailed discussion on object expressibility, even if some chapters seem old-fashioned at first glance, but it is still relevant today. Originally calculus 2 was introduced as an alternative representation to the existing widely-known. Both calculi are dual, which can formally be shown by full abstraction [179], [209], [65], [117]. Full abstraction requires to prove two different kinds of semantics given are equivalent, namely denotational and operational [9], [290], [6], [276], [250], [34], regarding the observed (object) behaviour. [220], [222] is provided for full reference. Although equivalent, in ACC soundness, it is worth noting that it is much easier to prove (especially the denotational part) and often is preferred in practice. However, strong supporters of the calculus may dispute the latter remark. The reason why object-based calculi with operational semantics are so much more difficult is explained by recursion. If recursion is denoted symbolically, then it is much easier to detect and refer to such than guessing boundaries of object boundaries, especially when it comes to object specifications. Baby Modula 3's syntax is based on term expressions of kind a , as shown in fig.17, where A denotes a typed expression.

$a ::=$	x	.. variable
	$\text{fun}(x : A)b$.. sub declaration with body b
	$b(a)$.. call of b with parameter a
	nil	.. nil type
	$a[f=b, m=c]$.. object extension
	$a.f$.. field access
	$a.m$.. method invocation
	$a.f:=b$.. field assignment
	$a.m:=c$.. method invocation
	wrong	.. wrong type

Figure 17: Definition of object terms after Abadi-Leino

A term expression is very similar to Pascal's expressions, so it does not require further details. $\text{fun}(x : A)b$ defines

an anonymous procedure equivalent to λ -abstractions with a single input x of type A . W.l.o.g. anonymous procedures accept zero or more arguments. Variable x is in the procedure's body b and bound on call. A procedure call, e.g. $b(a)$, implies actual and formal parameter types match. An empty value nil is by definition applicable with all pointer types. For example, uninitialised object fields contain nil too. An object extension adds initialised fields not clashing with existing fields. Methods are extensible similar to field extension as just described. Methods may be updated. "wrong" is a reserved keyword that indicates an incorrect calculation encountered. An object can always be defined using a vector that consists of a poset in lexicographical order, and its elements are pairs of field/method name and corresponding value. The content may again be an object, which is defined in analogy to fig.17.

Its authors provide the semantics of Baby Modula 3 as denotational semantics, and top-level has two stages: type checking (a fixed rule set) and one for verification (another flexible rule set). Object type-checking must be component-wise and requires some subclass relationships $A <: B$, which holds iff B contains all fields and methods of A . Since no object identification possible in the object-based calculus as with the class-based calculus, recursively-defined objects must be simulated by fixpoint combinators as in the untyped λ -calculus having then similar restrictions. $\mu(X)$ may be used to achieve just the said for any object X according to fig.17. It is assigned after $\mu(X) \tau$ is applied the same way as for λ -terms, e.g. in $\lambda x.x\tau$. So, object checking includes variable environments, subtypes (including sub-classes) and common structural rules. They are used to perform type checking and object verification (see later, cf. (minimalistic) LCF [209]). For the sake of simplicity (see [155]), structural operational semantics are often used [208], although, as mentioned earlier, a transformation into/from denotational semantics remains a quite difficult act.

However, μ -objects are a considerable problem because, for the same initial values, reasoning may differ, so unsoundness becomes evident. Let us consider the rules from fig.18 as an example.

$$\frac{\begin{array}{l} \vdash \text{nil} : \mu(X)\text{Root} \\ \text{Self} = \mu(X)\text{Root} \end{array}}{\vdash \text{nil} : \mu(X)\text{Root}} \quad \frac{\vdash \text{nil} : \text{Root}}{\vdash \text{nil} : \mu(X)\text{Root}}$$

Figure 18: Example of unsound rule set

So, rules containing recursion may be violated or not provable due to non-confluent proofs (cf. fig.7). Here, only the trivial solution may be considered as the only reliable. This situation is, unfortunately, not satisfactory. That is why an object in ALCs, in general, may not be typed in first-order and second-order calculi. This hinder may be overcome by enriching verification and typing rules with additional context-sensitive rules. However,

this dramatically worsens simplicity. In ALC, classes as such do not exist. Objects may have an arbitrary number of fields with other objects as content. So, a class may depend on other classes, including itself. This additional dependency motivates the introduction of the third-order λ -calculus λ_3^\rightarrow (see def.1.11). Thus, verification confluency and type closure significantly impact static analyses with class-types [2]. If confluency is decidable in a finite amount of time and verification is countable, all named types may be joined together in a union-typed struct. Thus, the newly obtained struct unions all dependent types. The authors of [2] mention united types as described are all enclosed, and all gained (sub-)types may again be used for object-composition. The gained object type is an algebraic ideal based on object comparison " $<$ ", see further.

a, b	$::= x$.. variable
	$ \text{false} \text{true}$.. logical predicate
	$ \text{if } x \text{ then } a_0 \text{ else } a_1$.. branch
	$ \text{let } x = a \text{ in } b$.. symbolic assignment
	$ [f_i = x_i^{i=1..n},$ $m_j = \psi(y_j)b_j^{j=1..m}]$.. c-tor
	$ x.f$.. field accessor
	$ x.m$.. method invocation
	$ x.f := y$.. field assignment

where x, y, z, w are variables, f, g are field objects of object x , and m denotes a method.

Figure 19: Simplified Abadi-Leino object definition

The PL presented in [4] (see fig.19) simplifies the language from fig.17. However, assignments do not exist. Instead, there is a symbolic assignment (one-time only) and a conditional branch, which is factually additional syntactic sugar. Furthermore, dynamic methods are prohibited. The syntax is defined as in fig.19. Renaming on runtime is allowed, but only if the caller and callee obey calling conventions. Locals are prohibited in procedures. Method parameters are prohibited too if they alter in a method with no accurate restriction towards expressibility since additional fields can always be simulated. Assignment returns an object as a result. An essential difference, though, from [2] is ALC excludes recursively defined objects. The subtype relationship is defined in fig.20.

$$\vdash A <: A' \Leftrightarrow [f_i : A_i^{i=1..n+p}, m_j : B_j^{j=1..m+q}] = A \wedge [f_i : A_i^{i=1..n}, m_j : B_j^{j=1..m}] = A', \quad p, q \in \mathbb{N}_0,$$

Figure 20: A possible definition of subclassing

where A' is some class, and A is its subclass. The relation $<$: facilitates type checking, and most importantly,

the object construction rule (CONS).

$$\begin{array}{c} A \equiv [f_i : A_i^{i=1..n}, m_j : B_j^{j=1..m}] \\ E \vdash \diamond \quad E \vdash x_i : A_i^{i=1..n} \\ E, y_j : A \vdash b_j : B_j^{j=1..m} \\ \text{(CONS)} \frac{}{E \vdash [f_i = x_i^{i=1..n}, m_j = \psi(y_j)b_j^{j=1..m}] : A} \end{array}$$

This relationship is defined over A being some object type (non-class here), E an object environment, x_i some field value, and b_j some method value (procedure body). Verification follows in ALC this judgement

$$\sigma, S \vdash b \rightsquigarrow r, \sigma'$$

where σ is an initial stack, S denotes stack state, b given statement sequence ("the program"), r denotes the result which accommodates in the virtual register of potentially unlimited size, and σ' denotes the final memory state. Specification of objects is recursively defined component-wise as

$$[f_i : A_i^{i=1..n}, m_j : \psi(y_j)B_j : T_j^{j=1..m}],$$

where A_i, B_j are specifications, y_j is some parameter of anonymous procedures ψ used in B_j, T_j , and where T_j denotes the specification transition from one memory state in the following.

Narrowing specifications is defined among $E \Vdash a : A : T$, where E is an object environment, a denotes a program, A is some type, T is the transition description. So, type checking A and transition states in B are applied simultaneously, even if spread around different stages. It is not hard to see that B is too bloated, and even tiny changes may lead to enormous consequences. The type relationship $<$: [4] proposed is accordingly to specifications. Analogous problems affect specifications. For example, let us verify the program: $\emptyset \Vdash ([f = \text{false}].f := \text{true}).f : \text{Bool} : (r = \text{true})$. The corresponding annotated proof tree can be found in fig.21.

The definitions of used rules are in fig.22.

Assertion \diamond denotes true. More on the chosen rule set's soundness property can be found in Abadi's paper [2] and its accompanying technical report with the same title. It is worth noting ALCs lack abstraction techniques, as introduced in the previous sections. The parameter visibility only goes from outside in, but not vice versa. For instance, in $b_1 \equiv \text{let } x = (\text{let } y = \text{true in } [m = \psi(z)y]) \text{ in } x.m$, the inner y cannot be checked outside the procedure. According to the rule set from [2] and the difference between predicates (whichever order and restrictions it may finally be) and assertions, this comes as a surprise. Abadi and Leino suggest future work improvement of specification abstraction, further research on mutable parameters, especially w.r.t. completeness, pointers over objects and object fields, and research on recursively defined objects. None of the selected calculi, neither ACC nor ALC, pay attention to pointers or aliases (also see

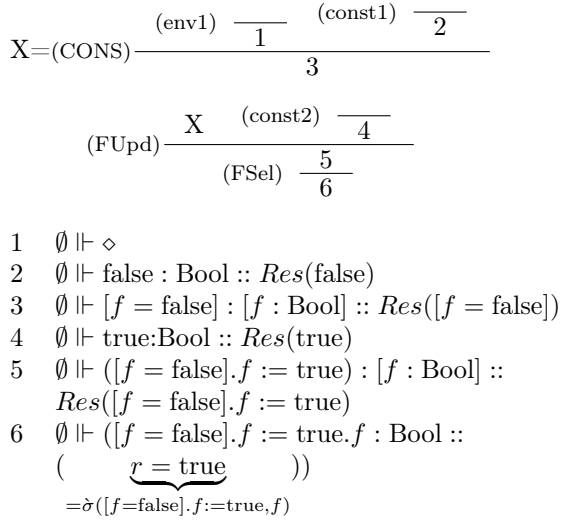


Figure 21: Proof tree example for an object-based calculus

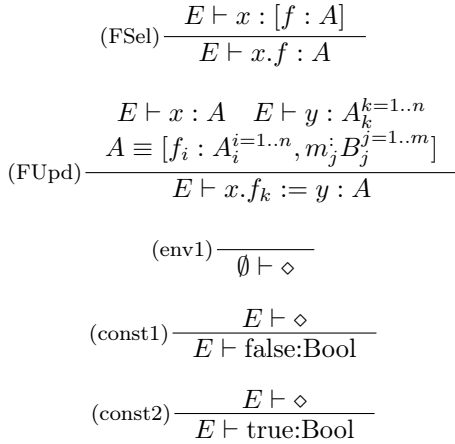


Figure 22: Example rule set for an object calculus

later). In [3], essential extensions are named but not yet been proposed: multi-threaded execution, addressing fields, use of abstraction in specifications as initially was proposed by Hoare [116].

Banerjee [21] presents a language that supports objects accommodated in the stack within the same memory region (cf.[258]). Banerjee's approach moves all local variables into the stack. However, dangling pointers are forbidden by default.

Recursive predicates over objects are also forbidden. Unique about global invariants is the dependencies between objects that remain invariant. He warns about a strongly emerging problem of abstraction and supports the initiative of an object-centric predicate view.

Programming Threads. In [4], objects qualify as ADT but not as a usual record (struct) [90]. The difference is that records are defined and identified not necessarily by their structural components, not primarily by their fields.

Graph transformation can be considered as reductions over records. Ehrig and Rosen suggest a subcategory of procedures known to be safe, so it does not mix dependent object fields with analysis using Category Theory [202]. Their approach may be considered safe towards single-threading application if access to a subset of object fields does not depend on each other. That is how the authors grant sufficient field access without blocking an entire thread. Thus, the inherited procedure and GC may simultaneously run if they do not influence the program's behaviour. Similar approaches in accessing object are in [127].

Huisman [120] also investigates multi-threaded access to an object, as do Hurlin [121] and [90]. By design-by-contract, Huisman tries to grant method access, but he also attempts temporary access control. Huisman suggests tracking a specification's history of accessed objects and methods. It is also suggested to enrich object descriptions with class stereotypes of collaborating object commands, due to a lack of abstraction level, especially in multi-threaded method calls.

Frameworks. Alternatives or modified formal methods are needed (see def.1.12) to achieve a specification of whole programs, one of which Meyer's approach about Separation of Concerns [175]. Meyer [172] suggests, as many did before him, a methodology based on Liskov's modularity approach, in analogy to Parnas' hiding principle. In tight algorithms, actors are assigned stereotypes according to which they act. The definition of a role in a given ontology of many participants and collusions allows a better understanding of the given object structure. Meyer's theorem may be summarised as:

The responsibility is divided [among ontology units], the more such derived objects may be trusted.

The intention is: the smaller a program gets, the more its complexity is reduced. There, the initial program is not touched, except for the performed reduction. A metric, e.g. McCabe's metric, is a real number that measures the complexity of a given program w.r.t. its CFG. The more a program is split to easy to control and logically related units, the simpler the CFG becomes. Metrics correspond to programs, which becomes easier to compare. We notice that an object that may occur simply at first glance may have many dependencies with an arbitrary number of other objects, which may not be known before whether the program is rather complicated. Such unprecedented, unexpected dependencies often are covered and hard to grasp totally at first glance. Besides, they often appear as sources of errors due to poor design and are a clue in serious mismatch to specifications. Often remote objects being not related to a scenario are involved, which to simple models and algorithms are unlikely and lead to situations where two related objects actually may not be connected.

Riehle [227] suggests tests be introduced covering specifications, s.t. localising specification mismatches on object-level is simplified within (object) collaborators. From his role-based inheritance models, variability can be observed as the single most important property besides extensibility, which is granted by zero or more aggregations. Variability and extensibility together can be summarised as essential platform features (API) for (re-)designing, and modelling frameworks — the heap verifier in this work, is a framework.

Interconnection between object modules are checked against specifications, e.g. using Modular Algebra [30] or Component Algebra [93], [239], [259]. These two approaches are well-founded and formalise interfaces between class objects and other objects. The interface description, however, is bound by input and output method parameters. [94] describes a navigational attempt over objects according to a given specification. In [30], [93] and [17], the method calls are recommended to track and be callable in constraints, so, e.g. a method may not be called until a list of all previously called methods is completed. This approach seems very similar to Huisman’s approach. Since program verification often insists on a full specification, it makes the overall verification and specification a nightmare since only a single gap would invalidate the whole specification. When it comes to bigger programs, all that becomes close to absurd. However, nearly all the approaches presented rely on a full specification and do reason about dynamic memory. A method call sequence may be useful not only inside an object as proposed but also as an extension that might be beneficial for the web of objects, e.g. exclusion of method calls to m_2 on any object first unless method m_1 is called on the third object. Currently, the programmer must know somehow a certain method may not be called unless a certain condition is met — the same holds for the initialisation of field objects or arbitrary other calls and order. This learning experience is crucial for any framework. Instead, a static approach in analysing the object calling order would be convenient.

The Object Constraint Language (OCL) [1] is an extension of the Unified Modeling Language (UML). OCL is graphical and textual and is the de-facto standard when modelling static and dynamic aspects of the desired software. OCL allows insertion of formulae describing object interdependencies, e.g. it may restrict types in object relations. Formulae describe mainly second-order predicate logic terms (see def.1.9), such as atomic types.

Apart from the earlier mentioned restrictions from previous sections, the lack of pointer specification solely remains. Safonov [231] introduces and analyses many examples in compiler construction and related field areas. His analysis accumulates in postulated criteria upon trustworthy compilation. The author chooses compilers due to their very high complexity comparing their vast state transitions with others. The complexity can easily be validated, for example, by a thorough code inspection

generated, especially regarding branch instructions, or by analysing metrics for some PL processor, e.g. for C+++. The complexity analysis might be quite challenging when showing any given transformation is sound and optimal (also complete, reminding the quality ladder from fig.1). In order to better achieve this objective, Safonov refers to Meyer’s methodology. However, as a concrete counter-argument against Meyer’s approach, Leroy’s CompCert [31] shall be named, which researches soundness, but only partially does the research performance. Although the methodology proposed seems promising, unfortunately, it is tough to derive a significant practical meaning out of it because of the harsh practical restrictions. Hence, Safonov considers the following criteria reasonable in practice instead:

- Correct and plausible error diagnosis, including counter-example generation.
- Model transformation, including objects, is preferred due to small specification efforts.
- The option to extend and adjust object-based calculi.
- Use of formal descriptions if usability does not suffer. Particularly, Safonov considers complete coverage of a formal model and locality of a specification’s most critical single criteria.
- ADTs describe object invariants.
- IRs must be flexible enough and abstracted, s.t. they might be used on different verification stages.

C. Dynamic Memory Models

1) Transformation into Stack: In sec.I-B, a discussion on OCs and transformation into stack took place. [258], [257], [274] research the functional paradigm for verification where all variables are moved to the stack windows (in [52], a formal proof of soundness is demonstrated by Tofte and Talpin [258]). Grossman’s C-dialect called Cyclone is presented in [109] and implemented in ML. It reasons about so-called regions (in the so-called memory Region Calculus) and is defined as a set of corresponding heap elements, which may be utilised at once in a release phase. Particularly the transformation into stack must now pay special attention w.r.t. variable visibility, s.t. accidental destruction is avoided by any means. In [98], variable visibilities beyond a current stack window are discussed in more detail, and an extension towards Cyclone is proposed. If the variable visibilities are not carefully transformed, then derived aliases, particularly the "maybe-aliases", may become unsound. The functional approach excludes dynamic parameters, recursively defined structures and procedure which return functionals. All function types must be defined at compilation time. In Meyer’s [173], [174] opinion GC (see [153]) is most important beside soundness. Hence, he proposes to fully avoid dynamic memory and re-arrange algorithms to work only with the stack instead. As mentioned in [258], the push into the current stack window does not occupy more than through a minimal size. He insists object

abstraction is dedicated to more attention and suggests letting dedicated variables be in a specification. However, the full proof for soundness is missing. Even a simple assignment may be unsound – as not mentioned in the paper, it may alter the program code whilst program runtime. However, this sporadic case can, under usual circumstances, be ignored. Access to stack content may be faster than to dynamic memory but always requires overhead for pushing in and popping out data, which depending on the considered algorithms, may significantly reduce the overall performance, s.t. the use of dynamic memory may again be faster (cf.[12]).

2) Shape Analysis: The main objective of AA [232], [189], [199], [85], [275] is to find invariants in a heap on program runtime, e.g. for the localisation of aliases. Shapes are corresponding invariant and flexible partitions of the dynamic memory [275], e.g. for a simply-linked list [85] or a doubly-linked list [60]. A dependency graph is always fully described by its transfer functions like empty shape, field or pointer assignment, new dynamic allocation. Sagiv et al. [232] introduce relationships between two pointers: "is alias", "is not alias" and "maybe alias".

Pavlu [199] noticed first that [232] and [189] might lead to an imprecise (meaning unsound) reasoning depending on a given program. Namely, if for a given if-then-statement in one case "maybe alias" and in the alternative case "alias" is inferred. Since the overall "alias" defined by Sagiv's calculi would not be sound, the correct answer would be "maybe alias". Moreover, [199] contains a detailed comparison between [232] and [189]. [199] assesses [189]. The finding of [189] is a more precise method and allows a path optimisation of shape graphs with identical beginnings and aliases. These shape graphs may be reused as more effective and shorter. The optimisation proposed has an upper bound of $\Theta(n^2)$ and reduces the calculation on average by approximately 90%, which is quite impressive. Pavlu suggests complex AAs is simulated extra-procedural, s.t. procedure calls and globals are turned into local intra-procedural elements as much as possible by renaming. His proposition has already been applied to the current GCC implementation. Both, Pavlu and the author of this work consider context-independent attempts in exact AAs have no future (cf.[113]) since characteristics seem evident and devastating. Furthermore, he suggests an optimised separation of merged vertices, which build up sub-graphs from the vertices, which strictly do not contain aliases.

[192] represents a tool for visualising heap shapes for fast analysis and localisation of invariants and rarely used bridge-edges between loosely coupled shapes for navigation in a graph abstraction and concretisation. Here, concretisation allows to fold and unfold subgraphs (all manually). Visualisation of transfer functions leaves much to be desired. A transfer function implies a folds or unfolds of or into subgraphs. However, a principal improvement is not expected soon due to fundamental restrictions here.

[54] presents an attempt based on heap separation to shapes. The approach compares potentially matching beginnings of rules by length (longest first). Special is the approximation of both sides of considered rules for a rule selection based on bound abduction.

3) Pointer Rotation: [249] suggests "pointer rotation", which is safe under these conditions: (1) the content of heaps remains invariant, (2) all elements in memory remain valid before and after rotation, (3) the total number of variables remains invariant. The advantage of a safe rotation is, first, the absence of GC – this can easily be defined, and, second, effective list operations, e.g. copying. Although pointer rotations do not insist on a direct specification, a minimal parameter modification can still lead to a hard-to-predict situation, especially when pointers are aliases. [249] suggests a base asset of rotations. However, this may be insufficient in practice, as more flexibility and a plausible framework upon base rotation composition are crucial. Furthermore, rotations are very sensitive to minimal changes on calls. For example, changing the order of compatible parameters may look safe at first glance – but it may fatally destroy or even free the existing heap totally as a surprise and, in fact, as an undetected corner-case. Surprise also occurs with harmless-looking input data – e.g. when the first parameter is an empty list – or when rotations are sequenced. Any rotation may be represented as an element of a group permutation, where its components x_j denotes some pointer location – for instance:

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{n-1} & x_n \\ x_2 & x_3 & x_4 & \cdots & x_n & x_1 \end{pmatrix}$$

Naturally, rotations may be composed. For example, let us consider a modified sample from [249] which is illustrated in fig.23.

```
var temp: T;
y:=NIL;
while x!=NIL do begin
    temp:=x^.next;
    x^.next:=y;
    y:=x;
    x:=temp;
end
y:=NIL;
⇔ while x!=NIL do
    rotate(x,x^.next,y);
```

Figure 23: Code example for a pointer rotation after Suzuki (in Pascal)

The code illustrated operates with a single-linked list with three difficult elements to transform and consists of steps 1 to 4 (see fig.24).

Depending on input data, one or more properties are observed, some of which are quite hard to generalise, others are not. For instance, $rotate(x,x,y)$ is a congruential mapping, s.t.

$tmp:=x; x:=y; y:=x; x:=tmp;$

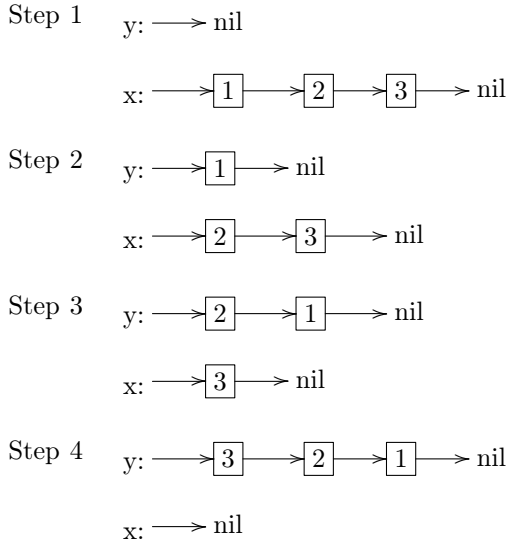


Figure 24: Dynamic Memory whilst rotating pointers

Even a tiny modification may invalidate previously considered properties. So, naturally appearing symmetries suddenly may not hold, which would occur alienating and spooky to a verifier, e.g. $\text{rotate}(x, y, x^{\wedge}.\text{next})$, since x and $x^{\wedge}.\text{next}$ are connected, and its intersection is not empty apriori.

4) File System: As we understand right now, a heap graph can also be simulated by a file system, s.t. vertices are files, and links are edges (e.g. "ln -s" creates a so-called symbolic link under Linux). Directories may be considered as objects, data containers literally. The content of a vertex is in its file so that content may be huge. Thus, a file system imitates a heap graph. Now a schema may describe a given file system without tracing symbolic links. The proposed structure is a tree and maybe encoded as semi-structured, such as an XML-document [292], [293]. In Linux, all operational resources are files. Operations over files now correspond to operations over heaps. The objective of verification may be defined as a check of a given file (system). From another perspective, a file operation may be checked too by a soundness check (e.g. by an XML-schema), which may immediately reduce errors and defects with big and many files. For the sake of simplicity, "sha1sum" or "md5sum" shall be used, especially for big and many files.

For check operations [294] and knowledge representation [299], a declarative language might be used, ideally Prolog. The outlined example [294] calculates two files from the top-level directory a and matches both cases. The top-level directory may be prefixed.

```
template(element(top,_,[A,A]),[text(T)]):-
  A=element(a,_,_), transform(A//p#1,T).
```

A maximal approximation in XSL-T would be:

```
<xsl:template match="top[count( child::*)=2] and
  a[1] and a[2]">
  <xsl:text>
    <xsl:value-of select="//a//p"/>
  </xsl:text>
</xsl:template>
```

D. Further Areas

Discussion and basic definitions on aliases and GC can be found in sec.I-C. Furthermore, related areas are presented, which may be added to the framework suggested from sec.IV-E and can be characterised as pointer analysis.

Alias Analysis: Weihl [269] gives an illustrative and still up-to-date review on this topic regardless of its age. According to Weihl, AA is an emerging approximation process of pointers to the same memory cell, which is mutable, and as such, the cardinality of a dependent set of aliases rises exponentially. AA beyond a procedure's boundaries is much more difficult in general because all possible calls and continuations of incoming pointers may be altered anywhere else. Pointed content may alter in continuations, and this makes the overall analysis inequally more complex. Weihl stratifies aliases to simplify, s.t. its complexity weights each program statement.

[181] contains a full review of past and present AAs, including his well-established too. The papers from Muchnick and Weihl can, without exaggeration, be considered as the single most influential and most important in AA. He parts analyses into dependent from a given CFG and independent. He also divides analyses by their result into "alias" and "maybe alias", and into closed subprograms and subprogram calls. Naturally, although not done yet, Muchnick's AAs may be distinguished even further. For example, Landi [151] focuses on pointer visibility scopes.

Opposite to Muchnick, Cooper [70] suggests first an independent AA. The primary motivation behind it is a substantial simplification because this is indispensable to track pointers and operations. Imprecision is a significant drawback here.

It is worth noting that GCC [252] allows the C-programmer to tweak directives and pragmas manually, s.t. (strict) AA is skipped for selected functions. Thus, generated code may become much more performant.

The approach in [118] can be considered as Muchnick's extension. By replacing the connectivity data structure with bitfields, this approach becomes more effective. A general improvement may be derived from the analysis framework proposed by Khedker [137]. Moreover, the presented framework is dedicated to assignments too. It is extensible, might be generalised and is expected to incorporate even SSA-form [76], [245], [289], [238]. Naeem [183] asserts that access is improved by hashing (all) subsets of calculated aliases. Notably, Naeem's approach contains a hidden proposition in rewriting AAs as a problem towards SSA. Notably, pointers are not just the

only variables, which are hard to locate whilst static analysis [242] beyond a procedure’s boundaries — they are one of the hardest problems ever. Srivastava’s approach [242] is useful, apart from all other discussed work, because global optimisations during linking, e.g. whilst dead-code elimination, often may not be fully triggered on earlier compilation stages.

Pavlu [199] divides AAs into two groups: a) unification-based [246], which finds more aliases, b) floating-based approaches that are much faster for the cost of higher imprecision.

Both [150] and [214] reasonably question why alias-analysis is not yet resolved satisfactorily. The answer is found in its complexity in locating aliases beyond procedure boundaries and its current limitation for the case "alias". In compressed dependency subgraphs, naming remains an unexpected but hard problem [232], [189]. Moreover, these approaches are restricted in numerous ways: pointer access by index only allows constant expressions; pointers with objects are forbidden; C arrays with a dynamic length are forbidden (as so-called variable-length arrays introduced by C99 and available by default in Clang/LLVM); interleaving memory regions are forbidden (as union-structures in C [243]).

Clint [64] deals with program verification and the complexity of soundness proofs related to aliases dealing with co-procedures. Clint’s contribution can be considered as first in the area. A generalisation of Clint’s work is the verification, including functionals, where [169] must be mentioned at least towards pointers in higher-order logic, as well as Paulson’s technical report [198], which tries to apply abstraction over procedures as substitution decision for a more effective pointer-based verification rule.

Gotsman [108] presents an approximation approach towards inter-aliases based on SL. Although the paper presents runtime characteristics and compares basic operations, the relationship is missing towards Muchnick’s and Cooper’s results but would be very helpful.

Garbage Collection: Jones et al. [127] present an over-complete review on GC focusing on parallel algorithms. In contrast to the first edition, the second edition of [127] is a total rewriting and almost exclusively parallel approaches. Withington [277] and Doligez [88] also give a review and can be considered as a genuine subset of the 2nd edition from [127]. Blackburn [40] summarises the most important recent GCs and a whole chapter in [127].

Appel [12] states that there are stack access limitations on code level in practice, especially w.r.t. copying onto and from the stack. The von-Neumann architecture and ABI primarily cause them. Appel further suggests in that case, the use of dynamic memory might be better under the condition no additional overhead is needed or at least only a few resources are used for the stack housekeeping (see [258], [174]). Appel’s multi-threaded contribution [127]

acts only on writing data, which may need seven times more free memory for the heap.

Regardless of its age, Larson’s paper [153] proposes a division between a fast cache and slower but massive memory is critical still valid up-to-date, not only with dynamic memory but with memory management in general. Larson’s Compacting GC as a function of the number of memory regions to be freed (R), the amount of operational data (A) and the amount of available fast memory (H). He postulates two optimal allocation/deallocation strategies: strategy no.1) maximise R , if $A \ll H$ does not hold, and strategy no.2) set $R = H$ when $A \ll H$.

Apart from the mentioned restrictions from [12], GC is also restricted due to addressing. When XOR-calculated edges link memory regions, then the garbage cannot be localised the traditional way because addresses belonging to objects are not absolute but are relative. For example, this may affect object fields or pointers to some next element in a list. Thus, the next and previous elements in a doubly-linked list may be calculated, if any, by just one relative offset instead of two absolute addresses (namely pointers).

[128] suggests a Generational GC, so allocated regions are assigned an age value that encodes a period that object may remain in memory until being collected. If an object is rarely used, then after some iterations, that object may be moved into a bigger memory space which may be slower to access. However, if an object is often referenced, then that object is moved to a faster memory region – this is in analogy how a program is managed by OSs and other memory managed facilities [261], [181], [260], [217]. Runtime performance is approximated close to the optimal solution based on extensive practical heuristics tracked and Sun’s experiments.

[119] assesses current SSD-drives regarding different access operations. The characteristics of access operations on HDD-hardware drive behaviour is much closer to heap access than those of SSD-drives – if implemented as such. Essentially, heap writing is, on average, ten times slower than reading. GC on SSD-based drives using a greedy-strategy is worst at a waiting rate of 45%. The worst significant performance experience is achieved by writing through all-new blocks. Writing blocks of consecutive data chunks achieve the best performance with GC turned off.

Calcagno et al. [53] notice programs with a high abstraction level do not always have an advantage over programs with a low abstraction level altering heap. For example, it is found that GC often is ineffective in functional PLs. Functional programs often cause small but dangerous programs. On the one side, the danger is due to inaccurate uses of pointers. On the other side, it is due to side-effects that cripple down the performance.

Waite-Schoor [234] suggest the first and most popular wide-spread approach. A counter characterises the approach for each heap element. The counter changes when elements are either freed (holding no further references) or

when new elements are allocated. The allocation is due to resources that the OS manages. The same goes obviously for deallocation.

About 50 different well-defined GC techniques in total can be counted [127]. The more recent approaches are all focused on parallel execution. The chances of further research on GC brings a break-through soon are nearly nought and not expected. The meaning of such research is even more diminished by recent significant hardware improvements and available analysis tools. After all, as also discussed, GC's overall role due to plenty of memory available changed over the years and is no more such a hot topic as it used to be in the previous 2-3 decades.

Code Introspection: Introspection means on runtime static program units are available in a dynamic environment so that code may be loaded, modified and added on runtime, e.g. for an object method. Naturally, introspection makes basic reasoning much more complicated due to the Halting problem and, finally, the program verification in total. All CI issues are theoretically bound by decidability and depend on PL and assertion feature and what is allowed during runtime. In any case, a dependency mechanism must be implemented which controls communication between caller and callee. For instance, in C++, CI is based on RTTI [243] and in Java [96], each object has a unique identifier of a complex struct, which is then read on runtime.

Forman [99] defines CI in Java as a possibility to read and modify data structures and the loaded program itself during runtime. Thus, code not only needs to be loaded but also compiled beforehand or interpreter on runtime. The loading of objects is performed within a particular container providing all life-cycle operations needed. Statements with reserved meaning perform alteration and access to classes, objects, and components.

Cheon [59] gives a short review of recent CI issues with Java and provides tractable solutions. Questions are hardly up-to-date, and almost all questions are resolved by now. As executing unknown code is not only a security threat, it may also degrade soundness and completeness. Here only a concise specification could take countermeasures. It would be unfortunate to have a method with a specification that looks complete but would eventually not run, and the reason for that would be that specification is still missing some essential parts, especially when the specification is already bloated. Imagine that there was just one case that would not work or work wrong among many working cases. In order to tackle this problem, Cheon formulates critical circumstances that always must be taken into consideration:

- 1) Loading must be possible at any time, where name clashings must be excluded in a container.
- 2) On runtime, object accessors must obey typing.
- 3) It is tough to track the specifications of inherited objects altogether. It is hard to understand huge

hierarchies — therefore, keep hierarchies flat.

- 4) By its nature, specifications usually refer to objects in stack or heap — how then to behave exactly w.r.t. introspection and stack windows, since stack unrolling may invalidate and roll back to a previous stable state.

Nevertheless, what exactly is then considered "stable"? That would need to be considered from the user's perspective as well. Major application fields on introspection are application loadings and web-servers, loading and access facilities for dynamic runtime libraries, e.g. [282].

E. Existing Tools

[224], [27], [223] present an excellent introduction to SL, accompanying tools. SL is a Substructural Logic [218], [219], [89], which is free of constants, e.g. boolean values and uses symbols as structural replacements, so as constants. In SL as structural rules serve according to [218] rules of thinning, contraction, substitution. Constants are dynamic memory cells (see sec.III). In the rules ", " is replaced by \star , which separated two non-interleaving and differing from each other heaps, except said differently. Dynamic memory heaps are inductively defined. The operator \rightarrow , e.g. in the expression $a \rightarrow b$, defines a relation between symbol variables on the left-hand side and some value expression to the right (e.g. an object). Examples on SL imply the conventions lists, as well as other SL-specifics, hold. The frame rule states that if a subprocedure call does not alter parts of the heap, so there exists some frame denoted by F catching this invariant behaviour, then for the antecedent, it is sufficient to prove that the Hoare triple without F also holds. Let us consider an example of the frame-rule on heaps (definition later):

$$(\text{FRAME}) \frac{\{P\}C\{Q\}}{\{P \star R\}C\{Q \star R\}}$$

Here, P and Q are pre-and postconditions, R denotes the heap frame. This principle is a basic modularisation rule, and we will refer to it when needed, except when stated differently. If recursive specifications are allowed together with functionals, then the core frame rule might be violated because the context may be modified by any calling instance (can be implied from [36] and [211]). Thus, recursive specifications must be generalised.

[27] performs verification examples based on SL for an unbound arithmetics over offsets to pointers with increasing arrays and recursive procedures. For example, $p+x$, where p is a pointer and x an integer variable, is not decidable in general. It attempts to define the dynamic memory recursively by a closed built-in rule set. Berdine et al. [27] question whether typing is a self-esteemed verification (cf. obs.1.15). The answer is that verification is not typing, as discussed earlier. The paper implies non-decidability of unbound pointer use leads to fuzzy trigger events in GC, even for very trivially looking expressions

as offsets. Furthermore, it leads to an ambiguous rule set selection for verification based on greedy heuristics.

Bornat [44] suggests a similar model to SL, which he calls "remote separation", and transforms data objects into an array. Thus, any object becomes a list. Naming convention, the object identifiers, and field functions slightly differ. Nevertheless, all object fields are interchangeable between both models. For a general uncurbed definition of heaps in this model, Bornat postulates that first-order predicates are required.

Hurlin's [121] main contribution to SL are newly introduced patterns for multi-threading. He suggests unblocking functions that improve performance for the sake of a partial blockage of complex cells.

Not all heaps insist on a full specification, which might be shortened by using the anonymous operator "`_`".

Parkinson [195], [194], [193] presents an object-oriented extension of SL [224] (before Hurlin), using Java as incoming language. Modularity and inheritance are modelled using the "inversion of control and "abstract predicate" (AP) family. Bornat's [44] object accessors can easily be implemented in terms of preexisting rules from an existing Hoare calculus supporting arrays – there are no needs to break (accidentally) rules in this case. For instance, the frame rules on objects remain unchanged since the actual difference may be handled in additional rules critical for objects only. He mentions, the dependency between predicates stratifies predicate calls. His paper implies the built-in predicates he suggests cover most of the stack and heap, but they cannot be used to define user-defined predicates. Assertion predicates, which heavily differ by syntax and semantics from the input language, are not restricted in types. However, the use of symbols has a series of restrictions due to the non-symbolic use of "ordinary" variables decorated with additional constraints to mimic symbolic variables used in class logics. Factually, predicate symbols are used as locals in imperative PLs, and they cannot appear arbitrarily – this, however, is a hard limitation. As future work, he pleads to research in more detail: method calls from inherited classes, static fields, CI of objects, inner classes and quantification of those in predicates.

The theorem prover "Smallfoot" [27] is the first to implement SL by reference. It currently works experimental and has a minimal set of built-in predicates for heap definitions. Apart from that, no further predicates are allowed, including user-defined. The current implementation permanently crashes, hangs, and tons of related errors are present. Arbitrary uses of some tactics eventually lead to non-termination or other system errors. After all, it is still a great tool to get familiar with SL, and some examples make its help to understand the theory behind much better. The verifier system "SpaceInvader" [54] is Smallfoot's successor and includes simple abductive reasoning elements. "jStar" [86], [194] can be considered as an object-oriented extension of Smallfoot. jStar supports

class invariants and some heavily restricted APs. It turns all program statements into JIMPLE (IR), which is close to IR from GCC (GCC's original IR was first and called GIMPLE [171]) and is used internally by a corresponding Java-object to perform the verification, which is all Java-implemented. For industrial use, this makes perfect sense. Verifast [124] incorporates an input C-dialect. It allows user-defined definitions with nearly the same restrictions as SpaceInvader in APs. In case of a proof refutation, the user must manually modify proof commands and provide hints to proceed with the proof. Hurlin's prover [121] is experimental also and very closely related to [86].

Cyclone [109] is a heap verifier based on RC (see sec.I-C1). SATlrE [199] is a verifier based on Shape-Analysis [232] and is implemented in Prolog, which is very unusual compared to all others. "SATlrE" differs from the other tools introduced by shapes together with their dependent shapes are not calculated again from scratch, instead only altering edges are. "Y-not" [187] is an SMT-solver implemented fully in OCaml.

Finally, the approaches (1) to (4) and program utilities shall be honourably mentioned. (1) KeY/VDM++ [23], [271] allows an industrial use of object-oriented specifications and an integration with UML, which initially does not support proofs of dynamic memory. (2) debugging and profiling tools, most prominently Valgrind [254] or ElectricFence [128], [91] [141]. (3) integrated into programming packages and libraries, such as within compiler projects, such as LLVM, SAFECode [75]. (4) transforming programs and assertions into semi-structured data [20] with optional post-mortem transformations [125], [87] (see sec.I-C). Sec.I-A3 contains a detailed review of abstract interpretation. Valgrind loads an executable program containing debugging symbols with calling arguments into memory and replaces all dynamic memory access with special instructions. Thus, each invocation records each invalid access to memory as well as memory leaks.

GCC [252] and LLVM [253] are compiler frameworks. Both contain modules on static analysis, such as [154], [75]. Khedker's [137] proposition is a static framework based on transitive closures upon graphs to analyse data dependencies. The CompCert-project [43], [161] proposes a purely academic framework for soundness analyses based on transformations for the PowerPC architecture only using the general-purpose verifier platform Coq. Other general-purpose verifiers that are relatively robust include PVS, Proof General, Isabelle and others. A concise comparison of verifiers, including those mentioned, may be found in [92]. Verifiers specialised in dynamic memory may be found in [307]. Appel [13] lists recent issues that are resolved successfully. Articles from the iX-journal [140], [139] consider it most comfortable to use dynamic verifiers (all of which mentioned earlier for the problems described in sec.II). The static analyser ESC Java (stands for "Extended Static Checking for Java") [96] introduces a modular specification fully in Java (see

[105], [28]). Unfortunately, pointers are absent, and the memory models assume that all data is in a heap. ESC does not consider CI. Java-ML [20] proposes yet another Java-based specification.

"Jahob" [283] proposes a prototypical verification of linked lists for Java-programs based on functionals and is implemented in a LISP-dialect. A heuristic is used, which imposes on rules a strengthened filter. This project's objective is automation and runtime improvement due to specification abstraction using higher-order functions (cf. with Paulson's approach [198]).

Verifiers that fulfil industrial use include, e.g. KeY [182]. The popular but mainly academic-only verifier Baby Modula 3 [2], [56] may be applied to some more complex examples but suffers from the scalability restrictions described in sec.I-B.

II. Issues related to Dynamic Memory

This section formulates typical problems with dynamic memory verification by carefully analysing the essentials from the previous section. Afterwards, a short motivation is given for each problem on why research on that particular problem is actually from a theoretical and practical perspective. Under dynamic memory (see fig.25), that part of RAM is meant the OS loads for a process [163], [164].

A heap is an unorganised memory portion (see fig.27) compared to organised memory, e.g. stack. Organisation implies automatic allocation and deallocation of local variables w.r.t. scope visibility (see fig.26), with an agreed implicit linkage between elements. In the case of a stack, the ABI ABI forces an implicit and strict ordering of element accommodation into the local variables' current stack windows. For example, declared locals are visible on a conditional branch and maybe overlayed by other local variables with the same name.

While program execution, local variables are not visible outside the block in which they are defined. The same can be noted with procedures and subprograms. Visible locals, as well as call-by-value parameters, are pushed onto the stack when entering a procedure. All local variables from the current window are popped when leaving a procedure. Additional deallocations may be required invoked by destructors due to objects' life-cycle [252]. In fig.26, a stack window, basically a memory interval, is illustrated with some local *o*, an integer "1" in this example. There is also an array (local, not determined) of pointers to "*o*" and the upper element. All elements are compactly pushed to the stack, so there are no gaps between stack elements.

In contrast to this, structs do not have to be compact, except the keyword "packed" is used. However, in practice, often, this is not the case. Hence, optimisation for runtime is the best default behaviour than optimisation for size.

In contrast to this, heap cells of a process may be spread all over the heap memory segment. The visibility of heap cells does not depend on syntax blocks. It depends only on statements with a special meaning for allocation and

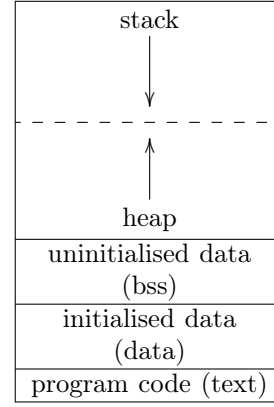


Figure 25: A typical memory layout for a Linux process

deallocation. If after a program statement or at the end of a block statement, a heap is not freed, then by default, the entire heap is freed with the most global destructor available to the process before passing control back to the OS. In C++, `.dtor` does this task when all (global) objects' destructors are called in declaration order. The OS defines concrete stack and heap layouts. Both are in virtual memory space. At this stage, we are not further interested in allocation/deallocation techniques. Neither stack nor heap does have an apriori fixed boundary on process initialisation. The boundary is depicted by a dashed line in fig.25 and is not fixed. If the stack size may increase vastly, then the available heap size may be balanced. BSS (block start symbol) denotes a memory segment, which contains all global variables without an initial value assigned (occasionally, other non-local variables may be included depending on the compiler implementation [243]). All other non-locals and non-dynamic variables are assigned to the ".data" segment.

Program code is loaded from the ".text" segment and has a starting point called the starting process memory address. Absolute addresses substitute all relative addresses representing program variables after process loading. In practice, the program code must have different stages of program execution, e.g. destructors.

Any cell from any segment from fig.25 may be addressed linearly. It implies that access to memory content may be obtained in consecutive increasing order. Any memory cell has a successor at address $+1$, where "1" is a symbolic value here denoting one type's actual width to be iterated over once. However, according to fig.25, there is an imaginary floating boundary, which in practice is never reached, which is good for a process' stability. For example, if some integer is of type `uint16_t`, then "1" may become "2".

Let us pay attention, that "exclusive-or" (\oplus) allows us to express two pointers in a doubly-linked list just by one "jump field". The content of the field stores $a \text{ xor } b$, where a denotes the start address of the field,

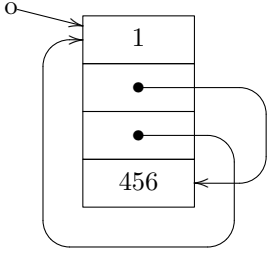


Figure 26: Example for a stack

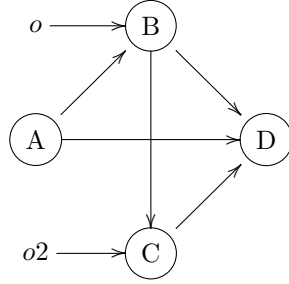


Figure 27: Example for a heap

and "b" denotes the next field, s.t. $a \oplus (a \oplus b) \equiv b$ holds, as well as $(a \oplus (a \oplus b)) \oplus (a \oplus b) \equiv b \oplus (a \oplus b) \equiv a$ (see [196], [240], [308]). Thus, one pointer may be saved, although GC requires a different algorithm. Assume a doubly-linked list is enqueued, then reachability of all list addresses needs to be calculated first.

The memory models of C++ [252], [253] and Java [128] differ significantly. There is even a different memory organisation and translation between C and C++, although the latter's syntax may be considered an approximate superset. So, for instance, PLs compatible with ISO C++ do not consider a GC. In Java, GC often leads to overhead. Fortunately, garbage collectors operate in parallel Java threads in a VM environment. The Java VM, as a compromise solution, integrates Generational GC, which, for a practical need, is an optimal compromise solution. In Java, all variables and data are stored in a heap compared to C or C++ (but not C#). C-dialects generally allow weak typing [243]. Incompatible types upon varying bit interpretations may be transformed without a cast in C, e.g. a byte into a real by a union.

A. Motivation

The technical report [176] contains a research study over several decades of traced back and committed errors in numerous open-source and commercial software development projects. The characteristics found in [176] hardly change from year to year. This reluctance can be confirmed by several newer research studies, e.g. [177], [113], [5]. The results in [176] imply commercial Unix distributives contain over 23% of incorrect code, wherein open-source platforms, the rate is significantly lower for GNU-Linux it is 7%. The authors note that the rates are stable for years. Moreover, their conservative estimation is that commercial software has even more errors than open-source. According to Miller, these are the most frequent errors committed during programming:

- 1) Errors related to pointers and fields. In commercial applications, the authors emphasise bugs are either not located at all or are located too late, e.g., porting to a different platform. The former happens during software development and at early testing phases due to a lack of test coverage. The authors are

very concerned about the errors are not obvious to detect and delay later projects, including portation projects due to unforeseen issues that need to be fixed first and affect several products at once. Here invalid memory access is the most often problem – an indicator of vague and contradictory design decisions, which precise specifications may catch. Uninitialised data cells or memory leak also occur and lead sooner or later to unreachable and lost data, or even program crashes.

- 2) Either invalid memory access to arrays beyond valid boundaries or modified data structures even if a pointer remains unmodified.
- 3) Insufficient checks when working with files. Often reading is done not thoroughly enough. Implicit assumptions are made that do not match with invalid files.

Dynamic memory verification is problematic because the heap is described in one way, but the program is described differently and still corresponds [126] in an indirect manner. If interpreting a heap as a graph (see next sections) and a program as an instruction sequence of that graph, then the description of just the same heap may be done in different ways. While the heap is checked, both sides must correspond. Hind [113] asks the fair question considering the huge efforts already put into over several decades, why AA is not solved yet. He calls for research on soundness and performance (cf. fig.1) since aliases not yet found may degrade compiled code. If during compilation it was safe to assume some two local variables must alias, then register allocation [181], [135], [237], [238], [226] could reuse one CPU register instead of spilling several registers, and it would consequently reduce the need of synchronising two or more registers (see [245], [154], [76], [181]). Even with a conservative estimate, it would mean a great runtime improvement and a significant code simplification.

Hind [113] is certain about effective alias localisation requires a thorough analysis of the incoming program. Landi [151] proposes a grouping of AAs. Analyses are NP-hard problems. He suggests the following groups: (1) aliases that "must-alias" or "may-alias" and (2) intra-procedural AAs as well as inter-procedural AAs. Intra-procedural AAs are effective [114], where interprocedural analyses are ineffective and still require improvement. Hind [113] proposes, in general, to use only very poor visibility scopes of variables when programming. It can be observed that Hind's proposition is also beneficial from a performance viewpoint since long-living locals may, in general, degrade register allocation and scheduling effectiveness. Hind also proposes to minimise visibility towards dynamic allocation and aliases.

In his paper [119], Hu considers the technical correlation between writing cycles and reading from recent flash memories. Hu's approach is of interest here because of the permanent storage characteristics in large, giving

theoretical upper bounds in the small. The OS allocates heap randomly when needed, and several patterns should be considered when designing and reasoning about heap-managed memory regions. Reading is approximately ten times faster than writing on average, and reading and writing handy memory blocks is dramatically faster than addressing individual blocks due to cache coherency and other architectural facilities. Hu's main contribution in dynamic memory is that GC is not needed for almost all considered applications. Significantly, turning GC off extends the lifespan of flash devices remarkably. Hu equitably questions whether GC nowadays is still an issue for non-critical applications. Except for being used as permanent memory, flash memory can also be used as RAM disks in embedded devices. It may crucially influence the runtime speedup of programs.

In order to improve the unsoundness of results in several verifiers, Bessey [33] suggests: (1) getting rid of programs with CI, (2) always stay with the principle: "simple errors shall be found simply", (3) accept finally that numerous iterations do not necessarily improve code quality, after all, this is because verification is a qualitative technique and not quantitative. As already mentioned, point (1) is not essential, after all. It only changes the time when a particular program code is defined. On one side, CI increases flexibility, but on the other side, the semantic analysis may be cribbled, for instance, type checking or other phases – or those that need to be implemented on a new as-you-execute base, so moving it towards a full-scaled interpreter with all its consequences. Naturally, verification is theoretically bound towards static checks mainly due to the Halting problem. Due to the restrictions mentioned (see [221], [39], [235], [117]) hot-code updates (code that is updated during runtime) is not considered any further. In general, when speaking about erroneous access to dynamic memory, these immediate consequences are implied:

- access to inaccessible memory
- access to uninitialised memory
- lack of dynamic memory by the need
- decrease of runtime characteristics
- memory leak (see following).

Each of those is discussed next. Errors may lead to very unpredictable situations. In the worst case, a program may continue execution with corrupt data. In the best case, the program may terminate immediately when the first corrupt data shows up with an appropriate hint. Termination may indeed be considered the best of all errors since a defined behaviour is still better than any undefined. Termination signals a fault, which complies with soundness and completeness.

Bessey [33] summarises his analyses on successful verifiers in general and explains why they are successful. Most essentially, Bessey considers in favour of a verifier:

- Theorem proving is an exact science. Therefore,

regardless of heuristics and tactics applied, the key to success lies in soundness and how quick a valid proof can be derived. Quantitative results shall always be considered very critical. A verifier that finds fewer known errors than another is undoubtedly weaker. Bessey remarks heuristics towards rule selection such as "take the longest rule first" in practice regularly succeed, and there is reason to believe this is some meta-pattern. Although not explained by Bessey, his experience might be explainable by this observation: Long rules are very concrete cases that are often only applied to prepare a shorter but more aggressive rule. It is recommended to choose representative examples as suggested by [282], such as OSs as input program verified in practice or open-source projects.

- Non-trivial proofs shall be standardised. If possible, sub-processes shall divide detailed verifications and join them by handing over IRs in a most normalised and most simplified form before continuing the primary verification process. Concrete rules must be separated from structural rules. The main motto shall be: "simple errors shall be detected simply". If, however, the motto is not obeyed, then any verification may be considered useless.
- Exclude as early and as often as possible extensions to input languages, which may be excluded w.l.o.g. of expressibility, e.g. the "hot update" of code. Full specifications of program systems shall be forbidden. Same counts for code fragments that are not subject to specification (see def.1.3) at all or can only be specified by tremendous efforts, which would not be in balance with the expected specification size. Everything should be simple and plausible. Surprises in proofs are always nasty.

As mentioned earlier, heap programming may slow down [153]. There are cases when an algorithm implemented using the heap rather than stack may be faster [12], especially when GC is turned off. However, this observation may not be lifted in general (see sec.I) since each algorithm would require a separate investigation. Efficiency using heap also significantly depends on freed and active lists heavily managed by the OS. A stack-based decrease in performance is often due to superfluous instructions pushed into the stack and popped from the stack as an ABI-guaranteed convention.

This problem worsens with big objects that do not fit in ABI-reserved registers. Since then, everything must go to the stack and requires additional copying routines that otherwise would not be necessary. Every copying of data structures may be potentially superfluous, either it is a word or a complex class type, especially when talking about pointers. If its value entirely passes an object(s), any duplicate is redundant and wasted. Unfortunately, redundancy detection is intentionally kept too conservative in GCC and LLVM [253] due to some scarce situations where

it might be essential to avoid unsound removal. It can be found that any algorithm implemented with heap may be rewritten solely by using stack, as suggested by Meyer (see [173], [174]). Addresses of arbitrary objects may freely be moved from heap (to stack) by assigning them to a fixed stack window under the condition that every stack element remains uniquely addressable. This conversion requires a different convention on consecutive type ordering. The maximum threshold for pushing objects to the stack must be obeyed — the threshold increases when the heap decreases (see fig.25). Array elements, e.g. uniform objects on the heap, may be pushed to the stack by copying elements consecutively. It is essential to obey the stack type sequence. Thus, the only unanswered questions relate to: (1) Is it indispensable for the sake of an algorithm's readability? (2) Is this variant always valid or not? The first question is highly disputable, especially when comparing tree elegance in heaps (see [196]). The second question is not always decidable, mainly when limits are known during runtime. Of course, a sizeable pre-allocated array may fit all needs. However, a lavish memory allocation is not a reliable approach and not helpful in practice. Everything that may be pre-calculated statically is only of use in terms of the stack. Unfortunately, often there are situations when this is unacceptable, e.g. for technical reasons. It must be stated that both stack and heap are finite.

Let us consider some concrete dynamic memory problems in a not yet defined C-dialect.

B. Issues related to correctness

Example no.1– Memory leak.

A leak occurs whenever memory is allocated to dynamic memory but never freed. Often this does not cause an (immediate) crash. However, this is far from satisfactory. A program may crash any time after start without further notice. Often this happens at an unexpected moment. Whenever the OS finds a shortage of available memory or the OS is not granted access to a memory region requested. It may also happen when the OS runs out of free memory. However, this may happen not too often nowadays since the memory available is much more than it used to be one or two decades ago. In a typical scenario, some flaky program runs a couple of minutes or weeks without any incident whatsoever. Then suddenly, it may be caused by some external event registered by the OS, that flaky program crashes without any prior notice. This kind of problem might be a nightmare to reproduce, and these problems happen in real life.

Often, debugging, if possible at all, cannot localise the origin of the error, but random code places every time executed. So, the genuine problem may come from somewhere else actually – what is observed on a crash is just the symptom, but not necessarily the cause for the symptom(s). Occasionally to diagnose the genuine problem might be quite challenging sometimes.

```
MyClass object1 = new MyClass();
...
object1 = new MyClass();
...
(end of program)
```

Figure 28: Example for classically instantiated objects

For example, the program's problem from fig.28 is the content of *object1* never utilises after the next assignment. Assume according to ISO-C++ [243], the OS would start to process ".dtor", and all globals call their destructors where applicable, then by lousy coincidence, that phase may crash and could be extraordinarily difficult to debug. This situation occurs because, on every run, the thresholds responsible for crash or non-crash could change dynamically. So, the problem is about the analysis of "danger-zones", which may leave occupied cells reserved.

Example no.2 – Invalid memory access.

From all examples in this section, invalid memory access to dynamic memory occurs relatively often. This problem occurs because some object is uninitialised or has a temporary value that semantically becomes invalid at a specific code position. It is worth noting that objects are occasionally handled differently among different OS if they are in ".bss". For example, OS Windows often does not initialise locals. That leads to cells having uninitialised values on runtime. If this is not handled safely by the algorithm, the behaviour gets erratic. It may also mean a security breach to the process. The reason is incorrectly assigned or uninitialised variables for a given algorithm (see fig.29).

```
...
// object1.ref equals NULL
// (no assignment, or left NULL initially)
...
value = (object1.ref).attribute1;
```

Figure 29: Example for an incorrect assignment of an object pointer

Naturally, debugging should focus on all possible assignments after the variable declaration of *object1*. Invalid memory access may include access to objects that may have been freed before access. Invalid memory access may also refer to an incorrect data representation of address or type, e.g., a processor word regarding an incorrect type (cast) with pointers. E.g. typecasting (down- and upcasts) in terms of the C-language between (int*) and void*, alternatively (char*) or (int8_t*) may go utterly wrong if specific platforms do not consider those are equivalent. Moreover, depending on the platform

```
sizeof(struct(int a, char b)), sizeof(int)+sizeof(char)
```


does not have to be identical as described. Struct sizes may also vary depending on bits to represent.

Assuming a occupies 2 bytes, and b occupies 1 byte (depending on a platform may differ again if platform-dependent types are being used), the content may become one of the variants in fig.30.

$a_0a_1a_2a_3$	$a_4a_5a_6a_7$	$a_8a_9a_{10}a_{11}$	$a_{12}a_{13}a_{14}a_{15}$	$0\ 0\ 0\ 0$	$0\ 0\ 0\ 0$	$b_0b_1b_2b_3$	$b_4b_5b_6b_7$
$a_0a_1a_2a_3$	$a_4a_5a_6a_7$	$a_8a_9a_{10}a_{11}$	$a_{12}a_{13}a_{14}a_{15}$	$b_0b_1b_2b_3$	$b_4b_5b_6b_7$	$0\ 0\ 0\ 0$	$0\ 0\ 0\ 0$
$0\ 0\ 0\ 0$	$0\ 0\ 0\ 0$	$b_0b_1b_2b_3$	$b_4b_5b_6b_7$	$a_0a_1a_2a_3$	$a_4a_5a_6a_7$	$a_8a_9a_{10}a_{11}$	$a_{12}a_{13}a_{14}a_{15}$
$b_0b_1b_2b_3$	$b_4b_5b_6b_7$	$0\ 0\ 0\ 0$	$0\ 0\ 0\ 0$	$a_0a_1a_2a_3$	$a_4a_5a_6a_7$	$a_8a_9a_{10}a_{11}$	$a_{12}a_{13}a_{14}a_{15}$
$a_{15}a_{14}a_{13}a_{12}$	$a_{11}a_{10}a_9a_8$	$a_7a_6a_5a_4$	$a_3a_2a_1a_0$	$0\ 0\ 0\ 0$	$0\ 0\ 0\ 0$	$b_7b_6b_5b_4$	$b_3b_2b_1b_0$
$a_{15}a_{14}a_{13}a_{12}$	$a_{11}a_{10}a_9a_8$	$a_7a_6a_5a_4$	$a_3a_2a_1a_0$	$b_7b_6b_5b_4$	$b_3b_2b_1b_0$	$0\ 0\ 0\ 0$	$0\ 0\ 0\ 0$

Figure 30: Examples of bit/byte ordering

That is why making arbitrary assumptions on a specific platform is wrong. When Intel is assumed, but PowerPC or ARM is found with a 64 or 32bit processor word, assumptions will eventually fail. If a field is not initialised for some reason, then a harmless looking program such as in fig.31 may not terminate or terminate not correctly.

```

object1.next = object;
...
root=object1;
while (root.next!=NULL){
    printf("%d", object.data);
    root=root.next;
}

```

Figure 31: Example of an incorrectly linked pointer and non-terminating program

Example no.3 – Dangling pointers and aliases.

A dangling pointer [8] appears when initially several pointers (possibly aliases) share an object, and some pointer manipulations lead to one of the pointers is mistakenly separated from the remaining. Although intuitively clear, this may be challenging and imprecise in practice. An analysis requires not only to check the procedure where a pointer is declared but also to check the whole fan-in and fan-out. Containing objects of dangling pointers shall be disposed of since those are garbage by definition.

Pointers that become dangling may be turned into non-dangling during program execution and vice versa. However, heap elements becoming garbage are lost forever and must not become addressable again. Dangling pointers may be the result of the situations described. Furthermore, a pointer may become dangling by different memory cell interpretation using "union", as described earlier.

Example no.4 – Side-effects.

Instead of copying unneeded data structures, often pointers may be more effective. However, this approach has the risk unaffected data regions may (accidentally) be

corrupted. This problem is a generalisation of example 2 and 3: Pointers do not alter on runtime, but the content suddenly gets changed. It can be generalised: modification suddenly alters other variables. A modification of a heap shall not alter other heaps.

C. Issues related to completeness

Example no.5 – Problems with expressibility.

Some issues with expressibility have already been presented in this section. Essential expressibility issues are: (1) Can all valid heaps be specified under the condition that all valid heaps are syntactical correct for a given rule set? (2) Do invalid heaps always verify false? (3) Which predicates may be used? (4) Which constraints must predicates obey? (5) Which dependencies between heaps exist, and how adequate are formulae it? (6) Which restrictions are there w.r.t. symbols in heap definitions? (7) How to define single or multiple heaps best? (8) How to express dependency between aliases? (9) Are existing heap definitions ambiguous, and if so, how to exclude ambiguity effectively? (10) Which abstraction level is required for a precise and handy heap definition, particularly for verification? (11) How much further can a heap be abstracted, s.t. is well understood by specifier, verifier and developer? (12) Can heap formulae be transformed, s.t. there is no need to re-specify on local program code updates? (13) Can more familiar concepts from programming be reused, s.t. specification and programming become more familiar to a programmer?

Example no.6 – Issues related to a complete representation.

According to fig.1 in [249], Suzuki proposes "safe" pointer operations. As described earlier, its use must be handled with care since the clockwise rotation of one data structure may quickly lead to corruption or disposal of another data structure, for instance. Apart from that, implicit assumptions are too often not immediately apparent. Suzuki's approach and similar approaches introduced almost always suffer from incomplete rule sets and incomplete heap definitions. Too often, the situation is this: Given a rule set of 25 rules. Questions: (1) Are those 25 rules enough, or are any further needed? Do even existing rules need to be shrunk? (2) What is the overall policy with overlapping or even redundant rules? As any heap state depends on a given program statement, heap subsets need to be formulated and then compared with the expected. (3) Does it make sense to limit expressibility, s.t. termination is decidable but with acceptable limitations? (4) Is there a possibility to specify and verify only parts of a heap? (5) May a simple(r) heap model be proposed, s.t. a proof using a simple data structure and incoming program shall be simple? For instance, list inversion should be simple (cf.[223]).

Preferably, a verification should not insist on a complete specification since a full specification and verification is not economic in practice and is in harsh disbalance to

the benefit ever gained on average. It is often sufficient to specify only focus on procedures and class objects one may be interested in the practice. That would mean leaving unrelated program fragments unspecified. An engineering requirement is to add additional constraints at random code places wherever the engineer wants to perform a more detailed analysis (see the algo.1). A developer may also be interested in adding checks at random places in code in addition to pre- and postconditions.

Example no.7 – Issues related to the level of automation. According to the quality ladder from fig.1, these problems belong to the second category. Main automation problems from earlier sections are related to defining dynamic memory rules and separating them from other non-related rules. If rules related only to heap are put into a separate formal theory, then the whole verification may be better logically structured, and the overhead might be diminished and more reliable towards future modifications. Such a separation attempt would also diminish the amount and complexity of rules. There is a need in comparing specifications with heap states. Unfortunately, currently, all existing approaches make comparison manually (cf. following sections). It is hard to predict when a theorem is used and when to be applied with the needed symbols. The same problem exists while transforming one heap state into another. A locally optimal proof may still lead to non-decision.

While transforming a heap deductively, confluency shall be improved (cf. fig.7) – this can converge by abduction. The necessary theoretic restriction might be expressibility. Terms may be partially defined during static analysis, or they are non-decidable in general. Offset limitations in arithmetic expressions leads to expressibility limitation, but also a higher automation level. So, the question arises how generous are algebraic heaps then? How proper is strict typing for an input PL?

D. Issues related to optimisation

Example no.8 – Issues related to runtime performance. Runtime performance problems directly compete with soundness (see fig.1). Assertions about "pointers alias" or "pointer do not alias" are more important than "may alias", but those are more difficult to find. The second and third assertion has a more substantial effect on generated code. The faster the generated code is, the more effective it becomes because a lack of need to store CPU registers to stack means improvement. Unfortunately, data dependency analysis over pointers is much more complicated than with locals because a pointer's p content may alter at potentially any place in code. Therefore, AA is hard. Often it can be observed from frameworks with pointers that some function on pointers works only for a very restricted domain since pointer have a very high expressibility, and

it is challenging to guarantee the most general assertion upon pointers.

Remarkably, if a data structure is used only once and there are no duplicates, far less effort is needed for immediate modifications than in cases with duplicates. In implementations, two main approaches can be observed: either complex and straightforward variables are passed manually (though including auxiliary remarks, e.g. in C by using the keyword register [252]), or in exceptional cases, AA is done (mainly intra-procedural only [253]). This case is not excluded from C [252] and can be achieved using const. Let us consider a small motivating example: list reverses with alteration [223], [196]. Here, the initial list vanishes. Depending on the concrete context, this might be desired behaviour. Reynolds' algorithm traverses the list only once in the forward direction. There is no need for next or previous pointers.

Thus, a list does not need to be copied. All operations are performed on the given list, which heavily speeds up. If only the data structure changed and the original is safely not needed afterwards, then the old list may be dropped, and the algorithm's overall behaviour would speed up. GCC and LLVM [252], [253] do not perform such a test yet. May the ABI be modified, s.t. non-referenced objects are popped from the stack by the caller [243], [252] unconditionally? May existing objects in dynamic memory not just be used immediately, mostly when objects are known for sure they are not changed on calls? It must be mentioned that the proposition made in [240] is non-standardised.

However, the average efforts needed on linear lists seem to be strongly reduced, and the GC changed drastically.

When the number of iterations is known apriori to entering a cycle after static analysis (see [12]), then the code portion may be optimised responsible for memory allocation and alignment. All problems related to optimal GC, beginning with White-Schorr's algorithm [234] and continuing until today, are more than extensively researched [127]. Micro-operations related to dynamic memory are done by the OS, which traces memory resources, including stack and stack for each process.

Example no.9 – Issues related to program security and access protection.

In analogy to stack overflow [138], when the stack is flooded with undesired dangerous data in order to compromise a program by moving the actual instruction pointer beyond the actual stack window on procedure call or return from the procedure — there is also an attempt of pushing a return address to malicious code during GC the heap [130], [8]. Obviously, in contrast to stack, the heap does not contain program locations nor addresses of (modified) program code. Consecutively, the attack based on malicious code injection may not work on-the-fly as with the stack. Stack overflow may lead to security risks for an individual program and comprise the whole OS.

When at stake, the problem worsens even more when remote servers and services and specifications are interfaces when access via device driver is acquired (cf.[71]). Since several instances may load drivers simultaneously, the risks of not being able to restore due to a heap issue are susceptible and delicate. In the worst-case, non-reliability may crash the core OS as it is an existential thread to monolithically designed OSs GNU-Linux.

III. Expressibility of Heap Formulae

This section researches heap models, namely heap graph and heap predicates, which will later be reasoned in logical programming. First, the differences between heap and stack are elaborated, and crucial properties are analysed. Then, occurring phenomena are observed based on the fundamental problems from the previous section. Finally, based on a pre-existing model, an (extended) heap term is introduced, and properties are investigated. The heap term definitions are implemented in the Prolog-dialect (see sec.VI-H).

Assume some imperative program is given, which has the CFG [137] as shown in fig.32. Let us explain another example from [76] the difference between automatically allocated and dynamically allocated variables. Automated variables are automatically allocated and deallocated. These are bound to a stack window. The stack window contains all locals and parameters passed in before and out after a procedure call. These stack-local variables shall not be mixed up with "fan-in" or "fan-out" parameters.

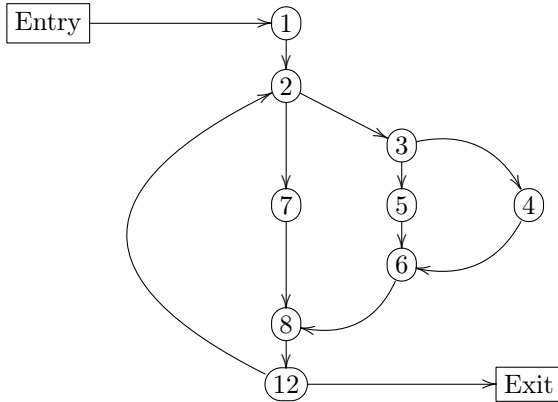


Figure 32: Example CFG.

According to fig.32, visibility scopes can be established. A scope interval of the whole procedure [Entry,Exit] denotes a simple directed graph in which passed variables are visible to all vertices between Entry and the ending vertex Exit.

A "block" is defined as a joining sequence of non-branching program statements. Next, in order to avoid possible naming clashes with existing definitions, the SSA-form as defined by [76], [237], [245] shall be used. A

branching might be any branching or unconditional jump. However, immediate, unconditional jumps shall not be allowed for the sake of expressibility considerations in the following. Assume some blocks have locals represented in SSA-form as in fig.33.

block 2: $b_0=4$; $a_0=b_0+c$; $d_0=a_0-b_0$;
block 7: $b_1=a_0-c$;
block 3: $c_0=b_0+c$;
block 5: $c_1=a_0*b_0$; $f(a_0)$;
block 4: $a_1=a_0+b_0$;

Figure 33: Example of SSA-placements by basic blocks

Let us assume further, all other blocks are either artificial, empty or do not contain relevant just introduced variables. Block 5: f is a block that accepts one variable. At first glance, there is nothing unusual. However, if inside f access to a parameter's content is performed, which in C can be done using the de-reference operator "&", variables may be altered even beyond f 's boundaries. Fortunately, this scenario can be caught with the earlier analysis of f 's incoming and outgoing variables. Even if the scenario described may not frequently occur in practice, this scenario is the reason why a vast majority of code optimisation remains slow for the sake of soundness in the most general case. If in block six a was redefined, then $a_2 = \phi(a_1, a_0)$. Function ϕ is auxiliary. It means a union of different definitions that can be made over a variable. ϕ is an implicit function (hence its origin: phoney). The whole concept of implicit functions seems intriguing on the first look, as we may see later when it comes to heap definitions. What the phoney functions do is express data dependencies of variables compactly. It may be applied to arbitrary automatic data in imperative programs. The data dependency structure, in general, cannot be a tree. ϕ -functions forbid this when there are dependencies, which refer to some previous block, which might be outside a loop.

Regardless, we are most interested in existing algorithms on scope visibility using ϕ -functions [245] of locals. We rely on the remark that upper bounds exist regarding visibility scopes. These bound may be defined recursively over the stack. Bounds are calculated using the CFG and ϕ -functions of each local (dominator algorithms may be found in [245], and the classic survey is [76]). If variables are redefined in two different branches, then the content after a join may differ and its index increases.

When attempting to apply a given SSA-form to dynamic variables, it must fail due to the following reasons: (1) there are program statements that allocate and deallocate dynamic memory explicitly. These statements must not necessarily be in the bounds of a procedure. Heap cells may unconditionally exist after some procedure is called and even after the stacked pointer is freed. So, the definition place in code (same goes for redefinitions and

deallocation), and its place(s) of use differ from those for automatic variables. So, the two places often do not match. Pointer's content may alter even when pointers are not referenced immediately. (2) Size, frequency and the context of heap memory allocation are, in general, not always defined (see fig.25).

In analogy to CFG, not only the content of a variable may be annotated in graph vertices [97], but also assertions about dynamic memory may be annotated. An example may be Khedker's framework [137] which analyses for each pointer using a very conservative algorithm – assuming a may-alias for all not found pointers based on Floyd's transitive closure algorithm. Thus, after every program statement, not only is the considered pointer re-calculated, but potentially everything related to it. Khecker's algorithm is based on a long bitfield. Some optimisations may be done towards the bitfield. However, it is not done because the estimated improvement would not necessarily be significant and, most importantly, beneficial and a base to many flow analysis techniques described. Mandatory checks of all dependencies can hardly be simplified further due to transitive comparisons and connectivity checks. The comparison of aliases chosen is based on Horwitz' [118] and Muchnick's [181] algorithms.

Observation 3.1 (Organised Memory and Fresh Context). The stack is organised memory. The order of elements in it is well-defined. Every time a procedure is called allocation and deallocation are performed (may also be the case for compound statements). Every time in a new context, a new allocation means containing all elements from the surrounding procedure and is initially not linked.

Next, an analogy might be shown in which every state of dynamic memory may be recorded as a single state. Any state transitions may exist, but there must always be an entry and an exit, even when the heap is empty. On exit auxiliary states may be modelled, s.t. all finite states are merged with the final exit state.

Observation 3.2 (Unorganised Memory and Unique Context). The heap (as the unit of dynamic memory) is unorganised. On one side, elements may be in arbitrary order and allocated anyhow. On the other side, the heap graph (yet to be introduced in sec.III-A) alters after each program statement, and a new context linked to the current state is absent. There is only one unique context.

For example, functional PLs assume the principle of independent data as their central concept. It guarantees a fresh context permanently. It contains initial parameters without dependencies. Afterwards, the result is assigned and returned to the caller. A continuation (see [180], [273], [78], [255]) is a calculation state which is passed to another instance by need. The transiting state is not interrupted since the context does not change. Equal states mean the whole state of calculation, which contains stack and heap (see fig.25). In the case of higher-order functions, a contin-

uation can nicely be described by denotational semantics. Denotational semantics, in general, describes a program as a function, so it is assumed the correspondence to any environment is superfluous or not existent. Continuations do not change, but process stack windows do. Joël [180] considers continuations in functional-logical contexts by the example of common LISP. Introductory remarks are: (1) continuations lead to copying, pushing and popping of memory regions, transition addresses and returns to the stack, (2) readability and algorithms' modelling may significantly be improved. Remark (1) causes concerns about performance (cf.[12]). Remark (2) has priority and is in contrast to the first remark. Therefore, a meaningful compromise must be found in practice.

Observation 3.3 (Phenomenon of Remote Manipulation). Due to the separability of memory cells and due to dynamic memory in general, the phenomenon of "remote manipulation" may be encountered, as was described earlier. The phenomenon is that the evaluation of some (sub-)expression in some program statement may "magically" alter some unrelated content being addressed by some pointer which is not part of that expression and hence may come as a total surprise to the caller of that procedure. This phenomenon is neither locally bound to a specific BB only nor a procedure but can modify variables even beyond a procedure's boundaries.

Observation 3.4 (Variable Visibility Scope). A pointer's visibility scope, in contrast to static and logical variables, may from the place of allocation till deallocation be interrupted one or more times, even if the pointer does not change (cf. fig.34, where the axis denotes the line number for some given program. The solid line indicates stacked variables may overlay visibility) because of progressing stack alteration over BBs. It may happen accidentally, intentionally, or even temporary whilst the invocation of some program statements only.

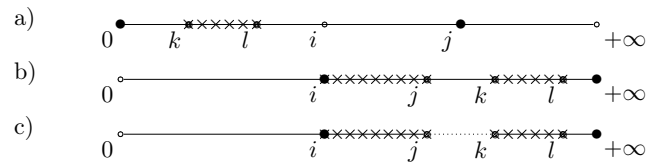


Figure 34: Visibility of locals in a),b) and dynamically allocated variable in c)

In the example in fig.27, if $\text{free}(o.B)$ frees object C from the heap, access to C cannot be provided via $o2$. If $o.B$ redefines a freshly allocated object, then C is not notified about it, except if the new object is assigned the same address the previous old object used to be. For the sake of formalism, it can be agreed upon that dangling pointers are assigned "nil" and a universal model, even if, in reality, the pointer contains the old address. So, all other pointers

need to be analysed too.

Other pointers may be aliases, which are vertices in a corresponding heap graph. Those may be o or $o.B$ (see issues from sec.II). Heap cell interpretation depends on a pointer's type, which is checked accordingly during semantic analysis. The type does not change anything except for subclassing (see sec.IV).

A. Heap Graph

Now the fundamental aspects of dynamic memory are discussed in detail (including obs.3.1, obs.3.2), it is time to think about a heap graph representation. Early but still essential to agree upon detailed heap models are introduced in sec.V and sec.VI. The essential pair of heap allocating operations are "malloc" and "free". Essentially, compactness and flexibility determine the success of a heap graph model.

Heap graph as regular expression. In the beginning, let us consider the simple graph \mathcal{A}_1 , which obeys the constraints discussed earlier. This graph could be described by a regular language and can be recognised by a simple finite automaton, as shown in fig.35, and was suggested by the author, e.g. by [299], [293] in the context of semi-structured data as Prolog terms. Regular expressions can also be justified because they describe a heap graph consisting of states and explicit state transitions of some calculation.

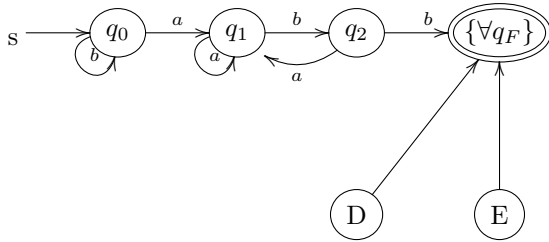


Figure 35: Example finite automaton \mathcal{A}_1

Arden's lemma [79] turns the determined finite automaton into this regular expression: $b^*(a^+b)^+b$. So, what do this heap graph and the corresponding expression denote? The graph's vertices represent a set of non-interleaving heap cells. The graph's united final state is $\{q_F | \forall q_F \in F \subseteq Q\}$. Naturally, all finite states may be merged into one finite state. For example, in the graph, vertices $D, E \in Q$ denote some states that merge to $\{q_F\}$. The graph's edges are directed links encoded as addresses of a processor word's width in an edge's source. So, the first question that arises: How are heap edge labellings represented? These may be pointers or object fields, so locations in both cases.

Both cases are not satisfactory because pointers always have to be dealt with individually from all other memory cells since those are in the stack. Second, labelling all edges must be distinguishing. Assume this is the case, then

regular expressions cannot be described by the proposed compact representation (see following). However, this means the initial very compact notation suffers dramatically. Third, it is not yet clear what exactly are "initial" and "final" states? At least, a pointer considered at one moment to be initial may be final at another moment or neither nor. However, it could serve if certain strict constraints were invariant, e.g. by default, the last function parameter always denotes a final state. An initial state may always be denoted as any stack variable transition - this is always valid to do. Final states are more challenging to describe, e.g. whether labelling is the last one for some given calculation or not. If q_F were dropped, then the expression would be undefined. A new state might be introduced which accepts those transitions that signal a final calculation of the data structure.

Now assume, all mentioned problems are resolved by now acceptably, and we continue with the question on heap alteration by using program statements after finding all (dis-)advantages of regular expressions. If that notation were compact, then it would be required to check whether this is a stable solution regarding alteration. If a tiny modification was made, then only one edge should change, and the overall regular expression should not change much - if so, then this notation would be tractable indeed. If this notation does not meet the requirements mentioned, then it shall be reasoned, and perhaps another model should be chosen.

For example, the last graph is added a new edge b . The new graph becomes \mathcal{A}_2 and is illustrated in fig.36. This graph is semantically equivalent to the regular expression $b^*a^+b((a^+b)^+ + bba^+b(a^+b)^+)^*b$. Now we remove edge a and obtain \mathcal{A}_3 (see fig.37).

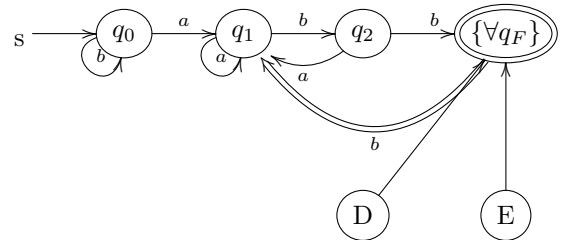


Figure 36: Example finite automaton \mathcal{A}_2

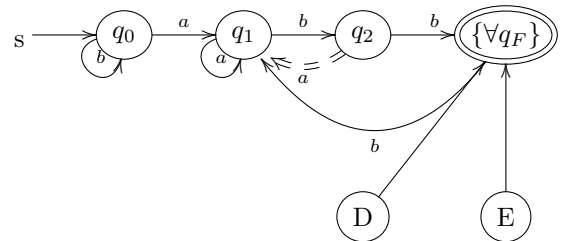


Figure 37: Example finite automaton \mathcal{A}_3

We get the regular expression $b^*a(a^*bb(\varepsilon + ba^*bb))^+$. All three expressions may be rewritten and further simplified – here, however, this is not the critical factor. The real problem is if an edge is inserted to any place in the graph (and this could happen indeed in practice), then the regular expression given may heavily change – in both cases, on average and on worst case quite severely. The bigger the heap graph gets, the more complex the regular expression gets. It would be optimal and similar to the previous expression. The linear equalities system based on Arden’s lemma does not change much on the alteration of a single edge in general. For example, the first graph can be described as shown in fig.38.

$$\begin{array}{ll}
Q_0 &= aQ_q + bQ_0 \\
Q_1 &= aQ_1 + bQ_2 \quad \underline{bQ_1} \text{ denotes insertion of} \\
Q_2 &= aQ_1 + bQ_F \quad \text{an outgoing edge from } q_F. \\
Q_F &= \varepsilon + \underline{bQ_1}
\end{array}$$

Figure 38: Equalities describing the automaton

It is not difficult to see, the system of linear equalities has a solution, but it heavily differs from the previous, although almost all equalities remain the same. However, the corresponding regular grammar heavily changes.

Heap graph upon alteration. First, it is required to research the sequence of joint program statements to discuss some "adequate" representation of the dynamic memory and the situation with pointer and transition descriptions. Let us consider list inversion as proposed in [223]. Both Reynolds [223] and especially Parlante [196] bring numerous examples, and we decide on one. Given the program from fig.39 in a C-dialect with a special syntax for pointers. In the program listing, i , j and k denote pointers. $*(i+1)$ can grant access to the memory cell following i , which depends on i ’s type. Naturally, elements are linked to each other. They are supposed to be a unit and monolithic and a contiguous memory region in a heap, even if a similar syntax reminds us about it. The example may clarify the semantics from fig.40, where a number denotes the iteration step until the loop is visited.

```

j:=nil;
while (i!=nil){
  k=*(i+1);    // access to the element following i
  *(i+1)=j;    // the pointer following i alters
  j=i;
  i=k;
}

```

Figure 39: C code example for list inversion

i denotes a list until entering the loop (cf. fig.4). On leaving the loop, i is empty, and j contains the initial list of i in reverse ordering. No copies are created. The input list

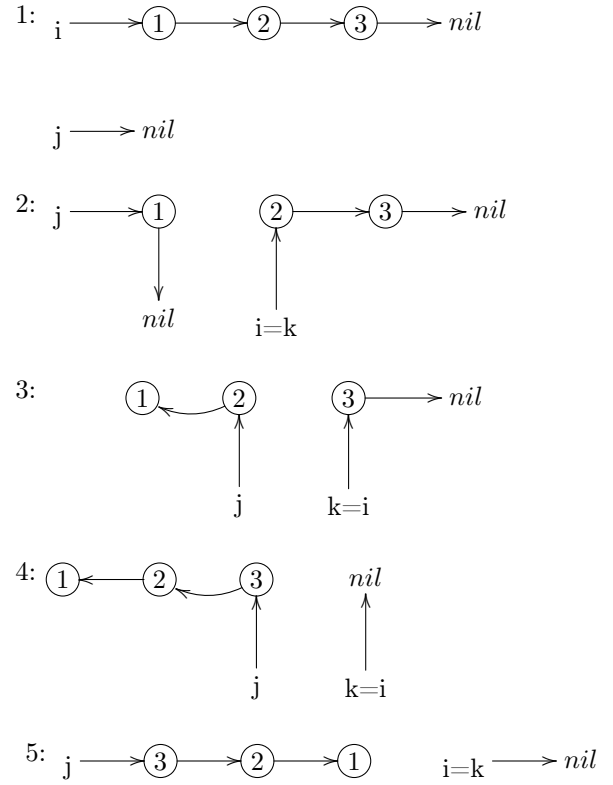


Figure 40: Example heap trace for list inversion

is iterated precisely once. We notice edges are not labelled in the example due to the selected implicit definition statement over pointers. Of course, in general, heap edges may be labelled. However, pointers exist, which are local variables. Those are (not) assigned to heap vertices (when a pointer is uninitialised). k is an uninitialised pointer until entering the loop. It is not hard to notice that compact notation is barely used, for example, from (1) to (2). The main reasons are expressibility and adequate graph representation. Although the presented regular notation is bare of any use, compact notation still played an essential role in formulating an automated approach (see sec.VI).

It may be obvious why other global approaches, like RC, SA and others introduced in sec.I, failed. The reason is the same as demonstrated by the last two examples. Dodds’ approach [87] is also not further considered for the same reason, even if here, instead of the heap graph transition is described. Still, his approach is not specific to pointers and does not consider imperative PLs (see sec.I). Regarding graph transitions as specifications, there are further harsh reasons against (see next section).

Observation 3.5 (Graph-based Representation of Dynamic Memory). The graph in dynamic memory (heap) can be defined as triple $(V, E, L \times V \cup \{nil\})$, where V are the heap graph vertices, E is the edges set, L is the set of pointer labellings. A pointer points either to some $v \in V$ or to nil , e.g. when it is uninitialised.

We observe the graph represented: (1) separately by each component, or (2) in a mixed form. Obviously, (1) is not straightforward because it describes the vertices separately (in this case, independent from pointer labelling), and as such, the final specification might become too bloated and thus too hard to read. A heap's specification must be easy to read, short and adequate. Approach (1) requires denoting each vertex separately and insert all of them into the specification. As mentioned in the introductory by numerous examples, the disadvantages outweigh all benefits; hence this approach is dismissed. Approach (2) assumes naturally either (2a) describe by vertices or (2b) by edges. The problem with (2a) is that there are duplicates in specifications since edges fully identify vertices, and because of two vertices, there is always at most a single edge. Each edge related to a given vertex must be annotated, identical to having each vertex a list of all neighbouring vertices. Unfortunately, such an approach is very cumbersome. For example, one vertex is connected to two or more vertices. So, that all neighbouring vertices also need to store the source vertex into their lists. Moreover, if a heap is altered, then specification massively changes – this is something that needs to be avoided at any cost.

In contrast, approach (2b) only describes edges, and vertices are inserted into these. This approach contains fewer duplicates than with approach (2a). If only directed edges were allowed, then the total amount of checks would be halved. Several outgoing edges per vertex are prohibited because one pointer may not point to more than one cell simultaneously. Also, on a closer view, program statements more frequently alter the calculation state than vertices do. Moving data, GC and allocating heap memory are quite expensive, which may invoke system calls to the OS. Conversely, pointer manipulations are cheap since no additional conditions need to be met, and no resource management is involved. In the worst case, the approach mentioned allocates and utilises garbage, but pointers hardly change. Then it is essential to recall whether this approach can be corrected.

Fig.60 (a) illustrates a regular graph whose maximal vertex degree is three. Here, we assume, each vertex represents an object with three fields that are pointers. For approach (2a), 11 vertices need to be specified, each of which has three edges, where the number of incoming and outgoing edges may differ, and this needs to be considered separately. In total, there are 18 edges. In approach (2b), only 18 edges need to be specified. Here, vertices connected with more than one edge may be just symbols. The more a given graph differs from the full graph, the fewer edges need to be specified. If an edge alters, then a specification needs to change less, namely the altered edge only. If a vertex changes, then all connected edges need to be checked. A directed graph may be traversed in $\Theta(n) = n$ to scan both sides of an edge. According to approach (2b), given some rule

set using predicates, proof might be found faster and friendlier to handle. Pointers and access expressions to fields denote graph vertices (see sec.IV). Inaccessible fields during specification are beyond our interest because, by definition, those memory cells are garbage (see sec.I) and lost forever. Nevertheless, in specifications, our concern is on locating ambiguous places.

Jones [127] defines a "heap" as a contiguous leap of RAM with size 2^k , where $k \geq 0$. The leap may be interpreted as any data structure depending on the application. Alternatively, it is a sequence of non-contiguous blocks of non-contiguous words. For example, a tree may have fillings between its vertices in the memory layout, but individual vertices may not be interpreted other than (CPU) words. According to Jones, an object is a set of memory cells that are not necessarily interconnected but whose fields are addressable. Each allocated memory cell has a pointer. The question may arise whether an object is alive or not between allocation and deallocation? It is hard to disagree with Jones that fragmentation is a problem. However, intra-object fragmentation is excluded.

Cormen claims, on page 151 in [72] as Burstall [51] does, any data structure in dynamic memory is automatically a tree. Here, a tree does not only implies some relation " \leq " to its child vertices V_j , but it also obeys the ordering $f(V_{parent}) \leq f(kid(V_{parent}, j)), \forall j$. Atallah [18] considers a heap as an array interpreted as a tree with wide memory usage but with high flexibility. In Atallah's monography, several definitions of heap might be found. First, a heap is defined as a priority queue (see page 79). Fibonacci heaps (cf.[101]) are presented as specialised and effective queues for insertion and deletion. Next, on page 105, a heap is defined as a binary tree preserving all queue elements with priority. In contrast to RAM, Atallah emphasises on page 111 the importance to reference on pointers only. Thus, any random access is excluded. The responsibility of heap separation is assigned to connect heaps (in an implicit way) rarely and shall be supervised by a programmer and software designer. Rarely connected heaps may effectively be separated and can effectively be processed by different methods. It is hard to disagree with Cormen on random addressing because of the previously mentioned regulations regarding expressibility. However, the programmer's responsibility in creating a data structure can hardly be disputed, even if occasionally data structures shall be trees and not graphs. Sleator [241] suggests for the sake of minimalistic GC and faster heap access to balance trees and their sibling vertices, which leads to an overall fast search below $\Theta_{min}(n) = 1$ and deletion below $\Theta(n) = \log(n)$. Even if his proposition is intriguing, still this approach is not further considered because it is currently not needed enough w.r.t. a small number of conjuncts and the possibility of linear search by locations.

Reynolds defines a heap set as a union of mappings

from address space onto non-empty memory cells' values. Following this definition, a heap is some address set that refers to some well-defined data structure (without further notice). Reynolds' definition is structuralistic (the word origins to philosophical structuralism) because, strictly speaking, a single heap as an individual and an independent unit does not exist in Reynolds' terms (cf. sec.V). Pavlu [199] defines a heap as an arbitrary graph.

B. Predicates

Apart from the previous remarks, the most critical requirements towards predicates are: (1) after each statement touches the heap implies the corresponding graph alters too minimally (2) heap specification also allows minimal alteration only.

When obeying these requirements, then the next question relates to adequacy representation.

In ancient Greece, Plato's philosophical school taught the concept of epistemological definition and research. The object is to describe some object of interest by following a well-known allegory in a strictly defined order of questions and answers in dialogue form between two sides: a human who has some object in front of himself but is not able to show it to others due to isolation, and another human in freedom. As often is the case with Greek legends, the earlier human is massively hindered from his luck and captured in a cave. This man is keen on the understanding that object but has minimal possibilities. He communicates with his outside world only by his voice and some eternal torch. The torch's light hits the object and casts only the shadows on the cave's wall visible to the outside world. However, the shadows are not exact, but the captured man's voice helps understand that object. This allegory is better known as the "allegory of the cave". It proposes to describe an object as a two-sided dialogue whose primary goal is to find properties of that object which may not be evident in the context of minimal communication bandwidth. There are several philosophical concepts very close to the allegory, so-called "Gedankenexperimente" (from German "thought experiments"), for instance, a dialogue that is speechless and written only and better known as Searle's "Chinese Room". For simplicity, we restrict ourselves to Plato's classic cave myth, which already contains all we need to understand the phenomenon of heap predicates here. Intuition may narrate to us what a heap abstracted predicate may tell us, but comparing previous definitions of it will lecture us the opposite. An abstract explanation of a heap in practice is a concrete placement of incoming terms and symbols, but it hardly tells us about incoming properties (so-called reification — a concept of abstraction for a concrete realisation). These philosophical concepts will help us bring some light to heap representation and processing in this section and sec.V, sec.VI. A modern philosophical discourse in idealism can be found in Hegel's classic (philosophical) method. First, a thesis is established

founded on numerous observations made. Second, more sophisticated analyses are performed and checked against the established thesis — here, additions may be added to the theory build-up. However, counter-positions are formed, s.t. a counter-thesis is established. Third, thesis and counter-thesis are examined thoroughly, and synthesis is formulated — an assertion based on previous theses. One can notice all heap properties are thoroughly analysed at the current stage so that a first proposition thesis might be formulated here. An in-depth dialectic analysis (after Hegel) is required to localise the potential imprecision — all very close obviously to the latter methodology mentioned.

Regarding reification, heaps must have both syntax and at least one semantics — both will be defined soon, generalising the heap term as a (heap) predicate. Therefore, a summary is needed to find the essence starting with Aristotle's predicates called syllogisms. A syllogism is a logical rule containing three assertions (also compare with Hoare triples): if A and B , then C follows. This oversimplification is just fair for our objective. One remark must be made. Most deductive systems nowadays do not use the over 2000 years old syllogisms but on slightly modified variants (see later), as may be of help in sec.VI.

As was seen, the previous attempt in using regular expressions failed because modifications affected a heap graph's transitions. A minimal requirement refers to a rule set but not to a given assertion to be proven itself because the representation is not too stable for the given problem. In general, reasoning about and transforming abstract notations (cf. sec.IV-C) is widely discussed and under constant research. For example, Conway's cell automata [278] attempt to establish invariant expressions — to mention one example.

In sec.VI, the inverse method is observed: patterns are observed from which properties of rules are derived. Predicates connect heap graph vertices regardless of whether in the context of a formal or natural language first of all. According to semiotics, a predicate may have two meanings: (i) an intuitive meaning, this relates to the question: "What exactly is a heap supposed to mean"? (ii) a connotative meaning — What is a heap associated with exactly? Next, the question related to heap representation arises: may/must a heap use symbols and relations and what exactly are they denote? May perhaps a heap be defined partially?

By assessing (i), it is found that a heap represents a set of pointers, which are somehow connected and point to heap objects. Since previously issues were found related to ambiguities and massive potential restrictions, it is wise to keep definitions as atomic as possible and reduce everything to a minimum. By assessing (ii), the input program determines the connection between all components, and the heap is not organised. That implies graph vertices may occur in any order, at any place in specifications, and the memory layout they fit in must not be contiguous. Heaps may be linked to others.

It is important to note that a predicate must provide a possibility to express a connection between two heap graph vertices but must also express that a link is forbidden. If there is no such possibility, then separation automatically becomes an implicit result of an analysis of all heaps, which is unfortunate due to effectiveness concerns. The definition of connectivity has different levels of graininess: "connected", "maybe connected", and "not connected", "maybe not connected". With time, a heap's mode is not of immense significance: first, because "connected" and "not connected" may be checked in linear time. Second, the search efforts are discrete, especially before and after each program statement. In heap predicates, due to logical operators, varieties must all be considered. So, for instance, logical disjunction must be expressible regardless of the non-repetitiveness principle and predicate negation. The solution to this question is solved in sec.IV, where a proof over heaps will be based upon logical programming. We shall not lose track that pointers may be arbitrary, including locals and dynamic variables and object fields.

In the very first work on SL, Reynolds [224] introduces the \star -operator over heaps and introduces the following properties:

Theorem 3.6 (Reynolds' Spatial Properties). For propositions about heaps q, p, p_1, p_2 , the set of free symbols $FV(\cdot)$ and a binary spatial disjunction \star the following rules (1-6) hold:

- (1) Non-repetitiveness:
 $p \not\star p \star p, p \star q \not\star p$, if $\exists q, q \neq \text{emp}$
- (2) Commutativity:
 $p_1 \star p_2 \Leftrightarrow p_2 \star p_1$
- (3) Associativity:
 $(p_1 \star p_2) \star p_3 \Leftrightarrow p_1 \star (p_2 \star p_3)$
- (4) Neutral element:
 $p \star \text{emp} \Leftrightarrow \text{emp} \star p \Leftrightarrow p$
- (5) Distributivity:
 $(p_1 \vee p_2) \star q \Leftrightarrow (p_1 \star q) \vee (p_2 \star q)$
 $(p_1 \wedge p_2) \star q \Leftrightarrow (p_1 \star q) \wedge (p_2 \star q)$
- (6) Quantification:
 $(\exists x.p) \star q \Leftrightarrow \exists x.(p \star q)$, if $x \notin FV(q)$
 $(\forall x.p) \star q \Leftrightarrow \forall x.(p \star q)$, if $x \notin FV(q)$

Proof. Non-repetitiveness implies that p does not occur twice – this matches the non-repetitiveness of heap descriptions [219]. However, in contrast to classic logical assertions, $p \star q \not\star p$ does not imply strict p as a separate assertion. The reason is not p is mandatorily connected with q . As supposed, descriptions and intuition about the separating operator might be referred to as introduced on separability. Though this a solely scenario only. The problem is in describing the element search on the heap. However, this does not imply that one heap may suddenly vanish from an assertion about two arbitrary heaps. This difference must be considered.

Rules (2-4) are understood so that the heap graph

definition may be well-founded. The soundness of rule (5) may be shown by applying induction to the remaining rules. Here two cases may be distinguished. First, when p_1 and p_2 clash and second when there is no clash with q .

Rule (6) may seem obvious. Hints may be possible naming clashes that may be avoided by variable renaming, which in terms of λ -calculus is an α -conversion.

Neither rule (1), nor (6), nor any other rule do not exclude free variables as in verifiers like Smallfoot or jStar. One variable may be used, e.g. as a pointer in one heap and as a referenced pointer as subexpressions in another heap. \square

Let us consider the heap from fig.41.

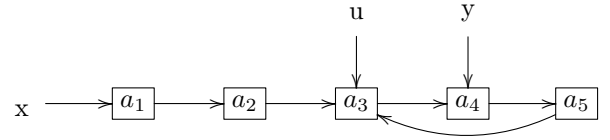


Figure 41: Example heap with pointers x, u, y

The heap has references to the following pointers x, u, y . The rectangles frame its content which is a_1, a_3 and a_4 . Burstall suggests not to reference the content directly but by an address. He also suggests noting all intermediate pointers and labellings in some minimal model, s.t. a big heap may be equivalent to a single compact expression $x \xrightarrow{a_1, a_2, a_3} y$. This expression has overlayed meanings: pointers x and y exist, a path between these is guaranteed, and naturally, the whole path describes part of the overall heap graph. In linear lists and trees pointers, "next", if any, are skipped by default. One expression after Burstall denotes a whole linear list. The heap graph describes the union of such expressions. Let us consider the following data structure, a "cactus" (see fig.42).

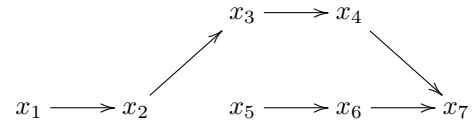


Figure 42: Example cactus in dynamic memory

For its description, only two expressions are required. x_1 is a pointer, which is on the stack. Assume, all other cells are not related to any pointer locations. Consecutively, it is all in dynamic memory. A handy, though compact, notation destroys the previously established minimality criteria. Hence, Burstall's notation is no further consideration. However, the abstraction of predicates is considered towards a more flexible description based on an edge-based graph.

For full pointer and expressibility analyses, random access to dynamic memory is not required. All accessory operations may be fully substituted, as mentioned earlier, by either read or write upon valid non-random locations only. If, however, random heap access is needed for performance, most often access to consecutive memory cells, this would be a typical case of an algorithm using the stack.

Allocation of arbitrary memory sizes is not dedicated to heap only. It may be implemented by both stack and heap. Checks are going to be performed neither for dangling pointers nor for garbage nor invalid cells. It is not hard to imagine auxiliary functions over memory regions that may perform any computable transformation. Pointers can only provide path accessors and be well-defined. C(++) Objects are special struct, where visibility is private by default rather than public [243]. Objects can either be fully on the stack or heap, where the pointer location itself is most likely in the stack, except when pointers of pointers are taken into consideration for a full heap accommodation. On occasions, when stacked objects are tiny, they may even be put into CPU registers. The latter variant fundamentally does not exclude the use of dynamic memory. It must be stated, $e_1.f_1 \mapsto val_1$ may mean object e_1 may have two or more fields, and in generated code, $e_1.f_1$ may be different by use and memory layout then, for instance, $e_1.f_2$ due to optimisation heuristics [135], [181], [252] regardless of previous assumptions. However, this does not imply a required division on the input PL or specification language, where any object must be modelled as a contiguous memory region whose fields may have references to further objects.

As introduced to SL there were made numerous contributions and some propositions regarding improvement [224], [223], [51], [121], [193], [195], [194], [44], [281], [27], [26], [190], [233] (see sec.I). Reynolds [224] introduces the "sequentialiser-operator" $" , "$ for an implicit linear list construction. "Implicit" means no assumption is made on how the concrete memory layout looks. It only insists addressing has to be consecutively obeying the order of the $" , "$ -operator. Thus, from the earlier example, a cactus may be defined as $x_1 \mapsto x_2, x_3, x_4, x_7 \wedge x_5 \mapsto x_6, x_7$. Alternatively to the implicit operator, some explicit pointers may be used, e.g. by pointer containing objects or Bozga's [45] length-delimited definition.

As discussed earlier, higher expressibility may be achieved by parameterisation. Parameterisation may fundamentally make existing heap predicates more flexible. In order to achieve this, symbolic variables must be introduced to assertions. An assertion may be valid or invalid for a given heap. Symbols are not typed apriori, as terms are in Church's type calculus. Initially, heap predicate-argument types seem closer to Curry's type calculus. The introduction of (symbolic) variables, predicate definition, is closely related to parameterised terms in the λ -calculus.

So, a predicate is abstracted and must be applied to other predicates. In contrast to the functional paradigm, a predicate may return more than just true or false. It may unify partially defined unground terms (see sec.IV).

Let us consider a recursive example of a binary tree taken from [224]:

$$tree(l) ::= nil \mid \exists x. \exists y : l \mapsto x, y \star tree(x) \star tree(y)$$

According to Reynolds' definition, the operator \star defines a heap, consisting of two separated heaps. It shall be mentioned, as stated earlier, that the initial definition of the \star -operator may still contain connecting elements. Thus, starting with one tree x , there may be a path leading to some adjacent tree y regardless of $tree(x) \star tree(y)$. It is assumed the whole region pointed by x indeed does not overlap with the analogous region pointed by y . It is essential that without any change of the given predicate, this was made impossible. However, during further parameterisation and predicate alteration (cf. predicate tree in sec.IV), the problem does not change. More illustratively, this is depicted in fig.43. Abstraction of predicates will be formalised and a new approach introduced in sec.VI.

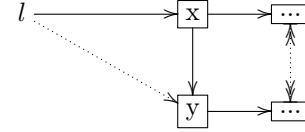


Figure 43: Example of schematic separability of heap

Based on Reynolds' definition, Berdine [26] introduces the heap satisfaction relation as shown in def.3.7.

Definition 3.7 (Heap Satisfaction Relation). $"\models"$ denotes the model relationship over heap formulae $s \in \Sigma$, where a pointer is defined on the stack and pointing to content in the heap is denoted by $h \in \Pi$. $r(t_i)$ is the t_i -th component of structure r (see fig.44). E, F denote arbitrary assertions. $\llbracket \cdot \rrbracket$ is the functional denotation for some assertion mapping onto the boolean set.

$s \models E = F$ $s \models E \neq F$ $s \models \Pi_0 \wedge \Pi_1$ $s, h \models E_0 \mapsto t_1 : E_1,$ $\dots, t_k : E_k$ $s, h \models \text{emp}$ $s, h \models \Sigma_0 \star \Sigma_1$ $s, h \models \Pi \wedge \Sigma$	if $\llbracket E \rrbracket s = \llbracket F \rrbracket s$ $\llbracket E \rrbracket s \neq \llbracket F \rrbracket s$ $s \models \Pi_0$ and $s \models \Pi_1$ $h = [\llbracket E_0 \rrbracket s \rightarrow r]$ $h = \emptyset$ $\exists h_0, h_1. h = h_0 \star h_1,$ $s, h_0 \models \Sigma_0, s, h_1 \models \Sigma_1$ $s \models \Pi$ and $s, h \models \Sigma.$
---	---

Figure 44: Formal heap definition according to SL

A denotational semantics is a function $\llbracket \cdot \rrbracket$ of type $\Phi \times \Sigma \rightarrow \text{Bool}$, where Φ is a set of assertions on a heap, and Bool is the boolean set. For a given linear list $s, h \models E_0 \mapsto t_1, \dots, t_k$ with corresponding types $\forall i, j \in \mathbb{N}_0. E_j, r(t_i) = \llbracket E_i \rrbracket s, 1 \leq i \leq k$. Left of \models is the calculation state, which has type $\Pi \times \Sigma$, right of it is some arbitrary boolean assertion.

In [27], Berdine refers to problems, particularly the frame may remotely alter (see obs.3.3). However, deleting a memory cell's content referenced by some global pointer is a separate issue (see sec.I).

For the same reason, subprocedures are neither considered further. It must be noted that embedded procedures may only increase the complexity of a specification and verification w.r.t. expressibility. They may, however, not increase computability. Berdine fairly notices that the application of the frame-rule may lead to non-determinism of symbols to be substituted. However, when heaps are under investigation, non-determinism may be excluded by renaming and further constraints (cf. sec.V, sec.VI). Moreover, logical conjuncts fit into the logical PL (see sec.IV).

Further, the heap graph is refined according to [295], and afterwards, syntax and semantics are introduced, obeying the previous complex analysis.

Definition 3.8 (Finite Heap Graph). A finite heap graph is directed and connected. The graph may contain cycles and must be simple. It is transferable to dynamic memory by compilation, but also vice versa. Each vertex contains content, has some type and a memory address and occupies some contiguous memory region. In the case of object types, the target address (of any field) can be calculated from some offset base address, and the size an object occupies – both are derived from the object's type. Graph vertices do not overlap. For the sake of simplicity, but w.l.o.g. each edge's destination refers to some absolute address in dynamic memory. Locations may be assigned to vertices. Vertices are finite.

In contrast to sec.III-A, it is not intended to distinguish yet initial state and final states explicitly.

Implicit definitions, for example, in SSA-form, often succeed as they fully cover, though implicitly, data dependencies. The initial definitions contain implicit definitions, which are investigated in this work regarding heaps. Relations, spatial operators, and partially implicit definition refer to graph vertices, typing and symbolic variables. In sec.V, spatial heap operators are strengthened, constant functions and other conventions are introduced for objects. From theo.3.6, def.3.8, and previous conventions introduced (see [295]), a "heap term" may be defined.

Definition 3.9 (Heap Term). Heap term T is inductively defined as follows and denotes a heap graph.

$T ::=$	$loc \mapsto val$.. simplex (simple heap)
	$ T \star T$.. conjunction
	$ \underline{true} \mid \underline{false} \mid \underline{emp}$.. constant predicates
	$ (T)$	

where loc denotes some location. A complicated expression or some symbol representing a heap may serve as a location. val is a type, a compatible graph vertex with some value. \star denotes the spatial operator proposed by Reynolds (cf. theo.3.6, but replaced later (see sec.V, sec.VI))

\underline{true} denotes a tautology independent from some concrete heap. The same holds for \underline{false} . Predicate \underline{emp} is valid only when a given heap is empty. Otherwise, it is false. In sec.V, conjunction is strengthened and resolves in two operations. For logical assertions, logical conjunctions are introduced into the recursive definition of T .

Definition 3.10 (Heap Term Extension). The heap term extension ET extends T from def.3.9 by logical conjunctions and is defined as follows.

$ET ::=$	T	.. heap term
	$ p(\alpha)$.. abstract predicate call
	$ \neg ET$.. logical negation
	$ ET \wedge ET$.. logical conjunction
	$ ET \vee ET$.. logical disjunction

Logical conjunctions " \wedge, \vee, \neg " do not require further explanation. A predicate call requires it has previously been defined in Γ (considering def.6.5 and cor.6.6). Whilst a predicate call actual and expected heaps are compared. Free symbols from the predicate declaration need to be unified. Unified terms only contain bound variables. Otherwise, the call is undetermined (cf. sec.IV).

If a logical PL is used to reason about symbolic variables, then many restrictions, such as one-sided assignments, impossibility to refer to symbols instead of values, and many others (cf.[26], [27], [195], [193]) may be lifted finally. When unifying terms, then comparisons become simplistic, and gaps get filled by meaningful content. Otherwise, all subterms need to be compared manually and placed into the right places, but this is tractable, though it requires further differentiated conditions. It may result in new mistakes and even further limitations, but in practice, limitations are often observed when for the sake of the non-logical language, whole comparisons are dropped, or symbolic use degrades, for instance, when call-by-value. Usually, this can be observed mostly in imperative PLs, but also some functional ones.

Let us consider the predicate call (more details in sec.IV)

"?-pred1(s(s(zero)),_)"

where for the sake of simplicity, the first term is incoming, but the second is outgoing. Conclusively the question arises: Does some anonymous variable "_" exist,

s.t. predicate `pred1` holds for incoming term `f(a)`? If the answer is true, then the goal succeeds, and the result is dropped. If not, then predicate `pred1` does not hold. `s(s(zero))` represents integer "2" in Church's arithmetic (cf. fig.10). If, for instance, instead of `s(s(zero))`, say, `s(s(_))` is chosen, then the result may be derived, for instance, to

`s(s(s(zero)))`, then the query without alteration (see def.4.3) might be replaced by `"?-pred1(s(s(_)), s(s(s(zero))))"`, assuming the predicate has double-sided definition. In general, this does not only affect two but several directions. Prolog has a strict LR evaluation ordering. So, symbols may replace concrete heaps. If some goal requires a concrete heap and that heap is assigned in some later subgoal only, either the subgoal order may be changed, or the overall calculation does not terminate (see sec.IV).

Now, it is required to investigate the properties of the mapping from a heap definition onto some heap graph and properties of separate pointers.

Property 1 – Soundness.

Whenever from def.3.9 a strict difference is encountered between connected and non-connected heap (see sec.V), then syntactic description covers any heap graph. If normalising according to theo.3.6, including, for instance, prenex-normal-form, then obtained formulae commute. Constant predicates may be exclusions, and therefore may be single-sided enrichments: the set of satisfiable heaps maps onto one set representative. It is not hard to find out what a non-inverse mapping denotes in this context. Furthermore, when excluding anonymous symbols, then the syntactical description fully corresponds to a heap graph. By excluding the only sources of non-deterministic representations, it is easy to find the mapping is now isomorphic, and consecutively, two differing heap graphs may not be expressed by one description, and vice versa.

Property 2 – Completeness. A heap graph can be fully described by simple heaps and enriched by pointers. Knowledge representation of heap vertices may lead to syntactic antinomies if addresses of objects to be referenced are not distinguished. For example, if there co-exist $a \mapsto 3$ and $b \mapsto 3$, then it does not mean that both memory cells containing "3" are identical in practice. For modelling purposes, this means precisely it. Namely, if a new object is not allocated and no pointer points to that cell, then the pointer becomes an alias. Annotations may avoid this situation in the term-based object.

Pointers to pointers have an integer as address and therefore do not differ from other pointers. The difference between some integer and a given address is only up to its interpretation, namely a variable's type. On mappings from graph onto formula, the evaluation order and the predicate structure naturally may not be derived uniquely. The mapping might be generated, but it may differ. Assume a specific set of abstract predicate definitions is

given, then the mapping described would, in general, not be decidable because of the Halting-problem. The mapping from a heap graph to T is fully defined, obeying mentioned remarks. The inverse mapping is complete. If in $loc \mapsto val$, the left-hand side is no pointer, then the annotation may, in general, be done by an additional field $f: loc \mapsto_f val$. For a generalised structure of a heap graph, the additional annotation has no significance. Hence, additional fields are not announced by default.

Property 3 – Equivalence relation. For comparison might be used that \mapsto is a binary functor, and $a \mapsto b$ is a heap. Thus, it might be confirmed that the equivalence relation \sim maybe well-founded by showing properties (i-iii). It is agreed upon \mapsto has a higher priority than \sim . (i) Reflexivity: $a \mapsto b \sim a \mapsto b$. (ii) Symmetry: $a \mapsto b \sim c \mapsto d$, then $c \mapsto d \sim a \mapsto b$. (iii) Transitivity: $a \mapsto b \sim c \mapsto d$ and $c \mapsto d \sim e \mapsto f$, then $a \mapsto b \sim e \mapsto f$.

Property 4 – Locality. The heap graph, its corresponding term IR and its content hardly change on deletion, alteration or insertion of a pointer. Edge removal leads to a reduction to some simple heap. Alternatively, it leads to abstract predicate parameterisation or alteration of used abstract predicates because the relation between formula and graph is undecidable in general (see earlier), and therefore, predicates need to be considered separately. A maximal alteration may lead to vertex removal if no predicates because it means a single vertex removal and all its connected edges. An analogous insertion is tractable because edge insertion is done stepwise. In the worst-case scenario, predicates may lead to a formula, which is very different from the previous step. Hence, recursive structures are naturally and effectively described by recursive schemes, and one minor modification in a fragment does not affect all other elements, except neighbouring elements. This estimate is just heuristics and depends on a concrete algorithm and graph separability of most independent subgraphs. The same holds for the heuristic: "Some heap graph can be described better by abstract predicates than by compact descriptions". The separability problem is too general and beyond this work, particularly the integration of SMT-solvers (see sec.V, VI, cf. [85]).

In conclusion to this section, some notes shall be made on higher-order predicates. As found in the previous section, they do not have a theoretical meaning for comparing heap. Eventually, predicates having predicates as parameters seem to be promising regarding the expressibility of concise descriptions. However, considered heap predicates are inductively-defined. So, arbitrary higher-order predicates may destroy these properties if not imposing further constraints. Higher-order predicates over heaps may absorb recursion from rules, so recursion can no longer be noticed immediately within the rules — this conflicts with LALR, LL(1) and some SLR-parsers. However, theoretically, it does not break CF-mighty recognisers (cf.

sec.VI). Thus, it is considered not targeted when using anything different than formal grammars (see sec.VI). It must be noted by introducing higher-order predicates essential properties break, such as the CFG and calls with alternating evaluation order and subgoal processing, as well as static typing. However, from a heap expressibility's view, nothing changes. According to the quality ladder from fig.1, properties 3 and 4 belong to property 1, and the last note on higher-order predicate recognition and the second half of property 4 belong to optimal stability.

IV. Logical Programming and Proof

This section researches how a heap (see sec.III) shall be represented in Prolog and obeyed criteria. Afterwards, general theorems on heaps using Prolog are outlined. The syntax of terms and rules is defined. The cuts and applicability of recursive definitions are discussed. All this enables logical reasoning, which will eventually solve verification as designed in more detail in sec.VI-H. The abstract predicates' declarative characteristics are analysed in more detail reused later in sec.V and sec.VI to unify specification and verification. The languages are represented in terms of Prolog based on relations and accompanied by software metrics. Finally, a Prolog-based verification system is proposed. The representation and integration of objects w.r.t. Prolog is discussed.

A. Prolog as Logical Reasoner

This section does not introduce Prolog whatsoever. Instead, the core Prolog features are probed to reach this section's objective in designing a heap verification architecture based on Prolog. This section refers to [248] and [46] as the first sources on Prolog, highly recommended. Prolog has already been found as a convenient general-purpose logic PL for academic and practical needs. For example, Feigenbaum's theorem was proven with a Prolog verifier [142]. Furthermore, a rare but very severe bug with real numbers critical for Intel Pentium could be proven incorrect using the Prolog-based theorem prover ACL2 [133]. Though considered by many purely academic, Prolog found application in verifier HOL Light [213], validating and transforming terms and semi-structured data in general [294].

A Prolog program is a knowledge base, a rule set of Horn rules. One or more subgoals might request an inquiry to the knowledge base. In order to define rules and subgoals, Prolog expression terms need to be defined.

Definition 4.1 (Generic Prolog-term). A term T in Prolog is defined as:

$$T ::= \begin{cases} x & \text{symbol } x \in \overline{X} = \text{alphabet} \\ X & \text{symbolic variable } X \in \overline{X} \\ [] & \text{empty list} \\ [T \mid Ts] & \text{head of list term } T \in \overline{X}, \\ & \text{where } Ts \text{ is a list} \\ [T_0, \dots, T_n] & \text{list with } T_j, \forall j \in [0, n] \\ f(T_0, \dots, T_n) & f \text{ functor, } T_j, \forall j \in [0, n] \\ p(T_0, \dots, T_n) & p \text{ predicate, } T_j, \forall j \in [0, n] \end{cases}$$

A symbol denotes some logical object, e.g. "me", "Santa Clause", the integer "33", or just some local variable. In Prolog, a symbol starts with a lowercase letter followed by an arbitrary sequence of letters and digits.

In contrast to symbols, a symbolic variable always starts with a capital letter or is the unique character "_". For example, the variables X is assigned (or unified) some value, e.g. "33", afterwards X might be used in (complex) terms or subgoals (see def.4.2). Whenever "_" is used, then referencing it will not be an issue at all. Thus, "_" is used exclusively in cases where precisely one term is applied, and further use of that value is not needed – as it usually is the case with pattern matching over terms. The visibility of variables is bound to a rule.

Lists defined over binary operations "," or "|" must have at least two components. The check of whether a list is linear is performed by the predicates itself, which accept terms. Example lists are [12|[]] and [1,2,[4|5]]. So, the base type of any list is a struct.

A functor is a structural operator, which links terms and denotes a new complex value. An object or struct may be (partially) symbolic. For example, the list constructor functor "." applied to head H and list Hs works the same as $[H|Hs]$. Another example is the successor of a natural number *succ*. Its arity is one and accepts either one Church-term to *succ*, or which is *zero* with arity 0 (cf. fig.10). The latter case denotes a constant (see obs.4.13).

The predicate returns "yes/no" depending on if some given terms coincide according to the predicate or not. If the predicate is defined for any terms combination, then the predicate is total (see next section). For example, the assertion *older(plato, aristotle)* denotes the proposition "Plato is older than Aristotle".

Definition 4.2 (Horn Rule). A Prolog-rule consists of head p and body q_0, q_1, \dots, q_n of subgoals q_j and $j, n \in \mathbb{N}_0, j \leq n$. Subgoals are evaluated consecutively with increasing $j \geq 0$. Head p may contain an arbitrary number of terms (term vector), which may be used in the body. A rule with empty body, where $j = n = 0$, is called a fact.

The syntax of some rule *pred* in EBNF is defined by

$\langle \text{head} \rangle ::= \langle \text{ID} \rangle \langle ' \rangle \langle \text{term} \rangle \{ \langle ' \rangle \langle \text{term} \rangle \} \langle ' \rangle$
 $\langle \text{rel} \rangle ::= \langle '=' \rangle \mid \langle '!=' \rangle$
 $\langle \text{call} \rangle ::= \langle \text{ID} \rangle \langle ' \rangle \langle \text{term} \rangle \{ \langle ' \rangle \langle \text{term} \rangle \} \langle ' \rangle$
 $\langle \text{goal} \rangle ::= \langle \text{term} \rangle \langle \text{rel} \rangle \langle \text{term} \rangle \mid \langle \text{call} \rangle$
 $\langle \text{body} \rangle ::= \{ \langle \text{goal} \rangle \langle ' \rangle \} \langle \text{goal} \rangle$
 $\langle \text{pred} \rangle ::= \langle \text{head} \rangle [\langle ':-' \rangle \langle \text{body} \rangle] \langle ' \rangle$

Here *ID* is a symbol identifier – but it is not a symbolic variable. Binary operator "=" denotes unification, and "!=" impossibility of term unification. "." denotes the end of a predicate definition. Symbolic variables are visible inside a rule definition only. The separator ":-" defines *head* to the left and *body* of a rule to the right.

The example from fig.45 shall be considered for illustration. Fig.45 a) contains two obvious facts from Ancient Greece: (1) Socrates is a human, and (2) Zeus is immortal. In analogy, other facts might be defined: the designer's responsibility of a (closed) knowledge base. A fact by default is an indisputable assertion from the considered context of discourse. The third rule states: "every human is mortal". In more technical detail, this means: if some term *X* has the predicate "human", then term *X* is unconditionally assigned the predicate "mortal". Unconditionally implies in an immediate sense the absence of further subgoals, except for the subgoal *human(X)*.

human(socrates).
noneternal(zeus).
mortal(X):-human(X).
(a)

a2(0,M,Res):-Res is M+1.
a2(N,0,Res):-N1 is N-1, a2(N1,1,Res).
a2(N,M,Res):-N1 is N-1, M1 is M-1,
a2(N,M1,Res2),
a2(N1,Res2,Res).
(b)

Figure 45: Example on Prolog rules and facts

Terms obeying def.4.1 may be noted in infix-notation in the case of the "rl"-operator modifier. An even more generalised relation can be written by using predicate $p(T_0, \dots, T_n)$. Next, fig.45 b) deals with Ackermann's function, for example. It demonstrates that any recursion (e.g. left, right, primitive, mutual) may be defined in Prolog, which shows full theoretical expressibility. The operator "is" is an arithmetic functor, a Carnap functor [57], which denotes arithmetic term calculations. They are not logical, after all. Ackermann's function is defined and total. However, due to memory limitation and physical device management, a calculation might be interrupted in practice. Thus, a predicate made of a function may be helpful in termination check for inductively-defined

incoming data. Examples might include natural numbers and lists.

Subgoals *goal* as countable sub-constraints of a predicate can be defined as follows.

Definition 4.3 (A Query in Prolog). A query of subgoals in Prolog is defined as a sequence of unification of defined (Horn) rule calls. Symbolically bound symbols are pushed to the local symbol environment and are unified for each subgoal call. A call implies a matching predicate is found with a fixed arity, and all passed terms obey def.4.1, though not necessarily fully bound, at the moment of the call. In case several predicates match, then w.l.o.g. the first matching predicate occurrence is selected first, the following matching predicates may be considered alternatives if the first matching subgoal fails (cf. fig.53). The syntax is described by EBNF rule "goal", the semantic of a single subgoal can be described as a call to a Horn rule (see def.4.2).

Alternative subgoals might be excluded by cuts (see later). Alternatives are considered in the order of appearance in the program. Besides its use, the essential difference between a procedure and a predicate is the calling convention, the passed terms and the permanent and mandatory search for alternatives (see later, see obs.1.5).

CI in Prolog [83] is rather limited, but still, it allows the check and definition of user-specified class types, so-called "kinds" for a given term, which may be: var, atom, number, compound and other less important embedded predicates. The merge of common case terms into one is allowed, so predicates may considerably ease predicate definitions. "atom" checks the property of a symbol, e.g. if atom(a) or atom([]) are correct, but atom([1]) or atom([1,2]) would be not. "var" checks whether a given term is an unbound symbolic variable. Hence, var(X) is correct, but X=1,var(X) is not. "list" checks whether a given term is a (weakly-typed) list (as it is by default in Prolog, cf.[83] with [243]). So, both, list([]) and list([1,2,3]) are correct, where list(a) is not. To define properties over a given list or for compound terms (check may be done using built-in predicate compound), in both cases, "=.." is used. This operator splits a given term into the associated functor to the left-hand side and passed terms as a list to the right-hand side.

Predicate calls are considered later. However, term unification by default is not done in Prolog due to a full evaluation of sub-expressions before processing them. Thus, by default, X=X may be unified, where X=f(g) may not. Depending on Prolog implementation to be used, recursion may or may not detect recursion in rules. That is why unification may occasionally only be performed on the top term level, alternatively not at all. Nevertheless, for the example, X=f(g(X,X)) unification may often lead to failure or termination in the best case, and in the worst case, may crash execution of WAM (due to stack-overflow

since version 1.3.0 "GNU Prolog" [83]). Conservative estimates show that 95% of all cases do not require unification term checks. However, these are the essential percentages for generalised assertions about term representations and transformations since often complex terms may contain symbolic variables that may (by accident) contain mutual recursion. Often limits of given algorithms need to be checked. Here Ackermann's predicate might be quite helpful in AT the incoming domain. That is why now a simple algorithm is provided to exclude that critical 5% entirely. Those problems may indeed correspond to, e.g. object definition according to sec.I-B, see fig.46.

```
unify_with_check(X,Y):-var(X),var(Y),X=Y.
unify_with_check(X,Y):-var(X),nonvar(Y),
    not_in(X,Y),X=Y.
unify_with_check(X,Y):-nonvar(X),var(X),
    not_in(Y,X),Y=X.
unify_with_check(X,Y):-nonvar(X),nonvar(Y),
    X=..[H|L1],Y=..[H|L2],
    unify_list(L1,L2).
```

Figure 46: Example code on occurs-checks

Term structures and lists must be defined as in fig.47.

```
unify_list([],[]).
unify_list([H1|L1],[H2|L2]):-
    unify_with_check(H1,H2),
    unify_list(L1,L2).
```

```
not_in(X,Y):-var(Y),X\==Y.
not_in(X,Y):-nonvar(Y),Y=..[_|L],not_in_list(X,L).
```

```
not_in_list(X,[]).
not_in_list(X,[H|L]):-
    not_in(X,H), not_in_list(X,L).
```

Figure 47: Example code on list unification

In sec.VI and fig.71, an example is provided when a predicate is used as a passed term. In analogy to functor analysis, a predicate's call is also done within a given stack window's boundaries. The difference is in the computation model and reference implementation of Prolog and its stack synchronisation (see next section) regarding caller and callee.

Next, let us consider the example from fig.45 b) with subgoals and their calls. Given a program and subgoal "?-a2(X,1,3)" (see fig.48), which is put in by interactive interpretation. First, rule (1) is taken when unifying with σ_1 . The substitution σ_1 leads to contradiction because of $\text{Res}=2$. In fig.49, a set of unification bindings is given for the considered example's derivation tree. The search is stopped for the given predicate because it failed, and therefore the next alternative is chosen (see obs.1.5).

Selecting the third rule with unification σ_2 , applying the second rule with σ_5 , and finally applying the first rule with σ_9 finishes the search successfully. Since there is no cut (see further), alternatives are checked, and finally, yet another solution for the given subgoal is found. The path from the first subgoal over all-new intermediate subgoals till successful termination is called the path to a solution. Every path to a solution in fig.49 is marked with a black square. For the example given, there are two, and both solutions are identical. Here it shall be noticed that even if paths to solutions vary, the search could be cut as soon as a first solution is found. However, this is very example-specific and cannot be generalised.

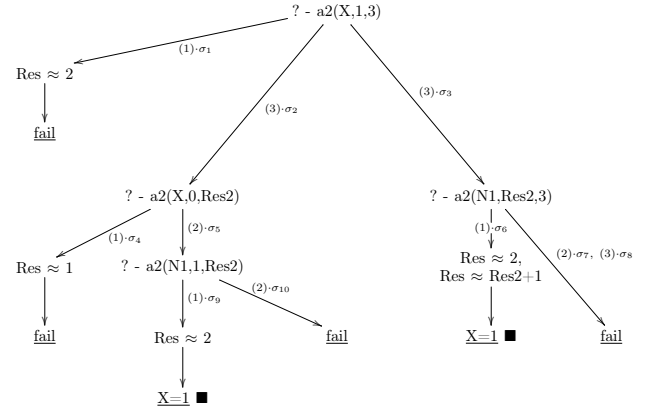


Figure 48: Derivation tree for the Ackermann-predicate

$\sigma_1 =$ $X \approx 0, M \approx 1, \text{Res} \approx 3$
 $\sigma_2 =$ $N \approx X, M \approx 1, \text{Res} \approx 3$
 $\sigma_3 =$ $\text{Res} \approx 3, N \approx X, M \approx 1, N1 \approx X-1, M1 \approx 0$
 $\sigma_4 =$ $X \approx 0, \text{Res} \approx \text{Res2}, M \approx 0$
 $\sigma_5 =$ $N \approx X, M \approx 0, \text{Res} \approx \text{Res2}, N1 \approx X-1$
 $\sigma_6 =$ $N1 \approx 0, M \approx \text{Res2}, \text{Res} \approx 3$
 $\sigma_7 =$ $N \approx N1, \text{Res2} \approx 0, \text{Res} \approx 3, N1 \approx N1-1$
 $\sigma_8 =$ $N1 \approx N, M \approx \text{Res2}, \text{Res} \approx 3, N1 \approx N1-1$
 $\sigma_9 =$ $N1 \approx 0, M \approx 1, \text{Res} \approx \text{Res2}$
 $\sigma_{10} =$ $N \approx N1, M \approx 1, \text{Res} \approx \text{Res2}, N1 \approx N1-1$

Figure 49: Unifications for the proof tree from fig.48

Considering fig.49, we notice that the evaluation strategy may essentially change with cuts when stratifying subgoals in a declarative paradigm. For example, if cutting logical reasoning in fig.48 after subgoal "?-a2(N1,1,Res2)", we are confident the whole branch (3)· σ_3 may be skipped. For this, the cut needs to be defined.

Definition 4.4 (Cutting Solutions). Cutting solutions prevents a local search for alternatives at a given subgoal position in a given query according to def.4.3 after finding the first solution till that subgoal position.

Locality always applies to all subgoals inside a considered predicate until the cut operator "!". However, cutting does not imply that any algorithm becomes more compelling or automatically better somehow since this depends on how the cut is applied. Cut only provides a possibility depending on the given rules to skip further constraints if a solution found is obvious, and further constraints shall not be considered anymore. It may be used to exclude duplicate solutions. A cut is effectively a built-in predicate used as a subgoal and interprets the current calculation's state, namely the Prolog execution stack for non-deterministic solution branches. Let us consider the cut's semantics by the factorial fact example from fig.50.

```
fact(0,1).
fact(N,Res):-N1 is N-1,fact(N1,Res2),Res is N*Res2.

fact2(0,1):-!.
fact2(N,Res):-N1 is N-1,fact2(N1,Res2),Res is N*Res2.
```

Figure 50: Example code for the factorials in Prolog

The first term represents an incoming integer, and the second term represents the outgoing result term. A predicate is a relationship between all incoming and outgoing terms passed. In the example, the order input-to-output used is from left to right. The predicate fact2 almost equals the first predicate, except the base case contains a cut as the only subgoal. Cut affects the first alternative of fact2 is called only whenever incoming and outgoing terms unify for the subgoal query according to def.4.3, e.g. "?-fact(5,R)". — This happens only once for recursion descent when the incoming number equals zero. Whenever this situation happens, cut guarantees in all processed, then in subgoals for no further alternatives will be searched. On the recursive rise, alternatives are not considered. If there were no matching subgoals on the recursive rise, then alternatives would be considered, except for cut alternatives, if any. Therefore, the cut in fact2 is essential. It improves the understanding of the calculation of all its subgoals and its optimisation. It is noted that the rules order heavily influences soundness. For example, heavy influence is reached by changing the ruling order or introducing a cut, see fig.51.

```
wrong_fact2(N,Res):-!,N1 is N-1,
                    wrong_fact2(N1,Res2),Res is N*Res2.
wrong_fact2(0,1).
```

Figure 51: Counter-example code on factorial in Prolog

In this example, the base case is unreachable because 0 and 1 both also unify in the first alternative. Cut leads here to ignoring the second alternative. Next, N1 is assigned -1 when calling "?-wrong_fact2(0,1)". Thus, left-recursion

is present. So, it does not terminate. In this case, the cut is superfluous because left-recursion does not allow to view any alternatives, although all logical facts and rules are defined. The derivation tree contains one infinite branch since the corresponding calculation does not terminate. In Prolog, this Halting-derived problem is better known as the prioritisation issue. Thus, for readability, rules must be defined in the order, s.t. base cases occur first. It seems trivial, but it is not — especially not when later Prolog is tuned (see sec.VI). So, particular and specialised rules, as well as facts, must be defined first. Otherwise, they are suppressed by more generalised ones.

On the other side, non suppressed rules mean that rules corresponding to alternatives may alter according to their position. Here, in addition to simplicity reasons, the preference shall always be given to simple and less constrained rules over more complicated rules. In order to achieve this, it is mandatory, as much as possible, to differentiate incoming term vectors (see later on heap calculus in sec.V).

It must be stated that cut is essentially syntactic sugar. It is sugar because it may always be entirely rewritten (proof would be inductively over Prolog predicates), s.t. all possible continuations of the cut may be un-factored (contrary to rule factorisation). Soundness may also be shown by excluding cut by introducing an additional argument to the predicate, which stores the temporary calculation result. If the result is reachable, then there is a unique base case. In all other cases, a strictly monotone raising chain exists. The search may be generalised and expressed for a fixpoint in terms of μ -expressions. A full prove may be found in [262], also refer to discussion in sec.I. Logics that allow cuts must implement and obey (CUT) formalisation (as a rule):

$$(CUT) \frac{\Gamma \vdash \Phi, \Omega \quad \Phi, \Delta \vdash \Lambda}{\Gamma, \Delta \vdash \Omega, \Lambda}$$

Prolog upper consequents of form $A \vdash B$ may be considered A is the subgoal of a rule's body, and B is the predicate head, so the logical consequent. Consequents are specific and abstract simultaneously and may cause unnecessary distraction and, therefore, are not mentioned later except explicitly needed. (CUT) cuts non-determination. Cuts do not guarantee termination nor full determination whatsoever (see mentioned earlier example). Alternatives may occur even with cuts, for instance, in following "!" subgoals. Whenever an (intentional) cut does not threaten to drop the right solutions, the cut is "green". Otherwise, that cut is "red".

Discussed solutions, constraints, rule modelling and subgoals will be applied later, particularly in sec.VI. Negated assertions shall be discussed in more detail next since they are an essential logical operation to (heap) predicates (cf. def.4.1). Negation may be applied to predicates, and meaningful definitions may be found for relations, however symbolic variables (not propositions) may not

have a meaningful negation in general. Apart from the singleton case, it is trivial to note that negating a set (also infinite sets, but inductively-defined) is not decidable. The method presented in sec.VI is decidable, even if inductive definitions are allowed due to the properties mentioned, mainly due to non-repetitiveness and heap locality. Naturally, a similar problem of undecidability encounters for predicates. The situation is undefined for functors in general: if any function with any unspecified domain and any unspecified co-domain is negated – what would this hypothetical function then denote? – This is more a rhetoric question, and it is obvious there is no obvious answer since it is undetermined. That would change if the functor would act as a predicate and its co-domain would be boolean. So, a meaningful negation shall be found for Prolog predicates.

A possible semantics of negation in Prolog is to fail since, in Prolog, a predicate searches for some solution and must find it in a negative sense only. Prolog implements a built-in predicate with arity 0 called fail, and from now on, this shall be used unless stated differently.

B. Reasoning as Proof Search

Prolog has successfully been used as a language processor to formal as well as natural languages [201], [168], [285]. As shown later, some formal words must be generated and validated according to a given rule set. Natural languages are characterised by mutations [201], [131] compared to formal languages due to cultural-sociological development. Ambiguity is the primary factor for differences between both languages. Even so, methods on natural language processing have been well studied over the last decades [131], [200], which leads to intriguing results in Artificial Intelligence and Natural Speech Recognition of human speech. However, this work is focused on relatively easy lexical analyses. This work's main objective is to find the most straightforward and adequate dynamic memory model and checks on it. For a prototype's implementation but also for research of crucial topics, Horn rules will be used. Warren's proposition of the "use of predicate logic in order to solve logical tasks" is put into life, even if he warns about his thoughts about Prolog's use may not be fully capable and tractable in real-life due to limitations of predicate logic's expressibility (cf.[144]). These limitations are due to Turing-computability. A simple example demonstrates this complexity — assume some function with incoming and outgoing term vectors encoded as a predicate, as it may be done in Prolog. Then, for a given incoming vector, the result may be hardly tractable, e.g. in the case of one-time functions for message encryption or functions that may be partially defined only, e.g. a 2D-mapping onto an ellipse. The paper [200] researches similar parsing methods, but, unfortunately, the theoretical limitations of syntax analysis are not (entirely) considered. That is why parsing is heavily constrained, mainly due to recognisers of the LL(1) category or purely

extended analysers based on it. Unfortunately, it impairs expressibility in total. [299] shows whenever generation and checks of data (in the contributions only terms are considered for common data) are of interest as two competing processes, then:

- 1) Syntax analysis is bound by expressibility, first of all. If expressions were widened and artificial limitations were lifted in previously mentioned work, then w.l.o.g. both syntax and semantics of the whole checking process may aggressively be simplified.
- 2) Simplification may also be achieved by a generalised IR.
- 3) Particularly due to the functional paradigm, a comparably bloated description is the result. In total, only five functionals are used, like concatMap, foldl. The probability is high that the check process semantics could have been formulated even closer in mathematical-logical terms similar to this work (see later).

The papers [294] and [299] show a non-standard solution at first glance may lead to a friendly and straightforward but effective overall solution based on genuinely logical terms. The reasons for that are diverse. First, there is the representation of term transformations as rules and compactness. Widefield analysis is made w.r.t other functional languages as imperative languages worsen all characteristic metrics regarding quality and compactness. Second, simplicity is due to the comparison made between a given program and its description, which may be caught by regular expressions in the most general form, even by some context-sensitive expressions in rare cases, as shown by examples on macro calls. Qualitative analyses are taken out on each input operator and a quantitative comparison based on software metrics. The result is perhaps unexpected because nearly by all parameters, Prolog leads followed by functionals [294]. Next, results are discussed in sec.IV-C.

Thesis 4.5 (Proof over Heaps is equivalent to Syntax Analysis). Logical programming on dynamic memory is the same as syntax analysis.

Proof. A heap verifier based on a Prolog-dialect is introduced, allowing to resolve the issues from sec.II by the theorems of this and the following sections, particularly on proof automation in VI (cf. sec.I). When talking about proofs over heaps, it is assumed that heaps are represented as Prolog terms, and those are automatically entailed [296] to compare equality (see following sections). Naturally, core verification rules, e.g., subtraction, are not directly affected by automation since those still co-exist. \square

A prerequisite to this thesis is that syntax analyses allow resolving issues related to dynamic memory proofs. This section induces how to do it, which preconditions have to be obeyed and why. Prolog does not only qualify as a theoretical apparatus, but it also qualifies as an

instrument for solving a problem complex at once (see this and following sections). Prolog is exceptional because only assertions derive true derived from a given Horn-rule set (see obs.1.13). If a theorem was not derivable, then the reason may be in the rules (e.g. lack of abstraction), reasoning techniques, or the way subgoals are represented. Naturally, there are practical bounds w.r.t. syntax analysis.

The idea to use a syntactical analyser as a solver of heaps (cf. sec.III) came into mind after several observations made (see sec.VI):

- 1) Prolog rules are very compact and are unique among similar approaches, especially when it comes to logical tasks.
- 2) A program in Prolog is a set of rules. Successful reasoning constructs, in fact, a tree. The proof of some theorem has the structure analogous to a program (cf. isomorphism discussed earlier). The same goes for queries that span a tree.
- 3) Expressions may be syntactically analysed if further needed. The locality of pointers constraints memory models, namely its expressibility of corresponding generated grammars. So, some formal grammar here for a pointers theory may not supersede CF grammars in general. That is very useful to keep in mind.
- 4) However, on one occurrence, a propagandist of Semantic Web attempted to advertise his and other persons contribution would be lingua franca for at least the next 25 years. The argument presented was used as self-defence that the Semantic Web solves almost all actual technical and scientific problems. As an argument of superiority, Semantic Web was described as higher than abstraction and, as he called it "legacy methods", as explicitly mentioned syntax recognition, he later added that it would have no future. As can be seen and understood today — that presenter overemphasised, at least. Regardless of that, it can be found that syntax analysis may still be found useful today, not to forget about the base of any semantic web application since syntax still has to be recognised in a first instance. Apart from that, real problems, e.g. related to rule-based recognition, still emerge sometimes.

Now it is up to note and compare the objectives of the discipline in more detail:

- | | |
|------------------------|-----------------------------|
| 1. Programming | → find solution |
| 2. Logical Programming | → find (logical) solution |
| 3. Syntax Analysis | → find (syntactic) solution |

When we try to type the mappings of 2 and 3, then characteristics emerge as shown in fig.52.

So, whenever the attempt in narrowing down input sets, the solution obtained by one approach may be replaced by a solution obtained by a different approach.

Logical Programming	
Input:	Prolog rules, query
Output:	"yes/no", proof tree with all unifications
in comparison to that we have	
Syntax Analysis	
Input:	formal grammar, input word
Output:	"yes/no", syntax tree (AST) (and symbols as attributes replaced)

Figure 52: Characterisations of typings from points 2,3

The approaches mentioned earlier for recognising natural languages differ from those for formal languages by some ambiguity and deviation level. In the languages considered, a deviation is nearly absent.

Lemma 4.6 (The Double-Semantics of Prolog Predicates). A Prolog predicate has two semantics: (1) a procedural semantics based on calls, and (2) a relational semantics based on relational interpretations.

Proof. Since any Horn rule (see def.4.2) can be represented almost identically by its syntax in Prolog, Prolog predicates are considered synonymous for Horn rules. Full semantics and explanations of Prolog predicates can be found in [248], [266] (cf. def.4.3). □

For the sake of this work's objective, only (2) will be reviewed and slightly modified later. According to lem.4.6, a (Prolog) semantics (1) based on calls denotes a classic procedure (as in Pascal or C) with some execution stack. So, a stack frame is pushed to the top (see fig.54) when entering a predicate and removed on leaving. In analogy to reference parameters, unified terms are used amongst stratified predicate layers and passed to the calling predicates on leave. Any violation of consecutive stack frames leads to term invalidation and even other severe errors. In contrast to imperative PLs, a symbolic variable may not just be passed immediately but may also be used as a genuine logical part in a unifiable term. So, any term can be passed in any direction across the stack. This passing style allows any class object to be used with high flexibility and compactness. It allows the transformation to keep processes extraordinary complex and flexible if needed, but compact at the same time, which is remarkable.

The anonymous operator "_", the built-in predicate "concat" as well as higher-order predicates in general, support practical expressibility on a high level, so recursion does not necessarily have to be defined through the predicates but allow flexible and shorter notations (as can be seen later and in the reference implementation of the prototype). Expressibility increases whenever expressions get significantly simpler based on functors and shorter data models used. The latter includes linear lists. The

need to specify all list elements is dropped. In contrast to pattern matching, the remainder is not dropped but just unused, allowing simpler operations to be performed. Let us remind verification of heaps is performed stepwise after each program statement, so usually, only a small portion alters, often only the part referred.

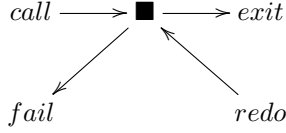


Figure 53: Calling subgoals

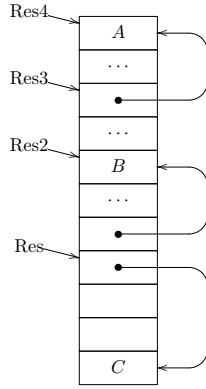


Figure 54: Example of stack windows and related subgoal references with ingoing and outgoing terms

Prolog treats predicate calls, as illustrated in fig.53, namely a black box with four traceable options. A predicate call, so a subgoal, is generic and has these four options: (a) *Call* implies a stack window (frame) is created, which contains all passed terms. (b) *Exit* returns on success only when all subgoals succeed and the predicate head fully unifies. (c) *Fail*, when at least one subgoal fails or (d) *redo*, a retry when (c) happens to one subgoal, then an alternative to the current predicate is searched, if it exists. The danger with inaccurately formulated predicates is inefficiency due to a too broad range of alternatives. Another extreme is when a cut is too restrictive, s.t. no (valid) result remains. Both cases need to be avoided. Predicates call and fail from fig.53 indeed exist in GNU Prolog [83], although the fifth case, "exceptions", is removed for the reasons discussed in sec.I.

Semantics (2) of predicate interpretations implies that any predicate is a generator of non-determinism. A common predicate (as discussed in sec.I and sec.VI) may have a) different definitions for different combinations of incoming and outgoing vectors, but also b) different derivable results for the same subgoal.

For example, if there was a predicate "mortal" from fig.45 (a) and a few more facts are added, according to b) "?-mortal(X)" implies $X = \text{socrates}$; " $X = \text{plato}$ ". If for Ack-

ermann's function "?-ack(0,X,15)" or "?-ack(1,1,Res)" was called, then depending on the concrete implementation of the WAM, the predicate is either defined (although it may take a very long time, or is decidable in theory, but not in practice for reasons of bound resources) or (partially) undefined as can be seen in fig.45 (b). In the example for the given outgoing term "Res" the predicate does not determine the incoming vector, even if the mathematical-logical definition certainly exists according to the given schema, which is in the rules factually without a change (see obs.1.5, obs.1.13). The discussion regarding this limitation continues later in this section, as the invertibility and representation of a relational model do.

Observation 4.7 (Equality of Proof Elements). The search for proof is a search for a subgoal solution. Both search structures, the theorem-proof about a heap and the subgoal query shape a directed search tree.

Proof elements are theorems, lemmas, (recursively enumerable) definitions, conclusions — those need to be expressed in Prolog. Theorems and lemmas are assertions, which are expressed by terms, and formulated as subgoals. APs can express lemmas and recursively-enumerable definitions (see sec.VI). Conclusions are valid subgoal sequences with concrete symbols being unified, e.g. proven theorems. Prolog is no general-purpose PL, apriori just by definition (cf. with [266], [267]), even if it is nicely applicable in specific logical domains. Not every kind of proof may unconditionally be solved with Prolog because of the fundamental limitations (see sec.I). The critical problem is reducing a given problem, which might be better solved by narrowing down languages, as will be seen soon. A subset of Prolog is used to solve complex verification problems based on logical reasoning based on WAM architectures. Let us characterise subgoals and argument terms:

- Built-in predicates, for instance, "concat", may be used anywhere in programs. These (universal) predicates may be added to arbitrary formal theories written in Prolog, as successfully demonstrated by [299], [293]. Reserved predicates and functors may be defined as multi-paradigm.
- Singleton and overloaded definitions. Predicate definitions may appear as singleton or in a row but with an identical arity. This mechanism allows an introduction of new (Prolog) theories, including multi-paradigm. The effect might be extensibility, variability, flexibility and polymorphism (the last two are on a different abstraction level compared to the first two criteria). Apart from that, overloaded predicates, as "concat", enable a flexible ordering of incoming and outgoing term substitutions.
- Operations over heaps are terms. Together with (class) objects, the relative position of a heap may be expressed by terms. Virtually, a heap graph can fully be represented by a heap term. Terms are arguments

to subgoals, so are lemmas and theorem (sub-)proofs over heaps.

The universal call mechanism described in fig.53 implies backtracking. Backtracking on predicates manifests a (mutual) recursion scheme, and by doing so, exactly describes a proof tree (see CF imposed by Prolog rules in sec.VI). The limitations mentioned earlier must not be forgotten. When a (sub-)search succeeds, then that (sub-)branch is considered proven. When a branch is rejected, it is either not proven or just not provable in principle or may lead to an apparent contradiction. Both variants, however, are sufficient to establish a refusal, as the universality of the formula must be shown. If interpreting predicates declaratively, then predicates may easily be interpreted as procedures.

Consecutively, logical programming in Prolog may, in reality, be approximated to proving. Even if a program's properties are specified and verified, the incoming programming is neither debugged nor executed. As will be shown soon, Prolog is excellently qualified to be used as a heap verifier. Expressibility is increased in this context by the heap IR, rule abstraction, inductively defined predicates, genuine logical symbols and (quantified) formulae in terms of Horn-rules. For example, in contrast to the lifted formulae in first-order predicate logic, a compromise is sought, s.t. the heap graph construction is performed stepwise. Here, the heap is described bottom-up based on separate simplices, namely simple heaps. A complete representation of logical expressions in formulae allows maximum flexibility towards heap expressibility and flexible strategies to be added and modified.

Observation 4.8 (Deduction with Backtracking). The search with backtracking spans a formal proof tree in Prolog.

From obs.4.7 follows, the (proof) structure spans a tree in Prolog compatible with general heap searches (cf. sec.I). If some open cycle occurs, this might be related to subproofs or symbols reapplied. However, closed cycles shall not occur. Otherwise, the proof does not terminate, and this would be an observed regression. Regression is an indicator an applied rule did not succeed with a new calculation state, so there is no progress, so all consecutive regression states shall ideally be rejected. Invalid states, in general, may only be implied from an unsound rule set. If proof is found, then for a subgoal, all related results shall be bound accordingly (unbound (symbolic) terms shall not further be considered since they result in questionable predicate semantics and shall not be considered crucial for proof).

Prolog's search solely bases on rule deduction (cf. sec.I). Only what is derivable by Modus Ponens upon facts and rules is valid. Other modes, as Modus Tollens, are invalid since not considered in ISO-Prolog. In practice this means, that predicate falsification may only be decidable in general if considered sets are finite (e.g. by introducing

common symbols for class object definitions instead) and are defined. Thus, self-contradictory cases are excluded. Thus, proofs may become bloated, and some proofs cannot be taken out in classical deduction schemes (see the example of Peirce's third excluded in sec.I). Predicates may be defined finitely, even if the incoming set is infinite. Then cut-as-fail may represent a predicate cut or any other explicit definition upon it.

The motivation behind search with backtracking is that the search continues with the first failing predicate relative to the parent's axis. It works by guarding a minimal nominal value and implies permanent stack context switching.

In contrast to the method "return on fail", the method "return on directed focusing" may be considered generalised, s.t. in the most common cause, the focus is set to some extreme integer value. That extreme value directs the choice of the next subgoal. It leads to the insight that this kind of problem may be fully reduced by the strategy "branch and bound" [179]. The generalisation of the extreme value is an (extreme) term, namely some bound term, s.t. it fits with the heads of the left-hand sides of rules by pattern-matching towards the most general unification. Regardless of the bound looks, the stack-switching naturally involves backtracking already available to the Hoare calculus verification scheme (cf. fig.48).

Observation 4.9 (Stack-based Predicate Calls). Prolog's underpinning WAM is characterised on the top-level neatly by a declarative semantics, the Prolog-dialect itself. For example, stacked terms may be referenced and partially unified among several stack windows – in order to do that in an imperative PL, this is much more complicated, especially since stack requires occasional state flips, as is the case with backtracking. Prolog's syntax and semantics are relatively small compared to languages like C(++) to perform just what was stated. However, backtracking and term processing are core language features that cannot merely be mimicked by C(++).

Hoare triples in Prolog may be represented as a predicate with arity 3, where the first two components are terms, and the third component is encoded as the last outgoing predicate argument. Of course, in general, any Prolog predicate may be implemented invertible, if whatever the concrete semantics might be and if desired. However, we are not interested in that question yet (see sec.IV-C and following). The reasons for dependency will be emphasised in the following.

Discussion about declarative approaches to the stack

- Performance. It is mainly about improving re-active systems' runtime behaviour (systems under another system's control). Although Warren [266] emphasises performance is not the only factor, a slowly OS may be the effect of a slow algorithm (this is due to rule definitions), e.g. frequently copying used memory regions. There are two reasons: First, the frequent use

of (sub-)expressions indicates a high data coupling, which may effectively be resolved by an algorithm redesign and thus rewriting the rule set. Second, performance improvement may come from outside (e.g. optimisations implemented multi-paradigm) regardless of overhead costs due to an additional redirection because, in practice, it may be lower by a particular memory-managed technique like e.g. memory-mapped I/O [164]. Thus, the second problem is resolvable due to variability. So, a predicate may be replaced by an alternative behaviour but with the exact specification. Lingual extensions and variability are both of permanent interest in this work, especially in sec.IV-C.

- Evaluation ordering. Infinite data structures, like "take" (see sec.I), shall be exempted from operational semantics according to [267] for core language features. However, this does not necessarily exempt other semantics and tests as discussed in the introductory since this will be the essential application field. Since operational semantics has to fully accommodate any passed (possibly infinite) argument to the stack, hence the Prolog ABI would not terminate, thus would be incomplete. A partial push of terms to the stack would be thinkable. However, this would require severe modifications and a total redefinition of how WAM deals with ABI. Since the disadvantages of massive expected changes would far outweigh any benefit gained, this is not intended yet. A slight modification of WAM's original operational semantics may seem possible, but changes would be too massive. It must be stated, term unification in Prolog implies naturally a difference check for the most common terms that would hold even for heap terms – and this expected (for further details, see sec.VI). Only lazy-expression (term) evaluation outside-in (cf. sec.I) would w.l.o.g. allow the full support of infinite data structures natively. So the only critical phase remaining would be the invertibility of predicates. Thus, the only modifiable factor is the evaluation order. In case it is not yet modifiable at all in practice, the order may need to be modified manually by rewriting the rule set.

- Semantic context. Predicates may be overloaded or defined multi-paradigm.
- IR. Term-IR may evolve, so more and more not properly designed IR may become bloated. It may be required to redesign an IR, including more significant deletion and modifications.

Thus, variability and extensibility (cf. API) are vital properties, which Prolog allows, which can easily be checked, e.g. against [83]. If, for the sake of local optimisation, fast memory access and B-trees [72], [18] shall be introduced instead, then this can quickly be indexed of built-in and hidden predicates, bridged by multi-paradigm stubs.

The question of whether stack may be substituted by heap shall better be negated because past attempts suffered from tremendous performance bottlenecks and restrictions (see certain F#-implementations, for example). The reason was mainly recursion schemas used to be through the stack, suddenly had to be implemented in unorganised heap mimicking stack windows. Even when some passionate fans may dispute it, that experiment was no real break-through and could be considered failed so far.

Furthermore, recent CPUs come almost always with optimisations that depend immensely on stack allocation and disposal, and breaking this rigid convention would require a good excuse since it affects several significant processor designs [123], [215]. The declarative paradigm for the calculation state of heaps must be logical in order to tackle verification.

Discussion on proof search using relations

Predicates conjunct terms, which consist of symbols, variables and other terms. It is not hard to notice that there exist B^A different mappings between A incoming and B outgoing terms – for the sake of simplicity and w.l.o.g., no mixes are allowed here. Several mappings may be bound by only one predicate. Whether for a given input and output vectors, a predicate is decidable remains a question obviously (again without mixes). This problem, however, can be reduced to Post's (3-)SATisfiability problem of some logical formula. Naturally, from a practical view, it is the verifier's responsibility to write sound and complete predicates which are overloaded, implementing a variety of singleton-predicate mappings so. The more mappings a predicate includes, the higher is its functionality and potential reuse. Overloaded predicates escalate the question regarding invertibility because non-termination of a particular aspect automatically leads to non-termination of a whole predicate, and so, to non-termination of a proof. It will be considered later.

When considering some predicate as a Cantor set, this is a discrete Cartesian product of domain (contains all incoming terms) and co-domain (contains all outgoing terms). As domain and co-domain may contain more than one component, they may still be countable due to bi-directional diagonalisation, hence be processed by recursive-schemes. As domain and co-domain join, a predicate is just another indirection level. Diagonalisation will do the job here too. Hence recursive schemas are computable, and they are not another theoretic hinder from complexity' view here. From a practical perspective, this is not less important but an essential universal consideration. If we succeed in showing universal properties for all relations, then we might imitate it successfully. As Codd proved, relational algebra was sound towards universal properties we are interested in most. All that is required is to establish expressibility equality. Most

modern relational and object-relational query languages are known for their expressibility bounds.

Thesis 4.10 (Expressibility of Relations in Prolog). The expressibility of Prolog rules can be considered as pure relational.

Proof. A full proof can be found in the author's contribution [294]. The proof is direct and straightforward. All properties from Codd's algebra, e.g. projection, must be replaced by equivalent Prolog rules one by one, avoiding naming clashes for two given relations, R and S (see fig.55).

Union:	
$T = R \cup S:$	$t(x_1, \dots, x_m) : -r(x_1, \dots, x_m).$ $t(y_1, \dots, y_n) : -s(y_1, \dots, y_n).$
Set minus:	
$T = R/S:$	$t(x_1, \dots, x_n) : -r(x_1, \dots, x_n),$ $not_s(x_1, \dots, x_n).$
Cartesian product:	
$T = R \times S:$	$t(x_1, \dots, x_m, y_1, \dots, y_n) : -$ $r(x_1, \dots, x_m), s(y_1, \dots, y_n).$
Projection:	
$T = \Pi_S(R):$	$t(s_1, \dots, s_n) : -r(x_1, \dots, x_m).$ $\forall s_i \in \{x_1, \dots, x_m\}$
Selection:	
$T = \sigma_S(R):$	$t(x_1, \dots, x_n) : -r(x_1, \dots, x_n),$ $s(x_1, \dots, x_n).$
α -conversion:	
$T = \rho_S(R):$	$t(x_1, \dots, x_n) : -r(x_1, \dots, x_n).$

Figure 55: Relational model over Prolog predicates

In analogy, the transformation from Prolog back into Codd's algebra can be done. Further steps, such as canonisation and cut (removal), may be required, though, but which can always be achieved – as was mentioned earlier, e.g. in def.4.4. \square

Here, [149] shall be mentioned, where an optimal representation of incoming and outgoing data types is questioned. His contribution is that data types in term notation may be more beneficial for most logical puzzles than any other paradigm, mostly not functional. [205] researches fundamental properties of domains as relations. It proves a relation invariant solely always exists. Even so, the question regarding invariants remains exciting research and partially still open. One good example deals with adaptations of caching heaps in specifications (see sec.V).

After we just introduced relations and defined their basic properties, the following pleasant properties may be derived:

- Declarativeness. When logical reasoning, arithmetic calculations may not bother too much, but objects are essential, so are heaps and their interconnections. This selection is not just a question of favour but

is essential to the whole deductive system. Prolog is already a platform for term and knowledge representation as well as processing, and heaps are atoms or composed terms. Rule predicates are heaps. Aliases are symbolic variables, which are used in different places. All this is sufficient in order to define a theory on heaps.

- Term-tree. According to Birkhoff's theorem (about term products) [202], [79] an abstract algebra implies that each term corresponds to a tree representation. The transformation, unfortunately, must not necessarily be unique if canonisation is skipped. The inverse transformation can be uniquely defined if canonised earlier. These properties raise the need to either define tree canonisation or to trim. So, e.g. associativity helps to make tree canonisation implicit (see sec.V). Initially, we do not want to restrict ourselves to trees but would like to have unconstrained heaps (cf. sec.III). Even a heap graph consisting of a single vertex would be valid. By a single vertex, we imply either a simple, a complex, e.g. an object, vertex or a placeholder for a sub-graph.
- Term Generation. Research on this topic [294] shows Prolog is brilliantly for processing terms compared to other functional and imperative programming or transformation languages. That research includes a field study and so is based on numerous examples. Also, a quantitative analysis is included and based on metrics, such as expressibility level and intellectual language level and many more. For various examples, nearly without exceptions, Prolog always supersedes functionals, occasionally even significantly.
- Term validity. The thematic research [299] shows that if both processes, generation and checking of terms, are narrowed down, then the critical limitation becomes the validation language's expressibility. W.l.o.g. the research considers a generalised regular language. The validation process of semi-structured data may intuitively be understood to compare terms with gaps filled on runtime. A term is a generalised IR and may widely be used, e.g. to verification. Operators describe not the program but the structure of the document to be generated. Statically, a loop not always may be bound. Hence, some loop containing vertex a in a tree representing an XML-document only denotes a^* .

It implies the loop condition may be validated only against the most common assertion.

Naturally, a finite automaton may not recognise $a^n b^n$, but that is dispensable. The major hinder is always the expressibility of the assertion language, namely its expressions. Most curiously, among all approaches investigated [294], relations come out to fit best in representing knowledge, e.g. for assertions, logical rules, transformations. For example, functionals must calculate each gap individually, whereas logical rela-

tions can be more elegantly and compact due to its term expressions and rule notation. In [294], rule-based transformations mainly imply $\tau \rightarrow \sigma \rightarrow \tau$, where τ represents some term IR, and σ denotes some environment with symbolic bindings. When interpreting this transformation of a relationship that denotes a predicate, then the transformation may be extended as $\tau \rightarrow \sigma \rightarrow \tau \rightarrow \mathbb{B}$, where \mathbb{B} is the boolean set. Now heap verification may be represented the same way as a family of transformations. Its main difference is the use of (abstracted) predicates and automated reasoning. On transforming needed terms, the heap models, however, will vary. In contrast to regular expressions and appropriate recognisers [50], the specification schemas are mainly CF. The prediction of the next element is a special operation in both methods. Due to its context, both may significantly differ after all.

Thesis 4.11 (Simplification using Term IR). The use of (Prolog) terms eases the specification and verification of heaps.

Proof. The solution to this thesis is presented in this and the following sections. Simplification is mainly achieved by a direct heap term IR, which matches patterns straightforward in rules, and by a unified heap data structure to be used for both heap specification and verification (see sec.IV-C, cor.4.14). \square

Apart from terms, other IRs may be used, for instance, tetrads, Polish-inverse notation, triads or others. The advantage of terms here is the description of a heap state, mainly its simplicity and maximum expressibility. An immediate term IR for program statements may also be used since both statements and term are tree-like. Hence, other IRs are not being considered (cf.[291], [181]). However, term-IR in Prolog has the advantage (sub-)terms do not require additional context definitions apriori, and its explanation of the link is straightforward and quite simple after all. A heap term can "just be written", where other IRs cannot, since they would require many additional conventions, constraints holding, be explicitly added. Not only does this helps in lecturing students and rapid prototyping, but it also simplifies even the whole definition and transformation of terms (cf.[19], [87]). Analogous implementation on a comparable practical level includes LLVM-bitcode [253], GCC GIMPLE [171] and further annotated objects as IRs in terms of the ROSE [228], for instance. In all these cases that use tetrads, the incoming program's temporary IR must first be transformed into an AST.

Syntax parsing in LLVM/CLANG is performed more flexible than in GCC due to a supplementary phase CLANG provides [251]. Even if the AST may theoretically be derived without CLANG, but in practice, that would fail due to the very bloated LLVM-IR as a human-readable

format. It should be remarked that the binary format is compact, but the manual restriction of IR transformations is heavily ineffective, and apart from that, is subject to permanent evolution. Regardless of bloated namings and superficial-looking syntax definitions, variability and extensibility are raised in contrast to GIMPLE.

For the sake of closure and simplicity, and in contrast to bitcode, the Prolog implementation excludes unconditional branches to arbitrary program statements. The implementation does not object to maximising program statements' coverage, even if expected future extensions may introduce new program statements.

Essential questions on the extensibility and variability of heap models include: May a heap be easily modified, s.t. any stepwise heap modification may be mimicked? May new phases be added to the existing reasoning framework?

The chosen IR naturally corresponds to Prolog, for example, from bitcode or GIMPLE. Nevertheless, none of those is practically considered in this work. Prolog-terms represent program statements (specification and rule set too), and as earlier in this section mentioned, may be represented as a tree. Instruction tetrads may indeed be chosen (e.g. tetrads of some hypothetical abstract machine for the moment). Regardless of the specific IR to be chosen, the AST is always the first IR directly derived from a given listing (see fig.12). Choosing an IR different from AST or terms could provoke the drop of one or more phases depicted in fig.12. However, this simple remark, was and often still is violated by several projects, including GCC, LLVM, and by jStar [193], where verification is performed on optimised triads just shortly before and during code generation. Many other projects implementing static analysis violate the remark, too, though for different reasons. Although the remark seems simple, in consequence, more exact feature definitions are required, to which aliases must be added. The following features seem essential in achieving the goal: (1) having the possibility to extend and vary existing phases of heap analysis, (2) to represent adequately, to avoid bloated semantic contexts as well as assets of external data containers. The absence of possibility (2) is an indicator of a model with raising imprecision and complexity. The simplicity of a model depends on a complete representation of all required data. If needed, representation primarily affects term IRs of incoming programs and semantic fields, containing data such as depicted in fig.12. Additional data is not mentioned in fig.12, even if it still may be needed in local phases. Thus, they do not imply changes to the default computation model for heaps (see fig.56, see obs.1.14). Since this work's main objective is to perform verification, its critical IR is bound for static analyses. Hence, terms ideally cover any hierarchical, tree-structured IRs — also w.r.t. future extensibility, variability, and possible later implications with GIMPLE or bitcode.

The advantage of terms is their direct notation and direct access to the whole expression and sub-expressions.

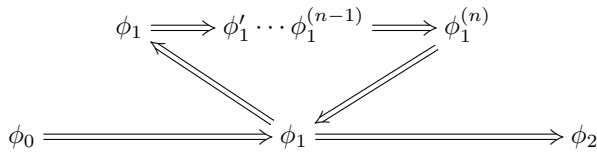


Figure 56: Pipeline architecture for the prover and syntax processors

If direct notation were absent, it would have to be composed individually, which would be a laborious task. – It is disadvantageous but essential what is mimicked by functionals. Finally, the full description would have been bloated compared to direct term-IR, even if auxiliary functions and semantic fields would be introduced (e.g., approximating limits).

C. Language Compatibility

According to the introduction, verification is often considered over-engineered and too academic. The reasons are diverse: too many (too rigid) conventions imposed on models and formal theories. All descriptions involved are too bloated, cluttered and hard to understand before doing anything reasonable at all. They are too many diverse formalisms to learn. From thes.4.11 and the previous section follow generalisations regarding specification and verification languages for heaps (see sec.II, see obs.4.12):

Observation 4.12 (Comparison of Declarative Paradigms). The declarative paradigm, logical first of all, fits heap verification better than the functional or imperative paradigms due to formula representation and logical reasoning.

This observation may occur too insignificant on the first look. It means that verification of Hoare triples is more comfortable in terms of a logical PL, the specification and verification of triples – this may appear first evident. However, only a few verifiers were built based on the logical paradigm, and even those often are too restricted or closed for variability or extensibility (see sec.I).

Logical predicates describe calculation states. Predicates first do not insist on side effects to express a state nor on any global state. Visibility depends on predicate variable symbols, not on external memory containers. In an axiomatic system as Prolog is, rules may be altered individually. By using (logical) programming, we allow solving problems related to verifying heaps. From [302] follows functionals are less suitable for describing hierarchical elements – as heap terms are (see def.3.10, def.6.1, cf. sec.VI-H). Mixed input and output terms make the representation and query very compact and powerful simultaneously (cf. def.4.3) and handy for proofs (cf. obs.4.7). Hence the Prolog-dialect is more appropriate than the functional paradigm for verification and specification over heap terms (cf. sec.VI).

Lämmer [149] suggests a proof framework focused on confluency smoothly tying up program components [93]. Although it is not related to dynamic memory, it makes propositions of narrowing down further quasi-minimalistic specification and verification languages w.r.t. class objects (cf. sec.I).

Observation 4.13 (Simplification of Inductive Proof Primitives by Generalisation). If simple definitions and assertions may be formulated easily, proof searches are often generalised and straightforward.

The easier some (recursively-enumerable) definition gets from the introductory examples, the less often corner cases exist, the less often exceptional cases need to be implemented and specified, the higher the reuse level. It is common sense that the fewer paths a CFG spanned by lemmas, theorems, and inductive data structures have, the simpler it gets. For example, replacing some existentially quantified symbol in a formula with its polymorphic all-quantified symbol may look simple, but it may impose restrictions that indicate unreliable code, imprecise specification or both. Restricting some symbol a , at least one predicate call and symbol binding is needed. It implies all-quantified symbols may, by default, significantly increase expressibility.

Replacing atoms by symbols lifts the hosting formula. Symbols are naturally in Prolog and may be bound by term unification, namely, the finite normalised resolution form [83]. As discussed in the previous section, formal verification checks whether some given program (or the resulting structure of its calculation) matches a specified structure. As also discussed previously, both processes are heavily influenced when being generalised. Naturally, both processes are different from the beginning. The most remarkable difference is due to expressibility.

Corollary 4.14 (Minimisation of Differences between Generational and Checking Languages). Simplified and lifted heap terms may be reused in expressions of the same language for describing

- (1) specification,
- (2) verification and
- (3) the incoming PL.

Proof. Using one language for all three cases is extreme for the task of minimising the difference between languages. This extreme position is to be used unless a plausible counter-example rejects it. Whenever the difference between (1) and (3) is resolved, either by letting the incoming PL be logical or letting the obtained IR be terms of an incoming (imperative) program, then assertions are noted as subgoals (def.4.3) and the incoming program as terms (def.3.10). Contribution [293] can be considered a broader field study on the proposed minimisation of a language and with validation being a regular-mighty typing issue (cf. sec.1.14, sec.III-A, fig.35). Assertions about the program refer to the incoming program's term (see sec.VI, sec.V).

The other way round is not permitted. This congruency is sufficient to resolve the difference between (1) and (2). Formulae and other referenced inductive definitions may all be written as Prolog facts and rules. Those are sufficient as a specification in order to perform a verification. Tactics, specification rules, auxiliary predicates, and new user-defined predicates may be added to an empty or existing Prolog theory.

Tasks (2) and (3) rival: (2) sets how the generation processes some heap graph, and specifically (3) attempts to verify based only on provided assertions. The description must be heap graph focused, where the verification process has the "understanding" (recognition) and analysis needed in that role. In sec.VI, the analysis bases on syntactic definitions. The precursors are the unification of syntactic, semantic and pragmatic heap definitions and their checks. \square

Lee's fair remark [184] is that higher-order logics are of utmost importance to applicability. As initially mentioned, Prolog supports it (cf. fig.71). Rules may evolve, but not whilst runtime (see sec.I). Hence, defined rules are accessible in both processes (2) and (3).

Observation 4.15 (Language Confluency upon Verification). Given a PL P , specification language S , and verification language V . P 's listings manipulate the dynamic memory. The relationship, as illustrated in fig.57, is inspired by Reenskaug's meta-pattern Model-View-Controller (MVC) (see fig.57).

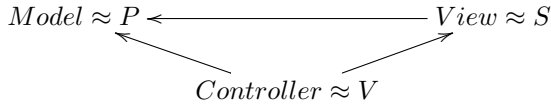


Figure 57: Roles in the Model-View-Controller meta-pattern applied to heap verification

The heap model is described by S and processed by V (when discussing MVC's components, we refer to particular instances, e.g. a specific program). Some user may use V to alter the state and observes results by S (see def.1.3). However, in Reenskaug's classic pattern, V immediately manipulates P , which varies here. P may have different graph representations of S with the properties mentioned earlier. As a side-effect, a narrowing down also leads to the interfaces that communicate in one language.

D. Knowledge Representation

This section considers core Prolog listings as a knowledge base, a well-founded and well-defined formal logical PL. It is founded on a quantitative and qualitative comparison of terms, rules and subgoal queries.

Initially, rules may be represented in any declarative paradigm: functional or logical. For XSLT and Prolog, a quantitative analysis was made [294] for semi-structured

data (including terms, see the previous section), as well as a qualitative comparison of over 80 selected typical examples (cf. sec.IV-B, process signatures apply for heap verification). The latter analysis bases on carefully assembled examples from monographies, tutorials and other relevant online resources available. Based on Hålsted metrics (see fig.58), the comparison showed:

- 1) Prolog leads in all, except one, examples on average of approximately slightly about 30% compared to XSLT, which may be derived from the ratios $N_T : N$ and $\eta_1 : \eta_2$.
- 2) On average, the equivalent Prolog algorithm is 50% shorter. Often it is even shorter. It bases on N , λ and $\Delta_N = \|N_T - N\|$.
- 3) Furthermore, functional implementations suffer from closure, so only built-in operators may be used. User-defined are not allowed by default but could be user-defined with significant efforts needed, but still tractable as in Kiselyov's SXSL-T implementation [294]. Prolog may introduce user-defined terms, IR and arbitrary user-defined operators and rules, although a rich list specification covers most spatial elements.

The qualitative analysis explains why expressions and rules may be represented easier based on lingual and expressibility considerations and non-metric measures. Mainly this is due to the genuinely logical representation of terms and relations. In contrast to functional languages (having a compact denotation), logical languages are based on atoms, terms and prioritised rules (see. theo.4.10). As denotational semantics are declarative, a complete representation can be reduced to near to minimalistic expression. Results are calculated on input vectors, and no further constraints are needed for this. Variables are not symbols. Symbolic variables are variables with dedicated semantics. In a λ -abstraction, they are only used as bound and one-way, namely a unique binding. Their scope visibility is similar to those of program variables. A general substitution of parameterised function as a replacement for relations does not solve the problem, as found in [38]. An axiomatic semantics should be preferred over denotational semantics if the logical inference and its logical units are in focus, as with heap verification. Prolog listings are a particular way to define axiomatic semantics. Logical units include atoms, logical expressions, terms in general and relations over those, and predicates. Knowledge representation, transformation and comparison succeed whenever the chosen paradigm fits, as for one case, it is demonstrated in [294].

Apart from these, there are further remarks to take into consideration on heap verification:

- Prolog Rules are compact and may be called at any analysis phase. Goals and subgoals may be arbitrary. Non-termination, in general, is unavoidable and are not artificially bound. However, for the sake

N	..	program length
N_T	..	theoretical program length
L	..	intellectual language level
λ	..	language abstraction level
η_1	..	total amount of operators
η_2	..	total amount of operands

$$\begin{aligned} \eta &= \eta_1 + \eta_2 & V &= Nld(\eta) \\ N_T &= \eta_1 ld(\eta_1) + \eta_2 ld(\eta_2) & \lambda &= VL \end{aligned}$$

Figure 58: Quantitative analysis using Hålstead metrics [112]

of efficiency, to the approach presented in sec.VI, a harmless restriction may be introduced.

- Eager evaluation of terms is used. Lazy evaluation is excluded. For instance, this leads to recursive data that the Ackermann function (see fig.45) cannot be evaluated until all passed arguments are thoroughly evaluated first. This restriction is powerless since programs may constantly be rewritten, s.t. an infinite data stream is replaced by finite, except the infinite case itself, but that is excluded by practical means. Moreover, term unification already leads to undefined term portions, so symbolic variables are assigned. There is no need to recalculate everything again in recursive definitions, but only those subterms affected by the change are in the obedience of the principle from fig.54.
- The base type of verification is a term. Next, the base type may be considered parameterised as in the λ -calculus of third-order, so a type is of $\Lambda_{T_{\lambda 3}}$, which allows quantified variables. A type built up from other types is a dependent type (see def.1.9). A composition is according to def.4.1 using some functor. Thus, heap comparison can be formalised as term comparison. However, terms may theoretically in Prolog contain self-application by referring to symbolic variables. Self-application may be checked by the predicate `unify_with_check` as introduced at the beginning of this section. The higher the level of λ -calculus, the higher constraints impact, so the fewer paradoxes matter. Functors may be used for modelling arbitrary data structures, including lists and tree and (class instantiated) objects.
- In case a subgoal succeeds, the set of all unifications is issued. For example:

$$?-H=\text{pointsto}(a,2), VC=\text{pointsto}(a,X), H=VC.$$

issues the result set: $H = \text{pointsto}(a,2)$, $VC = \text{pointsto}(a,2)$ and $X = 2$. Counter-example generation may be obtained for free from term unification, e.g. by "`unify_with_check`". For improved traceability, it should be enriched by calls to write as a subgoal with all relevant symbols [248]. The nearest term shall

be evaluated top-down in order to locate the first differing sub-expression. In general, ISO-Prolog allows several tracings, including built-in predicates for just that purpose [83]. If verification continues stepwise, then recording each step into a DOT-file is very recommended for understanding and troubleshooting purposes. Counter-examples have to reproduce at least one valid case that makes the verification fail at a specified position. Term unification leads to the most common substitution. Hence, a non-matching functor, arity or not unifiable variables are a perfect shot as counter-example — this is so universal that no further explanation is needed except the information about the current position in the proof tree traceable via DOT, for instance. In general, a particular example reflects a term that makes the verification refute intentionally – this may be when some atom does not unify with a functor, or atoms differ from functors.

- Relief of symbolic restrictions according to the heap definition from [27] on runtime (see sec.II), including rule set analysis for deductive reasoning ((bi-)abductive) [54], [211], which may be better modelled (also cf. sec.V, sec.VI), is Horn-rules. Secondly, analysing rules and alternatives may succeed during a search without additional efforts. However, due to applicability, the amount of alternatives needs to be bound. If a rule is selected, then abduction may be mimicked by a Horn-rule of kind "`b:-a1,a2,...,an`". If any of a_j remains undetermined, so some remain symbolic, then arbitrary different b may be chosen if any alternatives were available. That requires preceding terms, and head arguments of b are not excluded. It must be noticed, in order to fit Prolog for heap verification, no further (auxiliary) predicates are required to interpret a term since it represents straightforwardly just itself. The lexicographical order on pointer names contributes to normalisation. The same goes for simple heaps regarding the left-hand location and calls to built-in predicates and lists, for instance, when dealing with "`concat`". `concat` and further one-pass scanning predicates are effective due to non-repetitiveness. Hence, numerous transforming and evaluating predicates may not be needed. W.l.o.g. reasoning rules are invertible, iff between all subterms of the precondition and the postcondition either an isomorphism exists, or non-invertible built-in predicates are safe not to be called in the inverse case. In case isomorphism is violated, either the mapping from the incoming vector to the outgoing is extended, or the inverse case is extended (see abstract interpretation in sec.I). An extension is problematic in inverse mappings since co-domains thin the domain, so the mapping becomes non-continuous.
- Rules overloading and prioritisation may be performed and enriched by different bodies. Auxiliary predicates may be written, e.g. in Java. Argument

terms to those predicates may be incoming, outgoing or a mixture of both. It is not sufficient to use DCGs for this work's objectives (cf. sec.I) because the control flow and tactics are subject to change. This work's objective also includes heavy heap term interpretation, as shown in the following sections. The best example for this will be discussed in due course in sec.VI, referring to strategies of top-down or bottom-up syntactical analysers.

E. Verification System Architecture

In [300] and [298], a verification architecture is suggested for dynamic memory reasoning based on Prolog. The architecture is illustrated in fig.59. The architecture follows the principles discussed in sec.I:

- (1) automation,
- (2) openness,
- (3) extensibility and
- (4) plausibility.

(1) states that proof should be found automatically without further interaction. In Prolog, a solution will be found depending on the given rules if there is no infinite recursion and all needed rules are provided. Otherwise, the proof does not terminate or does quit prematurely. Next, thanks to the approach from sec.VI, which contains design and implementation details, automation is provided. (2) means there shall be no artificial limitations introduced to terms nor rules. On one side, Prolog is open for extensibility and variability so that new rules may be added and existing ones be modified. On the other side, Prolog is closed to what is derivable from the rules only. (2) relates to the architecture and used memory models discussed in sec.III till sec.VI. (3) means a memory model is extensible and, if needed, variable too in its rules. Modifications are always possible due to allowed Horn-rule redefinitions in Prolog. The extensibility of terms and rules was discussed in full detail in the previous main section. (4) means any verification step may be traced and checked for plausibility. DOT-files' generation visualises each step and serves as evidence in case of proof refutation right with a counter-example beside the last corresponding formula. The possibility to debug verification immediately without any additional preparation and overhead tremendously simplifies debugging. It is an essential contribution to Extreme Programming. Essential parts include the rule set (acting as "programming listing"), the subgoal sequence to be investigated and a specified memory state, including the stack and heap. No other conventions need to be obeyed. No more massively overcomplicated set-up is needed.

In fig.59, the incoming program is at the entry. C or any other Pascal-like imperative PL should be recognised in — at least immediate IR injection works. The program is turned into a Prolog term IR which is then together

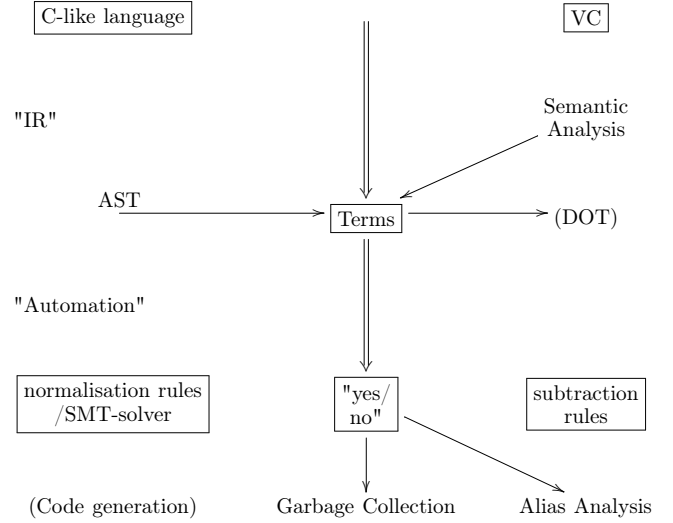


Figure 59: CFG on heap verification

with assertions about the program turned into yet another Prolog terms and rules. First, the incoming listing is checked syntactically, then semantically, including type checking and further IR-related constraint checks. Every term may at any time be visualised in the DOT-format. Assertions may refer to lemmas and theorems, which might be noted immediately as Prolog term and, if needed, may be used then during verification. During verification, several rules get activated, namely, those provided in Prolog theories and are loaded while interpreting those, e.g. with tuProlog's environment [82], [81]. Either external SMT-solvers or Prolog itself may be used as formal theory solvers. Let us recapitulate that Prolog is widely prevalent among constraint solvers [248], [46].

New phases to the heap verification may be inserted according to fig.56. Minor and significant phases are bridged by handing over the calculation state explicitly. This data-driven approach (see fig.59) is by design very closely incorporating with the assembly line architecture from [135], [252], but differs in the visibility scope of heap variables (cf. sec.III). However, the proposed conveyor may be used under the condition alias-analysis establishes individual visibility scopes, see obs.3.4.

Furthermore, in [301] are proposed and discussed the required criteria for an extensible and variable heap verifier architecture. The criteria include a minimal IR for statements of the incoming program (PCF-based [179]) with object extensions (cf sec.I-B). The presented computation model, namely the class-based calculus, is typable, so properties from the second and third-order λ -calculus (see def.1.9 and def.1.10) apply. However, as discussed earlier, now the hot-code update is excluded. Furthermore, arguments are passed either arbitrarily, by-value or by-call. In the latter case, an indicator is required, which is implemented by a reserved functor. Extensibility applies to the incoming PL, static analysis phases, and rules

(including pre-existing ones).

In [302], frames are introduced and reviewed, as well as heap definitions and interpretations. For all considered concepts, the use of Prolog is suggested to address the spotted current restrictions effectively. As heaps are term interpretations that may be bound not before in subgoals calls, in case of unification succeeds. Otherwise, unification fails, and non-unified terms illustrate a valid counter-example. It must be noticed that verification and its type signature are similar to the comparison process of template-instantiation and validation [299]. The theoretic foundation behind is a pattern-matcher, a finite comparison tree-automaton, a tree graph matcher (cf.[66]). Although the initial model is similar, the comparison differs from predicate calls, abstract predicates, pre-and postconditions, and the heap graph model. The previous analogy implies that if an assertion is a schema or type, and a given program builds up the heap graph stepwise for each program statement, and the cell's content is compatible (cf. fig.13), then verification is as robust as type checking.

Corollary 4.16 (Minimisation of Incoming Program). The result of the inhabitant check is some minimal incoming program, which alters dynamic memory.

Proof. First, it needs to be shown the claimed program always exists. Considering fig.13, the inhabitant problem here states: "Given a heap graph, which program will construct this graph (with a minimalistic number of steps)?" The heap graph can inductively be constructed by inserting incrementally (but bound by an upper limit of) edges for well-defined labelling. Second, it needs to be shown that the program is minimal. Cor.4.16 implies a (minimal) statement sequence may always be derived for a given pre-and a postcondition (corresponding to type). The calculation steps are essential before comparing with arbitrary heap states. However, the relation between "type" and "expression" cannot always be unique. So, the question arises: Which program is finally generated (cf. fig.13)? The program is generated stepwise when needed according to the assertion provided. The program is build up in a minimalistic manner because almost every edge of the heap graph corresponds with new program statements – this is under the condition of a minimalistic program only. So, a cycle in the heap graph does not necessarily have to correspond to a cycle (a loop) in a compound statement – it may be the case actually, e.g. it may correspond to two statements. Infinitely many edges may be excluded from the graph. Therefore only similar chains correspond to a cycle as a program statement whose condition is determined by the heap graph. Whilst construction by the incoming program minimality means only a set of unrelated statements to the final graph are removed. The correspondences are as follows: the "new"-operator adds heap vertices, vertex content is altered by assignment statements, which may link two heap vertices

in case of pointers.

Only those statements remain that are essential for the final's heap graph. Thus, the inhabitant check for a given type may generate a minimal program, which may be compared with a given program. Program minimisation is (implicitly) subsumed by reasoning Hoare triples, and there it is not considered separately. On a domain level of Prolog, program minimisation may indeed be subsumed by ongoing triple verification if predicates are invertible (see sec.4.9). \square

The proposed Prolog-based architecture resolves the following issues without any extra costs:

- Any incoming PL is allowed as long as its term IR is sound. Soundness definitions and new PLs may be added. Rule sets may be extended and varied. An incoming program may even be left empty, and syntax analysis is dropped totally if some program's IR and accompanying verifications terms are manually inserted. The architecture illustrated in fig.59 excludes syntax and semantic mismatches because of the most flexible phases (cf. fig.56).
- Modest specifications allow avoiding fully-fledged specifications since only those modules are specified that later must be verified. Except for full specification and a very few exceptions ("footprint"), there were almost alternatives that would have avoided tremendous efforts and hard to read assertions in the past, such as partially Smallfoot in SL. In contrast, Prolog's principle is straightforward: if some assertion is found correct, the proof succeeds and terminates unless non-termination within rules is encountered. Otherwise, the verification continues until a contradiction is found or it succeeds finally. Verification is applied only to those modules that contain assertions. Partial auxiliary predicates, such as *true* (see sec.V), shall avoid full specification and increase readability.

Polymorphism over classes is excluded here for the sake of simplicity (see discussion in sec.I, III and followings). The dependency graph of given Prolog rules and lemmas are analysed by the Prolog interpreter whilst runtime. It is also checked during syntax analysis and compilation of abstract predicates (see sec.VI).

F. Class Objects

In sec.I-B, both two prominent OCs were introduced, namely after Abadi-Cardelli and after Abadi-Leino. Since simplicity of specifications has higher importance for this work's objective, the class-based calculi choice is evident (see sec.I-B) [155], [220]. For this work's sake, there is no need to prove the soundness of adapted objects separately, nor a full prove w.r.t. polymorphism, inheritance and encapsulation again – it can be found, e.g. in [3], [48].

Remarkably, pointers to object theories do not invalidate existing constructs. They extend variable references with new semantics that used to be missing.

Consequently, an object is, first of all, an instance of some class. For the sake of simplicity, polymorphism is excluded since it does not directly affect core functionality (generic polymorphism, according to Cardelli's taxonomy, is not considered in the C++-dialects). Even "ad-hoc"-polymorphism is allowed only in boundaries of subclassing [55], namely by deriving subclasses [48] and only for the sake of improved comfortability and modularity (see sec.I-B). In Hoare calculi, polymorphism is tractable and expressible (cf.I, [185]). For the sake of this work, its only contribution does not affect expressibility. Hence, an object represented as a heap is enclosed a mapped onto some memory region without gaps containing just (object) fields. Methods are not stored in dynamic memory since it is considered the code is static and since the hot-code update is prohibited in the first place. Code updates on runtime are also prohibited because of the significant problems introduced regarding completeness and soundness (see discussion in sec.I-B). As every object is of some class type, its methods are entirely determined and typed before execution. Inherited fields and methods are fully defined too. W.l.o.g. it is agreed upon objects, their tuple pairs (all fields as Cartesian product \times its value domains) are always sorted in lexicographical order for simplicity and comparability.

Thus, object definition and transformation (down-cast in C++) into a subclass may be implemented in two different manners: (1) each field is checked according to the relation ">:" (see def.1.11), here the fields in upper and lower subclass instances diverge or (2) all fields are grouped according to some identifier inheritance. Thus, there must be an effective method to compare objects of (sub-)classes. In order to demonstrate (2), we choose, for example: "SubClass1 s1; SuperClass o1=(SuperClass1)s1;". Assume, s1 contains [o1,o2,o3], then the calculation of o1, where the upper class from SuperClass1 inherits only the fields o1 and o2, may be generated copying the first two fields, so by the initial contiguous range of s1.

Object fields are noted as a list of tuples of a kind: (identifier, value). Symbolic variables may express pointers to objects (including cycling). $A = \text{object}(A, A)$ is prohibited and may be recognised by `unify_with_check`. $A = \text{object}([(a, A), (b, A)])$ is allowed. The simplified notation $A = \text{object}((a, A), (b, A))$ is assumed because the functor implemented by core Prolog already builds the list head containing an object. Since the tuple contains precisely two elements, the composed term is always well-defined and unique w.r.t. the object web spanned. Object fields are accessible by the "."-operator and may be used within program statements and assertions. Unsound access paths are recognised during semantic analysis. Fields for some objects are (all) specified on

the abstract predicates level. These may also be defined, particularly particular (see sec.V and following).

Conventions from sec.I rising precision in this section and conv.5.17 and conv.5.18 are introduced to avoid paradoxes and narrow down towards a tractable UML extension.

V. Strengthening Heap Expressibility

In this section, SL is introduced and analysed w.r.t. the problems generated by the spatial conjunction operator. One operator may be used to separate and link heaps, dependent on pointers and their content [297]. Ambiguity allows a comfortable notation but induces several disadvantages. A major flaw is context-sensitivity. In this context, dependency, first of all, means the need to analyse a whole formula. The extra steps needed may become cumbersome and end up in analysing all possible and unrelated subexpressions. The dependent notation of the same heap graph needs to be probed first (a syntactically context-sensitive) to define an independent heap graph (a semantically CF). Although this is not a paradox, it, however, desires better. Next, w.l.o.g. heap graphs are syntactically defined in a CF manner by excluding ambiguity and improving the verification automation simultaneously from the automation perspective syntax analysis over heap formulae means overhead. In general, a heap relation may state two heaps are connected, or they are not. Rewriting an overloaded (ambiguous) formula into a singular (non-ambiguous) might not be trivial at all since all possible transitions have to be taken into consideration. However, it is always decidable because any sound heap formula corresponds to some heap graph and vice versa. An (un-)related heap to some other remains untouched regardless of which context or if it is a hierarchical heap.

Using a CF formula to describe a semantically context-independent model of a heap graph merges both concepts of what a heap is. Objects are considered complex SL units, which obey the same rules as simple units and (simple) pointers. Later are discussed applications of formal properties towards a stricter memory model, the possibilities and limitations of the proposed model.

A. Motivation

Let us look at the following very generic syntactic definition of some term expression E over integers in some classic integer arithmetics as ambiguity problem:

$$\langle E \rangle ::= \langle k \rangle \mid \langle E \rangle ' \otimes ' \langle E \rangle$$

It is relatively easy to conclude that the syntax in (E)BNF is inductively defined, and the base case denotes any arbitrary but fixed integer k . Assume \otimes is some binary operator that is total and defined over integer, like addition. If we have the situation when for expressions e_1, e_2, e_3 : $E_0 \cdots \otimes e_1 \otimes e_2 \otimes \cdots E_n$ and $n \in \mathbb{N}_0$ calculates $e_{1,2}$, where $E'_0 \cdots \otimes e_1 \otimes e_2 \otimes \cdots E'_n$ calculates $e'_{1,2}$, where

$e_{1,2} \neq e'_{1,2}$, then either the rules of this calculation are unsound (possibly by design, but not later than that), or calculation is context-sensitive, so depends on E_0 and E_n , or E'_0 and E'_n . It must be noticed that if $E_0 \equiv E'_0$ holds and so forth, then $E_n \equiv E'_n$. So, the problem of differentiation matches with the problem of (un-)proper calculation. Beginning with the base case, namely, $e_{1,2} \neq e'_{1,2}$ where $E_0 \neq E'_0$, $E_n \neq E'_n$, it may be stated that both E_0 and E_n are not empty at the same time. Hence, dependency means that with $(e_1 \otimes e_2) \otimes e_3$, that e_3 contains syntactic information, which influences $e_1 \otimes e_2$. Thus, for each j multiplication, $\otimes_{0 \leq j}^n e_j$ means a complete analysis of all remaining factors in the worst case. The polynomial's rank $\binom{n}{2}$ binds complexity. So, which relation does this bound have towards heaps?

Observation 5.1 (Operator Overloading). The operation \star is ambiguous (see def.5.6). It might be used for connecting and separating heaps and impacts the overall logical analysis of heaps.

There is a structural analogy between the definition of \star in SL and the previous definition of \otimes (cf. def.5.6). Each heap needs to be thoroughly analysed during heap interpretations (it denotes E in the previous example).

Thesis 5.2 (Strengthening Expressibility of Ambiguous Spatial Operation). If the expressibility of SL's spatial operator \star is strengthened, semantic ambiguity can be diminished. The exclusion of context-dependency eventually allows automation and eases heap analysis.

Proof. The proof consists of two parts. First, it needs to show that operation strengthening implies less semantic ambiguity. Second, it has to be shown that the absence of context-sensitivity implies automation and enables a more accessible heap analysis.

The first part is common sense. If some expression has many (semantic) meanings, then the context determines its denotation. The fewer meanings (ideally one) some expression has, the less ambiguous it is. In the case of a single meaning, the expression is non-ambiguous. W.l.o.g. this naturally also applies to \star (proofs on properties will follow with the following theses in this section).

The second implication follows from the new heap calculus to be established in this section, which is based primarily on the core properties of \circ and \parallel , as well as the concept that objects are also heaps (see sec.V-D) and validated later practically by sec.VI-H. The relevant properties of \circ are def.5.7, theo.5.8, and the theorems relevant for heap analysis lem.5.10, theo.5.11. Due to remarks made in this section w.r.t. duality def.5.14 and lem.5.15 suffice for \parallel . For the new heap calculus, it is essential to perform improvement calculations based on spatial distributivity, founded on theo.5.16 and lem.5.13. \square

Thesis 5.3 (Simplification by Differentiating Heaps). When the syntactic and semantic unity is obeyed, an

adequate representation simplifies the comparison and specification of given and expected heaps. Diff(-erentiat)-ing heaps may conduct the comparison.

Proof. Here it is necessary to show that heap differentiation leads to simplification. If two and more heap (terms) may be compared, then the difference may be calculated effectively as a term. The calculation is founded on term unification, the anonymous " $_$ " operator, heap normalisation in theo.5.16, inversion (conv.5.12), thes.5.2, the properties established in sec.VI-G and reference implemented as described in sec.VI-H. That may be applied to a rule set to check completeness (cf. sec.V, particularly def.5.19). Missing and overlapping heaps in rules may be calculated. Partial heaps simplify specifications due to a shorter notation (see sec.V-E). \square

This thesis implies that CF-ness allows defining formal theories about equalities and inequalities of heaps. The integration of SMT-solvers may further automate those theories.

Thesis 5.4 (Complete Heap Rules by Incomplete Specifiers). The notation of incomplete heaps allow solving the problem of complete heap rules.

Proof. This thesis is a specialisation of thes.5.3. \square

Corollary 5.5 (Strengthening Modelling). The strengthening of the spatial operator does not violate the locality principle of (object) heaps. The strengthening is a proposition for extending the modelling language(s) UML/OCL by pointers.

Proof. The idea behind this is introducing strengthened spatial operators, which may either connect (cf. theo.5.8, lem.5.10) or separate heaps (refer to def.5.14 and lem.5.15).

It must be noticed that UML/OCL's expressibility is equivalent to third-order λ -calculus (cf. [1] for a direct proof), so it can be defined as in def.1.9. Hence, it can be represented in Prolog terms described in sec.IV and extended by APs described in sec.VI. \square

These observations made, and those follow from previous analyses sections and remarks. The following might be implied:

- 1) A simple model must be represented in simple terms. [249] may serve here as a negative example. It must be stated that Suzuki's model at the end is only manageable at first glance since the objective complexity is hidden in short but very hard to predict proper pointer semantics. An incomplete set at first glance represents a complete rule set, which may commit considerably complex pointer operations. Even very trivial modifications may easily lead to unexpected behaviour. So, in a highly dynamical system, minimal edits shall not affect the overall

behaviour, mostly not remote spatial parts of a heap specification.

- 2) Various previously mentioned memory models, particularly their conventions, are not that important after all. It was shown that introducing new conventions does not necessarily extend but restrict expressibility. Potential new features from new or improved PLs too often are too specific, s.t. rules will often still need to be modified. Hence, variability and extensibility are that important (see sec.I-B, sec.IV). It is more important to describe and provide a given memory model adequately with constraints rather than covering full language features from the practical perspective. The heap graph is agreed to be the primary domain of all possible heap denotations since it is the minimal consent that all possible heap verifiers may agree on unconditionally. This decision is motivated by a utilitarian approach. For details, please refer to sec.III for an epistemological definition of the term "heap".

The proposed strengthened model stands for a more effective verification, where the heap theory may be separated from Hoare logical non-heap-related rules. Verification rules are represented as Horn-rules. Their interpretation terminates due to Prolog's term interpretation and finite transducers [298] (see thes.4.11, cor.6.17). In the next step, the strengthened operator \circ replaces \star , s.t. APs may be automatically recognised during syntax analysis later (see sec.VI).

B. Ambiguity of Spatial Operators

Hoare initially suggested using mathematic formulae as a most precise specification and verification language. Later, predicate logics was preferred, as well as multiple logics derived. In the case of heap specification and verification, practice showed that specialised logics might be applied even more successfully (see sec.I-A, sec.I-C). However, unbound formulae may be more comfortable when it comes to automation, as will be seen later. One of these more acceptable conditions of automation may be non-ambiguous spatial operators. Strengthening conditions in a formula leads to restrictions.

The problem with precision and expressibility is fundamental and is not only due to logics. It covers different areas, starting with recognition, passing-over notation, obeying constraints and ending with expressions. The reason for emerging ambiguity shall be researched (sec.III, sec.V). For example, it is no surprise when some given expression language differs from its declarative specification, and as such, there are apparent gaps in their semiotics (see sec.IV).

A fundamental question concerns the equality of two heap representations. It may significantly complicate equality if having different heap normal-forms or canonicalisations.

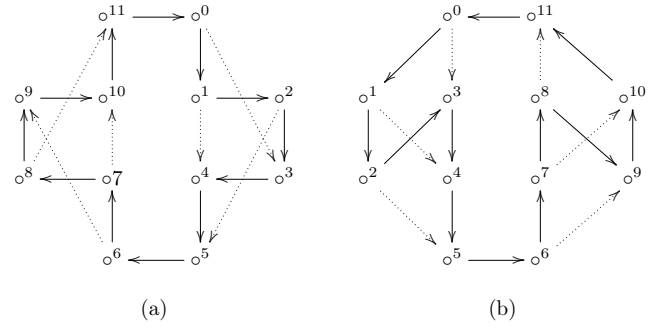


Figure 60: Isomorphic 3-regular heaps with objects

So, the question regarding an isomorphism of two lifted heap graphs can be estimated as essential and further be discussed, referring to fig.60. In general, graph isomorphism is bound by exponential complexity, even for worse predictions. In practice, exponential algorithms exist, which can be approximated by a third-order polynomial for a small number of graph vertices. If the heap from fig.60 (a) contains only solid lines, later during analysis, there might be a connection between vertices 0 and 5 and both vertices were specified. Deciding if isomorphism is present might become difficult. However, complexity is reduced with types and labellings, which remain invariant. The isomorphism complexity remains if pointers to a graph are renamed, and apart from that, this heap graph remains unchanged. For fig.60, this might be the case when applying the permutation $(0\ 11)(1\ 8\ 2\ 10\ 3\ 9)(4\ 7)(5\ 6)$, starting with the graph from fig.60 (b). Notice the relatedness of permutations of heap locations w.r.t. arbitrary pointer rotation (see sec.I-C). From a practical perspective, the isomorphism problem is only actual when it is necessary to check whether, in principle, a given abstract heap graph may be transformed into another abstract heap graph (cf. def.6.9). This transformation would be relevant only if naming may be parameters – this is when names may change.

Sec.VI considers APs in more detail. For example, let us consider fig.61.

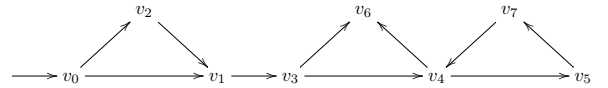


Figure 61: Example of a connected heap graph

According to a minimal coupling, this graph may be bisected into sub-graphs among the bridge $v_1 \mapsto v_3$, see fig.62.

The graph may be described by separate predicates $\pi_0(v_0, v_1)$, $\pi_1(v_3, v_4)$ and by predicate $\pi_2(v_4, v_5)$. Alternatively, it may be abstracted to $\pi_0(v_0, v_1)$, $\pi_{1,2}(v_3, v_5)$, where the graphs represented by predicates are connected,

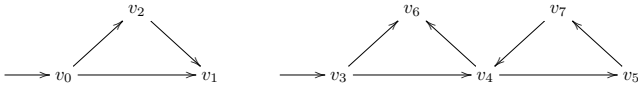


Figure 62: Example of a disconnected heap graph

and visible vertices appear as arguments by the implicit definition π_j , see fig.63.

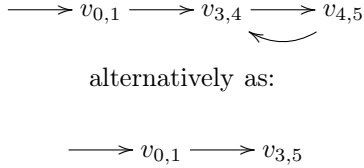


Figure 63: Example of a possible heap dissection

Unfolding, according to the definition of π_j , leads to the inverse.

Now, more generalised questions regarding an adequate heap representation may be asked:

- 1) How to specify non-ambiguous formulae and perform the utmost determined verification?
- 2) How to resolve isomorphism, locality and graph abstraction in simple means (w.r.t. heap representation)?
- 3) How to restrict mandatory checks of objects in program statements (object representation)?
- 4) How to solve equalities effectively of heaps if not all vertices (and edges) of the heap graph are defined (partial specification)?
- 5) How to avoid redundant heap analyses (as well as redundant checks at each heap analysis phase; stepwise verification)?

Sec.III introduced to Reynolds' and Burstall's heap models. This section reviews Reynolds's conclusions and effects and discusses derivable graphs and graphs generated after parameter modifications. Properties and expressibility are observed.

Definition 5.6 (Observable Heap by Reynolds). Heap is defined as $\bigcup_{A \subseteq Addr} A \mapsto Val^n$ with $n \geq 1$, where A is some address space, and Val denotes some values domain (e.g. integers or composite). The observed heap operations behaviour (cf. theo.3.6, def.3.7) may imply the following properties: Given two heaps H_1 and H_2 , then $H_1 \star H_2$, where H_1 denotes some heap assertion $H_1 = (V_1, E_1)$ ($H_2 = (V_2, E_2)$ in the analogy), where directed heap edges $E = V \times V$ are s.t. $\forall v_1 \in V_1, v_2 \in V_2$ with $v_1 \neq v_2$ and $V_1, V_2 \subseteq V$ hold in the following cases:

- First case (Separation): $(v_1, v_2) \notin E_1$, and $(v_1, v_2) \notin E_2$.

- Second case (Merge): $\exists s \in V_1, \exists t \in V_2 : (s, t) \in E_1$ or $(s, t) \in E_2$, then H_1 or H_2 contains \star -separated $s \mapsto t$.

Both variables and pointers are stored in the stack. A pointer's content is stored in a heap. The following domain equation holds according to [26]: $Stack = Values \cup Locals$. As program statements run, the internal memory state evolves and is checked against the explicit assertion annotations provided to the program. Heap assertions are either true or false, depending on a specific heap to be interpreted. The syntax of assertions is defined by def.3.10. From def.5.6 implies the binary operator \star may be used with two intentions: either to specify two heaps do not overlap, or two heaps do overlap and share at least one common heap vertex. Operator \star is used as logical conjunction. It is a spatial operator, which expresses the (relative) memory location and connectivity. Conjoining heap formulae define how two heaps are located and related to each other. Heaps imply dynamic memory is occupied at a variable but fixed address. The heap's types define their size. If defining connectivity between two heaps as a bipartite graph (bigraph), then on its left-hand side, there are pointer locations, and on its right-hand side, the assigned content set. A maximal matching is required to reduce the number of conjunctions for a given heap formula to describe a connected heap graph fully. This approach is cumbersome in practice since there is no definite desire from the developer's side to describe a most compact heap graph whatsoever (see sec.III-A). Nevertheless, if the obtained heap graph strongly differs from the expected, then unexpected superfluous regions of the heap are indicators for an incorrectly working incoming program. Other criteria may be critical too, for example, a good relationship between syntactical representations and a graph to locate vertices and edges and navigation through edges. A compact does not benefit here, in fact, the opposite is the case, and it would be hard to read. Concrete dynamic memory cells must be compared. Hence, regular expressions as the proposed comfortable variant are excluded. Regular expressions, as mentioned, suffer from non-locality: as soon as the heap graph changes locally at one place, then often the complete regular expression changes. Desired behaviour is different. Ideally, a single edge insertion has to change the formula hardly, and if, then only the affected part. (Sub-)heaps not affected shall not impose changes to unrelated parts of the formula.

When comparing def.5.6 with the definitions from sec.III, quite considerable complexity may be implied, and definitions are ambiguous as long as only fragments are analysed. In order to fully resolve dependencies, it is always required to analyse all conjuncts comprehensively. The given definition may be considered an attempt to define a single heap because Reynolds did not define it as a singleton. He defines a heap set instead. Unfortunately,

other authors (see sec.I) also only define a heap in fact as plural, although many author's informal remarks and sympathies tend to support more a singular definition even if it is plural. It must be considered heap definition in def.5.6 as derived from observations is a direct singular definition and does not contradict its origin plural definition. That is why the motivation sparks off to strengthen \star and replace it with a direct operation. Reynolds' \star is a classic example of structuralism. As soon as the new two operators are defined ($\circ, ||$), properties and equalities are researched, and a new term algebra is defined. It will lead to a new quality level regarding progressive confluency since the heap calculus to be obtained may be decided on enclosed terms. Term algebras define new formal theories over heaps, which may immediately be used as Horn-rules in Prolog (see thes.4.11).

C. Strengthening Spatial Operators

Due to ambiguity, \star may be used for heap conjunction or disjunction. Apart from strict differences (thes.5.2) in different SL implementations, \star is often used as another logical conjunction. The solution to this problem is presented in this section. Heap conjunction is formally introduced as well as its properties. Afterwards, disjunction is introduced. W.l.o.g. expressibility is not restricted by the new operations (cf. theo.3.6).

Definition 5.7 (Heap Conjunction). Heap conjunction $H \circ \alpha \mapsto \beta$ is defined as heap graph, where $G = (V, E)$ is the corresponding heap graph for given heap H , and where $\alpha \mapsto \beta$ denotes a base (simple) heap:

$$\begin{cases} (V \cup \{\alpha, \beta\} \cup \beta', & \text{if } isFreeIn(\alpha, H) \\ E \cup \{(\alpha, \beta)\} \cup \{(\beta, b) | b \in \beta'\} & \text{if } H = \underline{emp} \\ & (V = E = \emptyset) \\ \underline{false} & \text{otherwise} \end{cases}$$

Here $\beta' = vertices(\beta) \subseteq V$ defines all the heap graph vertices, which are pointing from β . In case β is an object, then also all object fields are considered that are pointers. As α may point to just one unique heap graph vertex (e.g. path accessor to some object), no more than one matching vertex exists in $isFreeIn$ for some given heap H . The general assumption of the definition above is that a stepwise heap graph construction using conjunction always exists. There always exists one matching vertex. Otherwise, two heaps may not be joined.

For example, three pairs of pointers need to be joined (pointer points to some content) a, b, c (see fig.64). First, heap a has to be expressed, which may either be arbitrary or $\underline{emp} \circ a$. Only if a exists, a points to some content that equals the initial heap b and is not connected (for the moment being, we consider this to be the initial state), only then both heaps are connectible. If assuming the opposite, so when in the heap graph there are two same content cells, then by definition, this is not possible, since only one unique content (see later) is allowed though with an arbitrary number of aliases.

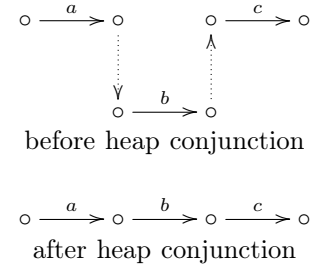


Figure 64: Heap graph before and after conjunction

Assuming there are the exact contents, but not the same as mentioned, then the accessor path must vary. Otherwise, a contradiction is found. In both cases, the possibility of incorrect conjunction is excluded. So, the result is a connected heap $a \circ b$. Now conjunction may continue under just mentioned conditions for c . In case of success, we get the heap graph as illustrated in fig.64. As we are interested in the conjunction of arbitrary graphs, e.g. binary trees, we allow conjunction in any parts of the connected graph. For example, $a \mapsto 5$ is valid conjunction. However, $a \mapsto 5 \circ b \mapsto 5$ is not. Thus, we may express aliases, for example, heap graph $x \circ \longrightarrow \circ^z \longleftarrow \circ y$ as heap term expression $x \mapsto z \circ y \mapsto z$.

Heaps may be connected in different ways when a graph vertex is an object. For example, it may be agreed upon object assignment only changes a pointer or just one single qualified field. The assignment may also be subject to different terms. For example, when all fields are simultaneously assigned either to some input vector (e.g. array or string with specified delimiters), only a single field is assigned, and all others are dropped (see sec.III). For simplicity, but w.l.o.g., for a C(++)-dialect further, only the assignment of kind one-to-one is considered (see sec.V-D).

Remark: Let Φ_0 be some heap, then $\Phi = \Phi_0 \circ a_0 \mapsto b_0 \Leftrightarrow \exists (a_m \mapsto b_m) \in \Phi_0 \wedge (a_m = a_0, b_m \neq b_0 \vee a_m \neq a_0, b_m = b_0)$ follows.

Theorem 5.8 (Conjunction of Generalised Heaps). If given two heaps H_1 and H_2 , the conjunction \circ links those together to $H_1 \circ H_2$, if at least one common vertex exists in both heap graph representations. By default, it is agreed upon $H_1 \circ \underline{emp} \equiv \underline{emp} \circ H_1 \equiv H_1$ holds.

In contrast to def.5.7, the first part of the \circ -term is scanned as potentially matching vertex – this is chosen arbitrarily and does not impose any obligation. Otherwise, it may freely be changed. Further, it is agreed upon that $H_1 \circ H_2$ denotes a united heap graph.

Proof. This theorem is a generalisation of def.5.7. Both H_1 and H_2 may be simple heaps $a_1 \mapsto b_1 \circ a_2 \mapsto b_2 \circ \dots \circ a_n \mapsto b_n$. If a shared element does not exist in both graphs, then according to def.5.7, this yields \underline{false} – if this is shown first, then soundness holds. This implication,

however, matches the expected conjunction. Otherwise, if at least one common element exists, then according to induction, we select one element, and then both heaps connect. It shall be noted that conjunction only assumes graphs are connectible, and we are not interested in more than one shared elements to be connected. All vertices except one may hypothetically be used for joining. The only exception is naturally the one to be used for joining graphs. In this case, the resulting graph remains simple. Otherwise, the joined heap graph's beginning or end is either in H_1 or in H_2 .

Furthermore, it must also be in both graphs H_1 and H_2 simultaneously. The latter, however, can be excluded. Due to this contradiction, the validity of the theorem follows.

By definition, $a \circ a$ equals *false*, which needs to be filtered for all conjuncts. The discussion on $a \circ a$ -solver will be later. It may be implemented using some "active set", which contains statically all successfully processed simple heaps. \square

Convention 5.9 (Locations). In APs, locations may be symbols. For the sake of usability, it is agreed upon APs and locations (mainly w.r.t. object fields and locations), the left-associative binary operator grants that field access ". ". Field access may be inductively recursed.

Left-associativity denotes some term
`object1.field1.field2.field3` by default to equal:

$$(((object1).field1).field2).field3.$$

Thus, symbolic variables may replace parts of the access expressions to a field. That increases modularity, but particularly also expression flexibility.

Lemma 5.10 (Monoid over Conjunction). $G = (\Omega, \circ)$ is a monoid, where Ω denotes the set of well-defined heap graphs and the binary operator \circ denotes heap conjunction.

Proof. In order to show that G is a monoid, it is necessary to show: (i) Ω is closed under \circ , (ii) \circ is associative, and (iii) $\exists \varepsilon \in \Omega. \forall m \in \Omega : m \circ \varepsilon = \varepsilon \circ m = m$.

Let $\omega \in \Omega$ be some connected heap graph obtained by the binary functor \mapsto according to def.3.9. According to def.5.7 $\forall \omega \in \Omega : \omega \circ \omega = \text{false}$ holds. Otherwise, for $\omega_1, \omega_2 \in \Omega$ there may be only two cases. If ω_1 and ω_2 share at least one vertex, then according to theo.5.8, the corresponding heap graph is defined, otherwise the result is *false* (denoting ω_1 and ω_2 do not intersect). Thus, we showed that Ω is enclosed over \circ and that a heap graph is the result of conjunction. In that case, a link is successfully established.

Next, associativity must be shown. Namely, $m_1 \circ (m_2 \circ m_3) = (m_1 \circ m_2) \circ m_3$ holds. Fig.64 immediately implies the validity of the equation from both sides. The equation holds because of two possible options. First, it does not matter if the contents of a and b are connected. Second, it does not matter whether a is linked to $b \circ c$. The

latter might be because the connecting vertex b remains invariant, where the ordering of conjunction changes.

G builds up a subgroup. It remains to show the existence of a neutral element ε s.t. (iii) holds. The equations follow from a lifted theo.5.8. \square

Remark: (i) implies $c \notin b \wedge c \neq a : a \mapsto b \circ c \mapsto d \equiv \text{false}$, and $a \mapsto b \circ a \mapsto d \equiv \text{false}$ holds. It is evident if there is a choice, then it does not matter which vertex to connect first – the result will be the same due to confluency due to (ii) property shown later in lem.5.11 (cf. fig.7).

Remark: Closure (i) indicates the non-repetitiveness of a substructural logic (SL as such, see sec.III-B), which still holds and will be shown later.

Theorem 5.11 (Abelian Group over Conjunction). $G = (\Omega, \circ)$ is an Abelian group.

Proof. Due to lem.5.10, G denotes a monoid. Hence, it is still necessary to show, (i) the existence of an inverse for any element from the carrier set over heap graphs, s.t.:

$$\forall \omega \in \Omega. \exists \omega^{-1} \in \Omega : \omega \circ \omega^{-1} = \omega^{-1} \circ \omega = \varepsilon \quad (1)$$

hold and (ii) \circ is a commuting operator.

Let us show first (ii) holds that in the base case, $loc_1 \mapsto var_1 \circ loc_2 \mapsto var_2 = loc_2 \mapsto var_2 \circ loc_1 \mapsto var_1$ holds due to the inductive def.3.9. Also, the inductive case holds as long as conditions hold of \circ . The induction condition may be obtained from fig.64 the \circ -operator commutes for two arbitrary connected heaps. However, as soon as APs are considered, the denotation of \circ -connected terms may be limited by a predicate's boundaries, and those terms may then not be dropped, as there still might be a subgoal in APs. From a practical perspective, this does not bother. On the contrary, it requires the developer to obey stricter software modularity, positively affecting the specification.

The proof continues by showing property (i). An inverse element, if existing, neutralises any given element. So, we better answer the following questions: What specifically hinders us from defining an inverse heap? When discussing natural numbers, then the inverse of addition is subtraction enclosed to the same carrier set (for simplicity, we skip corner cases). The same happens to a field over complex numbers, which is an extension of real numbers. Moreover, even if real or complex numbers are not countable, in practice, arithmetic field extension still leads to a significant simplification of calculation. Even if the answer to numerous questions related to real numbers might seem vague, such as: "What does the imaginary number i stand for in reality"? Still, it showed that i is useful for calculations in numerous applications due to the identity $i^2 = e^{i\pi}$. So, it would only be fair then to ask: Why not postulate some inverse heap in eqn.1, at least so we can be sure to calculate the right thing until shown otherwise?

Thus, what can intuitively be understood by some inverse heap? If natural or real numbers are meant, then

a new imaginary axis is introduced: numbers increase or decrease relative to zero depending on the axis' direction. However, how to deal with heaps, for example, with ordinary ones of form $a \mapsto b$? May perhaps an invertible heap be assigned the inverse of an accompanying predicate? It might not be accurate. May a heap inversion perhaps be assigned the nil denotation? However, this may not be correct since any non-empty heap will, by definition, then be empty. Furthermore, what about inversion of the empty heap? Such a naïve definition is counter-productive since it does not seem to cover all heaps comprehensively. What if sides of heap graph edges flip, e.g. $a \mapsto b$ turns into $b \mapsto a$? This variant would be just an interesting idea but not tractable yet because conjunction does not contradict such a definition. What is needed instead is conjunction yields the empty heap. In such an approach, the left-hand side would be left undefined in the case of an object. It is easy to imagine that joining heaps removes some positive heap if connected with its negative supplement. Thus, inversion means some transcendental removal operation of a heap, and the operator may be applied to any heap, including a complex. $(a \mapsto b)^{-1}$ may denote " a not pointing to b " or better as " a points inversely to b ". The first explanation fails, because "does not point" by mistake might be considered as $a \mapsto c$, where $\exists c \in \Omega, c \neq b$ — this implies vertex a exists and between a and some element whose content differs from b — all this is false because there is no such evidence to trust. Hence, the hypothetical case "inversely points to", namely "inversely has a reference to", requires some deletion regardless of the strange value, which may have allowed a clean deletion of all superfluous elements, which require a further check. At first glance, this looks odd. Until now, only heap parts are specified existing. Inversion changes the rules of the play.

Inversion shall not be mixed up with a heap that may not be in a heap. It would be predicate negation, but heap inversion is an operation — currently, our focus is on eqn.1. The given equation means that for "the negated points-to", $a \not\mapsto b$ holds. — It is a predicate relation between a and b . In generalised form a negated heap H^{-1} , which by default holds: $a \mapsto b \circ a \not\mapsto b = \text{emp}$ and $a \not\mapsto b \circ a \mapsto b = \text{emp}$, and lifted $H \circ H^{-1} = H^{-1} \circ H = \text{emp}$. It implies that $\omega \circ \omega^{-1}$ removes a heap. If needed, the superfluous edge and vertex are removed from the heap graph if no more incoming from or outcoming to edges remain w.r.t. still existing graph vertices. Thus, the given equality about inverse pointers becomes clear. It is not difficult to check the equality $H \circ H^{-1} \circ H \equiv H$. In the example from fig.65, the heap state before inversion is $d \mapsto a \circ a \mapsto b \circ c \mapsto b$, but when inversion $\circ(a \mapsto b)^{-1}$ is applied, this results in $d \mapsto a \circ a \mapsto b \circ c \mapsto b \circ (a \mapsto b)^{-1}$, which equals $d \mapsto a \circ a \mapsto b \circ (a \mapsto b)^{-1} \circ c \mapsto b$ equals $d \mapsto a \circ c \mapsto b$, which is not evident since both pointers do not overlap. So, this calculation is not fully cleaned up and requires further steps to correct superfluous elements. Thus, two

more normalisation steps are needed.

Normalisation – First step: This step is generic. If a bridge exists between the considered heap graphs as the only connection between those, then the operator shall be replaced by disjunction (see later).

As a bridge between a and b is found, \circ is replaced by \parallel in the remaining term. The result may be considered plausible. For completeness, it may become needed vertices must be entirely removed from the corresponding heap graph. This need occurs on object field locations.

Normalisation – Second step: Deleting vertex a can be accomplished when there are no more pointers left to a in the remaining heap.

We apply those two normalisation steps to avoid the mentioned exclusions (cf. generalised heaps with obs.4.13). \square

Remark: Generalised heaps were not discussed. For the soundness proof, it is necessary to show $H \circ H^{-1} \equiv \text{emp}$. The proof can be taken out inductively over \circ by using $(g_1 \circ g_2)^{-1} \equiv g_1^{-1} \circ g_2^{-1}$, s.t. a homomorphism exists for " \cdot^{-1} " relating \circ (see lem.5.13).

Convention 5.12 (Heap Invertibility). Condition (i) implies a partial case $\text{emp} \circ \text{emp}^{-1} \equiv \text{emp}$ because we agree upon $\text{emp}^{-1} \equiv \text{emp}$.

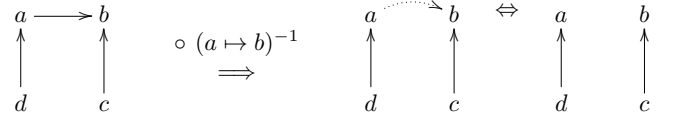


Figure 65: Heap graph before and after inversion

Explanation: $H \circ a \mapsto b \circ (a \mapsto b)^{-1}$ denotes:

- 1) remove edge between a and b
- 2) remove vertex a , if there are no references to it in graph H
- 3) also remove vertex b , if there is no reference to it in graph H

Group properties allow us to establish equalities for heap terms, so improving proof confluency or transformation into normal-form (see thes.5.3). Thus, bloated heap term IR may be reduced. Partial specifications allow a reduced rule notation (see sec.V-E). Further work includes SMT-solver integration for practical heap term simplification. It is required to consider when the content is a pointer again, e.g. $a \mapsto o.f \circ (a \mapsto o.f)^{-1}$, where o denotes an object containing field f . The field $o.f$ is not removed from dynamic memory. Otherwise, object encapsulation will be under threat — further research here is highly appreciated but is beyond this work's scope (see discussion in sec.IV-F). That is why by default, it is agreed upon that any field remains in memory as a unit of some contiguous object memory layout and may point to nil. Thus, all the mentioned steps shall remain without change as is.

Lemma 5.13 (Homomorphism over Simple Heaps). $(g_1 \circ g_2)^{-1} \equiv g_1^{-1} \circ g_2^{-1}$ holds for any non-simple heaps g_1 and g_2 .

Proof. If we succeed in showing the generalised form $G = g_1 \circ g_2 \circ \dots \circ g_n$, then the problem would be solved. For doing so, $G \circ G^{-1} = \text{emp}$ must be shown. This equation may be proven inductively using n . In the base case ($n = 1$), $g_1 \circ g_1^{-1} \equiv \text{emp}$. It holds because an inverse element must exist. For the inductive case, we assume

$$G = \underbrace{(g_1 \circ g_2 \circ \dots \circ g_k)}_{G_k} \circ g_{k+1}$$

Then for

$$G \circ G^{-1} = (G_k \circ g_{k+1}) \circ (G_k \circ g_{k+1})^{-1}$$

, the inverse part of the heap is a natural extension of the heap. The first part of equality holds

$$\underbrace{G_k \circ G_k^{-1}}_{\text{emp}} \circ \underbrace{g_{k+1} \circ g_{k+1}^{-1}}_{\text{emp}} \equiv \text{emp}$$

because of the inductive property of inversion, obeying conv.5.12. \square

Definition 5.14 (Heap Disjunction). Heap disjunction $H \parallel a \mapsto b$ denotes a heap H , and some simple heap $a \mapsto b$, which does not overlap. If G_H is some heap graph H , then $G_H = (V, E)$, for all edges $(_, a) \notin E$ and there is no path from any location of b to H , and there is no inverse path from H back to a . " $_$ " denotes some variable term placeholder.

Thus, $x.b \parallel x.c$ does not hold for any x with fields b and c if at least one common vertex exists for any path from $x.b$ or $x.c$.

Assume, $\Sigma = X_0 \parallel X_1 \parallel \dots \parallel X_n$ where $n > 0$ and X_j has form $x_j \mapsto y_j$, then $\Sigma = \Sigma_0 \parallel a_0 \mapsto b_0 \Leftrightarrow \forall (a_j \mapsto b_j) \in \Sigma_0 : a_j \neq a_0 \wedge b_j \neq b_0$.

Lemma 5.15 (Monoid over Disjunction). $G = (\Omega, \parallel)$ is a monoid and group, if Ω is a set of heap graphs and \parallel denotes heap disjunction.

Proof. In analogy to lem.5.10, $\forall m_1, m_2 \in \Omega : m_1 \parallel m_2$ holds when m_1 and m_2 do not share a common vertex because when there is no path from m_1 to m_2 , and there is no graph surrounding both m_1 and m_2 . If m_1 and m_2 differ, then $m_1 \parallel m_2$ again is a valid heap in Ω , because m_1 is from another part of the heap graph than m_2 is, and vice versa. Hence closure follows. Associativity follows for apparent reasons. emp may serve as a neutral element, then $\text{emp} \parallel m_1 = m_1 \parallel \text{emp} = m_1$. Let by default $\text{emp} \parallel \text{emp} = \text{emp}$ hold. Finally, it is agreed upon $s \parallel s^{-1} = s^{-1} \parallel s = \text{emp}$, which is similar to \circ . In general, heaps follow this convention. \square

Conjunction and disjunction of heap fragments may be expressed by rules and rules that are dual to those in the following manner:

$$\circ_{[B,C]} \frac{U \circ B \parallel C}{U \circ B \circ C} \qquad \parallel_{[B,C]} \frac{U \circ B \circ C}{U \circ B \parallel C}$$

$$\parallel_{[B,C]}; \circ_{[B,C]}; \parallel_{[B,C]} \equiv \parallel_{[B,C]} \quad (2)$$

$$\circ_{[B,C]}; \parallel_{[B,C]}; \circ_{[B,C]} \equiv \circ_{[B,C]} \quad (3)$$

Operations \parallel and \circ are dual. They may be transformed into each other using the dual operation (see eqn.2 and eqn.3), where ";" denotes the sequential operator. Equalities hold because the operations are self-inverse and because of the provided assertion about the existence of both heap vertices B and C .

Theorem 5.16 (Distributivity). Distributivity holds for $\forall a, b, c \in \Omega$ for \circ and \parallel :

- (i) $a \circ (b \parallel c) = (a \circ b) \parallel (a \circ c)$
- (ii) $(b \parallel c) \circ a = (b \circ a) \parallel (c \circ a)$

Proof. Only (i) has to be shown because (ii) immediately follows from the duality of \circ and \parallel . Two implications show equality (i). " \Rightarrow " means that from $a \circ (b \parallel c)$ follows $(a \circ b) \parallel (a \circ c)$. " \Leftarrow " denotes implication for the opposite direction.

" \Rightarrow ": $b \parallel c$ implies no connections between b and c exist. Thus, $a \circ (b \parallel c)$ means either between a and $b \parallel c$ there is also no connection, which eventually leads to false, or one connecting vertex exists, and by default, it must be in b or c . W.l.o.g. a connecting vertex in b is assumed, then $a \circ b$ holds. The analogous may follow from c . Regardless of which, but one graph is to be extended: b or c . Other graphs do not extend. Thus, the second graph is always false.

" \Leftarrow ": Either $a \circ b$ or $a \circ c$, both equal to false due to def.5.7, because a may not connect to b and c at the same time, otherwise it would contradict def.5.14. W.l.o.g. it may be stated that if $a \circ b$ equals true, then $a \circ (b \parallel c)$ would be too. \square

Remark: Since the neutral element for both operations \circ and \parallel is emp , there is no way to define an (algebraic) field (e.g. a Galois field) over these operations since lem.5.10, lem.5.11 and lem.5.16 hold and regardless of the fact the carrier set Ω is finite. Hence, any finite heap and all operations defined over it are also generating a finite heap.

Remark: In analogy to logical conjuncts \wedge and \vee , a normalised form using \parallel always exists. Previously mentioned equalities and lem.5.13 can achieve this in order to invert a generalised heap.

It is necessary to hoist \parallel as far out as possible by either applying distributivity rules or reordering non-complex heaps to shrink a heap graph. So, the left-hand sides of pointers are sorted ascending by their location in lexicographical order. The idea is to cut redundant

searches, e.g. for stepwise verification, s.t. only changing heap parts are re-calculated.

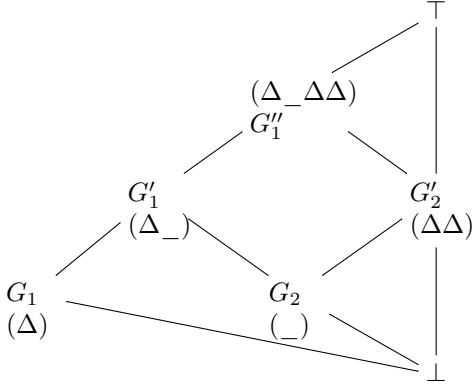


Figure 66: Poset over heap graph inclusion

A poset may be established over heap graphs and set-inclusion as lattice join operator \circ . The infimum (\perp) is the empty heap. It is the least bound. The least (upper) bound is the full graph (\top). For example, absorption does not hold for heaps. So, the poset may not be a complete lattice. Fig.66 the poset G contains $\{G_1, G_2, G'_1, G'_2, G''_1\}$, which hold the following inequalities in ascending ordering $G_1 \sqsubseteq G'_1 \sqsubseteq G''_1$, $G_2 \sqsubseteq G'_1$ and $G_2 \sqsubseteq G'_2 \sqsubseteq G''_1$. The heaps \perp and \top are always there and may always be added if not present. Hence, these may sometimes not be explicitly mentioned. G''_1 is the supremum, and $\inf(G) = \underline{emp}$ is infimum, where \sqsubseteq defines the subset relation over graphs. It is not difficult to realise two not connected heaps having no common vertex under conjunction (so are equal \underline{emp} due to def.5.7) always remain unconnected according to the Hasse-diagram. Thus, a merge is always *true* because either (first contradiction) $a \mapsto b \circ a \mapsto d$ cannot be implied from the first conjunction or any other complex heap. Because of (the second contradiction), $a \mapsto b \parallel b \mapsto d$ contradicts the definition of \parallel . However, it is essential to notice a poset's ordering may be violated after introducing heap inversion (see earlier) if using inversion unbound. Currently, inversion satisfies our needs w.r.t. a more comfortable heap comparison, particularly for the specification to be checked, therefore the locality property from sec.III remains unchanged.

D. Class Object as Heap

Let us consider how class objects are modelled in the heap graph according to fig.67. In fig.67 a), there is a separate assignment presented for an existing graph (without details). The object in the rectangle refers to a particular object instance. In fig.67 b), only the second field of the object instance is assigned to some compatible value. All remaining fields are assigned nil. Fig.67 c) and fig.67 d) have the same meaning as in b), except assignment is performed on all fields. Following up, we

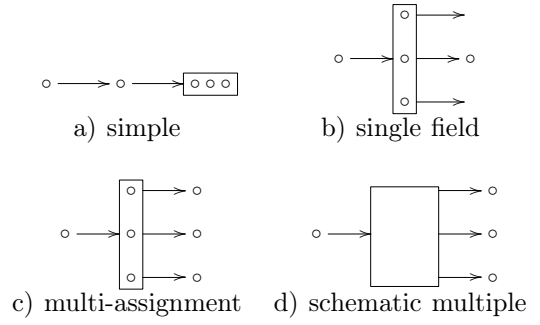


Figure 67: Shapes of object assignments

introduce additional restriction w.l.o.g. for better reuse of operators still to be defined:

Convention 5.17 (Modelling of Object Instances). Object instances are modelled w.l.o.g. as

- There are no inner objects. Inner objects may always be modelled equivalently to separate objects associated with an externalised object [48]. References are only allowed to those objects that are replaced by non-overlapping. Hence, w.l.o.g. union are excluded from modelling objects since they do not increase expressibility.
- Object fields differ and may be used by further objects and be defined in inherited classes. In the case of name clashing amongst the class inheritance hierarchy, clashing classes closer to a common superclass may be renamed, s.t. all references to the problematic reference may be renamed.
- Due to closure during their life-time, objects do not grow, except cases where the pointer casts to a new object of a differing (sub-)class. The problem of memory fragmentation may only arise where memory is limited. It may be worth transforming dynamically allocated objects into automatically managed ones to avoid fragmentation with reasonable efforts in this context since a stack frame dynamically grows when an additional block guards objects.

Due to inheritance, objects may only monotonously grow according to the $<$: relationship from fig.20 (when intentionally disobeying enhanced class visibility modes, as it was defined in C++, for instance). Consequently, regions in memory layouts may only grow. An increase may lead to severe problems, whose solution may involve utilisation and renewed memory allocation but with different addresses. In general, this problem is not decidable because of the Halting problem. However, if the problem on maximum limits may statically be resolved just in particular cases, an improved variant may be chosen. In reality, object fields may also vanish due to visibility and class inheritance. Therefore a monotony of object fields is only a heuristic, where a fixed class size may

be a reasonable estimate when late object binding is prohibited. Assigning arbitrary objects of a (sub-)class is prohibited. Since Burstall’s separating heaps [51] do not obey compactness, object fields may not occur more than once in one conjunction in a heap expression as (left-hand side) location.

- d) Arrays as base type is prohibited. The heap graph must remain simple. However, this does not prohibit an arbitrary number of pointers pointing to a particular address.
- e) Common heap graph vertices may be complex. W.l.o.g. attributes of APs may be generalised.

In order to avoid contradictions in the following definitions, two steps are needed. First, to be able to check relations between two vertices real quick. A given non-empty complex heap contains one or more simple heaps. To check whether two heap graph vertices are connected, it is required to check all left sides of simple conjuncts in the worst case, so a full edge-scan is required.

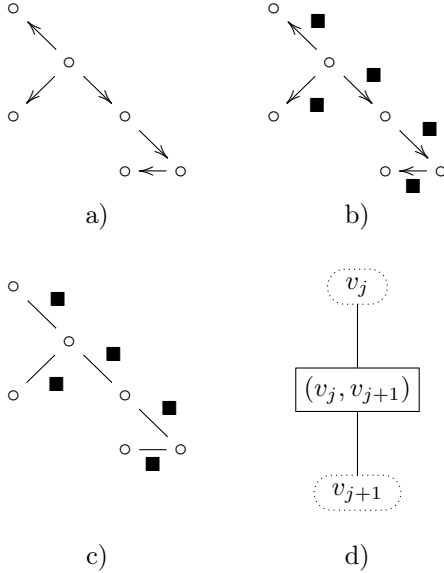


Figure 68: Transformation of schematic heap graph

Second, to obtain all neighbouring vertices for a given vertex, a model is beneficial that is quickly traversed by vertices and not by edges. For a quick but accurate definition of neighbours, e.g. $\text{reaches}(x,y)$, $\text{reaches}(x,Y)$, $\text{reaches}(X,y)$, $\text{reaches}(X,Y)$ is proposed, where x denotes a well-defined vertex, and X denotes a vertex (sub-)set (to y and Y in the analogy). The model based on vertices is illustrated in fig.68. Small opaque squares accordingly allow gaining a more effective iteration as described. Both models, where a) is vertex-based and b) is edge-based, are dual, so both w.l.o.g. are interchangeable. Vertex pairs, including source and destination, are encoded over the middle of an edge (see (d)). Then this is interpreted as one vertex with a unified name and is connected to

neighbouring vertices (see fig.68 (a) and (b)). Turning one model to another and vice versa according to the scheme from fig.68 c) is possible without losses, so the mapping between both structures is bijective regardless of the edge directions (see (c)).

Hence, transforming the graph with conjunctions or disjunctions is allowed. It is more convenient for normal-forms and optimisations.

Convention 5.18 (Object Fields). Object fields do not overlap, and field addresses are different (cf. conv.5.9). However, pointers may have aliases. An object’s content may be expressed as $x \mapsto \text{object}(fld_1, fld_2, \dots)$. W.l.o.g. by default, object field pointers may not be used as an L-Val [243] in arbitrary arithmetic expressions. It may only be used by locations according to obs.5.9. Late binding is not considered. The lack of late binding means, polymorphism mimicked by subclassing during runtime is absent, implying an additional restriction. However, all accessor fields, including field types, maybe thoroughly analysed statically.

Consequently, whilst static analysis, only the most common class amongst the inheritance hierarchy may be used. The question of which class to use during object instance generate is undecidable in general. The program statement responsible for generation may be accessible or not. To predict it earlier is, in general, not possible. So, only the most common heap can be built whilst verifying.

E. Partial Heap Specification

As mentioned earlier, according to def.3.9, object instances may be interpreted as data containers for each field $\text{obj}.f_1 \mapsto \dots \circ \text{obj}.f_2 \mapsto \dots \circ \text{obj}.f_n \mapsto \dots$. All fields generate some heap slices. In contrast to abstraction, this transformation may be characterised as concretisation. Class object fields have restrictions on naming and types, which both have to match those of the corresponding class. All fields of one object co-exist. Initially, they relate to simple heaps only, which later may be extended by \circ -conjunctions. Object fields may not always be freed one by one (see obs.3.5 and the last discussion). Local object fields must also have the possibility to specify parts, so subclass objects, as do have ordinary local variables in SL-extensions. In analogy to non-object pointers, constant functions over heaps may be defined. For example, $\text{true}(\text{obj})$ or $\text{false}(\text{obj})$ from def.3.10 and def.3.9. In contrast to non-object pointers, $\text{true}(\text{obj})$ introduces some object term as an additional parameter. This way, APs may be used to modularise further a specification, which syntactically and semantically insignificantly differs from the non-object case.

In synchronisation with the proposed $a \circ a$ -solver based on a stack and a stratified AP (see sec.VI), incoming and outgoing terms of APs may be traced and skipped for

redundant or superfluous calculations. The comparison may be made either on the stack for the same levels or by labels between predicates' arbitrary levels using translating rules (cf. sec.VI-E).

Definition 5.19 (Incomplete Predicate). An incomplete predicate is an AP, where the term argument(s) passed if unfolded denote only a partial heap graph, although all remaining fragments are automatically accepted upon heap interpretation. For simplicity, the AP $\underline{true}(obj)$ is considered next. $\underline{true}(obj)$ defines some heap of \circ -conjunctions of all fields of some object obj (includes the empty heap, which represents an empty object).

All directly specified fields are calculated first from the set of remaining fields. Whilst verification, all fields are meant when referring to constant functions, which were not directly specified in a considered AP. More details will follow in sec.VI. It is not hard to agree on the correctness of \wedge, \vee, \neg -conjunctions for $\underline{true}(obj)$ and $\underline{false}(obj)$. These constant functions may accept any number of object fields (see thes.5.3). Its boolean value does not depend on concrete fields. However, compound heaps combined with these may cause unexpected behaviour, which can be excluded during context analysis. Partial specifications, which use constant functions, partially describe fields, but they may cover much more. Although a specification is partial, its denotation includes more heaps (see thes.5.4). Moreover, a calculation may compare given heaps with expected ones, and it can localise heaps that are missing. This shortcut allows determining heaps in the rule set fully.

Example 5.20 (Incomplete Predicate no.1). Given an object a , which has three fields, f_1, g_1 and g_2 . $\mathcal{C}[\cdot]$ denotes a semantic (implicit) function over heap terms of type $ET \rightarrow ET \rightarrow \mathbb{B}$, where ET from def.3.10, \mathbb{B} is the boolean set, where the first extended heap is the expected and the second is the obtained heap, then:

$$\begin{aligned} \mathcal{C}[a.f_1 \mapsto x \circ \underline{true}(a)] &= \mathcal{C}[a.f_1 \circ a.g_1 \circ a.g_2] \\ &= \mathcal{C}[\underline{true}(a) \circ a.f_1 \mapsto x] \neq \mathcal{C}[p(a) \circ a.f_1 \mapsto x] \end{aligned}$$

where p is an AP and denotes $\underline{true}(a)$ (see def.5.19).

However, $\mathcal{C}[a.f_1 \mapsto x \circ p(a)]$ would mean equality because recognition, based on the actual stack window, finds all remaining fields even if several layers of abstracted calls are hidden beneath. $\mathcal{C}[\cdot]$ denotes a homomorphism w.r.t. the discussed constant functions and conjunction \circ .

Example 5.21 (Incomplete Predicate no.2). $\mathcal{C}[\underline{true}(a) \circ \underline{true}(a)] = \mathcal{C}[a.f_1 \circ a.g_1 \circ a.g_2] \circ \mathcal{C}[\underline{true}(a)] = \mathcal{C}[a.f_1 \circ a.g_1 \circ a.g_2] \circ \underline{emp}(a)$.

F. Discussion

Two stricter operations replaced one spatial operation. The SL did not change initial properties, except for unbound heap inversion, which was discussed. If replacing \star with \circ in theo.3.6 (for disjunction replace with \parallel),

correctness follows immediately due to the exclusion of axiom no.5 for conjunction because of strengthening \star .

Given a form allowing normalisation of heap terms, then specifiable heaps may now be analysed linearly (cf. sec.V-E). Due to the non-repetitiveness of simple heaps, complicated heaps may effectively be excluded by applying memoisation. In practice, repeating locations must be localised and excluded (potentially with differing syntactic but semantically equal expressions), as was mentioned in sec.V-C. Otherwise, heaps and heap graph contradicts as well as SL-properties may be infringed. The essential principle of non-repetitiveness must be obeyed. A simple heap specifies one time only. If principles are not correctly obeyed, then applying rules may lead to incorrectness.

Consequently, from a wrong precondition, any result may be derived, including the correct one. Hence, repeating heaps must be excluded. However, this problem may be resolved without running the program (just the verifier is sufficient). APs may be interpreted procedurally (see sec.VI). Consequently, a stack architecture is used for its analysis (cf. sec.IV). Its semantics is very close to Warren's [266] operational semantics, except for parameters by call. The minor modification of WAM may be applied to AP interpretation using strengthened conjunction and disjunction. For instance, this allows recognising $\forall a \in \Omega. a \circ a$ to check whether non-repetitiveness is obeyed. The memoiser can only cache those calls of APs that do not alter the global calculation state. The memoiser can recall (i) incoming or (ii) outcoming or (iii) both incoming and outcoming variable terms at the same time. If further unbound symbols inside an AP by some later subgoal are restricted, this must be considered in the order of subgoals (definition must follow the LR order, see sec.VI).

Prolog [248] as a general-purpose logic PL may be used (see thes.4.11) as a platform based on recursively-defined rules and terms for logical reasoning (cf. sec.IV). It is based on theorems about heap term extension and APs. In Prolog, the well-defined generalised induction scheme after Peano may always be defined as "p(0)." for base cases, and as "p(n):-n1 is n-1, p(n1)." for the inductive cases using auxiliary predicate is for determining n1. It is not hard to see in Prolog any generalised μ -recursive predicate may be expressed. The proof is straightforward, constructive and direct and is not special at all. Hence it is skipped here. In general, predicates do not need to be determined (e.g. when a procedural call does not terminate).

The advantage of Horn-rules is Prolog, in contrast to classic one-way functions as used by [193], can interpret terms as (i), (ii) or even (iii). By doing so, it effectively unions exponential many different classic one-way functions. Not every aspect may be defined. Therefore, function inversion requires further attention. Arithmetical calculations and green and red cuts [248] are possible reasons why a predicate may not be invertible [299]. Invertibility of arithmetic expressions may partially be compensated by replacing natural

numbers with Church-terms (see [299], cf. fig.10). Basic operations over naturals are invertible if only using constants, monad-styled unitary term-constructors and unification is used as its main basic operation. Generally speaking, there must be a strong correlation between input and output terms, becoming an isomorphic mapping between both domains. Moreover, Prolog's cuts may be replaced with w.l.o.g. and expressibility since they are essentially only syntactic sugar (see sec.III).

Expressions in OCL [1] are formalised and kept intentionally close to predicate logic. It supports quantified variables, arrays and ADTs, particularly classes and "ad-hoc" polymorphism by subclassing. OCL allows specifying the life-cycles of objects and their methods. However, OCL apriori does not know about pointers nor aliases. Expressions about pointers are missing. Therefore, UML/OCL may currently not be used to model pointer involvement, e.g. in rapid prototypes, as described in sec.I (see [298], cor.5.5).

Hence, it is proposed that pointers are introduced to OCs, namely into UML/OCL directly. An object state matches how a stack is executed, and heaps are processed, so it fits in the context of the pre-existing object model in UML/OCL. Complex objects have fields of simple or complex type. APs are proposed to be introduced to OCL's logical predicates (see sec.IV). There is no obligation why one predicate describes only a single object. Nevertheless, it is strongly recommended to follow this recommendation. Exceptions may be made when intricate behavioural patterns are described, such as with the Observer design pattern. Spatial relations between objects is described by \circ and \parallel . Relations do not insist on spatial components if clear from the context it is about OCL. Future work may involve the integration of APs into OCL [296]. The begun proposition so far shall be researched further, especially considering conv.5.17 and def.3.10. An expressibility in modularity, increase, and abstraction are expected. A useful review in calculus extensions with pointers may be found in sec.I and [193].

VI. Automated Verification with Predicates

Let us consider a doubly-linked list as an example from Computational Geometry [29]. This list will have for each edge two adjacents for a polyhedron in 2D or 3D space representing a wired mesh. After triangulation, this mesh will consist of triangles. So, each vertex will be connected to precisely two neighbouring vertices. Each edge starts and ends with well-defined vertices. A normal vector is required for visibility and shading calculations of geometric objects. It can be determined by any two edges from any polygon, e.g. a triangle. In a simple heap, the location points to its content. For the example given, this may be vertices or edges. According to the doubly-linked list, each element has pointers forward to the next edge and a pointer back to the previous edge. A simple heap contains edges that are interconnected. Unconnected edges are not specified by default. It is agreed upon that a mandatory absence of heaps is either excluded (see sec.V) or is not considered separately due to Abelian group properties and previously mentioned restrictions. Each time a pointer is dereferenced, copies of all three vertices are allocated to the memory. It is not hard to see this attempt would be pretty inefficient. When working with pointers, this problem is dropped, especially when additional abstraction is introduced. These abstractions, namely APs, allow expressing complicated heaps intuitively. For example, the Prolog subgoal $\text{face}(p1, p2, p3)$ may denote three vertices $p1, p2, p3$, which are connected by a triangle instead of specifying again and again fully $\exists v1.v2.v3$, where $p1.\text{data} \mapsto v1 \star p2.\text{data} \mapsto v2 \star p3.\text{data} \mapsto v3 \star p1.\text{next} \mapsto p2 \star p2.\text{next} \mapsto p3 \star p3.\text{next} \mapsto p1 \star p1.\text{prev} \mapsto p3 \star p3.\text{prev} \mapsto p2 \star p2.\text{prev} \mapsto p1$.

First of all, abstract means generalisation by the introduction of additional parameters. AP here implies a Horn-rule with an arbitrary number of parameters. Some authors tend to use instead "Abstract Predicate" as a new term as by [195]. Abstraction does neither require a new definition (see sec.III) nor the introduction of a new concept because, in both cases, it is already there — the same counts for predicates. Well understood concepts as abstraction and predicates do not require new definitions, mostly since predicates' parameterisation is already covered by predicate logic. That is why "abstract" is an adjective to (genuine logical) predicates. Essentially, an abstract predicate does not differ from a predicate since there is not a single semantic justification for distinguishing from a predicate, especially not after applying Prolog-dialect to reasoning over heaps. An AP has an arbitrary number (including nil) of term parameters and may contain an arbitrary number (including nil) of subgoals to built-in or previously declared predicates. In the given example $\text{face}(p1, p2, p3)$ equals the unfold \star -formula of subgoals mentioned earlier. Depending on which state of calculation the subgoal face is, it may either fold or unfold. The predicate face may depend on further predicates. However,

currently, insufficient information is available on when to fold or unfold the AP definition. If unfolding fails, then this might be because it is impossible to do so in general or because unfold and fold were performed at the wrong time or in a wrong order. Next, a new approach is considered, which allows us to resolve this issue with heaps automatically.

Warren [266] uses the term "programming by proving" to emphasise Prolog as a PL that might be used to find a solution for a problem formulated as Horn-rules. The isomorphism by Curry-Howard [179] states there is a dependency between proof and programming. W.r.t. heaps, the philosophical motto behind might be characterised as "proving is a syntax problem", which means that syntactic analysis may prove the soundness of a specifiable heap and heap representation is close to programming models – in fact to Prolog's rules. The major clue in this section is that APs describe a formal language (see thes.4.11). Later we will see that the formal language is a logical dialect. Consequently, problems with the heap, which by its nature are mostly semantical, may be resolved by syntactic methods and recognition.

A. Fold and Unfold

The approach presented in this section heavily deviates from existing traditionalistic ones.

According to Reynolds [224], [193], the spatial operator \star conjuncts two separated heaps. By doing so, the properties of the underpinning substructural logic remain, and the thinning rule does not hold. Sec.III shows the classic operator \star is ambiguous. That is why in the following, only the stricter conjunction operator \circ is meant to replace its spatial predecessor predicate.

APs are used by the user having the specification role the same way as proposed by Verifast [124]. The conclusion may be achieved faster by tactics, which may be defined inductively in the verifier Coq [32] and is derived in a semi-automated manner. Systems are based on the fold/unfold principle, which first was proposed by Hutton [122]. Hutton's approach would fully automate if a complete proof hint list were provided. Proof hints indicate which redex shall be used next to get a proof finished and finished quickly.

Prolog is used as assertion language. [144] illustratively demonstrates the essence use of Horn-rules as a concrete instance of formulae in predicate logic. [144] proposed Prolog to be used as a PL, which, unfortunately, is not always possible due to computability (see sec.IV). [266] contains a logical reasoning implementation based on operational semantics. Kallmeyer [131] demonstrates Prolog as a recogniser of morphemes and a so-called grammar mutation by the example of some natural languages. Notably, adjoint trees are proposed as a processing technique in natural languages based on explicitly defined λ -terms, which do not occur in formal languages, particularly in PLs avoiding default ambiguities. Examples

show overloading and having difficulties in the analysis is due to the exponential growth of required checks of side-effects. [168] shows in examples of how Prolog might help to resolve ambiguity problems using syntactic analysis. Matthews widely uses recursively-descendent recognisers, which work on trees and are implemented very effectively and simple in Prolog. The implementations base on stack automata recognising LL(k)-grammars with modifications: finite states are explicitly defined, and the stack mimics recursive Prolog rules. Matthews uses difference lists to implement regular languages based on an automaton of partially derived regular expressions [50]. Brzozowski proposes Prolog's formal grammar utility DCG and built-in subgoals to Prolog for updating knowledge bases he believes shall be extended. His approach is bound to regular expressibility (cf. sec.III). Pereira's contribution [201] may be assessed as a classic on Prolog and natural language processing. However, there are no apparent limitations. These include certain unsupported pattern sets and diverging examples, but those can easily be bypassed. For example, this refers to the inability to effectively resolve left-recursion in given Horn-rules since LL(1)-recognisers cannot recognise all predecessor tokens to determine which rule was applied. Furthermore, Pereira proposes λ -calculi over trees in order to recognise natural languages. Thus, morphemes and lexemes are linked and get a dependent denotation by introduced parameters. Next, we introduce the first prototypical heap definition obeying def.1.8 and sec.III, which can immediately be defined in Prolog.

B. Predicate Extension

Definition 6.1 (Heap Assertion). A heap assertion H is inductively defined as

$$H ::= \text{emp} \mid \text{true} \mid \text{false} \mid x \mapsto E \mid H \star H \\ \mid H \wedge H \mid H \vee H \mid \neg H \mid \exists x.H \mid a(\vec{\alpha})$$

Assertion *emp* denotes an empty heap, which is true if the passed heap is empty (cf. sec.III-B). Empty heap behaves neutral towards spatial conjunctions (see sec.III, sec.V). The operator \star separates two heaps into two independent heaps. For the sake of simplicity, this section does not stress the specific strictness w.r.t. \circ or \circ (see sec.V), although it shall be taken into account. However, stricter operations shall always be preferred over \star . Assertion *true* denotes any heap (including empty) is accepted, where false always fails regardless of which heap is about to be passed for interpretation. These definitions are close to Reynolds' [224]. Reynolds' foundation to all definitions is the ordinary (simple) heap: $x \mapsto E$, where x denotes some location (e.g. object field accessor *o1.field1*), and E is some valid expression that is assigned to a memory cell at location x .

Type checking is done at an earlier stage (see [298]). Currently, it does not matter whether an immediate value or a pointer to some memory cell is in memory (see [51]).

Let us consider two arbitrary compound heaps in Prolog as depicted in fig.69.

```
p2(X,Y):-pointsto(loc2,X),pointsto(loc3,Y).
p1(X,Y):-pointsto(loc1,val1),p2(X,Y).
```

Figure 69: Example of compound heaps

Here $p2$ denotes some predicate with two symbols X and Y , representing some value pointed by locations $loc2$ and $loc3$. In contrast to this, $p1$ is defined by predicate $p2$. As we call $p2$ with two syntactically correct arguments, we obtain the $a(\vec{\alpha})$ form.

An interpretation of a heap formula H for a given heap denotes a mapping of two heaps, namely the calculated and the expected heap, onto the boolean co-domain. It means, if two given heaps are equal, then interpretation succeeds. Otherwise, it fails. Only deductively obtained conclusions are considered for a given (heap) interpretation (see sec.I-A1 and sec.I-A2). A search for a logical conclusion succeeds when a query succeeds. In all other cases, it fails. Without any doubt, this is what is expected to obtain from the expected behaviour (see thes.4.5). For simplicity, it is agreed upon that the heap formulae must be canonised by lexicographical ordering to

$$a_0 \star a_1 \star \dots \star a_n \equiv \prod_{\forall j}^n a_j, n \geq 0$$

The \wedge and \vee -connected heap graphs are noted in Prolog as queries in the form $s_j, s_{j+1}, \dots, s_{j+k}$. Alternatively, disjunctions of Prolog subgoals may be split into alternatives whose heads differ from each other using the operator ";". Assertion negation is considered predicate negation. In general, sequence negation does not mean predicate negation. Double negation, in general, does not hold w.r.t. subgoals, especially not when a predicate is not defined totally. Existential variables may be introduced at any place in Prolog rules. However, it is expected that all introduced variables are bound and used.

The constant functions *true* and *false* are syntactic sugar since these may be rewritten by other rules specifying concrete heaps that would qualify. However, constant functions simplify specifications towards any matching heaps. *true* may be replaced by boolean truth. *false* may be replaced by boolean contradiction.

Corollary 6.2 (Heap Soundness). Any syntactically correct heap formula describes a corresponding heap graph. Moreover, any heap graph may be represented by a corresponding heap formula. In general, both sides hold, except infinite heaps, which intentionally are not considered.

Proof. Soundness holds, except APs (see later). Def.6.1 may be applied to theo.3.6, def.3.7 and in consequence to def.3.10. For the sake of simplicity and for historic reasons of publication ordering, here we are assuming \star instead of \circ — as was already mentioned. \square

Definition 6.3 (Informal Heap Graph sketch). A heap graph denotes a connected graph that is directed, simple and resides in the dynamic memory segment. Dynamic regions are allocated and freed by the OS. They can be altered in a program by wrapped special-purpose function calls to some virtual C-library (which is not of interest in this work and therefore not further considered). Graph vertices are pointed by at least one local variable (as a pointer) or are addressable by available locations. Each graph vertex is corresponding to some address inside the dynamic memory segment. The width of each vertex is variable but fix and depends on the pointer type. When one vertex points to another, then both vertices are neighbouring in the corresponding heap graph. If a vertex is associated with two pointers, then the first pointer aliases the second pointer.

Def.6.3 is a specialisation of obs.3.5.

C. Predicates as Logical Rules

APs allow abstraction from simple heaps to complex ones, making them more intuitive. For example, [193] introduces APs, which annotate a given incoming program and are translated together with program statements till assembly output is generated. The presented approach automatically is an attempt to overcome the gap between specification and logical reasoning. Prolog in this section is used as a PL, in which assertions and APs over heaps are specified. However, a semantic mismatch exists between program and specification language: two formalisms exist simultaneously and often two not related implementations using different IRs. Diverging notations and representations are the consequence. PLs may and sometimes even must differ from the exemplary language, e.g. chosen in this work. Following Hoare calculi, logical formulae are described in predicate logic, so in a logical paradigm. Unfortunately, sometimes this is violated (see sec.I), and further restrictions are unavoidable. Thus, for example, variables (objects) are used as locals instead of terms, resulting in many restrictions and workarounds to achieve real-term behaviour. Thus, a specification language, namely its units, are degrading to a statement sequence, and nothing else is left in common with the initial idea of a Hoare calculus. Units would not have anything in common with the declarative-logical paradigm (see obs.4.7, obs.4.9): the calculation state needs to be described referring to symbols and predicates. Symbol and its visibility scope differ from local variables. If symbols are suddenly redefined, then those are not symbols anymore. By definition, a symbol's value is bound exactly once compared to conventional non-constant variables as known from imperative PLs. The difference may not look that big, but this is already a severe unpassable barrier for symbol and predicate definitions. Logical algorithms often (but not always) rely purely on symbols and not on variables. Terms and predicates are vital concepts in

logical reasoning. In both models, heap specification and verification, a minimal Turing-computable subset (cf. PCF [179]) of Prolog (cf. LCF [209], [65]) may be chosen. Verification requires comparing calculation states to decide the proof finished adequately. The heap comparison does not exclude arithmetic expressions, but Hoare's main characteristics remain declarative initially intended (cf. sec.I).

The approach in [27] introduces symbols on heaps but with problematic limitations, e.g. the possibility to describe whole heaps as $X \star Y$ is not foreseen (full restrictions are listed in sec.I). Here, we allow symbols to remain arbitrarily in a logical sense, so as allowed by Prolog (see sec.IV).

When it comes to non-determinism with rule selection, Berdine [27] suggests selecting the longest as a heuristic. We do the same, which is naturally achieved by prioritising rules by their position in a Prolog listing. In general, the search strategy of Prolog is preferred for proves. In cases when a specified depth shall not exceed, branch-and-bound shall be taken into consideration [248], [46] (cf. obs.4.8). WAM [266] is the closest approach to functional or imperative in comparison. When we describe heap state checks, it is easier to refer to facts and rules than program statements or operational semantics (cf. sec.III). The program developer is responsible for a compact programmer, the specifier for facts and rules. The following formalisms help in transforming APs into formal grammar used for further representation. All encountered advantages are characteristic for Prolog and are used further in the method proposed.

Definition 6.4 (Predicate Rule). A predicate rule is defined as $\forall n. a : -q_{k \times n} \Leftrightarrow a : -q_{k,0}, q_{k,1}, \dots, q_{k,n}$ for $k \in \mathbb{N}_0$, where a denotes the predicate head, $q_{i,j}$ denotes some subgoal $\forall i, j$.

It is intentional def.6.4 is close to def.4.2. The first definition is used for descriptions and calls to heap predicates. By default, it is agreed upon a is valid iff all subgoals $q_{k,j}$ in a hold for $0 \leq j \leq n$. The EBNF from fig.70 defines the syntax for the predicate rules. $\langle \text{number} \rangle$ denotes any valid Prolog number, $\langle \text{atom} \rangle$ $'(' \langle \text{arguments} \rangle ')'$ denotes some functor with some simple name $\langle \text{atom} \rangle$ and an arbitrary number of arguments. $\langle \text{var} \rangle$ denotes some symbol variable, which starts with a capital letter, e.g. X . Fig.71 in sec.III, and sec.IV both present an example of the useful functional "map" in Prolog. Using this kind of functionals, together with "fold" and "concat", often allows very compact notations, including recursion-free notations (cf.[299]).

Let a denote some predicate, then its subgoals $q_{k,j}$ are evaluated LR. The symbolic environment σ is updated after each subgoal call inside a predicate's body, according to fig.53. Non-assigned symbols remain but may be assigned after a subgoal. The resulting terms of previous subgoals do not require updates as symbols are assigned compatible

```

(predicate) ::= <head> [ ':' <body> ] ':'
(head) ::= <atom> [ '(' <arguments> ')' ]
(body) ::= <sub_goal> { ',' <sub_goal> }*
(sub_goal) ::= '!' | 'fail' | <functor_term> | <term> <rel> <term>
(rel) ::= '=' | '\=' | '<' | '<=' | '>' | '>='
(functor_term) ::= <atom> '(' [ <arguments> ] ')'
(arguments) ::= <term> { ',' <term> }*
(term) ::= <atom> | <var> | <list> | <number> | <functor_term>
(list) ::= '[' <term> ']' | <arguments> ']'

```

Figure 70: EBNF for logical rules

value. The semantics of a predicate call is defined as:

$$C(a)[a(\vec{y}) : -q(\vec{x}_{k,n})_{k \times n}] \sigma = \\ D[q_{k,n}] \sigma(\vec{x}_{k,n}) \circ \dots \circ D[q_{k,1}] \sigma(\vec{x}_{k,1})$$

By default, the term vector \vec{y} may contain common elements with vector $\vec{x}_{k,n}$, $\forall k, n$, and $C[\cdot]$ of type $atom \rightarrow predicate \rightarrow \sigma \rightarrow \sigma$, $D[\cdot]$ has type $subgoal \rightarrow \sigma \rightarrow \sigma$, and σ is of type $term^* \rightarrow term$, where \star denotes Kleene's star [79].

The subgoal $q_{k,j}$ does not necessarily have to define apriori the connected graph. However, if so, then this indicates the heap (sub-)set is fully defined. At least, it is complete regarding the intuitive understand of a data structure. Modularity and "separation of concerns" may always be considered a good virtue of program development. Thus, an AP forces a designer sooner or later to describe a data structure's intention.

Consequently, it may imply that one AP shall correspond to one heap. Next, adding more and more \star -conjuncts, the corresponding heap graph grows continuously. \star -conjuncts build up heaps, possibly connected ones corresponding to APs. When reviewing fold and unfold of APs (in analogy to procedures), it can be noted it has parameters, heap graph vertices to be precise, which may be on both sides, on the callee's side as on the caller's side of a predicate call. Also, vertices may exist, visible only inside a predicate, which may not be used outside (at least not directly).

W.l.o.g. it is agreed upon object access is granted by the functor ".", e.g. $a.b$ (see fig.70) or $oa(object5, fld123)$ [298]. For the sake of demonstration and modularity, it is further agreed upon an object with its fields can be used to predicate parameters as well as part of their subexpressions. The difference between objects and ordinary stack-local parameters is nil. A detailed explanation is given later.

Definition 6.5 (Predicate Rule Set). A predicate rule set (also called "partition" or "family") $\Gamma_a \subseteq \Gamma$ for some predicate named $a \in T$ and $\forall i, j. q_{i,j} \in (T \cup NT)$, where T are terminals, and NT denotes non-terminals (NT), is defined as:

$$\begin{array}{lcl}
\Gamma_a ::= & a : -q_{m \times n} & \\
& a : - & q_{0,0} \quad , \quad q_{0,1} \quad , \quad \dots \quad , \quad q_{0,n} \\
\Leftrightarrow & \vdots & \vdots \quad \quad \quad \ddots \quad \quad \vdots \\
& a : - & q_{m,0} \quad , \quad q_{m,1} \quad , \quad \dots \quad , \quad q_{m,n}
\end{array}$$

If $n = 0$, then a is a fact. Terms may be associated with a (containing symbols, for instance, when $m = 0$, $n > 0$). If $t \in T$, then t is of kind $loc \mapsto val$, otherwise $t \in NT$ denotes a predicate named t in Γ .

By default, it is agreed upon the sequence $q_{k,0}, q_{k,1}, \dots, q_{k,m}$ from $q_{m \times n}$ any line is in canonised form, s.t. for $\exists s \leq m$ non-trivial elements the first s subgoals are positioned, and for all remaining $m - s$ subgoals it is a tautology as subgoal each, whose domain is fully defined as truth (\top). Furthermore, it is agreed upon that

$$\exists k. a : -q_k \preceq a : -q_{k+1}$$

holds, meaning that the predicate listed earlier in Γ_a has higher priority than the priority listed later.

Corollary 6.6 (Predicates Environment). For the predicates environment Γ for a given Prolog program, $\Gamma = \bigcup_{t \in T} \Gamma_t$ holds. All predicates Γ_t , which depend on each other, must be located in a closed section of a predicate $\bar{\Gamma}_t$. $\bar{\Gamma}_t \subseteq \Gamma$ holds.

Proof. The main idea is to show: all dependent $\forall t. \Gamma_t$ are in one partition of the predicate, and all independent partitions are independent of the dependent predicate environments. All predicate environments are located in $\bar{\Gamma}$, including both dependent and independent ones. Predicates Γ_a and Γ_b from non-neighbouring partitions from $\bar{\Gamma}$ can never depend on each other. \square

Remark: Obviously, due to the Halting problem, the predicate call from a partition is, in general, not decidable. Next, the expressibility of predicates is considered.

Remark: Naming clashes in Γ may be dispatched by choosing a proper encoding. The predicate location shall be encoded into the name, for example, the class for which the predicate is foreseen is prefixed, so it becomes possible to distinguish predicates. By default, predicates with equal location are part of the same predicate partition, so there is no more conflict.

Lemma 6.7 (Predicate Completeness regarding Expressibility). APs cover all first-order predicates for describing a heap.

Proof. A complete proof on expressibility of first-order predicates in Prolog is already done. It can be found in [144]. \square

Lemma 6.8 (Higher-order Predicate Expressibility). APs may express second-order and even higher-order.

Proof. First, let us briefly stick to the essence of expressibility of first-order Prolog predicates. Next, we increase

```

map([],P,[]).
map([X|Xs],P,[Y|Ys]) :-
    Goal =.. [P,X,Y],
    call(Goal), map(Xs,P,Ys).

```

Figure 71: Functional map/3

the expressibility level. The higher-order differs from the first-order by further predicates abstraction. So, e.g. a predicate may be used as a logical expression or variable. In Prolog, this may happen during calls using some built-in predicate call, which accepts incoming and outgoing terms, e.g. `pred1(X):-call(pred2,X)`.

Given some predicate P with arguments: list of incoming terms $[X|Xs]$, list of outgoing terms $[Y|Ys]$ and some terms list used for incoming and outgoing terms. W.l.o.g. the last mixed-use term list may be empty for the sake of induction here. The predicate "map" may then be defined as shown in fig.71, which accepts a predicate to each incoming term consecutively in the LR order. Higher-order predicates may be useful in modules and for single compact data structure accessors. For example, class-based objects alter while execution, according to the CFG. Here, even the control may be bidirectionally passed between caller and callee instances, as is the case with most behavioural patterns, e.g. the Observer pattern [136], [146]. The pattern behaviours are very important use-cases that decide usability of proposed heap definitions, as was investigated by [146], [145], [211].

The predicate type of map/3 is

$$list_a \rightarrow (list_a \rightarrow list_b) \rightarrow list_b$$

, so the second incoming type makes a single predicate a a predicate family, which accepts a list of some base type as input, and base type b as output. There is no hint, whether $a = b$ and $a \neq b$. By $list_a$, we denote a dependent Prolog definition of a list whose elements are homogeneous of type a — third-order λ -terms (cf. def.1.9). Thus, recursion may be replaced by the third- and higher-order predicates, for example, by using left folding (`foldl`), which applies some predicate \oplus to a given list of incoming terms to the current intermediate result of the calculation. When starting with the given neutral element,

$$foldl(\oplus :: a \rightarrow b \rightarrow a, \varepsilon :: a, X :: list_b) :: a$$

right-folding works in analogy, starting with the right-hand side and continuing calculation in right-to-left order. "foldl" determines the initial algebra with some initial value ε and carrier set X and binary operation \oplus , which is defined over the same type as ε is and is applied element-wise for each element from X consecutively. The operation \oplus determines the result, which is of the same type as ε . Assume a equals b , and both variable integers and $X = [1, 2, 3]$ are of the kind integer list. Assume

further, the initial value ε equals 7, then foldl calculates $((\varepsilon + 1) + 2) + 3$, which yields 13, which is an integer. As we see later, higher-order predicates are not that useful for heap verification as they are for user-defined limits and predominantly arithmetic lists. It shall be mentioned that higher-order (except parameterised Prolog terms) will explicitly not be considered since they otherwise may not be expressible by some CF-grammar to be parsed. \square

For the sake of completeness of syntactical definitions in fig.70 and the translation (next section), it shall be considered whether transforming Prolog subgoals stepwise using the sequence operator adequately ";" and cut operator "!" is needed. If a predicate's body contains ";", then the whole sequence after ";" shall be turned into a new predicate with the same left-hand side. For instance,

$$b : -a_0, a_1, \dots, a_m; a_{m+1}, \dots, a_n$$

is $\exists m. 0 \leq m \leq n$ divided into

$$b : -a_0, a_1, \dots, a_m. \quad b : -a_{m+1}, \dots, a_n.$$

If in analogy to that "!" occurs in

$$b : -a_0, a_1, \dots, a_m, !, a_{m+1}, \dots, a_n$$

, then a_0, a_1, \dots, a_m may contain alternatives, which will be considered in case of a fail. "!" asserts that if only one subgoal ranging from a_{m+1} to a_n fails, then b completely fails without any further search for alternatives. All alternatives may be left-factorised starting at "!" s.t. other alternatives are excluded. In short, this is the reason why ";" and "!" may be excluded from Prolog w.l.o.g. and expressibility (see obs.4.13). The question of further predicate generalisation is without any doubt exciting, but w.r.t. this work's main objectives will be skipped. Paulson [198] researches generalisation by introducing functionals to abstraction and logical rules (cf. with [206], [170], [106], [80] and the resolution method [286], [288], [103] — which for this work's main objectives are also not further considered). The tactics modules in Coq [32] (cf. sec.I) base on the same principle as [198].

The essence of lem.6.7 and lem.6.8 is arbitrary equality predicates in Prolog that may be expressed without the significant limitations considered in the introductory. Due to higher-order predicates, even explicitly stated (mutual) recursion might be replaced. We do not restrict ourselves and allow μ -recursive predicates for the cost of partial correctness and the uncertainty if predicate interpretation will eventually halt.

Definition 6.9 (Predicate Folding). The unfold and fold of some predicate definition $a(\vec{\alpha})$ for/into some predicate a for the given predicates Γ_a with the actual term denotation $\vec{\alpha}$ and subgoals q_k is defined as follows.

From lem.6.8, we allow Γ_a w.l.o.g. equals $a(\vec{y}) : -q_k$ with $q_k = q_{k,0}(\vec{x}_{k,0}), q_{k,1}(\vec{x}_{k,1}), \dots, q_{k,m}(\vec{x}_{k,m})$. If $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_A)$ and $\vec{y} = (y_0, y_1, \dots, y_A)$, then

$$a(\vec{\alpha}) \Leftrightarrow q_{k,0}(\vec{x}_{k,0}), q_{k,1}(\vec{x}_{k,1}), \dots, q_{k,m}(\vec{x}_{k,m})$$

with:

$$\alpha_0 \approx y_0, \alpha_1 \approx y_1, \dots, \alpha_A \approx y_A.$$

In the " \Rightarrow "-case for the equality from above $a(\vec{\alpha})$, the predicate is unfolded. In the " \Leftarrow "-case, the right-hand side of the predicate definition is folded into a predicate call, namely as a subgoal. \approx denotes term unification. It is required predicates are well-defined in their environment according to cor.6.6.

D. Interpretation of Heap Predicates

The approach proposed in this section is universal though not classic.

- 1) Transforming the input program and annotated assertions into Prolog terms, which then are processed by the heap verification system within Prolog (see fig.59, [298]).
- 2) Definition of APs is lodged into a reserved section of a resulting Prolog listing and IR of the imperative input program in Prolog. The rules are part of the heap interpretation and therefore require syntactical correctness. As point 1, this is analysed in more detail in sec.IV-E.
- 3) Definition of formal grammar for APs. The grammar is passed to a language processor, which generates a concrete syntax analyser on success.
- 4) The use and integration of previously transformed APs into a corresponding syntax analyser enriched by subgoals as translating attributes during the verification phase.

Observation 6.10 (Narrowing down with Formal Languages). Looking at the heap structure, it reminds the definition of a formal language.

A simple heap assertion of kind \mapsto becomes a terminal (see def.6.5). An AP becomes an NT, namely a call. Terminals may be linked consecutively using the binary operator \star , which commutes (see theo.3.6). A terminal denotes a unit of some sub-grammar, which is equivalent to some edge of a heap. Assertions of kind \mapsto may effectively be linked together when left locations are sorted in lexicographical order. Whenever a naming clashes, α -conversion resolves that issue depending on which module the clash occurs, e.g., introducing naming prefixes.

Thesis 6.11 (Syntax Recognition is Proving). The recognition of APs is interpreted as proof.

Proof. Particularly, def.6.20 and def.6.21 allow defining a corresponding syntactic analyser, which is total and terminates according to cor.6.17. The derived "word" (in terms of a formal grammar) contains heap terminals and NTs defined in def.6.19. (see later this section for the constructive part of the proof). \square

Corollary 6.12 (Context-Freeness of Heap Expressions). The family of APs describing a set of rules is CF.

Proof. The left-hand side of the predicate cannot contain by default more than one NT. Terminals are neither allowed. Consequently, only one NT is allowed on the left-hand side. The lack of the requirement, where the right-hand side must strictly be right-recursive, so the absence of a regular grammar with rules of a kind $S \rightarrow aA$, leads to CF-ness. Grammar recognition is allowed, which is equivalent to some bracket grammar [110] (CF-grammars whose rules may be of a kind $S \rightarrow (S)$), namely when $n \in \mathbb{N}_0$ for some terminals a, b, x_0, x_1 and x_2 , which might be \mapsto -assertions, s.t. $x_0 a^n x_1 b^n x_2$ and $x_0 \neq a$, $x_0 \neq x_1$ and $x_1 \neq b$, $b \neq x_2$. If a predicate's head contains arguments, then this situation still does not change the predicates' static dependency. Each predicate partition may be assigned an initial NT. \square

Observation 6.13 (Heap Reduction). The generation of heaps by APs raises the question about abstraction level and checks since a heap is a generated element subject to checks — as being generalised from my research [299].

It implies both the derived and expected heap may contain folded predicate definitions, which may need to unfold for a final decision on equality. After a closer look, one can find this is a bi-directional process. Folded heaps may occur in both heaps. It is essential to notice, this kind of problem can be reduced to Post's Correspondence Problem (PCP) [79], which from its theoretical foundation would not be decidable in general, but in some cases, only it is. Hence, this general problem w.r.t. PCP upon heaps is not being considered further.

Obs.6.10, together with obs.6.13 may, however, be considered as a precursor to this formulation: Given a \star -connected heap. Question: Does it match or not the given heap specification? It may also be valid to ask: Which heap is the closest to the correct one, s.t. specification holds? It must be noted that the answer to this question would eventually answer the problem of generic counter-example generation and minimal correction.

Lemma 6.14 (Heap as Word). The word problem for a partition of APs P is defined as follows. Given $\alpha_1, \alpha_2 \in L(G(P))$, is then $\alpha_1 \equiv \alpha_2$ decidable whenever α_1 derives $\exists \alpha_3$, and α_2 derives α_3 too (cf. fig.7), where $G(P)$ denotes a formal CF grammar obtained from predicate partition P .

Proof. Here $\alpha = (a + A)^*$, $a \in T$, $A \in NT$, α is a sentence (cf. def.6.19). T denotes the set of terminals, which are parameterised and noted as units of pairs with both sides' content of corresponding \mapsto -assertions. NT denotes the set of NTs, which contains all predicates and syntactically correct input terms, which may be parameterised. The predicate partition P establishes a formal grammar $G(P)$. From thes.6.11 and cor.6.12 follow CF-grammars. This and sentences imply the theorem of some CF-generated

language $L(G(P))$ regarding the generated language is not context-sensitive, as can formally be seen referring to the pumping lemma. The start NT denotes a predicate call from α_1 or α_2 . Initially, it is necessary to calculate and define while analysing the follow-set of terminals $\sigma(\alpha)$, as well as the set of NT beginnings (so-called first-terminal set) $\pi(\alpha)$ must be calculated (see def.6.20, def.6.21). $\sigma(\alpha)$ and $\pi(\alpha)$ are calculated only once for any fixed P . Here it must be noticed that for a given $G(P)$, the initial NT may differ — if the corresponding analyser is flexible enough to support a start change. It essentially depends on the subgoals to be chosen from α_1 and α_2 .

Moreover, one path is searched starting with $\alpha_1 \vdash^* \alpha_2$ and $\alpha_2 \vdash^* \alpha_1$, where \vdash denotes a one-time-only rule application. Only when no path is found from both sides can it be stated that α_1 does not match with α_2 , and vice versa does not hold. It is required to build one path between predicates and accept both starting and intermediate terminals of a kind \mapsto to check whether two (formal) sentences over heaps match. Parameters in terminals and NTs in semantically correct assertions are connected, so there are no unrelated (non-)terminals. Therefore, a parameter is guaranteed to exist, which assigns some value in both α_1 and α_2 . The proposed platform (see sec.IV) promotes additional checks on predicates, if needed, maybe toggled user-defined, for example, checking the presence of specific terminals inside a predicate body. It is better to assume for both α_1 and α_2 some α_3 to which both sentences may derive to, in order to lift terminals and allow abstract sentences, which may contain NTs (def.6.19). Here, α_3 may be abstract again, containing NTs — so, CRT holds for heap words (cf. fig.7). \square

E. Translating Horn Rules

In this section, the translation of APs into rules of an attributed CF-grammar is considered. APs are given as Prolog rules. Before this, it is required to turn ordinary heap assertions of kind $loc \mapsto val$ into tokens. It is a mandatory lexico-analytical step in interpretation taken by Prolog. The use of multi-paradigm programming [81] allows interpreting Prolog rules during execution by different language processors. Thus, the verification process may be initiated, controlled by and terminated by an incoming program. The translation process of Prolog rules into some formal grammar is unexpectedly simple. Prolog is well-known and has a simple syntax and semantics. However, Prolog rules may contain arguments on both sides of ":-" in the rule definition. Parameters and arguments of the grammar to be generated may be modelled w.l.o.g. as formal grammar attributes. Consequently, the translation process $C[\cdot]$ may be characterised by the following definition.

Theorem 6.15 (Transduction into Attributed Grammar). $C[\cdot]$ denotes a semantic transducing function taking APs as input and turning them into an attributed grammar.

Proof. The proof is constructive by providing the actual transducer:

$$\begin{aligned} C[\Box] &= \emptyset \\ C[C_1.C_2] &= C[C_1] \dot{\cup} C[C_2] \\ C[a(\vec{x}) : -q^0(\vec{x}), \dots, q^n(\vec{x})] &= \{a_{\vec{x}} \rightarrow q_{\vec{x}}^0 \dots q_{\vec{x}}^n\} \end{aligned}$$

In contrast to the notations earlier introduced in the following subgoals are used. Now the input vector \vec{x} contains all symbolic variables for a comfortable notation inside each predicate. If some subgoal q_j for $j \geq 0$ does not require all components of \vec{x} , then the subgoal does not need it either. $\dot{\cup}$ is the set union, preserving sequences and duplicates. Both notations are dual and very similar to each other. An AP describes a heap. Thus, $C[\Box]$ transduces a heap, so it interprets some associative heap (see lem.6.14). The transducer $C^{-1}[\Box]$ turns an attributed grammar back to Prolog. \square

Theorem 6.16 (Inverted Transduction from Attributed Grammar). $C^{-1}[\Box]$ denotes a transducer of some attributed grammar as input and a set of APs as output.

Proof. Again the proof is given by a direct transducer definition.

$$\begin{aligned} C^{-1}[\Box] &= \emptyset \\ C^{-1}[C_1.C_2] &= C^{-1}[C_1] \cdot C^{-1}[C_2] \\ C^{-1}[a_{\vec{x}} \rightarrow q_{\vec{x}}^0 \dots q_{\vec{x}}^n] &= \{a(\vec{x}) : -q_0(\vec{x}), \dots, q_n(\vec{x})\} \end{aligned}$$

\square

Corollary 6.17 (Transducer Termination). Both $C[\Box]$ and $C^{-1}[\Box]$ permanently terminate for any incoming well-defined finite vector.

Proof. The proof is relatively simple as infinite cycles are excluded. Both transducers $C[\Box]$ and $C^{-1}[\Box]$, according to theo.6.15 and theo.6.16, scan incoming rules stepwise in LR ordering. Assuming an infinite cycle was in the given rules, e.g. mutual recursion through CF rules was hypothetically allowed, transducers would still terminate because that cycle would only affect the analysis. The start of the predicate partition corresponds 1:1 with the start NT of the corresponding sub-grammar. As APs may have more than one entry point w.r.t. subgoal call, this behaviour may be mimicked to the corresponding formal grammar by selecting an arbitrary defined NT as starting NT. Naturally, rules do not change. A fitting syntax analyser may be used if allowing all NTs from the caller's side, which is the subgoal call level. The selection of the starting NT without the need to rebuild the recogniser from scratch can be observed in specific parsers, e.g. ANTLR. It is observed that many other parsers do not allow to change the NT even when the static rule set does not change. Recognition of different NTs means the recognition of different (sub-)expressions for a given grammar. \square

Soundness and completeness still need to be researched $C[\Box]$ and $C^{-1}[\Box]$.

Corollary 6.18 (Soundness and Completeness of Transductions). $C[\Box]$ and $C^{-1}[\Box]$ are complete and sound.

Proof. Trivially, that $C \circ C^{-1} \circ C \equiv C$ and $C^{-1} \circ C \circ C^{-1} \equiv C^{-1}$ hold by comparing correct definitions. The punchline of sec.VI-B is neither "!" nor ";" as subgoals do not affect expressibility after all. If for any element $C[\Box]$ does not terminate, then the co-domain, too, is not defined. The same affects $C^{-1}[\Box]$ due to cor.6.17. \square

It is not hard to notice that Prolog rules are not the only representation, but it is an IR that is very close to formal grammar. In general imperative PLs supporting procedures may be included based on automated stack execution.

F. Syntax Parsing as Heap Verification

For the sake of a simple and intuitive algorithm understanding, constants from def.6.1 are still considered further. Regarding class objects, the predicate *true* may mean accepting all \mapsto -assertions until some marker, requiring different conventions and depends on a rule. Such a marker would technically represent a safe synchronisation point used in error-production rules in certain parser classes (cf.[110]). The marker would allow proceeding syntax analysis for a derived stream of tokens until it gets stuck due to an invalid or unexpected token sequence. It is assumed, the input word representing the heap is always finite since we are not interested in infinite verification conditions (cf. discussion in sec.I-A2). This assumption is considered fair because memory is finite and linear in address space. Purely hypothetical, the amount of committed unfolds and folds together approximates infinity. Later we show that for $\exists j$ functions, π_j and σ_j are bound by polynomial complexity.

This section further proposes and discusses the basic conventions needed to implement a syntax analyser for heap verification (further considered by LL(k)-analysers by example). A LL(k)-parser is a syntactic analyser that can look up ahead k tokens to resolve the ambiguity.

Parsers other than LL(k)-based fulfilling required interfaces are more than welcome to be used but are unfortunately not considered in this work for simplicity. Those alternative syntax analysers may include, for instance, LALR, SLR, Earley analysers. Jourdan [129] proves the soundness of his LR(1) analyser using Coq. The question of analyser soundness is undoubtedly essential too, but not considered further, because its overall impact here is too small. Next, a sentence is defined as a composition of separate \mapsto -assertions and subgoals as NTs. Second and third, in analogy to LL(k)-analysers, where separate terminals are given as ordinary assertions, the operations "*first*" and "*follow*" are introduced. Fourth, both operations (SHIFT) and (REDUCE) are introduced, s.t. generalised analysers may be defined, presumably with minor modification upon existing wide-spread parsers.

Definition 6.19 (Abstract Sentence). An abstract sentence α is a \star -conjunction of heaps. Simple heaps are noted as $a \mapsto b$, where a is a location and b denotes a value, e.g. an integer or some value, which contains either meaningful (composite) value or nil.

For example,

$$\alpha ::= [\text{pointsto}(x, \text{nil}), \text{pointsto}(y, 1), \text{member}(x, [y])]$$

describes the actual heap state during verification for a given imperative program. \star is replaced in the previous list by a comma. The rule specification may depend on

$$[\text{pointsto}(Y, 1), \text{member}(X, [Y|_]), \text{pointsto}(X, _)].$$

Hence, in order to check an abstract sentence (specification) for a given program (generating the heap), it is needed to compare whether one of both sides is derivable from the other side or not.

An abstract sentence may also contain term unification, e.g. $\text{pointsto}(X, 5), X=Y$. Term unification must be thoroughly checked and separated from both \mapsto -assertions and predicate calls – so, NTs. Unbound term recursion must be limited, so self-application is excluded by definition. Therefore, as stated, self-containing terms must be bound, as they often may occur in definitions in Prolog (see sec.IV-A), where a check for self-containment is absent by default. Analysers that are forced to process unbound terms tend to be incomplete whenever they run into non-termination. It is agreed upon that by default, checks on cycles are done (presumably) during semantic analysis or not at all in order to avoid running into a previously mentioned problem.

Let us consider now the naïve approach for comparing equality of two abstract sentences. Let us consider algo.2. π denotes the function of starting terminals for a given rule set and a given sentence, as defined earlier. The problem with this approach is uncertainty. Uncertainty arises from when and how often shall "unfold" or "fold" be applied. There is always the risk of running into infinity on unfolding or folding. It remains uncertain, especially after finding one (sub-)solution candidate since it is not clear the found solution is optimal indeed – which depends undoubtedly on the given rule set. Let us assume

$$\begin{aligned} \alpha_1 &= [\underbrace{a \mapsto b}_{i_0}, i_1, \dots, i_{m_1}, \underbrace{q_1(x)}_{p_0}], \\ \alpha_2 &= [\dots, \underbrace{a \mapsto b}_{j_3}, \dots, \underbrace{q_1(x)}_{q_7}] \end{aligned}$$

These two heaps shall be compared. The shift operations on terms (SHIFT-TERMS) leads to unifications i_0 and j_3 . The comparison would continue with the remaining terms. First, the reduce operation (REDUCE-PREDS) checks whether predicates are matching and applicable for unfolding. Thus, the first terminal of the predicate may be requested first. The unfolding of $\text{expand}(p_k, \alpha_1)$ replaces

Algorithm 2 Naïve algorithm for equality check of abstract sentences. Input: $\alpha_1 = [i_0, \dots, i_{m_1}, p_0, \dots, p_{n_1}]$, $\alpha_2 = [j_0, \dots, j_{m_2}, q_0, \dots, q_{n_2}]$ with i and j as points-to-terminals and subgoal p and q as NTs. Γ contains all defined predicates. Result: True if α_1 equals α_2 , False otherwise.

```

1: procedure SHIFT-TERMS( $\Gamma, \alpha_1, \alpha_2$ )
2:   for all  $k \in \{0, \dots, m_1\}$  do
3:     if  $\exists l. l \in \{0, \dots, m_2\} \wedge i_k \approx j_l$  then
4:        $\alpha_1 \leftarrow \alpha_1 \setminus i_k$ 
5:        $\alpha_2 \leftarrow \alpha_2 \setminus j_l$ 
6:     end if
7:   end for
8: end procedure

9: procedure REDUCE-PREDS( $\Gamma, \alpha_1, \alpha_2$ )
10:  for all  $k \in [0..n_1]$  do ▷ compare terminals
11:    if  $\exists l. l \in [0..m_2] \wedge j_l \in \pi(p_k)$  then
12:       $\text{expand}(p_k, \alpha_1)$ 
13:    else ▷ reduce in  $\alpha_2$ , if possible
14:      if  $\exists l. l \in [0..n_2] \wedge (\pi(q_l) \cap \pi(p_k) \neq \emptyset)$  then
15:         $\alpha_1 \leftarrow \text{expand}(p_k, \alpha_1)$ 
16:         $\alpha_2 \leftarrow \text{expand}(q_l, \alpha_2)$ 
17:      else ▷ Match
18:        if  $m_1 = m_2 = n_1 = n_2 = 0$  then
19:           $\text{true} \rightarrow \text{Halt!}$ 
20:        else ▷ No match
21:           $\text{false} \rightarrow \text{Halt!}$ 
22:        end if
23:      end if
24:    end if
25:  end for
26: end procedure

```

the subgoal with the body of predicate p_k (see def.6.9 and fig.70) and generates the new abstract sentence α' , which may be described in Prolog as $\text{concat}(\alpha, [i_7, i_8, i_9], \alpha')$ if $q_1(x)$ unfolds to list $[i_7, i_8, i_9]$.

Remark: Notice the remarkable similarity between folds and unfolds, expansion and reduction, template instantiation and schema validation, as well as heap construction and verification.

Definition 6.20 (First-Set of Non-Terminals). The set of starts of NTs (first-set) is defined as a co-domain of the total mapping π of kind $(T \cup NT) \rightarrow 2^T$ for $m \in \mathbb{N}$, s.t. holds

$$\pi(a) ::= \begin{cases} a & \text{if } a \text{ is } X \mapsto Y \text{ or } \Gamma_a ::= a. \\ \bigcup_{0 \leq j \leq n} \pi(q_{j,0}) & \text{if } \Gamma_a ::= a : -q_{m \times n}, n \in \mathbb{N}. \end{cases}$$

Independent from concrete arguments, π defines all terminals, either \mapsto -assertions or the first terminal(s) of some predicate subgoal. It is implied that both subgoal unification and calls to built-in subgoals are filtered and are no further considered during π and σ .

Definition 6.21 (Set of Following Terminals). The set of following terminals (follow-set) $\sigma(t) \subseteq T$ for $t \in (T \cup NT)$ is defined as:

$$\sigma(t) ::= \begin{cases} \bigcup_{i,j} \pi(q_{i,j+1}) & \text{if } t \text{ at } (i, j < n) \text{ in } q_{m \times n} \\ & \wedge 0 \leq i \leq m \\ & \wedge q_{i,j+1} \neq \top \\ & \wedge \exists a. \Gamma_a ::= a : -q_{m \times n} \\ \bigcup_a \sigma(a) & \text{if } t \text{ at } (i, n) \text{ in } q_{m \times n} \\ & \wedge \Gamma_a ::= a : -q_{m \times n} \\ & \wedge \exists b. \Gamma_b ::= b : -q_{m_b \times n_b} \\ & \wedge a \text{ at } (i_b, j_b) \text{ in } q_{m_b \times n_b} \\ \emptyset & \text{otherwise} \end{cases}$$

An informal remark may illustrate the key characteristics better. The set of following terminals defines all terminals that may follow a given actual \mapsto assertion or a given subgoal if some terminal may be the last of a sentence in a rule. According to [110], LL(k)-recognisers may be fully defined based on just π and σ .

Example 6.22 (Rules Ambiguity). Given the production rules $q_1 \rightarrow a$, $q_2 \rightarrow aq_2 \mid q_3b$, $q_3 \rightarrow \varepsilon \mid q_3a$. As can easily be found these rules are ambiguous, because

$$\pi(q_2) = \{a\}, \sigma(a) = \{\varepsilon\} \cup \pi(q_2) \cup \pi(q_3) \cup \sigma(q_3).$$

Example 6.23 (Example for Word Correctness). Given the following finite specification

$$[(loc1, v1), p1(loc1, loc2), (loc2, v2)]$$

as well as the conditional chain fitting to it: $[(loc1, v1), (loc2, v2)]$. The chain is a correct word for the given specification only in case $p1$ generates the empty heap.

If the word that is given is not just a sequence of terminals, but it is some abstracted sentence, so it contains an arbitrary sequence of terminals and one or more NTs, then the comparison problem may arise at different places of the sequence again (cf. validation of semi-structured data [299]). One of these problems described may be the re-calculation of repeating (sub-)heaps and abstract parts of predicates. Thus, it is advantageous when calls to APs are remembered. Since this is about temporary associativity, a memoiser as a software-based cache-system should be a perfect match. In Prolog, seldom can be found in [268] — in it, memoisation is called "tabling". Applying memoisers subgoals may be compared much faster if a matching instance as compared previously. A Prolog-based memoiser would benefit that its size can be diminished significantly since symbols unground to subgoals act as parameters. The tremendous reduction is for the cost of additional unifications per matching subgoal predicate, which in this context pays off rather than reiterating whole sub-proofs. Thus, predicates may

be compared as procedure calls but without inflicting side-effects and without changing the calculation state several times in a row. All term-arguments (possibly unground) need to be stored, presumably in a table, to memoise a predicate.

Predicate negation does not require further discussions for the reasons provided in sec.V-C, sec.V-E, sec.V-F, sec.IV-A, and sec.IV-B.

G. Properties

In fig.72, an example of a heap configuration is shown. Every vertex v_j with $j \neq 2, j \neq 5$ has outgoing edges for class instances having more than one field of type pointer. The configuration consists of 8 triangles, each drawn with solid, dotted and tortuous lines. Between v_0 and v_3 , a line starts in the mid. It ends in M_1 and spans a triangle $\Delta(v_0, M_1, v_1)$. Thus, fig.72 demonstrates a variety of the same structure in dynamic memory using various descriptions. It is assumed that two and more outgoing pointers imply a corresponding number of different fields in the united instance (see sec.III and fig.60). So, vertices may cover the same graphs but with different APs, e.g. triangles, dotted or tortuous lines. All vertices have to be taken into account in different representations — this is a mandatory criterion, but it is not sufficient. The question about equality of two (syntactically) different directed graphs can be reduced to graph isomorphism.

When the input token stream is analysed, the next state of the analyser may be determined using the current token and following tokens as far as it may be necessary to resolve the ambiguity. In the worst case, all or at least many input tokens need to be checked — a decision will eventually be made. This case is when the heap describes an object instance, and bounds need to be determined. If an object were either defined only within the bounds of one predicate, or object fields which are pointers were described by predicates, then this convention would avoid the described problem and would allow generic heap canonisation by predicates. A syntactical analysis obeying this convention is bound by polynomial complexity [110]. In the following, however, a convention-free syntax analysis will be traced. If object boundaries are not considered, then the analysis may become unsound. Namely, it may overlap with other heaps belonging to other object instances. This overlap would

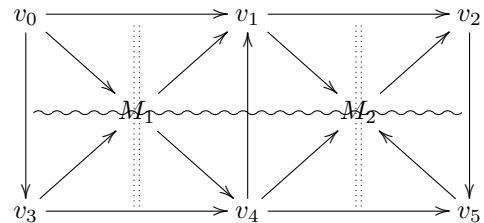


Figure 72: Example of a heap configuration

allow, in practice, partial or parallel analyses of different heaps at the same time – which is believed not to be advantageous after all on the big picture since there may still be many dependencies in between sub-proofs. First, as Was mentioned in the introductory, separability was a hard hinder in any parallelisation attempts – this all is due to tight dependencies, auxiliary definitions and predicate hierarchies and inductive definition dependencies in general as well as local frames. Second, a realistic estimate shall be questioned, as may seem after all doubtful regarding the benefits, if any. Thus, parallelisation is from both theoretical and practical consideration not appropriate, at least not now. In practice, parallel heaps would partially be of interest when separable, and very elementary specifications may only be considered.

Trieber’s stack seems to be the most promising approach in an SL-environment [44], even if it currently fights unsoundness issues. If all predicate partitions may be parsed under the convention mentioned, then analysing \mapsto -assertions are tractable and terminate either with a positive answer or a refusal. On refusal, parsing fails, and either the invalid token or the concrete sentence for a given NT are yielded. The error shows the heap state and explains the difference between the currently calculated and expected heap. Moreover, it is worth mentioning that the confluency of calculations is held while parsing a LL/LR-grammar because the calculation state can be recorded as a tuple (*state*, *word*), and for each state, the transition is determined. This final result is that the main-memory model does not change. However, it is extended by APs instead.

H. Implementation

The system is based on GNU Prolog [83] and implemented using ANTLR version 4 [197]. The work with APs is foreseen [298], [302]. Initially, both contributions are based on Prolog. They were selected for the sake of simplicity and lecturing. For maximum support, implemented packages are based on GNU Prolog-dialect for maximum portability and generic definitions only. For extension and the possibility of supporting numerous software libraries even in different PLs, the multi-target paradigm [81] is applied so that code may be loaded dynamically. Therefore, Denti’s [81] library is chosen, Java-libraries are then loaded as-you-verify. For the sake of simplicity, it is agreed upon that further references to Java are by example. Whenever Java is mentioned in Denti’s library, this implicitly implies any other loadable modules in arbitrary languages that match the interfaces required. Procedures in Java communicate via a Proxy-interface which comes as a Java-class file and can be loaded on a Prolog subgoal. The caller layer “tuProlog” acts as Mediator in the Mediator-pattern as well as Adapter (cf.[136]). Here, call and results may be passed from both sides by implementing the Proxy-pattern, as the remote-procedure call was performed locally in Prolog. This

technique also allows defining new built-in and auxiliary predicates in Java, but visible to the user as Prolog subgoal. Immediate Prolog-defined subgoals are, of course, allowed too. Due to its dynamic context, newly created predicates may call existing predicates and vice versa. So, a subgoal in Prolog remains in full compliance with the principle from fig.53.

The implementation turns an incoming program into an IR, which is a pure Prolog term. Afterwards, assertions are copied one by one to the Prolog theory. APs are turned in a formal ANTLR-grammar as described earlier. Then, syntax analysis is triggered. The generated recogniser is activated after the full ANTLR-grammar is available. The recogniser is generated Java-code, but this is not of primary interest in this work. Afterwards, the process quits, and control is passed to the calling instance back again. If needed, APs may dynamically be checked fully automated to preempt the Prolog core to fail due to syntax and semantic errors, which will eventually be checked. In case of a syntax mismatch, the generated parsing error is issued accordingly.

ANTLR uses two technologies to fight ambiguities in its definitions, “syntactic predicates” and “semantic predicates” [197]. Both terms sound very similar and may accidentally be mixed up with those terms in this work, but this should thoroughly be avoided. Except for these two techniques, as an alternative, there is always the possibility to rewrite Prolog rules, s.t. ambiguity is not emerging, e.g. by factorising rules.

Unfortunately, in practice, ANTLR does not fully cover the class of all LL(k)-recognisers. Predicates are limited and often require a rewriting of (term) rules in case of a conflict. Often ANTLR is not able to distinguish automatically complex expressions, especially not regular expressions.

Consequently, this leads to a full code generation for the needed recogniser. The same problem with limitations of LL(k) is observed in many other compiler-generators (CC), for instance, in YACC or BISON [162]. From a practical standpoint, this means a given grammar is formal and correct, but its recogniser just cannot be built due to some definite limitations that are specific. Luckily, rewriting that grammar often resolves this practical flaw. Involved top-down recognisers often can overcome this problem solely by huge additional memory reserves just for all transitions possible, as BISON does it, for instance, working on the shift-reduce principle, which is very close to the approach proposed earlier in this section. Detailed surveys on syntax recognisers may be found in [291], [110].

An example with required transformations at a proper level shall be shown for processing lexemes and tokens. First, *bar* \mapsto *foo* is transformed into *pt_3bar_3foo*, where the number “3” is either the number of names or some complex expression denoting an integer location required to distinguish consecutive namings. If a location is intricate, e.g. *b.f.g*, then a location together with length

determines the assertion expression in mangled notation (cf.[163]). For example, `pointsto(X,2)` is transformed into the Prolog atom `p_X_2`. The transformation's objective is to obtain a single atomic symbol, representing a simple heap assertion, so a terminal. A terminal may be fully restored to a heap assertion whenever needed. So, all annotated information is available and makes every Prolog atom subject to this encoding unique. These straightforward and backward processes may be implemented as a built-in predicate. Afterwards, they are used either in the essential parts of the verification or other built-in predicates in Java (see prerequisites, see [81]).

Furthermore, the left-hand side of (de-)canonising (in Prolog)

$$p1(X,[X|Y]):-\dots$$

is transformed into

$$p1(X1,X2):-X1=X,X2=[X|Y],\dots$$

The Prolog rule `"p(X,Y):- α ."` may be transformed into the following ANTLR-grammar (rule)

$$p[\text{String } X, \text{String } Y]: \alpha.$$

In this style, all synthesised attributes may be passed top-down. Some predicate `p` may be decorated with inherited attributes. In ANTLR, this can be achieved by adding the keyword "returns", followed by the attribute names before the colon. Thus, once it is clarified which attribute is synthesised and inherited, all attributes need to be included in the corresponding ANTLR-rule accordingly. Rules, conflicts and limitations of Prolog on this topic are almost identical to those from ANTLR.

When APs are turned into some concrete grammar, e.g. an ANTLR-grammar, there are significant problems encountered. Unified terms, \mapsto -assertions (terminals) and NTs are supposed to be transformed according to the provided syntax into grammar together with annotations. ANTLR also allows translating rules, which define a program's semantics and are noted in an ANTLR file definition in curly brackets. The negation of a (sub-)sentence (remember, an arbitrary concatenation of terminals and NTs) may be specified by " \sim " and parentheses, which denote a given regular expression of \mapsto -terminals must or must not follow. Next, elements of the translation grammar are not discussed here because attributes and translating rules may imitate all other expressions and sentences, including a negative match of a predicate (cf.[291], [290], [110], [197], [252], [179]).

User Interface: The graphical user interface (see fig.73) consists of three major parts: (i) the left part, which contains the program listing in a C-dialect, (ii) the right upper part, which displays the state of the current verification, including the dynamic memory and (iii) right lower part which contains IRs of the program in Prolog terms. The memory content and the program IR may be

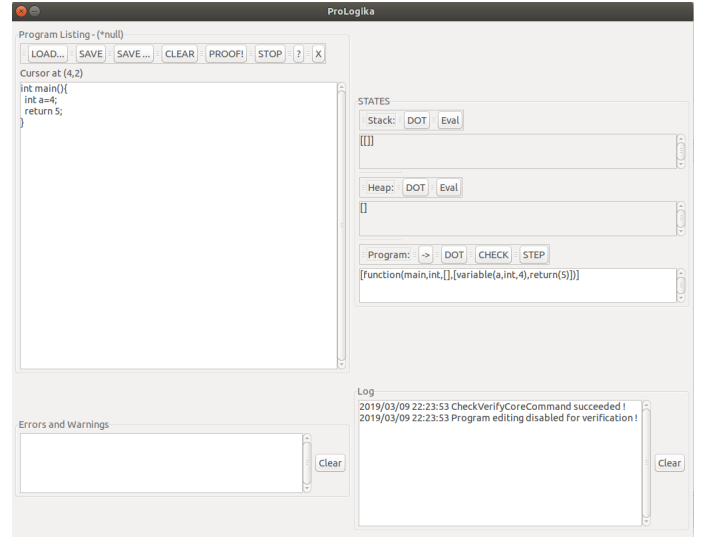


Figure 73: Graphical user interface

turned into a visual IR (and screened as DOT-file). Apart from that, the white section informs about errors and warnings and logs major verification news.

The GUI comes in handy when verifying and running demos. So, automation of transformations, tracing proofs and heap IR may be probed and verification rules, the imperative input program. It appears more effortless if all it needs to reason about a program's properties are nearby.

Use Cases: A programmer can edit a given input program in C-dialect (see fig.74). Numerous checks are implemented, including the syntactic analysis and semantic checks on program IRs, which may also be transformed into DOT (for visualisation only).

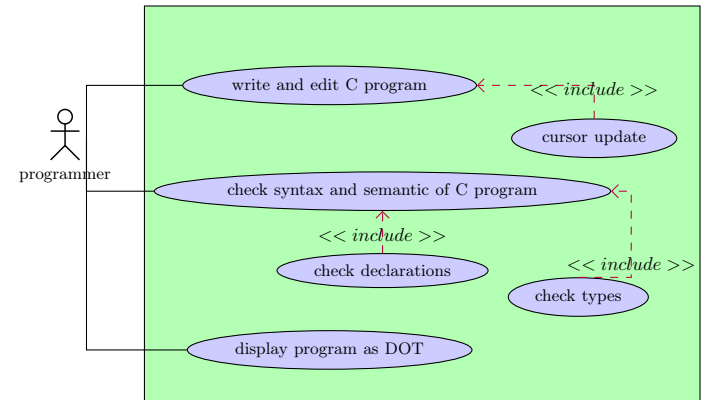


Figure 74: Programmer's view (UML use case)

The role of a typical user who specifies differs from the traditional role a programmer might have (see fig.75). Specifications are very formal logical formulae that catch a program's behaviour. A specification may be added to the system, edited before and after program execution.

When running a specified program, the program is not run. Instead, specifications are checked. In case a problem encounters, it will be placed to the right lower part. Specification checks include pre-and postconditions of procedures, APs, class invariants but may also include a check for rules completeness for some predicate partition. All specification and verification of relevant entities are entirely in Prolog. The current heap state is checked against an explicitly annotated assertion to the program.

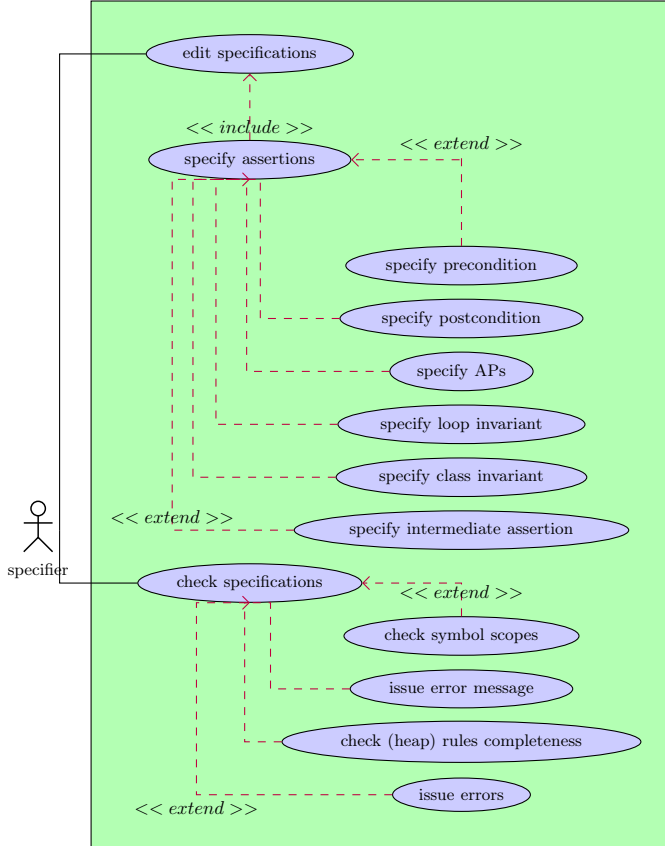


Figure 75: Specifier's view (UML use case)

The essence of heap verification (see fig.76) is the calculation of heap state and checking against explicitly defined assertions by referring to heap specification being annotated to the program. Therefore a verification requires some heap to be normalised and checked if needed. Each of this step can be traced in the GUI parts described. For simplicity and plausibility of the current verification, additional proof tree visualisation elements, generation (derivation) of counter-example, and memoisation of previously run (sub-)proofs for an increased proof are used.

Example 1) Reverse of a single-linked list

Let us assume we are given the list $\{1,2,3\}$, and pointer y pointing to the last element of a linear list. Then list inversion may recursively be defined by splitting off the last element and adding it to the beginning of the remaining list. This algorithm results in the list illustrated

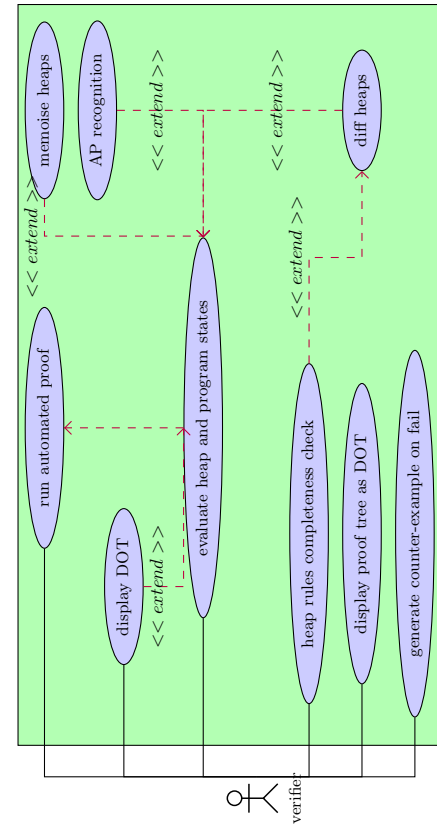


Figure 76: Verifier's view (UML use case)

in fig.77.

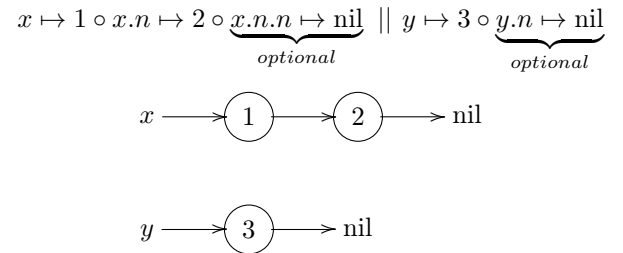


Figure 77: Example of a simply-linked list no.1

Next, its list is retrieved as depicted in fig.78.

Class Definitions: Class instances refer mainly to classes in the sense they are used in C++ or Java, except they only have very rudimentary functionality. Classes have a one-time bound identifier, fields and methods. Fields and methods are defined at most once in arbitrary order, except forwarding declarations which are allowed. Visibility is not mandatory, although allowed, for the universality of the model. Nested methods are prohibited. "this" grants access to fields of a class's instance.

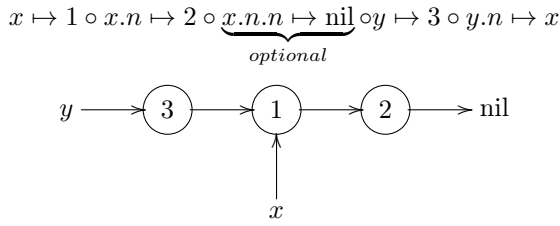


Figure 78: Example of a simply-linked list no.2

$$\begin{aligned} \langle \text{class_definition} \rangle &::= [\langle \text{class_modifier} \rangle] \text{ 'class' } \\ &\quad \langle \text{ID} \rangle \text{ '{' } } \langle \text{class_fields_methods} \rangle \text{ '}' } \\ \langle \text{class_fields_methods} \rangle &::= \{ \quad \langle \text{class_field} \rangle \quad | \\ &\quad \langle \text{class_method} \rangle \}^* \\ \langle \text{class_field} \rangle &::= [\quad \langle \text{class_modifier} \rangle \quad] \\ &\quad \langle \text{variable_declaration} \rangle \text{ ';' } \\ \langle \text{class_method} \rangle &::= [\quad \langle \text{class_modifier} \rangle \quad] \\ &\quad \langle \text{function_definition} \rangle \\ &\quad | [\langle \text{class_modifier} \rangle] \langle \text{function_declaration} \rangle \text{ ';' } \\ \langle \text{class_modifier} \rangle &::= (\text{ 'private' } \mid \text{ 'public' } \mid \text{ 'protected' }) \text{ ':' } \end{aligned}$$

Type declaration mainly follows the ISO-C++ standard recommendation, which allows uninitialised and initialised variables.

$$\langle \text{variable_declaration} \rangle ::= \langle \text{type} \rangle \langle \text{ID} \rangle \{ \text{'}, \langle \text{ID} \rangle \}^* \\ | \langle \text{type} \rangle \langle \text{ID} \rangle \{ \text{'}, \langle \text{ID} \rangle \}^* \text{'='} \langle \text{expression} \rangle$$

Function definitions are straightforward, as known from before C99, so variadic parameters are disallowed. The calling convention follows "cdecl". A return type for some method must be stated as either "void" or any other base type (complex types are currently not supported in the prototype). Object types are scheduled for support in the next future, but all complex modifications are recommended to be passed in function arguments until then.

$$\begin{aligned} \langle \text{function_definition} \rangle &::= \langle \text{function_declaration} \rangle \\ &\quad \langle \text{block} \rangle \\ \langle \text{function_declaration} \rangle &::= \langle \text{type_or_void} \rangle \langle \text{ID} \rangle ' (' \\ &\quad (\langle \text{formal_parameters} \rangle \mid)) ' , \\ \langle \text{type} \rangle &::= \text{'int'} \\ \langle \text{type or void} \rangle &::= \langle \text{type} \rangle \mid \text{'void'} \end{aligned}$$

Built-in Rules for Automated Logical Reason: Heap
normalisation is made by built-in predicates defined in
Prolog or Java.

simplify/2. This predicate accepts some heap term and returns a heap term in which $||$ is utmost outside. It is assumed that for an optimised and further processing, some heap is in $||$ -normal-form, so of kind $q_0||q_1||\dots||q_k$, where $\forall j.q_i$ is of kind $X_i \circ X_{i+1} \circ \dots \circ X_k$.

The "subtract" predicate does subtraction (set comparison). This built-in predicate accepts a list of Prolog terms and creates a list of missing heap terms. The predicate may be used to check a given predicate family is complete or if there are any missing heap terms (e.g. this is important to simplify, transform and process with Hoare triples in general).

Comparison is performed component-wise by selecting two terms: the expected heap term and the calculated.

Layered Verification Architecture: The proposed architecture of this work's verifier called "ProLogika" [306] has six main layers (see fig.79), which on its peripheral cooperates with libraries, for instance, the logical reasoning library "tuProlog" (its short form is "2p"), as well as the CC ANTLR version 4. The system is based on Java. Verification, specification and programs are all in (GNU) Prolog and may be defined and edited in the GUI. ANTLR currently generates Java code, but it may also create code in a different PL, as already mentioned. It shall also be noted that ANTLR may be replaced since the well-defined IR of an incoming input language may also be generated by other CCs. Thus, extensibility and variability principles hold by "ProLogika". Any replacement for ANTLR is fair as long as its recognition capabilities are compatible with the requirements from earlier in this section. Most notably is the ability to parse LL(k) or LR-grammars, select different NTs for a given formal grammar, annotate synthesised and inherited attributes, and process incoming and outgoing attributes as termed string or object expression.

The heap verifier ProLogika consists of internal, output, parsers, prolog, frontend and gui. gui represents the graphical interface and all controls needed. Results, IR, and visualisation are (interactively) communicating with the GUI.

The packages frontend and parsers are tightly coupled. The package frontend contains interfaces and modules of different abstraction level for lexicographical and syntactical analyses. The parameterisation of syntax analysis is one of the basics of verifying APs. The package parsers contain apriori generated lexical and syntactic analysers and analysers to be created whilst verification by need. The interpretation of APs is contained in package ProLogika.internals.ap.

The prolog package enriches the integrated logical reasoning core by additional Prolog predicates, such as heap term processing, failure location and analysis, and implementing intended side-effects, like I/O-operations. The implementation of additional built-in predicates is covered by this design, flexible and easy to extend. Prolog rules may always be added and extended during verification runs.

The package output provides auxiliary functions and predicates for term IR, e.g. for serialisation into DOT-format or formatted console output. Currently, the generation of OCL-code is not implemented yet.

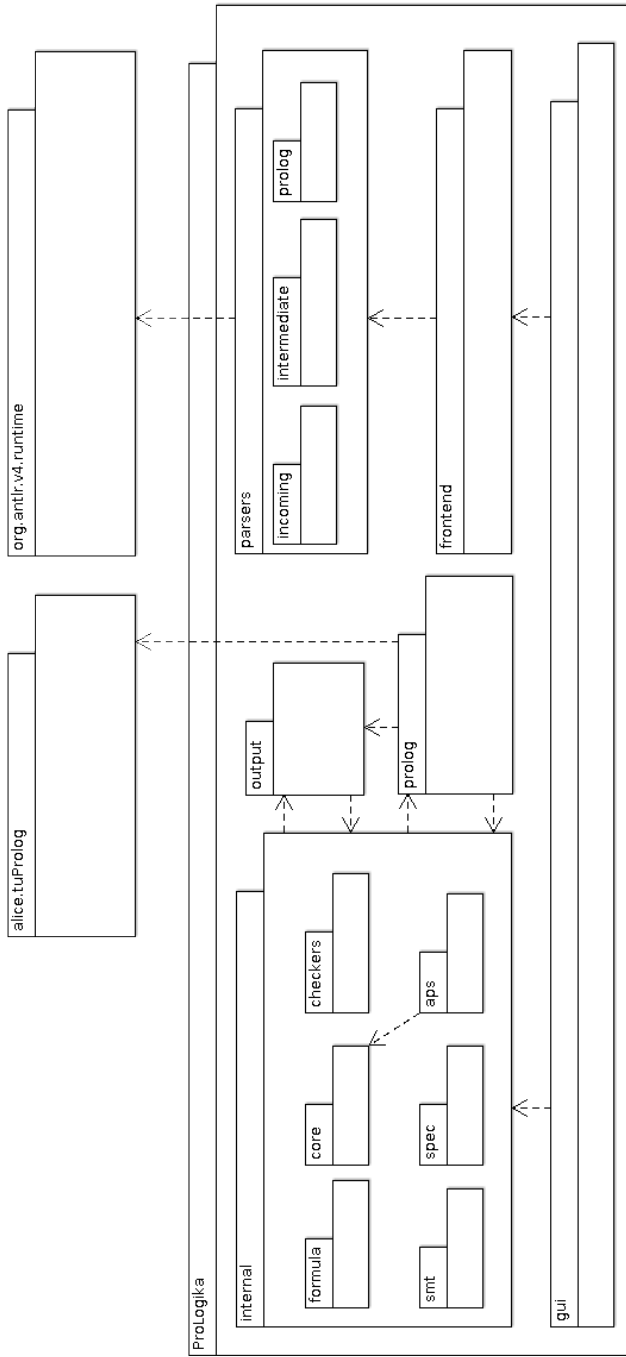


Figure 79: Layered architecture of verifier "ProLogika"

The package "internal" implements specification and verification of related functions. Package "core" contains different modules, which are related to heap term IR processing. Package "aps" relates to APs and contains all compulsory modules

Consequently, it is also related to the package core. Package checkers perform heap checks before, after and during a compound program statement is processed. All remaining packages are subject to permanent corrections and experimental modifications.

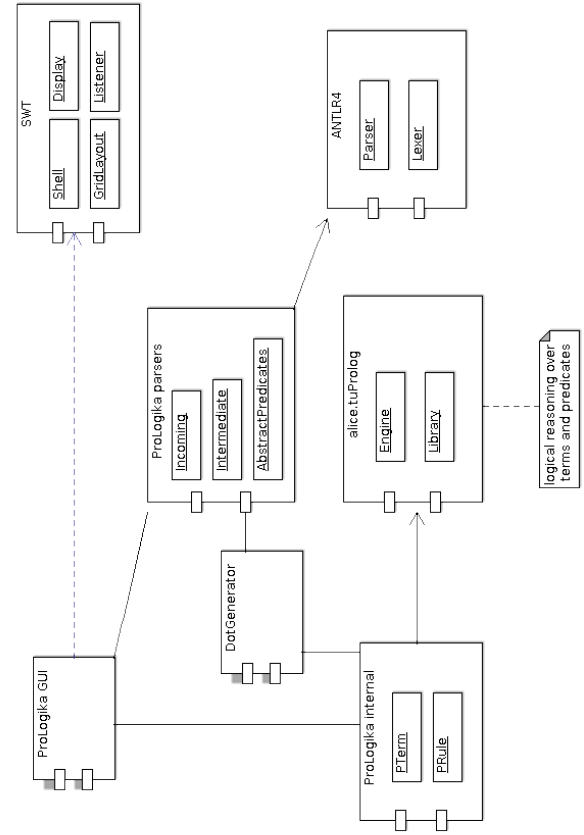


Figure 80: ProLogika components

Components: Following sec.VI-H, six main components can be derived (see fig.80): (i) ProLogika.GUI provides all functionalities with associated visualisation model, view and control, (ii) ProLogika.parsers provide all modules that perform syntax analyses, including constraints checkings on syntax and semantic of generated IR, as well as static checks on APs (all related to packages parsers, incoming, intermediate and AbstractPredicates). (iii) the Java SWT library, which is stubbed into dependent components. It is closely related to ProLogika.GUI and is introduced to dock OS-dependencies. (iv) Package ANTLR already establishes a component for building language processors. Its interfaces are already on a very high abstraction level. Hence, it is taken as is, and no further gapping is required here. (v) Package alice.tuProlog represents a library. Its primary functions are encapsulated on ProLogika's side, especially what is not intuitive with the logical engine initialisation and state transitions. (vi) Package ProLogika.internal represents a component representing Prolog terms (PTerm) and rules (PRule, PSubgoal), which are eagerly used by Prolog's other components.

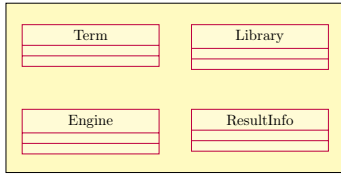


Figure 81: Package alice.tuProlog

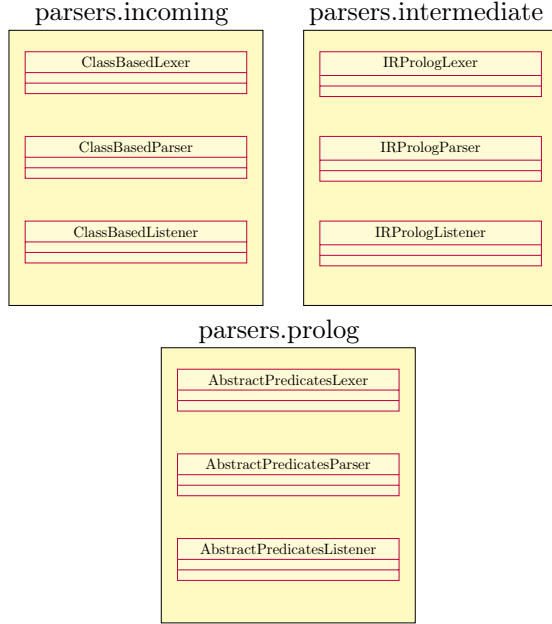


Figure 82: Package parsers

Packages: The package `alice.tuProlog` (see fig.81) contains: (i) class "Term", which represents a common Prolog term that is not abstract, (ii) "Library" is a Prolog-based library, which may contain a whole formal theory build of Prolog rules. "BuiltinLibrary" is a concrete implementation of `tuProlog`'s "Library". "Engine" is a container and controller for invoking logical reasoning based on Horn-based rules and a given formal theory. "ResultInfo" represents the result set as a table that may be accessed in a navigating way (by evaluating subgoals only).

Package `parsers`:

The package `parsers` (see fig.82) contains "incoming", "intermediate", "prolog", and the two classes "MetaType" and "MetaTypeManager". "MetaType" represents the definition of some type in the input program, e.g. class, integer. "MetaTypeManager" is the watchdog instance for all "MetaType" instances derived and referred to during verification.

Package `internal`: The package contains these sub-packages: "core", "checkers", "aps", "spec".

Package `internal.core`:

The package core (see fig.83) contains classes representing the model core for logical reasoning, e.g. terms, rules, symbolic variables, subgoals. Prefix "P" in the class names indicates each class is a Prolog representation. Each of the classes has a Prolog-equivalent, which is strictly ISO-conform.

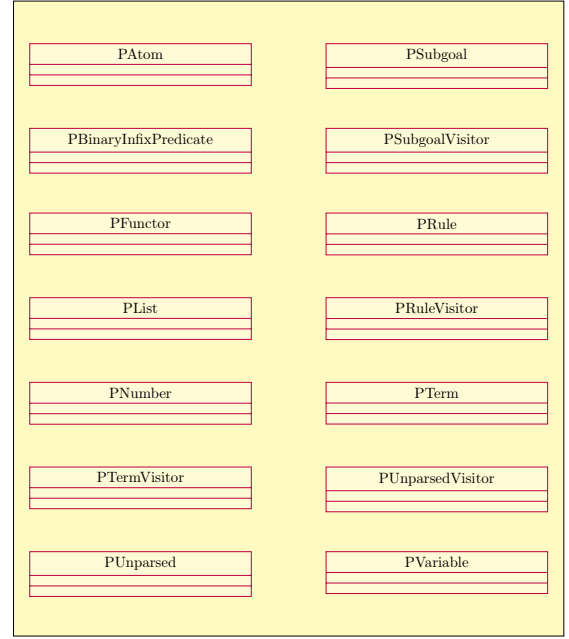


Figure 83: Package core

The main base elements are "PTerm", "PRule" and "PSubgoal". All remaining P-classes correspond to Prolog, except for class "Unparsed", which is a partially calculated Prolog-term. Partially means it contains gaps, filled in later (cf. gaps-concept for logical terms from [294]).

Package `internal.checkers`:

Checks are based on normalisation and subtraction rules, e.g. on APs (APCompletenessChecker, HeapCompletenessChecker, PrologAPsChecker) (see fig.84). Syntactic analyses are performed for some input program and verification conditions (e.g. by ANTLRGrammarChecker). All checks need to implement CheckerInterface.

Package `internal.aps`:

The package "aps" (see fig.85) contains ANTLRBuilder, ANTLRLauncher, GrammarBuilder, and all other AP-processing classes towards a formal attributed grammar (in a sense Knuth and Wagner introduced). ANTLBuilder is a specialisation of the class GrammarBuilder. ANTLR is supposed to represent only as an example a whole class of syntax analysers matching the conditions previously

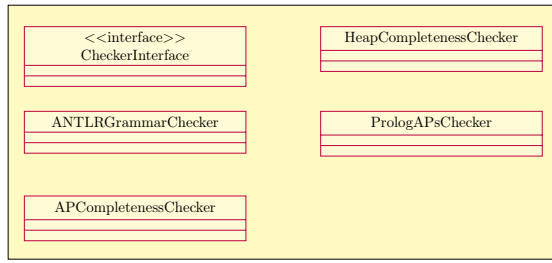


Figure 84: Packages internal.checkers

mentioned. Any other CC and hand-written analysers would be acceptable as long as they implement the standard interface needed.

In analogy to what was said, ANTLRGrammar is a specialisation of class FormalGrammar. ANTLRBuilder is a concrete example for a CC meeting the interface needed. Therefore it can be considered as a promotion for different analysers to be following.

ANTLRLauncher is a driver for the ANTLR-generator (for a fully-fledged ANTLR processor).

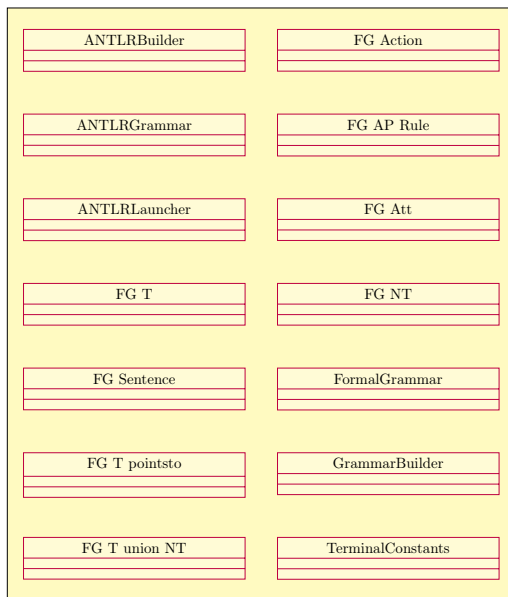


Figure 85: Packages internal.aps

Syntax analysers: Class Main (see fig.86 related to Parser from fig.87 and SyntaxAnalyzer from fig.88) controls three instances of syntax analysers according to the grammars: (1) ClassBased.g4, (2) IRProlog.g4, and (3) AbstractPredicates.g4.

Package frontend: see fig.89.

Remark: IRPrologCommand.execute() returns a IRPrologDescription object. Given the design pattern roles:

ADAPTER::(CLASS) ADAPTER:
SyntaxAnalyzerCommand

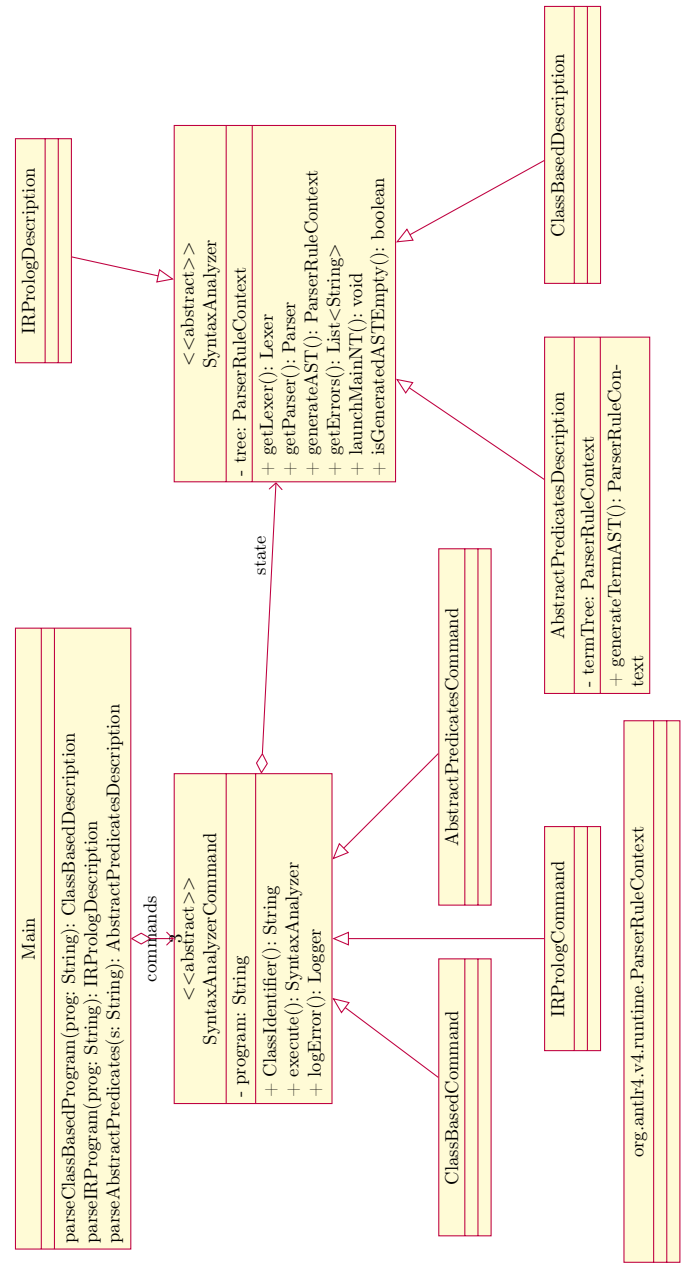


Figure 86: Class Main

ADAPTER::ADAPTEE:

ClassBasedCommand, IRPrologCommand,
AbstractPredicatesCommand

Package parsers.incoming:

The following structure is applicable, not just to parsers.incoming (see fig.90) but also to parsers.intermediate and parsers.prolog. (reduce) classes with Listener-suffixes were introduced to modify syntax analysis when entering and leaving an NT's rule.

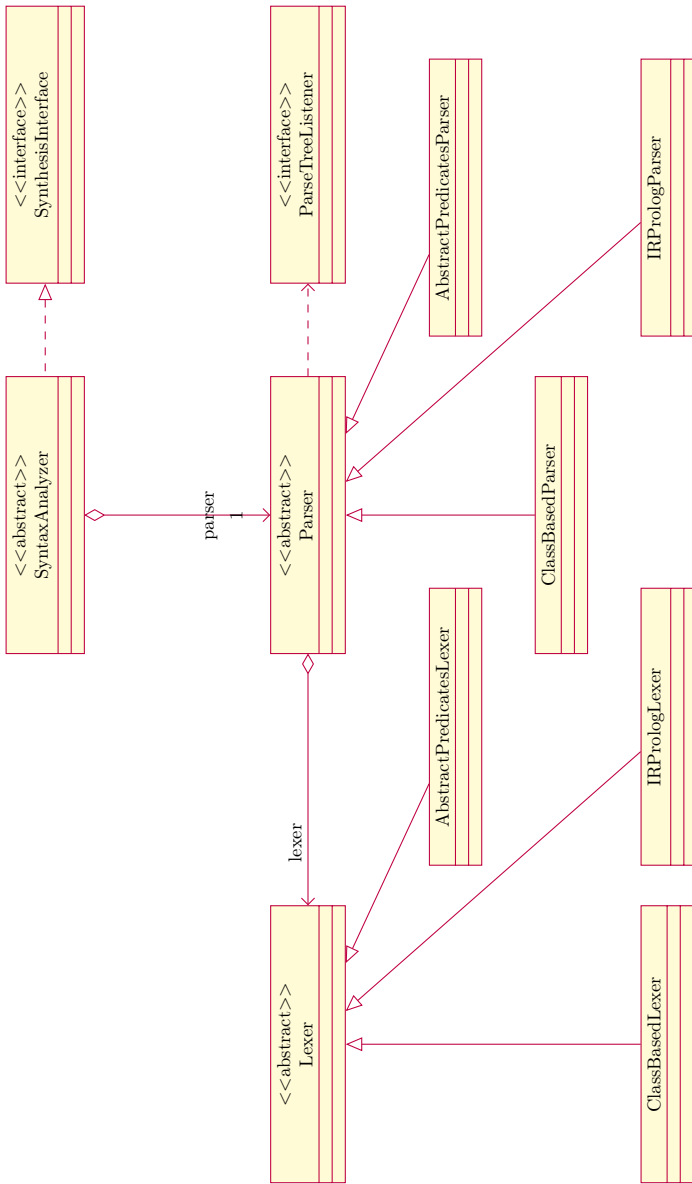


Figure 87: Class Parser

Package parsers: see fig.91.

The class MetaType represents the built-in and user-defined types found before type checking in an input program. Each type, though, is identified by some field, "typeID". However, during type construction, "typeID" is not assigned initially (just the name, but without a full signature, since recursive types are allowed). Statically defined built-in types are "INTTYPE" and "VOIDTYPE".

Elements of package parsers.intermediate act as DIRECTOR for the class "MetaTypeManager".

Package frontend see fig.92.

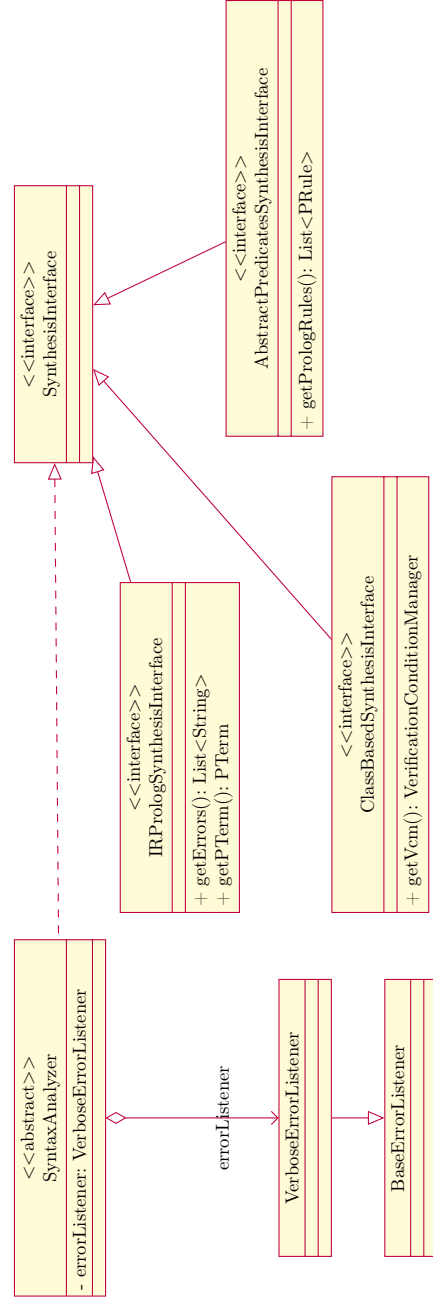


Figure 88: Class SyntaxAnalyzer

Remarks:

- STRATEGY::TEMPLATE:
SyntaxAnalyzer.launchMainNT()

STRATEGY::CONCRETE STRATEGY:
ClassBasedDescription.generateAST()
IRPrologDescription.generateAST()
AbstractPredicates.generateAST()

- The method SyntaxAnalyzer.launchMainNT is:
prelaunch();

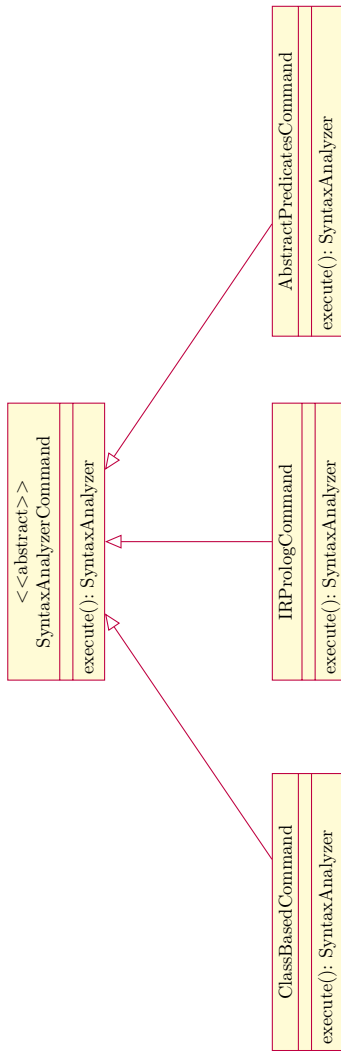


Figure 89: Package frontend

```
this.tree=generateAST();
postlaunch();
```

- In class "IRPrologDescription", get-methods mean access to synthesised attributes of the corresponding formal grammar.
- Class "ParserRuleContext" contains all that is needed by inherited and synthesised attributes.

Prolog Terms: Package internal.core see fig.93.

This package contains all IR with terms, subgoals and rules.

COMPOSITE::COMPONENT:

PTerm

COMPOSITE::COMPOSITE:

PTerm

COMPOSITE::CONCRETE COMPOSITE:

PAtom, PVariable, PFunctor, PNumber, PList

PAtom.getChildren returns null. PAtom.setChildren ig-

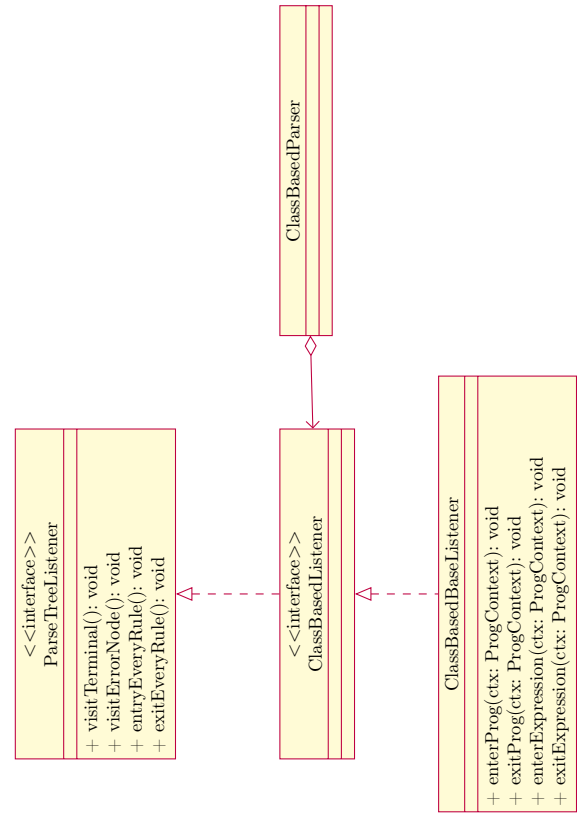


Figure 90: Package parsers.incoming

nores the set and, if possible, issues a warning to the console. PSubgoal represents a subgoal, which may further contain PTerm as content (non-subgoals).

Remarks:

- In package "internal.core" (see fig.94), there is no need for some "PSubgoal", since it is already included in "PRule", and since subgoals are part of queries (which are not part of the grammar generated by APs).
- The method "GrammarBuilder.loadRules" reads all "PRule" and puts them into the formal grammar, where attributes remain the way they are in Prolog. Class "GrammarBuilder" implements both interfaces "PTermVisitor" and "PRuleVisitor". This distinction is required for rule interpretation and because one starting NT is required.
- "PTerm" and "PRule"-instances are generated in dependency of instance descriptions (Description-objects).

Abstract Predicates: APs are needed for representation and logical processes. Used analysers all have one starting NT symbol, although an analyser must have provided the possibility to switch starting NTs. For demonstration purposes, ANTL-grammars are considered.

Package internal.aps see fig.95.

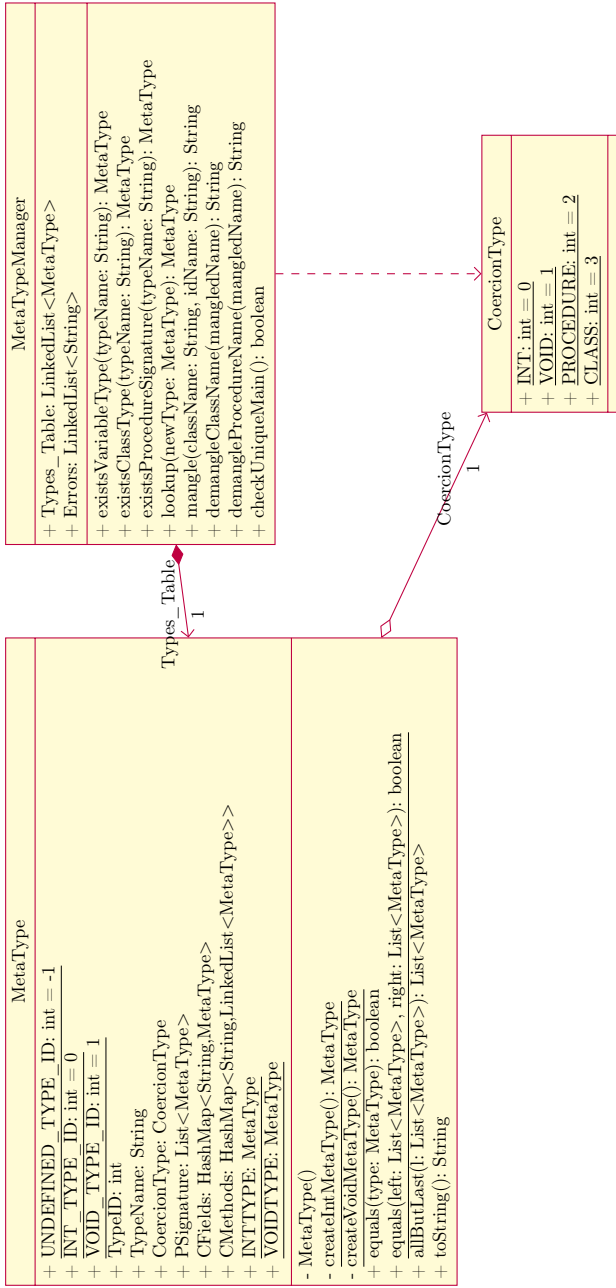


Figure 91: Package parsers

Remarks: All these classes are involved in a formal grammar's notation (further implementations shall be considered using ANTLR). "PRule" may be presented in the form "FG_AP_Rule", (and vice versa) in the following sense:

$$\begin{aligned}
 & p1(X, pointsto(X, value1)):- \dots \\
 & \Leftrightarrow \\
 & p1_{x1, x2} \rightarrow \{X_1 \approx X\} \{X_2 \approx pointsto(X, value1)\}, \dots
 \end{aligned}$$

Next, FG_NT has attributes List<PTerm>, except List<FG_Att>, because it refers only to an existing NT with a concrete sequence of PTerm, by the ordering of

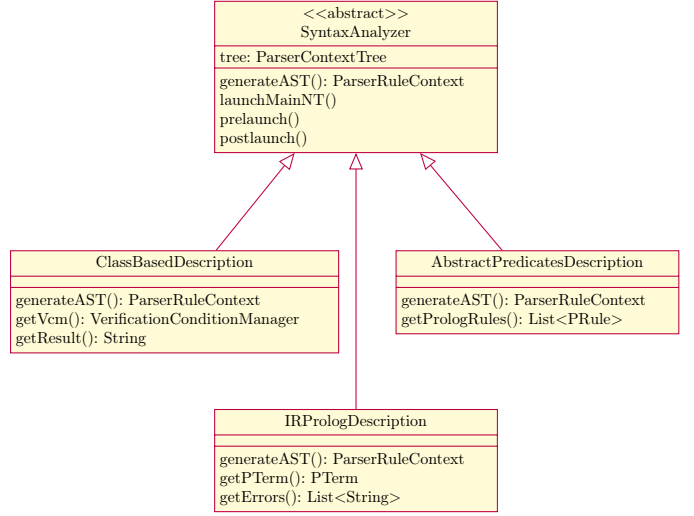


Figure 92: Package frontend

attribute definitions.

Heap Terms: Prolog terms are defined inductively over operators $\{\circ, ||\}$. The term obtained is the result of previous syntax analysis.

Package internal.ht, see fig.96.

Subgoals in APs may generate a connected (sub-)graph. $a \circ a$ is currently done for the general case for simplicity purposes. $a_1 \circ a_2 \circ a_3$ may directly be noted using a_1, a_2, a_3 (as part of some AP) or as APs $a_x : -a_1, a_2.$, wherein the following may act as some subgoal: \dots, a_x, a_3, \dots

Example 2) $a_1 \circ (a_2 || a_3)$ may be rewritten as AP

$$a_x : -a_2, disj, a_3.$$

, where there is some sequence as part of an AP \dots, a_1, a_x, \dots

Remarks:

- HeapTerm is an internal IR for heaps based on SL. Heap terms over $\{\circ, ||\}$ may also contain partial specifications. A heap term is build up stepwise during data analysis of APs.
- HeapTerm.simplify refers to BuiltinLibrary.simplify_1(). Heap term simplification using overloaded built-in Prolog predicates simplify_2.
- A heap term represented by heap term may also be described partially using Prolog's anonymous placeholding operand $_$. The normalisation of given conjuncts is subject to lexicographical sorting of all left-hand sides on simple heaps.
- DotGenerator generates DOT vector graphics as a single string expression that optionally may be serialised to an output file.

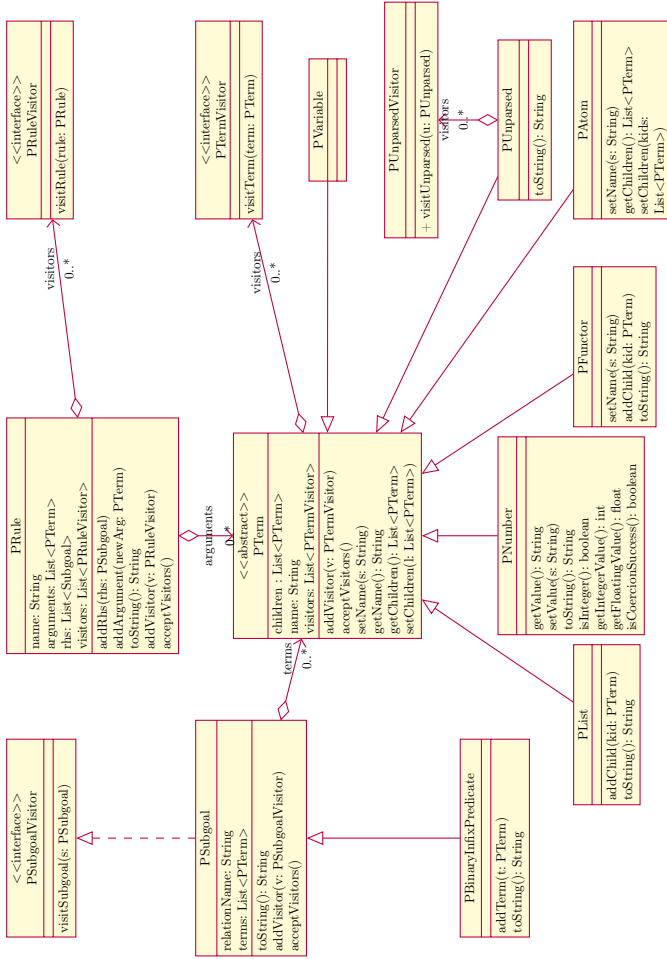


Figure 93: Package internal.core

- Soundness proof is considered, whether (i) non-repetitiveness is obeyed, (ii) a heap is connected.

Package prolog (see fig.97).

The library BuiltinLibrary contains all Prolog predicates, which are granted access for the logical analysis by subgoals. If an AP is entirely accepted by the recogniser and terminates afterwards, the kind $a \circ a$'s condition is checked.

Remarks:

- "BuiltinLibrary:disj_0" accomplishes one step in heap verification. Unique markers may be introduced in case of inaccessibility.
- "BuiltinLibrary:unify" is a replacement for the classic term unification ($=/2$) using as wells as by not using checks on repetition.
- Class "HeapTerm" refers to "BuiltinLibrary:simplify_1".
- "BuiltinLibrary::serialize_1" is almost equivalent to "serialize_2", except the content is issued to the console.

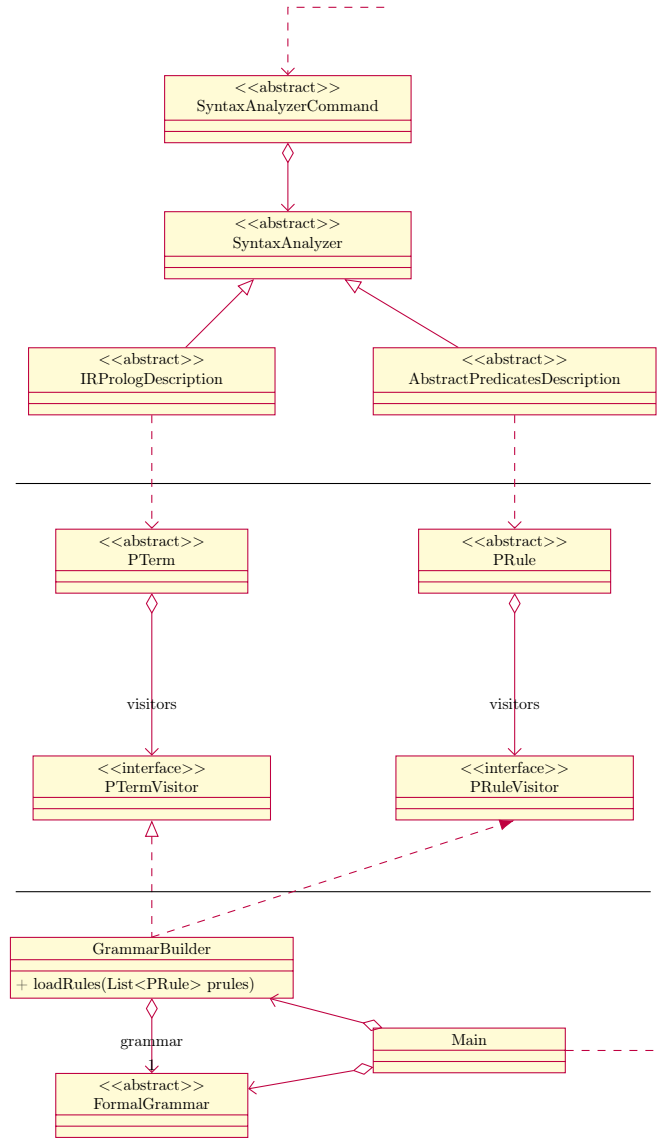


Figure 94: Package layers frontend, internal.core, internal.aps

- "StackState" is needed for checking visibility scopes. For example, it checks whether a symbol is in scope after all other semantic checks are accomplished. Its signature is of type $\sigma :: String \rightarrow Type \rightarrow Value$.

I. Conclusions

The approach introduced presents a new technique for automated verification of \mapsto -assertions in APs by syntactic analysis. It avoids manual predicate "folds" as well as "unfolds". If some predicate partition may be represented as the proper rule set of a syntax analyser, then a solution will be found, if any. Otherwise, the failing simple heap will be provided automatically by the syntactic analyser as a generic counter-example. Remarkably, the latter remark is identical with non-AP-related heap comparisons. After Knuth-Wagner, an attributed grammar is applied

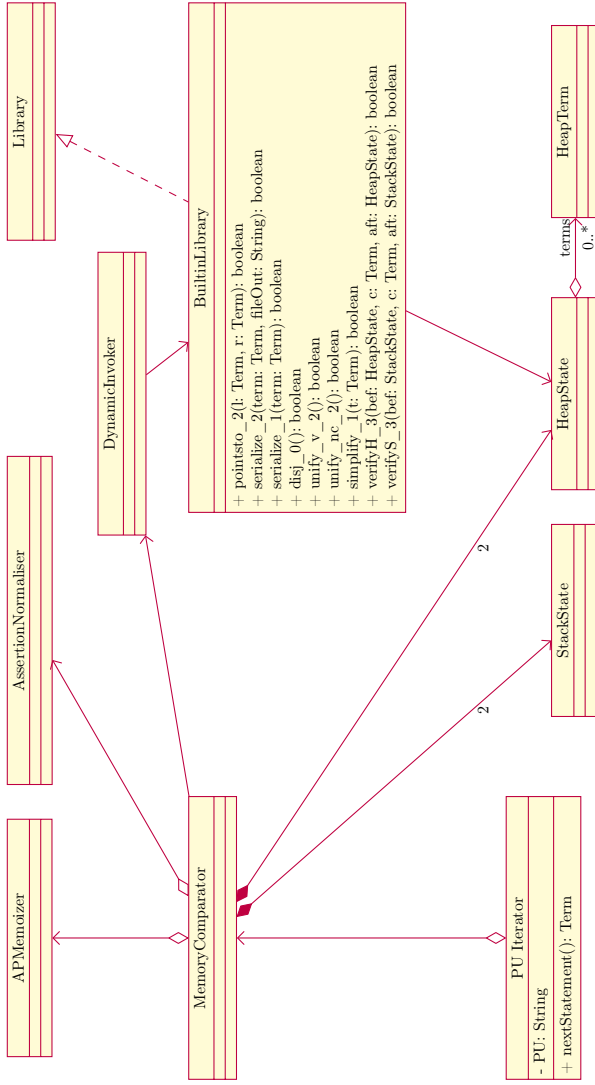


Figure 97: Package prolog

analyse the real problem behind it – however, this will not incorporate with several compiler generators, especially not with LR-styled ones. Thus, a finite automaton based approach is suggested for minimising the edit distance between calculated and expected heaps, in analogy to Levenshtein’s algorithm [287], [264], [11]. Its complexity is expected to be bound by $\Theta(n^3)$ for the heap model suggested in this work. The expected edit trace would include positive and negative (sub-)heaps (cf. sec.V) – this is expected to be fully compatible with Levenshtein’s insertion and deletion operations.

Regarding term IR [230], [284], [10] shall be mentioned as proof that Levenshtein’s algorithm is tractable to terms. "Panic mode" as described in [110] and in [197] attempts to continue parsing till some well-known safe marker is put in artificially to a formal grammar in case of an emerging syntax error in the input word. The effect on heaps shall

be researched for a stable error restore and its usability towards proofs.

Furthermore, it is recommended to consider partial specification, as was introduced earlier by constant functions "*emp*", "*true*" or "*false*", for the sake of proof simplification. Notably, the research shall focus on whether partial specifications may locate inaccessible bridges in heap graphs, which connect independent heaps, for the sake of a better specification rewriting.

VII. Conclusions

Proof automation:

- 1) Analysis of gaps between specification languages and verification languages for dynamic memory. Analysis of narrowing down both languages.
- 2) Expressibility analysis and measurement of term transformations in the logical paradigm using a Prolog-dialect. Finding confirmation for logical assertions based on symbols, variables, terms, and relations is more convenient and closer to heap verification in Prolog than other existing approaches.
- 3) Prolog terms as IR fit best for the whole static analysis assembly line.
 - Foundation and use of a logical language for specification and verification heap. The main idea — logical programming for proving theorems about the heap.
 - The proposed platform, designed as open, extensible and variable. The platform allows the integration of additional external libraries and optionally logical solvers directly in Prolog.
 - Research done showed numerous advantages of Prolog over competing techniques, including direct SMT-solver injection in Prolog.

- 4) Proposition on heap verification automation as a syntactic analysis of abstract predicates based on heap graph edges’ stepwise processing.

Expressibility of specification and verification languages:

- 1) Now, w.l.o.g. abstract predicates and subgoals to be proven may contain symbols and variables in Horn-rules, which extends its previous limitations. Predicates may now have any recursive definitions, where the chosen syntactic analysis method may bound recursion requiring a rule rewriting (e.g. a left-factorisation).
- 2) A rise of expressibility is imminent due to a strengthening of heap operations. A strict relationship was established between heap expressions and their graph representation. Now spatial heap operators build up unique term assertions. Algebraic properties were proven, founding a new heap calculus, which obeys monoid and group properties. The proposition was made to extend the de-facto standard UML/OCL by pointers enriched by a Prolog notation.

- 3) Expressibility and completeness were lifted due to partial heap specifications of variables, and within bound of object-instances was observed. Comparison of heaps is now enabled, s.t. incoming heaps of one set may be compared to another, so "gaps" and "intersections" may effectively be spotted. Now, rules may be written potentially shorter and more readable and cover potentially more cases simultaneously.
- 4) Theoretical possibility is now given, based on a stricter representation, to localise and check a given input program for minimality w.r.t. full heap graph coverage ("inhabitant problem") while excluding abstract predicate definitions in general.

Conclusions:

- 1) A unified specification and verification language. Narrowing down specification languages to verification languages, and vice versa, to a logical programming language, namely a Prolog-dialect, is considered an extreme solution to a target function with numerous unknown parameters, which is considered ambiguous. The unified solution fights ambiguity and resolves several issues analysed w.r.t. expressibility and completeness. The fewer languages there are, the fewer exceptions and the less, in general, need to be considered. That is the case when specification and verification are essentially the same w.r.t. syntax and semantics. The verification process is represented as a comparison of some expected and a calculated heap.
During the research of existing heap verifiers and related projects, both tools, "shrinker" and "builder", were developed as helpful universal analysis tools. Research showed that despite claims made, other verifiers still are restricted to a few academic examples only, beyond which its practical meaning sharply drops. Tremendous efforts could be seen to be put by scientists worldwide to be put into infrastructural re-definitions of well-known verification concepts, again and again, hindering further break-through massively.
- 2) "No" to new and duplicate (re-)definitions. Prolog use allows avoiding the (re-)introduction of conventions, specification, programming, and verification language features and software modules based on those. There is no need to introduce more and more model heap definitions. There is now one adequate heap definition. Important properties and criteria were derived, which are now covered by the platform proposed. Now heaps and parts of it may be denoted by (sub-)terms and symbols. Abstract predicates are now represented by Prolog rules and fully fit in the context of Prolog. The term IR is used as the input programming language for a C-dialect or any other imperative programming language, including no programming language. Instead, in this case, direct Prolog terms may be injected and interpreted directly by the verification core. Specification and verification are now defined in one language instead of two, namely a Prolog-dialect. Optionally the input listing may too be provided in the Prolog-dialect.
- 3) Increased expressibility by direct and unrestricted use of Prolog symbolic variables. Heap predicates became genuinely logical and abstract (but not "Abstract"), namely Prolog predicates. In predicates, symbols are now allowed at random places, and no more restrictions exist here. Logical reasoning is based on symbols. Due to unification and a WAM-based execution stack, logical reasoning has by its nature the same deductive structure for no extra costs. The discussion showed that the heap graph model presented completely covers all desired heaps. Additional emphasis was put on optional higher-order predicates. Class-objects are heaps too. Class methods as functions do not insist on pre- and postconditions. The frame rule is applied to procedures and among the object life-cycle. Symbolic parameters may pass objects to abstract predicates. Thus, modularity raises, and due to partial constant functions, objects may still be fully specified.
- 4) The relational model proposed showed that Prolog implementations are complete and adequate, particularly towards abstract predicates. In contrast to competing, the relational model was chosen as the most promising for checking heaps' comfortability. References and comparisons to literature references were discussed. Although quantitative analysis is complicated and occasionally not representative, still representative examples were chosen and analysed using metrics. So, the field expertise showed Prolog terms are nearly always better on average by 30% than equivalent functional notations. "Better" means especially compacter and more flexible. Typical examples were cherry-picked for the sake of demonstration that cannot be represented (at all or with immense difficulties only) in functionals or imperative paradigms.
- 5) In Prolog, a new verification platform based on a conveyor/assembly line architecture. The platform is minimalistic and centric to terms derived from the incoming program and annotations and verification rules, all in Prolog. The platform is from a user's perspective altogether in Prolog from the specification and verification view. It is explicitly designed for heap reasoning and allows user-specified definitions and rules to be added dynamically. The platform follows the core principles: (1) automation, (2) openness, (3) extensibility, (4) plausibility. It can only be derived what follows by the given Prolog rules (or its multi-paradigmatic built-in predicates) – this is a quick but fair and intentional design

decision. Verification rules, lemmas and inductively-defined abstract predicates are all noted in Prolog. A proof tree can be traced (e.g. by DOT-visualisation) and by logging messages. Any problematic case can be debugged individually by jump-starting with arbitrary memory state (stack and heap) and some input program statement or Prolog-equivalent term statement – so debugging is possible at any phase.

- 6) Simplification of specification and verification due to strengthening spatial operation. A stricter heap definition denoting single simple heaps was found instead of the previous ambiguous heap definition. Strengthening means obeying the atomism of heaps. More precise, more straightforward heap results, and as such, specification and verification rules become simpler. A mandatory comparison of a heap in the context of all other heaps is no more needed. Now heaps, including one-to-one as well as one-to-many, can be done more effectively. Due to established group properties, now heaps can be calculated. Heaps may be differentiated for a rule set, and comparison may indicate missing parts, so a rule set may effectively be checked for completeness. Due to partial specification, now the total amount of heap rules that need to be specified can be reduced and simplified. Exceptions in heap expressions remain excluded, but the rule set completeness can effectively be checked using partial (incomplete) specifiers. In practice, a strengthening means that heap subexpressions do no more need to be extensively analysed.

As UML/OCL does not support pointers, the models introduced are compatible, so it is proposed to enrich it with pointers, and the logical notation introduced.

- 7) Possibility defining new heap theories. Shown algebraic properties allow the definition of equalities and inequalities over heaps. These formal theories may immediately be expressed either in Prolog or in SMT-solvers that can be integrated using multi-paradigm programming as Prolog subgoals. Now rules and (heap) theories can be checked easier and without superfluous checks.
- 8) Abstract predicates form an attributed grammar. In analogy to schema validation and templates processing, semi-structured data bridge verification and specification processes by similar data, namely heap data terms. Here abstract predicates are found to be a heap abstraction technique containing "gaps" as templates do. The gaps are filled during verification with concrete data. This meta-concept finally leads to syntax analysis. As a result, logical reasoning on abstract predicates may be interpreted as syntax analysis. Comparing an actual heap with the expected may be considered as a word problem for formal languages. This universal method has recognition limitations. However, the method is

convenient, regardless of the well-founded theoretic apparatus underneath.

- 9) Universal approach in automating assertion checks. Predicates and proof are based on a Prolog-dialect and may multi-paradigm include arbitrary libraries. So, proving becomes programming essentially. The need for redundant process definitions of translation and rule description becomes obsolete because it is implicitly already expressed by Prolog terms and rules, even when the language introduced is minimalistic. There is no more manual fold and unfold needed for recursive definitions applied to abstract predicates. If a heap is not definable according to given abstract predicates for an individual parser, they may either be rewritten or not definable in principle, e.g. if they are not context-free. Syntactic analysis is decidable for heaps, and termination is guaranteed, e.g. for LL-recognisers in polynomial (approximately linear) time. An analyser is generated by need and only if rules change. Its process is initiated once on-the-fly. Depending on the reachability of starting non-terminals, the recognition of subgrammars avoids new recogniser rebuilds. In practice, all non-terminals may be available after a recogniser is built once. Syntactic analysers do not require further research for this work's objective because they have been researched to a near full extent over the last decades.

In case of an error, the automated reasoning, either with or without parsing, can immediately derive counter-examples from a simple term comparison of having an expected term founded on simple term unification and without any further efforts required.

Future Research: Future works shall include the following theoretic and practical work (not prioritised):

- 1) Integration of further formal theory solvers. After and during the definition of heap theories, SMT-solvers shall be integrated for improved and even more simplified proofs. Solvers may naturally be written in Prolog. Prolog's constraint programming abilities is one primary reason for its widespread popularity, at least in academia, so this would be considered a bargain.
- 2) I Integration) into existing environments. Besides the mentioned limitations and for the sake of broader popularity, term-IRs shall be turned into GIMPLE and LLVM bitcode, and vice versa for full industrial compliance.
- 3) II Integration) into existing environments. A detailed code analysis, namely detecting "growing" points (memory regions bloating), may lead to an improved allocation strategy w.r.t. fragmentation, memory segmentation and layout. Here the not initially compatible abstraction interpretation technique shall be further tracked towards and incorporated with the

stricter memory model introduced in this work. Also, memory addresses with static offsets shall be further integrated into the existing heap model for a broader acceptance and easier integration towards GIMPLE.

- 4) Heap isomorphism. The check for graph isomorphism relates to how a heap is not fully specified, so containing gaps or symbols is still effectively compared?
- 5) Finding (even minimal) deviation from a specification. During syntax analysis, in case of an error, a minimum global search might be better instead of an exist on first error occurrence, e.g. by using Levenshtein's edit distance. Here further research is needed.
- 6) Further Pointer dependency analysis. In contrast to alias analyses, it is highly suggested to research some extended SSA-forms incorporating pointers. Nobody has even tried that before, presumably since it is feared it is too complicated, although both SSA and pointers are about analysing data dependencies. Initially, a deviation is expected, but if synergies could be found, this would not only ease pointer analysis but would for free provide a powerful optimisation technique with in-depth knowledge of how the heap graph is supposed to be used most efficiently.
- 7) Verifying existing code repositories. The approach proposed here remains academic, after all. Verification of more extensive source repositories always was and still is a separate research branch. So, eventually, such a field study would be an outstanding practical achievement. However, that would require first to cover GIMPLE entirely for a realistic estimate.
- 8) Further research on transformation languages by practical means. Discussed transformation languages may provide a compact and rule-based notation, usually including the calculation states before and after. However, a significant gap is expected between the introduced memory model, the expressibility model and content in dynamic memory, and the input language. This gap will need to be clarified first – and after all, could be an alternative to this work's main contribution.
- 9) Abstract reasoning. Rare Prolog-dialects do support abductive reasoning in addition to Prolog main's reasoning: deduction. This issue becomes prominent, especially since O'Hearn's attempt in introducing abduction to separation logic. In general, abstraction techniques are considered an additional mechanism in matching rules that otherwise would not be selected. The ordering of logical conclusions made may be further simplified if the relationship between the incoming and outgoing terms are invertible in terms of predicate inversion, as discussed in section IV.

Recommendations for practitioners:

- A practical heap specification was simplified. A given program is annotated by verification conditions and user-defined (abstract) predicates, namely the specification.
- Abstract predicates need to be well-defined and valid Horn-rules. If those build up in Prolog a proper context-free grammar, then subgoals to these can be recognised. Alternatively, rule rewriting may resolve recognition problems.
- The use of stricter spatial operators allows extending UML/OCL specifications by pointers and a well-founded calculus.
- The introduction of new programming languages is not mandatory, although it is open potentially to any language obeying requirements. A programming listing may be missing if it is injected by a Prolog term instead. The extensible and variable IR gains maximum flexibility. Verification architecture has the same properties.
- The heap comparison of a given expression with the expression from rules allows now to find differences in heaps. In more details, it may check all heaps for a predicate partition in order to find missing heaps in rules.
- The overloading of relations simplifies logical reasoning, e.g., abduction and different techniques shall be considered in the future.
- The use of SMT-solvers for given heap theories, either in Prolog or by a multi-paradigm implementation, may increase transformation speed in normalised heap forms.
- The integration of memoisation (in Prolog called tabling) to abstract predicates may lead to an improved performance throughput.
- When introducing new or modifying existing phases in heap verification, it is highly recommended to stick to Prolog term IR.

Formal Concept (G, M, I) on Achievements:

Set G — Objects are the achievements:

- (1) Unified heap specification and verification language
- (2) Architecture principles for heap verification
- (3) Increase of expressibility
- (4) Relational model for heap description
- (5) Prototypical reference implementation
- (6) Interpretation and introduction of heap theories
- (7) A fresh definition of a singleton heap
- (8) Simplification of heap specifications based on $\circ, ||$
- (9) Pointer-based object calculus proposed
- (10) APs represent attributed grammars

Set M — Features are the central theses:

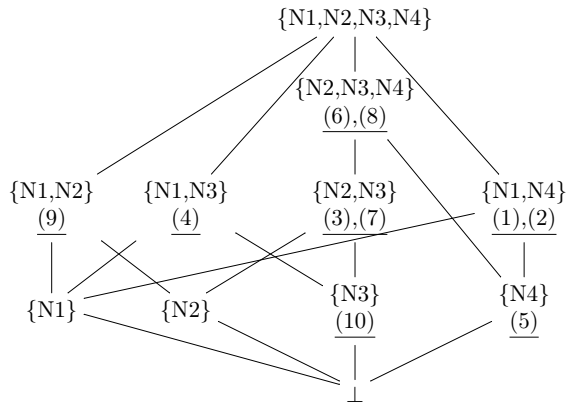
- N1 Prolog-dialect as heap specifier and verifier
- N2 Strengthening approach of ambiguous heaps

N3 AP verification as attributed grammar parsing
N4 Unit of utils for heap analyses

$I \subseteq G \times M$ — Incidence relation:

G/M	N1	N2	N3	N4
(1)	x			x
(2)	x			x
(3)		x	x	
(4)	x		x	
(5)				x
(6)		x	x	x
(7)		x	x	
(8)		x	x	x
(9)	x	x		
(10)			x	

The corresponding Hasse diagram for I can effectively be constructed and visualises the dependencies:



VIII. Original

In the original translation, all figures, algorithms, tables and additional materials are stripped off. Here, the original text refers to the English translated figures. In most cases, this is believed to be accurate.

Введение

Для введения в предметную область диссертации «Логический язык программирования как инструмент спецификации и верификации динамической памяти» приводится этот раздел. Первый раздел посвящается вычислению Хора, основным определениям и постановлению решения вычислением, альтернативным подходам и свойствам систем вычислений Хора.

Далее для сравнения различных динамических и статических подходов, можно использовать «качественную лестницу» из рисунка 1 в любой момент. Эта лестница является моим личным предложением для классификации качества, которое должно соблюдать любое программное обеспечение. Чем больше программа соблюдает критерии качества, тем искреннее можно считать данную программу качественной. То есть, если программа некорректно вычисляет результат, то на самом деле можно считать неважным, насколько данная функция выполняет критерий входного домена, и тем более безразлично, насколько быстро это сделано. Самое главное - это корректное вычисление программы. Если это соблюдается, то только тогда можно считать уровень «базисно надёжным».

С растущим спросом в надёжности растёт спрос на универсальность данной функции, т.е. тогда имеет смысл распространить качество на любые входные функции. Если базисные операции работают правильно, то тогда можно требовать, что для всех входных данных функций всё работает правильно — это второе требование, которое мы обозначим «полностью надёжным», более жёстким, чем первое. Если первые два критерия соблюдаются, то с вычислительной точки зрения, данная функция корректна и полна. Тогда имеет смысл, далее вводить оптимизации, которые мы обозначим «оптимально надёжными» и которые не меняют вычислительные свойства корректности и полноты. Надёжными оптимизациями могут послужить, например, ускорение часто востребованных программных блоков, визуализация эффектов, работа с файлами и т.д. Визуальные эффекты и работа с файлами не будут рассматриваться.

Каждый из установленных критериев можно чётко обозначить и можно предложить некую метрику для измерения выполнимости. Не имеет смысла рассуждать о качестве программы, когда программа вычисляет корректно и быстро, но не полностью, потому, что универсальность применения подрывает

качество существенно, когда не имеется определение для входного вектора, даже, если все остальные случаи высчитываются очень быстро. Тогда можно, либо ограничить диапазон видимости входного вектора для полного покрытия функции, либо сузить покрытие ради неполной надёжной функции. Когда будут рассматриваться различные подходы, качественная лестница будет использована как ориентир для принятия или отклонения предложений в дальнейшем.

В данной работе рассматриваются императивные и искусственно-гипотетические языки программирования. Для практической применимости необходимо рассматривать объектно-ориентированные модели, поэтому в следующем разделе вводятся основные понятия объектно-ориентированных вычислений, в частности, Теория Объектов (ТО). Далее рассматриваются теоретические и практические проблемы работы с динамической памятью, а затем вводятся модели представления динамической памяти, как, например, анализ образов (АО), вычисление регионов (ВР), а также другие модели представляющие косвенно-динамическую память. Логика распределённой памяти (ЛРП) является основной теоретической моделью представления динамической памяти этой работы. Затем даётся обзор по автоматизации доказательств и обсуждаются её факторы противостояния. С целью лучшего понимания проводимых далее доказательств с помощью модели Хора и улучшения сходимости деревьев доказательств, вводятся представления «абстракции». С кратким обзором по тематике можно также ознакомиться в [303]. Затем, с целью ознакомления, рассматриваются области применения и связанные с главным направлением работы в этой области, в частности — анализ псевдонимов (см. раздел I-D), сбор мусора и верификация кода с интроспекцией. В конце этой главы представляются существующие программные системы и среды.

Вычисление Хора

Вычисление Хора (назван в честь информатика Чарльса Антони Ричард Хора, в литературе также встречается фамилия «Хоаре» вместо «Хор», однако известно, что сам автор пишет свою фамилию как «Хор» на русском, а также это способствует избегать неверные произношения других авторов) - это формальный метод верификации, который позволяет проверить верность данной программы, данной некоторой спецификации, т.е. согласно описанию, характеризующему свойство поведения программы. Спецификации описывают состояние вычисления с помощью математических формул и теорем, а вывод происходит согласно аксиомам и правилам рассматриваемой области дискуссии.

Цель верификации программы, с помощью вычисления Хора, - это проверка соблюдения

свойств программы, что является повышением качества и надёжности программы. Если программа соблюдает свойства утверждениями, то это позволяет нам характеризовать программу и сравнивать её с другими программами, где одно или иное свойство, возможно, не соблюдается.

Любое правило Хора необходимо рассматривать, как логическое суждение $A \Rightarrow B$, которое читается: «если суждение антецедент A выполняется, тогда выводимое суждение консеквент B следует». Рассмотрим рисунок 2:

Правило Хора ($P1$) является аксиомой, пусть A будет пустым антецедентом. Главная идея аксиомной системы заключается в проверке верности следствия согласно применению конечной последовательности определённых правил. Отныне, мы не различаем между правилами и аксиомами, т.к. первое является обобщением второго. Правило ($P2$) является аксиомой, если антецедент $B \vee \neg B$ выполняется всегда аналогично логике утверждений и сопоставляется «истинно». Однако, изначально не имеются искусственные ограничения в вычислении Хора, например, касательно суждений. Утверждения могут быть сопоставлены предикатами, а логический вывод становится суждением над предикатами. Различные методы могут быть применены для вывода с предикатами первого порядка, например: метод естественного вывода [262], метод резолюции или метод семантических таблиц («Tableaux method»). Перечисленные методы являются дедуктивными. В отличие от дедукции, ещё имеются абдукция и индукция. Индуктивный метод вывода предлагает ввод ещё не существующие или тяжело выводимые, явным образом, утверждения в набор рассматриваемых правил. Индуктивное правило введённое «кажется» искусственно, нельзя отклонить из-за отсутствия противоречивого примера. Классическим примером индукции служит теория опровергаемости по Попперу: данное утверждение «все лебеди белые» на практике, из-за ограничений не может быть проверено целиком за конечный промежуток времени. Поэтому, предлагается исходить из верного утверждения до тех пор, пока не будет замечен противоречивый экземпляр, например, не будет найден чёрный лебедь. Индукция нам предлагает ради преодоления необъяснимых и неотрицаемых феноменов в рамках рассматриваемого ракурса ввод нового правила, согласно которому феномен может быть обоснован. Свойства индуктивно определенных перечисляемых, возможно бесконечных структур, проверяются с помощью конечной формулы. Когда наблюдается противоречивый индукцией экземпляр, мы вынуждены скорректировать наши утверждения о мировоззрении. В отличие от этого, абдукция ищет необходимые и допустимые предпосылки, чтобы следствие было выводимо из набора правил.

Вычисление Хора можно охарактеризовать, как

дедуктивное суждение, применив к императивному программному оператору (как это было предложено изначально Хором), а каждое выводимое суждение описывается состоянием вычисления, до и после выполнения оператора и программным оператором (см. раздел I-A1). Ради улучшения сходимости доказательства, часто можно добавлять индукцию и абдукцию в качестве метода вывода. Вывод дедукции интуиционистен [47] потому, что утверждение только тогда верно, когда даны условия и соответствующий факт предусловия. Когда мир расследуемых выводов производится строго согласно правилам и пересекаемые в антецеденте, правила исключены, то космос выводимых следствий является замкнутым, к примеру, правила ($P3$) и ($P4$) из рисунка 2, интерпретации возможных логических утверждений также замкнуты.

Тройка Хора: Для формальной верификации с помощью спецификации, Хор в [116] предлагает для императивных языков программирования определить тройку.

Декларативные языки программирования, например, функциональные, отличаются от императивных тем, что состояние вычисления меняется в зависимости от содержимого переменных. Порядок выполнения программных операторов не строгий. Декларативную парадигму программирования можно отделить от императивного с помощью модели организации памяти касательно символов и переменных. Далее в этой работе рассматриваются исключительно императивные языки программирования, в качестве входного языка программирования. Изначально Хор предлагал, в качестве языка программирования простой императивный язык наподобие диалекта Паскаль и нотацию $P\{C\}Q$. Скобочная нотация над оператором оказалась не популярной, поэтому скобки стали ставить вокруг P и Q . P и Q оба описывают состояния вычисления в качестве утверждений до и после C . C может содержать любое количество императивных операторов. Из сказанного следует, что C меняет пошагово состояние вычисления, если C не делится далее, а следовательно, состояние памяти меняется пошагово. Под памятью мы подразумеваем список процессорных регистров, стек и динамическую память (см. рисунок 25). Тройка Хора интерпретируется так: если имеется состояние вычисления P и программный оператор C выполнен, то вычисление совершено и находится в состоянии Q . Другими словами, P и Q описывают состояния памяти до и после C . Если тройка Хора соблюдается, то переход состояний памяти верный, в противном случае, имеются следующие причины несоблюдения:

- 1) Если C не завершает работу, то данные правила Хора назовём «неполной определённой» и состояние Q не достижимо. Такое поведение C

опишем формально как: $\vdash \{P\}C\{Q\} \rightarrow (\llbracket C \rrbracket \neq \perp) \wedge Q$, где $\llbracket \cdot \rrbracket$ денотационное преобразование программного оператора [9], [6], [276].

- 2) Аксиоматические правила не полны. Выбираемое правило отсутствует для данного состояния P .
- 3) Полученное актуальное состояние вычисления Q не является ожидаемым состоянием Q' .

На рисунке 3 указаны наиболее важные аксиомы и правила для императивных языков программирования. Программу написанную императивной парадигмой можно преобразовать в программу декларативной парадигмы, а также обратно, благодаря симуляции машиной Тьюринга о вычислимости. Программы можно более абстрактно представить блок-схемами. Вызовы подпрограмм завершаются «обычной» стековой архитектурой. Изначальное вычисление Хора [116] не накладывает дополнительные ограничения на описания утверждений в математических формулах, также как и предложенные подходы из [16] не накладывают дополнительные ограничения. Апп предлагает вычисление Хора для верификации одно- и многопоточных программ, а также утверждения классифицировать на входные и выходные переменные. Позже мы оценим достоинства и недостатки различных подходов верификации программ.

Итак, правило последования (SEQ) из рисунка 3 служит примером и означает: если имеется оператор разделитель «;», то для доказательства корректности $A_1; A_2$ с предусловием P и постусловием R необходимо доказать, что существует промежуточное утверждение Q , если доказать сначала первый оператор A_1 с предусловием P , а затем Q служит в качестве предусловия в доказательстве A_2 . Корректность последования считается доказанным, как только A_1 доказано, а A_2 доказано с постусловием R .

Вторым примером служит правило логического последствия (CONSEQ), которое является обобщением правил (SP) и (WP). Конкретизированные правила, либо ужесточают предусловие, либо обобщают постусловие. Если предикат верный в общем случае, тогда для некоторого множества V предикат также верен в частном случае для любого $v \in V$ или для любого подмножества $V_1 \subseteq V$. V является обобщением от V_1 , а V_1 является конкретизацией V . Нетрудно убедиться в том, что импликация $V \Rightarrow V_1$ в силе, однако, $V_1 \Rightarrow V$ не для каждого предиката действительно. Исходя из общего случая, можно выводить верность предиката без ограничения общности для конкретного случая, поэтому в силе правило (SP), а также в силе (WP). Если (SP) и (WP) объединить, учитывая переименование переменных состояний вычисления, то как раз получается (CONSEQ).

Третьим примером служит правило цикла (LOOP). Это правило гласит, что если имеется цикл в качестве программного оператора и мы имеем предусловие P и

постусловие Q , то достаточно доказать корректность блока цикла S , как единый программный оператор и добавить к P условие цикла B . При выходе из блока цикла необходимо добавить в постусловие отрицательное условие цикла.

Отмечается, что благодаря циклу и правилу присвоения возможно преобразовать любой другой вид цикла в данный вид цикла (LOOP) как изложено в рисунке 4.

Ради простоты, договоримся, что в правиле (FOR) ранее известных количеств итераций n переменная i является свежей, т.е. неиспользуемой в предикате P или Q . Если переменная не свежая, то согласно диапазону годности переменных, вводится свежая переменная. С проблемами индексации термовых выражений и подхода избежания коллизии наименований можно ознакомиться в [204]. То есть, правило (REPEAT) можно преобразовать в (LOOP) и обратно, однако, в общем (FOR) можно только в (LOOP) преобразовать, т.к. для обратного шага всегда необходимо заранее знать количество итераций, что не всегда известно. С вопросами преобразования примитивной рекурсии, μ -рекурсии и общими видами взаимной формы рекурсии, а также с вопросами свойств терминации при взаимной рекурсии можно ознакомиться в [25].

Правило для оператора условного перехода здесь отдельно не вводится потому, что он без ограничения общности может быть сопоставлен правилом цикла (LOOP). Для полного понимания преобразуемости, рекомендуется ознакомиться с минимальным языком с точки зрения вычислимости «PCF» [209], [65]. Основной идеей вычислимости является симуляция Тьюринг-вычислимых функций с помощью минимального набора программных операторов. Особенность циклов, в отличие от других линейных программных операторов, заключается в том, что один и тот же блок повторяется множество раз, при этом, состояние переменных обычно меняется. Чтобы зафиксировать совокупность всех изменений блока цикла, необходимо проанализировать зависимость данных и все изменения переменных до выхода из цикла. Повторение цикла необходимо абстрагировать, обычно вручную, подставляя новые искусственные переменные, для определения наиболее обобщённого уравнения целевых переменных (ср. рисунок 11), которые формируют инвариант цикла. Нахождение инварианта может часто оказаться трудным, по крайней мере не тривиально и чисто автоматически не может быть выявлен, поэтому требует построение спецификации вручную. Постусловие блока цикла представляет собой формулу, которая содержит инвариант. Аналогично к фиксированному отображению в проективной геометрии, когда одна точка при трансформации остается фиксированной, тогда инвариант блока цикла это утверждение,

которое остается верным при любом множестве раз итераций. Итак, данная инвариантная формула Φ должна соблюдать равенство $\Phi \circ Y = Y \circ \Phi \circ Y$, где Y является некоторым комбинатором плавающей точки, а \circ является бинарным оператором применения функций. Y является некоторым синтаксическим методом симуляции повтора, либо его цель может определиться как «поисковиком минимума», который широко применяется в λ -вычислениях [22]. Можно использовать альтернативную нотацию вычислимости μ -оператора Клини, указав в качестве минимизирующих параметров меняющиеся переменные.

Рассмотрим пример из рисунка 5.

Инвариантом здесь может быть $a \cdot y + b = x^b \geq 0$, т.к. равенство остатка при делении на y не меняется циклом. y является делителем целого числа $x \geq 0$, a целое частное число, а b это остаток при делении x на y . Правило оператора присвоения (ASN) означает: если переменной x присваивается годное значение e , то, до и после присвоения состояния P остается без изменений. Состояние до присвоения среды присвоенных символов необходимо расширять, включив x . В случае возникновения коллизии с именем, необходимо сначала в спецификации провести переименование конфликтующих переменных.

Полнота правил зависит от полноты троек Хора в виде $\{P\}C\{Q\}$, которая зависит от покрытия всех программных операторов C вместе со всеми допускаемыми предусловиями P (см. опр.1.7). Постусловия Q являются лишь логическими последствиями троек, которые выводимы из P и C . Так как правила для любой годной программы могут применяться потенциально в любом порядке, возникает вопрос, а может ли одно правило нечаянно или преднамеренно исключить любое другое данное правило? Найти ответ наивным подходом может оказаться сложным делом. Очевидно, что если имеется постусловие Q и данная программа C выводит различные P_1 и P_2 , то это явно показывает на некорректность правил Хора. Кроме полноты и корректности, согласно лестнице качества из рисунка 1, оптимальность ресурсов также важна. Вопрос, насколько эффективны или «удобны» правила Хора, затрагивает также вопрос о компактном, но понятном для пользователя представлении. Если идет вопрос об автоматизации, то это также затрагивает вопрос о вычислительной технике. В этом разделе мы увидели, что задача постановления инварианта может оказаться сложной попыткой, т.к. для разумного и обобщенного вывода, необходимо включить все переменные блока цикла, включая все переменные памяти. Обратим внимание на то, что автоматически выделенные переменные имеют диапазон видимости, а у динамически выделенных

переменных диапазон отличается. Кроме того, необходимо заметить, что сравнение равенства между имеющейся и ожидаемой спецификацией может потребовать некоторый консенсус по представлению состояний вычисления.

Логический вывод: Правило ($P1$) из рисунка 2 представляет собой самую обобщенную форму логического правила. Верификация, это проверка данной программы C с условием, что при начальном предусловии P , следует постусловие Q . Верификация, это формализованный процесс (см. рисунок 4.8), который начинает проверку последовательности программных неделимых операторов с предусловием P и с постусловием Q . Результат верификации либо верный, либо неопределенный, когда постусловие отсутствует или оператор не терминирует, либо отрицательный. Применяя правила, может возникать необходимость разветвления доказательства на под-доказательства, в итоге, структура доказательства является деревом.

Определение (Входной язык программирования). Язык программирования является формальным языком, чьи слова соответствуют программам, которые являются последовательностью программных операторов. После запуска каждого из программных операторов, меняется состояние памяти. В качестве входного доказуемого языка программирования, рассматривается по умолчанию императивный язык, близкий к подмножеству Си с объектным расширением.

Императивный язык программирования выбирается по целому ряду причин. Во-первых, императивные диалекты, как Си или Ява, довольно популярны, и необходимость введения всё новых формализмов к большей части отпадает. Во-вторых, в этой работе выбирается прототипно Си диалект, который имеет возможность удобно и просто обсуждать синтаксис и семантику операций над динамической памятью. Естественно, Си имеет моменты, которые зависят от одной или иной платформы, однако это обсуждается и важно понять, например, для дальнейшего применения предложенных подходов.

Определение (Язык спецификации). Язык спецификации является формальным языком, который ссылается на переменные и единицы данной входной программы, символьные выражения, кванторы и вспомогательные единицы для проведения доказательств. Язык спецификации подлежит некоторой согласованной формальной логике. Спецификация, в отличие от входного языка программирования, несет декларативный характер, а не императивный.

Язык спецификации в каждом блоке графа потока управлений (см. рисунок 11) описывает состояние вычисления, опираясь на состояние памяти (см. рисунок 25). Рассмотрим свободно выбранное дерево вывода из рисунка 6 со следующими утверждениями $\{A_1, A_2, A_3, B_1, B_2, B\}$. Изначально требуется доказать

тройку B , согласно опр.1.1. Для этого применяется данное правило, в антецеденте которого должно иметься A_3 и B_2 , оба из которых следует отдельно доказать с соответствующими сопоставлениями так, чтобы имелось соответствие строго по правилу (например, преобразование локальных символов) с консеквентом B . Далее, применив некоторые имеющиеся правила, мы показываем, что B_1 является предусловием для B_2 , а B_1 , согласно правилу, всегда верное утверждение, например, $\{n = 0 \wedge n \geq 0\} a = 5; \{n = 0\}$ если очевидно, что a не связанная, т.е. свободная переменная с n . Далее доказывается A_3 , в результате чего, получается, что A_2 противоречит самому себе. Это условие достаточное, чтобы A_3 вычислялось как «ложь», а следовательно и B . То есть, мы только что доказали, что тройка утверждения Хора B неверна и причина тому A_2 . Поэтому в данном примере нет необходимости дальше доказывать A_1 , независимо, верно оно или нет.

Определение (Логическое следствие). Логическое следствие $A \vdash B$ обозначается как утверждение A , к которому применяется некоторое данное правило один раз. Оно приводит к утверждению B (по Фреге [263]). Если B получаем после применения правил несколько раз подряд, включая ни разу, то следствие получается $A \vdash^* B$. Если мы хотим выразить, что некоторая тройка A , согласно данному набору правил Хора Γ всегда истина, то мы это обозначим как $\models A$, либо как $\models_{\Gamma} A$ если ударение поставить на выбранный набор правил из набора Γ .

Определение (Доказательство как поиск). Доказательство в вычислении Хора, при данном наборе правил Γ и данного следствия B , является поиском аксиом, т.е. $\models_{\Gamma} B$.

В данном определении мы сознательно допускаем неточность в связи с набором правил и вычислением Хора. Например, ссылаясь на Γ , мы ссылаемся на формальную логику, которая состоит из замкнутого по зависимости подмножества данных правил Хора, как множество носителя и базисных логических констант. По умолчанию мы согласуем, что для любого данного набора правил, для логического вывода, мы подразумеваем присутствие корректно определённого вычисления Хора, согласно тройке Хора из опр.1.2, опираясь на опр.1.4.

Определение (Корректность вычисления Хора). Вычисление Хора является корректным, если исключен случай, когда синтаксически подлинная программа C и данный набор правил Γ выводят различные противоречивые результаты.

Если один логический вывод приводит к одному результату B_1 , а второй также допущен согласно Γ и вывод приводит к другому результату B_2 , который не выводим из B_1 или наоборот. т.е. $\{P\}C\{Q\} \vdash^* \{P_1\}C_1\{Q_1\}$ и $\{P\}C\{Q\} \vdash^* \{P_1\}C_2\{Q_2\}$ но, при этом, $\{P_1\}C_1\{Q_1\} \not\vdash^* \{P_2\}C_2\{Q_2\}$ и $\{P_2\}C_2\{Q_2\} \not\vdash^* \{P_1\}C_1\{Q_1\}$ (см. рисунок 7), то

правила являются не корректными. Это означает, что свойство корректности данного вычисления Хора соблюдает свойство диаманта/ромба, т.е. теорема Чёрча-Россера применяется к тройкам Хора (см. [203]). Если хотя бы одно утверждение при выводе противоречит результату другого вывода, то правила Хора являются не корректными и не полными (см. опр.1.7). Сходимость — более жесткое требование, чем корректность и не всегда соблюдается например, из-за незавершения вычисления (более подробнее можно ознакомиться в [247]). Однако, можно заметить, что корректность обязательное условие для сходимости. То есть, если вычисление не корректно, то имеется хотя бы один случай, когда выводятся два или более различных результата и это обязательно не корректно. Согласно Штайнбаху [247] и его рассматриваемой системе переписки термов (с англ. «term rewriting system») [19], терминация программ сильно определяет сходимость. Он представляет правила вывода в качестве правил переписки термов. С помощью ограниченности упорядоченных цепочек, он может в частных случаях доказать терминацию системы переписки. Аппроксимация верхнего порога выводов системы в общем из-за теоретической нерешимости не распространяется на самосодержащие термы или на неограниченные символы [207]. Идея нисходящей цепочки тесно переплетается с теорией доменов [236]. Штайнбах использует цепочки для решения лимита выводов, т.е. для решения вопроса терминации, которая является условием корректности.

Кук [67] рассматривает корректность и полноту различных вычислений Хора. Отмечается, что оба свойства существенно могут меняться, например, применив лишь несколько модификаций к переменным в процедурах. Общее понятие полноты по Куку определяется, как тотальная функция покрывая все входные программы, учитывая ранее упомянутые свойства в [15]. Корректность определяется, как эквивалентность между наблюдаемым и должным поведением, как это предлагается в [79], [189] с помощью операционной семантики [208] над тройками Хора. Вычисления интерпретируются с помощью абстрактного автомата. Для достижения «удобного» — здесь подразумеваются, либо полные, либо корректные вычисления, вводятся дополнительные ограничения в императивном языке программирования, такие как:

- Огран. №1 разрешается использовать глобальные переменные в процедурах, однако, запрещается их передавать в качестве актуальных параметров.
- Огран. №2 запрещаются параметры по вызову (или по ссылкам).
- Огран. №3 рекурсивные процедуры и функционалы (функции высшего порядка)

Почему такие ограничения, как только что были показаны, могут привести к некорректности или

к неполноте? Классический стек при передаче параметров по ссылкам нуждается в обратной связи сквозь стек-окон вызовов. Как только, прекращается вызов, то так прекращают существовать и значения. Передача по ссылке разрешает манипуляции единого содержимого в других стековых окнах, но адрес указателя на объект может меняться в каждом стековом окне. Если допускать параметры по вызову или рекурсивные функции, то это может привести к изменениям вне соответствия вызову стека, как например, глобальные переменные, они практически могут меняться везде. В таких случаях «наивные» спецификации могут быть просто неправильными в общих случаях. Этому можно противостоять, ограничив модус входных и выходных параметров процедур. Иерархические спецификации [235], [37] могут сильно раздуть спецификации, и из-за широкой периферии возможных мест в программе, где может поменяться один указатель, польза при этом, явно ограничивается. В итоге, они также могут оказаться мало эффективными, т.к. все встроенные процедуры специфицируются — при этом, исходя из наиболее общего сценария. В частности, объектные экземпляры могут потерять свойства идентичности и целостности, т.к. по обобщённой схеме передача процедур в качестве параметра, может привести к не непредвиденным действиям, а следовательно, может кардинально поменять состояние вычисления.

Кларк [62] выделяет исключительно актуальные ограничения вычисления Хора, которые остаются до сегодняшнего дня. Острые ограничения касаются:

- Огран. №4 выразимость и неполнота языка утверждений
- Огран. №5 ограничения в связи с инвариантами циклов (преобразование, и т.д.)
- Огран. №6 рекурсивные процедуры (не) использующие глобальные и статические переменные
- Огран. №7 со-процедуры в качестве входного и выходного параметра
- Огран. №8 динамическое выделение и освобождение ячеек памяти (см. [215])

Также как и Кук, Кларк подразумевает под корректностью гарантии о том, что все синтаксически корректные теоремы выводятся верно, а все не корректные теоремы, как ложные. Как любая формальная система, вычисления Хора тоже подлежат теоретическим ограничениям. Например, если рассмотреть теорию целых чисел, то можно всегда придумать всё новые теоремы над целыми числами, которые явно корректны, но которые нельзя доказать данным замкнутым вычислением. Этот феномен лучше известен, как теорема Гёделя о неполноте. Кларк также замечает, как это ранее до него заметил Кук, что если

вычисление Хора содержит не завершающийся цикл, то причиной служит рекурсия в правилах, которая применяется сама к себе, поэтому верификация может не завершаться. Он предлагает запретить псевдонимы ссылок (см. далее), а ради корректности исключить неограниченную рекурсию. Проблему Кларка можно частично разрядить, если правила сопоставления применяются сначала к крайне внешнему терму, вместо к крайне внутреннему терму. Это необходимо учесть при реализации правил Хора в программных средах, где сначала вычисляются параметры процедур, а только затем, передаётся содержимое параметров. Языки программирования без ленивого вычисления, как например, «OCaml», в отличие от ленивого вычисления, как например, «Хаскель», должны, если этого требует ленивый алгоритм, добавить ленивое вычисление искусственным добавлением дополнительных проверок на местах использования параметров. По Кларку выразимость всегда касается языка утверждений, который может быть представлен в виде термов. Ограничение №6 касательно рекурсивных процедур можно исключить, если: (i) рекурсия завершается, т.е. некоторая нисходящая цепочка вывода всегда существует (см. [247]) и/или (ii) последовательность параметров и типизация параметров [55] при вызове процедур должна точно совпадать и исключать переменные, выделенные в актуальном стековом окне, т.е. не глобальные, не статические переменные, и т.д.

Кофмэн [134] выделяет проблемы выразимости и возможность применимости на практике, как наиболее важные, которые сильно противодействуют популяризации формальному методу верификации — языки спецификации и языки программирования. Наиболее важными практическими проблемами выразимости он считает индукцию и абстракцию. Для того, чтобы простым образом различать ошибки некорректного вычисления от недостоверной спецификации, он также замечает необходимость, простого но обобщённого подхода для генерации контр-примеров — пример, который доказывает неверность данной формулы с помощью конкретных входных символов.

Герхарт [104] анализирует существующие к тому времени подходы для решения проблем полноты, которые к сегодняшнему дню решены не в полном объёме и решены не удовлетворительно: (i) наиболее обобщённый подход в решении терминации программ, (ii) решение открытых вопросов верификации переменных в различных областях памяти, как например, статические переменные (см. [62]), (iii) вопросы удобства наиболее обобщённого представления и использования систем верификации. Она отмечает, что индуктивные определения являются одним ключевым методом в решении проблем выразимости, и поэтому их рассматривает как

многообещающий технический аппарат. Герхарт выдвигает требование: простые доказательства должны ссылаться на универсальные и глобальные требования. Из [62] также следует, что проблемы из (ii) можно считать трудными и глобальными, что вряд-ли минимальная модификация вычисления Хора позволит их решить.

В случае нехватки хотя бы одного правила до завершения верификации, вычисление считается неполным, а сама верификация неопределённой. На практике, уже маленькая модификация программных операторов или свойств единиц спецификации, может привести к существенному изменению системы вычисления [62], [67], [68]. Это свидетельствует о большой сложности системы верификации. Пример 1: согласно ограничению № 6 отсутствие статических переменных или рекурсивных процедур может всё равно привести к полной программе, в зависимости от того, какая реальная часть программы рассматривается, и какие комбинации допускаются. Пример 2: полнота верификации программ с внутренними процедурами в общем недействительна, когда хотя бы одно из ограничений 6 или 7 не соблюдается. Если два правила приводят к различным результатам, т.е. из данного состояния A выводится $A \vdash B_1$ и $A \vdash B_2$, при этом B_1 и B_2 синтаксически различны, но свойство диаманта соблюдается, то B_1 и B_2 являются лишь промежуточными состояниями и оба состояния сходимы. Проблема проверки сходимости методом конечного отслеживания может оказаться неэффективным, т.к. во время верификации необходимо проводить экспоненциальное количество под-доказательств. Эту проблему можно избежать, если детерминировать все правила. Также Кларк приводит следующее ограничение для устранения неполноты:

- Огран. №9 частично-вычисляемые структуры данных.

У частично-вычисляемых структур данных все поля вычисляются в момент доступа. Типичный пример взят из [255] на языке Хаскель о потенциально бесконечных линейных списках.

```
take 10 [ (i,j) | i <- [1..], let k = i*i, j <- [1..k] ]
```

вычисляет

```
[(1,1),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(3,3),(3,4),(3,5)],
```

однако, определение линейного списка как второй аргумент от функции `take` не имеет лимита. Данная структура определяет множество, которое имеет только нижний порог (это целое число 1), но не имеет верхнего порога. С помощью частично-вычисляемых структур, можно проверить, насколько строго вычисляет данная процедура. «Строго» подразумевает, что данная процедура сначала вычисляет все входные параметры, а затем их записывает в память, а не строгие процедуры означают, что входные параметры

вычисляются частично и только тогда, когда они требуются на данном этапе алгоритма (см. [256], [255]). Таким образом, из этого можно сделать вывод, например, проверить терминацию программы можно, используя бесконечно определённую структуру данных в качестве быстрого теста.

Уэнд [265] подразумевает под полнотой функции определения Кука, уточняя, что каждый верный параметр на входе соответствует верному параметру на выходе, а каждый не верный параметр соответствует ошибке. То есть, переходная функция должна быть тотальной, и все не терминирующие функции не определены по умолчанию (см. опр.1.6). Уэнд показывает, что спецификация программы, представленная графом потока управления тогда не определена и не полная в общем случае, когда для описания графа используется логика высшего порядка. По Уэнду квантифицируемые предикаты должны давать «понятное определение» самым лучшим образом так, чтобы человек прочитав лишь спецификацию, мог бы сразу и интуитивно охватить полностью замысел предиката.

Кук [68] сравнивает решение проблемы выполнимости булевых формул с теоретическими оценками решения проблем верификации. Статья представляет теоретические пороги сложности. С практической точки зрения, статья не пригодна по двум причинам. Первая причина - пороги слишком грубые и поэтому для применения недостаточны. Вторая причина - основной характер статьи — это философский дискурс познавательного характера.

Лэндин [152] предлагает элементы формального вычисления преобразовать в выражения λ -термов, как это было изначально предложено Чёрчом. Под формальным вычислением можно также подразумевать вычисление Хора. Лэндин на примерах условных переходов и рекурсии показывает, что термы полностью покрываются. Более того, он показывает, что программы на основе функциональной парадигмы [255], [35] могут быть представлены также в программе на императивном языке программирования с помощью замыканий (с англ. «closure») и на основе операционной семантики. То есть, представляются обобщённые модели вычислимости, о которых важно знать при моделировании систем верификации.

Исходя из опыта последних декад, Апт [15] определяет некоторый обобщённый диалект Си с редуцированным множеством программных операторов для анализа полноты и корректности. В дополнении ранее обсуждаемых работ, Апт видит общую рекурсию, как наиболее важную проблему, которую трудно прогнозировать в отношении следующего состояния программы. Поэтому, он предлагает ограничиться примитивной рекурсией. Также Апт предлагает допускать только те

вызовы процедур, у которых актуальные параметры совпадают с формальными параметрами, например, «инкорректные параметры» исключать, т.к. они могут послужить целому ряду аномалий. Например, неверное разделение, неинициализированные поля, а также полученный функционал в связи с отсечением параметров при вызове, могут полностью поменять семантику процедуры, но принципиально не решить ни одну проблему. С помощью урезания параметров можно сильно варьировать семантику и заметно изменять синтаксис.

Кук [67] и другие упомянутые авторы рассматривают две основные проблемы полноты:

- Полнота №1 Незавершение вычисления процедуры.
- Полнота №2 Ограничение выразимости языка утверждений (например, предикаты и инварианты).

В виде примера корректных и полных правил Хора, Кук выделяет рисунок 8 (Кук использует обратную запись скобок, как и Хор). На рисунке A_j представляют программные операторы, D является блоком декларации переменных, σ является переменной средой, а $*$ обозначает звезду Клини. σ имеет тип:

имя переменной \rightarrow значение

В дополнении к ограничению Хора 6, надо отметить принципиальное ограничение:

- Огран. №10 не автоматически выделенные переменные

Ранее уже упоминалось, что подключение глобальных, статических и динамически выделенных переменных, может аннулировать правила Хора. Далее, локальные переменные используемые в некоторых нитях одновременно, могут также аннулировать правила, т.к. аспекты параллельного вычисления в общем не могут быть покрыты, например, правилами Кука. Тема этой работы посвящается однопроцессорному вычислению, а не параллельному запуску программы.

Для полной индустриальной применимости, необходимо включить обработку исключений, которые просто так не вписываются в существующие правила и довольно трудно формально корректно и полностью охарактеризовать не только, но и в целом из-за возможного изменения стека при каждом программном операторе по-разному (см. [84], [107]). До сегодняшнего дня не было найдено предложение о вычислении Хора, которое позволило бы (корректно и/или полностью) отматывать динамическую память, аналогично стеку [107].

Хор [116] считает абстракцию спецификации самой главной преградой для верификации мало тренированным инженерам, которые желали бы

быстро научиться верифицировать простые примеры. По Хору тяжело формализовать утверждения для программных меток, безусловных переходов и передач параметров по имени. Он не настаивает и не опровергает использование любой логики, любого порядка, однако, он считает декларативную спецификацию утверждения решительным фактором успеха.

Автоматизация логического вывода: Цель этого раздела заключается в введении и демонстрации практических и теоретических проблем автоматизированной верификации. В этом разделе мы рассмотрим примеры в системе верификации «Coq». В Coq [32] можно доказывать заранее специфицированные утверждения с помощью теорем, различных индуктивно определённых структур и различных команд на основе типизированного λ -выражений второго порядка. Утверждения задаются на функциональном языке «Gallina», а последовательность доказательств задается языком последовательных команд «Vernacular». «Coq» является ассистентом доказательств потому, что часто он сам не в состоянии полностью и самостоятельно, даже для простых примеров, находить доказательства. Вместо этого, в «Coq» имеется множество узкого круга поддерживаемых теорий, которые можно подключать в работающее ядро ассистента. Ассистент позволяет записывать и отслеживать доказательство и выявлять промежуточные состояния доказательства.

В последовательность команд включается набор так называемых «тактических команд». Они пробуют текущее представление программного состояния упростить полу-автоматически, используя рассматриваемую теорию. Теория вещественных чисел, например, используется для ускорения сходимости, результатом чего является, либо завершение доказательства, либо упрощение состояния вычисления. «Coq» — довольно мощная и широко используемая платформа для верификаций, что в области автоматизации доказательств теорем, можно встретить не так часто. Применение также включает в себя верификацию корректности фреймворков компиляции [225], [157], [41], [42], [158], [159], [215].

Формулы из логики предикатов задаются языком «Vernacular».

«Coq» использует при редукции нормализованные формулы, которые могут быть не определены или не полностью определены. «Coq»-схемы основаны на ленивой редукции на вычислительной модели λ -вычисления второго порядка (см. [55], [203], [179]). Разумеется, что из-за произвольного вида правил, естественно не может быть гарантии касательно полноты. Типизация λ -вычислений позволяет избегать целый ряд парадоксов типизации, в связи с рекурсивными определениями Канторовских множеств (см. [22], [34]), как термы содержавшие сами себя.

Отсутствие типизации может приводить, к парадоксу Расселя о брадобрея.

Примерами корректно определённых $T_{\lambda 2}$ -типов, являются например, $\forall a.a$ или $(\forall a_1.a_1 \rightarrow a_1) \rightarrow (\forall a_2.a_2 \rightarrow a_2)$.

Корректно определёнными $\Lambda_{T_{\lambda 2}}$ -типами являются, например, $\Lambda a.\lambda x : a.x$ или

$$\lambda x : (\forall a.a \rightarrow a).x(\forall a.a \rightarrow a)x.$$

Редукция (β -редукция, см. [22]) λ -термов проводится как применение возможно неопределённого терма к данной λ -абстракции, например:

$$(\Lambda a.\lambda x : a.x) \text{ Int } 3$$

можно редуцировать к $(\lambda x : \text{Int}.x) \ 3$, далее редуцируется к «3», при этом Int тип целых чисел, т.е. множество V .

Задача редукции $T_{\lambda 2}$ -термов заключается в: (1) вычислении результата и (2) проверке типов вычисления. Проверка типа отличается от задачи верификации, отсутствием состояния.

Ради простоты, в определении базовые правила были упущены, т.к. универсальность разрешает их определить более обобщёнными не типизированными λ -вычислениями [22], например, аксиома $\bar{\Gamma} \vdash x : t$ или правила (\exists -Intro) и (\exists -Elim), которые определяются аналогично (\forall -Intro) и (\forall -Elem).

Так как Coq основан на $T_{\lambda 2}$ и редукция редексов производится снаружи во внутрь, то проблема проверки типов решима. Сложность проверки линейная. Для стратегии редукции с внутренней стороны к внешней, в общем случае, проверка не решима (см. [203] и [32]).

Рассмотрим относительно простой пример «исключённого третьего» на рисунке 9. Пример тавтологии $p \vee \neg p$ можно считать интуитивно понятным, но при отсутствии логических таблиц и при использовании только правил импликации — так оно положено в интуиционистском суждении логических утверждений, задача может оказаться гораздо труднее. В зависимости от набора правил, тавтология Пирса может быть в принципе не выводима.

Рассмотрим пример из рисунка 9. Нам необходимо доказать, что первое определение reigse , которое обходится без дизъюнкции и отрицания, но содержит импликацию « \rightarrow » может быть преобразовано в определение lem . Обратим внимание, что оба определения содержат квантифицируемые утверждения. Доказательство является последовательностью команд, начиная после ключевой команды Proof и заканчивая перед ключевым словом Qed (перевод с латинского «quod erat demonstrandum» означает, «что и требовалось доказать»). Сначала имеется лишь теорема о равенстве обоих теорем, затем обе стороны

равенства развёртываются. Затем firstorder пробует сопоставить \forall -квантифицированные утверждения преобразованные в нормальную форму Сколема. Теперь необходимо доказать на правой стороне определения lem , что для любого предположительного верного утверждения p , $p \vee \neg p$ также верно. В этом случае, левая сторона является доказуемой гипотезой $H = \forall p,q.((p \rightarrow q) \rightarrow p) \rightarrow q$, которую необходимо доказать для любых утверждений p и q . Сейчас $p \vee \neg p$ заменяется p , q сопоставляется $p \vee \neg p$. Таким образом, мы получаем $(p \vee \neg p \rightarrow \neg(p \vee \neg p)) \rightarrow p \vee \neg p$ — в качестве доказуемой текущей гипотезы, по-прежнему условию, что p является верным утверждением. Теперь, чтобы доказать верность гипотезы, необходимо следствие reigse отделить от предусловия. Необходимо текущую гипотезу абстрагировать и затем опять преобразовать в нормальную форму Сколема, чтобы q более не являлась квантифицируемой переменной. Затем мы получаем новую более простую гипотезу $H_0 = (p \rightarrow q) \rightarrow p$, которую нам удастся доказать, если предположить, что из $H = \forall p.p \vee \neg p$ правая часть дизъюнкции верная. То есть, мы вводим новую гипотезу $H_1 = \neg p$. Такой выбор произвольный и применив $\neg p$ к H_0 , нас сразу приведет к тому, что p верное, потому, что импликация всегда верна, как только левая сторона импликации ложная. Так как мы предположили изначально, что p является верным утверждением, мы доказали правоту теоремы. Тактика tauto обязательна для успешного завершения доказательства теоремы, которая из данных существующих гипотез и верных утверждений пытается простейшим образом, механически найти завершение доказательства без каких-нибудь дополнительных знаний о теореме или используемых лемм.

Обратим внимание на то, что, хотя пример простой и интуитивен, успешное доказательство все-таки требует довольно не малых ресурсов для преобразования в нужную форму. Для применения одной или иной тактики требуется также применение, не очевидных формул абстракций. Не трудно заметить, что автоматически такого рода нестандартные преобразования будет очень тяжело выявить и распознать.

Если правила Хора полны и удастся провести доказательство из аксиом до доказуемой теоремы, то доказательство может быть автоматизировано. Если правила Хора полны, то любая теорема может автоматически доказываться — ответ, либо положительный, либо отрицательный. Чтобы выразить формальную теорию, необходимо определить: семиотику, синтаксис (см. например опр.1.8), семантику. Когда речь идёт о языках, а формальная теория обозначается именно выражениями некоторого языка, целесообразно определить прагматику. Семантики, например, аксиоматичная семантика,

обозначают в формальной системе, например в вычислении Хора, какое выражение выводимо или нет. Знаки и взаимосвязи формул являются абстракцией некоторых реальных предметных объектов или физики (классический термин был введён в аналогии реальных объектов, которые принадлежат естественным правилам природы). Поэтому, описание элементов «физики» исторически часто называется метафизикой, т.е. абстрагированной физикой, либо логикой. Необходимо отметить, что любая формальная логика также является по определению специфической формальной алгеброй.

Аналогично модульному программированию, доказательства могут строиться с целью упрощения и выявления основных мыслей доказательств. Более подробное обозначение находится в следующих главах. Для аналогии послужат единицы доказательств леммы (вспомогательные теоремы), теоремы и индуктивные определения. Самым простым примером индуктивного определения можно считать естественные числа (см. рисунок 10).

Мы не будем отдельно описывать тактики, т.к. тактики лишь вспомогательные образцы последовательности команд при доказательствах. Они лишь имеют некоторый абстрактный характер для упрощения написания доказательств. Абстракция предикатов, для написания и восприятия человеком, имеет большое значение. Можно в общем считать: чем проще доказательство, тем оно лучше. Символы и предикаты могут быть использованы и их определение необходимо развёртывать, лишь при необходимости. Исходя из текущего состояния вывода и сочетаемых правил, желательно было бы автоматизировать принятие решения системой верификации — когда развёртывать определение и когда свёртывать часть данной формулы обратно к определению. Количество и порядок развёртываний и свёртываний заранее не предсказуемо. По ранее упомянутым причинам, лучше редуцировать термы лениво и снаружи во внутрь, иначе текущая редукция может приостановиться, хотя имеются редексы.

Из рисунка 9 можно выявить: следующие проблемы касательно автоматизации доказательств.

- 1) Описание проблемы соперничает с выразимостью. Это может привести к серьезным ограничениям выразимости и к раздутым описаниям.
- 2) Упрощение равенств косвенной теории раздувает объём и количество правил Хора, хотя, например, арифметическая теория не связана на прямую с состоянием памяти или программными операторами. Это также препятствует автоматизации.
- 3) Объяснения при отрицательном выводе, либо отсутствуют полностью, либо желают лучшего,

например, интуитивный и обобщённый метод генерации контрпримера.

Подробнее ознакомиться с проблемами автоматизации доказательства теорем можно в статьях Воса [280], [279], несмотря на возраст статей, до сих пор проблемы в основном остаются актуальными. Проблемы Воса можно разбить на три класса: (i) представление модели утверждений, (ii) представление правил вывода, (iii) выбор оптимальной стратегии и тактик логического вывода. Для повышения эффективности верификации, Вос предлагает вводить параллелизацию, индексацию баз данных и знаний для более быстрого доступа и обработки данных, а также анализировать модифицированные технологии вывода. В статьях можно обратить внимание на следующие, часто неявные, замечания Воса:

- Проверка типов может быть полезной с целью избежания статических ошибок, но на самом деле бесполезной для верификации.
- Нотация формул, возможно, не столь важна, но охватить семантику (императивную) программы важно.
- Хотя метод резолюции широко обсуждается в статье, естественный вывод все-таки рассматривается как более эффективный, особенно на практике, чем, например метод резолюции. Причину этому, наверное можно искать только в близости к классическим математическим доказательствам.
- Существует соперничество между локальным и глобальным поиском оптимума в доказательствах.

Из всех проблем, которые Вос выявляет [280], наиболее важной можно считать избавление от избыточных формул при спецификации, а при верификации от избыточных частей повторного вывода. Главный лозунг Воса: «Лучше упрощать утверждения, чем перебирать различные варианты». Эвристика Воса считает в худшем случае лучше с полиномиальной частотой проводить упрощения насколько возможно, чем рисковать экспоненциальный взлет поискового пространства проверки. Вос исходит из 90% сбережений. Престон [212], ссылаясь на Воса, ожидает, что удовлетворительное исследование каждой из первоначальных проблем Воса [279] займёт объём работы, как одна диссертационная рукопись. Овербейк [191], ссылаясь на [279], даёт каждому из перечисленных проблем обзор практических примеров. Мекок [165] является старой, но не устаревшей в целом, обзорной статьёй. Галлье [102] является более актуальной и подробной монографией по теме автоматического доказательства. Его проблемы совпадают большей частью с обсужденными. В [160] Леруа задаёт вопросы к общему процессу верификации и даёт критические оценки с практической точки зрения, его оценки совпадают в основном с

упомянутыми. Он, Апфель и Докинз [14] предлагают обществу разработчиков и исследователей соблюдать общие принципы при разработке верификаторов для простого сравнения между собой.

Абстрактная интерпретация. Кусо(-вые) [74] [73] предлагают первыми формальный метод (см. опр.1.12) «абстрактной интерпретации», как универсальный статический метод, основанный на аппроксимации пошагово вычисляемых интерпретаций данной программы. Метод анализирует граф потока управлений [189] данной программы. Если граф не нормализован, т.е. либо нет ровно одного состояния входа, либо одного состояния выхода, то граф преобразуется именно в такой, объединив входные и выходные состояния. Программные операторы упорядочиваются не строго согласно алгебраической решётке по порядку операторов. С помощью абстракции, интерпретация пытается приблизить лимит [6] ради введения новых зависимых параметров с помощью ограниченного случая (сужения диапазона видимости) и с помощью общего случая (расширения диапазона). Таким образом, неинициализированные переменные имеют порог $[-\infty .. \infty]$. Процесс пошаговой аппроксимации интерпретации считается завершённым, как только, две последовательные интерпретации равны. Интерпретации обновляются после каждого программного оператора. Из-за проблемы приостановки интерпретации могут иметь не предсказуемые, т.е. арифметически очень большие, либо очень маленькие лимиты, например, в циклах с неопределёнными значениями переменных при входе в цикл. Статическое вычисление допустимых порогов значений [189] является одним классическим применением. Методы Кусо могут быть модифицированы и применены в самых различных областях, например, в [252] для улучшения быстродействия в связи с предсказыванием более оптимального ветвления запуска кода. Чтобы сравнить равенство между двумя абстрактными интерпретациями, вводится условие для изоморфизма изображений. Две интерпретации I_1, I_2 считаются эквивалентными, когда существуют два отображения α, α^{-1} , которые инъективны и сюръективны, с которыми интерпретация I_1 преобразуется с помощью α в I_2 , и I_2 обратно в I_1 с помощью α^{-1} . Хотя метод Кусо(-вых) универсален, его можно было бы автоматически с трудом преобразовать в правила Хора и наоборот из-за целого ряда причин. Во-первых, метод Кусо предполагает аппроксимацию, а правила Хора знают только точные результаты, либо символьные значения. То есть, можно было бы расценивать систему правил Хора, как частный случай метода Кусо(-вых), хотя цель метода направлен все-таки на арифметическую аппроксимацию интервалов.

Во-вторых, для верификации вычисления Хора, используются термовые утверждения некоторого языка спецификации и т.д. Комментированный пример абстрактной интерпретации находится на рисунке 11.

Штайнбах [247] демонстрирует наглядно, что терминация является жестким условием, предположением сходимости (например, применив алгоритм Кнута-Бендикса) и полноты, а сам вопрос терминации в частных случаях является решимым.

Кроме упомянутых ограничений, отдельно от этого, имеется теоретическое ограничение в связи с арифметикой Пресбургера. Арифметика Пресбургера является настоящим подмножеством более известной арифметики Пиано над натуральными числами, которая знает только об операции «+» (или инверсная ею операция минус) [244], и где любые другие операции отсутствуют. Это приводит к тому, что «простые входные программы» содержавшие плюс, можно в выражениях за конечное время решить в предикатной логике первого порядка (например, в решении офсета для ссылочных указателей, см. позже), в отличие от выражений по арифметике Пиано или сложнее. В частности, это имеет значение для решимости автоматического доказательства теорем [69], [61] (см. набл.1.13). Решимость выражений из арифметики Пресбургера ограничена $\Theta(m, n) = 2^{2^{n \cdot m}}$, где n минимальное количество предлагаемых разветвлений поиска, а $m \geq 1$ некоторый константный фактор [95]. Сложность разрастает очень быстро для n . Важно заметить, что несоблюдение арифметики Пресбургера, например, включение дальнейших операторов, на практике не обязательно приводит к нерешимости частных случаев, однако, соблюдение арифметикой может сильно снизить верхний порог решимости доказуемых теорем.

Поммерель [210] оценивает теоретические критерии сложности и приходит к выводу, что неэффективные реализации прикладных теорий являются самым большим барьером эффективной верификации. К примеру, он приводит состояния моделирование троек Хора в качестве огромных линейных систем уравнений, строки чьи, почти все пустые. Ситуацию можно переломить, если прикладные теории изолировать от правил Хора. Рекомендуются использовать решатель, который упростит анализ полноты основных (логические) и прикладных правил (структурные). Из практического опыта, решатель резко повысит эффективность решения прикладных теорий [188]. Решатели запускаются во время верификации при необходимости. Примерами решателей являются функциональные языки «Why» [272] и «Y-not» [187].

Альтернативные подходы: Как было упомянуто в начале главы, верификация является формальным методом с помощью которого, можно проверить, соблюдает ли данная программа спецификацию или

нет. Верификация троек Хора является статическим методом без запуска программы. В зависимости от точности спецификации для достижения максимально качественного уровня ПО при разрастающейся сложности и функциональности данной системы, на практике может потребоваться добавление, уточнение и сокращение специфицируемых свойств. Необходимо заметить, что сокращение правил происходит всегда тогда, когда правила обобщаются, т.е. отпадает необходимость специфицировать детально. Кроме представленного подхода в прошлых разделах, упоминались ряд иных статических подходов, как, например, проверка моделей и локализации проблемы с помощью удаления синтаксического и окружающего кода. Также имеются динамические подходы, как, например: тестирование, безошибочная разработка программного обеспечения и расширенная проверка типов.

Подход №1 – Тестирование. Тестирование является динамическим подходом проверки ранее подготовленных сценариев, в которых данная программная система или модуль (не) вычисляет ожидаемый результат. Сценарии это тесты, которые задаются разработчиком вручную и описывают свойства по отдельности. Когда тест успешен, следующий тест проводится до тех пор, пока все тесты выполнены. Тест, это критерий качества, который (не) соблюдается при запуске программы. Если хотя бы один тест не успешен, то тестирование провалилось. Когда сценарий теста известен, то, все, входные данные и выходные результаты, сравниваются согласно данному модулю. Если при проведении теста требуется ручное вмешательство, то тест не автоматизирован. Автоматизация теста (АТ) [24] дает существенные преимущества: высокая эффективность, т.к. за короткий промежуток времени можно проверить большое количество тестов. Далее, исключаются ошибки из-за неточных входных данных. Все внешние зависимости должны описываться тестом. Если тесты простые, то модули можно легко понять и вероятность выше, что ошибки отсутствуют.

Для данной программы p и набора тестов $\forall i.t_i(p)$, каждый из тестов запускается для p и наблюдается, либо успех, либо провал. Каждый из тестов можно рассматривать как утверждение одного аспекта функциональности ПО. Недостатками АТ можно считать ручную постановку, в зависимости от сложности графа потока управления p . Число n необходимых тестов p_1, p_2, \dots, p_n для покрытия всех ветвей может сильно возрастать. Чем сложнее получается граф в частности, когда граф содержит обратные связи и циклы, тем сложнее ПО в общем.

Подход №2 – Автоматическая проверка моделей. Основной проблемой подхода №1 является экспоненциально возрастающий объём тестов, который трудно автоматизировать для представительного

множества тестов. Идея проверки модели заключается в описании данной программы с помощью утверждений и временных выражений, которые затем проверяются пошагово, изучив выполнимые входные. Проблема заключается в том, что решения дискретных проблем часто не тривиальные и могут быть выявлены, либо с большими затратами, либо вовсе не могут быть выявлены. Если уравнения сильно ограничиваются, то вероятность высокая, что результаты пропускаются. Если уравнения слишком обобщённые, то результаты тоже могут теряться или быть не найденными из-за отсутствия быстрого нахождения, либо отсутствия решения в принципе. К уравнениям модели, которые описывают булеву формулу выполнимости и при правильных результатах всегда верна, применяется стратегия поиска для расширения найденных результатов [63], согласно данной формуле. Отсутствие эффективной стратегии поиска равномерно к незавершению или к очень медленному завершению проверки [143]. Предлагается целый ряд оптимизаций, как например символьное использование [63] при работе с моделями или статистические методы над контролем расширения [148]. Программные инструменты включают в себя, например «VDM++» [271], [270].

Альтернативно к аксиоматическим правилам можно назвать (автоматическое) тестирование [167] и проверку моделей, как это было впервые введено Пеледом и Кларком [63] ([147] [270] представляют собой обзоры современных инструментов). Преимущество тестирования, в отличие от проверки моделей, является простота проверки поведения программы без дополнительных формул, но, проблема полного перебора всех возможных тестов, остается без изменения в обоих случаях.

Подход №3 – Безошибочная разработка программного обеспечения. Альтернативой ранее представленных подходов можно считать «программирование вообще без ошибок», при котором не требуется статическая или динамическая фаза проверки, точнее фаза проверки проводится одновременно с моделированием ПО, упираясь на знакомые и «хорошие» паттерны [136]. Если ошибок мало или ошибки незначимые с точки зрения быстродействия в не критическом месте, то естественно количество ошибок будет стремиться к нулю. Если количество программных строк приближается к нулю, то и количество возможно совершенных ошибок будет приближаться к нулю – эти утверждения всегда в силе, независимо от конкретной программы и не требуют дополнительного объяснения: пустая программа содержит минимальное количество ошибок. Ошибки в программе создаются человеком. — Почему? При создании программы полностью исключить «человеческий фактор» по определению не возможно: ПО и спецификация задаются человеком. Ошибки

в программах тоже создаются человеком. Отладка и обнаружение возможных ошибок проводится человеком. Абстрактные типы данных, алгоритмы и интуиция — всё это свойственно для человека. Разработка и описание модулей и интерфейсов ПО проводится человеком. Следовательно, не удастся исключить человека при написании ПО, но могут иметься подходы, которые пытаются исключить ошибки на более ранней стадии при создании ПО.

Разработка ПО. Вопрос об отсутствии ошибок в ПО на раннем этапе нужно искать при построении и моделировании, например с помощью языка моделирования «UML» и «OCL». На практике много раз доказано, что с помощью тщательного моделирования можно избежать множество типичных ошибок, но увы, не всегда и не все виды ошибок это покрывает потому, что:

- индивидуальности предполагаемого разработчика, создание ПО является творческим трудом человека.
- трудности в предсказывании ошибок со ссылками и в том числе, из-за трудности локализации проблем.

Преобразования. Задача проверки корректности трансформаций структур данных заключается в соблюдении корректного перехода от одного графа к другому [87], соблюдая программные операторы. Подход похож на позже представленную модель динамической памяти в отрезках. Однако, внутри описывается и работает трансформация как «система переписывания», поэтому в дальнейшем она не будет рассматриваться. Системой переписывания является, например «Stratego XT» [125] или [294], [87]. [132] предлагает использовать эвристики систем переписывания для лучшей сходимости верификации программ.

Подход №4 – Проверка типов. Проверка типов исключает большинство ошибок, которые могут возникать из-за некорректного применения типов переменных и выражений. Например, присвоение 32-разрядного целого числа, 8-разрядному числу плавающей точки, в лучшем случае, может «проглатить» или быть безобидным, а в худшем случае, может привести к совершенно иному числу, если интерпретируются и копируются только все передние 8 от 32 битов.

Задача проверки типов заключается в выявлении проверки совместимости данных и выявленных типов в выражениях программных операторов. Однако, если проверка типов соблюдается, то можно сказать, что семантическая сходимость типов соблюдается. Из совместимости типов не следует утверждать, что данный цикл «правильный». Для того, чтобы можно было это утверждать, необходимо сначала определить свойство, а затем проверять. Увы, проверка типов является лишь предыдущим шагом

перед верификацией. Проверка типов не содержит информацию о зависимостях данных и тем более не содержит никакой информации о том — какие, на каком этапе и сколько объектов будет выделено в динамической памяти. Эта информация проверяется на этапе «статического анализа» и является независимой от этапов построения программы:

Проверку типов можно задать как $\langle \Gamma \vdash e : t? \rangle$, где Γ переменная среда содержащая термы вместе с типами, является проверяемым термом и t является проверяемым типом (см. [22]). Для проверки, имеет ли данная последовательность программных операторов e тип t , используя аксиомы и правила типизации Γ , необходимо проверить каждый из операторов в e . В отличие от троек Хора, термам представляющие программные операторы, присваивается тип, т.е. множество допустимых значений. В отличие от вычисления Хора, проверка типов только устанавливает принадлежности к множеству возможных значений, т.е. к некоторому типу и проверяет сходимость типов. Частное значение некоторого объекта не специфицируется. Имеются исключительно программные операторы и типизированные выражения. При проверке типов отсутствует также понятие как «состояние вычисления», при корректной типизации состояния, либо выводимы из набора правил Γ типизации, либо нет.

Аналогично вычислению Хора, проверка типов проводится снизу-вверх, т.е. проверка начинается с данного e и успешно завершается в случае вывода. Проверка типов является проверкой узкого круга свойств программ, т.е. является сильно ограниченной формой верификации троек Хора. Проверка типов программы является обязательной семантической проверкой программы, которая должна проводиться до любых других семантических проверок, как например, верификации свойств динамической памяти. Как мы увидим позже, представленные модели динамической памяти, также как и другие семантические фазы исходят из того, что выражения при присвоении годные, иначе нельзя считать входную программу корректной, как тот язык программирования интерпретируется строго согласно спецификации, например [243].

Если далее сравнивать проверку типов по Хиндлей и Миллнеру [115], [203], [48] с тройками Хора, то необходимо заметить, что при проверке типов, предусловие всегда самое универсальное, а значит верное. Далее, при проверке типов, имеются фундаментальные проблемы, которые являются следующими эквивалентными проблемами при проверке упрощённых троек Хора (см. глава IV на рисунке 13).

Были предприняты расширения, которые

позволяют: проверять совместимость записей, ужесточение типов, свойства неприсвоенности и статические лимиты объёмов базисных структур данных [96]. Но для проверки свойств динамической памяти, увы, даже те упомянутые расширения, совершенно здесь не достаточны. Например, приведем правило последовательности:

$$(\rightarrow\text{-elim}) \frac{\Gamma \vdash e_1 : (s \rightarrow t) \quad \Gamma \vdash e_2 : s}{\Gamma \vdash (e_1 e_2) : t}$$

Правило ($\rightarrow\text{-elim}$) наглядно демонстрирует, что указание типа (например, $s \rightarrow t$) может служить как элементарное утверждение процесса верификации (см. [58], [186]). В [22] широко представлены доказательства всех важных теорем и лемм λ -вычисления в связи с определением его синтаксиса и семантики, в том числе, кратко о проблемах и ограничениях не типизированного и типизированного λ -вычислений. Статья [207] посвящается вопросам теоретической нерешимости редукции λ -термов в общности без явной типизации (например, в вычислениях Карри, в отличие от вычислений Чёрча). Например, терм $\lambda x.xx$ не может быть решён в общем, но при типизации становится очевидно, что данный терм не принадлежит регулярной типизации. Если бы $\lambda x.xx$ был типизирован, то допустимый второй терм x имел бы некоторый тип t_2 , а первый x обязательно должен иметь некоторый тип функционала $t_0 \rightarrow t_1$, что невозможно приравнять к t_2 в типизированном λ -вычислении первого порядка, в котором типы далее не специфицируются. Следовательно, $\lambda x.xx$ не типизируемый терм. Однако, можно сконструировать в качестве бесконечно приближенного типа лимит [166]. Этот тип соответствует рекурсивно определённый абстрактному типу данных, который имеет в общем случае зависимость (возможно, рекурсивную) к другим типам данных и представляет собой тип данных записи.

Подход №5 – Автоматическая редукция проблемы: Автоматическая редукция проблемы пытается редуцировать строки программы, чтобы данная ошибка, либо иное поведение программы, например «результат функции возвращает 5», сохранялось. То есть, если некоторая программа вычисляет некоторую таблицу, используя различные формулы, а нас интересует только одна ячейка в ней (например, единственная с ошибкой), то можно весь код удалить, который не нужен для вычисления той самой критической ячейки. Таким образом, получается редуцированная и более простая программа, которую можно легче анализировать. Очень часто бывает, что ошибка в программе связана лишь с маленькой частью изначальной программы. Увы, особенно в больших или незнакомых программах, локализация программ занимает очень много лишнего времени.

Допустим, мы строим проект одной командной

строкой. Вместо «GNU make» [100] ради простоты, используется сильно упрощённая программа для построения любого ПО «builder» [304]. Для автоматизации и редукции входной программы используется программа «shrinker» [305]. Программа работает циклически: строит ПО, анализирует или запускает ПО, сравнивает наблюдаемое поведение программы с ожидаемым результатом. Если программа после сокращения по-прежнему строится, запускается и сравнение успешное, то редукция продолжается, иначе редукция проваливается. Если редукция проваливается, то, либо берётся другая редукция, либо прежняя (успешная), как окончательная. Программа при запуске выдаёт всё, что важно на «stdout» и «stderr». Уговаривается по умолчанию, что любое другое поведение можно записывать в «stdout» или «stderr», в том числе, интересующее нас поведение программы (так называемый «симптом»), без ограничения общности. Если симптом всё ещё наблюдается при запуске программы, то поведение инвариантно и мы «пробуем» сокращать, далее пока не останется возможности. Предложенный подход описывается на рисунке алгоритм №1. Представленный алгоритм наивный и не оптимальный, т.к. выбор *lineseq* не детерминированный и может содержать любое количество строк, равно хотя бы одной или более строк. Нужно заметить, что объём выбранных строк может расти, но также уменьшаться со временем, когда варианты редукции отклоняются несколько раз подряд, в зависимости от стратегии редукции.

Объектные вычисления

Объектные вычисления представляют собой формализм для различных вычислений с объектами. Вычисления могут в себя включать, например, совместимость типов, проверку верности условий. Объектные вычисления можно разделить на два вида, по Абади-Карделли и по Абади-Лейно (см. рисунок 14).

Итак, зачем на самом деле нужна формализация объектов? Почему нельзя сопоставить объекты простыми переменными? Отвечая на второй вопрос первым: да, можно сопоставить на самом деле. Однако, в связи с введением объектов поля, больше абстрагируются. Вследствие этого, алгоритмы упрощаются и обобщаются. Класс объектного экземпляра, это прежде всего, «абстрактный тип данных» (АТД), а не только хранитель данных. АТД также является носителем множества объектов, предусмотренные для решения комплексной проблемы (см. [156]). Операции над объектом замкнуты, т.е. сам объект не может распадаться на некоторые другие объекты при запуске операций. Поэтому программист, при написании обязуется, определять в объектах лишь те операции, которые к нему подходят и которые

действуют только на внутреннем состоянии всех полей самого объекта – поля других объектов не доступны. Это подразумевает разделение данных аналогично записям. Операции объектов на практике, это методы классов, а объект, это объектный экземпляр.

Объектно-ориентированная парадигма популярная, и успешно использовалась в индустрии на протяжении последних десятилетий, опираясь на АД. Одним из преимуществ АД является — возможность строить надёжное, гибкое, интуитивное и быстрое ПО за счёт технологии моделирования, как например «объектно-ориентированное моделирование» (ООМ) [77], [229] или «паттерны» [136]. Перечисленные методы и идея широко применяются в индустрии до ныне. Нельзя недооценивать важность использования паттернов на практике, которые способствуют к существенному снижению ошибок при написании кода, благодаря четкому распределению ролей вовлечённых объектов. Паттерны программирования являются стереотипами, т.е. эпистемологическим механизмом - идиомой, которая способствует человеку «быстрее» воспринимать во времени вовлечённые объекты и связывать их, для решения поставленной задачи, не читая весь программный код полностью. Многие классические, философские идеи и течения вовлечены в представление объектов, как, например атомизм, коннективизм и т.д. Паттерны можно интерпретировать, как сравнение объектов ООМ с ролями актёров сценария, для решения определённого сценария: каждый актёр в определённой ситуации ведёт себя так, как этого требует «манускрипт», точнее спецификация. Прагматизм паттерна повышается, если сценарий можно объяснить лучше и понятнее.

Объектное вычисление может быть использовано для семантических анализов, например для проверки типов или для верификации, что будет представлено чуть позже. Кроме того, оно может послужить анализу зависимости полей данного объекта, например для эффективного распределения процессорных регистров. В частных случаях может иметь смысл, все объектные поля преобразовать в массив или отдельные локальные переменные, если граница массива известна и не велика [44] и размер объекта не велик. При распределении регистров, зависимость данных на прямую определит какие регистры будут использованы (например, регистры общего пользования) или стековые поля. Быстрые ресурсы, т.е. процессорные регистры, в разы быстрее, чем доступ к операционной памяти, однако, они сильно ограничены по объёму и ёмкости. С другой стороны, процессорные регистры, в зависимости от архитектуры ЭВМ, могут, согласно двоичному интерфейсу приложений «АВІ» (см. [252], [253], [160]), временно хранить только несколько слов. Слова ограничены и тем не менее, имеющийся АВІ обычно не делит общие блоки памяти представляющие объектные экземпляры потому, что при компиляции трудно

предугадать точно, когда и где, какие поля будут или не будут использованы. Однако, если возможно было бы это уточнить, стоило бы модуль предсказания «GCC» в этом плане улучшить, т.к. на данный момент всегда принимается отрицательный прогноз. Реальность такая, что объекты остаются неделимыми и если памяти не остаётся, то всё выкладывается на стек, что тормозит и желает иметь лучшее.

Вычисление записей [90] отличается в основном от объектов тем, что они являются чистыми хранителями данных. Запись можно рассматривать, как кортеж различных типов, что может быть полезно для описания вычислений одновременных процессов. Скотт [236] характеризует любой тип данных (т.е. в обобщённом виде, в качестве кортежа) как алгебраическую решётку, которая имеет инфимум как изначальное (возможно не инициализированное) значение и окончательный результат (возможно параметризованный), как супремум и все состояния между обоими экстремальными точками объясняются, как состояния кортежей, которые соблюдают порядок вычисления. Для более подробного ознакомления применения и обоснования верификации с объектами, особенно в связи с нединамическими переменными, можно ознакомиться в [58] и [182]. Для дальнейшей дискуссии в качестве примера мы приведем работу [23]: условия верификации задаются формулами логики предикатов первого порядка. Атрибутные поля моделируются, либо отдельно, т.е. атрибуты выделяются в отдельные регионы памяти, либо встроено в содержащий объект, т.е. все поля и типы известны. Наиболее комфортабельным вкладом работы можно считать предикаты `rack` и `unpack`, которые свёртывают, либо развёртывают предикат вручную. Аналогично к [23] и [58], рекомендуется моделировать зависимые поля, как отдельные зависимые объекты. Обе работы предлагают ввод новых утверждений для инвариантов объектов, которые всегда верны до тех пор, пока некоторый объект жив. Никакой из упомянутых подходов не имеет отношения к указателям (см. глава II).

Вычисление объектов классных экземпляров упоминаются только коротко. Этот вид вычисления доминирует современные языки программирования, как, например, Ява или Си(++) [252], [243]. Класс используется для генерации объектных экземпляров при запуске программы. В этом разделе нас пока не интересует область выделенной памяти. Используются командные операторы `new`, `malloc` и `calloc`. После короткой характеристики, мы переходим к обыкновенному виду вычисления объектов.

Оба вида вычислений представляют возможность проверки типов и спецификации/верификации программных операторов. Абади и Карделли мотивируют предложенное вычисление

необходимостью формализовать вычисление с объектами из-за различных эффектов, как подклассы, полиморфизм и замкнутость/рекурсия объектных типов. Оба автора ссылаются на систему типизации лямбда-вычислений как одним примером второго порядка. Нужно заметить, что λ -термы, представляющие объекты, могут быть использованы, как квантифицируемые типы (т.е. типовое множество классов, которое выражается знаком \forall , см. [203], [48]) с помощью неопределённых символов. Далее, рекурсивные и нерекурсивные классы требуют уточнения структуры. Другими словами, «зависимые от новых параметров типы», которые представляются абстракцией λ -типов высшего порядка дополнительную абстракцию над объектными типами по Абади-Карделли.

Без ограничения модели памяти, например, в каком регионе операционной памяти содержится объект, или, где объект расположен в соответствии материнского объекта: внутри и снаружи, любой объект по модели Абади-Карделли имеет указатель. На рисунке 15 x указывает на объект, который имеет один внутренний объект, а он опять же имеет два содержания abc и def и некоторое содержимое ghi . Кроме того, имеется указатель y , который ссылается на объект содержащий jkl , при этом, объект x содержит некоторое поле (или любое из подполей одного из полей), которое ссылается на содержимое от y , т.е. jkl .

Классная иерархия наследования представляет собой упорядоченное множество, инфимум чей по конвенции пустой класс, например `Object` или `[]`. То есть, любые два класса из иерархии можно сравнить с самим собой, два класса, которые ничего не связывает и не связаны между собой, т.е. имеются следующие сравнения порядка наследованности: \sqsubseteq , $\not\sqsubseteq$.

Абади и Карделли лишь предоставляют возможность наследования в своей модели вычисления, также как и делегация или внутреннее представление полей и объектов. Использование ключевых слов `self` и `super` в языке Си++ [243] допускается, однако, использование подлежит к заранее проводимому семантическому анализу контекста ссылаемого класса. Эта предосторожность сильно увеличивается, вместе с целым рядом других способов вычисления, при использовании обыкновенного объектного вычисления. Карделли замечает, что дополнительные накладные расходы в связи с проверками актуального и ссылочного класса, например, при использовании `self`, приводят к принудительным проверкам всей иерархии классов, которые можно было бы избежать, если контекст достаточно однозначен. Нужно отметить, что на практике это замечание не столь важное потому, что определение класса по иерархии не является критической проблемой при компиляции программы. Поиск наследованности по иерархии слияния фактически является поиском по дереву, что

можно сделать за счёт $\Theta(n) = \log(n)$ в худшем случае. Это вполне достаточно. Серьёзным ограничением наследованности, является угадывание, какой именно метод будет запускаться. С вопросами практической и теоретической реализации наследованности множества классов на языке Си++ можно ознакомиться в работе Рамана [216].

Методы объектов содержат код, который доступен только объекту. Ради простоты, мы смоделируем автоматически выделенные методы, которые в отличие от статических методов, означают, что методы доступны исключительно тогда, когда соответствующий объект был ранее выделен оператором `new`. В случае статичных классов, нет необходимости доступа к заранее выделенной памяти объекта, т.к. переменные в стековом окне выделяются глобально независимо от объекта. Далее, обозначим по умолчанию, что любой объект, если не уговорено по другому, всегда имеет один метод «конструктор» для построения объекта и инициализации нейтральным значением всех полей (что записывается в отдел `.ctor` на ассемблере, в случае языка Си++ [243] при переводе) и один аналогичный метод утилизации объекта, который записывается в `.dctor`. Таким образом, можем определить следующие фазы объектов (см. рисунок 16), которые нам послужат в качестве спецификации:

Только что были обсуждены пункты 1 и 2. Пункт 3 касается любого состояния «немёртвого объекта». Объект немёртвый, когда он «жив», это когда программный оператор вызывается после момента конструкции, но до утилизации объекта. Пункты 4 и 5 подразумевают ту самую спецификацию, как у процедур. Ради применимости пытаемся избежать принудительную спецификацию всей программы. Обозначим это «лёгким» подходом, но пока что не будем рассматривать такой вариант. В целях увеличения гибкости и локализации проблем, уговаривается по умолчанию, что любые «дополнительные» утверждения разрешаются, которые также могут быть упущены (пункт 6).

Методы в обоих вычислениях изначально не ограничиваются. Однако, не ограниченные методы также могут включать в себя изменение методов в любой момент запуска программы, удаление существующих методов и добавление новых методов. Очевидно, что при неограниченном вычислении спецификация становится всё сложнее, и возможные изменения трудно, или даже теоретически и практически не решимы. Следовательно, максимальная возможность приводит к жесткому ограничению верификации.

Как было упомянуто, неограниченные методы не дают и не расширяют с теоретической точки зрения «Тьюринг-вычислимость», изменения методов при

запуске («динамические методы») и умолчании далее не рассматриваются. Когда речь идёт о динамических методах, только тогда, они могут рассматриваться.

Системы объектных вычислений имеют следующее логическое суждение:

$$E \vdash obj : A :: B$$

где, E объектная среда, содержащая существующие объекты в момент актуального состояния вычисления программы, obj является объектным представлением (т.е. переменной в вычислении №1, а целым объектом в случае вычисления №2). A является типом obj (т.е. наименование класса объектного экземпляра obj). B является спецификацией объекта obj , которая содержит, например, состояние объекта. Если вместо obj проводится вызов метода $obj.m()$, то B содержит состояние obj до и после вызова m , но B также может далее содержать утверждения из рисунка 16, которые не противоречат данной фазе программного запуска. На результаты до и после запуска программного оператора или метода, можно сослаться с помощью встроенных вспомогательных операторов и регистра специального назначения, который содержит, либо весь объект (в случае №2), либо объектное поле. В центре объектного вычисления стоит объектное суждение вместе с типом и утверждением. Отметим, что B может меняться и при этом A , т.е. типизация, остаётся без изменения. Это становится актуальной проблемой, когда сигнатура/тип дальнего метода знакома, но само состояние нет. Это тот случай, когда используется архитектура веб-сервера или драйвера, когда известно как метод должен выглядеть, но детали функциональности не (полностью) известны.

Отметим, что обе модели, Абади-Карделли и Абади-Лейно, не поддерживают изначально ссылочные указатели на любые объекты, которые были бы выделены во время запуска программы. Указатели будут рассматриваться позже, однако, уже сейчас обсудим, что избегая лишние операции копирования, можно существенно улучшить быстродействие, если гарантированно, что некоторые объекты разрушаются и эти объекты не будут использоваться далее, или все копии объекта остаются без пользы.

Классовые типы T определяются рекурсивно. Тип — либо целое число, либо состоит из классов. Классовый объект содержит поля f_i и методы m_j и все наименования отличаются друг от друга согласно конвенции. Все поля имеют некоторый тип T . Методы имеют $T_j \rightarrow T_{j+1} \rightarrow \dots \rightarrow T_k$ в качестве типа сигнатуры.

Далее рассматривается вычисление №2, объектное вычисление по Абади-Лейно.

Язык программирования «Baby Modula 3» [2] был предложен Абади и компанией «Digital Equ-

ipment Corporation» в качестве экспериментального модулярного языка. Он содержит минимальный набор операторов языка Modula 2, который очень близок к синтаксису и семантике языка Паскаль, с дополнениями для прототипизации языка объектного вычисления обыкновенного вида. Язык похож на предложенные и далее расследованные языки Абади, Карделли, Лейно и содержит все необходимые единицы для μ -рекурсивных схем: присвоение и рекурсию. С более подробными дискуссиями на тему модели объектов и выразимость объектов можно ознакомиться в [111], где имеются чуть устарелые, но значимые статьи по данному вопросу. Целью ввода иного вычисления является альтернативное представление формализации. Однако, имеется эквивалентность обоих видов, которую можно доказать методом «полной абстракции» [179], [209], [65], [117], при которой необходимо доказать эквивалентность денотационной и операционной семантик [9], [290], [6], [276], [250], [34], касательно наблюдаемого поведения объектов. Доказательство изложено в [220], [222] и следует отметить, что в целях простоты модель Абади-Карделли описывается в разы проще. Кроме того, попытка доказать полную абстракцию увенчается успехом, но за счёт очень сложной операционной семантики в объектном вычислении. Это можно обосновать тем, что возможные рекурсивные типы гораздо проще вывести, если рекурсия содержится лишь в наименованиях типов, т.е. классов, чем определяется рекурсией объектных экземпляров.

Синтаксис языка «Baby Modula 3» определяется с помощью термовых выражений a как определено на рисунке 17, где A является типовым выражением.

Термовое выражение эквивалентно к выражениям языков «Modula» или «Паскаль» и не нуждается в дополнительных объяснениях, кроме: $\text{fun}(x : A)b$ определяет анонимную процедуру (эквивалентно к λ -абстракциям) с одним входным параметром x с типом A . В общем разрешаются анонимные процедуры с нуля или более параметрами. Переменная x является в теле процедуры b связанной переменной. Вызов процедур, например $b(a)$, подразумевает, что типы последующих аргументов совпадают с типами декларации процедуры. Пустое значение nil совместимо со всеми другими типами указателей. Например, не инициализированные объектные поля равны nil . Объектное расширение добавляет поля с указанным значением к предлагаемому объекту, таким образом, что объекту добавляется новое поле. Методы также расширяемы. Метод может обновляться, т.е. код метода может также как и переменная меняться во время запуска программы. wrong является резервированным ключевым значением, который показывает на неверное вычисление. Данным определением объекта всегда является вектор, который состоит из лексикографически

упорядоченного множества пар из наименований полей/методов вместе с содержанием. Содержание опять же может быть объектом, которое определяется аналогично определению из рисунка 17.

Семантика «Baby Modula 3» определяется аксиоматически и проводится двумя шагами: сначала проводится проверка типов (один набор правил), затем верификация с другим набором правил. Проверка типов объектов также требует определение на подкласс, которое может проводиться по-компонентно: $A <: B$ тогда и только тогда, когда B содержит все поля и методы с наименованиями как в A . Из-за отсутствия классовых идентификаторов в объектном вычислении, рекурсивные объекты необходимо симулировать подобно случаю «комбинаторам плавающей точки» в λ -вычислениях, которые имеют похожее ограничение. Итак, смешано-рекурсивные объектные определения выявляются с помощью искусственного комбинатора $\mu(X)$ для любого объекта X к данному объектному выражению согласно рисунку 17, который приписывается после $\mu(X)$ τ , таким же образом, как аппликация λ -термов, например, $\lambda x.x\tau$.

Следовательно, для проверок объектов имеются: переменные среды, подтипы (в том числе подклассы) и общие структурные правила. Ими производятся проверка типов и верификация объектов (см. позже, ср. минимальную логику вычислимости «LCF» [209]). Ради простоты (см. [155]) часто ссылаются на структурные операционные семантики [208], хотя, как было упомянуто ранее, преобразование в/из денотационной семантики(-е) в общем случае остается тяжелой проблемой.

Однако, μ -определения объектов — существенная проблема, т.к. для одних и тех же начальных данных вывод может быть различным, т.е. некорректность очевидна. Приведем в качестве примера правила из рисунка 18.

То есть, правила с рекурсивными определениями могут быть подорваны и недоказуемы из-за возможных расходящихся доказательств, при этом, лишь тривиальное решение, т.е. неподвижная точка, может действовать единственно «надёжным» путём. Такая обстановка, увы, не удовлетворительна. Это как раз и есть причина, почему объекты в вычислениях Абади-Лейно в общем не могут быть типизированы в вычислении типов первого и второго порядка. Разрешить эту проблему возможно, если правила верификации и проверки типов обогатить дополнительными правилами, которые сильно зависят от контекста. Это резко ухудшит простоту правил. По Абади-Лейно классы как таковы, не существуют. Объекты могут иметь произвольное число полей других объектов, следовательно, классы могут зависеть от других классов, включая от собственного класса. Это поражает тип третьего порядка, а вычисление эквивалентно λ_3^{\rightarrow} (см. опр.1.11). Поэтому,

сходимость и замкнутость по типу имеет большое значение для решения при статическом анализе классического типа [2]. Если сходимость конечная и процесс верификации перечисляем, то таким образом, можно сложить все перечисленные типы вместе, в одну запись. Таким образом, новой записью является тип объединяющий все зависимые типы. Авторы [2] обращают внимание на то, что любые операции полученные объединением типа замкнуты и все полученные (под)-типы также могут использоваться как базисный объектный тип. То есть, полученный объектный тип является идеалом, опираясь на сравнение объектов «<:», см. позже.

Язык программирования представленный в [4] (см. рисунок 19) является упрощением языкового представления рисунка 17, однако, присвоение отсутствует, а вместо этого имеется символьное присвоение и некоторый дополнительный синтаксический сахар условного перехода. Далее, динамические методы запрещаются. Синтаксис определяется следующим образом:

Переименование во время запуска разрешается, если оно соблюдается вызывающей и вызванной сторонами. Локальные переменные в процедурах запрещаются. Также запрещаются параметры методов, которые меняются внутри методов. Для выразимости это не является ограничением, т.к. это всегда можно симулировать с вводом дополнительных полей. Особенность присвоений заключается в том, что присвоения полей возвращают в качестве результата объект, в котором некоторому существующему полю было присвоено значение. Важным ограничением в отличие от [2] является по Абади-Лейно в частности, исключение рекурсивно-определённых объектов.

Отношение подтипов определяется в рисунке 20.

где A' это некоторый класс, а A соответствующий подкласс.

Соотношение $<:$ позволяет вместе с другими правилами проводить проверку типов, например, самое главное — это правило объектного построения:

$$\begin{array}{c} A \equiv [f_i :: A_i^{i=1..n}, m_j :: B_j^{j=1..m}] \\ E \vdash \diamond \quad E \vdash x_i :: A_i^{i=1..n} \\ E, y_j :: A \vdash b_j :: B_j^{j=1..m} \\ \text{(CONS)} \frac{}{E \vdash [f_i = x_i^{i=1..n}, m_j = \psi(y_j)b_j^{j=1..m}] : A} \end{array}$$

где A некоторый объектный тип (не класс), E это объектная среда, x_i некоторые значения полей, а b_j некоторые значения методов, т.е. тела процедур. Проверка верности программы по упрощенному Абади-Лейно проводится согласно следующему суждению:

$$\sigma, S \vdash b \rightsquigarrow r, \sigma'$$

где σ является начальным состоянием стека, S описывает состояние стека, b данная

последовательность программных операторов («программа»), r является результатом, который сохраняется в виртуальном регистре неограниченной ёмкости, и σ' описывает финальное состояние памяти. Спецификации объектов определяются рекурсивно по компонентам:

$$[f_i : A_i^{i=1..n}, m_j : \psi(y_j)B_j :: T_j^{j=1..m}],$$

где A_i, B_j это спецификации, y_j параметры анонимных процедур ψ используемые в B_j, T_j , а T_j определяет спецификации перехода памяти из одного состояния в следующее.

Суждение спецификации определяется по $E \Vdash a : A :: T$, где E это объектная среда, программа, A тип, T переходное описание. То есть, проверка типа по A и переходные состояния записаны в B и применяются одновременно, если даже технически по разным этапам, всё равно не трудно увидеть, что B окажется сильно раздутым и незначительное изменение памяти может привести к большим последствиям. Предложенное соотношение $<:$ [4] аналогично применяется к спецификациям. Аналогичные проблемы распространяются на спецификации. Например, требуется доказать очевидную программу: $\emptyset \Vdash ([f = \text{false}].f := \text{true}).f : \text{Bool} :: (r = \text{true})$. Дерево доказательства с аннотациями использованных правил находится в рисунке 21.

Определения использованных правил находятся в рисунке 22.

Утверждение \diamond обозначает истину. Корректность представленного набора правил можно прочесть подробнее в статье [2] и в её сопровождающей технической статье. В подходе Абади-Лейно необходимо отметить, что ситуация с абстракцией желает иметь лучшее. Параметры в методах видны только снаружи во внутрь, но не наоборот, например в $b_1 \equiv \text{let } x = (\text{let } y = \text{true in } [m = \psi(z)y]) \text{ in } x.m$ внутренний y не может быть проверен снаружи, согласно правилам из [2] и разница между предикатами (какого именно порядка и ограничения) и утверждениями всё-таки не достаточно ясна. Абади и Лейно предлагают в качестве дальнейшей работы следующее: улучшение абстракции спецификации, исследование меняющихся параметров, а в связи с этим, вопросы о полноте, использовании указателей на объекты и на поля объектов, а также более детально разобраться с рекурсивно-определёнными объектами. На данный момент не вычисление по Абади-Карделли и по Абади-Лейно не обращают внимание на указатели или псевдонимы (см. позже).

Оба вида вычислений страдают от того, что отсутствует поддержка указателей. В [3] перечислены важные и нужные расширения: поддержка параллельности, возможность ссылаться на адресные поля и

использования абстракции в спецификациях, так как впервые это уже заметил Хор [116].

Банерий [21] представляет язык, который поддерживает объекты, размещённые в стеке и в том же регионе памяти (см. [258]). Подход в [21] перемещает все локальные переменные в стек, но висячие указатели по определению языка не допускаются. Рекурсивные предикаты над объектами запрещены. Особенность глобальных инвариантов заключается в не меняющихся зависимостях между объектами. Он предупреждает о сильно возрастающей проблеме абстракции и поддерживает инициативу по-объектного взгляда индивидуальных предикатов.

Программные нити.

В [4] объекты квалифицируются как абстрактные типы данных, но только не как обыкновенные вычисления записей [90]. Отличие определяется в первую очередь не по имеющимся полям, а по структуре данных. Записи имеют любые зависимости к иным записям.

Переходы из одного состояния записи в другое, можно получить с помощью применения правила редукции. Таким образом, трансформации графа можно рассматривать как редукции с записями. Эриг и Роузен предлагают подкласс процедур, который безопасен тем, что он не смешивает зависимые поля объектов вместе с анализом с помощью теории категории. Их подход можно считать «безопасным» при запуске нескольких нитей одновременно, если доступ к подмножеству полей объекта не зависит друг от друга. Таким образом, авторы дают возможность к более эффективному доступу полей, без необходимости полной блокировки при много-поточных программах. Поэтому, процедуры порождения и утилизации, при соблюдении условия, могут запускаться одновременно без изменения поведения и корректно. Похожие подходы к доступу объектов представляются более подробно в [127].

Хойсман [120] задаётся также вопросом параллельного доступа к объектам, также как и Хурлин [121] и [90]. Хойсман пытается с помощью «контрактов между объектным взаимодействием» дать возможность не только определить полный или никакой доступ к методу класса, но также подключить временные условия доступа. Хойсман предлагает подключать в спецификацию историю объектов и вызовы методов. Также предлагается объединить описание различных объектов при отдельных стереотипах и совместных действиях объектов, т.к. предложенный вариант видимо страдает от необходимого уровня абстракции, в первую очередь, для параллельного запуска методов объектов.

Фреймворки.

Для достижения цели проверки спецификаций целых программных комплексов, представляются иные формальные подходы (см. опр.1.12). Один из наиболее широко известных и популярных подходов,

является подход Мейера «о делении ответственности» [175]. Мейер [172] предлагает, как и многие до него, методологию «модулярный подход», аналогично принципу Лискова и принципу скрытия по Парнасу. В алгоритмах связанных между собой, актёрам ответственности приписываются стереотипы, согласно которым, выполняются ранее определённые роли. Определение ролей в соответствующей онтологии участников и взаимосвязей позволит лучше охватить и понимать объектную структуру. Принцип Мейера можно вкратце охарактеризовать как:

Чем сильнее деление ответственности [каждого из единиц онтологии], тем более таким объектам, можно доверять.

Замысел заключается в том, что, чем меньше становится программа, тем сильнее редуцируется её сложность, если изначальную программу не менять (кроме сокращения). Например, метрика, в том числе по Мак-Кейбу, вычисляет показательное число, которое оценивает сложность графа управления данной программы. Чем сильнее разбита программа на маленькие легко-контролируемые и логически связанные между собой единицы, тем проще получается граф потока управлений. Метрики можно сравнивать, т.е. и сложности двух программ. Заметим, что объект, который кажется на первый взгляд простым, может в реальности иметь зависимости с любыми другими объектами, которые заранее неизвестны. Такие «неожиданные зависимости» часто на первый взгляд скрыты и их трудно обнаружить. Неожиданные связи уже являются признаком тому, что в отличие от данной спецификации, данный объект вероятно содержит ошибку или серьезную не выявленную проблему. Неожиданные связи соединяют часто отдаленные объекты между собой, что для простых моделей и алгоритмов маловероятно и приводят к ситуации, когда два объекта связаны между собой, хотя на самом деле не должны быть связаны.

Рилэ [227] предлагает вводить тесты, покрывающие спецификации для обнаружения отклонений объектов и взаимосвязей между объектами, так называемые «коллаборации». Проверяются взаимосвязи между объектными модулями с помощью спецификаций, например, «модульной алгеброй» [30] или «компонентной алгеброй» [93], [239], [259]. Эти подходы формализованы и описывают интерфейсы между классовым объектным и иными экземплярами. Описание интерфейсов, увы, ограничивается лишь входными и выходными параметрами методов. В [94] предлагается подход навигации по объектам, согласно данной спецификации. В [30], [93] и [17] предлагается добавлять последовательность вызовов методов в качестве утверждения, для избежания ошибок в связи с не правильным порядком вызовов методов.

Это предложение похоже на подход Хойсманой. Далее, программы, часто страдают от того, что их необходимо специфицировать целиком. Это очень неудобно, когда речь идет о средних и больших программах. Фактически, все представленные подходы исключают указателей из языка программирования, т.к. любые утверждения о программе могут просто оказаться ложными. Порядок вызовов методов может оказаться практически значимым не только внутри одного объекта, но а также для целой сети объектов, например: исключение возможности вызова метода m_2 первым объектом, до тех пор, пока не будет вызван метод m_1 третьего объекта. Программисту важно помнить в какой момент безопасно вызывать метод, а когда требуются инициализации или иные вызовы и в каком порядке. Это нужно рассматривать как постоянную «классическую» проблему при изучении любого нового фреймворка. Вместо детальной и длинной спецификации с практической точки зрения, хорошо бы иметь спецификацию, которая статически обнаруживает соответствующие зависимости между объектами и порядком загрузки.

Язык объектных ограничений «OCL» [1] является расширением языка «UML». Он графический и текстовый де-факто стандарт по статическому и динамическому моделированию ПО. «OCL» позволяет добавлять формулы взаимосвязей, например, ограничить связь типов связанных между собой объектов. Формулы описывают в основном лямбда-термы второго порядка предикатной логики (см. опр.1.9), т.е. с атомными типами. Кроме ранее упомянутых ограничений в разделах, остаётся отсутствие возможности специфицировать указатели.

Сафонов [231] представляет и анализирует целый ряд примеров из области компиляции и связанные с ней проблемы. Цель анализа заключается в постановлении критерий доверительных компиляторов. Необходимо заметить, что автор выбирает компиляторы преднамеренно, т.к. они являются по сложности одними из наиболее сложными ПО. В этом можно убедиться, например, с помощью тщательного анализа кода, особенно переходы и ответвления, например используя метрики. Сложность проверки для данного компилятора заключается в том, как определить, что любая преобразованная программа верна и оптимальна? Для получения этого, Сафонов ссылается на метод Мейера о делении ответственности. В качестве контр-аргумента можно привести, например подход Леруа из проекта «CompCert» [31], который также исследует корректность, но также частично быстроедействие. Увы, подход не имеет, большого практического значения из-за слишком резких практических ограничений. — Поэтому, по Сафонову, можно выявить следующие критерии значимые на практике и которые решают уровень приемлемости:

- Верный и понятный диагноз ошибки, включая

генерацию контр-примеров.

- Трансформация моделей, включая объекты, предпочитается переход между моделями из-за относительно малых затрат спецификации.
- Возможность расширять и модифицировать объектные модели вычисления.
- Использовать формальные описания, если применимость от этого не страдает. В частности, Сафонов считает полноту покрытия формальной модели и локальность спецификации важными критериями.
- Абстрактные типы данных описывают собственные инварианты объектов.
- Промежуточные представления должны быть достаточно гибкими и абстрагированными так, чтобы они могли быть использованы на различных этапах верификации.

Модели динамических куч

Преобразование в стек: В разделе I-V в связи с объектными вычислениями уже велась небольшая дискуссия о преобразовании в стек.

В [258], [257], [274] расследуется функциональный подход, в котором все переменные перемещаются в стековое окно (в [52] приводится формальное доказательство корректности подхода Тофти и Тальпина [258]). Реализован подход Гросманов диалектом Си «Cyclone» при поддержке языка «ML» (также см. [109]). Регоин определяется как совокупность связанных элементов динамической памяти, которые, например, при удалении полностью могут утилизироваться в один раз. Стековое преобразование, в частности, должно следить за диапазоном видимости, чтобы исключить нечаянного уничтожения, согласно автоматическому выделению и утилизации стека. В [98] обсуждаются диапазоны видимости за пределами стекового окна и демонстрируется расширение в системе «Cyclone». При перемещении переменных, необходимо следить за интервалами годности, иначе полученные «псевдонимы» и «возможно-псевдоним» могут стать ложными. Функциональный подход исключает динамические списки как параметры, рекурсивные структуры данных и процедуры, которые возвращают функционал. Все типы функций должны быть определены при компиляции. Мейер [173], [174] считает, что кроме корректности программы, важным является быстрый сбор мусора (см. [153]). Поэтому он предлагает, по-возможности, целиком избавляться от динамической памяти и переоформить алгоритмы для работы только над стеком. Как уже было предложено в [258], вталкивание в стековое окно не занимает большие затраты при минимальных объемах. Он требует, чтобы к абстракции объектов необходимо уделять больше внимания и предлагает использование вспомогательных переменных для

уменьшения спецификаций. Корректность присвоений в статье полностью не доказана, а только для полного класса данных, как утверждается в статье. На самом деле, присвоение может оказаться ложным, когда, например, допускаются изменения программного кода во время запуска программы. Доступ к содержимому в стеке может быть быстрее, чем в динамической памяти, но всегда требует дополнительные затраты на вталкивание и выталкивание в стек и из стека, которые, в зависимости обсуждаемого алгоритма, могут резко снизить общее быстродействие так, что использование динамической памяти может быть быстрее [12].

Анализ образов: Главной целью анализа образов [232], [189], [199], [85], [275] является выявление инвариантов в кучах памяти при запуске программы, например, для обнаружения псевдонимов. Выявляются фигуры описывающие инвариантную и гибкую часть динамической памяти [275], например, для линейного списка [85] или двусвязного списка [60]. Граф зависимостей между образами всегда описывается полностью с помощью трансферных функций, таких как: пустой образ «пуст», присвоение полю или указателю и выделение новой динамической памяти. [232] вводит основные соотношения между двумя указателями: «псевдонимы», «не псевдонимы» и «возможно псевдонимы».

[199] замечает, что [232] и [189] могут привести в зависимости от данной программы, к не точному, а следовательно, к не правильному выводу, если для «если-тогда»-команды в одном случае вычисляется «возможно псевдонимы», а в альтернативном случае «псевдонимы», тогда результатом вычисления послужит «псевдонимы», хотя правильный ответ «возможно псевдонимы».

Более того, [199] содержит подробное сравнение подходов [232] и [189]. [199] оценивает [189], как более точный метод и предлагает оптимизацию путей по графам образов с одинаковыми началами и псевдонимами, в качестве более эффективного описания, которое одновременно и короткое. Предложенная оптимизация имеет верхнюю сложность $\Theta(n^2)$ и сокращает вычисление в среднем, примерно на 90%. Павлу предлагает симулировать более сложный анализ псевдонимов за пределами процедур, преобразуя, насколько это возможно, вызовы процедур и глобальные переменные в локально интра-процедуральные элементы через переименование. Подход в его работе был, на самом деле, уже ранее успешно применен в системе «GCC» для решения комплекса иных проблем. Павлу, так же как и я, считает, что контекст-независимые подходы в точном анализе псевдонимов, малоперспективны (ср. [113]), сравнив характеристики. Далее он предлагает оптимизацию отделения объединяющих вершин, которые образуют подграфы, от вершин, которые

твёрдо не содержат псевдонимы.

[192] представляет собой среду для визуализации образов куч для быстрого анализа и обнаружения инвариантов, редко используемых связей между образами. Для навигации по графу используются операции «абстракция графа» и «конкретизация графа» с помощью чего, удаётся подграфы свёртывать и развёртывать. Визуализация трансферных функций, которая приводит к развёртыванию/свёртыванию более одного подграфа, желает быть лучше, однако, ограничение принципиальное и следовательно улучшение не ожидается.

[54] представляет собой подход, основанный на распределении куч по образцам. Подход сравнивает предположительно подходящие начала правил по длине и выбирает наиболее длинное правило первым. Особенность подхода заключается в аппроксимации обеих сторон рассматриваемых правил для выбора принимаемых правил с помощью ограниченной абдукции.

Ротация указателей: [249] предлагает «ротацию указателей», которую можно считать безопасной, если: (1) содержание куч не меняется, (2) все элементы ротации годны до и после ротации (3) количество переменных не меняется. Преимуществом безопасной ротации можно считать отсутствие нужды сбора мусора, который определяется просто, но также эффективные операции над списками, как, например, копирование. Хотя ротация указателей в явной спецификации не нуждается, всё-таки минимальное изменение параметров может привести к трудно-прогнозируемому поведению программы, особенно часто, если указатели неожиданно оказываются псевдонимами. [249] предлагает базисный объём ротаций, однако, на практике этого далеко не достаточно, в следствии чего, необходимо компонировать индивидуальные ротации из базисных. Далее, ротации очень чувствительны к минимальным изменениям вызовов. Например, поменять местами аргументы, на первый взгляд — безопасная операция, но она может привести к полной утилизации всех входных списков. Неожидаемость также возникает часто с безобидными данными, например, когда один входной список пуст или ротации комбинируются.

Ротация может быть представлена как пермутация, где все её компоненты x_j являются указателями:

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{n-1} & x_n \\ x_2 & x_3 & x_4 & \cdots & x_n & x_1 \end{pmatrix}$$

К примеру рассмотрим из рисунка 23 модифицированный пример ротации из [249].

Это соответствует линейному списку с тремя элементами следующей сложной трансформации, которая состоит из шагов (№1–№4), см. рисунок 24.

В зависимости от входных данных, можно выявить отдельные свойства, которые иногда тяжело обобщать,

но иногда просто, как на примере `rotate(x,x,y)` является тождественным отображением, т.к. `tmp:=x; x:=y; y:=x; x:=tmp;`. Очевидно, даже маленькая модификация может привести к негодности свойств, а следовательно свойства симметрии могут быть нарушены, а следовательно доказуемые свойства больше неверны, например, `rotate(x,y,x-next)`, т.к. x и $x^{\wedge}.next$ связаны и пересечение между y и $x^{\wedge}.next$ не полностью исключено априори.

Файловая система: Граф кучи отображается в файловую систему так, что вершинами являются файлы, а зависимости между ними — ярлыки (например с помощью команды `ln -s` под Линуксом). Папки могут быть использованы как хранитель объектного экземпляра. Содержимое вершины находится внутри файла. Таким образом, файловая структура имитирует графовую кучу. Теперь можно описать схему файловой системы, не отслеживая символьные ссылки. Полученный перечень имеет структуру дерева и может быть записан в качестве слабоструктурированной единицы, например, в XML-документ. Под Линуксом все операционные средства преобразованы в виде файла. Операции над файлами теперь соответствуют операциям над кучами. Задача верификации теперь может быть задана как проверка данного состояния файловой системы. С другой стороны, операции над файловой системой можно проверить на корректность с помощью (например, XML-) схемы, что явно может упростить ошибки или дефекты с большими и многими файлами. Во избежание траты времени на сравнение многих и больших файлов и папок, можно использовать команду `shasum` или `md5sum`, т.к. писание и чтение на носителе часто ограничивается физическим барьером.

Для проведения операций [294] и описания [299] может быть использован декларативный язык, основанный на Прологе. В выделенном примере из [294] высчитываются из верхней папки ровно два файла a (например, файлы с указанным префиксом) и высчитывается содержимое, которое должно совпадать в обоих случаях.

`template(element(top,_,[A,A]),[text(T)]):-`

`A=element(a,_,_),transform(A//p#1,T).`

Приближенный аналог на языке XSL-T является:

```
<xsl:template match="top[count( child::*)=2] and
a[1] and a[2]">
<xsl:text>
<xsl:value-of select="//a//p"/>
</xsl:text>
</xsl:template>
```


Побочные области

Основные определения псевдонимов, мусора и обсуждения находятся в разделе I-C. Далее представлены побочные области, которые в принципе могут быть добавлены к предложенному фреймворку из раздела IV-E и характеризуются как анализ указателей.

Анализ псевдонимов: Вайль [269] представляет наглядный обзор по тематике, несмотря на возраст статьи. По Вайлю анализ псевдонимов является побуждающим процессом приближения указателей, ссылающихся на одну и ту же ячейку памяти, которая может быть изменена из-за того, что создаёт множество псевдонимов с экспоненциальным ростом вариантов. Анализ псевдонимов за пределами процедуры гораздо тяжелее, потому, что необходимо анализировать все возможные вызовы и продолжения, в котором далее будут существовать переменные. Естественно, что в продолжении переменные так же могут меняться, и это является причиной трудного анализа. Чтобы упростить анализ, Вайль вводит ярусы псевдонимов, по которым оценивается сложность каждой программной команды.

[181] содержит полный обзор всех нынешних и прошлых анализов псевдонимов, в том числе свои собственные. Статья Мучника вместе со статьёй Вайля представляются самыми важными в области. Он делит анализы на зависимые от графа потока управлений и независимые, на «псевдонимы» и «возможно псевдонимы», а также на замкнутые подпрограммы и вызовы подпрограмм. Анализы псевдонимов по Мучнику можно уточнять, однако, классификация по сложности Лэнди [151] тоже ориентируется по диапазону видимости указателей.

В отличие от Мучника, Купер [70] предлагает, одним из первых, подход анализа псевдонимов независимый от графа потока управления. Главной мотивацией тому служит резкое упрощение алгоритмов, т.к. необходимо следить за указателями и операциями использования. Недостатком является неточность.

Стоит отметить, что система «GCC» [252] разрешает программисту языков Си устанавливать директиву для компиляции вручную, по которой возможно твёрдо исключать псевдонимы для определённой функции. Таким образом, генерируемый код становится более эффективным.

[118] является расширением подхода Мучника. С помощью битовых векторов, подход становится более эффективным. Общий подход улучшения анализа следует также искать в [137]. Более того, представленный подход анализа присвоений и использований может быть обобщён в подходе к «SSA» [76], [245], [289], [238]. Наим [183] утверждает, что улучшение доступа можно достичь через хеширование подмножеств псевдонимов. Остаётся отметить, что подход Наима содержит предпосылки и намерения

переписать проблему анализа псевдонимов как проблему «SSA». В общем следует отметить, что указатели не единственные переменные, которые трудно выявить при статическом анализе [242] за пределами процедур. Они являются одними из самых трудных проблем. Подход Сривастава полезен, независимо от всех остальных обсужденных работ, по причине, что глобальная оптимизация на уровне связывания кода, например, передвижение мало-эффективного кода или устранение ненужного кода часто не может полностью быть исключено во время предыдущих фаз компиляции.

[199] делит анализ псевдонимов на две методологии: подход с помощью «унификации» [246], который находит больше случаев «псевдоним» и на подход с помощью «плавления», который ради скорости слабее.

[150] и [214] задаются вопросом, почему сегодня анализ псевдонимов остаётся в общем не решённым. Ответ лежит в сложности выявления псевдонимов за пределами процедур и в ограниченности решаемости для случая «псевдонимы». В сжатых подграфах зависимостей наименование вершин остаётся общей проблемой в [232] и [189]. Далее, эти подходы имеют целый ряд ограничений, как например: доступ к указателям с индексом, разрешает лишь не переменные выражения; исключаются объектные указатели; запрещаются массивы с гибкой шириной; исключаются пересекаемые в памяти структуры данных (например, «union»-структуры на языке Си [243]).

Клинт [64] занимается верификацией программ, и его центральная проблема заключается в доказательстве сложности корректности псевдонимов в связи с со-процедурами. Работу Клинта можно считать одной из первых в этой области. Обобщённой областью Клинта можно считать верификацию с функционалами, в которой необходимо упомянуть работу [169] для указателей с логикой высшего порядка, и работу Поулсона [198], который пробует применить абстракцию процедур для принятия более эффективного правила при верификации с указателями.

Готсман [108] представляет подход приближения псевдонимов между процедурами с помощью модели ЛРП. Хотя статья представляет характеристики запуска и сравнения базисных оценок, для сравнения было бы интересно узнать о соотношении подходов Мучника и Купера.

Сбор мусора: Джоунс и соавторы [127] представляют, более чем полный, обзор на тему сбора мусора и детально обсуждают актуальные подходы с большим вниманием на параллельные алгоритмы, однако, это не цель данной статьи. Помимо первого выпуска [127], второй выпуск одноимённой монографии не только сильно отредактирован и представляет целый ряд новых параллельных подходов, но

практически одновременно является совершенно другой книгой. Стоит лишь упомянуть Уиттингтона, [277] в качестве обзора на тему, который сфокусирован в основном на многопоточные реализации сбора мусора, также как и Долигез [88]. Блэкбёрн [40] приводит сравнения наиболее важных сборщиков мусора, что также упомянуто в [127].

На мой взгляд, Апшель [12] прежде всего опасается на то, что на практике из-за архитектуры фон-Неймана и программного интерфейса «ABI» на кодовом уровне имеются ограничения с обращением к стеку, связи с копированием данных в и из стека. Апшель предполагает, что, в таком случае, выгоднее использовать динамическую память, но при условии, что либо вообще ничего не потребуется, либо меньше ресурсов, чем для стека (см. [258], [174]). Подход Апшеля заключается в многопоточной реализации с «копирующим сборщиком мусора» [127], который действует только, если было совершено изменение в данных, а зарезервированный превышает в семь раз объём свободных куч.

Несмотря на возраст [153], деление памяти на быстрый кэш и медленную, большую память принципиально остаётся в силе. Ларсон рассматривает «уплотняющий сборщик мусора» в зависимости от объёма освобождающей области (R), объёма активных данных (A) и объёма быстрой памяти (H). Он постулирует две оптимальные стратегии для быстрого действия и выделения/очистки динамической памяти: стратегия №1) Максимизировать R , если $A \ll H$ не соблюдается. Стратегия №2) Приравнять $R = H$, если $A \ll H$.

Кроме упомянутых в [12] ограничений, сбор мусора ещё имеет ограничение в связи с адресацией. Если речь идет о данных «XOR»-связанных структурах, то мусор не может быть локализован классическим методом потому, что адреса принадлежащих объектов (например, поля объектов или ссылки на последующий элемент в списке) получают не абсолютными, а относительными. То есть, для дважды связанного списка с помощью одного «оффсета», можно выявить следующий и предыдущий элемент, если таков имеется, вместо двух отдельных указателей, которые содержали бы два абсолютных адреса.

[128] предлагает сбор мусора по возрасту выделяемых ячеек, т.е. в зависимости от того, как часто выделенный объект употребляется и как долго он остаётся. Если объект используется редко, то через несколько итераций он уже может оказаться в менее быстром сегменте памяти. Если объект используется часто, то он, наоборот, перемещается в более быстрый регион памяти — это касается не только сбора мусора, а также запуска программ в целом [261], [181], [260], [217]. Быстродействие в среднем приближено к оптимуму, исходя из большого практического опыта и множества экспериментов.

[119] даёт оценки к нынешним технологиям «SSD»-дисководов. Операции доступа к «HDD»-дискам похожи на динамические кучи. Писание превышает длительность чтения в 10 раз. Сбор мусора на «SSD»-дисках при «жадной» стратегии, становится наихудшей при задержке на 45%. Самая худшая стратегия по производительности — писание всё новых блоков. А лучшая стратегия — писать последовательные данные без сбора мусора, по отдельности.

Кальканё [53] замечает, что программы высокого абстрактного уровня не всегда имеют преимущества по сравнению с программами, которые манипулируют динамической памятью. Например, замечается, что сбор мусора во многом неэффективен в функциональных языках программирования. Выходит, что маленькие программы «опасны» потому, что неверное использование с указателями может иметь побочные эффекты, но с другой стороны эффективны.

Подход Уэйт-Шора [234] классический и первозванный в данной области. Он характеризуется тем, что все элементы динамической памяти имеют счётчик активных указателей. Если, по каким бы то ни было причинам, ячейка вдруг более не жива, т.е. количество ссылающихся указателей становится ноль, тогда система управления (обычно ОС) активируется и принимает соответствующие шаги по утилизации ненужного объекта.

Ситуацию вокруг сбора мусора на данный момент лучше всего можно охарактеризовать: подходов имеется больше, чем достаточно, в общей сложности, как минимум 50 различных. Выигрыш через новое открытие на сегодняшний день кажется мало вероятным и бесперспективным, т.к. на данный момент сборщики мусора в системах эксплуатации могут быть запрограммированы так, чтобы они не мешали запуску программы с помощью нитей.

Интроспекция кода: Интроспекция означает, что при запуске программы единицы модуля определяются, например, код вставляется, меняется или добавляется во время запуска. Очевидно, что интроспекция фундаментально усложняет статический анализ, ради проблемы приостановки, а значит, и верификацию программы. Принцип интроспекции основан на решимости, которая приводит к загрузке, либо известного, либо внешнего неизвестного кода. В любом случае должен существовать механизм в заимосвязи, который определяет коммуникацию между вызывающей и вызванной сторонами. Например, в Си++ интроспекция основана на «RTTI» [243], в Яве [96] каждый объект содержит ещё, кроме полей и адресов, идентификатор в качестве смежной записи, которая читается при запуске.

Формэн [99] определяет интроспекцию программы на Яве, как возможность вычитания и модификации данных и самой программы во время запуска. Это включает в себя загрузку кода, который может

определился даже только во время запуска. Следовательно, это потребует, кроме запуска, ещё компиляцию кода во время запуска. Запуск совершается объектами из определённого загрузочного контейнера. Манипуляция и доступ к классам, объектам и их компонентам осуществляется с помощью зарезервированных операторов.

Чеон [59] даёт краткий обзор текущих и предложений вопросов интроспекции в области Ява. Вопросы частично ещё актуальны на данный момент. Так как запуск неизвестного кода представляет собой не только возможную опасность, но и сильно могут пострадать корректность и полнота. Печально было бы, если вдруг метод, именно для одного входного значения, вообще не работает, либо вычисляет неправильный результат. Для этого Чеон формулирует список предложений и важных обстоятельств, как например: (1) загрузка и избегание конфликтующих имен в контейнере, (2) при запуске доступ к объектам должен соблюдать типизацию, (3) спецификацию наследованных объектов очень тяжело понять и отследить, если иерархия наследованности велика, (4) спецификации обычно ссылаются на объекты в стеке и куче, как в таком случае быть при интроспекции с окнами стека, которые просто разваливаются, т.к. объектная замкнутость может нарушаться при интроспекции?

Главными областями применения интроспекции являются загрузка приложений или методы веб-серверов, загрузка и доступ к динамическим библиотекам, например [282].

Существующие среды

[224], [27], [223] представляют собой хорошее введение в ЛРП, в том числе при поддержке программных средств. ЛРП является подструктурной логикой [218], [219], [89], которая избавляется от констант, например, булевых значений и использует символы для структурных замещений, в качестве констант. В ЛРП структурными правилами служат, согласно [218], правила сужения, контракции и сопоставления, а константами служат ячейки динамической памяти (см. главу III). В правилах « \rightarrow » заменяется на « \star », которая разделяет две непересекаемые и различные друг от друга кучи, кроме того случая, когда уговаривается что-нибудь иное. Кучи в динамической памяти определяются индуктивно. Оператор « \rightarrow », например в выражении « $a \rightarrow b$ », определяет соотношение между переменным символом на левой стороне и выражением (например объект) на правой. Когда мы рассматриваем примеры ЛРП, то подразумеваем, что эти конвенции вместе с правилом фрейма соблюдаются. Правило фреймов означает, что если вызов подпроцедуры не меняет части куч, а именно раму обозначенной F , то в antecedенте достаточно доказать, что тройка Хора без F верна.

Рассмотрим к примеру правило фрейма над кучами, которые определяются позже:

$$(\text{FRAME}) \frac{\{P\}C\{Q\}}{\{P \star R\}C\{Q \star R\}}$$

Здесь P и Q являются пред- и постусловием, а R является кучевым фреймом, т.е. сложное утверждение, которое не зависит от выполнения C , а также, на чью верность C не имеет эффекта. Этот принцип является основой модуляризации и мы будем всегда исходить из того, что принцип в силе, кроме отдельно уговариваемых случаев. Если допускаются рекурсивные спецификации вместе с функционалами, то основные свойства фреймового правила могут нарушаться в связи с контекстом, который может меняться любой вызывающей инстанцией [36], [211]. Следовательно, рекурсивные спецификации, в таком случае, должны обобщаться.

[27] вводит вычисление на основе ЛРП с безграничной арифметикой в офсетах над указателями, с возрастающими массивами и рекурсивными процедурами. Например, $p+x$, где p указатель, а x переменное целое число, не решимо в общем. Оно представляет собой попытку определить области динамической памяти рекурсивно, с помощью замкнутого объёма встроенных правил. Бёрдайн и соавторы, лишь задают вопрос, не является ли типизация достаточной верификацией (см. набл.1.15)? Из статьи например следует, что нерешаемость безграничного использования указателей, приводит к не точному определению момента сбора мусора, даже для самых безобидных выражений в качестве офсетов памяти и к не точному выбору правил для верификации, которые управляются жадной эвристикой.

Борна [44] предлагает модель очень похожую на ЛРП, которую он называет «дальнее разделение» и которая преобразует объекты данных в массив. Таким образом, любое объектное поле получается индивидуальным указателем с конвенцией для наименования и идентичности. Для общего определения куч он постулирует, что необходимо использовать предикаты первого порядка.

Главной заслугой Хурлина [121] в ЛРП, является нововведенный паттерн для верификации доступа к кучам с многими потоками. Он предлагает разблокировать функции, которые улучшают производительность за счёт частичной блокировки сложных ячеек. Все кучи не нуждаются в полной спецификации, которую можно сократить, используя анонимный оператор « $_$ ».

Паркинсон [195], [194], [193] представляет объектно-ориентированное расширение подхода ЛРП [224] до Хурлина, используя Ява в качестве входного языка. Модульность и наследование моделируются с помощью «передачи собственности над вызовами» и «семейством

абстрактных предикатов». Модель доступа Борна [44] применяется, т.к. свойство непрерывности наблюдается у правила фреймов для объектов. Он замечает, что зависимость между предикатами создает порядок вызовов предикатов. Из статьи можно выявить, что его предикаты разрешают определить всю динамическую память и стек, но они не разрешают, например, определить любые предикаты первого порядка. Предикаты утверждения, которые сильно отличаются синтаксисом и семантикой от входного языка, не ограничены в типах, однако, использование символов имеет целый ряд ограничений, которые связаны с несимвольной реализацией сопоставления переменных символов. Фактически, предикаты используются как локальные переменные в императивных языках программирования — это существенное ограничение. Для дальнейшего расследования, он предлагает: вызовы методов из родительских классов, статические поля, интроспекцию объектов, внутренние классы и кванторы над предикатами.

Система верификации «Smallfoot» [27] является первым верификатором на основе ЛРП. Она работает чисто экспериментально и имеет маленький объём встроенных предикатов для определения куч. Система сильно ограничена в представленных и предложенных к применению структур данных. Она очень часто выходит из строя из-за быстрой прототипизации и связанных с ней множеством ошибок. Часто наблюдается нетерминация всяки с неограниченной тактикой применения подходящих правил. Система «SpaceInvader» [54] является наследником «Smallfoot» и включает в себя простые элементы абдукторного вывода. «jStar» [86], [194] можно рассматривать, как объектно-ориентированное расширение «Smallfoot», которое уже поддерживает классные инварианты и ограниченные (абстрактные) предикаты. «jStar» преобразует все программные команды в форму «JIMPLE», которая очень близка к IR от «GCC», язык который называется «GIMPLE» [171] и с помощью которого, проводится верификация поблочно-управляющим командам. Для индустриального применения, это решение является наиболее приемлемым. «Verifast» [124] работает с входным диалектом Си и разрешает произвольные определения абстрактных предикатов. При невозможности вывода, пользователю приходится вручную добавлять команды и подсказки к правилам для завершения доказательства. Программная среда Хурлина [121] очень похожа на [86].

«Cyclone» [109] является верификатором динамической памяти на основе ВР (см. раздел I-C1). «SATlrE» [199] верификатор, который работает на основе анализа образов [232] и реализован в Прологе. «SATlrE» отличается тем, что образцы и зависимости между ними вычисляются не каждый раз заново, а только меняющиеся пути. «Ynot» [187]

является «SMT»-решателем на основе «OCaml».

Далее, имеются следующие подходы и программные среды: (1) «KeY/VDM++» [23], [271] способствуют применению в индустрии объектно-ориентированные спецификации и интеграции с языком моделирования «UML», которое не допускает доказательства динамической памяти, (2) отслежка ячеек памяти при запуске программы (динамический подход), например «Valgrind» [254] или «ElectricFence» [128], [91] [141], (3) программные среды интегрированные (статический анализ) в пакете компиляции «LLVM», как например, «SAFECode» [75], (4) преобразование программы и утверждений в вид слабоструктурированных данных [20] и возможной трансформацией ею [125], [87] (см. раздел I-C). Раздел I-A3 содержит подробнее обзор по теме «Абстрактной интерпретации». Пункт 2 это динамический подход, который можно коротко описать на примере «Valgrind». Оно загружает данную программу с аргументами запуска в память и сопоставляет все доступы динамической памяти своими командами. Таким образом, каждый запуск записывает все неверные доступы к памяти, а также утечки памяти.

«GCC» [252] и «LLVM» [253] являются фреймворками компиляции. Обе содержат модули по статическому анализу [154], [75]. Хедкер [137] предлагает статический фреймворк, основанный на вычислении транзитивного замыкания достижимости в графах для анализа потока данных. Проект «CompCert» [43], [161] предлагает чисто академический фреймворк для анализа корректности трансформаций кода для процессорной архитектуры «PowerPC» при поддержке верификатора «Coq».

В качестве верификаторов общего назначения можно образцово привести уже упомянутую систему «Coq», но также имеется ряд иных верификаторов, например, «PVS», «Proof General», «Isabelle» и многие другие. Сравнение выбранных верификаторов можно найти в [92], а для верификаторов динамической памяти в [307]. Аппель [13] представляет перечень, какие проблемы за последние годы были хорошо решены и какое имеется сравнение. Статьи из немецкого популярного технического журнала «iX» [140], [139] посвящаются наиболее удобными динамическими программами, ранее представленными, для анализа проблем динамической памяти (см. главу II).

Статический анализатор «ESC Java» (с англ. «Extended Static Checking for Java») [96] вводит модульную спецификацию в Ява (см. [105], [28]), но увы, указатели исключаются и модель памяти исходит из того, что все элементы существуют в динамической памяти, а интроспекция не учитывается. Спецификация Ява-программ предлагается подходом «Java-ML» в [20].

Система «Jahob» представленная в [283] предлагает прототипную верификацию линейных списков

для Ява-программ на основе функционалов на функциональном языке программирования близок к языку «LISP». Используется эвристика, которая выбирает правила с более жёсткими требованиями. Цель проекта заключается в поиске автоматизации или ускорения за счёт абстракции спецификации функциями высшего порядка (см. подход Поулсона [198]).

Система верификации объектно-ориентированных систем, как в этой главе уже было изложено, которые более близки к индустриально применимой верификации являются, например, также «KeY» [182]. Система «Baby Modula 3» [2], [56] может быть применима, но страдает от множества ограничений (см. раздел I-B).

Проблемы динамической памяти

В этом разделе имеется короткое введение в типичные и актуальные проблемы в работе с динамической памятью. Затем дается короткая мотивация, почему изучение и исследование этих проблем актуальны с теоретической и практической точки зрения.

Под динамической памятью подразумевается (см. рисунок 25) та часть операционной памяти процесса, которая выделяется во время загрузки по запросу [163], [164]. Куча является неорганизованной частью памяти (см. рисунок 27), в отличие от организованной части памяти, т.е. стека. Организованность подразумевает автоматическое выделение и утилизацию локальных переменных по диапазону видимости (см. рисунок 26), с чёткой пропиской связи между элементами. В случае стека, при компиляции «ABI» вынуждает к строгому порядку помещения в текущее стековое окно локальных переменных. Например, задекларированные локальные переменные, при условном переходе видны в нём и могут перекрываться другими локальными переменными с таким же наименованием. При выполнении программы, локальные переменные не доступны за пределами блока видимости. Такое же наблюдается с процедурами и подпрограммами: локальные переменные, а также параметры по значению вталкиваются при запуске процедуры в видимое окно на стеке, т.е. актуальное. При выходе из процедуры, стековые переменные выталкиваются из стека, окно утилизируется (подробные реализации можно найти в [252]). На рисунке 26 имеется стековое окно с локальной переменной o , которая в данном случае, — целое число 1. Также имеется на рисунке массив, (локально, не обозначен) с указателями, которые ссылаются на o и на высший элемент. Все элементы стекового окна компактно помещены в стек, т.е. между ячейками обычно не имеются дыры. В отличие от этого, запись не обязательно должна быть компактной, точнее, если не упоминается ключевое слово «packed», то часто

это и не происходит, благодаря генерации наиболее оптимального кода по быстродействию или размеру кода.

В отличие от этого, ячейки кучи процесса могут быть разбросаны как угодно. Видимость ячеек кучи не зависит от синтаксических блоков, а зависит исключительно от момента выделения динамической памяти до явной утилизации памяти. Если куча не утилизируется программным оператором, то по умолчанию все кучи утилизируются глобальным деструктором программы перед завершением процесса операционной системы. С этой целью кодовый сегмент `.dctor` в программах Си++ содержит все адреса деструкторов переменных объектных экземпляров, которые перед передачей контроля ОС вызываются. Стек и куча определяются операционной системой, они находятся в виртуальной памяти. Подробные механизмы памяти выделения и утилизации в данный момент нас пока не интересуют. Для стека и кучи нет фиксированного порога при запуске программы, а имеется плавающий порог (штрихованный, см. рисунок 25), который может, либо расти, т.е. стек увеличивается за счёт уменьшения кучи, либо наоборот, в зависимости от объёма употребления памяти. «bss» обозначает сегмент памяти, который содержит все глобальные (часто могут включаться иные, не локальные, в зависимости от конкретных реализаций при компиляции [243]) переменные, которым не было присвоено изначальное значение. Все остальные, не локальные и не динамические переменные выделяются в сегмент «data». Загружается программный код. В нём содержится объектный код с адресом точки запуска. Все относительные адреса заменяются абсолютными адресами. На практике программный код может и должен содержать различные фазы запуска программы, например, деструкторы.

Любая ячейка любого сегмента из рисунка 25 может быть адресована линейно. Это означает, что доступ к содержимому памяти можно получить по последовательному увеличивающемуся порядку. Любая ячейка памяти имеет последовательную по адресу $+1$, где 1 является символическим числом, которое представляет собой размер одного элемента соответствующего типа. Однако, согласно рисунку 25, имеется плавающая граница, которая практически никогда не достижима. Например, если целое число имеет тип `uint16_t`, то размер 1 станет 2. Обратим внимание, что с помощью эксклюзивного бинарного оператора «ИЛИ» (XOR, \oplus) можно моделировать два указателя в двусвязанном списке с помощью лишь одного «поля прыжка», если в качестве содержимого поля записывается $a \text{ xor } b$, где a является адресом начального поля, а b следующее поле, т.к. действует $a \oplus (a \oplus b) \equiv b$, а также $(a \oplus (a \oplus b)) \oplus (a \oplus b) \equiv b \oplus (a \oplus b) \equiv a$ (см. [196], [240], [308]).

Таким образом, можно сэкономить один указатель, хотя, утилизация ненужных ячеек памяти не может быть решена стандартно. Допустим, производится манипуляция двусвязного списка, тогда необходимо проверять достижимость с помощью сумм всех адресов списка.

Памятные модели между языками Си(++) [252], [253] и Ява [128] сильно отличаются, даже между Си++ и Си, если даже на первый взгляд это не очевидно. Так например, у языков программирования, которые совместимы с ISO Си(++) сбор мусора ненужных элементов часто не проводится. С одной стороны, это экономит дополнительные расходы, с другой стороны, это перекладывает большую ответственность на программиста. В языке Ява, сбор мусора очень часто приводит к дополнительным затратам, к счастью, сбор мусора работает часто в параллельной нити внутри Явы в виртуальной машине, что способствует к избеганию больших дополнительных расходов. Ява, как компромиссное решение, использует подход «сбора мусора по поколениям», который можно считать, приближенным к субоптимальным решениям со стороны практических порогов и объёмов мусора. В Яве все переменные и данные хранятся в кучах. Диалекты Си допускают слабую типизацию [243]. Не совместимые типы при различной интерпретации битов могут быть преобразованы, например, байт в вещественное число с помощью Си оператора union.

Мотивация

В техническом докладе [176] на протяжении десятилетий анализируются совершённые и отслеженные ошибки при разработке открытых и коммерческих программных систем обеспечения. Результаты [176] практически из года в год без изменения подтверждаются многочисленными новыми исследованиями, как например [177], [113], [5]. В [176] демонстрируется, что в приложениях для коммерческих дистрибутивов операционной системы «UNIX», содержатся около 23% ошибочного кода, а код открытых проектов содержит лишь около 7% на платформах «GNU». Авторы осторожны и оптимистичны. По Миллеру наиболее часто встречаются следующие ошибки:

- 1) Ошибки с указателями и полями. Авторы обращают внимание, что для коммерческих приложений, ошибки либо вообще не обнаруживаются во время разработки программ и начального тестирования из-за недостаточного покрытия тестов, либо обнаруживается лишь при портировании продукта на другую платформу. Авторы более всего обеспокоены этим видом, т.к. их трудно обнаружить и исправить так, чтобы другие модули не пострадали. Чаще всего замечаются следующие трудности: неверный доступ к памяти, неинициализированные ячейки

данных или утечки памяти, которые рано или поздно становятся не доступными.

- 2) Неверный доступ к массивам с преодолением доступных границ, либо в связи с изменением структуры данных, хотя указатель остаётся без изменений.
- 3) Недостаточная проверка работы с файлами. Часто при чтении, достижение конца файла вообще не проверяется.

Верифицировать динамическую память тяжело потому, что описывается состояние куч, а данная программа с описанием корреспондирует [126] «неявным» образом. Если интерпретировать кучу, как граф (см. следующие главы), а программа — это последовательность инструкции построения того графа, то описание одной и той же кучи может быть сделано разными путями. При проверке, обе стороны должны корреспондировать.

Хинд [113] задаётся вопросом, почему анализ псевдонимов до сих пор не решён. Он призывает заняться исследованием корректности и быстродействия (см. рисунок 1), т.к. не выявленные псевдонимы означают возможную деградацию откомпилированного кода. Если во время компиляции известно, что некоторая пара локальных переменных обязательно ссылается друг на друга, то при выделении регистров [181], [135], [237], [238], [226], можно гарантировано использовать один регистр, тогда отпадает необходимость синхронизировать два или более регистров (см. [245], [154], [76], [181]).

Хинд [151] убеждён в том, что для эффективного выявления псевдонимов нужно анализировать входную программу. Лэнди [151] вводит классификацию анализа псевдонимов. Анализы являются NP-твёрдыми. Они делятся на: (1) псевдонимы, которые «должны ссылаться» или «могут ссылаться» и на (2) псевдонимы внутри процедуры или за её пределами. Анализ внутри процедуры считается эффективным [114]. Анализ за пределами процедуры считается неэффективным и нуждается в улучшении. Хинд [113] предлагает использовать маленькие отрывки области видимости с локальными переменными при использовании эвристического подхода для решения вопроса псевдонимов.

Ху [119] представляет статью, которая посвящена техническим границам циклов писания и чтению актуальных флэш-памятей. Флэш-память как постоянный накопитель, здесь упоминается потому, что виртуальная память ОС при необходимости использует её и это быстрее чем использование винчестерского диска. Писание в память в среднем занимает приблизительно в десять раз больше времени, чем чтение, а блочная запись имеет наибольший эффект. Результаты Ху можно растолковывать так: сбор мусора не нужен вообще, в связи с продолжительностью жизни флэш-устройства, т.к.

сбор мусора сильно задерживает процессы писания и чтения остальных процессов. Кроме постоянного накопителя, флэш-память также может быть использована как виртуальная память во встроенных системах. Оно может критически повлиять на быстродействие целого приложения.

Бэссей рекомендует из-за неточности сред верификации для решения различных проблем с динамической памятью: (1) избавляться от программ, которые при запуске меняют программный код (2) соблюдать лозунг: «обыкновенные ошибки должны быть найдены обыкновенно» (3) учесть, что проведение анализов программы не обязательно приводит к улучшению качества программы. Отметим, что пункт (1) лишь меняет момент определения программного кода. С одной стороны — имеется увеличение гибкости, с другой стороны — имеется возможность ограничения семантического анализа, например, с проверкой типов, но также дополнительные расходы на динамические проверки и генерации кода во время запроса. Естественно, верификация не в состоянии угадывать поведение статически из-за проблемы приостановки. Из-за упомянутых недостатков (см. [221], [39], [235], [117]) динамически меняющегося программного кода далее динамические изменения не рассматриваются. В связи с ошибочным обращением к динамической памяти подразумеваются:

- доступ к недоступной памяти
- доступ к неинициализированной памяти
- нехватка динамической памяти при востребовании
- снижение быстродействия
- утечка памяти (см. далее).

Далее все эти последствия рассматриваются. Ошибки могут привести к самым непредсказуемым ситуациям, в худшем случае вплоть до неверных дальнейших ответов программы, а к приостановке в лучшем случае. Приостановку можно без преувеличения считать «наилучшим» вариантом, т.к. выход в определённой точке программы предпочтительно к неопределённому выходу. Факт приостановки программы говорит о неисправности, а далее коррумпированное состояние не является предпочтительным в различных смыслах корректности и целостности.

Бэсси [33] приводит итоги анализа успешных верификаторов в общем, и объясняет актуальные причины и принципы. Наиболее важными пунктами Бэсси считает:

- Верификация теорем всегда является точной наукой: эвристики могут применяться, но в конце интересует — следует ли предполагаемый результат из аксиом и правил или нет? Поэтому, давать квантифицированный результат трудно. Малое количество обнаруженных ошибок может

означать, что верификатор плохой или хуже других. Бэсси обращает внимание, что эвристика «бери самое крупное правило первым» на практике даёт хорошие результаты. Рекомендуется выбирать представительные примеры из [282], как например операционные системы, либо программное обеспечение в публичном доступе.

- Нетривиальные доказательства должны быть стандартизированы насколько это возможно. Если имеется возможность, то посторонние подпроцессы должны независимо от правил доказательств приводить к состоянию вместе с программным представлением, в наиболее нормализованный и упрощенный вид, с которым можно продолжать верификацию. Конкретные специфические правила должны быть логично отделены от остальных структурных правил. Общим лейтмотивом должен послужить: «простые ошибки необходимо обнаруживать простым способом». Если лейтмотив не соблюдается, то можно считать верификацию мало полезной.
- По возможности как можно чаще и раньше исключать «дополнения» входного языка, которые можно исключать без большой потери выразимости, как например, динамическое обновление кода. Специфицировать всё подряд или то, что не связано со спецификацией (см. опр.1.3) или верифицируется с большими затратами в ущерб читаемости и при необоснованной потере ключевых свойств правил данного вычисления, не доступно. Всё должно быть простое и проверяемое, иначе доказательство может быстро оказаться неприемлемым, ради исключения редких случаев.

Как было ранее упомянуто, программирование с динамической памятью может быть накладным со стороны быстродействия [153]. Бывают случаи, когда использование куч быстрее [12], чем стека, в зависимости, как активно и эффективно работает сбор мусора. Нельзя говорить обобщённо (см. главу I) нужно разбираться индивидуально, чтобы принять решение, какой алгоритм лучше. Эффективность куч также в значительной степени зависит от свободных/занятых списков куч, которые контролируются операционной системой. Торможение из-за стека происходит в связи с генерацией ненужных инструкций вталкивания и выталкивания. Проблема увеличивается с большими объектами, которые не помещаются в регистры. Каждый процесс копирования структуры данных, будь-то слово процессора, либо комплексный тип, является потенциально лишним, как только речь идет о ссылках. Если значение передаётся, тогда любые дубликаты являются лишними. Увы, устранение по этому принципу не всегда наблюдается в «GCC» [252] или «LLVM» [253] из-за сильно консервативного подхода. Замечаем, что часто любой алгоритм,

который реализован с помощью куч, можно записать при использовании стека последовательно, как было частично предложено в [173], [174]. Адреса любого объекта куч можно свободно передвигать, присваивая зафиксированный адрес при условии, что каждый элемент стека можно однозначно адресовать. Для этого потребуется дополнительная конвенция идентификации последовательных типов (т.е. различия размеров) элементов на стеке. Важно соблюдать максимальный порог вталкиваемых объектов в стек, который увеличивается при уменьшении кучи (см. рисунок 25). Элементы массивов, т.е. кучевые объекты одинарного типа, можно вталкивать, просто копируя элементы последовательно. Важно, сохранять на стеке информацию о том, что следует массиву. Таким образом, единственными открытыми вопросами остаются: (1) Действительно ли так нужно поступать, ради читаемости, эффективности алгоритма и т.д.? (2) Всегда ли применим такой вариант или нет? Первый вопрос довольно спорный, сравним например, элегантность деревьев в кучах (см. [196]). Второй вопрос не всегда решим, в частности, когда лимиты устанавливаются только при запуске программ, прочитав например информацию из файла. Конечно, можно попытаться установить некоторый максимальный технический массив для покрытия большинства случаев, однако, таков алгоритм далеко не эффективен, а тем более неполон. Всё, что можно заранее вычислить и статическим образом установить, это очень полезно для вычисления только со стеком. Увы, часто бывают ситуации, когда это не приемлемо по техническим или другим причинам. Нельзя не заметить, что стек и куча конечны.

Далее рассмотрим некоторые конкретные проблемы динамической памяти на образном диалекте Си.

Проблемы в связи с корректностью

Пример 1– Утечка динамической памяти. Утечка памяти является одной из проблем, которая встречается очень часто. При утечке выделяется объект в динамической области памяти, которая, в конце концов, не освобождается. Часто это не приводит к краху загруженной системы, однако, нельзя сказать, что это удовлетворительно. Программа раньше выйдет из строя без предупреждений, либо в любой неопределённый момент. Это может произойти тогда, когда ОС вдруг обнаруживает нехватку доступной памяти, либо ОС не может разрешить доступ к памяти из-за специфических правил ОС по безопасности, либо просто в ОС не осталось достаточно иных ресурсов. Типичный сценарий такой, что программа работает пару минут или даже три недели подряд без событий, а затем, либо из-за внешнего события, либо сообщения, программа неожиданно выходит из строя или просто завершается без указания ошибки. Часто отслеживание, если оно возможно, может не

привести к самой ошибке, т.к. выделение памяти (если обнаружить) может являться только симптомом, но не настоящей причиной ошибки. Выявить настоящую ошибку крайне тяжело. Ошибкой программы из рисунка 28

является тот факт, что содержимое от `object1` не утилизируется после повторного присвоения. Если предположить согласно ISO Си++ [243], что ОС при завершении программы освободит все выделенные ячейки, то уже до завершения программа может выйти из строя из-за нехватки памяти. Проследить такой тип ошибок будет крайне тяжело или практически не возможно, в частности потому, что при каждом запуске пороги ответственные за провал могут кардинально отличаться. Проблема заключается в анализе «опасных» мест в программе, которые могут не освобождать ранее зарезервированные ячейки.

Пример 2 – Неверный доступ к памяти. Неверный доступ к динамической памяти является ошибкой, которая встречается относительно часто. Причиной служит тот факт, что некоторый объект не инициализирован, либо имеет не правильное значение. Отметим, что ОС по-разному относится к объектам, которые находятся в «bss». Например, ОС «Windows» часто не инициализирует локальные переменные. Это приводит к ячейкам с неопределённым значением, тогда продолжение программы не определено, т.к. вычисляются альтернативные пути программы. Это может уязвить процессы. Причиной является неправильное или неприсвоенное значение переменных в рассматриваемом алгоритме (см. рисунок 29).

Анализ ошибки должен сосредоточиться на все присвоения с момента первой декларации переменной `object1`, включая все присвоения, если значение было передано. Из всех присвоений необходимо выявить то присвоение, которое «неправильное» согласно формальной/неформальной спецификации данного алгоритма. Неверный доступ к памяти можно считать как попытку доступа к объектам, которые были нечаянно утилизированы. Неверным доступом можно считать множество ошибок связанных с неправильной разрядностью или шириной процессорного слова в связи с неправильным применением преобразования типизации указателей. Например, в связи с принудительной конверсией типов между (`int*`) или `void*`, либо (`char*`) и (`int8_t*`), которые в зависимости от компилируемой платформы могут различаться. Также в зависимости от платформы:

`sizeof(struct(int a, char b)), sizeof(int)+sizeof(char)`

не должны быть идентичны при типизированном доступе к адресу памяти. Размеры структур и её разрядность могут тоже отличаться. Если предположить, что *a* занимает 2 байта, а *b* занимает 1 байт (что на разных платформах может быть не

так), то содержимое, может быть одним из вариантов битовых масок из рисунка 30.

Поэтому, предпринимать какое-либо утверждение, зависимо от платформы, может быть даже ошибочным, если например речь идёт, об архитектуре «Intel», «PowerPC» 64-битных, «ARM» 32-битных или иных процессорах.

Если, по какой-то причине не инициализируется некоторое поле, то безобидная программа из рисунка 31 может не завершиться или завершиться не правильно, а также может выдать неверную информацию – любое из побочных эффектов является недопустимым.

Пример 3 – Висячие указатели и псевдонимы.

Висячие указатели (см. [8]) получаются, когда несколько указателей ссылаются на один объект и операции над другими указателями, возможные псевдонимы, приводят к тому, что хотя бы один указатель «нечаянно» ссылается по ошибке на пустое место или операции над одним указателем меняют связанную кучу. Хотя феномен интуитивно понятен, но на практике определение псевдонимов может оказаться довольно трудным и неточным. Необходимо анализировать не только одну процедуру с указателями параметров, но все возможные вызовы – т.е. одним вызовом множество содержимых указателей может поменяться, а в других случаях может ничего не поменяться. Содержавшие объекты висячих указателей подлежат утилизации, т.к. по определению они являются мусором. Указатели, ставшие висячими, могут стать невисячими в ходе запуска программы, а также наоборот. Однако, содержимые, ставшие мусором, навсегда утеряны. Феномен висячих указателей можно достичь именно таким способом, но также при использовании различных интерпретаций данных ячеек, например, предусмотренные структурой объединения с помощью «union».

Пример 4 – Побочные эффекты.

Вместо ненужного копирования структур данных, часто можно при вызовах процедур лучше использовать ссылки. Однако, этот подход содержит опасность, что нечаянно могут пострадать посторонние данные и переменные. Эта проблема является обобщением примеров №2 и №3: указатели не меняются в ходе запуска, но содержимое неожиданно меняется. Далее можно обобщить: модификация неожиданно меняет другие переменные. Модификация одной кучи не должна отражаться на другую.

Проблемы в связи с полнотой

Пример 5 – Проблемы в связи с выразимостью.

Несколько проблем с выразимостью уже были представлены в этой главе. Основные проблемы выразимости заключаются в: (1) можно ли все допустимые кучи специфицировать при условии, что

все корректные кучи действительно синтаксически верны, исходя из данного набора правил? (2) Выводится ли, что все выбранные неверные кучи верифицируют как неверные, согласно правилам? (3) Какими можно использовать предикаты? (4) Каким условиям и свойствам должны придерживаться предикаты? (5) Каковы взаимосвязи между кучами и насколько адекватно это отражается в формулах? (6) Какие ограничения имеются в связи с использованием символами в описаниях куч? (7) Как лучше описать множество и отдельную кучу? (8) Как можно выразить зависимость между псевдонимами? (9) Имеются ли многозначимые кучи или их описания, если да, то почему и можно ли их эффективно исключать? (10) Какой уровень абстракции нужно вводить для удобного описания куч и для решения задачи верификации? (11) Имеется ли возможность абстрагировать настолько, чтобы, интуитивно стало ясно, о чём идёт речь, и пользователь, без особого труда, имел бы возможность лучше «понять» спецификацию? (12) Можно ли формулы для описания куч преобразовать так, чтобы не было необходимости специфицировать повторно? (13) Можно ли, если потребуется дополнительное преобразование, использовать «что-то более знакомое» программисту для спецификации и верификации чем искусственно определённые и ограниченные подвыражения логики предикатов (например, первого порядка), которые вычисляются и поддерживаются не полностью и часто не интуитивно?

Пример 6 – Проблемы с полными представлениями.

Согласно рисунку 1 в статье Сузуки [249] были предложены операции над указателями, которые можно считать «безопасными». С использованием нужно быть крайне аккуратно потому, что ротация одной структуры данных по часовой может очень быстро привести к уничтожению или фальсификации куч. Кроме этой проблемы корректности, часто неявные условия не очевидны. Подход Сузуки, а также другие подходы страдают практически всегда от неполного набора правил и не полностью описанных куч. Часто имеется ситуация: дан набор 25 правил. Вопрос: (1) достаточно ли этих 25 правил или требуется ещё добавлять или даже необходимо удалять правила? (2) Как быть с «правилами дубликатами»? Состояния куч связаны с программными операторами. То есть, необходимо описать целые подмножества куч и их сравнивать. (3) Имеет ли смысл ограничить выразимость куч так, чтобы приостановка была решимой с приемлемыми ограничениями? (4) Имеется ли возможность только часть кучи специфицировать и доказывать? (5) Можно ли предложить или использовать простую модель памяти так, чтобы доказательство данной простой структуры данных была простой, как например, реверс линейного списка

(см. [223])?

Желательно, чтобы для верификации не было необходимости постоянно все методы полностью специфицировать. Выработка корректной и полной спецификации на практике означает большие затраты рабочего времени инженера, в чем часто нет необходимости. На практике часто специфицировать достаточно лишь некоторые процедуры или объектные классы. Для этого необходимо отдельные фрагменты программы оставлять не специфицируемыми. Практическим требованием для инженера является возможность добавления вспомогательных утверждений в те места программы, где инженер желает подробнее проанализировать некоторую нестыковку со спецификацией для локализации и выявления ошибки (см. алгоритм №1). Разработчик также может быть заинтересован в добавлении проверок в произвольных местах программы дополнительно к пред- и постусловиям.

Пример 7 – Проблемы в связи со степенью автоматизации.

Согласно лестнице качества из рисунка 1, эти проблемы входят во вторую категорию. Главные проблемы автоматизации в ранее упомянутых разделах связаны с необходимостью определять аксиомы и правило динамической памяти от общих логических и иных правил, которые не связаны с преобразованием элементов динамической памяти. Если установить формальную теорию, основанную на равенствах и неравенствах куч, и эту теорию записать в отдельный набор правил, то набор уменьшается и верификация упрощается. Такая попытка значительно уменьшила бы численность и сложность данных правил. Необходимо улучшить сравнение спецификации с данным состоянием куч, которое к большому сожалению проводится в существующих подходах практически вручную (см. далее разделы и главы). Когда данную теорему нужно использовать, а когда сопоставить с нужными символами — трудно предсказать. Проблема также существует при преобразовании из одного состояния кучи в другое. Локальное оптимальное решение доказательства может всё равно привести к полной нерешимости. При преобразовании куч с помощью дедуктивного метода, также стоит задуматься об улучшении сходимости доказательства, подключив например абдукцию. Основным теоретическим ограничением может выступать выразимость формул. Термы могут быть, либо не полностью определены во время статического анализа, либо они нерешимы в принципе. Ограничение офсетов в арифметических выражениях приводит с одной стороны к ограничению выразимости, с другой стороны к повышению уровня автоматизации. Возникает практический

вопрос, насколько полезны определения алгебры куч? Насколько достаточна строгая типизация во входном языке программирования?

Проблемы в связи с оптимальностью

Пример 8 – Проблемы в связи с быстродействием.

Проблемы быстродействия конкурируют напрямую с корректностью (см. рисунок 1). Выявление утверждений «указатели обязательно ссылаются» или «обязательно не ссылаются» важнее, чем «указатели могут ссылаться», но их одновременно труднее выявить. Первое и второе утверждения имеют более сильный эффект на генерацию кода. Чем больше сокращается время запуска соответствующего кода, тем эффективнее он, т.к. отсутствие необходимости сохранения процессорных регистров в стек, означает ускорение. Увы, анализ зависимостей с указателями данных сложнее, чем с локальными переменными потому, что содержимое указателя p может меняться не только там, где имеются присвоения к p , но теоретически в любом другом программном операторе.

Анализ псевдонимов является трудной частью, т.к. необходимо отслеживать все использования и вызовы процедур, что может привести к самым различным результатам. Часто, в фреймворках с указателями наблюдается, либо наиболее обобщённые утверждения, которые могут оказаться полностью без эффекта, либо утверждения вообще не рассматриваются.

Также важно заметить, что если структура данных используется только в одном месте и дубликаты отсутствуют, то требуется меньше расходов для непосредственной манипуляции. В реализациях наблюдаются в основном два подхода: либо вручную передаются простые и объектные переменные (но возможно с вспомогательными замечаниями, например, в Си с помощью ключевого слова `register` [252]), либо в исключительных случаях проводится анализ псевдонимов (в основном исключительно внутри процедур [253]). Этот случай не исключается в языках Си [252], используя ключевое слово `const`. В качестве мотивирующего алгоритма, например, реверса списка с изменением существующей структуры [223], [196], изначальный список исчезает, но это в зависимости от контекста может вполне устраивать. Алгоритм Рейнольдса только один раз проходит через линейный список (без явных и обратных указателей). Таким образом, отпадает необходимость копировать список. Все операции производятся по данному списку, что сильно ускоряет. Если бы знать заранее, что структура данных будет меняться и оригинал будет не нужен, почему бы и не забросить старый список и таким образом резко ускорить алгоритм? Данные компиляторы [252], [253] пока не в состоянии проводить такой анализ, по крайней мере, не детально. Далее, можно ли поменять «ABI» при компиляции так, чтобы не используемые объекты удалялись из

стека вызывающей стороны [243], [252] безусловно, и уже существующие объекты в динамической памяти были бы использованы непосредственно, если объекты строго не меняются при вызове? Надо отметить, что модель указателей в [240] не стандартная, затраты для линейных списков сильно сокращаются, сбор мусора изменен до неузнаваемости.

В частных случаях, когда заранее известно число итераций циклов статическим анализом (см. [12]), то можно оптимизировать место расположения ячеек памяти.

Проблемы оптимальности сбора мусора, начиная с алгоритма Уэйт-Шора [234] доныне, можно считать, более чем достаточно исследованы [127]. Микрооперации в связи с динамической памятью производятся операционной системой, которая следует за свободными ресурсами, в том числе, куча и стек.

Пример 9 – Проблемы в связи с целостностью и безопасностью программы.

В качестве оптимизации (см. рисунок 1) также рассматриваются проблемы в связи с анализируемой программой, где предполагаются корректность и полнота.

Аналогично к переполнению стека [138], когда стек наполняется нежелательными данными, с целью передвижения актуального указателя за пределы актуального стекового окна при вызове или возврате с процедуры — имеется такая же попытка вталкивания обратной метки, например, при сборе мусора в куче [130], [8]. Очевидно, что в отличие от стека, куча не содержит адреса программного кода, следовательно, атака включения вредного кода прямым образом не сможет сработать априори. «Переполнение куч» может привести к потенциальной уязвимости процесса, либо целой системы.

Особенно критично стоит вопрос о безопасности с интерфейсами дальних серверов и служб, а также со спецификациями, когда вызывается некоторый системный доступ к драйверу [71]. Так как, драйвера могут запускаться несколькими инстанциями одновременно, то неисправность в связи с ошибкой в динамической памяти является особенно критической. В худшем случае нестабильность может привести к краху ядра ОС, как это имело место быть в случае с монолитной архитектурой ОС «GNU Линукс» с одним ядром.

Выразимость формул куч

Предположим, что имеется некоторая императивная программа, где граф потока управления [137] выглядит, как представлено на рисунке 32. Пример из [76] послужит нам образцом выявленных различий между автоматически и динамически выделенными переменными. Особенность автоматически выделенных переменных заключается в том, что

они выделяются и уничтожаются автоматически открытием и закрытием стекового окна. Стековое окно содержит все локальные переменные и параметры, которые поступают во внутрь и выходят наружу. Нельзя это путать с «fan-in» и «fan-out».

Согласно рисунку 32 определяются интервалы видимости. Интервал видимости всей процедуры, например [Вход,Выход] означает, что передаваемые переменные видны на всех вершинах между начальным блоком «Вход» и конечным блоком «Выход». Блок определяется как объединение последовательных неразветвляющихся программных операторов. Далее, во избежание коллизий между различными переопределениями, предпочитается форма блоков в виде «SSA» [76], [237], [245]. Разветвлением может быть любой условный или безусловный переход. Программные операторы безусловного перехода исключаются.

Допустим, в некоторых блоках определены локальные переменные по «SSA»-форме как имеется в рисунке 33.

Предположим, все остальные блоки, либо искусственные, пустые, либо не содержат определения только что введенных переменных. В блоке № 5: f , является процедурой, которая принимает одну переменную. На первый взгляд в этом нет ничего не обычного, однако, если внутри f производится доступ к содержимому параметру, в Си это производится с помощью $\&$, тогда переменные могут меняться за пределами f . К счастью этот сценарий можно выявить с помощью предыдущего анализа всех входных и выходных переменных от f . Хотя описанный сценарий на практике может встречаться не часто, сценарий является причиной, почему множество оптимизаций не могут совершаться, спасая корректность в общности. Если в блоке № 6 a определяется заново, то он выглядит так: $a_2 = \phi(a_1, a_0)$. Функция ϕ является вспомогательной и означает объединение различных определений одной переменной. ϕ неявная функция (отсюда и название с англ. «phony», что означает ненастоящая или поддельная). Концепция неявно определённой функции интересна, с ней мы встретимся позже при определении куч. Такого рода определения данных переменных программ является определением зависимостей данных и может быть применено к любым автоматически выделенным данным в императивных программах. Структура зависимостей в общем случае не может быть деревом, это запрещают ϕ -функции когда имеются зависимости, которые показывают на более ранний блок, который снаружи от циклов.

Как бы ни было, нас интересует, какие подходы имеются для вычисления интервалов видимостей с помощью ϕ -функций [245] локальных переменных. Мы обходимся тем замечанием, что имеются максимальные границы, которые определяют интервалы. Эти

границы могут определяться рекурсивно по стеку. Границы вычисляются с помощью графа потока данных и ϕ -функций для каждого из локальных переменных (алгоритмы при поддержке вершин доминаторов представлены, например, в [245], классический подход смотри в [76]). Очевидно, что если переменные определяются в двух разных ветвях заново, то содержание после ветвления может отличаться, а индекс повышается.

Если попытаться применить «SSA»-форму к динамически выделенным переменным, тогда такая попытка не удастся из-за следующих причин: (1) существуют программные операторы, которые выделяют и уничтожают ячейку в динамической памяти явным образом. Эти операторы могут лежать за пределами блоков и процедур. Ячейки могут, безусловно, существовать за пределами процедур и после уничтожения переменной указателя. Это означает, что место определения (в том числе переопределений и уничтожения) и использования сильно отличаются от автоматически выделенных переменных, т.е. места не обязательно совпадают с местами употребления в программе. Даже могут меняться содержимые указателей, когда на указатели, вообще, ничего не ссылается и указатели уже давно утилизированы. (2) размер, частота и контекст выделения памяти в куче в общности не всегда определены (см. рисунок 25).

Аналогично к графу потока данных, можно приписывать не только содержимое переменных к вершинам графа аннотации о свойствах программы [97], но также, например, утверждения о динамической памяти. Примером тому, является фреймворк представленный в [137], который анализирует для каждого указателя при сильно консервативном подходе – возможность о псевдониме для всех остальных указателей (через расширенный алгоритм вычисления транзитивного замыкания). Следовательно, после каждого программного оператора высчитывается не только явно выявленный указатель, но также возможно всё связанное с ним. В качестве структуры данных, используется длинное битовое поле, алгоритм подлежит улучшению, но это не делается, потому, что битовое поле является ключевой структурой данных. Принудительные проверки всех взаимосвязей почти нельзя упростить из-за транзитивности операций сравнения и выявления возможной связанности. Сравнение псевдонимов основано на методе Хорвицы [118] и Мучника [181].

Далее, можно привести аналогию, при которой каждое состояние динамической памяти записывается как одно состояние. Очевидно, могут иметься любые переходы состояний, но всегда имеется начальная и конечная точка, когда все кучи пусты. При выходе можно смоделировать вспомогательное состояние такого рода, что все конечные состояния

присоединяются к общему выходу.

Например, функциональные языки программирования исходят из принципа независимости данных как главной концепции. Она гарантирует новый и всё свежий контекст. В нём находятся начальные параметры без взаимосвязей. Затем результат присваивается и передаётся высшей инстанции при возврате. Продолжение (с англ. «continuation») [180], [273], [78], [255] может быть характеризовано как состояние вычисления, которое передается другой инстанции. При переходе состояние не прерывается, т.к. контекст не меняется. Когда речь идет об одинаковом состоянии, то подразумевается всё состояние вычисления, т.е. прежде всего, нас интересует стек и динамическая память (см. рисунок 25). Продолжение хорошо характеризуется денотационной семантикой в случае функций высшего порядка, но денотационная семантика в общем означает вычисление как функции, т.е. без взаимосвязей с окружающей средой. Отмечается, что продолжения сохраняют и обрабатывают стековые окна. Джозель [180] рассматривает продолжения для функционально-логически смешанного языка «LISP». Основные итоги таковы: (1) продолжения повлекут за собой копирование, вталкивание и выталкивание регионов памяти, адреса переходов и возврата из стека, (2) читаемость и моделирование алгоритмов может быть существенно улучшено. Пункт (1) не может не вызывать озабоченность в связи со скоростью [12]. Пункт (2) приоритетный и противоположен к первому пункту, поэтому на практике необходимо находить разумный компромисс.

В примере на рисунке 27, если `free(o.B)` приводит к тому, что объект *C* утилизируется из динамической памяти, то доступ к *C* через *o2* недоступен. Если *o.B* снова присвоить новый выделенный объект, то *C* об этом не заметит, кроме, если новый объект находится по тому же адресу где находился старый объект. Ради формализма можно согласовать, что висячие указатели присваиваются ради простоты и универсальной модели `nil`, если даже в реальности указатель содержит устаревший адрес. Это означает, что при анализе зависимых указателей необходимо рассматривать также все другие указатели, которые могут быть псевдонимом вершин пути доступа, т.е. *o* или *o.B* (см. проблемы из главы II). Интерпретация ячеек динамической памяти определяется в зависимости от типа указателя, который проверяется согласно определению во время семантического анализа. Тип не меняется, ради исключения подклассов (см. главу IV).

Граф над кучами

Теперь, когда основные аспекты динамической памяти были подробно обсуждены (в том числе набл.3.1 и набл.3.2), пора задуматься о представлении

графа. Заранее оговаривается, что уточнённые модели динамической памяти будут вводиться в главах V и VI. Основными операциями манипуляции динамической памяти являются *malloc*, *free* и манипуляция с указателями.

Граф динамической памяти как регулярное выражение. Для начала рассмотрим простой граф A_1 с упомянутыми ранее условиями, который мог бы быть описан регулярным языком и, следовательно, распознан простым конечным автоматом (см. рисунок 35).

С помощью леммы Ардена [79] этот детерминированный автомат может быть представлен следующим регулярным выражением: $b^+(a^+b)^+b$. Что теперь означают этот граф и соответствующее выражение? Граф содержит вершины и грани. Вершины представляют собой не пересекаемые ячейки памяти. Имеется некоторое объединённое финальное состояние $\{q_F | \forall q_F \in F \subseteq Q\}$. Естественно, все конечные состояния можно обозначить одним состоянием. В графе вершины D и E означают, например, некоторые состояния, которые объединяются в $\{q_F\}$. Грани означают ссылки, которые записаны в качестве адреса в разряде процессорного слова в источнике грани. Возникает первый вопрос: что представляют собой наименования над гранями? Это могут быть указатели или поля объектов, т.е. локации. Оба случая не очень удобны: во-первых, указатели должны выделяться отдельно от ячеек, т.к. они расположены в стеке. Во-вторых, наименования всех граней должны различаться друг от друга. Допустим это так, тогда регулярное выражение уже никак не вписывается в данное компактное представление (см. далее). Это означает, что высокая изначальная компактность сильно страдает. В-третьих, не совсем ясно, что всё-таки означают «начальные» и «конечные» состояния? Начальное состояние можно всегда обозначить переходом одной стековой переменной, это всегда допустимо. Конечные состояния обозначить гораздо тяжелее и неординарно: является ли это обозначение конечным состоянием для вычисления? Если опустить q_F , то выражение просто не определено. Можно ввести новое состояние, которое принимает от всех состояний те переходы, которые сигнализируют окончательное вычисление структуры данных.

Допустим, все обозначенные проблемы в данный момент соблюдаются с достаточно удовлетворительным способом и мы продолжим вопрос о внесении изменения динамической памяти с помощью программных операторов после выявления (не-)удобств регулярных выражений. Если запись окажется компактной, то надо проследить, насколько она стабильна при манипуляции. Если имеется маленькая манипуляция, например, меняется только одна грань, то выражение не должно сильно

меняться, и тогда можно было бы нотацию считать практичной. Если вдруг запись не устраивает, то необходимо выявить причину и искать другую модель представления памяти. К примеру, для последнего графа добавляется новая грань b , после ввода граф выглядит как A_2 в рисунке 36.

Это эквивалентно выражению $b^+a^+b((a^+b)^+ + bba^+b(a^+b)^+)^*b$. Теперь мы удаляем грань a и получаем A_3 (см. рисунок 37).

и получаем регулярное выражение $b^+a(a^+bb(\varepsilon + ba^+bb))^+$. Допускается, что все три выражения могут быть переписаны и далее упрощены, но здесь это не решающий фактор. Проблема заключается в том, что если грань вставляется в любое место графа, а из этого надо исходить, то данное регулярное выражение может очень сильно поменяться, в реальном и худшем случаях практически полностью. Чем больше граф, тем труднее записывать регулярное выражение, которое было бы оптимальным и как можно больше похоже на предыдущее выражение. Причина лежит в том, что система линейных уравнений по Ардену при манипуляции подвергается малым изменениям одной грани. Например, первый граф описывается как в рисунке 38.

Нетрудно убедиться в том, что система линейных уравнений имеет решение, но оно сильно отличается от предыдущего. При этом, уравнения почти не меняются. Однако, соответствующая регулярная грамматика сильно отличается.

Граф при манипуляции. Сначала необходимо рассмотреть последовательность типичных программных операторов, чтобы обсудить некоторое «адекватное» представление динамической памяти, а также ситуацию с описаниями указателей и переходов. Рассмотрим инверсию списка из [223]. [223] и особенно [196] содержат многие примеры, но остановимся на выбранном примере, который можно вполне считать представительным. Дана следующая программа из рисунка 39 на диалекте Си со специфическим синтаксисом касательно указателей.

В программе i , j , j и k обозначают указатели. Доступ к последующему элементу в данной программе реализуется к примеру с помощью неявного оператора $*(i+1)$. Подразумевается, что элементы связаны между собой, а не только являются единым, монолитным, непрерывным регионом в динамической памяти, даже если об этом напоминает похожий синтаксис. Семантику программу можно пояснить на примере рисунка 40, где номер, означает шаг итерации до посещения цикла.

До входа в цикл, i содержит список, при выходе i пуст, а обратный список содержится в j . Копии не создаются. Входной список итерируется ровно один раз. Замечаем, что грани в примере не подписаны, но это в связи с выбранным неявным определением оператора над указателями. Конечно,

в общем грани могут быть подписаны. Однако, существуют указатели, которые являются локальными переменными. Они присваиваются к вершинам графа, либо не присваиваются, тогда, когда указатель неинициализирован. Не инициализированным указателем является k до вступления в цикл.

Нетрудно заметить, что компактная нотация даже при простых манипуляциях, например от (1) к (2), совершенно не приспособлена — главная причина лежит в выразимости и адекватном представлении графа. Хотя представленная регулярная запись для данной проблемы не пригодна, всё равно вопрос о компактном представлении также сыграла роль при формулировке автоматизированного подхода в главе VI.

Также нетрудно понять, почему другие глобальные подходы, которые были введены в главе I, например ВР, АО и т.д. не являются настолько успешными. Причина та же самая, которая была продемонстрирована в последних двух примерах. Подход Доддса [87] далее не рассматривается, хотя он описывает графы до и после трансформации и сосредоточен на описании трансформаций графов, но подход не специфичен для указателей и не рассматривает входной императивный язык программирования (см. главу I).

Исходя из наблюдения, граф можно описывать различными способами: (1) или каждую компоненту по отдельности, (2) или предпочесть смешанную форму. Очевидно, что подход (1) не целесообразен потому, что описывать вершины по отдельности (при этом независимо от наименований указателей) может быстро оказаться нечитаемым и не удобным, а спецификация к графу должна быть удобной, короткой и адекватной. Подход (1) требует все вершины графа обозначить по отдельности и затем включить их в спецификацию. Как было обнаружено в примерах введения, такого рода подходы подвергаются целому ряду недостатков и поэтому, в наших целях это не допустимо. Подход (2) подразумевает, либо (2a) описать вершины, либо (2b) грани, а другую компоненту выявить из данной. Проблемой при описании только вершин (2a), являются дубликаты в спецификации потому, что вершина полностью идентифицируется гранями. Каждая грань имеющая отношение к данной вершине должна приписываться. Это равнозначно тому, что к данной вершине надо иметь список всех соседних вершин. Увы, такой подход очень неудобен. Например, одна вершина связана с двумя или более того вершинами. Это означает, что все соседние вершины также должны вписывать вершину в свои списки. Кроме того, если происходит манипуляция кучи, то, спецификация подвергается сильному изменению, а этого нужно обязательно избегать.

Подход (2b) наоборот описывает только грани, а

вершины в них включаются. Этот подход содержит меньше дубликатов и ближе к программе, т.к. ссылки проводятся над реально существующими указателями программы. Если только направленные грани разрешаются, то проверять нужно на половину меньше. Несколько исходящих граней от одной и той же вершины запрещается потому, что один указатель не может ссылаться одновременно на несколько ячеек. Кроме того, программные операторы при более внимательном наблюдении меняют состояние вычисления чаще, чем вершины. — Перемещение, утилизация и выделение являются дорогими операциями, которые включают в себя вызовы операционной системы, а манипуляция указателями является недорогой. В худшем случае, упомянутый подход только выделяет и утилизирует элементы, а указатели мало или вообще не меняются. Тогда принципиально важно задаться вопросом, не подлежит ли подход исправлению?

На рисунке 60 (a) указан регулярный граф, вершины которого имеют степень «3», при этом подразумевается, что каждая вершина представляет собой объект, который содержит ровно три указателя. Для подхода (2a) необходимо специфицировать 11 вершин, каждая из которых имеет три грани, при этом, количество входящих и выходящих граней может различаться и это необходимо рассматривать отдельно. В общем, имеется 18 граней. При подходе (2b) необходимо специфицировать только 18 граней. При этом вершины связанные больше чем с одной гранью могут обозначаться символами. Чем больше данный граф отличается от полного графа, тем меньше граней необходимо специфицировать. Если меняется грань, то меньше нужно менять в спецификации, точнее, только меняющуюся грань. Если меняется вершина, то необходимо проверить все связанные грани. Направленный граф можно обыскать за линейное время все левые и правые стороны граней. Согласно подходу (2b) и данному набору вершин с помощью предикатов, проводить доказательства будет удобнее. Для описания вершин используются указатели или выражения доступа к полям (см. главу IV). Не доступные поля при спецификации нас не интересуют, т.к. такие ячейки по определению являются мусором (см. главу I), навсегда потеряны и не подлежат восстановлению, однако, при спецификации мы заинтересованы выявить такие места, если таковы имеются.

Джоунс [127] определяет кучу как непрерывный сегмент операционной памяти размером 2^k с $k \geq 0$, который представляет некоторую структуру данных — альтернативно, как последовательность прерывных блоков непрерывных слов. Например, дерево может иметь между вершинами свободные элементы, но отдельные вершины не интерпретируются иначе, чем

как данным(и) процессорным(и) словом(-ами). По Джоунсу объект является множеством ячеек памяти, которые не обязательно связаны между собой, но чьи поля адресуемые. Каждая выделенная ячейка памяти имеет указатель и с момента выделения до момента утилизации возникает вопрос, а жив ли содержимый объект или нет? Трудно не согласиться с Джоунсом в том, что фрагментация является проблемой, однако фрагментация внутри объекта исключается.

Коурмен [72] на стр. 151 определяет, также как и Бурстолл [51] любую структуру данных в динамической памяти, обязательно как деревом. Дерево не только подразумевает некоторую связь « \leq » к дочериним вершинам V_j , а также обязуется к соблюдению упорядоченности $f(V_{parent}) \leq f(kid(V_{parent}, j)), \forall j$. Аталлах [18] рассматривает кучу как массив, интерпретируемый как дерево с более широким использованием памяти, но с более высокой гибкостью. В работе Аталлаха можно заметить некоторые различающиеся определения куч. Сначала куча определяется как реализация «очередь с приоритетом» (на стр. 79). Приводятся и обсуждаются «кучи Фибоначчи» [101] как специализированные и эффективные очереди для добавления и удаления. Далее, на стр. 105 куча определяется как двоичное дерево, сохраняемое все элементы очереди с приоритетом. В отличие от свободного доступа к операционной памяти, Аталлах подчёркивает на стр. 111 важность доступа исключительно через имеющийся указатель. Таким образом, произвольная адресация исключается. Ответственность деления куч ложится на мало связанные кучи неявным образом, исключительно, на программиста и на моделирование ПО. Мало связанные кучи можно хорошо делить и обрабатывать эффективными методами. С Коурменом можно не соглашаться касательно произвольной адресации, из-за ранее упомянутых постановлений выразимости. Однако, с ответственностью программиста за создаваемую структуру данных нельзя не согласиться, если даже имеются строгие предпосылки в том, что все структуры данных должны являться деревьями, а не графами — если даже на практике это часто так. Слитор [241] предлагает, для ускорения доступа к куче и минимизации операций сбора мусора, балансировать деревья равняя соседние вершины в отличие от других сбалансированных деревьев, что позволяет произвести быстрый поиск за $\Theta(n)_{min} = 1$ и удаление за $\Theta(n) = \log(n)$. Хотя предложение интересное, всё равно далее подход не будет рассматриваться в данный момент из-за отсутствия острой необходимости реализации, в связи с относительно маленьким объёмом конъюнктов и возможности линейного поиска по локации.

Рейнольдс определяет множество куч, как объединение всех отображений от адресного

множества на не пустое значение ячеек памяти. Следуя этому определению, одна куча — это некоторое множество адресов, которые ссылаются на некоторую определённую структуру данных (без дальнейшего уточнения). Рейнольдское определение структуралистское, т.к. куча, как отдельная, отличающаяся и независимая единица просто не существует (см. главу V). Павлу [199] определяет кучу как любой граф, который не обязательно связан — с этим трудно не согласиться.

Предикаты

Кроме ряда замечаний и конвенций, наиболее важными требованиями остаются: (1) после выполнения каждого программного оператора имеющего отношение к динамической памяти граф кучи меняется наименьшим образом, (2) спецификация соответствующая куче должна также меняться минимальным образом.

Для описания состояния, соблюдая все требования куч, возникает вопрос, как это лучше описать, если очевидно, что сделать это не так просто?

В древней Греции в философской школе Платона эпистемология некоторого описываемого объекта предлагалось известной аллегорией при чётко урегулированном порядке задачи вопросов и ответов между двумя сторонами: человеку, который имеет объект и находится на свободе и человеку, который заперт в пещере и желает понять сущность того объекта с ограниченными возможностями. Запертая персона коммуницирует исключительно речью, а также имеется факел, который горит не бесконечно. Свет факела попадает на обсуждаемый объект и оставляет за собой на пещерной стене тень и силуэты — это неточное изображение и речь, всё, что воспринимает персона в пещере. Эта аллегория лучше известная как «миф о пещере». Она предлагает описание объекта через двустороннюю коммуникацию с целью последовательного выявления непосредственных свойств при имеющихся внешних преградах. Существует множество философских «Геданкеншпилей», например, лишённый естественной речи диалог, эксперимент искусственного интеллекта «Китайская комната» философа Серл. Мы ограничимся мифом о пещере ради классического и древнего характера, который содержит всё, что необходимо для понятия предикатов и куч. Казалось бы, интуитивно понятно, но абстрактное объяснение, получает конкретное присвоение входящих и не входящих свойств (так называемая «ре-ификация» — концепция от абстрактной мысли к конкретной реализации). Более современный философический дискурс по течению идеализма наблюдается в классическом подходе Гегеля: тезис, который устанавливается из отмеченных наблюдений, затем выводятся для более тщательного анализа

и определения свойств противоположных тезисов, что часто из-за не правильного или неточного определения тезиса приводит к конфликту, который затем разъясняется и выводится общий вывод — синтезированное утверждение. На данном этапе можно считать, что выявленные свойства и требования касательно куч проводились достаточно тщательным образом, чтобы предложить первые предложения. Для обнаружения неточностей и выявления более тщательного определения куч применяется подход, близок к этой концепции.

Что касается реификации, то кучи должны иметь синтаксическое и семантическое обоснование, и они будут основываться на предикатах. Предикаты уже были предложены Аристотелем, которые у него назывались «силлогизмом». Силлогизм, это единство трех компонентов логического правила формой: если « A » и « B », то следует « C ». Здесь нечего добавить, кроме того, что большинство логических систем основаны на слегка модифицированной модели.

Предыдущая попытка представить кучи с помощью регулярных выражений не увенчалась большим успехом потому, что изменения происходят в переходах графа. Минимальное требование применяется к правилам, но не к выражению, т.к. представление не слишком стабильное для данной проблемы. Но, в общем, выявление и преобразование представления из одной формы в другую очень широко обсуждается и расследуется. Довольно наглядно на примерах клеточных автоматов [278] можно наблюдать за установлением инвариантов выражений. В главе VI наблюдается обратный подход: наблюдаются образцы, из которых выводятся свойства о правилах.

Предикаты как связывающие вершины графа единицы языков, будь-то формальных/естественных, по семиотике имеют два значения: (i) интуитивное значение, это касается вопроса — что собой представляет на самом деле «куча»?; (ii) коннотативное значение — с чем «куча» ассоциируется? Далее, задаётся вопрос о представлении кучи: должна/может ли куча использовать символы и реляции и что они означают для ее представления? Может ли куча определяться не полностью?

Оценив (i) нужно заметить, что куча представляет собой множество указателей, которые «как-то» связаны между собой и указывают на объекты, которые находятся в динамической памяти. Так как в прошлом большие трудности могли быть выявлены в связи с многозначностью и резкими ограничениями, поэтому необходимо будущие определения редуцировать к минимуму. Оценив (ii) можно выявить, что связь всех компонентов задается данной программой, и куча не организована, это означает: вершины графа могут поступать в любом порядке, в любом месте и непрерывность сегмента

памяти естественно не должна соблюдаться. Кучи могут быть связаны с другими кучами.

Важно заметить, что предикат должен иметь не только возможность выразить связь между вершинами графа кучи, но также должен существовать эффективный способ выразить, что две кучи не связаны. Если такой возможности нет, то разделение автоматически получается неявным результатом анализа всех куч, что плохо из-за эффективности. Также у определения связанности имеются различные модусы: «связан», «возможно связан», «не связан», «возможно не связан». Модальность кучи, также как указание времени, не имеет большого значения: во-первых, «связан» и «не связан» можно проверить за линейное время, из графа кучи. Во-вторых, время отслежки дискретно и до/после каждого программного оператора. В предикатах вариации куч с помощью логических операторов необходимо учесть, что логическая дизъюнкция, несмотря на принцип неповторимости и отрицания предиката, должна быть выразительной — этот вопрос решается в главе IV, где доказательство куч будет основываться на логическое программирование. Нам нельзя упустить, что в качестве указателей могут действовать любые допустимые указатели, это локальные и динамические переменные, а также поля объектных экземпляров.

В первоначальной работе по «логике распределённой памяти» [224] вводится оператор \star над кучами и устанавливает законы следующим образом:

Несжимаемость подразумевает, что из p нельзя следовать p дважды — это совпадает с запретом повторимости описаний [219] кучи. Однако, $p \star q \not\Rightarrow p$, в отличие от классической логики утверждений, не подразумевает строго p как отдельное утверждение. Причина не в том, что p обязательно связана с q — как это можно предполагать, исходя из описаний и интуиции о делящем операторе, как было введено и продемонстрировано. Это лишь как частный случай. Проблема заключается в описании нахождения элементов в динамической памяти. Это означает, что из утверждения о двух кучах, как бы они не были связаны между собой, не следует, что одна куча вдруг может исчезнуть. Такую разницу обстоятельств надо иметь в виду.

Правила (2-4) понятны и нетрудно обосновать графом кучи. В верности правила (5) можно убедиться, используя индукцию к остальным правилам, при этом, различив два случая, когда p_1 и p_2 конфликтуют и когда не конфликтуют с q .

Правила (6) кажутся понятными. Эквивалентности с обеих сторон могут казаться очевидными. Предпосылками являются возможные конфликты термов утверждений согласно конфликтным ситуациям, разрешив заранее проводимое переименование, что согласно λ -вычислению конгруэнтно β -конверсии.

Однако, ни правило (1), ни (6) и ни другие, не исключают возникновения свободной переменной в двух кучах, которые связаны с помощью оператора \star , что и наблюдается в разработках, «smallfoot» или «jStar». То есть, одна переменная может быть использована, например, в качестве указателя в одной куче, а в качестве используемой ссылки в подтерме, в другой куче.

Рассмотрим кучу из рисунка 41.

В куче имеются указатели x, u, y . В прямоугольниках находятся содержимые a_1 , a_3 и a_4 . Бурстолл предлагает обозначить содержимое не напрямую, а лишь на адрес. Также он предлагает записывать в минимальную модель все промежуточные ссылки или наименования, таким образом, можно большую часть кучи описать лишь одним выражением $x \xrightarrow{a_1, a_2, a_3} y$. Это выражение означает многое: существуют указатели x и y , существует гарантированный путь между ними и естественно весь путь описывает отрывок графа кучи. В линейных списках, а также в деревьях указатели next, если таковы имеются, упускаются по умолчанию. Фактически одно выражение по Бурстоллу описывает весь линейный список. Совокупность таких выражений описывает граф кучи. Рассмотрим следующую структуру данных в виде «кактуса» (см. рисунок 42):

Для описания понадобятся лишь два выражения. x_1 является указателем, который выделен на стеке. Допустим, все остальные ячейки не имеют указателей, следовательно, она расположена в динамической памяти. Удобная, хотя и компактная, запись ломает обозначенные ранее критерии минимальности. Поэтому, запись Бурстолла далее не используется, но, рассматривается возможность абстракции с помощью предикатов для более гибкого описания, которое основано на гранях графа.

Для полноценного анализа указателей и динамической памяти со стороны выразимости нет необходимости разрешать доступ к динамической памяти с любыми выражениями вычисления адреса. Все операции доступа целиком могут быть выявлены писанием и чтением динамических ячеек. Если по причинам быстродействия нужен произвольный, последовательный доступ к памяти, то это является типичным сценарием применения стека. Однако, выделение любого доступного размера, допускается как для стека, так и для динамической памяти. Надо понимать, что память выделяется как один непрерывный сегмент и проверка на «неверные», «висячие» ячейки и на свойство «мусора» там, естественно, не проводится. Нетрудно себе представить вспомогательные функции, которые могут произвести любые преобразования типов с данным сегментом памяти, поэтому этот вопрос далее

не рассматривается. Обоснования и путь доступа к объектам имеют только указатели. Объектные экземпляры рассматриваются как структуры, выделенные в динамической памяти, в отличие от классических структур, например в Си [243], которые, либо расположены на стеке, либо в процессорных регистрах. Второй вариант принципиально не исключает подключение динамической памяти. Нужно отметить, что $e_1.f_1 \mapsto val_1$ может означать, что объект e_1 может иметь ровно два или более полей и в откомпилированном коде $e_1.f_1$ совершенно иным путем будет реально обрабатываться и располагаться, чем $e_1.f_2$ в процессе различных оптимизаций кода [135], [181], [252] и, несмотря на введенные конвенции, всё равно это так. Это не означает раздробление на уровне входного языка и спецификации, где объект должен моделироваться как единый не делимый регион памяти, где поля могут иметь ссылки иных экземпляров.

Как во введении уже было изложено, в ЛРП были внесены целый ряд предложений [224], [223], [51], [121], [193], [195], [194], [44], [281], [27], [26], [190], [233] (см. главу I). Рейнольдс [224] вводит оператор последовательности « \cdot » для неявного определения линейного списка. «Неявно» означает, что не уточняется, каким образом последовательные содержимые связаны между собой, лишь уговаривается, что элементы связаны. Таким образом, из раннего примера кактус можно определить $x_1 \mapsto x_2, x_3, x_4, x_7 \wedge x_5 \mapsto x_6, x_7$. Альтернативы неявному определению Рейнольдса можно считать, либо явное определение, которые всегда допустимое и полностью покрывает неявный оператор, либо по определению ограниченные по длине списки Бозга [45].

Если мы хотим параметризовать кучу, необходимо вводить символьные переменные в утверждениях. Утверждение верное или неверное для данной кучи. Символы априори не типизируются, как термы по Чёрчу, а информация о типе поступает из окружения, таким образом, оно более похоже на типизацию по Карри. Вводя (символьные) переменные, определение предиката относится как параметризованный терм в λ -вычислении, т.е. предикат абстрагирован и подлежит к применению с другими предикатами. Однако, предикат не возвращает иного результата как «истина» или «ложь», а присутствие входных и выходных данных отличается от классических функций (см. главу IV). Рассмотрим рекурсивный пример двоичного дерева из [224]:

$$tree(l) ::= nil \mid \exists x. \exists y : l \mapsto x, y \star tree(x) \star tree(y)$$

Согласно определению Рейнольдса, оператор \star определит кучу, которая состоит из двух

разделяющихся куч. Нужно отметить, как было упомянуто ранее, что изначальное определение \star -дизъюнкции может иметь соединяющие элементы. Таким образом, от одного дерева x всё-таки можно попасть в соседнее дерево y , несмотря на то, что имеется $tree(x) \star tree(y)$ и предполагается, что весь регион под x действительно не пересекается с регионом под y . Нужно, чтобы без изменения данного предиката это могло оказаться невозможным. Однако, при дальнейшей параметризации и при манипуляции предиката (ср. предикат $tree$ в главе IV) проблема принципиально остается. Более наглядно это можно увидеть в рисунке 43.

На основе определения по Рейнольдсу, Бердайн [26] вводит соотношения выполнимости куч в опр.3.7.

Денотационная функция $\llbracket \cdot \rrbracket$ имеет тип $\Phi \times \Sigma \rightarrow Bool$, где Φ множество утверждений о куче, а $Bool$ булево множество. Для линейного списка $s, h \models E_0 \mapsto t_1, \dots, t_k$ с соответствующими типами $\forall i, j \in \mathbb{N}_0. E_j, r(t_i) = \llbracket E_i \rrbracket s$, $1 \leq i \leq k$. Слева от \models записывается состояние вычисления, которое имеет тип $\Pi \times \Sigma$, справа имеется любое булево утверждение.

В [27] Бердайн указывает на проблемы, что фрейм может дистанционно поменяться (см. набл.3.3). Это является проблемой, которую предикатам необходимо учесть. Однако, удаление содержимого ячейки памяти, на которой ссылается глобальный указатель, является отдельной проблемой (см. главу I). Аналогичное касается подпроцедур, которые далее здесь не рассматриваются. Необходимо отметить, что встроенные процедуры с точки зрения выразимости в общем случае могут лишь усложнить спецификацию и верификацию, но вычислимость они не увеличивают. Бердайн справедливо обращает внимание на то, что применение правила фрейма в общем случае может привести к определённым трудностям в связи с недетерминированностью сопоставлений символов. Однако, когда речь идёт о кучах, недетерминированность можно ограничить наименованиями и дополнительными конвенциями (см. главы V, VI). Более того, логические конъюнкты вписываются прямо в язык логического программирования (см. главу IV).

Далее уточняем определение графа кучи согласно [295] и затем вводим синтаксическое и семантическое обозначение согласно предыдущему анализу.

Неявные определения, например, в «SSA»-форме, пользуются успехом, несмотря на то, что чёткого определения, например «зависимости данных» нет и не нужно. В изначальных определениях также имеются неявные определения, которые касательно куч уточняются в этой работе. Соотношения, пространственные операторы и частично неявное определение касаются вершины графа, типизацию символьных переменных и т.д. В главе V

пространственные операторы куч ужесточаются и для константных функций вводится дополнительное обозначение для объектов.

Из трм.3.6, опр.3.8 и предыдущих конвенций (см. [295]) терм кучи может быть определен следующим минимальным образом:

true обозначает тавтологию независимо от того, как выглядит данная куча. Обратное действительно для *false*. Предикат *emp* верный только тогда, когда данная куча пуста, во всех остальных случаях ложна. В главе V конъюнкция ужесточается и распадается на две операции. Для логических утверждений вводятся логические конъюнкции в рекурсивное определение T .

Логические конъюнкции « \wedge, \vee, \neg » не нуждаются в объяснении. Вывоз предиката подразумевает, что соответствующий предикат определен в Γ (при опр.6.5 и закл.6.6). При запуске предиката с целью сравнения с актуальной кучей, все свободные символы должны быть унифицированы термами не содержащие свободные переменные, иначе данный запуск не определён (см. главу IV).

Если в связи с символьными переменными использовать логический язык программирования, то ограничения как одностороннее присвоение и невозможность использования символа вместо значения и многие другие ограничения [26], [27], [195], [193] можно будет снять. Если унифицировать термы, то сравнение простое и «дыры» наполняются нужным содержанием, иначе нужно вручную все подтермы сравнивать и вставлять необходимые термы в нужные места подтермов. Это возможно, но необходимы дополнительные условия, вследствие чего, вводятся всё новые ошибки и ограничения. На практике ограничения наблюдаются в основном тогда, когда ради используемого нелогического языка упускаются полные сравнения или деградируется символьное использование полностью, как вызов по значению. Обычно это наблюдается в императивных и большом количестве функциональных языках программирования.

Возьмем к примеру вызов предиката (подробно о логическом представлении в главе IV)

«?-pred1(s(s(zero)),_)>

где ради простоты первый терм входной, а второй выходной. Запрашивается, существует ли таким образом, анонимная переменная «_», чтобы предикат $pred1$ был выполнен для входящего терма $f(a)$? Если ответ верный, то подцель успешная и результат забрасывается. Если нет, то предикат $pred1$ не соблюдается. $s(s(zero))$ представляет собой целое число Чёрча «2». Если например, вместо $s(s(zero))$ представить $s(s(_))$ и возможно предъявить результат, например

$s(s(s(\text{zero})))$, то без изменений запрос (см. опр.4.3) можно поменять на « $?\text{-pred1}(s(s(_)), s(s(s(\text{zero}))))$ », подразумевая, что предикат определён двунаправленно. Принципиально это касается не только двух, а нескольких направлений. Пролог имеет строгий порядок присвоения и вычисления термов слева направо. Это означает, что символы могут замещать конкретные кучи, но если подцель потребует конкретную кучу, а куча присваивается только в одном из следующих подцелях, то можно, либо порядок подцелей поменять, либо вычисление не завершается успехом (см. главу IV).

Теперь необходимо рассмотреть свойства отображения между определением куч и графом куч, а также свойства отдельных ссылок.

Свойство 1 – Корректность. Если из синтаксического опр.3.9 следует строгое различие между связанной и несвязанной кучей (см. главу V), то синтаксическое описание охватывает любой граф кучи, а также любой граф кучи может быть представлен данным синтаксическим определением. Если нормализовать согласно правилам трм.3.6, например, по пренекс-нормальной форме, то таким образом все, полученные формулы коммутируют. Константные предикаты являются исключением, и поэтому являются односторонним укрупнением: множество выполнимых куч отображается на один представитель множества. Не трудно убедиться в том, что такое отображение не обратимо. Если ещё исключить анонимные символы, то синтаксическое описание полностью соответствует графу куч. Исключив единственные очаги недетерминированного представления, легко убедиться в том, что отображение теперь изоморфное, а, следовательно, не могут быть выражены два различных графа куч из одного описания и наоборот.

Свойство 2 – Полнота. Очевидно, что граф кучи полностью описывается базисными кучами и аннотируется ссылками. Представление значения вершин графа может привести к синтаксическому парадоксу, если не различать адреса ссылаемого объекта. Например, если $a \mapsto 3$ а также имеется $b \mapsto 3$, то на практике это вовсе не означает, что обе ячейки памяти содержащие «3» идентичны. Для моделирования это именно то и означает. Если именно новый объект не выделяется и указатель на эту же ячейку не ссылается, то указатель становится псевдонимом. Избежать этой ситуации можно с помощью аннотации в объектном виде термина.

Указатели на указатели содержат целое число как адрес, и поэтому не отличаются от других указателей. Различие между целым числом и адресом производится за счёт типа переменной. При отображении от графа к формуле порядок вычисления и структура предикатов естественно не могут быть выведены однозначно. Отображение может

быть сгенерировано, но оно может различаться. Если допустить, что дан набор определений абстрактных предикатов, то отображение в общем случае не решимо из-за проблемы приостановки. Отображение от графа кучи к T полностью определено, соблюдая упомянутые особенности. Обратное отображение очевидно полное. Если в $loc \mapsto val$ левая сторона не указатель, то аннотацию можно принципиально решить дополнительным полем $f: loc \mapsto_f val$. Для общей структуры графа кучи дополнительная аннотация не имеет большого значения, поэтому дополнительные поля умалчиваются по определению.

Свойство 3 – Отношение эквивалентности. Для сравнения может быть использовано, что « \mapsto » бинарный функтор, а $a \mapsto b$ куча. Таким образом, можно убедиться в том, что отношение эквивалентности « \sim » может быть обосновано, показав свойства (i-iii). Оговаривается, что « \mapsto » имеет выше приоритет присваивания, чем « \sim ». (i) Рефлексивность: $a \mapsto b \sim a \mapsto b$. (ii) Симметричность: $a \mapsto b \sim c \mapsto d$, то $c \mapsto d \sim a \mapsto b$. (iii) Транзитивность: $a \mapsto b \sim c \mapsto d$ и $c \mapsto d \sim e \mapsto f$, то $a \mapsto b \sim e \mapsto f$.

Свойство 4 – Локальность. При удалении, изменении, добавлении указателя или его содержимого, граф кучи и соответствующий терм меняются минимально. Удаление грани приводит к редукции на одну базисную кучу, либо к параметризации или изменению используемых абстрактных предикатов, т.к. соотношение между обоими, формулой и графом, в общем случае не решимо (см. ранее), поэтому, необходимо предикаты рассматривать отдельно. В свободном от предикатов случае максимальное изменение может повлечь за собой удаление вершины, потому, что это означает удаление вершины и всех граней, которые с этой вершиной связаны. Аналогичное добавление не является «сложной», потому, что добавление грани производится пошагово. В худшем случае для предикатов — использование предикатов может привести к формуле, которая совершенно не похожа на предыдущую. Поэтому, рекурсивные структуры эффективно описываются рекурсивными описаниями и изменение одного элемента не затрагивает остальные элементы, кроме соседних. В общем случае, это лишь эвристика и зависит от конкретного алгоритма и от делимости графа на наиболее независимые подграфы. Также как и эвристика: «граф кучи описывается абстрактными предикатами лучше, чем компактными описаниями». Делимость проблем остается общей проблемой далеко за пределами этой работы, но возможность делить кучи на «удобные» кучи. Это интересно с точки зрения подключения логических решателей (см. главы V, VI, см. [85]).

В заключение этого раздела, хотелось бы сказать о предикатах высшего порядка. Они не имеют

теоретическую значимость для сравнения куч с практической точки зрения. Принципиально предикаты, которые используют предикаты в качестве параметра, интересны с точки зрения выразимости простых и коротких описаний. Однако, рассматриваемые предикаты куч имеют индуктивное определение, а произвольные предикаты высшего порядка в состоянии сломать эти свойства, если не вводить дополнительные ограничения. Поэтому, считается не целесообразно использовать иное, чем формально-грамматическое представление (см. главу VI). Нужно отметить, что при включении предикатов высших порядков меняются в общности существенные свойства доказательств, как например, поток и вызовы с продолжениями, порядок вычисления и обработки подцелей, а также статическая типизация, но с точки зрения выразимости кучи ничего не меняется, по крайней мере после обсуждения такая необходимость отпадает.

Логическое программирование и доказательство

В этой главе рассматривается вопрос, как куча (см. главу III) может быть представлена в Прологе, а затем теоремы о кучах логически выведены с помощью Пролога. Для этого берётся Пролог и определяется синтаксис термов и правил, обсуждается отсечение и применимость рекурсивных определений. Это способствует логическому выводу, который будет решать задачи верификации. Более детально анализируется декларативный характер абстрактных предикатов, который в главах V и VI используется для сближения языков спецификации и верификации. Представление языков с помощью Пролога выявляется на основе выразимости реляций, а также на основе метрик. Предлагается система, основанная на Прологе. Представление и интеграция объектных экземпляров обсуждается.

Пролог как система логического вывода

Данный раздел не представляет собой введение в Пролог, а лежит в основе построения архитектуры верификации куч на основе Пролога. Тем не менее, раздел ссылается на первоисточники Пролога, как [248] и [46], которые рекомендуются изучить досконально, прежде чем, читать далее. Пролог уже оправдался решением трудных теоретических и практических проблем. Например, при доказательстве теоремы Фейгенбаума [142], при доказательстве ошибки с делением вещественных чисел в процессорах «Intel Pentium» первого поколения с помощью логических диалектов «ACL2» [133]/«HOL Light» [213] или при обработке и проверке слабоструктурированных данных [294].

Программа в Прологе задаётся базой знаний, которая задаётся правилами Хорна. Запрос к базе знаний можно задавать одной или более подцелями.

Для определения правил и подцелей необходимо ввести определение прологовского выражения терма.

Символ представляет некоторый логический объект, например: «я», «дед мороз», число «33» или некоторая локальная переменная. В Прологе символ начинается всегда с маленькой буквы, а далее следуют любые буквы или цифры.

В отличие от символа, символьная переменная всегда начинается с большой буквы, либо является зарезервированным знаком «_». Например, переменной *X* присваивается (унифицируется) некоторое значение, например «33», после чего *X* может быть использован далее в сложных термах или подцелях (см. опр.4.2). Когда используется «_», тогда ссылаться на это же значение будет не возможно. Поэтому, «_» используется исключительно в тех случаях, когда должен приниматься ровно один терм, но дальнейшее использование этого значения не предусмотрено, как это обычно бывает в случае сопоставления с образцами термов. Видимость переменных ограничивается данным правилом.

Списки, которые определяются с помощью бинарных функторов «,» или «|» должны иметь хотя бы два компонента. Проверка, является ли список линейным, проводится самими предикатами, которые принимают термы. Примерами списков являются: [12|[]] или [1,2,[4|5]]. Таким образом, базисный тип списков является записью.

Функтор является структурным оператором, который связывает термы и обозначает новое сложное значение. Значение может быть символьным, аналогично объектному экземпляру или записи. Например, функтор списка конструктор «.», который, применив к голове *H* и списку *Hs* работает аналогично [*H*|*Hs*]. Иной пример, это наследник натурального числа *succ*, который имеет арность 1, либо принимает терм Чёрча по арифметике, который опять же снаружи имеет функтор *succ*, либо терм *zero* с арностью 0, т.е. является константной (см. набл.4.13).

На вопрос «да/нет» предикат даёт ответ в зависимости от того, связаны ли некоторые термы согласно данному соотношению или нет — если предикат тотален (см. следующие главы). Например, высказывание *older(plato, aristotle)* означает утверждение «Платон старше Аристотеля».

Синтаксис правила *pred* в расширенной форме Бэккуса-Наура можно определить как:

```

<head> ::= <ID> '(' <term> { ';' <term> } ')'
<rel> ::= '=' | '!='
<call> ::= <ID> '(' <term> { ';' <term> } ')'
<goal> ::= <term> <rel> <term> | <call>
<body> ::= { <goal> '.' } <goal>
<pred> ::= <head> [ ':' <body> ] ':'

```

Здесь *ID* идентификатор, который является символом, но не символьной переменной. Бинарные операторы «=» и «!=» обозначают унификацию, либо утверждение о невозможности унификации данных термов. «.» обозначает конец определения правила. Символьные переменные видны только внутри одного определения правила. Разделитель «:-» определяет голову *head* от тела *body* правила.

Для иллюстрации, рассмотрим примеры из рисунка 45. Рисунок 45 а) содержит два очевидных факта из древнегреческой мифологии: (1) Сократ человек и (2) Цевс бессмертен. Аналогично можно определить иные факты, за достоверность, за что отвечает создатель базы знаний. Фактом по умолчанию является только неоспоримое утверждение из проводимой области дискурса. Третье правило гласит: «любой человек смертный». Технически более подробно это означает: если некоторый терм *X* имеет предикат «человечно», то терму *X* безусловно приписывается предикат «смертно». «Безусловно» подразумевает в прямом смысле отсутствие дальнейших подцелей, кроме подцели *human(X)*.

Унификация термов из опр.4.1 является в частном случае инфикс-нотации, опираясь на *rl*. Более обобщённое соотношение записывается с помощью предиката $p(T_0, \dots, T_n)$. Далее, рисунок 45 б) на примере функции Аккерманна демонстрирует, что любая рекурсия (левая, правая, примитивная, взаимная, и т.д.) может быть определена в Прологе — не только примитивная. Оператор *is* является арифметическим функтором. Функторы по Карнапу [57] являются арифметическими вычислениями термов и не являются логичными. Функция Аккерманна является определённой и тотальной, однако, на практике, из-за ограничения памяти и операционных средств вычисление может быть прервано. По этой причине, предикат полученный из функции может оказаться полезной для проверки терминации алгоритмов для индуктивно-определённых входных данных. Примером могут послужить натуральные числа или списки.

Подцели *goal* как пересчитываемые подусловия выполнимости предиката обозначаются следующим образом:

Интроспекция в Прологе [83] разрешает проверку и определение типы классов, так называемые «виды», данного терма, которые могут быть: *var*, *atom*, *number*, *compound* и иные мало значимые встроенные предикаты. Слияние общих случаев термов к одному виду разрешается, а следовательно, предикаты могут сильно упростить определение предикатов. *atom* проверяет свойство символа, например *atom(a)* или *atom([])* верны, но *atom([1])* или *atom([1,2])* не верны. *var* проверяет, является ли данный терм символьной переменной, которая свободная. Поэтому, *var(X)* верно, но *X=1,var(X)* не верно. *list* проверяет, является

ли данный терм (слабо-типизированным) списком (как это принято считать в Прологе, ср. [83] с [243]). Таким образом, *list([])* или *list([1,2,3])* верны, а *list(a)* не верен. Необходимо отметить, что для определения свойства структуры списка, также как и для встроенного предиката *compound*, используется встроенный предикат «=..», который разбивает данный функторный терм на сам функтор и на список передаваемых термов.

Вызов предикатов рассматривается чуть позже. Однако, унификация термов по определению не производится в Прологе по умолчанию из-за необходимости полного анализа всех подвыражений термов. Поэтому, можно по определению унифицировать $X=X$, но $X=f(g)$ нельзя. Пролог, в зависимости от реализации, может замечать рекурсию в термах, т.к. иногда производится унификация исключительно на верхнем термовом уровне. Но, в примере $X=f(g(X,X))$ часто унификация приведёт к провалу или приостановке в лучшем случае, а в обычном случае к выходу WAM из строя (из-за переполнения стека в версии 1.3.0 «GNU Prolog» [83]). По осторожным оценкам на практике в 95% всех случаев не требуется проверка унифицируемости термов, однако, в общем случае необходимо рассматривать именно это, когда речь идёт об обобщённых утверждениях оценок стабильности, например преобразователей. Также нужно рассматривать границы ресурсов, например с помощью предиката Аккерманна. Поэтому, далее даётся алгоритм, который позволит полностью исключить те 5%, которые корреспондируют с проблемой, например, с определением объектного экземпляра из раздела I-B, см. рисунок 46.

Термы структуры и списки необходимо определить как изложено в рисунке 47.

В главе VI и на рисунке 71 дан пример, когда предикат используется в качестве передаваемого терма. Стоит заметить, что аналогично анализу функтора, вызов предиката также производится для данного стекового окна. Разница заключается в представлении вычислительной модели реализации Пролога и синхронизации стека (см. следующий раздел) между вызванной и вызывающей сторонами.

Далее рассмотрим пример из рисунка 45 б) с подцелями и их вызовами. Дана программа и дана подцель «?-a2(X,1,3)» (см. рисунок 48), которая задается интерактивным интерпретатором. Сначала берётся правило № (1) с сопоставлением σ_1 . Это приводит к противоречивости, т.к. $Res=2$. На рисунке 49 определена система сопоставлений для данного примера дерева вывода). Поиск по данному предикату приостанавливается, т.к. завершился провалом и берётся следующий альтернатив (см. набл.1.5). Выбрав третье правило с сопоставлением σ_2 , а затем, применив второе правило с σ_5 и наконец, применив первое

правило с σ_9 , успешно находит решение. Так как отсечение (см. далее) не производится, проверяются также альтернативы и наконец находится ещё одно положительное решение данной подцели. Путь от начальной подцели через все новые подцели до успешного решения, которые на рисунке обозначены чёрными квадратами, назовём «путь к решению». Для решения данного примера существуют два пути, при этом, результаты не отличаются друг от друга. Нужно обратить внимание, что если даже пути к решению доказательства различны, то после вычисления первого, решение можно было бы полностью приостановить. Однако, это нельзя обобщать.

Рассмотрев пример из рисунка 49, замечаем, что стратегия вычисления может кардинально измениться, если в декларативной парадигме использовать механизм, который позволит отсекаать и менять путь расследования, по крайней мере, по каждому уровню подцели. Например, если приостановить логический вывод на примере из рисунка 48 после подцели «?-a2(N1,1,Res2)» и мы уверены в этом, то всю ветку $(3) \cdot \sigma_3$ можно не проверять. Для этого мы вводим определение отсечения.

Отсечение не означает, что любой алгоритм станет эффективнее или лучше, это вовсе не так. Отсечение даёт лишь возможность, в зависимости от предложенного описания решения проблемы, ускорять нахождение предложенного решения, либо исключать дубликатные решения. Отсечение вставляется в тело предиката как подцель. Рассмотрим теперь семантику «!» на примере факториала в предикате fact из рисунка 50.

Первый терм представляет входное целое число, второй терм представляет результат факториала. Предикат представляет соотношение между входным и выходным вектором, но в данном примере определён только порядок вход-на-выход. Предикат fact2 почти ничем не отличается от первого предиката, разве что, в базисном случае имеется отсечение как единственная подцель бывшего факта. Отсечение приводит к тому, что первый альтернатив fact2 только тогда вызывается, когда входной и выходной терм унифицируются с правилом при запросе согласно опр.4.3, например, «?-fact(5,R).» — это происходит лишь один раз при индуктивно-определённом спуске, когда входное число равно нулю. Когда эта ситуация возникает, отсечение гарантирует, что во всех обработанных подцелях альтернативы далее не обыскиваются. При рекурсивном подъёме альтернативы дальше не рассматриваются. Если при рекурсивном подъёме нет совпадающей подцели, то альтернативные правила должны рассматриваться, кроме отсечённых альтернатив. Поэтому, отсечение в примере fact2 не лишнее. Оно улучшает понятие вычисления подцелей и ее оптимизацию. Обратим также внимание на то,

что порядок правил сильно влияет на корректность. Например, поменяв порядок правил или отсечения, см. рисунок 51.

В этом примере базисный случай не достижим потому, что 0 и 1 также унифицируются в первом альтернативе. Отсечение приводит к тому, что второй альтернатив не будет рассмотрен. Далее N1 присваивается -1 при вызове «?-wrong_fact2(0,1).». В итоге, имеется левая рекурсия, которая никогда не остановится. В данном примере отсечение даже не важно, т.к. левая рекурсия не разрешает рассмотрение второго альтернатива, хотя все логические факты и правила явно определены. Дерево вывода имеет ветвь, которая бесконечна. В Прологе эта проблема лучше известна, как проблема приоризации. Поэтому, ради читаемости правила должны определяться не по любому порядку, а строго по порядку базисного определения: частные и специализированные правила и факты должны определяться первыми, иначе, они могут быть поглощены более общими случаями.

С другой стороны, не поглощённые правила означают, что правила альтернативы могут меняться по позициям. Ради простоты программы, предпочтение всегда должно быть за простыми правилами и одновременно без дополнительных условий касательно порядка. Для достижения этого, необходимо, насколько это возможно, высчитывать входные вектора (см. позже касательно высчитывания куч).

Нужно отметить, что отсечение является синтаксическим сахаром, потому, что отсечение всегда возможно удалить из предиката (см. дискуссию из главы I, переписав его). Доказать корректность исключения отсечения возможно средством дополнительного аргумента предиката, который запоминает достижимость результата. Если результат достижим, то имеется базисный случай, который должен возникать только один раз. Во всех остальных случаях, имеется строго возрастающая цепочка. Поиск результата может быть обобщён и выражен как поиск плавающей точки для μ -выражения. В логиках, в которых допускается отсечение, соблюдается правило (CUT):

$$(CUT) \frac{\Gamma \vdash \Phi, \Omega \quad \Phi, \Delta \vdash \Lambda}{\Gamma, \Delta \vdash \Omega, \Lambda}$$

В контексте Пролога верхние консеквенты формой $A \vdash B$ могут рассматриваться как A подцель тела правила, а B голова предиката, т.е. логический консеквент (следствие). Для дальнейшего обсуждения не будут использоваться консеквенты. Отсечение, возможно, рассматривать, как попытку детерминации. При детерминации множество возможностей отсеивается, так именно и происходит при «!». Отсечение не гарантирует терминации (см. ранее упомянутый пример) и полной детерминации, потому, что всё равно могут возникать альтернативные

ответвления, например последующих «!» подцелях. Когда отсечение происходит намеренно и не угрожает потерям годных решений, то речь идет о «зелёных отсечениях» дубликатных решений, в противном случае о «красных отсечениях».

Обсуждённые решения, ограничения, моделирование правил и подцелей будут применены позже, в частности в главе VI. В связи с вопросом об отрицании, необходимо обсудить вопрос представления литералов, т.е. утверждений и отрицание утверждений (если будет необходимо для определения выразимости утверждений о кучах). Когда речь идёт об отрицании, необходимо рассмотреть выражения, которые строятся термами на основании опр.4.1. Отрицание переменной может создать практическую проблему, т.к. оно определяется контекстом. В отличие от единственного случая, отрицание множества (бесконечного, но индуктивно-определённого), в общем случае не решимо. Нужно отметить, что метод представленный в главе VI — решим, если даже допускаются индуктивные определения, благодаря обсуждённым свойствам, в частности, из-за неповторимости и локальности куч. Очевидно возникает похожая проблема нерешимости для предикатов. Ситуация для функторов в общем однозначно не определена: если дана функция, которая отображает из домена в определённую ко-область, тогда, каким образом можно универсально определить отрицание? — Это лишь гипотетичный вопрос потому, что отрицание по определению применимо только к булевым множествам. Следовательно, необходимо определить отрицание для предикатов в Прологе.

Отрицание в Прологе определяется как провал, т.к. Пролог ищет решение и должен его найти только отрицательным. Поэтому, в Прологе согласно обработке (см. следующий раздел) вводится на уровне тела встроенная зарезервированная подцель fail, которая сигнализирует прекращение поиска альтернатив и возврат к предикату вызова. В общих случаях уговаривается явное прологовское определение отрицания предикатов.

Логический вывод как поиск доказательства

С помощью Пролога было продемонстрировано множество применений в области обработки языков, формальных и естественных [201], [168], [285]. Как будет показано позже, слово данного языка необходимо сгенерировать и проверять согласно правилам. Естественные языки характеризуются мутациями [201], [131] в связи с культурно-социологическим развитием. Таким образом, они сильно отличаются от формальных и формализованных языков. Многозначность является основной разницей между естественными и формальными языками. Тем не менее, изучены методы распознавания естественных предложений [131], [200], которые приводят к интересным итогам

в связи с вопросами искусственного интеллекта и обработки человеческой речи, в общем. Однако, данная работа, сосредоточена на сравнительно простом уровне лексики и растолкования. Задача будет заключаться в нахождении максимально простой и адекватной модели динамической памяти и её проверки. Для реализации прототипа, а также для расследования ключевых задач, будут рассматриваться правила Хорна. Предложенный Уорреном подход «использование предикатной логики для решения логических задач» воплощается частично в жизнь, хотя Уоррен сам предупреждает о том, что его реализация Пролога не в состоянии полностью отобразить логическую «мощь» предикатной [144] логики, из-за теоретических ограничений в связи с вычислимостью. Простой пример проиллюстрирует одну фундаментальную сложность — допустим, имеется функция, где входной и выходной вектор записывается как предикат, т.к. это может быть реализовано в Прологе. Тогда, возможно, для данного выходного вектора, не решимо или очень трудно решить обратный результат, например в случае разовых функций для шифровки сообщений, либо функции, которые не полностью определены (в обе стороны) и имеют, например, двухмерное отображение в качестве эллипса. [200] расследует подробно методы перебора, но, увы, теоретические ограничения синтаксического анализа не принимаются (полностью) к сведению, поэтому перебор оказывается сильно ограничен, в связи с распознавателями категории LL(1) или слабо расширенные от него анализаторы. Это очень ограничивает выразимость в целом. [299], [292] показывают, что если речь идёт о генерации и проверке данных (в статье представлены исключительно как термы), то:

- 1) Синтаксический анализ является непосредственно ограничивающим фактором выразимости. Если выражения расширены и искусственные ограничения, а также упомянутых, а также и существующих подходов исключаются, то синтаксис и семантика всего процесса проверки могут быть сильно упрощены без потери общности.
- 2) Упрощение также может быть достигнуто ради обобщённой формы промежуточного представления. Однако, в статье речь не идёт об императивных языках.
- 3) В частности, из-за выбранной в статье функциональной парадигмы для сравнения, возникают проблемы с незначительно раздутым описанием. Отметим, что функциональное описание состояния вычисления всё равно удобнее и проще любого императивного представления. В общем используются лишь 5 функционалов высшего порядка, как например,

concatMap, foldl. Если бы использовалось логическое представление, то можно было бы семантику процесса проверки более близко сформулировать в стиле математико-логических термов, а это более важно в этой работе.

[294], [292], [293], [299] и [306] показывают, что на первый взгляд нестандартный путь, может привести к очень простому, но эффективному решению проблемы проверки с помощью термов. Причина разносторонняя: представление трансформации термов в виде правил и компактность (проводилась широкая экспертиза по отношению к иным функциональным языкам, т.к. императивные языки сильно ухудшают все показательные метрики измерения качества и компактности записи). Причина простоты лежит в сравнении данной программы и её описания, которая вписывается в регулярное выражение в более обобщённом виде, даже в контекст-зависимое выражение, в частных случаях, как было продемонстрировано на примерах вызовов процедур. Проводятся качественные анализы по каждому из входных операторов и количественные сравнения, основанные на метриках. Полученный результат неожиданный потому, что почти по всем сравниваемым параметрам представление и решение в Прологе торжествует к сравнению с функциональным представлением [294]. Далее результаты обсуждаются в разделе IV-С.

Предпосылкой этому тезису является то, что метод(-ы) синтаксического перебора позволяет решить проблемы доказательства динамических куч. Как это решить реально, какие для этого имеются условия и почему должны соблюдаться, объяснения даются в этой работе.

Позже вводится модифицированный диалект Пролога, который способствует к решению целого ряда проблем в связи с автоматизацией доказательства теорем (ср. главу I). Таким образом, язык похожий на Пролог, квалифицируется не только как язык, а как теоретический метод и инструмент к целому ряду проблем. Особенность Пролога заключается в том, что доказуемо только то, что выводимо (см. набл.1.13). Если что-либо не выводимо, то причина может лежать в правилах, в представлении правил (например, в абстракции), в ограниченности основной выводимости, а также в формулировке подцелей. Также могут иметься практические ограничения со стороны синтаксического анализа.

Идея использовать синтаксический анализ, в качестве решателя куч, появилась после некоторых наблюдений (см. главу VI):

- 1) Прологовские правила довольно компактны и очень хорошо приспособлены к решению логических задач.
- 2) Программа Пролога представляется правилами. Вывод правил генерирует дерево. Доказательство

теорем имеет структуру аналогично программе (изоморфизм обсуждённый ранее), это же относится к запросу или запуску программ, которые тоже генерируют дерево.

- 3) При необходимости выражения можно синтаксически анализировать. Локальность ссылочных моделей памяти ограничивает выразимость соответствующих генерируемых грамматик так, что ранг класса формальной грамматики не должен превышать ранг контекст-свободных грамматик. Это очень полезно с практической точки зрения.
- 4) Однажды, на одном мало интересном докладе пропагандист «Semantic Web» пробовал рекламировать свой новый подход, как подход будущего, как минимум в следующие 25 лет. В качестве защиты использовался аргумент, что «Semantic Web» решит почти все актуальные проблемы, технические и научные. Также упоминалось, что «Semantic Web» высшие по абстракции и устаревшие методы, как например, синтаксические, давным-давно решены и не имеют будущего. Как я сегодня понимаю и думаю — докладчик немного преувеличил, если даже считать, что синтаксический перебор можно действительно рассматривать как очень хорошо изученным. Несмотря на это, всё равно синтаксические методы могут пригодиться и сегодня, а также помочь решить реальные проблемы в области автоматизации доказательств.

Теперь необходимо заметить и сравнить цели дисциплин:

1. Программирование
→ нахождение решения
2. Логическое программирование
→ нахождение (логического) решения
3. Синтаксический анализ
→ нахождение (синтаксического) решения

Если отображения пунктов 2 и 3 типизировать, то получаем характеристики из рисунка 52.

То есть, если удастся сблизить входные множества, то решение одним подходом может быть сопоставлено решению другим подходом.

Упомянутые ранее подходы для распознавания естественных языков отличаются от формальных языков тем, что в них имеется некоторая степень неверности или отклонений. В рассматриваемых языках, отклонения практически отсутствуют.

Согласно лем.4.6. Семантика (1) по вызовам (декларативное свойство предиката) означает, что предикат рассматривается строго как процедура со стеком, которую можно выразить. То есть, создаётся стековое окно (см. рисунок 54) при вызове предиката, а после вызова окно утилизируется. Аналогично

параметрам по ссылкам в императивных языках программирования, унифицируемые термы, которые используются в различных слоях предикатов (т.е. которые расположены в последовательных стековых окнах – нарушение последовательности без глобальных хранилищ приводит к потере термов) передаются вызывающим предикатам. В отличие от императивных языков программирования, переменный символ может передаваться не только непосредственно, но и также как частица сложного унифицируемого терма. Это означает, что передача из одного слоя предиката в другой по умолчанию, может практически привести к построению сложного объектного экземпляра, за нулевую стоимость и преобразовать довольно сложный процесс трансформации объектов, что очень замечательно. Обратим внимание, что благодаря анонимному оператору «`_`», встроенному предикату `concat` и другим предикатам высшего порядка, нетрудно создать мощную выразимость. Выразимость резко повышается ради простоты выражения и сравнения данных частей функтора и структур в общем (включая списки), потому, что исключается необходимость определять весь перечень элементов списка, но, в отличие от сопоставления с образцами, остаток не теряется, а лишь остаётся без изменений, что упрощает описание простых операций. Напомним, что верификация куч происходит пошагово после каждого программного оператора, обычно меняется только маленькая часть всех куч.

Вызов предикатов из рисунка 53 осуществляется согласно модели «чёрного ящика», который можно отследить в Прологе, включив трассировку. Вызов предиката, т.е. подцели, обрабатывается независимо от содержимого предиката и имеет четыре возможных результата: (а) *call*, вызов, создаётся стековое окно, передаются присвоенные термы, (б) *exit*, возврат при успехе, когда все подцели тела выполнимы и голова предиката унифицируема, (в) *fail*, провал, когда хотя бы одна подцель невыполнима, или (г) *redo*, повторная попытка, когда (в) происходит в одной подцели, то находится альтернатив данному предикату, если он существует. Опасность не аккуратно сформулированных предикатов является не эффективной из-за широкого перебора альтернатив. Другой экстремальный случай возникает, когда применяется отсечение настолько часто, что годные результаты исчезают. Оба случая необходимо устранять. Предикаты *call* и *fail* из рисунка 53 действительно существуют в «GNU» Прологе [83], пятый случай «исключения» удалён из-за причин, обсуждённых в главе I.

Семантика (2) интерпретаций предикатов подразумевает, что предикат является генератором недетерминированности. Общий предикат может иметь (как обсуждено в главах I и VI) а) различные определения для различных комбинаций входных и

выходных векторов, а также б) различные выводимые результаты для одной подцели. Например, если имеется предикат *mortal* из рисунка 45 (а) и к нему ещё добавить несколько фактов, то согласно б) из подцели «`?-mortal(X)`» выводимы следующие результаты: *X=socrates*, *X=plato* и т.д. Если для функции Аккерманна вызывать «`?-ack(0,X,15)`» или «`?-ack(1,1,Res)`», то в зависимости от реализации, предикат, либо определён (но, возможно, очень долго занят или не подлежит практическому вычислению в связи с ограничением памяти), либо не (полностью) определён, как, например, на рисунке 45 (б). В примере для данного выходного *Res* предикат не определяет входной вектор, хотя математико-логическое определение явно существует согласно данной схеме, которая практически без изменений стоит в данных прологовских правилах (см. набл.1.5,набл.1.13). Дискуссия касательно этого ограничения, также в связи с обратимостью и представлением реляционной модели, продолжится позже в данной главе.

Как уже упоминалось, Пролог не является каким-то «универсальным решением всех задаваемых логических проблем» априори [266], [267]. Это правда, что не всякое доказательство можно решить прологовскими подцелями в связи с ранее обсуждёнными фундаментальными ограничениями. Однако, обратное всегда возможно. Задача заключается в минимизации проблем, которые будут лучше решаться в связи с сближением языков. Подмножество языков Пролога используется для решения целого ряда проблем верификации в связи с представлением и методом логического вывода. Охарактеризуем подцели и аргументы термы:

- Встроенные предикаты, как например `concat`, могут быть использованы везде в программах. Кроме того, имеются предикаты, которые могут добавляться в формальные теории, написанные в Прологе. Зарезервированные предикаты и функторы могут быть определены мульти-парадигмально.
- Отдельное и перегруженное значение. Отдельные предикаты могут быть перегружены так, что предикат с подходящей арностью, который определен ранее, используется первым. Этот механизм позволяет подключение прологовских теорий, в том числе мульти-парадигмальность. Полученный эффект, это расширяемость, вариабельность, гибкость и полиморфизм. Кроме того, перегруженные предикаты, как например `concat`, позволяют гибкий порядок сопоставлений входных и выходных термов.
- Операции над кучами являются термами. Вместе с объектными экземплярами, соотношения местоположения куч может быть представлено

термами. По сути, граф кучи представляется полностью термом кучи. Термы являются аргументами подцелей, т.е. (под-)доказательств теорем и лемм о кучах.

Из универсального описания механизма вызовов из рисунка 53 следует поиск с возвратом (с англ. «backtracking»). Эта стратегия просто реализуема рекурсией над предикатами, и точно описывает деревья логического вывода (см. контекст-свободность прологовских правил с главой VI). Описанные ранее ограничения необходимо обязательно учесть. Когда поиск завершается успехом, то ветка считается доказанной. Когда ветка опровержима, то она, либо не доказана или не доказуема в принципе, либо приводит к явному противоречию. Оба варианта достаточны для установления провала (под-)доказательства, т.к. всегда необходимо доказывать универсальность данной формулы. Если интерпретировать предикаты как декларативные, то предикаты можно с легкостью растолковывать как «процедуры» в императивных языках программирования, т.е. если даже это формально не совсем совпадает, то интуиция совпадает с подходом в решении задачи. Следовательно, можно в действительности рассматривать логическое программирование в Прологе максимально приближено к доказательству. Хотя специфицируются и доказываются свойства о программе, входная программа при этом не отлаживается и не запускается. Как будет показано в более поздних главах, особенность Пролога хорошо распространяется именно для решения постановки проблем динамической памяти. Представление модели куч, абстракции правил, рекурсивные предикаты, логические символы в формулах в итоге увеличивают выразимость. Например, в отличие от обобщённых формул логики предикатов первого порядка, нам удастся найти компромисс таким образом, чтобы построение графа кучи проводилось последовательно. При этом, описание графа проводится снизу-вверх, используя отдельные простые кучи. Логическое представление выражений в формулах разрешает широкую гибкость самих куч, но а также при реализации стратегий над кучами, в том числе и определения правил вывода.

Структура доказательства является деревом, если получается цикл внутри доказательства, тогда получается предыдущее состояние вычисления, которое означает ввод регрессии. Регрессия является индикатором того, что применённое правило не привело к новому состоянию прогресса, т.е. все следующие регрессии состояния подлежат к удалению. Ненужные состояния могли появиться только из-за неверных правил. Если доказательство правил завершается успешно, то и соответствующая подцель доказана, т.к. предикаты в обоих случаях

не отличаются (кроме возможно необходимых переименований предикатов и используемых символов). Поиск Пролога опирается исключительно на дедукции (ср. главу I): выводимо только то, что следует из фактов и правил, иные выводы, например модус толленс недопустимы. На практике это означает, что фальсификация предикатов может быть решимой в общности только, если рассматриваемые множества конечны (например, вводя общие символы для определения класса объектов) и полностью определены. То есть, исключаются случаи, которые могли бы сами себе противоречить. Следовательно, доказательства могут быть раздутыми или классической дедукцией просто недоказуемыми (см. пример исключённого третьего из I). Предикаты могут быть определены конечным образом, хотя входное множество бесконечное. Тогда, отсечение (см. опр.4.4), как провал, может представлять собой отсечение предиката, либо иное явное определение. Идея поиска с возвратом при провале заключается в продолжении следующего неверного предиката по родительской оси за счёт минимальной записи с тактикой переключения стека. В отличие от метода «возврат при провале», метод «возврат с направленным фокусированием» можно считать обобщённым, когда в самом простом случае фокус определяется некоторой целой отметкой и тактика переключения ориентируется на нахождение экстремума этой отметки. Отметка определяет, какая подцель будет доказываться следующей. Если внимательно задуматься, то такого рода задача может быть редуцирована без потерь в общую стратегию вычисления «ветвей и границ» [179]. Обобщением отметки является терм, который также отлично вписывается в головы левых сторон правил с помощью сопоставлений образцами.

Тройку Хора в Прологе можно представлять в качестве предиката с минимальной арностью «3», при этом, первые две компоненты записываются как входные термы, а третья — в качестве выходного терма. Конечно, в общем, предикат может быть обратим, но в данный момент мы не рассматриваем вопрос, что же является объяснением данному следствию и правилу (см. раздел IV-C и следующие). Причины зависимостей в дальнейшем подчёркиваются.

Обсуждение декларативных стратегий основанных на стеке

- Быстродействие. В частности, речь идёт об улучшении производительности «реактивных систем» (систем под наблюдением и контролем другой системы). Хотя Уоррен [266] подчёркивает, что быстродействие не решающий фактор, однако, медлительность может иметь причину в самом алгоритме (проблема определения правил), например в копировании часто используемых

сегментах стековых окон и построении сложных объектов из более простых. Имеются две причины: во-первых, часто копировать, т.е. использовать подвыражения — показывает на (очень) высокую зависимость данных, чего в общем можно избежать с помощью улучшения алгоритма и определения правил. Во-вторых, изменения обработки с поддержкой быстроедействия извне (т.е. мульти-парадигмальной) адаптацией можно при таком подходе существенно ускорить медленные точки, несмотря на дополнительные затраты в связи с загрузкой. То есть, вторая проблема разрешима с помощью вариабельности. Это означает, что предикат может быть заменён иным поведением, но одинаковой спецификацией. Языковые расширения и вариабельность, тоже входят в поле рассмотрения, но уже в разделе IV-C, поэтому, их всегда стоит рассматривать, независимо от данных пунктов.

- Порядок вычисления. Бесконечные списки (как например `take` из главы I) согласно данной операционной семантике [267] полностью исключаются. Операционная семантика полностью помещает список в стек, поэтому, частичное исследование для бесконечных списков отпадает. Частичное помещение в стеке всё равно, но только, если сравниваемый терм уже имеется в стеке, а разница между подвыражениями двух термов минимизируется. Изменение операционной семантики возможно, но требует полного изменения семантики, хотя порядок изменения и эффект вычисления сам по себе маленький. Надо отметить, что если прологовские правила унифицируются, то сравняются разницы между термами (точнее кучами, см. главу VI). Естественным дополнением было бы вычисление снаружи внутрь (см. главу I) термов параметров, но такое требование можно избежать, благодаря ранее не полностью вычисленным символам (под-)термов и не требует никаких изменений или дополнительных затрат, без ограничения общности. Единственный, возможно критический этап, касается обратимости предикатов. Следовательно, единственным фактором изменения порядка вычисления является само определение правил.
- Семантический контекст. Предикаты могут быть перегружены или определены мульти-парадигмально. В обоих случаях проблема зависит исключительно от конкретного данного определения правил.
- IR. Промежуточное термовое представление может в ходе разработки оказаться устаревшим или несовместимым требованием к императивной программе. В этот момент необходимо иметь возможность добавлять и менять существующие

термы (в том числе удаление). Поэтому вариабельность и расширяемость считаются ключевыми свойствами, которые Пролог допускает, в чём можно легко убедиться. Например, если ради локальной оптимизации и быстрого доступа к памяти, необходимо ввести В-деревья [72], [18], то это возможно с помощью индексации встроенных и/или скрытых предикатов, при этом, реализация предиката может по различным причинам проводиться на другом языке программирования.

Не использовать стек, не удастся, т.к. языки полностью свободные от стека и основаны только на рекурсивных схемах, на практике оказались совершенно не пригодными, тем более нисколько не приспособлены к модуляризации и следовательно не рассматриваются далее по практическим причинам. Современные ЭВМ настолько оптимизированы, что процессоры в состоянии ускорить выделение и утилизацию стековых окон практически без больших затрат [123], [215]. Описывающая парадигма состояния вычисления кучи должна быть логической для решения её проблем верификации.

Обсуждение поиска доказательства над реляциями

Предикаты связывают термы, которые состоят из символов, переменных и других термов, в любое определённое соотношение. Не трудно убедиться в том, что количество отображений между A входных и B выходных термов равно B^A . Множество отображений могут быть объединены в одном предикате. Вопрос о том, определено ли и решимо ли данное отображение для данного входного/выходного/смешанного вектора является отдельным и сложным вопросом (смешанный вектор ради простоты не рассматривается). Эта проблема может быть редуцирована на проверку выполнимости логической формулы. Естественно, с практической точки зрения только разработчик несёт ответственность за перегруженные по количеству отображений предикаты. Чем больше количество отображений одного предиката, тем выше его применимость. Для перегруженных предикатов вопрос об обратимости становится всё важнее, т.к. не совершение автоматически приведёт к нетерминации, а, следовательно, к не завершению доказательства. Позже это надо обязательно учесть. С точки зрения канторовых множеств предикат является перечисляемым множеством (возможно очень большое, но дискретное), которое объединяет элементы доменов с элементами ко-области — т.е. похожая концепция. С практической точки зрения это не маловажный универсальный вопрос. Если нам удастся показать универсальные свойства реляционной алгебры по Кодду, то мы её сможем симитировать. Это фундаментальное свойство, которое позволит

достичь уровня выразимости, хотя бы реляционных и объектно-реляционных языков баз данных на практике, что уже покрывает огромную и значимую часть выразимости.

Proof. Полное доказательство тому содержится в моей работе [294]. Доказательство простое и прямое: свойства Коддской алгебры, как например — проекция, связывание и т.д., можно заменить в правилах Пролога один к одному на каноническую запись без коллизий (см. рисунок 55).

Также обратное доказательство производится. При этом могут потребоваться шаги канонизации и удаления отсечений, что в общем случае можно всегда совершить, как это было ранее продемонстрировано. \square

Здесь нельзя не заметить, что например [149] задавался частично проблемами более эффективного представления входных и выходных данных. Итог расследования приводит к тому, что удобное представление может быть дано логическим видом, но не функциональным. Работа [205] расследует фундаментальные свойства доменов как реляций. Она посвящается большей частью доказательству существования инварианта реляций. Использование инварианта остаётся интересным и частично открытым вопросом в связи с улучшением кэширования куч в спецификациях (см. главу V). Примеры, где инварианты реляций пока что имели наиболее широкое поле применения, это «нумеральная логика» [204], [49].

После того, как мы ввели реляции и обосновали их свойства, сразу наблюдаются приятные свойства:

- Декларативность. При логическом выводе, арифметические вычисления не столь важны. Важны объекты, т.е. кучи и их взаимосвязи. Это не только вопрос «вкуса», но особенно является фундаментальным свойством именно логической системы. Пролог представляет собой среду представления и обработки знаний. Кучи являются атомами или сложными термами, а правила предикатами куч. Псевдонимы являются символьными переменными, которые используются в других местах или более того. Этого достаточно, чтобы определить теории куч.
- Терм-Дерево. По теореме Биркгоффа (о термовых продуктах) [202], [79] из абстрактной алгебры следует, что каждый терм корреспондирует с представлением в виде дерева. Преобразование, увы, не обязательно однозначное, если не проводить нормализацию. Таким образом, обратное преобразование однозначно определено. Отсюда сразу возникает необходимость, либо определить канонизацию для выравнивания деревьев, либо устранить, например ассоциативность, по которой выравнивание

деревьев было бы дано неявно (см. главу V). Мы не хотим сами себя ограничивать в том, что кучи могли бы быть только деревьями. Мы хотим, чтобы куча могла быть любым графом (см. главу III), поэтому допускается описывать кучу только одной вершиной. При этом, всё равно, вершину представляет простая или сложная куча, т.е. она является обыкновенной кучей или объектным экземпляром.

- Генерация термов. Тематическое исследование [294] показывает на то, что Пролог отлично приспособлен для обработки термовых структур, в отличие от функциональных/императивных языков программирования и трансформации. В исследовании использовалось большое количество примеров. Также проводился количественный анализ. Использовались метрики как компактность, уровень выразимости и интеллектуального уровня языка и многое другое. Для широкого объёма примеров, практически без всяких исключений, Пролог превосходит чётко с большим отрывом.
- Проверка термов. Тематические исследования [299], [306] показывают, что если процессы генерации и проверки термов сблизить, то основным твёрдым ограничением является выразимость языка проверки. В исследовании, без потерь общности, рассматривается обобщённый регулярный язык. Процесс сравнения термов слабо структурируемых данных можно интуитивно понять, либо как сравнение одинарных элементов, либо иерархических элементов с возможными дырами, которые наполняются данными во время запуска. Терм, как обобщённое представление, является уникальным IR и может быть широко использовано в различных областях, например для верификации. Операторы описывают не программу, а структуру генерируемого документа. Статически, цикл не всегда может быть ограничен, поэтому цикл вершины a некоторого дерева в XML-документе описывает лишь a^* . Отсюда ясно, условия цикла могут быть представлены и проверены только самым общим видом. Естественно, конечным автоматом так и не удастся распознать $a^n b^n$, но это и не главная цель исследования. Выходит, что главным ограничением проверки всегда является выразимость языка утверждений (выражений). Далее, главным результатом вместе с [294] является то, что реляции лучше приспособлены для представления знаний с термами и логическими правилами трансформации, чем функции, которые вычисляют для каждой «дыры» необходимые данные. Получается, логические соотношения ссылаются на имеющиеся компоненты. В [294] под логическими правилами

трансформаций в основном подразумеваются $\tau \rightarrow \sigma \rightarrow \tau$, где τ представляет некоторый терм IR, а σ среда, содержащая символьные присваивания. Если эту трансформацию расценивать как реляцию в качестве предиката, то трансформацию можно расширить как $\tau \rightarrow \sigma \rightarrow \tau \rightarrow \mathbb{B}$, где \mathbb{B} булево множество. Теперь верификация куч может быть представлена таким же семейством трансформаций, как и верификация куч. Её главная разница заключается в использовании (абстрактных) предикатов и в методах автоматизированного вывода. При трансформациях используемые термы — модели куч, различаются. В отличие от регулярных выражений и возможных распознавателей [50], схемы спецификаций в основном контекст-свободные. Предсказания следующего элемента в обоих методах являются одной из центральных операций, которые могут существенно отличаться.

Решение и доказательство этому тезису изложено не только в этой главе, но также и в последующих. Кроме термина можно использовать и другие промежуточные представления, как например тетрады, польско-инверсную запись, триады и другие. Преимуществом термов при описании состояний куч, как было упомянуто, в первую очередь является простота и максимальная выразимость. Термовое представление программных операторов может быть записано в Прологе непосредственно. Преобразование в другие IR отпадает [291], [181]. Однако, термовое представление в Прологе имеет то преимущество, что все термы и подтермы не нуждаются в дополнительных контекстах, конвенциях и дополнительных фазах преобразований. — Их «можно написать просто так». Это не только облегчает возможное использование в учебных целях, в быстрой прототипизации, но, а также облегчает преобразование и переписывание термов за счет прямого представления и анализа правил переписывания (см. [19], [87]). Аналогичные реализации на более реальном уровне являются, например, «LLVM-биткод» [253], GCC «GIMPLE» [171] или аннотированные объекты в качестве IR в проекте «ROSE» [228]. Во всех случаях, которые используют тетрады, необходимо предварительное IR входной программы преобразовать в синтаксическое дерево преобразуемое в тетрады. Синтаксический перебор в «LLVM» производится более гибко, чем в «GCC» с помощью представленного этапа и может быть совершен с помощью среды синтаксического анализа «CLANG» [251]. Дерево перебора может теоретически быть введено без «clang», но на практике это совершенно немыслимо, потому, что, даже крайне простое дерево, всё равно может и будет представлено очень большим промежуточным представлением,

если «LLVM» заставить вручную ограничиваться неэффективным и полным отсутствием всех дальнейших трансформаций IR. Несмотря на раздутые наименования и на первый взгляд «ненужные» синтаксические определения, гибкость и расширяемость сильно повышены в отличие от «GIMPLE».

Ради ограничений и простоты, в отличие от «биткод», реализация в Прологе исключает безусловные переходы к любому программному оператору. В реализации не стоит приоритет обеспечить максимальный объём программных операторов, если в будущем имеется возможность подключения любых иных программных операторов. Более важным вопросом является расширяемость и вариабельность модели кучи: «можно ли простым образом модифицировать кучу так, чтобы имитировать любую пошаговую манипуляцию кучи?», «Можно ли добавлять всё новые фазы и правила логического вывода?».

Принципиально, нужно заметить, что выбранное промежуточное представление естественно может быть преобразовано из Пролога, например в биткод или «GIMPLE», но практическая реализация не стоит вопросом исследования. Прологовские термы представляют собой программные операторы (а также спецификацию и правила вывода) и как ранее в этой главе обсуждалось, могут быть представлены в качестве дерева. Да, можно выбрать тетрады инструкций (например, близки ассемблеру некоторой целевой машине), но, первым итогом синтаксического анализа всегда является синтаксическое дерево (см. рисунок 12). Выбрать другую модель означает, что одна и более фазы из упомянутых на рисунке 12 просто пропускаются. Это простое замечание, но, увы, этот принцип часто (не умышленно) нарушался и нарушается в истории проекта «GCC», «LLVM», а также в проекте «jStar» [193], где верификация проводится на уровне оптимизируемых триад, коротко до и во время генерации кода и многих других проектов в области статических анализаторов — совершенно независимо друг от друга. Хотя замечание простое, последствия могут приводить к необходимости определять точно, в какую фазу анализ псевдонимов всё-таки нужно включать и это обычно является очень непростым вопросом. Важность заключается в следующем: (1) иметь вообще возможность расширять и менять существующие этапы анализа динамической памяти, а (2) возможность адекватного представления для того, чтобы избегать раздутые и сложные семантические контексты и множество экстерных хранителей. Отсутствие возможности №2 является признаком тому, что описание модели сильно усложняется. Простота модели зависит от полного представления всех необходимых данных. Прежде всего, это касается термовых представлений входных

программ и при необходимости семантических полей содержавшие данные из рисунка 12. Дополнительные данные не упомянуты на рисунке 12, но всё равно могут потребоваться на локальных фазах, а следовательно, не вовлекают за собой модификацию общей модели вычислений для работы с динамической памятью (см. рисунок 56, см. набл.1.14).

Преимуществом термов является их явное представление и явная манипуляция ими. Отсутствие их явного представления приводит к конструкции вспомогательных подтермов и к введению семантических полей (например, для аппроксимации какого бы ни было лимита).

Совместимость языков

В введении было описано, как замечают критики верификации, что часто дисциплина характеризуется «чисто академической, без практического применения». Основными причинами тому, являются: перечень конвенций к отдельным моделям, которые часто имеют резкие ограничения при сильно раздутом формализме. Из предыдущего раздела, особенно из тез.4.11, можно заметить сильные обобщения относительно языков спецификации и верификации для проблем динамической памяти (см. главу II, см. набл.4.12):

Наблюдение на первый взгляд может казаться малозначимым. Однако, оно означает, что для верификации троек Хора удобнее использовать логический язык программирования, спецификации и верификации троек, что на первый взгляд является очевидным. В реальности немногие системы верификации были построены на основе логической парадигмы, поэтому они, слишком ограничены или замкнуты (см. главу I).

Логические предикаты описывают состояния вычислений, именно поэтому необходимо проверять. Например, предикаты в первую очередь не нуждаются в побочных эффектах, чтобы выразить состояние, а в императивных языках они являются основными. Замысел предикатов заложен в том, что состояние можно было бы определить непосредственно без манипуляции каких бы то ни было глобальных переменных. То есть, диапазон видимости зависит от символьных переменных предиката, но не от экстерных хранителей памяти.

С другой стороны, на примере модификации Пролога, единицы логики могут быть сопоставлены один к одному элементами логического языка программирования. С помощью программирования можно решить вопросы верификации куч.

Не связанное с динамической памятью, но похожее применение, наблюдается в рукописи Леммера [149], в которой предлагается логический аппарат для верификации сходимости программных компонентов [93]. Идея его работы заключается в

предложении перехода на логические утверждения для спецификации и верификации, которая опирается на (различную) систему логического вывода из-за целого ряда проблем в связи с объектно-ориентированным программированием, точнее его спецификации.

Упрощение определений какой бы то ни было математико-логической проблемы, иногда означает упрощение или решение проблемы, а, как правило, бывает — наоборот. Часто бывает именно так: чем проще определение, тем меньше существует частных случаев, для которых необходимо вводить отдельные определения. Следовательно, объём годных единиц растёт. Например, сопоставление символам для данного случая $\forall a$ просто, а соблюдение всё новых конвенций усложняет в принципе. Ограничивая a , требуется хотя бы один дополнительный предикат. Это означает, использование квантифицированных переменных может резко увеличить выразимость даже маленьких формул. Аналогичное действует обратно: при инвариантной длине формулы несоблюдение утвержденного, приводит к спаду выразимости — это как раз те проблемы, о которых говорилось в этой и предыдущих главах.

Также можно заметить: если выводятся предикаты, которые содержат символьные переменные вместо конкретного атома, то следовательно, решение будет более общим (в Прологе это происходит автоматически унификацией термов, а на уровне вывода, как метод нормализованной и финитной резолюции [83]). Задача верификации заключается в проверке программы генерируемой структуры данных. Как было обсуждено в предыдущем разделе, проверка ограничивает сильнее, чем построение структуры. Оба процесса обычно различаются. Сложность проверки заключается в выразимости.

Заключение (Минимизация разницы между языками). Проверку куч можно упростить и расширить тогда, когда выражения описываются на одном и том же языке во время (1) спецификации, (2) верификации и (3) во входном языке.

Использование одного и того же языка является экстремумом по задаче минимизации разницы между языками, которое рассматривается до тех пор, пока не будет обнаружен аргумент нарушающий гипотезу, если таковой имеется. Когда ликвидируется разница между (1) и (3), либо будь-то входной язык логический, либо полученное IR в качестве термов из входной программы, то утверждения записываются в качестве подцелей, а входная программа как термы. Утверждения о программе ссылаются на термы входной программы (см. главы VI, V), обратное не допускается. Так как верное предложение является конгруэнтностью, достаточно ликвидировать разницу между (1) и (2). Формулы и любые необходимые им индуктивные определения задаются прологовскими фактами и правилами. Верификация полностью упирается на факты и правила, которые заданы

спецификацией. Кроме того, в качестве тактик, правила спецификации и иных вспомогательных предикатов, предусмотрена возможность включать новые правила в качестве прологовской теории.

Задачи (2) и (3) соперничают следующим образом: (2) устанавливает, как должен выглядеть процесс построения графа куч, а (3) конкретно, исходя только из данных утверждений, пытается доказать верность. Для этого описание должно быть сфокусировано на граф кучи, где процесс верификации является процессом «понимания» и анализа. В главе VI анализ опирается на синтаксическое определение. Предпосылкой тому являются граф кучи и унификация синтаксических, семантических и прагматических определений куч и их проверок.

Ли [184] справедливо замечает, что логики высшего порядка очень важны как критерий применимости на практике. Как было обсуждено в начале этой главы, Пролог поддерживает такую возможность. Правила могут даже меняться, но нет необходимости менять правила во время интерпретации правил (см. главу I). Поэтому, определённые правила доступны в обоих процессах (2) и (3).

Модель кучи описывается спецификацией S и обрабатывается языком верификации V . Пользователь использует V для изменения состояния и следит за результатами через S (см. опр.1.3). Однако, в классическом паттерне по Реенскаугу V непосредственно манипулирует P , что здесь варьирует. P может иметь различные графовые представления S с обсуждёнными ранее свойствами. Сближение приводит также к тому, что основные интерфейсы коммуницируют на одном языке.

Представление знаний

Правила могут в декларативной парадигме быть представлены, в функциональном либо логическом виде. На примерах языков XLS-T и Пролог в [294] проводился количественный анализ по обработке слабо структурируемых данных (также как и термы в общем, см. предыдущий раздел). Для качественного сравнения эквивалентных программ проводилось множество проверок более 80 выбранных типичных и образцовых примеров, аккуратно вручную подобраны из множества учебников, монографий и онлайн ресурсов. Прямое сравнение показало (см. рисунок 58):

- 1) Пролог во всех примерах (кроме одного) превосходит в среднем на более чем 30% XLS-T, что можно вывести из соотношения $N_T : N$ и $\eta_1 : \eta_2$.
- 2) В среднем описание той же самой функции в Прологе на 50% короче, а часто даже ещё короче. Обосновано такое решение на N , λ и $\Delta_N = \|N_T - N\|$.

- 3) Функциональный язык страдает от замкнутости, т.к. могут быть использованы только встроенные операторы. В отличие от этого, когда логический язык предусматривает определять термовое IR , любые иные операторы и правила.

Более того, качественный анализ показывает и объясняет, почему выражения и правила в логическом представлении можно выразить намного проще. Это в основном из-за логического представления термов и реляций. В отличие от функциональных языков (имеющие компактную денотационную семантику), логически основаны на атомах, термах и правил с приоритетами (см. тез.4.10). Денотационная семантика является декларативной, однако, полный перебор логических взаимосвязей редуцируется только на одно более оптимальное отображение, а результат высчитывается на основе входного вектора. Переменные не являются символьными, а лишь переменными, которые даже в λ -абстракциях используются только в одностороннем порядке: присваивание значения (даже если по-ленивому) при использовании и вычислении функции. Подставкой параметризованных функций взамен реляций проблему не решить, как это наблюдается, например, в [38]. Когда необходимо выразить атомы, выражения и термы в общем, а также определить потенциально любые соотношения между ними, тогда разумнее ориентироваться на аксиоматическую семантику или семантику, основанную на соотношениях. То есть, успех представления знаний трансформаций и сравнения с существенной частью зависят от выбранной парадигмы, как было продемонстрировано в работах [294], [292].

Кроме ранее упомянутых особенностей, имеются следующие, которые необходимо учесть при верификации динамической памяти:

- Правила компактны и могут быть вызваны из любой позиции интерпретатора. Цели и подцели могут быть любыми. Нетерминация в общем неизбежна и искусственно не ограничивается. Однако, ради более эффективной обработки, в главу VI может вводиться не значимое ограничение.
- Используется строгое вычисление термов, ленивое вычисление исключается. Это приводит к тому, что некоторые ситуации, например, передача рекурсивных данных Аккерманна (см. рисунок 45) не может осуществляться до тех пор, пока не будут вычислены все аргументы. Это ограничение практически не является значимым, т.к. всегда возможно написать программу без употребления незавершённых данных таким образом, что контроль записывается в тело правила. Более того, термовая унификация уже приводит к тому, что неопределённые частицы термов, т.е. символьные

переменные присваиваются и при определении нет необходимости вычислять всё заново потому, что присваиваются лишь ранее неизвестные подтермы, а сам терм не меняется. Это возможно согласно принципу из рисунка 54.

- Базовый тип верификации является термом. Далее он может быть рассмотрен как параметризованный тип λ -вычисления третьей степени, т.е. тип из $\Lambda_{T\lambda 3}$, который допускает квантифицированные переменные. Тип, который построен из других типов, это зависимый тип (см. опр.1.9). Построение проводится согласно опр.4.1 с помощью функтора. Таким образом, сравнение термов может быть формализовано как проверка термов, однако, термы могут теоретически содержать сами себя в Прологе, благодаря символьным переменным. Практически этого можно избежать, если использовать проверку на самосодержащие термы (см. предикат `unify_with_check` вначале главы). Чем выше уровень λ -вычисления, тем сильнее действуют ограничения, а это означает, что меньше ожидается парадоксов. Функторы могут быть использованы для моделирования любых сложных структур данных, в том числе списков, деревьев и объектных экземпляров.
- При успехе подцелей, выдается подходящее множество сопоставлений, например:

$?-H=pointsto(a,2), VC=pointsto(a,X), H=VC.$

приводит к результату: $H = pointsto(a,2)$, $VC = pointsto(a,2)$ и $X = 2$. Генерацию контр-примера можно встроить в процесс унификации, например `unify_with_check`, если в отрицательных возможностях добавить разъяснение, используя `write` [248], т.к. прямое присвоение некоторых символьных значений невозможно и не имело бы смысла. Необходимо выявить сверху-вниз самый ближайший терм, который несопоставимый со сравниваемым термом. Принципиально, отслеживание модели вызовов можно совершить с помощью встроенной трассировки [83]. Если верификация проходит пошагово, разумно каждый шаг верификации записывать в виде «DOT»-файла для понятия и документации доказательства. Контр-пример предоставляет хотя бы один случай, когда верификация отклоняется. Унификация термов в Прологе приводит к наиболее общему сопоставлению, поэтому несовпадающие функторы по имени, арности или неунифицируемые переменные, являются сценариями отказа. В общем, частный пример означает терм, который может быть приведён в качестве отказа, всегда тогда, когда атом не унифицируем с функтором, либо атомы или функторы различаются.

- Снятие ограничений символьного характера при определении куч [27] для запуска (см. главу II), в том числе и для анализа правил верификации с обеих сторон при дедуктивном выводе ((би-)абдукция) [54], [211], можно осуществить, если правила вывода удобнее моделировать в качестве хорнских правил. Правила Хорна позволяют, во-первых, квантифицировать \forall, \exists переменные в зависимости от того, где символьная переменная определяется и как она связана. Во-вторых, перебор правил и альтернатив может привести к успеху при поиске без дополнительных затрат. Однако, ради применимости, нужно объём альтернатив ограничивать. Если выбирается правило, то абдукцию можно имитировать следующим образом: дано правило Хорна «`b:-a1,a2,...,an.`». Если некоторые из a_j оставлять неопределёнными, т.е. имеют символьную зависимость, то, таким образом, могут быть выбраны различные b , если имеются альтернативы. Для этого строго требуется, чтобы начальные термы, аргументы головы b не исключались. Необходимо заметить, что Пролог не нуждается при выбранной модели кучи в дополнительных правилах, потому, что лексикографический порядок по указателю простых куч и возможностей уникального выбора (простых куч) встроенных предикатов по работе со списками, как например `concat`, уже дают широкий круг выбора и преобразований новых термов из старых подтермов. `concat` и иные сканирующие одним ходом предикаты эффективны благодаря свойству неповторимости. Поэтому, целый набор преобразовательных и вычислительных правил отпадает. Без ограничения общности, правила вывода обратимы, если между всеми подтермами предусловия и постусловиями, либо существует изоморфизм, либо необратимые встроенные предикаты декларативно в обратном случае не вызываются. В случае, когда изоморфизм нарушается, то, либо в отображении от входного вектора на выходной, либо в обратном случае производится расширение (см. абстрактная интерпретация из главы I). Расширение является проблематичным при обратных отображениях, т.к. относительно кообласти происходит сужение домена, т.е. отображение становится прерывным.
- Перегрузка значений правил может осуществляться и пополняться различными телами, которые внутри могут реализоваться, например, на языке Ява, до тех пор, пока коммуникация осуществляется с помощью входящих, выходящих и комбинированных термов. Для анализа прологовских правил не достаточно использовать «DCG» (см. главу I), потому, что необходимо изменить контроль и тактику

выбора. Лучший пример может обсуждаться при принятии стратегий восходящих и нисходящих синтаксических анализаторов (см. главу VI).

Архитектура системы верификации

В [300] и [298] предлагается архитектура верификации с динамической памятью на основе Пролога. Архитектура представляется на рисунке 59. Архитектура следует ключевым принципам, которые были обсуждены в главе I, это: (1) автоматизация, (2) открытость, (3) расширяемость и (4) обоснованность. (1) гласит о том, что доказательство находилось автоматически. В Прологе решение будет найдено, в зависимости от данных правил, если в правилах исключаются циклы и даны все необходимые правила, иначе, тогда доказательство не завершается, либо завершает верификацию преждевременно. Далее, с помощью подхода, в главе VI происходит автоматизация. (2) означает, что искусственные ограничения между термами, правилами и возможными реализациями должны отсутствовать. С одной стороны Пролог является открытым, т.е. могут быть добавлены все новые правила, а имеющиеся могут быть обновлены, если их определить ранее. С другой стороны, Пролог замкнут тем, что только то выводимо, что следует из данных правил согласно дедукции. Пункт (2) относится к архитектуре и используемым моделям представления памяти. (3) означает, что модель памяти может быть расширена и при необходимости изменены данные правила. Изменения всегда разрешаются благодаря переопределению правил Хорна. Расширяемость термов и правил также обсуждалась детально в предыдущем разделе. (4) означает, что любой шаг верификации можно отслеживать и проверять, как обоснованные шаги логического вывода. Генерация «DOT»-файла визуализирует вычисление проверки, а при отказе генерация контр-примеров даёт более подробные результаты и предпосылки. Возможность интерактивно без соблюдения каких бы то ни было конвенций сильно упрощает и способствует проверке на обоснованность принятых решений.

На рисунке 59 на вход поступает данная программа, предпочтительно на языке Си (или другом императивном), который вместе с утверждениями о программе преобразуется в прологовские термы и правила. Синтаксический, а затем семантический анализ проверяет и исключает недопустимые типовые ошибки и основные ошибки нотаций. Термы всегда можно визуализировать в файловом формате «DOT». Утверждения могут ссылаться на леммы и теоремы, которые могут быть записаны непосредственно на языке Пролог и при необходимости могут быть использованы при верификации. При верификации включаются различные правила, которые задаются в теориях Пролога и загружаются динамически

при интерпретации, например средой [82], [81]. Для решения отдельных теорий могут быть использованы, либо экстерные средства механизмом мульти-парадигмальной системы, либо подключением некоторых произвольно определённых SAT-решателей в самом Прологе. Напомним, Пролог широко используется в области решателей и «Constraint Programming». Новые этапы решения проблем динамической памяти могут быть подключены согласно принципу из рисунка 56. Переходы между маленькими и большими фазами совершаются, благодаря передаче состояний вычислений, т.е. процесс работает согласно потоку данных (см. рисунок 59) и может быть сравниваемым с общей архитектурой существующих конвейеров [135], [252]. Зависимость данных отличается от классического потока данных [137], из-за блока видимости динамически выделенных данных (см. главу III), который обычно не соответствует автоматически выделенным переменным на стеке. Однако, инфраструктура предложенного конвейера принципиально может быть использована при условии, если анализ псевдонимов установит отдельные интервалы видимости, см. набл.3.4.

Далее в [301] обсуждаются и предлагаются основные критерии для расширяемой и модифицируемой архитектуры. В первую очередь это относится к минимальности IR входного языка, который к сравнению с «PCF» [179] допускает присвоение для основы объектного вычисления по Абади-Карделли (см. раздел I-B), неограниченный цикл и вызов процедур. Так как представленная модель вычисления, согласно классному виду вычисления, может быть типизирована по Абади-Карделли (обновления кода во время запуска исключаются, например, передача аргументов производится выборочно, либо по значению, либо по вызову с особенностью вставленной конструкции более широкого функторного объекта), то и свойства, согласно второй и третьей степени λ -вычисления, (см. опр.1.9 и опр.1.10) применяются непосредственно. Расширение может быть применено к входному языку программирования, к фазам статического анализа и правилам (включая имеющиеся).

В [302] вводятся фрейм, куча и их интерпретации, а также даётся предложение практического представления в Прологе. Так как куча предположительно представляется как терм, который принадлежит предикатной интерпретации в Прологе, тогда: либо верно и меняются все неопределённые символьные переменные подцелей, либо даётся отказ с предположительной причиной. Верификация похожа на такой же процесс сравнения, как представленный в [299], [306], т.е. автоматом сравнения по образцам и деревьям (с англ. «tree graph matcher» [66]). Хотя изначальная модель постановления процесса очень похожа, всё равно её сравнение тяжелее, например:

за счёт вызовов процедур, абстрактных предикатов, пред- и постусловий и моделей графа кучи. Таким образом, из аналогии следует: если утверждения являются схемой/типом, а программа пошагово строит выражение, т.е. граф кучи, тогда верификация является проверкой типов. — В том случае, если означает содержимое (см. рисунок 13)?

Заключение (Минимизация входной программы). Результатом проверки содержимого является минимальная входная программа, которая манипулирует динамической памятью.

Ответ кажется простым: входная программа. Однако, соотношение между «типом» и «выражением» не может быть однозначным. Возникает вопрос, а какая действительная программа генерируется? Суть в том, что программа генерируется пошагово только при необходимости в соответствии с «утверждениями». Программа строится минимальным образом, потому, что каждая грань графа куч соответствует всё новым программным операторам. Цикл в графе кучи не обязательно равен циклу в программных операторах, а, например, может быть равен двум операторам. Бесконечно много граней в графах исключается, поэтому только похожие цепочки могут соответствовать циклу в качестве программного оператора, условие которое определяется графом. При конструкции входной программы минимальность означает лишь то, что множество операций, которые не имеют прямого отношения к итоговому графу, удаляются и остаются только те операторы, которые действительно необходимы для построения финального графа кучи. Таким образом, проверка содержимого выражения данного типа может сгенерировать минимальную программу, которую можно сравнить с данной программой.

Архитектура в Прологе без дополнительных затрат разрешает следующее:

- Любой входной язык допускается, если термовое IR соблюдается, которое также может быть изменено и добавлено в правилах. Входная программа может быть даже пуста и процесс синтаксического анализа пропущен, если IR программы или её части вводятся вручную для соответствующей части верификации. Архитектура, представленная на рисунке 59 позволяет исключить синтаксические и семантические ошибки с помощью гибких фаз из рисунка 56.
- Скромные спецификации разрешают избегать полную спецификацию, поэтому специфицируются только те модули, которые нуждаются в верификации. Кроме полной спецификации, никаких альтернатив не было, что раньше приводило к большим затратам и трудно читаемым утверждениям. Этот подход называется «footprint» и наблюдается в области верификации

куч с помощью ЛРП впервые в «Smallfoot». Принцип в Прологе прост, если имеется утверждение, то оно проверяется на верность, если нет, то верификация по умолчанию продолжается. Верификация применяется только для тех модулей, которые содержат утверждения. Чтобы избежать полную спецификацию кучи, надо использовать вспомогательные предикаты, такие как `true` или `false` (см. главу V), а также предположить данные спецификации выборочно и не полностью.

Полиморфизм исключен ради простоты из корневых программных операторов (см. дискуссии в главе I, III и далее). Граф зависимостей заданных правил и лемм утверждений анализируются при запросе интерпретатором Пролога, а также во время синтаксического анализа, например, при построении компиляции (см. главу VI).

Объектные экземпляры

В разделе I-B подробно обсуждались два вида вычислений с объектами — по Абади-Карделли и Абади-Лейно. Из-за широкого распространения в императивных языках программирования с объектно-ориентированным расширением используется первый вид. Как было продемонстрировано и обсуждено в ранних главах, объектный вид тяжелее проследить в связи с верификацией корректности и полноты. С теоретической точки зрения оба вида имеют одинаковую выразимость [155], [220] и полная абстракция может быть всегда найдена (см. ранее). Однако, написание программ может сильно отличаться и тогда доказательство полной абстракции, т.е. равенства операционной и денотационной семантики между обоими видами очень сильно расходится из-за трудной формализации относительно простых свойств объектного вида вычисления (см. раздел I-B). Так как простота спецификации имеет наиболее важный эффект на общую простоту доказательств, тогда выбирается именно классный вид вычисления.

Объект — это, прежде всего, экземпляр некоторого класса. Ради простоты, полиморфизм исключается, т.к. он не имеет прямого отношения к корневой функциональности вычисления (настоящий полиморфизм переменных не рассматривается, т.к. в объектно-ориентированных языках полиморфизм выражается спонтанным полиморфизмом [55] исключительно с помощью подклассов [48]), и представляет собой только более удобный способ вызова подходящего метода во время запуска (см. раздел I-B). В вычислении Хора полиморфизм выразим, но в наших целях предлагает лишь дополнительный эффект без увеличения выразимости (см. главу I, [185]). Поэтому, объект, моделируемый кучу, является замкнутым регионом памяти без дыр, т.е. определённого типа, который содержит лишь

поля. Методы не сохраняются вместе в динамической памяти, потому, что они статические и не меняются во время запуска. Изменение кода во время запуска также исключается из-за минимального успеха и огромных проблем свойств корректности и полноты (см. дискуссию из раздела I-B). Так как объект присвоен данному типу класса, методы полностью определены. Наследственные поля и методы также полностью определены. Для наиболее легкого сравнения объектных экземпляров, соблюдается конвенция, что пары (наименование поля \times содержимое) отсортированы по лексикографическому порядку. Таким образом, проверку и преобразование экземпляра на подкласс, можно реализовать двумя способами: (1) каждое поле проверяется согласно соотношению «>:» (см. опр.1.11), при этом, множество полей в верхних и нижних подклассных экземплярах расходятся или (2) все поля группируются согласно идентификатору наследованности. Таким образом, в памяти необходимо эффективно сравнивать экземпляры нижних классов только с маленьким подмножеством, которое представляет экземпляр верхнего класса. Чтобы продемонстрировать (2), возьмем пример: «SubClass1 s1; SuperClass o1=(SuperClass1)s1;». Допустим, s1 содержит [o1,o2,o3], тогда вычисление o1, где верхний класс в SuperClass1 наследует только поля o1 и o2, может производиться преобразование с помощью копирования первых двух полей, т.е. начальным сегментом s1.

Поля объектных экземпляров записываются в список кортежом (наименования, значение). Ссылки на объектные экземпляры (в том числе циклические), выражаются символьными переменными. $A = \text{object}(A, A)$ запрещается и может быть исключено с помощью `unify_with_check`. $A = \text{object}([(a, A), (b, A)])$ разрешается. Предполагается использовать упрощенную форму: $A = \text{object}((a, A), (b, A))$, т.к. функтор `object` внутри Пролога уже строит список головы, которая содержит `object`. Так, как кортеж содержит ровно два элемента, то сложный терм будет всегда четко определен и однозначен в отношении объектной сети.

Объектные поля доступны с помощью «.»-оператора и могут быть использованы в программных операторах и утверждениях. Исключение неверных доступов обнаруживается во время семантического анализа. Спецификация (всех) полей данного объекта производится на уровне абстрактного предиката, которые также могут быть определены, в том числе частично (см. главу V и далее).

Конвенции из главы 1, обсужденные в этой главе, а также конв.5.17 и конв.5.18 вводятся, во избежание парадоксов, с целью приближения к «UML».

В этой главе рассматривается ЛРП и анализируются проблемы в связи с пространственными операторами. Получается, что один и тот же оператор приспособлен, согласно графу куч, разделять и связывать между собой кучи, в зависимости от состояния указателей и их содержания. Получается, оператор имеет различные аспекты в зависимости от контекста используемой формулы. Другими словами, единый пространственный оператор в классической ЛРП является многозначным [297]. Многозначность, это удобная запись, но влечёт за собой недостатки. Наиболее важными недостатками являются контекст-зависимость. Зависимость, прежде всего, означает, необходимость анализировать всю формулу, что может быть (не) связано с данной кучей и все её содержащие кучи. Чтобы определить независимый граф кучи (т.е. семантически контекст-независимо), требуется использовать зависимую нотацию того же графа кучи (т.е. синтаксически контекст-зависимо). Это не является парадоксом, однако, желает иметь лучшее. Далее мы покажем, что синтаксически возможно определить граф кучи контекст-независимо без ограничения общности, исключить целый ряд проблем и улучшить процесс автоматизированного доказательства. Для автоматизации синтаксический анализ при интерпретации формул, которые описывают кучи, является накладным и избыточными, если пространственное отношение между кучами удастся явным образом выразить. Соотношение между кучами может быть связанное или не связанное. Переписывание многозначной формулы кучи в однозначную (единственную) формулу может быть не тривиально, т.к. необходимо рассматривать все переходы от одной кучи к другой, либо проверить отсутствие любых переходов из одной кучи в другую, на что может потребоваться значительное время. И наоборот, если имеется однозначная формула, то не ожидается сюрпризов в связи с соотношениями куч. (Не-)связанная куча с некоторой другой кучей сохраняется, при этом не имеет значения, какой предшествует контекст или следует иерархически определённой куче. Используя синтаксически контекст-независимую формулу для описания семантически контекст-независимой модели памяти графа кучи объединяет понятие о том, что такое куча.

Глава разбита на семь разделов. В первом разделе анализируются ЛРП и последствия многозначности. Во втором разделе проблема многозначности локализуется, и обсуждаются подходы к преодолению проблемы. В третьем разделе рассматривается ужесточение многозначности как решение проблемы. В четвёртом разделе в частности, рассматриваются объектные экземпляры классового вычисления. Объект рассматривается как комплексная единица

ЛРП, на который распространяются те же самые свойства ужесточения и для простых ссылок. В связи с ужесточением операторов в пятом разделе обсуждается возможность специфицировать лишь часть динамической кучи, благодаря свойствам строгого пространственного соотношения подкуч. В частности, обсуждается модульность спецификации и улучшения качества программного обеспечения в связи с объектами. В шестом разделе подробнее обсуждаются возможности применения формальных свойств ужесточенной модели памяти. В последнем разделе обсуждаются возможности и ограничения предложенной модели.

Мотивация

Возьмём следующее синтаксическое определение термовых выражений E над целыми числами в классической арифметике целых чисел в качестве рассматриваемой проблемы многозначности:

$$\langle E \rangle ::= \langle k \rangle \mid \langle E \rangle ' \otimes ' \langle E \rangle$$

Нетрудно убедиться в том, что синтаксис по Бэккуса-Науру представляет собой индуктивно-определяемые термы, где начальное определение любое, но определённое целое число k . Допустим, \otimes является некоторым бинарным оператором, который полностью определён для целых чисел, например сложение. Если мы имеем ситуацию, когда для выражения e_1, e_2, e_3 : $E_0 \cdots \otimes e_1 \otimes e_2 \otimes \cdots E_n$ и $n \in \mathbb{N}_0$ один раз вычисляется как $e_{1,2}$, а при $E'_0 \cdots \otimes e_1 \otimes e_2 \otimes \cdots E'_n$ вычисляется как $e'_{1,2}$, при этом $e_{1,2} \neq e'_{1,2}$, то либо правила вычисления не корректны (возможно, ошибка совершена в стадии разработки; далее исключается), либо вычисление зависит от контекста, т.е. зависит от E_0 и E_n , либо E'_0 и E'_n . Необходимо заметить, что если $E_0 \equiv E'_0$ и т.д. до $E_n \equiv E'_n$, то проблема различия всё-таки совпадает с проблемой (не-)корректности вычисления. Исходя из стандартного случая, т.е. $e_{1,2} \neq e'_{1,2}$ при $E_0 \neq E'_0$, $E_n \neq E'_n$, можем утверждать, что обе E_0 и E_n одновременно не пусты. Следовательно, зависимость означает при $(e_1 \otimes e_2) \otimes e_3$, что e_3 содержит синтаксическую информацию, которая влияет на результат $e_1 \otimes e_2$. А поэтому, для каждого j умножения $\otimes_{0 \leq j}^n e_j$ в худшем случае означает полный синтаксический перебор всех остальных факторов. Сложность ограничивается рангом полинома $\binom{n}{2}$. Какое отношение эта граница имеет к кучам?

Из набл.5.1 следует, что определение « \star » из ЛРП очень близко к определению « \otimes » вверху (см. опр.5.6). Поэтому при анализе каждую из куч необходимо внимательно проверять (что означает E в верхнем примере). Поэтому, имеется следующее предложение:

Доказательства этому и последующим тезисам будут следовать в этой главе.

Из этого тезиса следует, что контекст-независимость позволит определить формальные теории о равенствах

и неравенствах куч, которые далее можно будет автоматизировать ради подключения SMT-решателя.

Proof. Идея заключается в расширении пространственным соотношением, ссылаясь на трм.5.8 и лем.5.10, которое может связывать, либо разделять.

Язык моделирования «UML/OCL» основан на типизированном лямбда-вычислении второго порядка, следовательно, эквивалентен опр.1.9, следовательно может быть выражен в типизированном лямбда-вычислении третьего порядка, следовательно может быть представлен в прологовских терминах как описано в главе IV. \square

Данные наблюдения и тезисы следуют анализам предыдущих глав и замечаний. Из предыдущих наблюдений и анализов можно заметить следующее:

- 1) Простая модель должна быть представлена простым способом. Контр-примером здесь может послужить [249]. Там, на первый взгляд неполное множество представляет на самом деле полное множество правил, которое может совершать очень сложные операции с указателями. Самые незначительные изменения могут легко привести к иному или не предсказуемому поведению. То есть, в сильно динамической системе минимальные изменения не должны менять весь характер поведения, особенно не должны менять далекие пространственные части куч.
- 2) Различные предыдущие модели памяти, точнее, их конвенции, не столь важны, как может показаться на первый взгляд. Показано, что ввод всё новых конвенций не расширяет, а наоборот, ограничивает выразимость дополнительными условиями. Предлагаемые новые возможности входных языков или языков спецификации настолько специфичны, что применение и метод верификации не устойчивы к малейшим модификациям и расширениям (см. главу IV). С практической точки зрения гораздо важнее описать точно и адекватно ту модель памяти, которая имеется, вводя как можно меньше искусственных ограничений и описывая только основное. Для описания, включая все возможные ограничения, берётся непосредственно граф кучи. Это является утилитаристским подходом. Эпистемологическое определение термина «кучи» дается в главе III.

В итоге реализации получается формальная грамматика операторов, с одним бинарным оператором для слияния и одним оператором для разделения, которая контекст-свободная (например, подграмматика E). Предложенная ужесточённая модель предусмотрена для более эффективного проведения верификации, отделив правила теории куч от общих логических правил. Правила

верификации представляются в качестве правил Хорна, и интерпретация правил совершается с помощью Пролога [298] (см. тез.4.11). На следующем этапе ужесточённые операторы заменяют оператор \star так, чтобы абстрактные предикаты могли быть автоматически распознаны при синтаксическом анализе (см. главу VI).

Многозначимость операторов

В качестве наиболее точного языка спецификации в вычислении Хора изначально предлагалось использовать математику, как наиболее точный формализм. Позже математика уточняется логикой предикатов в самом общем виде. В области верификации и спецификации куч можно использовать специальные логики, что довольно успешно применяется на практике (см. раздел I-A). Однако, неограниченные формулы могут оказаться более удобными при автоматизации, которые увидим позже. Одно из таких «более приемлемых» условий автоматизации может оказаться однозначное представление пространственных операторов. Здесь необходимо пояснить возникающий парадокс: ужесточение операторов является условием расширения выразимости, что будет продемонстрировано позже. Ужесточение условий формул куч естественно приводит к ограничениям.

Проблема точности и выразимости является фундаментальной проблемой не только в области логики, но также в науке в самых различных областях, начиная от восприятия, до записи по согласованным конвенциям до выражений. Надо искать причину возникновения многозначности. Неудивительно, если язык выражений программных операторов и декларативный язык спецификации различны, то могут появляться разрывы в семиотике (см. главу IV) объектов и их взаимосвязи. Элементарный вопрос о равенстве двух различных представлений о куче (см. главу III) может существенно усложняться, если не использовать единую, либо согласованную форму — это причина, которая лежит в определении куч.

Итак, вопрос об изоморфизме двух графов куч в обобщённом виде обсуждается в отображении на рисунке 60, и может быть оценён как тяжёлый. Решение изоморфизма может быть оценено, в общем, с экспоненциальной сложностью, для довольно плохих прогнозов. На практике имеются экспоненциальные алгоритмы, которые приближаются к полиному третьего ранга для небольшого объёма входных вершин. Если куча из рисунка 60 (а) содержит только сплошные линии, а при дальнейшем анализе выходит, что также имеется в частности соединение между вершинами №0 и №5, когда обе вершины кучи уже были специфицированы, то выявление изоморфизма сильно усложняется. Однако, сложность сужается ради типов и наименований, которые не меняются в

итоге. Проблема сложности изоморфизма сохраняется лишь тогда, когда имеется набор указателей вместе с графом кучи, которые можно преобразовать в другой граф, который отличается от предыдущего только множеством наименований вершин. Для рисунка 60 это может быть совершено с помощью пермутации (0 11)(1 8 2 10 3 9)(4 7)(5 6), исходя из графа на рисунке 60 б). С практической точки зрения вопрос изоморфизма стоит только тогда, когда необходимо проверить, может ли в принципе данная структура быть преобразована в другой граф, если допустить, что наименования могут меняться.

В главе VI рассматриваются абстрактные предикаты более детально, однако, идея абстракции предикатов лежит в свёртывании и развёртывании графа. К примеру рассмотрим рисунок 61.

Данный граф согласно минимальной зависимости можно разбить на подграфы вдоль мостика $v_1 \mapsto v_3$, см. рисунок 62.

Граф можно будет описать отдельными предикатами $\pi_0(v_0, v_1)$, $\pi_1(v_3, v_4)$ и предикатом $\pi_2(v_4, v_5)$, либо более абстрактно как: $\pi_0(v_0, v_1)$, $\pi_{1,2}(v_3, v_5)$, при этом, графы представленные предикатами связаны между собой и видимые вершины снаружи появляются в качестве аргументов неявным определением π_j , см. рисунок 63.

Развёртывание согласно определению π_j приводит к обратному.

Теперь можно вывести более обобщённые вопросы в связи с адекватным представлением кучи следующим образом:

- 1) Как специфицировать однозначные формулы и проводить максимально детерминированную верификацию?
- 2) Как решить вопросы об изоморфизме, локальности и абстракции графов простым образом (представление кучи)?
- 3) Как ограничить принудительную проверку объектов в программных операторах кода (представление объектов)?
- 4) Как эффективно решать равенства с кучами, если не все вершины (и грани) графа кучи полностью определены (частичная спецификация)?
- 5) Как можно избавиться от повторного анализа куч (пошаговая верификация)?

В главе III уже была представлена модель кучи, которая была предложена Рейнольдсом, Бурсталлом и другими. В этой главе итоги и эффекты определения Рейнольдса рассматриваются и проводятся дискуссии о выводимом графе, а также графах получившие от модификации различных параметров. Наблюдаются свойства и выразимость, что и является главным замыслом этой главы.

Переменные, также как и указатели, хранятся в стеке, а содержимое указателей хранится в динамической памяти. Следующее доменное равенство

согласно [26] действительно: $Stack = Values \cup Locals$. Утверждения меняются программными операторами и генерируются при верификации, при проверке куч, исходя из программных операторов. Утверждения о кучах, либо верны, либо ложны, в зависимости от конкретной кучи. Синтаксис утверждений определяется опр.3.10. Из опр.5.6 следует, что бинарный оператор « \star » может быть использован двумя способами: для того, чтобы выразить две кучи не пересекаясь, а также, чтобы две кучи делили между собой один общий символ. Оператор « \star » используется как логическая конъюнкция для связывания истины о кучах. Кроме того, он является, пространственным оператором, который выражает место нахождения и связанность. Она выражается тем, что связывающие формулы о кучах определяют, как две кучи расположены в некотором адресном пространстве касательно друг друга. Пространство подразумевает, что кучи занимают некоторые поля динамической памяти. Если определить связанность между двумя кучами как двудольный граф (биграф), то имеется левая сторона указателей и правая сторона множеств содержимого. Для того, чтобы связанный граф можно было полностью описать, высчитав максимальное паросочетание с целью уменьшения количества конъюнкций для формулы куч, соответствовала бы полностью графу куч. Такой подход на практике очень не практичен, т.к. нет необходимости и желания, со стороны разработчика, описывать максимально сжатое представление графа куч целиком (см. раздел III-A). Но, если полученный граф кучи сильно отличается от ожидаемого графа, то неожиданные «лишние части» кучи являются показателем возможных очагов ошибок в программе. Важны и другие критерии, например, адекватное соотношение между синтаксическим представлением и графом, с целью нахождения вершин и граней, а также навигации по граням, и т.д. Компактное представление абсолютно не даёт преимуществ в данном случае, а наоборот, трудно читаемо. Необходимо сравнивать конкретные состояния ячеек в динамической памяти. По этой причине регулярные выражения, как удобный вариант отпадают. Регулярные выражения страдают проблемой нелокальности: как только граф куч локально меняется в одном месте, то может последовать изменение целого выражения. Желаемое поведение, должно быть таким, что добавление одной грани в граф кучи не должно менять всю формулу, а лишь ту часть подвыражения или части формулы, которая непосредственно связана с меняющейся частью. Не причастные (под-)кучи не должны меняться.

Сравнив с опр.5.6, а также определения и дискуссию из главы III, можно заметить, что оно довольно трудное, а данные формулы, использующие это определение, могут быть многозначными, если всегда

анализировать только часть от формулы. Для полного решения взаимосвязей всегда необходимо полностью анализировать все конъюнкты. Данное определение одной кучи, является результатом, если попытаться определить отдельную кучу. Напомним, что Рейнольдс определяет только множество куч, а отдельная куча у него, так и не определена. Увы, другие авторы (см. главу I) также определяют только множественные кучи, но не определяют единственную форму кучи, если даже между строками авторы дают неполные и неформальные предпосылки на неё. Надо обратить внимание на то, что выведенное определение кучи в опр.5.6 является явным определением одной кучи, при этом, множеству куч не противоречит определению. Отсюда — берётся мотивация необходимости строже и явным образом решить многозначность « \star ». Когда имеются однозначные операции, тогда можно обращаться к отдельной куче с помощью одного символа. Фактически модель Рейнольдса (и других) анализирует и подразумевает только смесь куч. Представление об отдельной куче отсутствует. Куча имеет только тогда значимое объяснение, когда оно задаётся вместе с чем-то. Ввод строгих операторов позволяет выразить семантику и замысел одной кучи, которая как таковой субъект естественно существует независимо от других куч. Следовательно, куча имеет идентичность. Таким образом, определение можно избежать лишь через значение нескольких куч, т.е. «структуралистские семантики» меняются на «не (строгие) структуралистские семантики». Как только два оператора будут определены (\circ , $||$), далее свойства и равенства могут быть исследованы, вследствие чего, термовые алгебры можно будет определить для решения прогрессивной сходимости верификации. Термовые алгебры разрешат установить всё новые и новые формальные теории над кучами, которые практически можно будет использовать на прямую, в качестве правил Хорна в рамках Пролог программы (см. тез.4.11).

Ужесточение операторов

Из-за многозначности, оператор \star может быть использован как конъюнкция (слияния куч), а также как дизъюнкция (деление куч). Более того, строгие различия (трм.5.2) в реализациях ЛРП часто \star используются равномерно логической конъюнкцией. Решение этих проблем является задачей данного раздела. Вводится формальное определение конъюнкции кучи и свойства этой операции, затем вводится дизъюнкция. Будет показано, что общность выразимости при обеих операциях не ограничивается.

Здесь $\beta' = vertices(\beta) \subseteq V$ определяет все вершины графа куч, которые указываются из β . В случае если β является объектным экземпляром, тогда также рассматриваются все поля объекта, которые являются указателями. Так как α может ссылаться

лишь на одну уникальную вершину графа (например, путь доступа к некоторому объектному экземпляру), тогда и существует не более одной совпадающей вершины в *isFreeIn* для данной кучи *H*. Общее предположение высшего определения заключается в том, что при пошаговом построении графа при использовании конъюнкции, всегда существует одна подходящая вершина, иначе, две кучи нельзя связать вместе.

Например, нужно связать три пары указателей (указатель ссылается на некоторое содержимое) *a, b, c* (см. рисунок 64). Сначала необходимо выразить кучу *a*, которая может быть любой, либо как *ptr* \circ *a*. Только когда *a* существует, *a* ссылается на некоторое содержимое, которое эквивалентно началу кучи *b* и не связано (на данный момент мы подразумеваем именно такое состояние как начальное), только тогда обе кучи связываются. Если предположить обратное, т.е. в графе кучи имеются две одинаково содержимые, то по определению это исключено, т.к. допускается только одно по-настоящему уникальное содержимое (см. позже), но с любым количеством псевдонимов. Допустим, имеются одинаковые, но не по-настоящему одинаковые содержимые, тогда путь доступа должен отличаться, иначе, создаётся противоречие. В обоих случаях исключается возможность конъюнкции некорректного связывания. Итак, мы имеем связанную кучу *a* \circ *b*. Сейчас можно продолжить конъюнкцию под теми же условиями, как только что было изложено для *c*. При успехе мы получим граф кучи как на рисунке 64. Так как мы заинтересованы в конъюнкции любых графов, например двоичных деревьев, мы допускаем конъюнкцию в любых частях связанного графа. К примеру, *a* \mapsto 5 является допустимой конъюнкцией графа куч, однако, *a* \mapsto 5 \circ *b* \mapsto 5 не является. Таким образом, мы сможем выразить псевдонимы, например, граф кучи *x* \circ \longrightarrow *o*^z \longleftarrow *o* *y* может быть выражен как терм кучи *x* \mapsto *z* \circ *y* \mapsto *z*.

Кучи могут быть связаны различными способами, когда вершина является объектом. Например, можно договориться, что при присвоении объекта меняется только указатель, либо одно идентифицируемое поле. Можно также договориться о различных присвоениях. Например, когда все поля одновременно присваиваются некоторым входным вектором (например, массив или строка с определённым разделителем), либо присваивается только одно поле, а все остальные сбрасываются и т.д. (см. главу III). Ради простоты, более популярный из языков программирования Си(++) , далее рассматривается только присвоение «один-на-один» (см. раздел V-D). Замечание: Пусть Φ_0 некоторая куча, тогда следует $\Phi = \Phi_0 \circ a_0 \mapsto b_0 \Leftrightarrow \exists (a_m \mapsto b_m) \in \Phi_0 \wedge (a_m = a_0, b_m \neq b_0 \vee a_m \neq a_0, b_m = b_0)$.

Proof. Теорема является обобщением опр.5.7. Обе, *H*₁ и *H*₂ могут быть обыкновенными кучами видом $a_1 \mapsto b_1 \circ a_2 \mapsto b_2 \circ \dots \circ a_n \mapsto b_n$. Чтобы доказать корректность теоремы, сначала необходимо показать, что если не существует общий элемент в обоих графах, то согласно опр.5.7 получаем *false*, что совпадает с ожидаемым от конъюнкции. В противном случае, если имеется хотя бы один общий элемент, то согласно индукции, выбираем один элемент и тогда обе кучи связываются. Нужно отметить, что конъюнкция исходит лишь от возможности связывать графы и нас не интересует количество более одного. Все вершины кроме той, которая используется для слияния графов, могут также гипотетично быть использованы для слияния. В таком случае, полученный граф всё равно остаётся просто связанным. В противном случае начало, либо конец слитого графа куч находится, только в *H*₁ или только в *H*₂, а также в обоих графах куч *H*₁ и *H*₂ одновременно, но это исключается. Из-за этого противоречия следует годность теоремы. По определению, *a* \circ *a* равно *false*, что необходимо фильтровать для всех конъюнктов. Обсуждение *a* \circ *a*-решателя будет проводиться позже и может быть реализован с помощью активного множества, которое содержит статически все успешно обработанные базисные кучи. \square

Лево-ассоциативность означает, что терм *object1.field1.field2.field3* по умолчанию равен:

$$(((object1).field1).field2).field3$$

– таким образом, части выражения доступа к полю могут сопоставляться символьными переменными. Это повышает модульность, а в частности, повышает гибкость выражений.

Proof. Чтобы доказать, что *G* является моноидом, необходимо доказать: (i) Ω замкнут под \circ , (ii) \circ является ассоциативной операцией, а также (iii) $\exists \varepsilon \in \Omega. \forall m \in \Omega : m \circ \varepsilon = \varepsilon \circ m = m$.

$\omega \in \Omega$ связанной граф кучи, полученный с помощью бинарного функтора « \mapsto » в соответствии с опр.3.9. Согласно опр.5.7 $\forall \omega \in \Omega : \omega \circ \omega = \text{false}$ в силе. В противном случае, для $\omega_1, \omega_2 \in \Omega$ могут быть только два случая: если ω_1 и ω_2 имеют, хотя бы одну, объединяющую вершину, тогда согласно трм.5.8 соответствующий граф куч определён, иначе, результат *false* (обозначив, ω_1 и ω_2 не пересекается). Таким образом, мы показали, что Ω замкнуто над \circ и что граф кучи может быть получен в результате конъюнкции. В таком случае, соединение успешно установлено.

Далее, ассоциативность должна быть доказана, а именно, что: $m_1 \circ (m_2 \circ m_3) = (m_1 \circ m_2) \circ m_3$ в силе.

Рассмотрев рисунок 64, можно сразу констатировать верность равенства с обеих сторон, так как не имеет значения *a* и *b* связаны первыми, либо *a* связывается

с $b \circ c$, потому, что соединяющая вершина b остаётся инвариантом, когда порядок конъюнкций меняется.

G создает полугруппу. Для этого остаётся доказать существование нейтрального элемента ε так, что (iii) остаётся в силе. Однако, это следует из обобщённой теоремы о кучах (трм.5.8). \square

Замечание: Из (i) следует: $c \notin b \wedge c \neq a: a \mapsto b \circ c \mapsto d \equiv \text{false}$, и $a \mapsto b \circ a \mapsto d \equiv \text{false}$ в силе. Очевидно, если имеется выбор, то безразлично какие две вершины связывать первыми – результат тот же самый, благодаря сходимости из-за (ii) свойства, которое доказывается позже в лем.5.11.

Замечание: Замкнутость (i) показывает на свойство неповторимости подструктурных логик (ЛРП рассматривается как такова), которое остаётся в силе и будет продемонстрировано позже.

Proof. Из-за лем.5.10 G является моноидом. Поэтому нам остаётся показать: (i) существование обратного к любому элементу из множества носителя графа кучи, так, чтобы соблюдалось:

и (ii) \circ является коммутирующим оператором.

Начнём доказательство с (ii): в базисном случае $\langle loc_1 \mapsto var_1 \circ loc_2 \mapsto var_2 = loc_2 \mapsto var_2 \circ loc_1 \mapsto var_1 \rangle$ индуктивного опр.3.9 равенство, очевидно, соблюдается. Также соблюдается индуктивный случай до тех пор, пока условия от \circ соблюдаются. Условие индукции можно получить, рассмотрев рисунок 64, если на данный момент предположить, что для любых двух связанных куч оператор \circ коммутирует. Но, как только, речь идёт об абстрактных предикатах, понятие о \circ -связанных термах может ограничиваться границами предикатов и не могут быть разбросанными как угодно, как подцель в абстрактных предикатах. С практической точки зрения, это не страшно, а наоборот, призывает к лучшей модульности, но с этим необходимо считаться при написании спецификации.

Доказательство продолжается показом свойства (i). Чтобы доказать обратимый элемент, это когда куча, существует, нужно задаться вопросом: а что с практической точки зрения означает «обратимая куча»? Когда речь идет о естественных числах, то обратимостью сложения будет вычитание на том же множестве носителя. То же самое происходит для поля комплексных чисел, которые являются расширением поля вещественных чисел. И хотя вещественные или комплексные числа неперечислимы, тем не менее, на практике расширение арифметических полей приводит к значительному упрощению вычислительных задач. Хотя ответ отсутствует для множества вещественных чисел на вопрос: «а что такое i »? При решении целого ряда задач всё равно i может быть полезным, зная о равенствах: $i^2 = -1$ и $e^{i\pi} = -1$. В связи с этим, было бы справедливо поставить вопрос: почему бы не предположить, что на данный момент существуют

кучи, и мы постулируем урав.1, хотя бы до тех пор, пока не будет доказано обратное?

Итак, что интуитивно подразумевается под обратимой кучей или «кучей инверс»? Если речь идёт об естественных и вещественных числах, то имеется модель числовой оси: числа возрастают/уменьшаются относительно нуля в зависимости от направления оси. Как быть с кучами, например, с обыкновенными, формой $a \mapsto b$? Можно ли обратимой куче (инверсия) присвоить инверсию сопровождаемого предиката? — Это будет не точно. Может ли быть присвоено инверсии кучи пустое значение — возможно это будет не правильно, так как любая не пустая куча будет определяться как пустая. Как же будет определяться инверсия пустой кучи, и т.д.? Такое наивное определение тоже не целесообразно, так как не полностью определено для всех куч. Что, если стороны граней в графе куч просто поменяют стороны, например, из $a \mapsto b$ становится $b \mapsto a$? Это является лишь интересной идеей, но не практикуемо, потому, что конъюнкция не противоречит такому определению, а надо, чтобы при конъюнкции получалась пустая куча. При таком подходе не определена левая сторона в случае объекта. Можно представить, что слияние кучи удаляет «положительную кучу», если её соединить вместе с «отрицательной кучей». То есть, инверсия означает «трансцендентную» операцию удаления кучи из памяти, при этом оператор может быть применен к любой, в том числе и сложной куче. Можно обозначить $(a \mapsto b)^{-1}$ как « a не указывает на b » или лучше, как « a инверсно указывает на b ». Первое объяснение неудачное потому, что «не указывает» по ошибке может расталкиваться, как $a \mapsto c$, при этом $\exists c \in \Omega, c \neq b$ — это подразумевает, что вершина a всё-таки существует и более того, между a и некоторым элементом, чьё содержимое отличается от b — всё это ложь, потому, что таких предположений не имеется. Поэтому, гипотетичный случай «инверсно указывает», точнее «инверсно имеется ссылка на», требует некоторое удаление, несмотря на странное значение, которое позволило бы чистое удаление всех «лишних элементов», которые требуют дальнейшую проверку. На первый взгляд это выглядит странно. Пока что, мы специфицировали только части кучи, которые реально существуют. Ввод инверсии теперь меняет ситуацию. Инверсию также нельзя путать с тем, что не должно быть в куче и это есть отрицание предиката, а инверсия кучи — это операция. В данный момент, мы допускаем и концентрируемся на урав.1.

Данное уравнение означает, что «отрицаемое указывает на» $a \not\mapsto b$ — это прежде всего предикатное отношение между a и b , а в обобщённой форме отрицательная куча H^{-1} , для которой в силе по определению: $a \mapsto b \circ a \not\mapsto b = \text{emp}$ а также $a \not\mapsto b \circ a \mapsto b = \text{emp}$, а более обобщёно $H \circ H^{-1} = H^{-1} \circ H = \text{emp}$. Это означает, что $\omega \circ \omega^{-1}$

«чисто» удаляет кучу, т.е. при необходимости также удаляется ненужная грань и вершина из графа кучи, если больше не остаётся входящих или выходящих граней касательно ещё существующих вершин графа. Таким объяснением данное равенство об обратимости ссылки становится понятным и сейчас не трудно проверить равенство $H \circ H^{-1} \circ H \equiv H$. В примере на рисунке 65 до применения инверсии состояние кучи является таким: $d \mapsto a \circ a \mapsto b \circ c \mapsto b$, но когда применяется инверсия $\circ(a \mapsto b)^{-1}$, то получаем $d \mapsto a \circ a \mapsto b \circ c \mapsto b \circ (a \mapsto b)^{-1}$, что равно к $d \mapsto a \circ a \mapsto b \circ (a \mapsto b)^{-1} \circ c \mapsto b$ равно к $d \mapsto a \circ c \mapsto b$, что не полностью очевидно, т.к. оба указателя не пересекаются. То есть, такое состояние пока очищено не полностью и нуждается в дополнительных шагах для исправления ненужных элементов. Поэтому, следует пройти ещё два шага нормализации.

Нормализация – Первый шаг: Шаг является генеричным (общим). Если между рассматриваемыми графами куч существует мост, как единственная связь между ними, то оператор должен быть заменён на дизъюнкцию (см. позже).

Теперь, когда обнаружен мост между a и b , \circ заменяется на \parallel в оставшихся терме. Результат можно снова считать обоснованным. Но, возможно, ради полноты вершины, должны быть полностью удалены из соответствующего графа кучи. Это требуется тогда, когда речь идёт о локациях объектных полей.

Нормализация – Второй шаг: Удаление вершины a может быть произведено полностью, когда больше не имеются ссылки на a в оставшихся графе куч.

Применив эти два шага нормализации, можно избежать проблему упомянутых исключений (ср. обобщённые кучи с набл.4.13). \square

Замечание: Обобщённые кучи не были обсуждены. Для доказательства корректности необходимо показать $H \circ H^{-1} \equiv \underline{emp}$. Доказательство нужно проводить индуктивно над \circ при использовании $(g_1 \circ g_2)^{-1} \equiv g_1^{-1} \circ g_2^{-1}$, так, что существует гомоморфизм для « \cdot^{-1} » касательно \circ (см. лем.5.13).

Объяснение: $H \circ a \mapsto b \circ (a \mapsto b)^{-1}$ означает:

- 1) удалить грань между a и b
- 2) удалить вершину a , если на неё в графе H не имеется больше ссылок
- 3) также удалить вершину b , если на неё в графе H не имеется больше ссылок

Свойства группы позволяют нам установить равенства над термами куч, например, для ускорения сходимости доказательства или для преобразования в нормальную форму (см. трм.5.3). Таким образом, можно будет проводить сокращение раздутых термовых представлений куч. Частичные спецификации разрешат сокращённое представление правил (см. раздел V-E). Дальнейшая работа включает

в себя подключение решателей для преобразования простейших термов куч. Необходимо рассмотреть случай, когда содержимым является указатель, например, $a \mapsto o.f \circ (a \mapsto o.f)^{-1}$, где o объект содержащий поле f . Очевидно, $o.f$ не удаляется из динамической памяти, иначе, целостность объектных экземпляров нарушается — дальнейшее исследование приветствуется, но находится за пределами этой работы (см. дискуссию в разделе IV-F). Поэтому, по умолчанию уговаривается, что поле остается в памяти как единица целого объекта, но ссылается на nil . Таким образом, замеченные шаги остаются без изменения в силе.

Proof. Если нам удастся доказать более обобщённую форму: $G = g_1 \circ g_2 \circ \dots \circ g_n$, то проблема будет решена. Для этого необходимо показать $G \circ G^{-1} = \underline{emp}$. Доказать это можно индуктивно, используя n . В базисном случае ($n = 1$) получаем $g_1 \circ g_1^{-1} \equiv \underline{emp}$, что естественно в силе из-за необходимости существования обратного элемента. Для индуктивного случая предположим:

$$G = \underbrace{(g_1 \circ g_2 \circ \dots \circ g_k)}_{G_k} \circ g_{k+1}$$

тогда для

$$G \circ G^{-1} = (G_k \circ g_{k+1}) \circ (G_k \circ g_{k+1})^{-1}$$

обратная часть кучи является настоящим расширением кучи. Правая часть равенства равна

$$\underbrace{G_k \circ G_k^{-1}}_{\underline{emp}} \circ \underbrace{g_{k+1} \circ g_{k+1}^{-1}}_{\underline{emp}} \equiv \underline{emp}$$

(из-за индуктивного свойства обратимости, соблюдая конв.5.12). \square

Поэтому, $x.b \parallel x.c$ не действительно для любого объекта x с полями b и c , если существует, хотя бы одна общая вершина для любого пути, начиная с $x.b$ или $x.c$.

Допустим, $\Sigma = X_0 \parallel X_1 \parallel \dots \parallel X_n$ с $n > 0$ и X_j имеет форму $x_j \mapsto y_j$, тогда $\Sigma = \Sigma_0 \parallel a_0 \mapsto b_0 \Leftrightarrow \forall (a_j \mapsto b_j) \in \Sigma_0 : a_j \neq a_0 \wedge b_j \neq b_0$.

Теорема (Моноид дизъюнкция). $G = (\Omega, \parallel)$ является моноидом и группой, если Ω является множеством графов куч и \parallel является дизъюнкцией кучи.

Proof. В аналогии к предыдущей лемме, прежде всего, $\forall m_1, m_2 \in \Omega : m_1 \parallel m_2$, только тогда, когда m_1 и m_2 не имеют общую вершину. Это всегда так, когда нет пути от m_1 до m_2 и не существует граф окружающий оба, m_1 и m_2 . Если m_1 и m_2 различны, то $m_1 \parallel m_2$ снова являются годной кучей в Ω , потому, что m_1 от другой части графа кучи, чем m_2 и наоборот, поэтому следует замкнутость. Ассоциативность следует очевидно. \underline{emp} может послужить нейтральным

элементом, тогда $\text{emp} \parallel m_1 = m_1 \parallel \text{emp} = m_1$. Пусть по определению $\text{emp} \parallel \text{emp} = \text{emp}$ будет в силе. Последним, уговаривается $s \parallel s^{-1} = s^{-1} \parallel s = \text{emp}$. Это похоже на \circ . В общем, кучи следуют этому правилу. \square

Конъюнкция и дизъюнкция частей кучи могут быть выражены правилами с помощью дуальных к нему правил следующим образом:

$$\circ_{[B,C]} \frac{U \circ B \parallel C}{U \circ B \circ C} \quad \parallel_{[B,C]} \frac{U \circ B \circ C}{U \circ B \parallel C}$$

Операции \parallel и \circ — дуальные, и они могут быть преобразованы друг в друга, используя дуальную операцию, получив из урав.2 и урав.3, где «;» оператор последовательности.

Равенства в силе, из-за самообратимости операции и поставленного утверждения о существовании обеих вершин кучи B и C .

Замечание: Так как нейтральным элементом для операций \circ и \parallel является emp , то нельзя определить (алгебраическое) поле (например поле Галуа) над этими операциями из-за того, что лем.5.10, лем.5.11 и лем.5.16 в силе и несмотря на то, что множество носителем Ω конечно, поэтому любая куча конечная и все операции над ними также производят конечную кучу.

Замечание: В аналогии к логическим конъюнктам \wedge и \vee , нормализованная форма с помощью \parallel всегда существует, применив ранее упомянутые равенства и лем.5.13 для того, чтобы произвести инверсию обобщённых куч.

Для оптимизации логического вывода с помощью уменьшения объёма графа, необходимо попытаться вывести операцию \parallel как можно дальше наружи в термах кучи, применив дистрибутивность, либо переставляя несложные кучи так, чтобы левые части ссылок были отсортированы по имени локации по лексикографическому порядку. Идея заключается в сокращении повторных поисков, например, для пошаговой верификации, так, что только меняющиеся части кучи принадлежат повторному вычислению.

Частично упорядоченное множество (ЧУМ) можно установить над графами для подмножества графов, операторам слияния ЧУМ служит \circ . Минимальный элемент является пустой кучей, а максимальный является полным графом кучи. Например, закон абсорбции не действительный для куч. ЧУМ не может быть полной решёткой. На рисунке 66 ЧУМ G содержит $\{G_1, G_2, G'_1, G'_2, G''_1\}$, которые соблюдают следующие неравенства по возрастающему порядку $G_1 \sqsubseteq G'_1 \sqsubseteq G''_1$, $G_2 \sqsubseteq G'_1$ и $G_2 \sqsubseteq G'_2 \sqsubseteq G''_1$. Кучи \perp и \top всегда присутствуют и при необходимости могут быть добавлены, поэтому каждый раз по умолчанию

могут быть не указаны. G''_1 является максимальным элементом, а $\text{inf}(G) = \text{emp}$ минимальным элементом, где \sqsubseteq определяет подмножественное соотношение графа. Нетрудно убедиться в том, что две не соединённые кучи при конъюнкции (т.е. равны emp из-за опр.5.7) в соответствующей диаграмме Хассе всегда остаются несвязанными. Слияние всегда верное, потому, что: (первое противоречие) $a \mapsto b \circ a \mapsto d$ не может следовать первой конъюнкции, либо другой сложной куче. Из-за (второго противоречия) $a \mapsto b \parallel b \mapsto d$ противоречит определению \parallel . Однако, необходимо учесть, что порядок ЧУМ может пострадать после ввода инверсии кучи (ср. ранее), если использовать инверсию без соблюдения ограничений. На данный момент нас вполне устраивает использование инверсии для «более удобного» сравнения куч, в частности с проверяемой спецификацией, поэтому свойство локальности из главы III остаётся.

Классовый экземпляр как куча

Рассмотрим подробнее, как объектные экземпляры классов моделируются как граф куча согласно рисунку 67.

На рисунке 67 а) отдельное присвоение к существующему графу представлено (без подробностей), объект в прямоугольной рамке является некоторым объектным экземпляром. На рисунке 67 б) только второе поле объектного экземпляра присваивается некоторое значение сходимого типа данных, все остальные поля присвоены nil . Рисунки 67 с) и 67 d) имеют тоже самое значение как и с), только присвоение производится для всех полей, например по лексикографическому порядку. Далее вводим дополнительные ограничения, но без ограничения общности, которые будут полезными для, позже вводимых, операторов:

Чтобы не противоречить дальнейшим определениям с одной стороны, необходимо иметь возможность быстро проверять соотношения между двумя вершинами. Данная не пустая куча состоит из одной или более того простых куч. Для проверки, связаны ли две вершины графа кучи, необходимо проверить в худшем случае все левые стороны простых конъюнктов, т.е. необходим перебор всех граней графа куч.

С другой стороны, чтобы получить для одной вершины все соседние вершины, нам выгоднее иметь модель, которую можно было бы итерировать по вершинам, а не по граням. Для быстрого определения соотношения (например соседства), предлагается например, $\text{reaches}(x, y)$, $\text{reaches}(x, Y)$, $\text{reaches}(X, y)$, $\text{reaches}(X, Y)$, где x является определённой вершиной, а X является (под-)множеством вершин (аналогичное для y и Y). Модель, основанная на вершинах, отражена на рисунке 68 маленькими закрашенными

квадратиками, соответственно, позволит получить более эффективную итерацию. Обе модели а) и б), основанные на вершинах и гранях, являются дуальными и они могут быть преобразованы друг в друга: вершины по серединам граней кодируют начало и конец (см. d)), как одна вершина с объединяющим именем и связываются с соседними вершинами (см. рисунок 68 а) и б)). Очевидно, преобразование из одной модели в другую и обратно, согласно схеме преобразования на рисунке 68 с) возможно без потерь, т.е. отображение между обеими структурами является биективным независимо от направления граней (см. с)).

Поэтому, нам разрешается преобразовать графовое представление с конъюнкциями или дизъюнкциями, так нам удобнее для решения.

Частичная спецификация куч

Как было сказано ранее, в опр.3.9 объектные экземпляры можно рассматривать, как хранители полей данных $obj.f_1 \mapsto .. \circ obj.f_2 \mapsto .. \circ obj.f_n \mapsto ...$. Все поля создают некоторую кучу по отрывкам, но в отличие от абстракции, это преобразование можно охарактеризовать как конкретизацию. Поля классовых объектов имеют ограничения в связи с наименованием и типами, которые должны совпадать с соответственным классом. Все поля одного объекта существуют независимо друг от друга, поэтому они являются простыми кучами, которые связаны между собой с помощью о-конъюнкции как это уже было упомянуто. Поля объектов не могут быть утилизированы по отдельности (см. набл.3.5 и последующую дискуссию). Локальные переменные поля объектов также должны иметь возможность специфицировать части, т.е. подклассовые объекты. В аналогии к необъектным указателям можно определить константные функции над кучами, например, $true(obj)$ или $false(obj)$ из опр.3.10 и опр.3.9. В отличие от необъектных указателей, $true(obj)$ вводит объектный терм в качестве дополнительного параметра. Таким образом, абстрактные предикаты могут быть использованы для дальнейшей модуляризации спецификации, которая синтаксически и семантически не значительно отличается от необъектного случая.

В соответствии с предложенным методом распознавания решателя $a \circ a$ на основе вталкивания и выталкивания в/из стека согласно данному уровню абстрактного предиката (см. главу VI), теперь входящие и выходящие термы абстрактных предикатов, возможно, отслеживать и пропускать при повторных или ненужных вычислениях. Сравнение может производиться стеком для одинакового уровня,

либо отметками между любыми уровнями предикатов с помощью транслирующих правил.

Подробности следуют в главе VI. Нетрудно убедиться в верности \wedge, \vee, \neg -конъюнкций для $true(obj)$ и $false(obj)$. Эти константные функции могут принимать любое число объектных полей (см. трм.5.3) и их булево обозначение не зависит от конкретных полей. Однако, сложные кучи в комбинации с ними, могут иметь неожиданное поведение, которое исключается при анализе контекста. Частичные спецификации, которые используют константные функции, частично описывают поля, но могут покрывать гораздо больше. Такими образом, спецификации частичные, но охватывают больше куч (см. трм.5.4). Более того, высчитывание позволяет сравнивать имеющие кучи и выявить те кучи, которых не хватает. Это позволяет полностью определить все входные кучи в правилах.

Пример (Неполный предикат №.1). Дан объект a , который имеет три поля f_1, g_1 и g_2 . $C[\cdot]$ означает семантическую (неявную) функцию над термами куч типом $ET \rightarrow ET \rightarrow \mathbb{B}$, где ET из опр.3.10, \mathbb{B} булево множество, где первая расширенная куча является ожидаемой, а вторая является полученной кучей, то тогда:

$$\begin{aligned} C[a.f_1 \mapsto x \circ true(a)] &= C[a.f_1 \circ a.g_1 \circ a.g_2] \\ &= C[true(a) \circ a.f_1 \mapsto x] \neq C[p(a) \circ a.f_1 \mapsto x] \end{aligned}$$

где, p абстрактный предикат означает $true(a)$ (см. опр.5.19).

Однако, $C[a.f_1 \mapsto x \circ p(a)]$ означало бы равенство потому, что благодаря распознаванию, используя актуальное стековое окно, находит все оставшиеся поля, если даже ниже спрятано несколько уровней абстрактных вызовов. $C[\cdot]$ является гомоморфизмом касательно обсуждённых константных функций и конъюнкции \circ .

Пример (Неполный предикат №.2). $C[true(a) \circ true(a)] = C[a.f_1 \circ a.g_1 \circ a.g_2] \circ C[true(a)] = C[a.f_1 \circ a.g_1 \circ a.g_2] \circ emp(a)$.

Обсуждения

Одна пространственная операция была заменена на две строгие. Изначальные основные свойства ЛРП не поменялись, кроме неограниченной инверсии кучи, которая тщательно обсуждалась ранее. Если в трм.3.6 заменить « \star » на « \circ », а в случае дизъюнкции « \star » на « $||$ », то верность аксиом следует непосредственно, ради исключения аксиомы №5 для конъюнкции как раз из-за ужесточения « \star ».

Имея форму, которая позволяет нормализовать термы кучи, специфицируемые кучи можно теперь анализировать линейно (см. с разделом V-E). Из-за требования о неповторимости простых куч, комплексные кучи могут быть эффективно исключены с помощью «мемоизатора» (с англ. «memoiser»). На практике, необходимо исключать и обнаруживать повторяющиеся локации (возможно с различными, но одинаковыми значениями), как это было упомянуто в разделе V-C. Иначе,

кучи и граф кучи становятся противоречивыми и свойства ЛРП нарушаются. Это приведёт к полной неповторимости теорем. Принцип должен соблюдаться: одна простая куча специфицируется один раз. Простая куча, специфицируемая в одном месте не должна специфицироваться заново, аналогично принципу локальности: одно изменение локально производится только в одном месте. Если принципы не верны, то и применение правил не верное, а следовательно, из ложного предусловия могут выводиться любые результаты, поэтому повторные кучи должны исключаться.

Однако, эту проблему в общем удастся решить только динамически, но без запуска программы. «Динамически» при статическом анализе означает, что во время верификации, абстрактные предикаты естественно могут быть произвольными. Абстрактные предикаты могут интерпретироваться процедурально (см. главу VI). Следовательно, используется стековая архитектура для их анализа (ср. главу IV). Она очень близка к операционной семантике предложенной Уорреном [266], где стек имеет ссылки на предыдущие стековые поля. Эта семантика отличается от семантик классических языков программирования, которая ради исключения, при использовании параметров по вызову, более близка к реализации логического языка Пролог. Также представление и переход предикатов более похожи на правила Пролога. Незначительно модифицируемая семантика машины Уоррена может быть применена к интерпретации абстрактных предикатов, с помощью строгих операций конъюнкции и дизъюнкции, с помощью которой удастся распознавать, например, $\forall a \in \Omega. a \circ a$ для соблюдения неповторимости.

Мемоизатор может кэшировать только те вызовы абстрактных предикатов, которые не меняют глобальные состояния. Мемоизатор может запоминать, что имеются (i) входные или (ii) выходные или (iii) входные-выходные переменные термы. Если далее, неограниченные символы внутри одного абстрактного предиката поздним подвызовом ограничиваются, то это необходимо учесть при порядке вычисления подвызовов (определение должно следовать порядку слева направо, чтобы разрешить подобные конфликты, см. главу VI).

Пролог [248], как общий логический язык программирования может быть использован (см. тез.4.11), как платформа, основанная на рекурсивно-процедуральных правилах и термах для логического вывода, используя теоремы о расширенных термов куч и абстрактных предикатов. В Прологе обобщённая схема рекурсивной индукции Пиано может быть всегда определена как « $p(0).$ » для базисных случаев, а « $p(n):-n1 \text{ is } n-1, p(n1).$ » для индуктивных случаев, используя вспомогательный предикат *is* для высчитывания $n1$. Не трудно убедиться в том, что в Прологе можно

выразить любую обобщённую μ -рекурсивную схему предикатов. В общем, предикаты могут быть не определены (например, когда процедурный вызов не приостанавливается). Преимущество правил Хорна Пролога, в отличие от классических разовых функций (как они были использованы, например в [193]), это способность рассматривать термы предикатов как (i),(ii) или даже (iii), объединившие таким образом экспоненциальное количество различных классических разовых функций. Не каждый аспект может быть определён, поэтому вопрос об обратимости функции требует дополнительного внимания. Арифметические вычисления, а также зелёные и красные отсечения [248] поисковых пространств, являются одной возможной причиной, почему предикат может быть не обратим. Арифметические выражения в Прологе вычисляются с помощью оператора *is*. Обратимость арифметических выражений можно частично восстановить, если заменить натуральные числа Чёрческими числами (см. [299]), а фундаментальные операции обосновать только, если использовать константу, одинарный функтор и унификацию, как универсальную монаду базовой операции. Говоря обобщённо, необходимо гарантировать сильную корреляцию между входным и выходным результатом, которая должна стать изоморфизмом отображением для полной обратимости. Более того, прологовские отсечения могут быть заменены без потери общности и выразимости, так как отсечения являются лишь синтаксическим сахаром (см. главу III).

Язык «Object Constraint Language (OCL)» [1] является языком спецификации для объектных экземпляров. «OCL» является расширением языка «UML», и существует, как графическая нотация для утверждений, либо как формулы. Формулы «OCL» выражают часть предикатной логики. Имеется: — поддержка квантификации переменных, поддержка массивов и абстрактных типов данных/классов и полиморфизм с помощью подклассов. «OCL» разрешает описывать цикл жизни объектов и методов. Однако, «OCL» не знает об указателях или псевдонимах. Утверждения об указателях отсутствует, поэтому на этапе моделирования и быстрой прототипизации имеются ограничения, как было описано в главе I (см. [298], закл.5.5).

Предлагается, чтобы указатели записывались в качестве множества наименований объектного экземпляра. Таким образом, псевдонимы записаны в одном месте, альтернативно вводится множество указателей, которое существует независимо от существующих экземпляров объектов. Состояние объектов совпадает с состоянием вычисления стека/кучи. Сложные объекты имеют поля, которые просты или ссылаются на любые другие объектные экземпляры. Абстрактный предикат предлагается

логическим предикатом (см. главу IV), возможно, с символами. Нет обязательства, что в одном предикате описывается только один объект. Но рекомендуется определять одним абстрактным предикатом один объект целиком зависевшие объекты рекомендуется описывать отдельными предикатами. Ситуация, когда одним предикатом описываются два или более того объектных экземпляров не исключена, но не приветствуется ради модульности. Пространственное соотношение между объектами описывается операторами \circ и \parallel . Соотношения не требуют обязательного обозначения пространственности, если из контекста ясно, что речь идёт расширении представления «OSL».

Будущая работа может заключаться в расширении с абстрактными предикатами [296]. Начатое предложение следует расследовать дальше, особенно, учитывая постановления из конв.5.17 и опр.3.10. Ожидается повышенная выразимость, модульность и абстракция. Хороший обзор нынешних попыток расширить существующие вычисления с указателями, можно найти в главе I, а также в [193].

Автоматическая верификация с предикатами

Рассмотрим простой пример из области вычислительной геометрии [29]. Двусвязный список содержащий грань данного многогранника, послужит примером, в котором каждая грань связывает две вершины некоторого 2 или 3-мерного пространства. Сеть многогранника после триангуляции распадается на треугольники. Каждая вершина дважды связана с двумя соседними вершинами. Каждая грань начинается и заканчивается определёнными гранями. Для определения нормального вектора, достаточно иметь треугольник. В простой куче локализатор указывает на содержимое. Для данного примера это могут быть вершины или грани. Согласно упомянутому двусвязному списку, каждый элемент имеет ссылку вперёд к следующей грани и назад к предыдущей грани. Простая куча содержит связанные между собой грани. Не связанные между собой грани по определению не указываются. Уговаривается, что принудительное отсутствие кучи (см. главу V) исключается, либо отдельно не рассматривается в связи с Абельской группой из-за ранее упомянутых ограничений. Представим себе, что каждый раз как ссылаться на указатели, копии всех трёх вершин заносятся в память. Нетрудно убедиться в том, что такой подход малоэффективен. Если работать с указателями, то эта проблема отпадает, особенно когда вводится дополнительный уровень абстракции. Эти абстрактные предикаты позволяют более интуитивно выражать сложные кучи. Например, прологовская подцель $\text{face}(p1, p2, p3)$ может означать, что три вершины $p1, p2, p3$ связаны между собой в одном треугольнике вместо того, чтобы каждый раз

полностью специфицировать $\exists v1.v2.v3$, при $p1.data \mapsto v1 \star p2.data \mapsto v2 \star p3.data \mapsto v3 \star p1.next \mapsto p2 \star p2.next \mapsto p3 \star p3.next \mapsto p1 \star p1.prev \mapsto p3 \star p3.prev \mapsto p2 \star p2.prev \mapsto p1$.

Прежде всего, абстракция означает обобщённость, вводя дополнительные параметры. Под абстрактным предикатом подразумевается правило Хорна с произвольным количеством параметров. Хотя некоторые авторы стремятся использовать «Абстрактный Предикат» как новый термин [195], нужно заметить, что абстракция не нуждается в дополнительном определении (см. главу III), как новой концепции. Аналогично распространяется и на предикаты. Ясны концепции абстракции и предикатов, поэтому считается не целесообразно заново обозначать термины, тем более, имеются случаи, когда к предикатам добавляются параметры, например, в логике предикатов первого порядка. Это и является причиной, почему предикаты по-прежнему рассматриваются как классические, а «абстрактные» как прилагательные к предикату. «Абстрактный Предикат» не отличается от термина предиката, поэтому отдельно взятое семантическое определение просто не существует. Абстрактный предикат имеет любое (включая ноль) количество термовых параметров и может содержать любую последовательность (включая ноль) подцелей ранее декларированных предикатов. В данном примере $\text{face}(p1, p2, p3)$ равен той самой развёрнутой \star -формуле подцелей, которая была указана ранее. В зависимости от того, в каком состоянии находится вычисление подцели face , либо свёртывание, либо развёртывание, может быть целесообразным. Предикат face может зависеть от других предикатов. Однако, на данный момент просто не достаточно известно о том, когда необходимо свёртывать или развёртывать определение абстрактного предиката. Если развёртывание проваливается, то это может быть потому, что это в принципе не возможно, а также потому, что развёртывание и свёртывание были совершены в не правильный момент, либо в неправильной последовательности. Далее, будет рассматриваться новый подход, который позволит решить проблему автоматизации с кучами.

Уоррен [266] использует термин «программирования через доказательство» для того, чтобы выразить, что Пролог может быть использован как язык программирования, который используется для нахождения решения формулированного запроса правил Хорна. Изоморфизм Карри-Хауарда [179] гласит о взаимосвязи между доказательством и программированием. Касательно куч, философский лозунг данного подхода можно охарактеризовать как «доказательство является проблемой синтаксиса», это означает, что с помощью синтаксического перебора можно доказать корректность специфицируемой

кучи и представительство кучи близко к моделям по программированию, т.е. к прологовским правилам. Главным наблюдением этой главы является: абстрактные предикаты описывают на самом деле формальный язык (см. тез.4.11). Позже мы убедимся в том, что формальный язык является логическим языком программирования. Следовательно, проблемы свойств куч, которые являются семантическими, можно решить синтаксическим распознаванием.

Сжатие и развёртывание

Представленный в этой главе подход сильно отличается от существующих традиционных.

По Рейнольдсу [224], [193] пространственный оператор \star связывает две отдельные кучи, при котором основы подструктурной логики остаются в силе, а правило сужения не в силе. Как было изложено в главе III, классический оператор \star многозначен, поэтому, далее используется только строго соединяющий оператор « \circ » в качестве пространственной конъюнкции.

Абстрактные предикаты задаются пользователем, как это было предложено в «Verifast» [124]. Вывод может осуществляться быстрее с помощью «тактик», которые могут определяться индуктивно в системе «Coq» [32] и выводиться в полуручном режиме. Системы основаны на принципе «сжать/распаковать» (fold/unfold) [122], могут при полной подсказке полностью независимо от начала до конца вывод осуществить логически. Подсказки доказательства показывают на тот редекс, который необходимо предпринять для выхода из неопределённого состояния и для продвижения верификации в целом.

Пролог здесь используется как язык утверждения. [144] наглядно демонстрирует пригодность к доказательству формул в предикатной логике с помощью правил Хорна. [144] в прошлом предлагал использовать Пролог в качестве языка программирования, что, увы, не всегда возможно из-за вычислимости (см. главу IV). [266] содержит определение реализации логического вывода, опираясь на операционную семантику. Каллмайер [131] демонстрирует использование Пролога для распознавания морфем и мутаций грамматики в естественных языках. В частности, «сопряжённые деревья» предлагаются как механизм обработки мутаций в естественных языках на основе явных определённых λ -термов, которые исключаются в формальных языках, в частности, языках программирования во избежание многозначности. Примеры показывают многозначную перегруженность и трудность анализа из-за экспоненциального роста необходимых проверок посторонних условий. [168] на примерах поэтапно излагает, как Пролог может способствовать к решению проблем многозначности синтаксического перебора. Мэттьюс широко

использует рекурсивные распознаватели, которые работают с деревьями и в Прологе реализованы эффективно и просто. Реализации являются стековыми автоматами, распознающие LL(k)-грамматики с модификациями: конечные состояния выделяются явным образом, а рекурсивные прологовские правила имитируются стеком. Мэттьюс использует «списки разниц» для реализации распознавателя регулярных языков, который на самом деле основан на «автомате частичных производимых регулярных выражений» [50]. Бжозовский предлагает «прологовские формальные грамматики DCG» и встроенные команды Пролога для изменения баз знаний во время запуска для увеличения гибкости, которую он считает необходимо расширять. Однако, подход Бжозовского имеет недостаток в том, что выразимость ограничена регулярностью (см. главу III). Работу Перейры [201] можно оценивать как классическую монографию по Прологу и обработке естественных языков. Однако, подход Перейры имеет фундаментальные ограничения, которые всё-таки легко можно устранить среди множества образцовых и отличающихся примеров. Невозможность разрешить лево-рекурсию правил Хорна, хотя решение в принципе существует, т.к. LL(1)-распознаватель не в состоянии опознать всех предшественников для решения принадлежности правила. Далее, Перейра вводит λ -вычисления над деревьями для распознавания естественных языков. Таким образом, морфемы и лексемы связываются и получают зависимое значение от введённых параметров. Далее, введём первое прототипное определение кучи, учитывая опр.1.8 и главу III.

Предикатное расширение

Утверждение emp означает пустую кучу, которая верна, если данная куча пуста. Пустая куча является нейтральным элементом относительно пространственным связям между кучами (см. главы III,V). « \star » разделяет две кучи на две независимые кучи. В этой главе мы не будем различать ужесточение между « \circ » и « \star » (см. главу V) — ради общности мы исходим из конъюнкции куч. Утверждение true означает, любая куча (в том числе пустая) разрешается, а false означает, любая куча не разрешается. Эти определения близки к определению по Рейнольдсу [224]. Основой всех определений по Рейнольдсу является обыкновенная куча: $x \mapsto E$, где x некоторый локализатор (например доступ к объектному полю $o1.\text{field1}$), а E является некоторым допустимым выражением, которое присваивается ячейке памяти обозначающейся локализатором x . Проверка совместимости типов проводится на более раннем этапе [298]. На данный момент безразлично, явное значение, либо ссылка на ячейку в памяти содержится в качестве содержимого по выражению

(см. [51]). Рассмотрим две любые сложные кучи на Прологе в рисунке 69.

Здесь $p2$ означает некоторый предикат с двумя символами X и Y , которые представляют собой некоторые значения, которые указываются локализаторами $loc2$ и $loc3$. В отличие от этого, $p1$ определяется через предикат $p2$. Как только мы вызываем $p2$ с двумя синтаксически корректными аргументами, так мы имеем одну форму $a(\vec{\alpha})$. Вспомним, Пролог не может найти решения для синтаксически корректных, но семантически некорректных термов потому, что «семантически некорректно» означает, нахождение не выводимых термов для данных прологовских правил.

Интерпретация формулы H для данной кучи означает отображение от двух куч, т.е. данной и сравниваемой кучи, в булеву ко-область. Это означает, что если две данные кучи совпадают, то интерпретация успешна, в противном случае, наоборот. Для данных интерпретаций рассматривается только дедуктивный вывод (см. разделы I-A1 и I-A2). Поиск вывода завершается успехом тогда, когда запрос успешен, во всех остальных случаях завершается провалом. Несомненно, это точно то, что ожидается получить от предлагаемого поведения (см. тез.4.5). Ради простоты согласуем, что формулы куч должны быть нормализованы в форму

$$a_0 * a_1 * \dots * a_n \equiv \prod_{\forall j}^n a_j, n \geq 0$$

Далее, \wedge и \vee -связанные графы куч задаются в Прологе в виде запросов формой

$s_j, s_{j+1}, \dots, s_{j+k}$. Альтернативно можно дизъюнкцию прологовских целей разбить далее на некоторые альтернативные правила, головы чьи различаются с помощью оператора «;». Отрицание утверждения рассматривается как отрицание предиката. В общем, отрицание последовательности не означает отрицание предиката потому, что последовательность для всех может быть просто не определена, кроме некоторого домена, это надо учесть. Двойное отрицание в общем случае не действительно при вызовах подцелей потому, что предикат может быть не тотален. Экзистенциальные переменные могут быть введены в любом месте правила Пролога, однако ожидается, что все введённые переменные когда-то присваиваются и используются.

Константные функции, как например, `true` и `false`, являются «синтаксическим сахаром», т.к. они могут быть заменены на любые другие кучи, которые квалифицируются в качестве вставных куч. Использование константных функций упрощает в спецификациях все возможные кучи. `true` может быть сопоставлена булевой истине, `false` наоборот противоречием.

Заключение (Корректность кучи). Любая синтаксически корректная формула кучи описывает соответствующий граф кучи. Более того, любой граф кучи может быть представлен соответствующей формулой кучи. В общности обе стороны действительны ради исключения бесконечных куч.

Опр.6.3 является уточнением впервые введённого графа кучи из набл.3.5.

Предикаты как логические правила

Абстрактные предикаты позволяют абстрагировать от обыкновенных куч к более сложным кучам, но более интуитивным человеку, используя выражения и формулы. Например, [193] вводит абстрактные предикаты, которые аннотируют данную входную программу и переводятся вместе с программными операторами до уровня ассемблера. Представленный подход автоматизации является попыткой преодолеть разрыв между спецификацией и логическим выводом. Пролог используется в этой главе как язык программирования, в котором утверждения и абстрактные предикаты о кучах специфицируются. Однако, между программой и языком утверждений существует семантический разрыв: одновременно имеются два параллельных формализма и реализации. Они приводят к всё более различающимся нотациям и представлениям. Естественно, язык программирования может и должен различаться, когда речь идёт о возможном императивном языке программирования. В согласии с вычислением Хора, логические формулы описываются логически. Увы, иногда это нарушается (см. главу I), а также имеются ограничения вычислимости (см. главу IV). Так, например, переменные (объекты) используются как локальные переменные вместо термов, вследствие чего, имеется целый ряд ограничений. Таким образом, язык спецификации, точнее ее частицы, «деградируются» в последовательность команд и больше не имеется ничего общего с изначальным замыслом вычисления Хора. Частицы не имели бы ничего общего с «декларативно-логической парадигмой» (см. набл.4.7 и набл.4.9): необходимо описать состояние вычисления, используя символы и предикаты. Символ и его диапазон годности всё-таки отличается от локальных переменных. Если символы «вдруг переписываются», то вряд ли это можно считать символом. По определению символам не приписываются новые значения заново, а переменным приписываются. Разница может казаться не слишком большой, но для определения и описания это имеет очень серьезные последствия. Вычисления часто (но не всегда) описываются символами, без переменных. При описании центральной концепцией являются термы, предикаты и рекурсии, а не цикл или условный переход, это нужно учесть. В обеих моделях можно установить минимальный набор

Тьюринг-вычисляемых программ. Для решения верификации необходимо сравнивать состояния вычислений для того, чтобы определить, вычисление было совершенно правильно или нет. Проблема сравнения не исключает возможность и необходимость вычислять арифметические или алгебраические выражения, но при этом, подход и замысел вычисления Хора декларативен.

Подход представленный в [27] вводит символы в кучах, но с ограничениями. Например, отсутствует возможность описывать целые кучи, как например $X \star Y$. В отличие от этого, мы допускаем символы без ограничений полностью как они допускаются в Прологе (см. главу IV). В различных вариантах мы вынуждены будем выбирать только между теми правилом, которое имеет более длинное совпадающее предусловие – как это было реализовано, например, в [27]. Мы принципиально следуем поиску Пролога, что в обобщённом случае может быть слишком много, но «метод ветвей и границ» [248], [46] позволяет нам произвольно сужать поисковое пространство. Таким образом, мы не ограничиваем себя в некоторой методологии, либо эвристике, либо тактике. Любая методология может меняться частично, либо полностью — мы в состоянии всё это учитывать.

Пролог используется для того, чтобы определить, какие существуют подлежащие в кучах и какие связи между ними, для этого мы используем предикаты. Поэтому, можно считать, например [266] более близким подходом, чем функциональный или императивный. Когда речь идёт о проверке состояния куч, в общем легче описать, опираясь на факты и правила, чем на последовательность инструкций. С помощью абстрактных предикатов описываются кучи. За компактность, представление фактов и правил, ответственный — разработчик программы. Следующие формализмы помогут преобразовать абстрактные предикаты в формальную грамматику для дальнейшего представления. Все перечисленные преимущества характерны для Пролога и используются далее в предложенном методе.

Неслучайно опр.6.4 близко к опр.4.2. Первое определение используется для описания и вызова предикатов куч. Уговаривается по умолчанию, что a действительно всегда тогда, когда все подцели $q_{k,j}$ в a в силе для $0 \leq j \leq n$. Синтаксис предикатного правила определяется расширенной формой Бэккуса-Наура как показано на рисунке 70. $\langle \text{number} \rangle$ определяет любое прологовское число, а $\langle \text{atom} \rangle$ $'(' \langle \text{arguments} \rangle ')'$ определяет некоторый функтор с простым именем $\langle \text{atom} \rangle$ и любым количеством аргументов. $\langle \text{var} \rangle$ означает некоторый переменный символ, который начинается с большой буквы, например X . Рисунок 71 в главах III и IV представляет пример полезного предиката функционала map на Прологе.

Допустим, имеется некоторый предикат a , тогда подцели $q_{k,j}$ вычисляются слева направо для $j \geq 0$. Символьная среда σ внутри тела предикатного определения обновляется после каждого вызова, каждого из подцелей тела согласно рисунку 53. Не присвоенные символы остаются, но могут присваиваться после подцели. Термы результаты ранних целей не нуждаются в обновлении, так как символам присвоено неопределённое символьное значение. Семантика вызова предиката определяется следующим образом:

$$C(a)[a(\vec{y}) : -q(\vec{x}_{k,n})_{k \times n}] \sigma = D[q_{k,n}] \sigma(\vec{x}_{k,n}) \\ \circ \dots \circ D[q_{k,1}] \sigma(\vec{x}_{k,1})$$

По определению вектор термов \vec{y} может содержать общие элементы с вектором $\vec{x}_{k,n}$, $\forall k, n$ и $C[.]$ имеет тип $\text{atom} \rightarrow \text{predicate} \rightarrow \sigma \rightarrow \sigma$, $D[.]$ имеет тип $\text{subgoal} \rightarrow \sigma \rightarrow \sigma$, и σ имеет тип $\text{term}^* \rightarrow \text{term}$, где \star означает звезда Клини (см. [79]).

Подцель $q_{k,j'}$ не обязательно должна определять связанный граф изначально. Но, если это так, то это признак тому, что подмножество кучи определено целиком, по крайней мере, единая по интуиции структура данных. При разработке ПО модульность и «разделение забот» можно всегда считать хорошим признаком. Таким образом, абстрактный предикат вынуждает к описанию целой структуры данных. Следовательно, можно вывести следующий лозунг: «один абстрактный предикат должен корреспондировать с одной кучей», где под подкучей подразумевается не пустой граф кучи, который содержит настоящее подмножество вершин и представляет собой кучу. Далее, добавляя все более \star -конъюнктов, соответствующий граф кучи растёт непрерывно. Набор \star -конъюнктов образует кучи, возможно связанные между собой, которые соответствуют абстрактным предикатам. Когда речь идёт о «сжатии или раскрытии» абстрактных предикатов (похоже на вызов метода), существуют параметры, точнее вершины графа куч, которые стоят на обеих сторонах: со стороны вызова и со стороны вызванного предиката. Также могут существовать вершины, которые видны только изнутри предиката, которые не могут быть использованы извне предиката (по крайней мере, явным образом).

Без ограничения общности мы согласуем, что доступ к объектным полям с помощью функтора «.» разрешается, например $a.b$ (см. рисунок 70) или $oa(\text{object5}, \text{fld123})$ [298]. Ради примера и модульности, мы согласуем далее, что объекты, а также объектные поля, передаются в качестве параметров предикатам. Отличие между объектами и простыми стековыми локальными параметрами отсутствует, подробное объяснение будет дано позже.

По умолчанию согласуется, что для последовательности $q_{k,0}, q_{k,1}, \dots, q_{k,m}$ из $q_{m \times n}$ любая

строка находится в нормализованном виде, так, что для $s \leq t$ нетривиальных элементов первые s подцели располагаются, а остальные $t - s$ подцели являются тавтологиями в качестве подцелей, чей домен полностью определён как истина (Т). Далее, согласуется, что:

$$\exists k.a : -q_k \preceq a : -q_{k+1}$$

в силе, означая, что предикат, появляющийся ранее, в Γ_a имеет выше приоритет, чем предикат, который определён позже.

Замечание: Очевидно, из-за проблемы приостановки, вызов предиката из раздела в общем не решим. Далее рассматривается выразимость предикатов.

Замечание: Разрешение конфликтов с именами в Γ может быть разрешено, если закодировать локацию предиката в имя, как например класс, для которого предикат предусмотрен, тогда станет возможно различать предикаты. По определению предикаты с одинаковой локацией являются частью предикатного раздела, а следовательно не конфликтуют.

Ради полноты синтаксического определения из рисунка 70 и перевода представленного в следующем разделе, необходимо задуматься о том, как правильно перевести прологовские операторы последовательности «;» и отсечения «!». Если тело предиката содержит «;», тогда всю последовательность после «;» необходимо перенести в новый предикат с той же левой стороной. Так, например:

$$b : -a_0, a_1, \dots, a_m; a_{m+1}, \dots, a_n$$

для $\exists m. 0 \leq m \leq n$ разбивается на:

$$b : -a_0, a_1, \dots, a_m. \quad b : -a_{m+1}, \dots, a_n.$$

Если аналогично встречается оператор отсечения «!» в:

$$b : -a_0, a_1, \dots, a_m, !, a_{m+1}, \dots, a_n$$

, то a_0, a_1, \dots, a_m может содержать альтернативы, которые будут рассматриваться в случае провала. «!» утверждает, что если только одна подцель от a_{m+1} до a_n проваливается, то b полностью проваливается без дальнейшего поиска альтернатив. Все альтернативы могут быть факторизованы слева от «!» так, чтобы иные альтернативы исключались. В кратце, это является причиной, почему «;» и «!» могут быть исключены из Пролога в общности без потери выразимости (см. набл.4.13). Вопрос обобщения предикатов, безусловно, интересен, но в целях задач поставленных в этой работе далее не рассматривается. Подход Пулсона [198] задаётся вопросом достижения обобщения с помощью введения функционалов на уровне абстракции и логических правил [206], [170], [106], [80] для метода резолюции [286], [288], [103] — которые здесь далее не рассматриваются. Модули

тактик в системе «Соq» [32] основаны на принципе, который также описывается Пулсоном.

Значение лем.6.7 и лем.6.8 таково, что можно выразить любые предикаты эквивалентности в Прологе беспрепятственно и без явной рекурсии. Мы не ограничиваем себя и допускаем μ -рекурсивные предикаты ценой частичной корректности в связи с не определением приостановки интерпретации предикатов ради беспрепятственной выразимости.

В случае « \Rightarrow » верхнего равенства $a(\vec{\alpha})$ предикат развёрнут. В случае « \Leftarrow » правая сторона определения предиката свёртывается в вызов предиката. « \approx » означает унификацию термов.

Интерпретация предикатов над кучами

Предложенный в этом разделе универсальный, но нестандартный, подход зависит от следующих этапов:

- 1) Преобразование входной программы и аннотированные утверждения в прологовские термы, которые затем вписываются в логическую систему на основе Пролога (см. рисунок 59, [298]).
- 2) Определение абстрактных предикатов в предусмотренной части прологовской программы вместе с представлением входной императивной программы. Правила принадлежат интерпретации и следовательно нуждаются в синтаксической корректности. Также как и пункт 1, этот пункт подробнее рассматривается в разделе IV-E.
- 3) Определение формальной грамматики для данных абстрактных предикатов. Обработка грамматики языковым процессором, которая при успехе генерирует конкретный синтаксический анализатор.
- 4) Во время доказательства использование и подключение ранее преобразованных в синтаксический анализатор абстрактных предикатов при вычислении подцелей.

Простое утверждение « \mapsto » становится терминалом (см. опр.6.5). Абстрактный предикат становится нетерминалом, точнее его вызовом. Терминалы могут связываться последовательно с помощью бинарного оператора \star , который коммутативен (см. трм.3.6). Терминал получает значение единицы некоторой подграмматики — это эквивалентно грани некоторой данной куче. Утверждения « \mapsto » могут эффективно связываться, когда левые локации сортируются по лексикографическому порядку. Когда происходит конфликт с одинаковыми именами, то α -преобразование, учитывая местонахождения в данном модуле, может разрешиться, например, вводя префикс.

Заключение (Контекст-свободность выражений куч). Раздел абстрактного предиката описывает систему правил, которая является контекст-свободной формальной грамматикой.

Proof. Левая сторона предиката не может по определению содержать более одного нетерминала, терминалы очевидно также не допускаются. Следовательно, только один нетерминал разрешается на левой стороне. Отсутствие требования, где правая сторона должна быть строго право-рекурсивной, т.е. отсутствие требования регулярной грамматики с правилами формой $\langle S \rightarrow aA \rangle$, приводит к контекст-свободности. Допускается распознавание грамматик, которые эквивалентны к «скобочным грамматикам» [110] (КС-грамматики, чьи правила могут иметь вид $S \rightarrow (S)$), а именно, когда имеется $n \in \mathbb{N}_0$ для некоторых терминалов a, b, x_0, x_1 и x_2 , которые могут быть $\langle \mapsto \rangle$ -утверждением, так, чтобы $x_0 a^n x_1 b^n x_2$ и $x_0 \neq a, x_0 \neq x_1$ и $x_1 \neq b, b \neq x_2$. Если голова предиката содержит аргументы, то это всё равно не меняет статическую зависимость между определениями предикатов. Каждому разделу предиката можно приписывать один начальный нетерминал. \square

Из этого следует: выведенная и ожидаемая куча, обе они могут содержать свёрнутые предикатные определения, которые должны быть развернуты для окончательного определения равенства. Не трудно увидеть, что этот процесс двунаправленный, так как свёрнутые подкучи могут содержаться в обеих кучах. Важно заметить, что этого рода проблема редуцируется к «проблеме корреспонденции Поста», которая в общем случае теоретически не является решимой, но только в частных случаях. Общая проблема для куч сформулированная Постом не рассматривается.

Набл.6.10 вместе с набл.6.13 может быть рассмотрено как предпосылка на формулировку: дана \star -связанная куча. Вопрос: совпадает ли она или нет с данной спецификацией кучи? А также можно задать вопрос — какая куча самая близкая к корректной куче, так, чтобы спецификация соблюдалась? Решение вопроса способствует к решению проблемы контр-примера.

Перевод правил Хорна

В этом разделе рассматривается перевод абстрактных предикатов, которые даны в качестве прологовских правил, в обобщённые правила контекст-свободной грамматики с атрибутами. Перед этим необходимо преобразовать обыкновенные утверждения формой $loc \mapsto val$ в токены, как принудительный лексико-аналитический шаг интерпретации Пролога. Применение мульти-парадигмального программирования [81] разрешает интерпретировать прологовские правила во время запуска различными языковыми процессорами. Это позволяет достичь максимальную расширяемость, например, подключение написанных процедур на различных языках программирования и запуск

в третьей загрузочной системе. Таким образом, процесс верификации может быть инициирован, контролирован и приостановлен входной программой. Процесс трансляции из правил Пролога в формальную грамматику удивительно прост, ради интерпретации правил Пролога. Однако, правила Пролога могут иметь аргументы с обеих сторон от знака определения правила $\langle :- \rangle$. Параметры и аргументы генерируемой грамматики можно моделировать как атрибуты формальной грамматики. Следовательно, процесс трансляции $C \mapsto$ можно характеризовать как:

В отличие от ранее введённых нотаций далее вводятся подцели и теперь входной вектор \vec{x} содержит все переменные символы, ради удобной записи внутри каждого предиката. Если некоторая подцель q_j для $j \geq 0$ не нуждается во всех компонентах \vec{x} , то подцель не нуждается в них. \cup является множественным объединением, с учётом последовательности и сохранения дубликатов. Нетрудно заметить, что обе записи сопоставимы и сильно похожи друг на друга. Абстрактный предикат описывает кучу. Таким образом, $C \mapsto$ преобразует кучу, т.е. является интерпретацией ассоциативной кучи, см. лем.6.14. $C^{-1}[\cdot]$ преобразует атрибутируемую грамматику обратно в Пролог:

Ещё осталось исследовать $C \mapsto$ и $C^{-1}[\cdot]$ касательно корректности и полноты.

Заключение (Корректность и полнота преобразований). $C \mapsto$ и $C^{-1}[\cdot]$ полны и корректны.

Proof. Не трудно убедиться в том, что $C \circ C^{-1} \circ C \equiv C$ и $C^{-1} \circ C \circ C^{-1} \equiv C^{-1}$, сопоставляя верные определения. Обсуждения из раздела VI-B, ни $\langle ! \rangle$ ни $\langle ; \rangle$ не влияют на выразимость. Если для любого элемента из $C \mapsto$ преобразование не приостанавливается, то кообласть также не полностью определена. Тоже самое распространяется на $C^{-1}[\cdot]$. \square

Нетрудно заметить, что прологовские правила не единственная форма, но очень близка к формальной грамматике. Более обобщённо можно включить императивные языки программирования с процедурами на основе автоматического запуска со стеком.

Синтаксический перебор как верификация куч

В целях простого и интуитивно понятного алгоритма, константы из опр.6.1 далее пока рассматриваются. Касательно классов объектов, предикат true может означать, например, принимать все $\langle \mapsto \rangle$ -утверждения до отметки, которую необходимо согласовать, в зависимости от данного правила. В данной отметке, которая представляет собой безопасный пункт синхронизации в качестве «правил генерации ошибок» [110], может продолжаться синтаксический перебор, если перебор застрянет из-за ошибочной последовательности в потоке токенов, либо

из-за не ожидаемого состояния на стеке при переборе. Предполагается, что входное слово, представляющее кучу, всегда конечное. Предположение основывается по той причине, что память — это линейно адресуемое конечное пространство. Чисто гипотетично, число совершённых развёртываний и свёртываний стремится к бесконечности. Позже мы покажем, что для $\exists j$ функции π_j и σ_j ограничиваются полиномиальной сложностью.

Этот раздел предлагает и обсуждает основные конвенции, необходимые для реализации общего подхода синтаксического перебора, в целях верификации куч. Это рассматривается на примере LL(k)-перебора. LL(k)-анализатор, является синтаксическим анализатором, который может смотреть вперёд любое количество токенов для разрешения многозначности одинаковых правил. LL(k)-анализатор выбирается образцово. Кроме LL(k)-анализатора, могут быть использованы другие анализаторы синтаксиса, как например, LALR, SLR, Эрли и другие. Журдан [129] с помощью «Соq» доказывает корректность LR(1)-анализатора — вопрос корректности анализатора, безусловно, важен, но в рамках этой работы отпадает, т.к. анализатор конструируется автоматически из данной формальной грамматики. Далее, первым определяется формальное предложение, как композиция отдельных « \mapsto »-утверждений и подцелей как нетерминалов. Вторым и третьим, в аналогии к LL(k)-анализатору, где отдельные терминалы представляются как обыкновенные утверждения операции, вводятся «first» и «follow». Четвёртым, обе операции сдвиг (SHIFT) и свёртка (REDUCE) представляются, чтобы иметь представление для более обобщённых анализаторов.

Например, $\alpha ::= [\text{pointsto}(x, \text{nil}), \text{pointsto}(y, 1), \text{member}(x, [y])]$ описывает актуальное состояние кучи при верификации данной императивной программы. \star заменяется в предыдущем списке запятой. Спецификация правил может зависеть от $[\text{pointsto}(Y, 1), \text{member}(X, [Y]_{-}), \text{pointsto}(X, _)]$. Поэтому, для проверки абстрактного предложения (спецификация) для данной программы (генерируемая куча), необходимо сравнить, выводима ли одна из сторон из другой или нет.

Абстрактное предложение может также содержать унификацию термов, как например, $\text{pointsto}(X, 5), X=Y$. Унификацию термов необходимо тщательно проверять и отделять от: « \mapsto »-утверждений и от вызовов предикатов, т.е. нетерминалов. Надо учесть, что неограниченная рекурсия термов должна ограничиваться так, чтобы терм сам себя не содержал по определению. Поэтому, самосодержащие термы необходимо ограничить, так как они часто имеются по определению в Прологе (см. раздел IV-A), где проверка самосодержимости по умолчанию отсутствует. Анализаторы, которые вынуждены

анализировать неограниченные термы, могут попадать в тупиковую ситуацию, если сам терм циклически определяется самим собой. Поэтому, во избежание проблемы принудительной работы, уговаривается, что проверка на присутствие циклов проводится отдельно от верификации, либо по умолчанию исключается.

Рассмотрим теперь «наивный» подход для сравнения равенства двух абстрактных предложений. Рассмотрим алгоритм № 2. π означает функцию начальных терминалов для данного правила и данного положения, как было определено ранее. Проблема в этом подходе (развёртывая фактически принудительно предикаты всё далее и далее, возможно бесконечно) заключается в неопределённости, когда и сколько раз применить точно развёртку и свёртку, тем более не известно в случае нахождения одного решения, не является ли решение оптимальным, что, безусловно, зависит от данных правил. Предположим, имеется:

$$\alpha_1 = [\underbrace{a \mapsto b}_{i_0}, i_1, \dots, i_{m_1}, \underbrace{q_1(x)}_{p_0}],$$

$$\alpha_2 = [\dots, \underbrace{a \mapsto b}_{j_3}, \dots, \underbrace{q_1(x)}_{q_7}]$$

необходимо сравнить сходимость термов обоих выражений. Сдвиг термов (SHIFT-TERMS) приводит к унификации i_0 и j_3 и продолжению сравнения остальных термов. Сначала свёртка (REDUCE-PREDS) проверит, подходящие и применяемые ли предикаты для расширения. Поэтому, первый терминал предиката может быть запрошен первым. Развёртывание $\text{expand}(p_k, \alpha_1)$ сопоставит подцель телом определения предиката p_k (см. опр.6.9 и рисунок 70) и преобразует новое абстрактное предложение α' , которое можно описать в Прологе как $\text{concat}(\alpha, [i_7, i_8, i_9], \alpha')$, если $q_1(x)$ развёртывается в список $[i_7, i_8, i_9]$.

Независимо от конкретных аргументов, π определяет все те терминалы, которые являются « \mapsto »-утверждениями, либо являются первым терминалом предикатных подцелей. Мы подразумеваем, что подцели унификации и вызовы встроенных (т.е. «встроенных») подцелей фильтруются и не рассматриваются при вычислении π и σ .

Неформальное объяснение таково: множество последующих терминалов определяет все те терминалы, которые могут следовать данному актуальному « \mapsto » утверждению или данной подцели в случае, когда терминал находится в конце правила. Согласно [110] мы теперь обладаем возможностью определить LL(k)-распознаватель с помощью определений π и σ .

Пример (Многозначность правил). Даны следующие правила нетерминалов $q_1 \rightarrow a, q_2 \rightarrow aq_2 \mid q_3b, q_3 \rightarrow \varepsilon \mid q_3a$. Нетрудно заметить, что эти правила многозначны, например из-за $\pi(q_2) = \{a\}, \sigma(a) = \{\varepsilon\} \cup \pi(q_2) \cup \pi(q_3) \cup \sigma(q_3)$.

Пример (Корректность). Дана следующая конечная спецификация:

$$[(loc1, v1), p1(loc1, loc2), (loc2, v2)]$$

и подходящая к нему условная цепочка $[(loc1, v1), (loc2, v2)]$. Цепочка является корректным словом данной спецификации, лишь в том случае, когда $p1$ генерирует только пустую кучу.

В случае, если данное слово не является просто последовательностью терминалов, но окажется «абстрагируемым» предложением, т.е. содержит произвольную последовательность терминалов и нетерминалов, то проблема сравнения может возникнуть в различных местах последовательности. Одной из этих проблем может оказаться вычисление повторяющихся куч и абстрактных частиц предикатов. Поэтому выгодно, когда вызовы абстрактных предикатов запоминаются в кэш (мемоизатор, например в [268]), а затем подцели могут быть сравнены гораздо быстрее, тем более, из-за декларативного характера предикатов, где символьные значения не присваиваются заново. Поэтому, предикаты могут быть сравнены чисто процедурно, без «опасных» побочных эффектов и изменения состояния вычисления несколько раз подряд. При ускорении кэширования необходимо запоминать наименование предиката и все термовые аргументы при вызове подцели.

Отрицания предикатов далее не рассматриваются из-за подробностей представленных в разделах V-C, V-E, V-F, IV-A и IV-B.

Свойства

На рисунке 72 показан пример конфигураций одной кучи, в которой любая вершина v_j при $j \neq 2, j \neq 5$ с отходящими гранями для классного экземпляра, более одного указателя в качестве атрибута. Конфигурация состоит из 8 треугольников, каждый из которых ограничивается сплошной, пунктирной или извилистой линией. Линия, начиная с середины между v_0 и v_3 доходящая до M_1 , выделяет треугольник $\Delta(v_0, M_1, v_1)$. Таким образом, рисунок 72 демонстрирует разновидность одной и той же структуры в динамической памяти, используя различные описания. Предполагается, что два и более выходящих указателей подразумевает соответствующее количество различных полей в объединённом экземпляре (см. главу III и рисунок 60). То есть, вершины могут охватывать те же самые графы различными абстрактными предикатами, например, треугольниками с пунктирными линиями или извилистыми линиями. Однако, при различных представлениях, необходимо учитывать все вершины — это является обязательным критерием, но не достаточным. Вопрос равенства двух различных куч,

эквивалентен к вопросу изоморфизма двух данных направленных графов.

Когда анализируется входной поток токенов, последовательное состояние анализатора можно определить с помощью проверки нескольких токенов вперёд. В худшем случае, придётся проверить все входные токены, но решение будет принято. Это в случае, когда куча описывает объектный экземпляр и необходимо определить границы объекта. Если ограничиться тем, что один объект может быть описан только в одном предикате, либо поля указатели описываются зависимыми предикатами, то такая конвенция позволит избежать описанную проблему и провести генерическую канонизацию по предикатам. Синтаксический перебор, соблюдая данную конвенцию, имеет полиномиальную сложность [110]. Проводится синтаксический перебор без дополнительных условий. Если объектные границы не соблюдаются, то перебор может повлечь за собой пересечение куч, которые могут относиться к другому объекту. На практике это может означать, частичный и параллельный перебор различных куч одновременно, что желательно избежать по различным соображениям. Во-первых, проблема плохо делима из-за множества взаимосвязей, определений и из-за иерархии вызовов и фреймов. Во-вторых, надо задаться вопросом о преимуществе такого подхода, который кажется довольно сомнительным на данный момент потому, что не предвидится никакого ощутимого выигрыша, но дополнительные затраты на параллелизацию поглощают все возможные преимущества. Поэтому, такой вопрос с теоретических и практических сторон пока не задаётся. С практической точки зрения необходимы параллельные кучи, которые наполнялись бы последовательно обработкой спецификации (см. стек Трибера [44]).

Если все разделы предикатов можно перебрать синтаксически, учитывая упомянутую конвенцию, то перебор « \mapsto »-утверждений решим и завершается с ответом или с отказом. При отказе, синтаксическая ошибка содержит неверный токен и/или данный сегмент в нетерминале (т.е. состояние перебора). Таким образом, она показывает на состояние кучи, которая не совпадает с имеющейся кучей. Также необходимо заметить, что сходимость вычисления соблюдается при сборе LL-/LR-анализаторов потому, что состояние вычисления записывается как кортеж (состояние анализа, входная цепочка) и для каждого состояния переход детерминирован. В итоге, главная модель памяти не была кардинально изменена, а лишь расширена абстрактными предикатами.

Реализация

Система реализована на основе «GNU Prolog» [83] при поддержке «ANTLR» версии 4 [197]. Работа с абстрактными предикатами предусмотрена для работы

[298], [302]. Изначально, обе работы, основанные на Прологе, были выбраны ради простоты пользования и в преподавательских целях. Для максимальной поддержки пакетов, написанные на Прологе, была использована дистрибуция «GNU Prolog», для максимального сходства с генеричной версией Пролога. Для расширения и возможности поддерживать различные библиотеки на различных языках, была использована многоцелевая парадигма [81], для динамического подключения загрузочного кода на разных языках программирования. Таким образом, программная библиотека Денти [81] разрешает подключать, например, Ява-библиотеку через соответствующую графическую оболочку. Процедуры на языке Ява или иных языках через соответствующий интерфейс при запуске прологовского запроса могут включить дальние вызовы. Слой вызовов «tuProlog» выступает в качестве «медиатора» и «адаптера». При этом, вызов и результаты могут передаваться с обеих сторон с помощью «прокси», как будто процедура дальнего вызова библиотеки является локальным правилом Прологу. Таким образом, не только на языке Ява можно создать всё новые вспомогательные и встроенные предикаты, но также новосозданные предикаты могут снова вызывать предикаты. Так вызов при запуске Пролог программы согласно принципу ящика из рисунка 53, производится полностью динамически.

Реализация преобразует входную программу в IR, которое состоит из термов Пролога. Затем, утверждения копируются отдельно в теорию Пролога, а абстрактные предикаты преобразуются в грамматику «ANTLR», как это было изложено ранее. Затем, запрашивается перебор, синтаксический анализ с помощью того распознавателя подключается, который генерируется после определения «ANTLR» грамматики (часто на языке Ява). Затем, выход, контроль возвращается вызывающей стороне. При необходимости, абстрактные предикаты могут проверяться автоматически. В случае синтаксической ошибки, выдаётся соответствующая ошибка.

«ANTLR» использует для разрешения синтаксической многозначности две технологии: «синтаксические предикаты» и «семантические предикаты» [197]. Термины очень похожи на проблемы данной работы, но их следует внимательно различать и не путать. Кроме этих двух технологий, всегда имеется возможность переписать правила, так, чтобы многозначность не возникала, например, с помощью факторизации правил. На практике «ANTLR», увы, не покрывает полный класс LL(k)-распознавателей. Предикаты ограничены и в случае конфликта часто нуждаются в переписке (термовых) правил. «ANTLR» часто не в состоянии различать самостоятельно, особенно регулярные, сложные выражения. Следовательно, приводит к полной

генерации кода для необходимого распознавателя. Такая же проблема с ограниченностью LL(k) наблюдается во множестве других генераторов компиляции, как например, в «уасс» или «bison» [162]. С практической точки зрения это означает, что данная грамматика, хотя формально и корректна, не может быть перебрана из-за ограничений в реализациях распознавателей. К счастью, на практике переписка грамматики часто разрешает этот конфликт в практических целях. Также необходимо заметить, что более мощные распознаватели, по принципу, «снизу-вверх» имеют возможность избежать различные ограничения за счёт сложных реализаций и объёма, генерируемых распознавателем, например, «bison» работающий по принципу «сдвиг-свёртка». Обзор технологий синтаксического анализа можно найти в [291], [110].

В качестве примера, приведём необходимые трансформации на более подробном уровне для обработки лексем и токенов. Сначала, $bar \mapsto foo$ преобразуется в pt_3bar_3foo , где число «3» это длина наименований, либо сложное выражение целой локации, которая требуется для различения последовательных наименований. Если локация сложная, например $b.f.g$, то локация вместе с длиной определяют выражение утверждения в смежной записи (с англ. «mangled» [163]). Например, $pointsto(X,2)$ преобразуется в прологовский атом p_X_2 . Цель преобразований заключается в получении одного атомного символа, который представляет собой простое утверждение о куче, это терминал. При необходимости терминал без потерь может быть полностью восстановлен обратно в утверждение о куче, т.к. для этого все данные имеются и данные компоненты строго различаются в прологовском атоме. Процессы прямого и обратного преобразования могут быть реализованы в качестве встроенного предиката, например на языке Ява. Затем, используются в главных частях верификации, либо могут быть использованы другими встроенными предикатами на Яве, либо на другом подключенном языке к Прологу (см. предпосылки, [81]).

Далее, левая сторона (де-)канонизации (на Прологе)

$$p1(X,[X|Y]):-\dots$$

преобразуется в:

$$p1(X1,X2):-X1=X,X2=[X|Y],\dots$$

Правило « $p(X,Y):-\alpha$ » из Пролога можно перевести в следующую «ANTLR»-грамматику:

$$p[\text{String } X,\text{String } Y]: \alpha.$$

Таким образом, все синтезируемые атрибуты можно передавать сверху-вниз. Порождаемые атрибуты можно приписывать к соответствующему предикату

р, добавляя в «ANTLR» ключевое слово `returns` вместе с наименованием атрибута перед двоеточием. Поэтому, необходимо определить, синтезируемы ли они и затем все атрибуты перевести и вписывать в соответствующее «ANTLR»-правило. Правила, конфликты и ограничения Пролога очень похожи на правила «ANTLR».

Когда абстрактные предикаты преобразуются в конкретную грамматику, например «ANTLR»-грамматику, то возникает проблема. Унифицированные термы, « \mapsto »-утверждения (терминалы) и нетерминалы следует преобразовать согласно данному синтаксису в грамматику вместе с аннотациями. Также «ANTLR» разрешает транслирующие правила, которые определяют семантику самой программы и записываются в «ANTLR» в фигурные скобки. Отрицание предложений и их под-предложений можно сформулировать в «ANTLR» с помощью « \sim » и скобок, которые означают, что данное регулярное выражение из « \mapsto »-терминалов должно или не должно следовать. Далее, элементы перевода грамматик не обсуждаются, т.к. с помощью атрибутов и транслирующих правил, можно имитировать все остальные выражения и предложения, в том числе и несовпадение предикатов (см. [291], [290], [110], [197], [252], [179]).

Графическая оболочка: Графическая оболочка (см. рисунок 73) состоит из трёх важных частей: (i) из левой части, которая содержит программу Си-диалекта, (ii) из правой верхней части, которая при выполнении программы содержит актуальное содержание динамической памяти и (iii) из правой нижней части содержащая программное представление в качестве термов Пролога. Содержание памяти и программное представление можно преобразовать в графическое представление. Кроме того, внизу имеются окна для ошибок и предупреждений, а также запись текущих операций верификации.

Разработка графической оболочки оказалась наиболее полезной в использовании, т.к. для автоматизации преобразования, отслеживания доказательств и представлений динамической памяти и правил верификации, вместе с программой, легче отслеживать, когда рядом имеются все необходимые данные.

Use Cases: Программист в данной оболочке задаёт и редактирует программу (см. рисунок 74). Для этого имеются синтаксические проверки, а также программное представление может отобразить в графическом представлении в формате «DOT» в виде дерева представить.

Роль персоны, которая специфицирует программу (см. рисунок 75), отличается от программиста — формальными, точнее логическими, формулами описывается поведение программы. Спецификации можно в систему заносить, редактировать до и

после загрузки программы. При запуске данные спецификации, которые размещены вместе с программой, проверяются. В случае возникновения ошибки, ошибка выделяется в правой нижней части. Проверка спецификации включает в себя при- и постусловия процедур, абстрактные предикаты, классные инварианты, но может также включать проверку полноты набора правил одного правила Пролога, касательно входной кучи.

Верификация кучи (см. рисунок 76) в отличие от редактирования программы заключается в вычислении и проверке имеющийся при выполнении программы состояния памяти с спецификацией. Для верификации необходимо проводить проверку сходимости куч, а также преобразование в нормализованную форму. Для упрощения и объяснения текущего доказательства имеются вспомогательные элементы, прежде всего, это визуализация дерева доказательства, генерация контр-примера, а также использование предыдущих доказательств для более быстрой сходимости.

Пример) Реверс линейного списка

Дан список {1,2,3}, имеется указатель *y* на последний элемент линейного списка. Тогда реверс списка можно описать рекурсивно, отделив последний элемент и присоединив его к началу отставшего списка. Таким образом, получается список как указано на рисунке 77.

Далее, получаем список как указано на рисунке 78.

Классовые определения Классовые экземпляры относятся в основном к классам Си++ или Ява и представляют упрощенный образ. Классы имеют разовый идентификатор, поля и методы. Поля и методы определяются в любом порядке и являются разовыми. Видимость для представления универсальности модели необязательна, но разрешается. Встроенные методы запрещаются, доступ к собственному классному экземпляру осуществляется с помощью `this`.

```

<class_definition> ::= [ <class_modifier> ] 'class' <ID> '{'
    <class_fields_methods> '}'

<class_fields_methods> ::= {          <class_field>          |
    <class_method> }*

<class_field> ::= [          <class_modifier>          ]
    <variable_declaration> ';'

<class_method> ::= [          <class_modifier>          ]
    <function_definition>
    | [ <class_modifier> ] <function_declaration> ';'

<class_modifier> ::= ( 'private' | 'public' | 'protected' ) ':'

```

Декларация типов следует в основном декларации по стандарту ISO-C++, которая разрешает неинициализированные и инициализированные переменные.

$\langle \text{variable_declaration} \rangle ::= \langle \text{type} \rangle \langle \text{ID} \rangle \{ ', ' \langle \text{ID} \rangle \}^*$
 $| \langle \text{type} \rangle \langle \text{ID} \rangle \{ ', ' \langle \text{ID} \rangle \}^* '=' \langle \text{expression} \rangle$

Определение функции осуществляется простым образом, т.е. неограниченные синтаксисом (variadic) параметры не допускаются. Конвенция вызовов подпроцедур следует схеме вызовов в языке Си. Тип возврата метода является либо void, либо базисным типом в данный момент. В ближайшее будущее объектные типы будут возвращаться, а до этого все изменения состояния вычисления передаются только с помощью параметров.

$\langle \text{function_definition} \rangle ::= \langle \text{function_declaration} \rangle \langle \text{block} \rangle$

$\langle \text{function_declaration} \rangle ::= \langle \text{type_or_void} \rangle \langle \text{ID} \rangle ' ($
 $\langle \text{formal_parameters} \rangle |) '$

$\langle \text{type} \rangle ::= \text{'int'}$

$\langle \text{type_or_void} \rangle ::= \langle \text{type} \rangle | \text{'void'}$

Встроенные правила для автоматизированного логического вывода

Нормализация куч осуществляется с помощью встроенного предиката Пролога simplify/2. Этот предикат принимает кучу в виде термина и возвращает терм кучи, в котором || оформляется крайней снаружи. Предполагается, для быстрой обработки, что входная куча уже ||-нормализована, т.е. в виде $q_0 || q_1 || \dots || q_k$, где $\forall j. q_i$ в виде $X_i \circ X_{i+1} \circ \dots \circ X_k$.

Высчитывание (“множественное сравнение”) осуществляется с помощью substruct. Этот встроенный предикат принимает список термов Пролога и генерирует список не хватающих термов кучи. Предикат может быть использован для установления полноты данного семейства предиката (например, важно для упрощения, трансформации и для обработки с тройками Хора в общем).

Сравнение производится покомпонентно с помощью двух термов: имеющейся и ожидаемой кучей.

Слойная архитектура верификатора

Предложенная архитектура верификатора “ProLogika” [306] состоит из 6 главных слоёв (см. рисунок 79), которые на периферии сотрудничают с библиотекой логического вывода “tuProlog” (2p), а также с генератором синтаксических анализаторов ANTLR в версии 4. Система реализована на языке Ява, хотя одновременно она тесно связана с реализацией Пролога и максимально близка к GNU Prolog. ANTLR может генерировать выходной код не только Ява, но также разных других языков программирования. Таким образом, обеспечены расширяемость и вариабельность системы “ProLogika”. “ANTLR” принципиально может быть заменено на любой другой синтаксический анализатор эквивалентной мощностью, под условием, что не только стартовый нетерминал может быть распознан, но также подграмматики используемых нетерминалов.

Система верификатора динамической памяти “ProLogika” состоит из следующих пакетов: internal, output, parsers, prolog, frontend и gui. gui предоставляет графическую оболочку и управленческие к ней модули. Результаты, промежуточные представления вычисления и визуализации выявляются в самой оболочке или могут быть запущены с ней.

Пакеты frontend и parsers тесно взаимосвязаны. Пакет frontend содержит интерфейсы и модули различного уровня абстракции для лексического и синтаксических анализаторов. Параметризация синтаксического анализа является одной из основных верификации абстрактных предикатов. parsers содержит изначально генерированные лексические и синтаксические анализаторы, а также анализаторы, генерируемые при запуске верификации. Интерпретация абстрактных предикатов входит в пакет ProLogika.internals.aps.

Пакет prolog обогащает встроенную систему логического вывода с дополнительными предикатами Пролога, например, для обработки термов куч, анализ и выявление ошибки, а также для реализации дальнейших побочных эффектов. Реализация дополнительных встроенных предикатов осуществляется таким дизайном, который гибок и легко может быть расширен. Правила Пролога могут быть всегда добавлены и расширены во время запуска программы верификации.

Пакет output предоставляет вспомогательные функции для писания термовых представлений, например, в DOT-файл или на консоль. На данный момент предусмотренная генерация OCL-кода не реализована.

Пакет internal производит саму спецификацию и верификацию связанных функций. Пакет core содержит различные модули, они связаны с обработкой термовых представлений куч. Пакет aps содержит все необходимые модули, которые связаны с абстрактными предикатами, следовательно, он связан с пакетом core. checkers производит проверку куч до, после и во время запуска программного оператора. Остальные пакеты подлежат сильному исправлению и находятся в настоящее время на стадии разработки.

Компоненты

В соответствии с разделом VI-H можно выявить 6 главных компонентов верификатора (см. рисунок 80): (i) ProLogika.GUI отвечает за графическую оболочку, (ii) ProLogika.parsers отвечает за всё, что связано с анализатором синтаксиса, включая проверки условий синтаксиса и семантики, а также за обработку абстрактных предикатов (пакеты parsers: incoming, intermediate и AbstractPredicates), (iii) библиотека Java SWT тесно связана с компонентом ProLogika.GUI и введён для поддержки платформы независимой от ОС, (iv) ANTLR компонент для построения языковых процессоров, (v) alice.tuProlog

представляет библиотечный компонент для реализации генеричного логического вывода, построен на основе Пролога, (vi) ProLogika.internal компонент представляющий Прологовские термы (PTerm) и правила (PRule, PSubgoal), которые используются другими компонентами.

Пакеты

Пакет alice.tuProlog (см. рисунок 81) содержит: (i) класс Term, который представляет собой общий Прологовский терм, который не является абстрактным, (ii) Library является Прологовской библиотекой, которая может содержать целую формальную теорию Прологовских правил. BuiltinLibrary является реализацией класса Library. Engine контейнер, который может производить логический вывод правил Хорна согласно данной теории. ResultInfo представляет совокупность любого количества результатов данному запросу (подцелей).

Пакет parsers:

Пакет parsers (см. рисунок 82) содержит пакеты: incoming, intermediate, prolog, а также два класса MetaType и MetaTypeManager. MetaType представляет определение типа во входной программе, например, класс или целое число (integer). MetaTypeManager является наблюдающей за определениями инстанций.

Пакет internal: Пакет содержит пакеты: core, checkers, aps, spec.

Пакет internal.core:

Пакет core (см. рисунок 83) содержит классы, которые представляют ядро модели логического вывода: термы, правила, символьные переменные, подцели, и т.д. Префикс -P ссылается на “Prolog”, классы строго соответствуют элементам ISO-Пролога.

Главными базисными элементами являются: PTerm, PRule и PSubgoal. Остальные P-классы соответствуют Прологу, ради исключения классу Unparsed, который частично вычисляемый терм, который полностью определён на более поздней стадии вычисления.

Пакет internal.checkers:

Проверки проводятся вместе с нормализацией и высчитыванием правил во время верификации, например во время анализа данного абстрактного предиката (APCompletenessChecker, HeapCompletenessChecker, PrologAPsChecker) (см. рисунок 84). Синтаксические анализы также проводятся во время анализа входной программы и проверки вставленных в программу спецификатором утверждения (например с помощью ANTLRGrammarChecker). Все проверки могут осуществляться, если реализовать интерфейс CheckerInterface конкретными методами.

Пакет internal.aps:

Пакет aps (см. рисунок 85) содержит ANTLRBuilder, ANTLRLauncher, GrammarBuilder, а также все остальные классы, которые обрабатывают абстрактные предикаты (APs) согласно формальной атрибутируемой грамматике (как было введено Кнудом и Вегнером). ANTLBuilder является специализацией класса GrammarBuilder. “ANTLR” используется изначально лишь как один пример генератора синтаксического анализа. Любой генератор или вручную написанный анализатор может послужить заменой, если предоставить необходимый интерфейс.

Аналогично выше сказанному, ANTTLRGrammar является специализацией класса FormalGrammar. ANTLRBuilder способствует к построению анализатора анализаторов.

ANTLRLauncher производит вызов драйвера ANTLR-генератора (для произведения различных функций ANTLR).

Синтаксические анализаторы: Класс Main (см. рисунок 86, связан с Parser из рисунка 87 и SyntaxAnalyzer из рисунка 88) управляет тремя инстанциями синтаксического анализа согласно формальным грамматикам: (1) ClassBased.g4, (2) IRProlog.g4, и (3) AbstractPredicates.g4.

Замечания: IRPrologCommand.execute() возвращает IRPrologDescription object.

Имеется паттерн:

```
ADAPTER::(CLASS) ADAPTER:
    SyntaxAnalyzerCommand
```

```
ADAPTER::ADAPTEE:
```

```
    ClassBasedCommand, IRPrologCommand,
    AbstractPredicatesCommand
```

```
Package parsers.incoming:
```

Следующая структура применима не только для parsers.incoming (см. рисунок 90), а также для parsers.intermediate и parsers.prolog.

Чтобы модифицировать синтаксический анализ при входе и выходе из правила нетерминала (срётка) были введены классы с суффиксом Listener.

Пакет parsers: см. рисунок 91.

Класс MetaType представляет встроенный или само-определяемый тип, который применяется при проверке типов над выражениями для входной программы. Каждый тип разово идентифицируется с помощью поля typeID. Однако, при построении типов typeID не присваивается изначально (только имя, но без полной сигнатуры, т.к. рекурсивные типы также разрешаются). Статически определёнными, встроенными типами являются: INTTYPE и VOIDTYPE.

Элементы пакета parsers.intermediate выполняют паттерн-роль “директора” для класса MetaTypeManager.

Пакет frontend см. рисунок 92.

Замечания:

STRATEGY::TEMPLATE:

SyntaxAnalyzer.launchMainNT()

STRATEGY::CONCRETE STRATEGY:

ClassBasedDescription.generateAST()

IRPrologDescription.generateAST()

AbstractPredicates.generateAST()

Метод SyntaxAnalyzer.launchMainNT выглядит следующим образом:

```
prelaunch();
this.tree=generateAST();
postlaunch();
```

В классе IRPrologDescription get-методы означают доступ к синтезированным атрибутам соответствующей формальной грамматики.

Класс ParserRuleContext содержит всё то, что употребляется наследованным и синтезируемым атрибутами.

Прологовские термы: Пакет internal.core см. рисунок 93.

Этот пакет содержит все представления всвязи с термами, подцелями и правилами.

COMPOSITE::COMPONENT:

PTerm

COMPOSITE::COMPOSITE:

PTerm

COMPOSITE::CONCRETE COMPOSITE:

PAtom, PVariable, PFunctor, PNumber, PList

PAtom.getChildren возвращает null. PAtom.setChildren игнорирует множество и при необходимости выделяет предупреждение на консоль. PSubgoal представляет подцель, которая далее может содержать PTerm как составляющее (не подцелей).

Замечания:

В пакете internal.core (см. рисунок 94) нет необходимости в PSubgoal, т.к. оно уже содержится в PRule, а также потому, что подцели являются частями запросов (которые не являются частью грамматики построенных абстрактных предикатов).

Метод GrammarBuilder.loadRules читает все PRule и заносит их в формальную грамматику, при этом, атрибуты остаются как в Прологе. Класс GrammarBuilder реализует оба интерфейса, PTermVisitor и PRuleVisitor, т.к. необходима интерпретация правил и должен иметься один нетерминал в качестве стартового символа грамматики.

PTerm и PRule-экземпляры генерируются в зависимости от экземпляров описаний (Description-objects).

Абстрактные предикаты: Абстрактные предикаты необходимы для представления и логической обработки в рамках верификации правил Хорна.

Используемые анализаторы имеют один начальный символ нетерминал, однако интерфейс анализатора должен предоставлять возможность распознавать одно или более того нетерминалов данной формальной грамматики, в данном случае (ANTLR-)грамматики.

Пакет internal.aps см. рисунок 95.

Замечания:

Все классы вовлечены в представление формальной грамматики (далее рассматривается возможность реализации на примере ANTLR).

PRule может быть представлено в виде FG_AP_Rule, а также обратно, следующим образом:

$$p1(X, pointsto(X, value1)):- \dots$$
$$\Leftrightarrow$$
$$p1_{x1,x2} \rightarrow \{X_1 \approx X\}\{X_2 \approx pointsto(X, value1)\}, \dots$$

Далее, FG_NT имеет атрибуты List<PTerm>, но только не List<FG_Att>, т.к. оно ссылается только на существующий нетерминал с конкретной последовательностью PTerm, согласно данному порядку определения атрибутов.

Термы кучи: Прологовские термы определены индуктивно над операторами { \circ , ||}. Полученный терм является итогом предыдущего синтаксического анализа.

Пакет internal.ht см. рисунок 96.

Подцели в абстрактных предикатах могут создавать связанный (под-)граф (ради простоты на данный момент, в общем случае с помощью проверок свойства $a \circ a$).

$a_1 \circ a_2 \circ a_3$ может быть записан непосредственно, используя a_1, a_2, a_3 (как часть абстрактного предиката) или как абстрактные предикаты $a_x : -a_1, a_2$, где оно же далее может опять же выступить в качестве некоторой подцели: \dots, a_x, a_3, \dots

Пример 2) $a_1 \circ (a_2 || a_3)$ можно перезаписать, как абстрактный предикат как: $a_x : -a_2, disj, a_3$, где имеется некоторая последовательность как часть абстрактного предиката \dots, a_1, a_x, \dots

Замечания:

HeapTerm является внутренним представлением кучи на основе ЛРП.

Термы кучи над { \circ , ||} может также содержать частичные спецификации. Терм кучи строится пошагово при анализе данных абстрактных предикатов.

HeapTerm.simplify ссылается на BuiltinLibrary.simplify_1(). Упрощения термов кучи осуществляется с помощью перегруженных встроенных предикатов Пролога simplify_2.

Граф кучи представленный термом кучи, может также описывать не полностью специфицированные части с помощью Пролог-оператора “_”. Нормализация данных конъюнктов заключается в лексикографической сортировке порядка всех левых сторон базисных куч.

DotGenerator генерирует векторную графику на основе DOT-формата или в качестве его представления в качестве одной строки, которую позже можно записать в файл, например.

Замечания:

Проводится проверка корректности, например (i) соблюдается ли неповторимость кучи, (ii) связана ли куча, и т.д.

Пакет prolog см. рисунок 97.

Библиотека BuiltinLibrary содержит все Прологовские предикаты, которые становятся доступными для логического анализатора на основе Пролога. Если распознавание одного абстрактного предиката будет завершено целиком, тогда проводится проверка $a \circ a$.

Замечания:

BuiltinLibrary:disj_0 совершает один шаг в верификации динамической памяти. Для этого могут вводиться специальные метки в случае не достижения границ куч.

BuiltinLibrary:unify предоставляет замену классической унификации термов ($=/2$) с помощью и без проверки повторений.

Класс HeapTerm ссылается на BuiltinLibrary:simplify_1.

BuiltinLibrary::serialize_1 почти эквивалентна к serialize_2, ради исключения, что содержимое выдается на консоль.

StackState необходимо для проверки диапазонов годности (например, является ли символ частью данного контекста, когда все остальные семантические проверки уже успешно завершились). Сигнатур имеет тип: $\sigma :: String \rightarrow Type \rightarrow Value$.

Выводы

Представленный подход представляет собой новую технологию для автоматической верификации « \mapsto »-утверждений в абстрактных предикатах синтаксическим путём, избегая ручные предикаты «сложить» и «раскрыть». Если раздел предикатов может быть представлен как корректное множество правил, синтаксических правил перебора, то ответ будет найден, совпадает ли данная спецификация с данной конфигурацией кучи или нет. Используется атрибутируемая грамматика [110] в качестве соединяющей модели представления правил

в Прологе и конкретное множество правил перебора. Атрибутируемая грамматика поддерживает наследованные и синтезированные атрибуты, которые переводятся как параметры головы правила Хорна. Кроме удобного представления значений, с помощью Пролога обработка сверху-вниз и с символами также совпадает с порядком вычисления и вывода. Без модификации логического вывода Пролога [266] совершается процесс верификации. Расширения, например, представленные преобразования термов и атомов, моделирование куч и т.д. не противоречит корневым свойствам ЛРП (см. главу III и V). Поэтому, свойства не меняются, если соблюдать локальность спецификации объектных экземпляров. Не ссылочные поля объекта необходимо специфицировать только в одном предикате один раз. Замечание о том, что прологовские правила могут обрабатываться WAM и поэтому могут пострадать в скорости, нельзя считать справедливым, т.к. интерпретация в принципе может быть заменена компиляцией оптимизированного кода для любой целевой машины. Однако, вопрос быстрой верификации стоит не на первом месте. На первом месте стоят вопросы сложности и выразимости. Таким образом, умышленно используется не самый быстрый способ верификации.

В отличие от предыдущих подходов, представлен новый подход, отличающийся резко тем, что символы больше не являются просто локальными переменными. Символы как логические используются произвольно в логических термах и предикатах. Язык утверждений и верификации теперь совпадают при использовании диалекта «Пролог». Теперь дополнительные преобразования для обеих сторон отпадают, также как и имеющиеся ограничения в предыдущих подходах (см. [32]).

Открытым вопросом остаётся, как правила ошибки могут быть эффективно подключены к генерации контр-примеров и какие имеются способы для отслеживания ошибок в связи с этим? Из-за приостановки при первой ошибке, все остальные ошибки не рассматриваются, если настоящей ошибкой по происхождению является одна из последовательных. Поэтому предлагается рассматривать «конечный автомат» для сравнения и минимизации «прописной дистанции» между имеющейся и ожидаемой кучами, аналогично глобальному алгоритму Левенштейна [287], [264], [11] для вычитания минимального количества операций замены за $\Theta(n^3)$, удаления и вставки подкуч. Метод Левенштейна может быть не обобщён, но модифицирован и расширен к деревьям [230], [284], [10]. «Метод паники» [110], [197] который при возникновении ошибки во время синтаксического анализа пытается продолжить перебор с помощью обнаружения самого ближнего следующего состояния, гарантированно верное и стабильное при удалении

всех «лишних» токенов.

Далее предлагается рассматривать вопрос о частичных спецификациях, как константных функций `emp`, `true` или `false` для достижения упрощённой верификации (см. следующие главы). В частности, задаётся вопрос, можно ли с помощью частичных спецификаций выявить недостижимые мосты, которые предположительно связывают независимые кучи для исправления имеющейся спецификации.

Заключение

«Значимые результаты» Во время работы были получены результаты, которые можно классифицировать: в области автоматизации доказательств:

- 1) Анализ разрыва между языками спецификации и верификации динамической памяти и анализ его сближения.
- 2) Анализ и измерение выразимости трансформаций термов в логической парадигме на примере диалекта Пролога. Выявление, что логическое описание утверждениями из символов, переменных и термов в общем, а также реляций, естественно лучше приспособливает и ближе к верификации задач динамической памяти в Прологе.
- 3) Термы Пролога как главное промежуточное представление на протяжении всего конвейера статического анализа проблем динамической памяти.
 - Обоснование и использование логического языка в качестве спецификации и верификации. Главная мысль — логическое программирование для решения верификации теорем.
 - Предложенная платформа, изначально построена как открытая для расширений и вариаций. Платформа позволяет включение дополнительных экстерных библиотек и логических решателей в Прологе.
 - Исследование демонстрирует преимущество Пролога.
- 4) Предложение об автоматизации верификации куч, как синтаксический перебор абстрактных предикатов, основано на пошаговой обработке граней графа кучи.

выразимости языков спецификации и верификации:

- 1) Теперь доказуемые абстрактные предикаты могут без ограничения содержать символы и переменные согласно правилам Хорна, что расширяет сегодняшние ограничения. Теперь предикаты могут иметь потенциально любые рекурсивные определения, где выбранный метод синтаксического перебора может ограничить рекурсию, возможно потребовав переоформление правил.

- 2) Повышение выразимости, благодаря ужесточению операций над кучами. Имеется строгое соотношение между выражением кучи и ее графом. Теперь пространственные операторы куч формируют однозначные термы утверждения. Доказываются алгебраические свойства моноида и группы, которые позволяют определение вычислений над кучами. Предложение о расширении и возможной стандартизации «UML/OCL» указателями.
- 3) Повышение выразимости и полноты, благодаря частичной спецификации куч переменных и объектных экземпляров. Сравнимость теперь позволяет все входные кучи одного набора сравнить и «ямы» или «пересечения» эффективно вычислить. Теперь правила могут быть написаны, охватывая потенциально больше случаев.
- 4) Теоретическая возможность, исходя из ужесточенного представления, выявить и проверить данную входную программу на минимальность для покрытия граф кучи полностью («проблема содержимого») при исключении определений абстрактных предикатов в общем случае.

Выводы:

- 1) Единый язык спецификации и верификации. Унификация языков спецификации и верификации к логическому языку программирования диалекту Пролога представляется как одна из крайних мер борьбы с многозначностью и позволяет решить поставленные перед собой проблемы выразимости и полноты. Чем меньше имеется языков и особенностей, тем меньше требуется рассматривать. Особенно, когда языки спецификации и верификации являются по синтаксису и семантике простым единым языком. Процесс верификации представляется как сравнение имеющейся и должной кучи. По ходу исследований существующих средств верификации динамической памяти и соответствующих проектов в качестве примеров, мною были разработаны «shrinker» и «builder» в качестве вспомогательных программных систем. Итогом расследования оказалось, что проблемы решённые верификаторами на практике крайне редкие или применимы только в случаях, для которых они были разработаны, а применение в других областях практически исключено.
- 2) «Нет» новым и дубликатным определениям. Использование Пролога позволяет избежать введение всё новых конвенций, определений, языков спецификации, программирования, верификаций и даже сред. Отсутствует

необходимость введения определений, которые оказывались в прошлом лишними и дубликатными. Выявлены важные свойства и критерии, которые учтены при построении платформы. Теперь кучи и части могут быть выбраны термами и символами. Абстрактные предикаты представляются обыкновенными прологовскими правилами. Используется промежуточное термовое представление, в качестве входного языка, а также разрешается Си-диалект, либо любой другой императивный язык программирования. Также допускается полное отсутствие входного языка, в таком случае, разрешается непосредственная передача промежуточного представления в ядро верификации.

- 3) Повышенная выразимость в связи с символами на основе Пролога. Он основан на и реализует предикатную логику в качестве модели и реализации. Предикаты куч стали по-настоящему логически абстрактными (и не «Абстрактными»), а именно прологовскими предикатами. В предикате символы допускаются в любых местах и ограничения касательно символьного использования отсутствуют. Логический вывод производится символами, логические выводы не возвращаются, благодаря унификации и реализации стека с возвратом на основе машины Уоррена. Проводилось обсуждение, что граф кучи можно полностью выразить. Объекты представляются как кучи, методы классов специфицируются не обязательно пред- и постусловием аналогично к процедурам. Правило фрейма способствует аналогичному поведению у процедур и позволяет включение в фрейм утверждения по всему циклу существования объекта. Объекты могут быть переданы в качестве символьного параметра абстрактным предикатам, таким образом, повышается модульность и благодаря неполным константным функциям неполный объект необходимо специфицировать.
- 4) Реляционная модель правильна и нужна для эффективного описания абстрактных предикатов. Реляционная модель в отличие от других представлений была в итоге выбрана как наиболее удобная для описания и проверки куч. Также упоминают источники из списка литературы. Хотя численный анализ трудный, из-за выбора адекватных примеров и численной значимости, всё равно, проведённая экспертиза показала, что запись в прологовских терминах для проверенного набора примеров всегда лучше, а в среднем арифметическом на 30% компактнее и более гибкая, чем например эквивалентная функциональная запись. Приведены типичные

примеры, которые не могут быть эффективно или точно представлены в функциональных или императивных парадигмах.

- 5) В Прологе предложена платформа конвейера. Платформа предлагает крайне простую архитектуру по обработке входного языка и правил верификации. Платформа основывается на Прологе, на конвейере фаз по обработке динамической памяти, которые могут индивидуально меняться и добавляться. Платформа отличается принципами: (а) автоматизацией, (б) открытостью, (в) расширяемостью и (г) понятностью. Выводимо только то, что выводимо из данного набора прологовских правил — это предоставляет известно резкое, но умышленное, ограничение. Правила верификации, леммы и индуктивно определённые абстрактные предикаты, всё записывается на Прологе. Модификации в структуре доказательства получаются задачами программирования и могут быть проверены на каждой фазе.
- 6) Упрощение спецификации и верификации ради ужесточения. Нашлось ужесточенное определение одночленной кучи, вместо множественного числа куч. Ужесточение заключается в атомизме куч. Благодаря этому, чётче, проще и короче можно специфицировать кучи. Принудительное сравнение куч со всеми остальными кучами отпадает, основные кучи сохраняются. Сейчас кучи можно эффективно сравнивать. Благодаря групповым свойствам, теперь можно высчитывать, устанавливать в наборе правил не хватающую кучу и таким образом, можно проверять полноту. Далее, благодаря частичным спецификациям, сейчас можно уменьшать и редуцировать количество и объём специфицируемых правил с кучами — исключения исключаются, полнота доказывается с помощью неполноты. На практике ужесточение означает, что подвыражения кучи больше не должны полностью анализироваться. Так как «UML/OCL» не содержит указателей, но представленные условия и критерии совместимы, то предлагается соответствующее расширение.
- 7) Возможность определения всё новых теорий над кучами. Выявленные алгебраические свойства позволяют определять равенства и неравенства между кучами. Эти формальные теории могут непосредственно задаваться в Пролог, либо соответствующим SAT-решателям (возможно, также на основе Пролога). Теперь правила и теории проверяются проще.
- 8) Абстрактные предикаты определяют атрибутируемую грамматику. Аналогично к проверкам схем при слабо структурированных

данных, абстрактные предикаты являются шаблонами, которые содержат «дыры». Они наполняются во время верификации. Эта мета-концепция приводит к синтаксическому анализатору. В итоге логический вывод абстрактных предикатов можно интерпретировать как синтаксический анализ. Сравнение актуальной кучи с ожидаемой, можно расталкивать как проблему слов в формальных языках. Естественно, этот универсальный метод имеет ограничения касательно распознавателя, однако, подход очень практичен, несмотря на теоретический формализм, на котором основан процесс перевода.

- 9) Универсальный подход к автоматизации утверждений. Предикаты и доказательство производятся на основе Пролога и могут мульти-парадигмально включать любые другие библиотеки. Доказательство приближается к программированию. Необходимость повторно определять процесс перевода и описания правил отпадает потому, что Пролог всё это включает в себя, хотя сам язык минимален. Необходимость проводить свёртывание и развёртывание вручную отпадает. Если куча не выводима по данным правилам, то можно их переписать. Синтаксический анализ решим и терминация гарантирована, например, на основе LL-распознавателей за линейное время. Процесс генерации анализатора производится лишь после изменения правил. В зависимости от доступности начальных нетерминалов, распознавание подграмматик избегает необходимости принудительного построения всё новых анализаторов. На практике все нетерминалы могут теоретически быть использованы после построения анализатора. Синтаксические анализаторы не нуждаются в дальнейших исследованиях, т.к. они отлично изучены на сегодняшний день, следовательно, не требуется дальнейшее исследование анализатора, который используется в данной реализации. В случае ошибки, автоматическая генерация и выдачи контр-примера, производится анализатором без дополнительных затрат.

«Дальнейшее исследование» В числе дальнейших исследовательских и практических работ можно выявить следующие (не отсортировано по важности):

- 1) Интеграция решателя. После определения теории куч, для ускоренного логического вывода необходимо подключение «SAT»-решателя. Решатель также может быть написан в самом Прологе.
- 2) I Интеграция в существующие среды. Помимо упомянутых ограничений, необходимо на

практике преобразовать термовое IR в IR пактов «GCC», либо «LLVM» для индустриального применения.

- 3) II Интеграция в существующие среды. Точечный анализ мест «разрастания» (образов) может также привести к более выгодному выделению и расположению памяти, подключая аппроксимацию метод абстрактной интерпретации. Также необходимо рассмотреть возможность выражений с статически выявляемыми офсетами ради широкой практической применимости.
- 4) Изоморфизм куч. Проверка изоморфизма графов в случае возникновения вопроса: может ли куча в принципе быть представлена данными указателями, при этом наименования кучи не уточняются?
- 5) Нахождения минимального отклонения от спецификации. При синтаксическом переборе может иметь смысл найти глобальный минимум прописной дистанции для проверки и возможной редакции спецификации.
- 6) Анализ зависимостей указателей. В отличие от анализа псевдонимов, рекомендуется исследовать расширение SSA-формы для динамических переменных, что до этого ещё никем не рассматривалось. Ожидается расхождение, т.к. понятие о зависимости различается. Возможность подключения может также подтвердить более безопасный код при оптимизации, т.к. на первый взгляд несвязанные ячейки связываются, либо точно не связываются. Это также способствует эффективному коду.
- 7) Верификация кодов баз. В этой работе после устранения технических ограничений в связи с быстрой прототипизацией, предлагается проводить анализ имеющихся кодов баз. Для этого предлагается использовать в открытом доступе пользования, потому, что они также значительно различаются.
- 8) Исследование применимости языков трансформаций на практические нужды. Обсуждённые языки трансформации могут иметь компактную запись и также часто записываются с помощью правил состояний до и после трансформации, однако ожидается большое расстояние между используемой моделью кучи, моделью выразимости и содержанием динамических куч, входным языком.
- 9) Абстракция вывода. Некоторые диалекты Пролога поддерживают абдуктивный вывод. В общем, абстракция механизма, который позволяет правила Пролога упростить, сравнить с подходящими пред- и постусловиями и выбрать наиболее подходящее правило. Порядок вывода можно упростить, если соотношения

между термами обратимы. Это как раз было предложено и обсуждено в этой работе.

«Рекомендации для применения» В числе рекомендаций по итогам работы можно вывести следующие:

- Практически спецификация куч стала (немного) проще, если даже не больше. Данная программа аннотируется спецификацией.
- Абстрактные предикаты должны быть синтаксически разборчивыми, тогда подцели соответствующей формальной грамматики можно распознать. В зависимости от мощи анализатора часто переписывание правил приводит к разборчивости.
- Использование ужесточенных операторов даёт возможность в спецификациях «UML/OCl» пространственность объектных экземпляров выражать.
- Введение всё новых языков программирования не обязательное. Язык программирования может даже полностью отсутствовать. Расширяемое и модифицируемое промежуточное представление позволяет максимальную гибкость. Архитектура верификации имеет те же самые свойства.
- Сравнение куч с данными выражениями в правилах верификации способствует выявить не специфицированные кучи, а более широко способствует к решению вопроса полноты.
- Перегрузка значений реляций упрощает гибкость логического вывода, например, в связи с абдукцией, но также может быть использована различными способами.
- Использование SAT-решателя для задаваемых теорий куч, будь-то в Прологе или мульти-парадигмально, может привести к резкому ускорению преобразования куч в нормализованную и упрощённую форму.
- Использование мемоизатора (в некоторых диалектах Пролога «tabling») для абстрактных предикатов может привести к резкому ускорению логического вывода, в частности при пошаговой верификации.
- При введении и модификации фаз работы с динамической памятью рекомендуется придерживаться к термовому представлению.

Nomenclature			
AA	Alias Analysis	RAM	Random-Access Memory
ABI	Application Binary Interface	ROSE	a compiler-compiler
ACC	Abadi-Cardelli Calculus/(-i)	RTTI	Run-time type identification
ADT	Abstract Data Type	SA	Shape Analysis
ALC	Abadi-Leino Calculus/(-i)	SL	Separation Logic
ANTLR	a compiler-compiler	SAT	SATisfaction of a logical formula
AP	Abstract Predicate	SMT	Satisfactority Modulo Theory
API	Application Programming Interface	SSA	Single Static Assignment
AST	Abstract Syntax Tree	SSD	Solid State Drive
AT	Automated Testing	tuProlog	a Prolog backend
BB	Basic Block	TIOBE	The Importance of Being Earnest (index)
BISON	a compiler-compiler	UML	Unified Modeling Language
BNF	Backus-Naur Form	VM	Virtual Machine
BSS	Block Started by Symbol	WAM	Warren's Abstract Machine
CF	Context-free	XOR	eXclusive OR
CI	Code Introspection	YACC	a compiler-compiler
Clang	LLVM's compiler frontend	XML	eXtensible Meta Language
CompCert	Leroy's Compiler Prover	iff	if and only if
Coq	a theorem prover	algo	algorithm
CPU	Central Processing Unit	cf	compare
CFG	Control-flow Graph	conv	convention
CRT	Church-Rosser Theorem	cor	corollary
DCG	Definite Clause Grammar	def	definition
DEC	Digital Equipment Corporation	eg	for instance
DOT	a textual vector graphics format	eqn	equation
ESC	Extended Static Checker (Java)	fig	figure
GC	Garbage Collection	lem	lemma
GCC	GNU Compiler Compiler	obs	observation
GIMPLE	GNU tree IR of Programming units	poset	partially-ordered set
GNU	GNU is Not Unix	stderr	console standard error
GUI	Graphical User Interface	stdout	console standard output
HDD	Hard Drive Disk	theo	theorem
EBNF	Extended BNF	thes	thesis
IR	Intermediate Representation	wlog	without loss of generality
ISO	Intl. Standardization Organization	wrt	with respect to
LCF	Logic of Computable Functions (Scott)		
LISP	List Processing (language)		
LL	Left-to-Left parser		
LLVM	Low-level Virtual Machine		
LR	Left-to-Right parser		
ML	Meta-Language		
MVC	Model-View-Controller		
NT	Non-Terminal		
OC	Object Calculus		
Ocaml	Oca-ML		
OCL	Object Constraint Language		
OOM	Object-oriented Modelling		
OS	Operating System		
PCP	Post's Correspondence Problem		
PCF	Programming Computable Functions		
PL	Programming Language		
Prolog	Programming in Logic (language)		
ProLogika	a Prolog-dialect heap verifier		
PVS	a theorem prover		
RC	Region Calculus		

Absorption.

In a boolean algebra, given some \uparrow propositions p and q the following holds: $p \wedge (p \vee q) \equiv p \vee (p \wedge q) \equiv p$.

Abstract Data Type.

Precursor concept of the \uparrow class concept where operations define interfaces, \uparrow methods and \uparrow fields. Defines operations for both, which change its interior behaviour and communication with external objects.

Abstract Interpretation.

\uparrow Static analysis method based on interval calculi and extended denotations.

Abstract Predicate.

In this work, a heap predicate with term parameters. Heaps are composed of simple heaps that are atomic \uparrow points-to \uparrow assertions.

Alias.

A \uparrow pointer, which points to the same content as another pointer.

(Algebraic) Field.

A discrete structure with two operations (a special ring), for which hold, e.g. rules over $+$ and \cdot , with two neutral and inverse elements. If the field is finite, then the field is Galois.

(Algebraic) Group.

A \uparrow monoid in which for each element the inverse element exists.

Antecedent.

A is the antecedent for any rule of kind: "if A then B ".

Assertion (about a Program Property).

Assertion about a calculation state described by some \uparrow formal language, e.g. by first-order \uparrow predicate logic.

Atomism.

An analytical (philosophical) concept suggests breaking complex problems down into small indivisible units, namely atoms. Has found wide adaption in many branches of science. Here a discussion of heaps and compositions were discussed.

Attributed Grammar.

A \uparrow formal grammar with rules that are extended by attributes may either be \uparrow inherited or \uparrow synthesised. Attributes may be considered as parameters in their rule bodies.

Automated Theorem Proving.

Proof of a \uparrow theorem using formal apparatus, s.t. the proof runs through from the beginning till the end without the need for human interaction. This is in contrast to \uparrow partially automated proofs or \uparrow interactive proofs, which both require interaction.

Automatically (Stack-) allocated variable.

See \uparrow stack

Calculation State.

Description of \uparrow stack and \uparrow heap, so a list of all \uparrow variables, which during a calculation step are allocated having some \uparrow content assigned.

Church's (Term) Arithmetics.

Arithmetic of natural numbers over terms instead of numbers. The mapping between both domains is defined by $0 \mapsto z$, $1 \mapsto s(z)$, $2 \mapsto s(s(z))$, and so on. So, $m+n$ may be defined as $s^m + s^n = s^{m+n}$. Minus as plus' inverse can be defined in analogy to that by structural induction and by term unification and pattern matching. The advantage of terms over natural numbers is \uparrow invertibility of terms due to term unification.

Class.

A record (struct) type uniting \uparrow fields and \uparrow methods.

Class Field.

Memory cell of arbitrary type (e.g. a class) of a class-object.

Class Inheritance.

Inheritance of \uparrow fields and \uparrow methods from a super-class into a sub-class according to defined \uparrow visibility levels.

Class Object.

A variable referring to some allocated, atomic and non-overlapping memory region, instantiated by a corresponding \uparrow class or subclasses.

Class Polymorphism.

An \uparrow object instance is of some \uparrow class. Type membership may change. It may be assigned to subclasses which would cause a different runtime behaviour if a subclass' method is overridden and called.

(Class) Visibility Mode.

\uparrow Fields and \uparrow methods of a \uparrow class may have an explicit visibility mode assigned and be inherited. Unlike C structs, fields and methods are private by default. The default class visibility is public. Visibility inherited in Java stays the same or is reduced by one level. In C, it is similar to Java, except for inheritance modifiers. The visibility levels are usually: private, public, protected.

Clause.

Disjunctive normal-form in which all \uparrow literals are interconnected.

Co-Routine.

A (sub-)procedure call simultaneously to some main procedure. \uparrow Functionals may often run as co-routine.

(Codd's) Relational Algebra.

Here relational "functions" as predicates, particularly as \uparrow Prolog predicates. The base operations in the original algebra are defined over sets: union, intersection, Cartesian product, projection, selection and renaming.

Code Introspection.

Modification and reading of any object's \uparrow fields and \uparrow methods during runtime. Code to be loaded may only be available during runtime, e.g. constructed from external data sources.

Control Inversion.

Usually, control is passed from the calling side (caller) to the called side (callee). Inversion flips the call direction and is occasionally needed in order to stick to the information hiding principle. It is an essential technique for \uparrow framework design, particularly for all callbacks.

Consequent.

B is the consequent for any rule of kind: "if A then B ".

Content Of Pointer.

Data in the memory cell pointed by some \uparrow pointer.

Counter-Example.

A single example showing that a certain \uparrow assertion does universally not hold.

Counter-Example Generation.

See \uparrow counter-example. Generation is due to Prolog term unification or abstract predicate derivation of calculated and expected heap terms.

Data Dependency Analysis.

Analysis based on the places in code for variables, namely its definition and uses and how these are influencing other variables, e.g. in a SSA-form.

Declarative Programming Language.

Logical or functional programming languages. "Imperative" solves a problem by an instruction list, where "declarative" only describes.

Dependent Type (also Recursive or Generalised type).

Type depending on type(s). E.g. records (struct).

Dynamic Memory.

The unorganised memory segment as \uparrow stack, allocated by a process spawn by the OS. Dynamic memory is synonym of \uparrow heap and contains all dynamically allocated variables.

Dynamic Memory Issues.

Problems such as \uparrow dangling pointers, \uparrow memory leaks, \uparrow invalid memory access.

Dynamic Variable.

Allocation and deallocation of \uparrow heap memory are specified by reserved statements, like new or free. Non-specified deallocations are freed when the OS releases the primary process.

Earley-Parser.

Some CF-parser pushing in rule definitions into the \uparrow stack.

Edge-based Heap Graph.

\uparrow Heap graph in which edges are a list with two columns: source and destination.

Erroneous Code Localization.

An \uparrow (erroneous) symptom search process terminating in the genuine reason a problem occurs. A manual search is called debugging.

Error-Production Rules.

Rules in case of a syntax error during parsing that define the further steps, including a possible error messaging, recovery or further restoration tasks to be triggered.

Evaluation Ordering.

The ordering in which (sub-)expressions are evaluated, e.g. left-to-right, outermost-first, \uparrow lazy evaluation.

Fail-As-Error.

Prolog built-in \uparrow predicate "fail" in combination with \uparrow cut alternatives.

Finite Automaton.

A simple directed graph representing \uparrow calculation states and whose edges represent state transitions from the

source state to the destination state. An automaton has one starting state and one or more final states. Transitions are rules which must be right-recursive, so of kind $A \rightarrow aB$, where a denotes a terminal, and A, B are non-terminals. Non-terminals are replaced with their right-hand side definition.

Fixpoint Combinator.

A syntactic, artificial operator is introduced and is no element of any programming language. It is to simulate recursion. Combinators are elements of λ -calculi.

Formal Grammar.

A formal notation proposed by Noam Chomsky to generate non-ambiguous formal languages, in analogy to natural language's grammars. Programming, specification, and verification languages are examples of formal languages. A formal language is defined as (S, T, NT, P) , where $S \in NT$ denotes some starting non-terminal, T a set of terminals, NT a set of non-terminals, and P a set of production rules. The expressibility level of a formal language depends on the P .

Formal Language.

Generated language for a given \uparrow formal grammar.

Formal Language Mismatch.

Formal languages may have different purposes, they differ in syntax, semantics and intuitive meaning. Symbols and alphabet may have different connotations with different level of ambiguity. The differences cause problems with expressibility, comparability, and further.

Framework.

A special library, also a non-standalone software, with dedicated functions. Framework functions often are due to a very special purpose only and have to obey dedicated instantiation constraints and are specially designed with software extension and variability points. A framework defines roles of interaction between several actors as abstract data types. The interaction points are designed by contract. A user does not have to know all details functions are implemented, but the user must know how to obtain and modify functionality as well as how to extend behaviour.

Garbage Collection.

E.g. \uparrow generational, \uparrow mapped. See \uparrow heap garbage.

Generalized Heap.

Is either a \uparrow simple heap, a composition of simple heaps, or a complex \uparrow heap possibly containing \uparrow abstract predicates calls as \uparrow subgoals.

Generational Garbage Collection.

\uparrow Garbage collection where pointers with an older timestamp or content since the last modification is moved or removed entirely from \uparrow dynamic memory.

Global Variable.

Global variables are accommodated once to the .bss memory segment managed by the OS containing uninitialised data. A global variable may be covered by other non-global variables, e.g. by \uparrow local variables with the same qualified name.

(Graph) Dominator (Vertex).

Vertex in a directed graph relative to another vertex, so no alternative path exists, except all passing the dominator vertex.

Heap Address Space.

Linearly addressable memory chunk in virtual memory allocated by an OS process occupied by the \uparrow heap segment.

Heap Assertion.

In terms of points-to model, an assertion about \uparrow pointers, their interdependencies and content in \uparrow heap.

Heap Cell.

A contiguous memory leap whose size is defined by the corresponding \uparrow pointer's type.

Heap Configuration.

Some concrete ground \uparrow heap graph.

Heap Conjunction.

Two \uparrow heaps are connected, implying at vertex is shared between both.

Heap Disjunction.

Two \uparrow heaps are separate from each other, so there is no connection between both.

Heap Inversion.

\uparrow Heap conjunction together with its inverse \uparrow heap is defined as the \uparrow empty heap.

Heap Formula.

Some \uparrow heap assertion has no unground free \uparrow variables. A heap formula is subject to interpretation, so it is true or false for some concrete heap.

Heap Frame.

Invariant \uparrow heap parts used to specify procedure calls.

Heap Garbage.

\uparrow Heap parts that are not pointed by \uparrow pointers nor locations. Heap parts are subject to \uparrow garbage collection.

Heap Graph.

A graph representation of a \uparrow heap, where edges define dependencies between heaps and vertices are pairs $loc \mapsto val$.

Heap Interpretation.

Comparison between a given \uparrow heap and a specified.

Heap Structure.

Spatial connected data structure located in the \uparrow heap segment. Its location may either be in \uparrow stack or \uparrow heap, and where its content is in heap.

Higher-Order Function.

Function accepting functions as input and output.

Hindley-Millner Type Systems.

\uparrow Type checking with typing rules, where the major inference rule is: Given some type a and some \uparrow functional (e.g. some unary operator) of type $a \rightarrow b$, then the result will have type b .

Hoare Calculus.

A formal method proving the presence of properties for a given program using mathematical-logical formulae. The effect of a given statement for some imperative programming language is caught by a \uparrow calculation state

before execution, called \uparrow pre-condition, and after execution, called \uparrow post-condition.

Hoare Triple.

A triple of kind $\{P\}C\{Q\}$, where (1) \uparrow calculation state P before C is executed, (2) statement C , (3) calculation state Q after C is executed.

Homomorphism.

If there is one function (or operation) g , then there is a homomorphism w.r.t. to yet another function h , if $h(g(x_0, x_1, \dots, x_n)) \equiv g(h(x_0), h(x_1), \dots, h(x_n))$ holds, where $\forall j. x_j$ are term arguments.

Howard-Curry Isomorphism.

Postulate according to which proving and programming are interconnected.

I/O-Term (in Prolog).

A Prolog term that is used as \uparrow I-term and \uparrow O-term at the same time. This is possible, for instance, in unground composed terms.

I-Term (in Prolog).

A Prolog term that can, but not necessarily has to, be ground. Applied to a subgoal, expects term is used but remains untouched.

Incomplete Heap.

Partially defined heap, which may contain unassigned symbols. Incomplete heaps may match patterns for short specifications.

Inductive Structure Definition.

\uparrow Linear lists, binary tree, \uparrow heap, etc.

Information Hiding Principle.

States by default \uparrow abstract data types need to restrict \uparrow visibility levels as much as possible in order to avoid too lax permission granting, so for instance, communication interfaces may adequately be defined, varied and extended later on.

Inherited Attribute.

An attribute in an \uparrow attributed grammar is passed from the calling rule down to the called rule. Here \uparrow predicates may act like rules.

Initial Denotation.

Denotation assigned to variables. Uninitialised variables may lead to a series of problems, especially when reading an uninitialised variable. \uparrow Heap variables and data on the .bss-segment are not initialised.

Input Token Stream.

A stream of \uparrow tokens obtained during lexical analysis.

Intermediate Representation.

\uparrow Terms, triads, tetrads and further notations representing some incoming program and annotated verification conditions and abstract \uparrow predicates.

Inter-Procedural Alias-Analysis.

Calculation of \uparrow alias parameters and \uparrow global variables, which may change between procedure calls. Compared to the \uparrow intra-procedural analysis, inter-procedural analyses are more complicated and usually are bound by exponential complexity.

Intra-Procedural Alias-Analysis.

See \uparrow inter-procedural alias analysis. It is only inside a procedure and often analyses are bound by polynomial complexity.

Intuitive Reasoning.

Judgements on reasoning that rely only on \uparrow facts and rules of form \uparrow if A , then B (so-called "modus ponens").

Invalid Memory Access.

May read unintended data and cause a page fault. In consequence, may corrupt execution, crash or even compromise the running process.

Lambda Abstraction.

A theoretical abstraction of a classic procedure, as known in Pascal or C. It was proposed in the 1930s by Alonzo Church in order to reason about computability.

Lazy Evaluation.

Expression evaluation from outside-in. Initially, parameters in a procedure call are passed non-interpreted and are interpreted in a procedure only if referenced concretely. Internally lazy expressions are assigned a symbol and passed that until some arithmetic or logical operation has to be performed.

Levenshtein's Algorithm.

The core algorithm for determining the minimal edit distance, an integer denoting the total edits required to equal two strings. The algorithm is of cubic complexity and may for the same complexity be enriched by path segment tracing.

Linear List.

A list whose elements have no pointers or are all pointing to nil. In Reynolds' memory model the `"`, `"` initialises a linear list.

Literal (Assertion).

An atomic \uparrow assertion or its negation.

LL-Parser.

Parsing where \uparrow input tokens are processed from left to right, and rules of given corresponding \uparrow formal grammar are processed top-down.

Local Variable.

\uparrow Automatically managed variable

Locality Principle.

Principle after which local changes to some \uparrow heap must not affect the whole \uparrow heap. If modelled correctly, then this may heavily improve heap analyses.

Location.

A variable, pointer or any path to any reachable object field.

Logical Heap Operator.

Logical implication, disjunction, conjunction, negation.

Loop Invariant.

A condition formula, which holds for the time a loop is executed. The condition does not hold anymore when that loop is quit. A full and exact invariant refers to all visible \uparrow variables from a loop's body in a single generalised formula. The loop invariant shall not contain unused variables as well as redundant cases. An invariant

shall not contain superfluous cases. Hence, invariants are challenging to derive automatically in a constructive way.

LR-Parser.

Parsing where \uparrow input tokens are processed from left to right, and rules of given corresponding \uparrow formal grammar are processed bottom-up.

Mapped Garbage Collection.

Regions of \uparrow dynamic memory are mapped and processed afterwards in parallel on the same principle as z-buffering works. Regions that often are altered are scattered along axes to the map. Closer regions are garbage collected depending on the chosen strategy.

Memoization.

Caching \uparrow predicate calls and functions. In Prolog, it is called "tabling".

Memory Cell Overlapping / Sharing.

When some memory cell is entirely or \uparrow partially interpreted differently, e.g. by varying \uparrow pointers (types), or memory alignment, byte and bit-ordering, or programming language constructs, like "union" in C-dialects.

Memory Leak.

\uparrow Memory cells in \uparrow dynamic memory unreachable from \uparrow stack variables.

Memory Location.

Memory addresses replacements of program variables in \uparrow stack and \uparrow heap.

Memory Model (by Burstall).

\uparrow Simple heaps in SL have the form: $location \mapsto address$.

Memory Model (by Reynolds).

\uparrow Simple heaps in SL have the form: $location \mapsto value$.

(Memory/Heap) Pointer.

Pointer is of pointer type, where its memory cell contains an address to some content in virtual memory, which is then interpreted according to the pointer type from its declaration. Dereferencing a valid memory cell accesses the pointer's \uparrow content. Pointer may be of type \uparrow pointer of some further type.

Meta Scheme.

In contrast, to \uparrow fold/ \uparrow unfold, it is a universal schema in proofs similar to, e.g. \uparrow analogy, \uparrow induction, \uparrow abduction.

Method Signature.

Consists of \uparrow method name, if within a class then a prefixed \uparrow class name, as well as all types of formal parameters (maybe further distinguished in incoming and outgoing parameters).

Model Checking.

Model described by (in-)equalities for a given \uparrow (formal) theory. \uparrow Calculation state is described by a formula that needs to be checked by a \uparrow (SMT) solver to be constructed.

Monoid.

A discrete structure with one \uparrow total operation for which closure, associativity, neutrality are obeyed. Half-group is a synonym.

Natural Deduction.

Logical proving scheme based on assumptions and consequences or its negations. The structure of a naturally

deducted proof is very close to \uparrow Hoare calculi in general. An alternative major to natural deduction is Robinson's resolution method.

Non-Interleaving Heap Cells.

A \uparrow heap graph cell is non-interleaving between two \uparrow heap graphs, if both graphs do not share a common vertex at the same time.

O-Term (in Prolog).

A Prolog term that can, but not necessarily has to, be ground. Applied to a subgoal, it is expected the term is bound afterwards.

Object Calculi.

(1st kind) class-based calculus after Abadi-Leino using \uparrow classes, very close to classes in Java and C++, or (2nd kind) object-based calculus after Abadi-Cardelli, where everything is an object, a record of methods and fields with possibly nested further objects all without classes, very close to objects in Baby Modula 3 and a few less known mostly experimental scripting languages from Cardelli.

Object Field.

A memory location for a given \uparrow class field will be assigned a memory address during runtime belonging to a surrounding object memory layout. A field maybe added, inserted and deleted statically by \uparrow class inheritance or dynamically by \uparrow code introspection.

Object Invariant.

An invariant \uparrow assertion (cf. \uparrow loop invariant), which shall always hold and regularly be checked during the lifespan of some \uparrow object instance, particularly before and after construction, destruction, arbitrary \uparrow method calls and \uparrow field modifications.

Object Life-Cycle.

The period between object creation until destruction.

Object Method.

A procedure within the scope of some \uparrow class, which may refer to the class \uparrow fields as well as to the \uparrow this keyword. In contrast to fields, in classic \uparrow object calculi without \uparrow introspecting code may not be modified during runtime.

(Full) Object Specification.

Includes \uparrow object invariant, \uparrow pre-condition, \uparrow post-condition of all methods and all inner specifications inside methods.

Object Type.

\uparrow class

Partial Correctness.

Correctness without the claim to terminate.

Partial Heap Specification.

\uparrow Heap specification containing special operands, some anonymous placeholder which is existentially quantified for each occurrence. It is used to summarise unspecified heap fragments.

Partial(-ly defined) Hoare Triple.

If execution of some program statement for some \uparrow Hoare triple not necessarily terminates, then its \uparrow post-condition is undetermined.

Peano Axioms.

Given the operations "+", ".", and some \uparrow ordering on (in

the common case some lifted and equivalent to) a set of natural numbers, on which popular axioms of addition are established. For example, equality can be defined as equality of the set's first element and (inductively continued) equality of the following numbers (cf. with \uparrow Church's arithmetics).

Pointer to a Pointer.

\uparrow Pointer whose content is pointer again.

Pointer Rotation.

Approach based on tiny pointer operation within the programming language to be reasoned, e.g. clock-wise permutation. Rotations seem very easy, but in fact, may become very difficult to maintain and apply due correctly to numerous not apparent exclusions.

Points-To Heap Model.

A \uparrow dynamic memory model consists of base \uparrow assertions of kind: "*location* \times *content*".

Polymorphism.

A dynamic effect when a \uparrow class method may on runtime be different from the declared class. In contrast to polymorphism by subclassing in C++ and Java (so-called "ad-hoc"), some \uparrow functional programming languages provide "real polymorphism" evaluating symbols and all-quantified variables.

Post-Condition.

The third component Q of a \uparrow Hoare triple.

Pre-Condition.

The first component P of some \uparrow Hoare triple.

Predicate Cut (in Prolog).

A reserved built-in \uparrow subgoal "!" with zero arguments for cutting the \uparrow proof search on further alternatives. If the cut is known to be safe applied to some algorithm, it is called "green cut", otherwise, called "red cut".

Predicate Fold.

A predicate contains a predicate head with a name and term arguments on the left-hand side, and a predicate's body containing its definition refers to arguments from the left-hand side. Fold describes within some \uparrow assertion a predicate's body can be unified and replaced by its predicate head. If the substitution is reversed, it is a \uparrow predicate unfold. It is called fold since a predicate's body often is longer than its head, and therefore the assertion after a fold is shorter than before.

Predicate Invertibility.

If a Prolog predicate is known to be sound and complete for a certain term arguments placement, then that predicate is invertible when term arguments are flipped, s.t. input term become output, and the predicate will still be terminated. As input parameters may commute and output parameters too, permutations of flipped arguments also need to be considered. An example is ISO-Prolog compliant predicate append/3.

Predicate Unfold.

Unfold describes within some \uparrow assertion its predicate body replaces a matching predicate's head. It is the opposite of \uparrow predicate fold.

Primitive Recursion.
 Recursion with apriori bound number of iterations.
 (Principle of) Non-Repetitiveness.
 Simplification principle after which parts of some \uparrow heap may not spatially re-occur.
 Post's Correspondence Problem.
 Given two \uparrow formal grammars. The question of whether the two \uparrow formal languages generated by both are in general undecidable.
 (Programming) Paradigm.
 E.g. \uparrow declarative, imperative, multi-paradigm [81].
 Programming By Proving.
 (Philosophical) concept stating programming can be done by proving.
 (Proof) Abduction.
 Logical reasoning (proof) \uparrow meta-scheme based on \uparrow facts and implications. It guesses from a conclusion a potentially "missing bit" in the antecedent.
 Proof Abstraction.
 Parameterising some proof in order to reuse it or parts of it w.r.t. planning.
 Proof Analogy.
 During \uparrow theorem proving a \uparrow meta-scheme that \uparrow abstracts from already accomplished proofs and tries to apply by tiny modification to a current problem that seems similar to a previously accomplished.
 Proof Coherence.
 If a proof fibres according to proper proof rules, application and each fibre succeeds with the same result, then the proof rules are coherent.
 Proof Deduction.
 As logical reasoning (proof) \uparrow meta-schema as \uparrow proof abduction. It implies from two antecedents a conclusion.
 Proof Fact.
 A logical fact is believed to be true within some discourse, particularly an axiomatic rules system.
 Proof Heuristics.
 An assumption made, often due to too high practical complexity, eases and approximates some (sub-)optimal solution, which is often sufficient, however, but not guaranteed. In terms of formal proofs, heuristics (as one form of a \uparrow meta-scheme) do not accomplish proofs, but they may occasionally be used to transform a non-matching \uparrow (calculation) state into a matching.
 Proof Induction.
 As logical reasoning (proof) \uparrow meta-schema as a \uparrow proof deduction. Induction is based on a generalised, often not directly provable, but not contradicting, assumption that is considered a true \uparrow assertion, unless found differently, and used in a proof.
 Proof Lemma.
 An auxiliary \uparrow theorem without a separate unique meaning often used as an intermediate step in a proof. Lemmas may also be \uparrow folded or \uparrow unfolded.
 Proof Refutation.
 A possible negative result of a theorem- \uparrow proof indicating

it is not valid. Often some \uparrow counter-example as a single case explains why a theorem does not hold.
 Proof Search.
 The search for some positive proof for a given \uparrow theorem. \uparrow (Proof) tactics may be applied sometimes in order to speed up the search.
 (Proof) Tactics.
 A \uparrow heuristics of a template sequence of predefined fixed verification steps applied to assist during a \uparrow proof search.
 (Proof) Theorem.
 An \uparrow assertion that can be proven using a selected set of axioms and rules.
 Proof Theory.
 A set of axioms and sets for some considered discourse in which proofs are taken out.
 Proof Tree.
 The structure of some proof. In this work, we are only interested in Hoare calculi. Any proof tree is a tree whose vertices represent a \uparrow verification state. Edges are transitions labelled with the rule applied. All leaves in a prove tree are the result of axioms.
 Prolog Query.
 One or more \uparrow subgoals in Prolog to defined \uparrow Prolog rules separated by a comma and ending with a period. A query may yield zero or more solutions, depending on how many solutions are derivable for the given rules.
 Prolog Rules.
 See \uparrow Prolog predicates
 Prolog Predicate.
 A Prolog notation for predicates in first-order predicate logic, which consist of head and body. It is often called Horn-rules. It consists of \uparrow ingoing and \uparrow outgoing terms as argument lists in the predicate head. The body has zero or more subgoals that may refer to the predicate's arguments. If a predicate has zero subgoals, the Prolog predicate may also be called \uparrow fact.
 Prolog Subgoal.
 See \uparrow Prolog predicate.
 Rapid Prototyping.
 A prototype whose only purpose is to document or reject if doable in practice or not. Its main purpose is to get at least some exploratory estimation. Often suffers from hard limitations and countless errors.
 (Recursive/Non-Recursive Term) Occurs-Check.
 Prolog does not check by default if a term contains self-applications, e.g. $X=s(1,s(2,X))$.
 Resolution Method (by Robinson).
 In contrast to \uparrow natural deduction, resolution proves a theorem by showing the falsified theorem refutes. The given theorem has to be in conjunctive normal-form. After negation, a disjunctive normal-form is obtained where each disjunct/clause has to be proven false separately. A modified resolution method is Prolog's default reasoning scheme over predicates.
 Safe Pointer Operations.
 See \uparrow pointer rotation. Safe rotations are to distinguish

from operations with flaky and hard to predict operational behaviour.

Scope.

A program slice in which \uparrow stack-local variables are pushed to \uparrow stack on entry and popped on exit.

Self-Applicable Terms.

See \uparrow recursive terms

Self-Inverse Operation.

Operation, when being applied twice, returns the origin argument. Often \uparrow totality helps in showing generalised properties.

Semantic Function.

Defined functions for denoting program properties.

Semi-Automated Theorem Proving.

A proof either terminates successfully or stops unfinished, requiring further input, which might either be missing lemmas, equalities (see \uparrow proof theory). If nothing is missing and the proof still does not finish, then the considered theorem just cannot be proven.

Separation Of Concerns.

Separation of roles and interfaces (e.g. into objects and procedures) by responsibilities.

Separation Logic.

See \uparrow points-to heap model.

Simple Heap (=Simplex).

A simple assertion of form: $a \mapsto b$ in Reynolds' \uparrow memory model. Others are \uparrow complex heap, \uparrow abstract predicate.

ShapeAnalysis.

A \uparrow dynamic memory model in which elements are described by its (geometric) shape.

SMT-solver.

An automated solution to a formula of (in-)equalities.

Spatial Heap Operator.

Describes a binary operator expressing how two heaps are spatial to each other in \uparrow heap address space.

SSA.

\uparrow IR for data dependency, which for each local variable strictly has one defining value and several references per basic block.

Stack Allocation.

See \uparrow stack

Stack.

Organised memory segment allocated by the OS. It accommodates all \uparrow local variables. When a procedure is called, local variables are put to the actual reserved \uparrow stack window and freed when leaving.

Stack(-ed) Variable.

See \uparrow stack

Stack Unwinding.

Restoring \uparrow stack required by exception-handling in the event of failure.

Static Analysis.

A code analysis performed without running a program.

Static Variable.

Allocation happens once on process creation. Deallocation happens once on process release.

Strong Post-condition.

Strengthening some \uparrow assertion Q' of post-condition Q restricts the latter. So, $Q \Rightarrow Q'$ implies $Q' \subseteq Q$.

Structural Rules.

In contrast to \uparrow subtraction rules, are rules focused on the second component of \uparrow Hoare triples.

Struct-Alignment.

Padding fields in contiguous blocks for structs or \uparrow objects in order to achieve higher access throughput.

Subtraction Rules.

Once applied, rules reduce the remaining proof for a given \uparrow theorem (cf. with \uparrow structural rules).

Subtyping.

A class subtype is any inherited \uparrow class according to its class hierarchy.

Symptom (of an Error).

See \uparrow erroneous code localization.

Synthesized Attribute.

An attribute in an \uparrow attributed grammar is passed from the called rule up to the calling rule. See also \uparrow inherited attribute.

Tableaux Method (by Beth).

Logical reasoning where all derivations may only be applied that are encoded in a given table.

Token.

An atomic unit resulting from lexical analysis. For example, the assignment symbol $:=$.

Total Function.

A function that accepts any element from a well-defined domain and terminates for each.

Trieber's Stack.

A \uparrow (execution) stack model supported by \uparrow separation logic in multi-threading environments.

Type Checking.

Checks for a given program all assignments and expressions are valid w.r.t. applied variable types according to its declaration.

Undermined Specification.

A specification containing unbound symbols, an abstract specification.

Variable Mode.

A variable's mode depends on its life-span and its scope of visibility. Modi might be \uparrow automated, \uparrow static, \uparrow dynamic, \uparrow global, register, thread-local or others.

Warren's Abstract Machine.

In addition to traditional operational semantics WAM defines an abstract machine based on an extended execution stack, where elements are (Prolog) terms with forward and backward references allowed towards (sub-)terms across several stack windows. Unification makes sure linked terms are interpreted as parameters by reference.

Weak Pre-condition.

Weakening some pre-condition P yields P' , s.t. P' is a generalisation of P , $P' \Rightarrow P$ implies $P \subseteq P'$.

References

- [1] Object Management Group (OMG). Object Constraint Language, version 2.2. Object Management Group (OMG). Feb. 2010. <http://www.omg.org/spec/OCL/2.2>.
- [2] Martín Abadi. Baby Modula-3 and a Theory of Object. Technical Report SRC-RR-95. Systems Research Center, Digital Equipment Corporation, 1993. <ftp://gatekeeper.research.compaq.com/pub/DEC/SRC/research-reports/abstracts/src-rr-095.html>
- [3] Martín Abadi, Luca Cardelli. A Theory of Objects. Secaucus, New Jersey, USA: Springer, 1996, 396p. ISBN 0387947752.
- [4] Martín Abadi, K. Rustan M. Leino. A Logic of Object-Oriented Programs. In: Proc. of the 7th Intl. Joint Conf. CAAP/FASE on Theory and Practice of Software Development. Springer, 1997, p.682–696.
- [5] Serge Abiteboul et.al. EDOS: Environment for the Development and Distribution of Open Source Software. In: 1st Intl. Conf. on Open Source Systems. 2005.
- [6] Samson Abramsky, Achim Jung. Domain Theory. In: Handbook of Logic in Computer Science. Clarendon Press, Oxford University Press, 1994, 168p.
- [7] Jean-Raymond Abrial. The B-book – Assigning Programs to Meanings. Cambridge University Press, 2005, (excerpt from 1–34), 816p. ISBN 978-0-521-02175-3.
- [8] Johnathan Afek, Adi Sharabani. Dangling Pointers – Smashing the Pointer for Fun and Profit (Whitepaper from Watchfire Corp.) online. 2007. <https://www.blackhat.com/presentations/bh-usa-07/Afek/Whitepaper/bh-usa-07-afek-WP.pdf>
- [9] Lloyd Allison. A Practical Introduction to Denotational Semantics. Cambridge University Press, 1989, 131p. ISBN 0-521-30689-2.
- [10] Pierre America, Jan J. M. M. Rutten. Elements of Generalized Ultrametric Domain Theory. In: Journal of Computer and System Sciences, Theoretical Computer Science 39 (1989), p.343–375. DOI 10.1016/S0304-3975(96)80711-0.
- [11] Alexandr Andoni, Krzysztof Onak. Approximating Edit Distance in Near-Linear Time. In: SIAM Journal on Computing 41.6 (2012), p.1635–1648.
- [12] Andrew W. Appel. Garbage Collection can be Faster than Stack Allocation. In: Information Processing Letters, Elsevier North-Holland 25.4 (1987), p.275–279. DOI 10.1016/0020-0190(87)90175-X.
- [13] Andrew W. Appel, Robert Dockins, Xavier Leroy. A list-machine benchmark for mechanized metatheory. In: Journal of Automated Reasoning 49.3 (2012), p.453–491. DOI 10.1007/s10817-011-9226-1.
- [14] Andrew W. Appel, Xavier Leroy. A List-machine Benchmark for Mechanized Metatheory: (Extended Abstract). In: Electronic Notes in Theoretical Computer Science, Elsevier 174.5 (2007), p.95–108. DOI 10.1016/j.entcs.2007.01.020.
- [15] Krzysztof R. Apt. Ten Years of Hoare’s Logic: A Survey - Part I. In: ACM Transactions on Programming Languages and Systems 3.4 (1981), p.431–483. ISSN 0164-0925. DOI 10.1145/357146.357150.
- [16] Krzysztof R. Apt, Ernst-Rüdiger Olderog. Verification of Sequential and Concurrent Programs. In: SIAM Review 35.2 (1993), p.330–331.
- [17] Uwe Assmann. Trustworthy Instantiation of Frameworks. In: Architecting Systems with Trustworthy Components. Vol.3938/2006. Springer, 2006, p.152–168. ISBN 978-3-540-35800-8. DOI 10.1007/11786160.
- [18] Mikhail J. Atallah, Susan Fox, eds. Algorithms and Theory of Computation Handbook. 1st. Boca Raton, Florida, USA: CRC Press, Oct. 1999, 1312p. ISBN 0849326494.
- [19] Franz Baader, Tobias Nipkow. Term Rewriting and All That. New York, USA: Cambridge University Press, 1998, 297p. ISBN 0-521-45520-0.
- [20] Greg J. Badros. JavaML: A Markup Language for Java Source Code. In: Proc. of the 9th Intl. World Wide Web conf. on Computer Networks, Intl. Journal of Computer and Telecommunications Networking. 2000, p.13–15.
- [21] Anindya Banerjee, David A. Naumann, Stan Rosenberg. Regional Logic for Local Reasoning about Global Invariants. In: European conf. on Object-Oriented Programming, eds. J. Vitek. Vol.5142. Lecture Notes in Computer Science. Springer, Berlin Heidelberg, 2008, p.387–411. DOI 10.1007/978-3-540-70592-5_17.
- [22] Henk P. Barendregt. Handbook of Logic in Computer Science. In: eds. Samson Abramsky, Dov M. Gabbay, Thomas S. E. Maibaum. New York, USA: Oxford University Press, 1992. Chapter on Lambda Calculi with Types, p.117–309. ISBN 0-19-853761-1. DOI 10.1017/CBO9781139032636.
- [23] Michael Barnett, et.al. Verification of Object-Oriented Programs with Invariants. In: Journal of Object Technology 3.6 (2004), p.27–56.
- [24] Kent Beck. jUnit Testing Framework. <http://junit.org>.
- [25] Hans Bekić. Definable Operation in General Algebras, and the Theory of Automata and Flowcharts. In: Programming Languages and Their Definition. eds. Cliff B. Jones. Vol.177. Lecture Notes in Computer Science. Springer, 1984.
- [26] Josh Berdine, Cristiano Calcagno, Peter W. O’Hearn. Smallfoot: Modular Automatic Assertion Checking with Separation Logic. In: Intl. Symp. on Formal Methods for Components and Objects. 2005, p.115–137. DOI 10.1007/11804192_6.
- [27] Josh Berdine, Cristiano Calcagno, Peter W. O’Hearn. Symbolic Execution with Separation Logic. In: 3rd Asian Symp. on Programming Languages and Systems. Tsukuba, Japan, Nov. 2005, p.52–68. DOI 10.1007/11575467_5.
- [28] Joachim van den Berg, Bart Jacobs. The LOOP Compiler for Java and JML. In: Proc. of the 7th Intl. Conf. on Tools and Algorithms for the Construction and Analysis of Systems. 2001, p.299–312.
- [29] Mark de Berg, Computational Geometry: Algorithms and Applications. 3rd. Santa Clara, California, USA: Springer Berlin, Heidelberg, 2008, 386p. ISBN 3540779736.
- [30] Jan A. Bergstra, Jan Heering, Paul Klint. Module Algebra. In: Journal of the ACM 37.2 (1990), p.335–372. DOI 10.1145/77600.77621.
- [31] Yves Bertot, Benjamin Gregoire, Xavier Leroy. A Structured Approach to Proving Compiler Optimizations based on Dataflow Analysis. In: Types for Proofs and Programs, Workshop TYPES 2004. Vol.3839. Lecture Notes in Computer Science. Springer, 2006, p.66–81.
- [32] Yves Bertot, Interactive Theorem Proving and Program Development – Coq’Art: The Calculus of Inductive Constructions. eds. Brauer, Rozenberg, Salomaa. Texts in theoretical computer science. Berlin, New York: Springer Publishing, Inc., 2004, p.472. ISBN 3642058809.
- [33] Al Bessey, A Few Billion Lines of Code Later: using Static Analysis to find Bugs in the Real World. In: Communications of the ACM 53.2 (Feb. 2010), p.66–75. DOI 10.1145/1646353.1646374.
- [34] Richard Bird, Oege de Moor. Algebra of Programming. Upper Saddle River, New-Jersey, USA: Prentice-Hall, Inc., 1997, 312p. ISBN 0-13-507245-X.
- [35] Richard Bird, Philip Wadler. An Introduction to Functional Programming. Hertfordshire, England: Prentice Hall Intl. UK, 1988, 310p. ISBN 0-13-484189-1.
- [36] Lars Birkedal, Noah Torp-Smith, John C. Reynolds. Local Reasoning about a Copying Garbage Collector. In: ACM SIGPLAN-Notes 39.1 (2004), p.220–231. DOI 10.1145/982962.964020.
- [37] Lars Birkedal, Noah Torp-Smith, Hongseok Yang. Semantics of Separation-Logic Typing and Higher-order Frame Rules for Algol-like Languages. In: Logic in Computer Science 2.5 (2006). DOI 10.2168/LMCS-2(5:1)2006.
- [38] Lars Birkedal, Hongseok Yang. Relational Parametricity and Separation Logic. In: Foundations of Software Science and Computational Structures. 2007, p.93–107. DOI 10.1007/978-3-540-71389-0_8.
- [39] Lars Birkedal, A Simple Model of Separation Logic for Higher-Order Store. In: Intl. Colloquium on Automata, Languages and Programming. 2008, p.348–360. DOI 10.1007/978-3-540-70583-3_29.

- [40] Stephen M. Blackburn, Perry Cheng, Kathryn S. McKinley. Myths and Realities: The Performance Impact of Garbage Collection. In: Proc. of the Joint Intl. Conf. on Measurement and Modeling of Computer Systems. SIGMETRICS'04. New York, USA: ACM, 2004, p.25–36. ISBN 1-58113-873-3. DOI 10.1145/1005686.1005693.
- [41] Sandrine Blazy, Zaynah Dargaye, Xavier Leroy. Formal Verification of a C Compiler Front-End. In: Intl. Symp. on Formal Methods. Vol.4085. Lecture Notes in Computer Science. Springer, Aug. 2006, p.460–475.
- [42] Sandrine Blazy, Xavier Leroy. Formal Verification of a Memory Model for C-like Imperative Languages. In: Intl. Conf. on Formal Engineering Methods. Vol.3785. Lecture Notes in Computer Science. Springer, 2005, p.280–299.
- [43] Sandrine Blazy, Xavier Leroy. Mechanized Semantics for the Clight Subset of the C Language. In: Journal of Automated Reasoning 43.3 (2009), p.263–288. DOI 10.1007/s10817-009-9148-3.
- [44] Richard Bornat. Proving Pointer Programs in Hoare Logic. In: Proc. of the 5th Intl. Conf. on Mathematics of Program Construction. eds. Roland Backhouse, José Nuno Oliveira. Vol.1. Lecture Notes in Computer Science, Springer 8. Ponte de Lima, Portugal, 2000, p.102–126. DOI 10.1007/10722010_8.
- [45] Marius Bozga, Radu Iosif, Swann Perarnau. Quantitative Separation Logic and Programs with Lists. In: Intl. Joint conf. on Automated Reasoning. 2008, p.34–49. DOI 10.1007/978-3-540-71070-7_4.
- [46] Ivan Bratko. Prolog: Programming for Artificial Intelligence. 3rd. Boston, Massachusetts, USA: Addison-Wesley Longman Publishing Co., Inc., 2001, 673p. ISBN 0-201-40375-7.
- [47] Luitzen Egbertus Jan Brouwer. Brouwer's Intuitionistic Logic. online free encyclopedia from May 2010. <http://plato.stanford.edu/entries/intuitionism>.
- [48] Kim B. Bruce. Foundations of Object-oriented Languages: Types and Semantics. Cambridge, Massachusetts, USA: MIT Press, 2002, 384p. ISBN 0-262-02523-X.
- [49] Nicolaas Govert de Bruijn. Lambda Calculus Notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem. In: *Indagationes Mathematicae (Proceedings)* 75.5 (1972), p.381–392. ISSN 1385-7258. DOI 10.1016/1385-7258(72)90034-0.
- [50] Janusz A. Brzozowski. Derivatives of Regular Expressions. In: Journal of the ACM 11.4 (Oct. 1964), p.481–494. ISSN 0004-5411. DOI 10.1145/321239.321249.
- [51] Rodney M. Burstall. Some Techniques for Proving Correctness of Programs which Alter Data Structures. In: Machine Intelligence. eds. Bernard Meltzer, Donald Michie. Vol.7. Scotland: Edinburgh University Press, 1972, p.23–50.
- [52] Cristiano Calcagno, Simon Helsen, Peter Thiemann. Syntactic Type Soundness Results for the Region Calculus. In: Information and Computation 173 (2001), p.173–2. DOI 10.1006/inco.2001.3112.
- [53] Cristiano Calcagno, Peter O'Hearn, Richard Bornat. Program Logic and Equivalence in the Presence of Garbage Collection. In: Theoretical Computer Science, Foundations of Software Science and Computation Structures 298.3 (2003), p.557–581. ISSN 0304-3975. DOI 10.1016/S0304-3975(02)00868-X.
- [54] Cristiano Calcagno, Compositional Shape Analysis by means of Bi-abduction. In: Proc. of the 36th annual ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages 36 (2009), p.289–300. DOI 10.1145/1480881.1480917.
- [55] Luca Cardelli. Type Systems. In: The Computer Science and Engineering Handbook. eds. Allen B. Tucker. CRC Press, 1997, p.2208–2236.
- [56] Luca Cardelli, Martín Abadi. A Theory of Objects, Digital Equipment Corporation, invited workshop presentation in Sydney, Australia on 19th December 1997, 574 slides.
- [57] Rudolf Carnap. Logische Syntax der Sprache. 2nd. Vienna, Austria: Springer-Verlag, 1968, 274p. ISBN 978-3-662-23331-3.
- [58] Ramkrishna Chatterjee. Modular Data-flow Analysis of Statically Typed Object-Oriented Programming Languages. PhD thesis. . . . Rutgers University, Jan. 2000.
- [59] Yoonsik Cheon, Gary T. Leavens. A Thought on Specification Reflection. In: Proc. of the 8th World Multi-conf. on Systemics, Cybernetics and Informatics, Orlando, Florida, USA, Volume II, Computing Techniques (appeared on Dec 2003 as TR03-16 at Iowa State University). eds. N. Callaos, W. Lesso, B. Sanchez. Jul. 2004, p.485–490.
- [60] Sigmund Cherm, Radu Rugina. Maintaining Doubly-Linked List Invariants in Shape Analysis with Local Reasoning. In: Intl. Workshop on Verification, Model Checking and Abstract Interpretation. eds. Byron Cook, Andreas Podelski. Vol.4349. 2007, p.234–250. ISBN 978-3-540-69738-1. DOI 10.1007/978-3-540-69738-1_17.
- [61] John C. Cherniavsky. Simple Programs realize exactly Presburger formulas. In: SIAM Journal on Computing 5.4 (1976), p.666–677.
- [62] Edmund Melson Jr. Clarke. Programming Language Constructs for Which It Is Impossible To Obtain Good Hoare Axiom Systems. In: Journal of the ACM, New York, USA 26.1 (Feb. 1979), p.129–147. DOI 10.1145/322108.322121.
- [63] Edmund Melson Jr. Clarke, Orna Grumberg, Doron A. Peled. Model Checking. Cambridge, MA, USA: MIT Press, 1999, 330p. ISBN 0-262-03270-8.
- [64] Maurice Clint. Program Proving: Coroutines. In: Acta Informatica 2 (1973), p.50–63. DOI 10.1007/BF00571463.
- [65] Avra Cohn. The Equivalence of two Semantic Definitions — A Case Study in LCF. In: SIAM Journal on Computing 12.2 (1983), p.267–285.
- [66] H. Comon et.al, Tree Automata Techniques and Applications, 2007. <http://www.grappa.univ-lille3.fr/tata>.
- [67] Stephen Cook. Soundness and Completeness of an Axiom System for Program Verification. In: SIAM Journal on Computing 7.1 (1978), p.70–90.
- [68] Stephen A. Cook. The Complexity of Theorem-Proving Procedures. In: Proc. of the 3rd annual ACM Symp. on Theory of Computing. 1971, p.151–158. DOI 10.1145/800157.805047.
- [69] David C. Cooper. Theorem Proving in Arithmetic without Multiplication. In: Machine Intelligence 7. eds. Bernard Meltzer, Donald Michie. Edinburgh University Press, 1972, p.91–100. ISBN 0-85224-234-4.
- [70] Keith D. Cooper, Ken Kennedy. Fast Interprocedural Alias Analysis. In: Proc. of the 16th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. ACM, New York, USA, Jan. 1989, p.49–59. DOI 10.1145/75277.75282.
- [71] Jonathan Corbet, Alessandro Rubini, Greg Kroah-Hartman. Linux Device Drivers. 3rd. O'Reilly Media, Inc., 2005, 597p. ISBN 9780596005900.
- [72] Thomas H. Cormen, Introduction to Algorithms. 3rd. MIT Press, Jul. 2009, 1292p. ISBN 0262033844.
- [73] Patrick Cousot, Radhia Cousot. Abstract Interpretation and Application to Logic Programs. In: Journal of Logic Programming 13.2&3 (1992), p.103–179.
- [74] Patrick Cousot, Radhia Cousot. Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. In: Proc. of the 4th ACM SIGACT-SIGPLAN symp. on Principles of Programming Languages. eds. ACM. Jan. 1977, p.238–252.
- [75] John Criswell, LLVM group. SAFECode project, University of Illinois at Urbana-Champaign, USA. <http://llvm.org>.
- [76] Ron Cytron, Efficiently Computing Static Single Assignment Form and the Control Dependence Graph. In: ACM Transactions on Programming Languages and Systems 13.4 (Oct. 1991), p.451–490. ISSN 0164-0925. DOI 10.1145/115372.115320.
- [77] Desmond F. D'Souza, Alan Cameron Wills. Objects, Components, and Frameworks with UML: The Catalysis Approach. Object Technology Series. Addison-Wesley, 1998, 816p. ISBN 9780201310122.
- [78] Zaynah Dargaye, Xavier Leroy. Mechanized Verification of CPS transformations. In: 14th Intl. Conf on Logic for Programming, Artificial Intelligence and Reasoning. Vol.4790. Lecture Notes in Artificial Intelligence. Springer, 2007, p.211–225.
- [79] Martin D. Davis, Ron Sigal, Elaine J. Weyuker. Computability, Complexity, and Languages: Fundamentals of Theoretical Computer Science. 2nd. San Diego, California, USA: Academic

- Press Professional, Morgan Kaufman Inc., 1994, 609p. ISBN 0-12-206382-1.
- [80] Anatoli Degtyarev, Andrei Voronkov. The Inverse Method. In: Handbook of Automated Reasoning (in 2 volumes). 2001, p.179–272.
 - [81] Enrico Denti, Andrea Omicini, Alessandro Ricci. Multi-paradigm Java-Prolog Integration in tuProlog. In: Science of Computer Programming, Elsevier Science 57.2 (Aug. 2005), p.217–250. ISSN 0167-6423. DOI 10.1016/j.scico.2005.02.001.
 - [82] Enrico Denti, Andrea Omicini, Alessandro Ricci. tuProlog: A Light-weight Prolog for Internet Applications and Infrastructures. In: Practical Aspects of Declarative Languages. eds. Ramakrishnan. Vol.1990. Lecture Notes in Computer Science. Springer Berlin, Heidelberg, 2001, p.184–198. ISBN 978-3-540-41768-2. DOI 10.1007/3-540-45241-9_13.
 - [83] Daniel Diaz, Salvador Abreu, Philippe Codognet. On the Implementation of GNU Prolog. In: Theory and Practice of Logic Programming 12.1-2 (2012), p.253–282. DOI 10.1017/S1471068411000470.
 - [84] Christophe de Dinechin. C++ Exception Handling for IA64. In: edition 8. Oct. 2000, p.72–79. <http://www.usenix.org/publications/library/proceedings/osdi-2000/wiess2000/dinechin.html>
 - [85] Dino Distefano, Peter W. O’Hearn, Hongseok Yang. A Local Shape Analysis Based on Separation Logic. In: Proc. of the 12th intl. conf. on Tools and Algorithms for the Construction and Analysis of Systems. Eds. Heidelberg Springer Berlin. Mar. 2006, p.287–302. DOI 10.1007/11691372_19.
 - [86] Dino Distefano, Matthew J. Parkinson. jStar: Towards Practical Verification for Java. In: Object-Oriented Programming, Systems, Languages and Applications. 2008, p.213–226. DOI 10.1145/1449764.1449782.
 - [87] Mike Dodds. Graph Transformations and Pointer Structures. PhD thesis. . . . University of York, England, 2008, 277p.
 - [88] Damien Doligez, Xavier Leroy. A Concurrent, Generational Garbage Collector for a Multithreaded Implementation of ML. In: 20th symp. on Principles of Programming Languages. ACM Press, 1993, p.113–123.
 - [89] Kosta Dosen, Substructural Logics. eds. Peter Schroeder-Heister, Kosta Dosen. Clarendon, Oxford University Press, 1993, 400p. ISBN 0198537778.
 - [90] Hartmut Ehrig, Barry K. Rosen. The Mathematics of Record Handling. In: SIAM Journal on Computing 9.3 (1980), p.441–469. DOI 10.1137/0209034.
 - [91] ElectricFence Project. <http://perens.com/FreeSoftware>.
 - [92] Pär Emanuelsson, Ulf Nilsson. A Comparative Study of Industrial Static Analysis Tools. In: Electronic Notes in Theoretical Computer Science 217 (2008), p.5–21. DOI 10.1016/j.entcs.2008.06.039.
 - [93] Loe M. G. Feijs, Yuechen Qian. Component Algebra. In: Science of Computer Programming 42.2-3 (2002), p.173–228. DOI 10.1016/S0167-6423(01)00009-0.
 - [94] Bernd Fischer. Specification-Based Browsing of Software Component Libraries. In: Automated Software Engineering 7.2 (May 2000), p.179–200. DOI 10.1023/A: 1008766409590.
 - [95] Michael J. Fisher, Michael O. Rabin. Super-Exponential Complexity of Presburger Arithmetic. Technical Report no.889578. Cambridge, Massachusetts, USA: Massachusetts Institute of Technology, 1974, p.27–41.
 - [96] Cormac Flanagan. Extended Static Checking for Java. In: Proc. of the ACM SIGPLAN conf. on Programming Languages Design and Implementation. 2002, p.234–245.
 - [97] Robert W. Floyd. Assigning Meanings to Programs. In: Mathematical Aspects of Computer Science. Eds. T.R. Colburn, J.H. Fetzer, Rankin T.L. Vol.19. Proc. of symp. in Applied Mathematics. American Mathematical Society. 1967, p.19–32.
 - [98] Matthew Fluet, Greg Morrisett, Amal J. Ahmed. Linear Regions Are All You Need. In: European Symp. on Programming. 2006, p.7–21. DOI 10.1007/11693024_2.
 - [99] Ira R. Forman, Nate Forman. Java Reflection in Action (In Action series). Manning Publications, Oct. 2004, 273p. ISBN 1932394184.
 - [100] Free Software Foundation. GNU make, <https://www.gnu.org/software/make/>.
 - [101] Michael L. Fredman, Robert Endre Tarjan. Fibonacci Heaps and Their Uses in Improved Network Optimization Algorithms. In: Journal of the ACM 34.3 (Jul. 1987), p.596–615. ISSN 0004-5411. DOI 10.1145/28869.28874.
 - [102] Jean H. Gallier. Foundations of Automatic Theorem Proving. Harper & Row, Jun. 2003, 534p. ISBN 0-06-042225-4.
 - [103] Holger Gast. Lightweight Separation. In: Intl. Conf. on Theorem Proving in Higher Order Logics. 2008, p.199–214. DOI 10.1007/978-3-540-71067-7_18.
 - [104] Susan L. Gerhart. Proof Theory of Partial Correctness Verification Systems. In: SIAM Journal on Computing 5.3 (1976), p.355–377.
 - [105] Alain Giorgetti, Specifying Generic Java programs: Two Case Studies. In: Proc. of the of the 10th Workshop on Language Descriptions, Tools and Applications, LDTA/E-TAPS 2010, Paphos, Cyprus, Mar. 28-29, 2010. p.1–8. DOI 10.1145/1868281.1868289.
 - [106] Fausto Giunchiglia, Toby Walsh. Abstract Theorem Proving: Mapping Back (unpublished). 1989.
 - [107] John B. Goodenough. Exception Handling: Issues and a Proposed Notation. In: 1975, p.683–696.
 - [108] Alexey Gotsman, Josh Berdine, Byron Cook. Interprocedural Shape Analysis with Separated Heap Abstractions. In: Intl. Static Analysis Symp. Springer, 2006.
 - [109] Dan Grossman, Region-Based Memory Management in Cyclone. In: Journal of Programming Language Design and Implementation. 2002, p.282–293. DOI 10.1145/512529.512563.
 - [110] Dick Grune, Criel J. H. Jacobs. Parsing Techniques: A Practical Guide. Upper Saddle River, New Jersey, USA: Ellis Horwood Publishing, 1990, 200p. ISBN 0-13-651431-6.
 - [111] Carl A. Gunter, John C. (eds.) Mitchell. Theoretical Aspects of Object-Oriented Programming — Types, Semantics, and Language Design. In: MIT Press, 1994. ISBN 026207155X.
 - [112] Maurice H. Hälstead. Elements of Software Science. New York, USA: Elsevier Science, 1977. ISBN 0444002057.
 - [113] Michael Hind. Pointer Analysis: Haven’t We Solved This Problem Yet? In: Proc. of the ACM SIGPLAN-SIGSOFT workshop on Program Analysis for Software Tools and Engineering. eds. USA IBM Watson Research Center. ACM, Jun. 2001, p.54–61. ISBN 1-58113-413-4. DOI 10.1145/379605.379665.
 - [114] Michael Hind, Anthony Pioli. Evaluating The Effectiveness of Pointer Alias Analyses. In: Science of Computer Programming. 1999, p.31–55. DOI 10.1016/S0167-6423(00)00014-9.
 - [115] Roger Hindley. The Principal Type-Scheme of an Object in Combinatory Logic. In: Transactions of the American Mathematical Society 146 (Dec. 1969), p.29–60. DOI 10.2307/1995158.
 - [116] Charles A. R. Hoare. An Axiomatic Basis for Computer Programming. In: Communications of the ACM 12.10 (Oct. 1969), p.576–580. ISSN 0001-0782. DOI 10.1145/363235.363259.
 - [117] Kohei Honda, Nobuko Yoshida, Martin Berger. An Observationally Complete Program Logic for Imperative Higher-Order Functions. In: Logic in Computer Science. 2005, p.270–279. DOI 10.1109/LICS.2005.5.
 - [118] Susan Horwitz, Phil Pfeiffer, Thomas Reps. Dependence Analysis for Pointer Variables. In: Proc. of the ACM SIGPLAN Conf. on Programming Language Design and Implementation. Portland, Oregon, USA: ACM, Jul. 1989, p.28–40. ISBN 0-89791-306-X. DOI 10.1145/73141.74821.
 - [119] Xia-Yu Hu, Robert Haas. The Fundamental Limit of Flash Random Write Performance: Understanding, Analysis and Performance Modelling. Technical Report no.99781. IBM Research Zürich, Switzerland, Mar. 2010.
 - [120] Marieke Huisman, Clément Hurlin. The Stability Problem for Verification of Concurrent Object-Oriented Programs. In: Electronic Notes in Theoretic Computer Science (2007).
 - [121] Clément Hurlin. Specification and Verification of Multithreaded Object-Oriented Programs with Separation Logic. PhD thesis . . . Université Nice – Sophia Antipolis, France, Sep. 2009, 207p.
 - [122] Graham Hutton. Fold and Unfold for Program Semantics. In: Proc. of the 3rd ACM SIGPLAN Intl. Conf. on Functional Programming. Baltimore, Maryland, USA: ACM Press, 1998, p.280–288.

- [123] Intel Inc. Intel 64 and IA-32 Architectures, Software Developer's Manual, Volume 3A: System Programming Guide, Part 1 (online). Oct. 2011.
- [124] Bart Jacobs, et al. VeriFast: A Powerful, Sound, Predictable, Fast Verifier for C and Java. In: Proc. of the 3rd Intl. Conf. on NASA Formal Methods. Pasadena, California, USA: Springer, Berlin Heidelberg, Apr. 2011, p.41–55. ISBN 978-3-642-20397-8.
- [125] Patricia Johann, Eelco Visser. Strategies for Fusing Logic and Control via Local, Application-Specific Transformations. Technical Report no.UU-CS-2003-050. Institute of Information, Computing Sciences, Utrecht University, 2003. DOI 10.1.1.10.8859.
- [126] Neil D. Jones, Steven S. Muchnick. Even Simple Programs are Hard to Analyze. In: Proc. of 2nd ACM SIGACT-SIGPLAN symp. on Principles of Programming Languages. 1975, p.106–118. DOI 10.1145/512976.512988.
- [127] Richard Jones, Antony Hosking, Eliot Moss. The Garbage Collection Handbook: The Art of Automatic Memory Management. 1st. Chapman & Hall/CRC, 2011, 481p. ISBN 1420082795.
- [128] Richard Jones, Sun Microsystems Inc. Memory Management in the Java HotSpot Virtual Machine. Technical Report Apr. 2006.
<http://www.oracle.com/technetwork/articles/java/index-jsp-140228.html>.
- [129] Jacques-Henri Jourdan, Francois Pottier, Xavier Leroy. Validating LR(1) Parsers. In: Programming Languages and Systems – 21st European symp. on Programming, ESOP 2012. Vol.7211. Lecture Notes in Computer Science. Springer, 2012, p.397–416. DOI 10.1007/978-3-642-28869-2_20.
- [130] Michel Kaempf. Smashing The Heap For Fun And Profit, Jul. 2006, version from 26.09.2015.
[https://web.archive.org/web/20060713194734, http://doc.bughunter.net/buffer-overflow/heap-corruption.html](https://web.archive.org/web/20060713194734/http://doc.bughunter.net/buffer-overflow/heap-corruption.html).
- [131] Laura Kallmeyer. Parsing Beyond Context-Free Grammars. eds. Dov M. Gabbay, Jörg Siekmann. Cognitive Technologies. Springer Heidelberg, 2010, 246p. ISBN 978-3-642-14845-3.
- [132] Shmuel Katz, Zohar Manna. A Heuristic Approach to Program Verification. In: Proc. of the 3rd intl. joint Conf. on Artificial Intelligence. 1973, p.500–512.
- [133] Matt Kaufmann, Panagiotis Manolios, Strother Moore, (eds.) Computer-Aided Reasoning: ACL2 Case Studies, Applicative Common LISP. 2nd. Kluwer Academic Publishers, 2008, 285p. ISBN 0-7923-7849-0.
- [134] Matt Kaufmann, J. Strother Moore. Some Key Research Problems in Automated Theorem Proving for HW/SW-Verification. In: Revista de la Real Academia de Ciencias Exactas, Serie A Matemáticas 98.1 (2004), p.181–195. ISSN 1578-7303.
- [135] Ken Kennedy, John R. Allen. Optimizing Compilers for Modern Architectures: A Dependence-based Approach. San Francisco, USA: Morgan Kaufmann Publishers Inc., 2002, 790p. ISBN 1-55860-286-0.
- [136] Joshua Kerievsky. Refactoring to Patterns. 2nd. Addison-Wesley, 2005, 384p. ISBN 3-8273-2262-6.
- [137] Uday Khedker, Amitabha Sanyal, Bageshri Karkare. Data Flow Analysis: Theory and Practice. 1st. Boca Raton, Florida, USA: CRC Press, Inc., 2009, 402p. ISBN 0849328802.
- [138] Peter Kim. The Hacker Playbook 2 – Practical Guide to Penetration Testing. Secure Planet LLC, Jul. 2015, p.339. ISBN 1512214566.
- [139] Christian Kirsch. Entwicklertrauma, Marktübersicht: Tools für die C-Entwicklung – Hilfe gegen Speicher- und Pointer-Fehler. In: Magazin für professionelle Informationstechnik, iX 6 (1994), p.124–129.
- [140] Christian Kirsch. Volle Checkung – C-Laufzeit-Debugger unter Linux. In: Magazin für professionelle Informationstechnik, iX 9 (1995), p.88–91.
- [141] Christian Kirsch. Zeig's mir – Freie Speichertools ElectricFence und Valgrind (german). In: Magazin für professionelle Informationstechnik, iX 3 (2003), p.82–84.
https://www.heise.de/artikel-archiv/ix/2003/03/082_Zeig-s-mir
- [142] Hans Koch, Alain Schenkel, Peter Wittwer. Computer-Assisted Proofs in Analysis and Programming in Logic – A Case Study. In: SIAM Review 38.4 (1996), p.565–604.
- [143] Rajeev Kohli, Ramesh Krishnamurti, Prakash Mirchandani. The Minimum Satisfiability Problem. In: SIAM Journal on Discrete Mathematics 7.2 (1994), p.275–283.
- [144] Robert A. Kowalski. Predicate Logic as Programming Language. In: Information Processing (IFIP). North-Holland Publishing, 1974, p.569–574.
- [145] Neelakantan Krishnaswami. Verifying Higher Order Imperative Programs with Higher Order Separation Logic (unpublished at Carnegie Mellon University), 2008.
<http://www.cs.cmu.edu/~neelk>
- [146] Neelakantan R. Krishnaswami. Design patterns in Separation Logic. In: Proc. of 4th Intl. Workshop on Types in Language Design and Implementation. 2009, p.105–116. DOI 10.1145/1481861.1481874.
- [147] Daniel Kröning, Georg Weissenbacher. Model Checking: Bugs in C-Programmen finden. In: Magazin für professionelle Informationstechnik, iX 5 (2009), p.159–162.
http://www.heise.de/artikel-archiv/ix/2009/05/159_Drum-pruefe
- [148] Marta Kwiatkowska, Gethin Norman, David Parker. Stochastic Model Checking. In: Proc. of the 7th Intl. Conf. on Formal Methods for Performance Evaluation. Bertinoro, Italy: Springer, 2007, p.220–270.
- [149] Sven Lämmermann. Runtime Service Composition via Logic-based Program Synthesis. PhD thesis. . . . Dpt. of Microelectronics, Information Technology, Royal Institute of Technology, Stockholm, Sweden, 2002, 204p.
- [150] William Landi. Undecidability of Static Analysis. In: ACM Letters on Programming Languages and Systems 1 (1992), p.323–337.
- [151] William Landi, Barbara G. Ryder. Pointer-Induced Aliasing: A Problem Classification. In: ACM Principles of Programming Languages. 1991, p.93–103. DOI 10.1145/99583.99599.
- [152] Peter J. Landin. The Mechanical Evaluation of Expressions. In: Computer Journal 6.4 (Jan. 1964), p.308–320.
- [153] Richard G. Larson. Minimizing Garbage Collection as a Function of Region Size. In: SIAM Journal on Computing 6.4 (1977), p.663–668. DOI 10.1137/0206047.
- [154] Chris Lattner, Vikram Adve. Data Structure Analysis: An Efficient Context-Sensitive Heap Analysis. Technical Report no.UIUCDCS-R-2003-2340. Computer Science Dpt., University of Illinois at Urbana-Champaign, USA, 2003, p.1–20.
<http://llvm.org/pubs/2003-04-29-DataStructureAnalysisTR.html>
- [155] K. Rustan M. Leino. Recursive Object Types in a Logic of Object-Oriented Programs. In: Nordic Journal of Computing 5.4 (Apr. 1998), p.330–360. ISSN 1236-6064.
- [156] K. Rustan M. Leino, Greg Nelson. Data Abstraction and Information Hiding. In: ACM Transactions on Programming Languages and Systems 24 (2002), p.491–553.
- [157] Xavier Leroy. A Formally Verified Compiler Back-end. In: Journal of Automated Reasoning 43.4 (2009), p.363–446. DOI 10.1007/s10817-009-9155-4.
- [158] Xavier Leroy. Formal Certification of a Compiler Back-end, or: Programming a Compiler with a Proof Assistant. In: 33rd symp. on Principles of Programming Languages. ACM Press, 2006, p.42–54.
- [159] Xavier Leroy. Formal Verification of a Realistic Compiler. In: Communications of the ACM 52.7 (2009), p.107–115. DOI 10.1145/1538788.1538814.
- [160] Xavier Leroy. Verified Squared: Does Critical Software Deserve Verified Tools? In: 38th symp. Principles of Programming Languages. Abstract of invited lecture. ACM Press, 2011, p.1–2. DOI 10.1145/1926385.1926387.
- [161] Xavier Leroy. The CompCert Memory Model, Version 2. Research report RR-7987. INRIA, France, Jun. 2012.
- [162] John R. Levine. flex and bison – Unix text processing tools. O'Reilly, 2009, p.292. ISBN 978-0-596-15597-1.
- [163] John R. Levine. Linkers and Loaders. 1st. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1999, 256p. ISBN 1558604960.

- [164] Robert Love. *Linux Kernel Development*. 3rd. Addison-Wesley Professional, 2010, 440p. ISBN 0672329468.
- [165] Deborah Y. Maccock. *Automated Theorem-proving and Program Verification: An Annotated Bibliography*. Technical Report no.CS75027-R. Virginia Polytechnic Institute, State University, Blacksburg, Virginia, USA, Nov. 1975.
- [166] David MacQueen, Gordon Plotkin, Ravi Sethi. *An Ideal Model for Recursive Polymorphic Types*. In: Proc. of the 11th ACM SIGACT-SIGPLAN Symp. on Principles of Programming Languages. New York, USA: ACM, 1984.
- [167] Darko Marinov. *Automated Testing of Refactoring Engines Using Test Abstractions*. <http://www.researchchannel.org/prog/displayevent.aspx?rID=28186&fID=5919>.
- [168] Clive Matthews. *An Introduction to Natural Language Processing Through Prolog*. 1st. White Plains, New York, USA: Longman Publishing, 1998, 306p. ISBN 0582066220.
- [169] Farhad Mehta, Tobias Nipkow. *Proving Pointer Programs in Higher-Order Logic*. In: Information and Computation 199.1-2 (2005), p.200–227. DOI 10.1016/j.ic.2004.10.007.
- [170] Tim Menzies. *Applications of Abduction: Knowledge-Level Modeling*. In: Intl. Journal of Human-Computer Studies 45 (Mar. 1996), p.305–335. DOI 10.1006/ijhc.1996.0054.
- [171] Jason Merrill. *Generic and Gimple: A New Tree Representation for Entire Functions*. In: In Proc. of the 2003 GCC Developers Summit. 2003, p.171–180.
- [172] Bertrand Meyer. *Applying Design by Contract*. In: IEEE Computer 25.10 (Oct. 1992), p.40–51. ISSN 0018-9162. DOI 10.1109/2.161279.
- [173] Bertrand Meyer. *Proving Pointer Program Properties – Part 1: Context and overview, Part 2: The Overall Object Structure*. In: ETH Zürich. Journal of Object Technology, 2003.
- [174] Bertrand Meyer. *Proving Pointer Program Properties – Part 2: The Overall Object Structure*. In: ETH Zürich. Journal of Object Technology, 2003.
- [175] Bertrand Meyer, Christine Mingins, Heinz W. Schmidt. *Providing Trusted Components to the Industry*. In: IEEE Computer 31.5 (1998), p.104–105.
- [176] Barton P. Miller, Lars Fredriksen, Bryan So. *An Empirical Study of the Reliability of UNIX Utilities*. In: In Proc. of the Workshop of Parallel and Distributed Debugging. Digital Equipment Corporation, 1990, p.1–22.
- [177] Barton P. Miller. *Nichts dazugelernt – Empirische Studie zur Zuverlässigkeit von Unix-Utilities*. In: Magazin für professionelle Informationstechnik, iX 9 (1995), p.108–121. http://www.heise.de/artikel-archiv/ix/1995/09/108_Nichts-dazu-gelernt
- [178] Robin Milner. *A Theory of Type Polymorphism in Programming*. In: Journal of Computer and System Sciences 17.3 (Dec. 1978), p.348–375. ISSN 0022-0000. DOI 10.1016/0022-0000(78)90014-4.
- [179] John C. Mitchell. *Foundations for Programming Languages*. 2nd. MIT Press, Cambridge, Massachusetts, London, England, 1996, 846p.
- [180] Joël Moses. *The Function of FUNCTION in LISP, or Why the FUNARG Problem Should be Called the Environment Problem*. In: (1970). <http://hdl.handle.net/1721.1/5854>.
- [181] Steven Muchnick. *Advanced Compiler Design and Implementation*. Morgan Kaufmann Publishers Inc., 2007, 856p. ISBN 978-1-55860-320-2.
- [182] Peter Müller. *Modular Specification and Verification of Object-Oriented Programs*. PhD thesis. . . . Fern-Universität Hagen, Germany, 2002, 261p.
- [183] Nomair A. Naeem, Ondrej Lhoták. *Efficient Alias Set Analysis using SSA form*. In: Proc. of the Intl. Symp. on Memory Management. Dublin, Ireland: ACM, 2009, p.79–88. ISBN 978-1-60558-347-1. DOI 10.1145/1542431.1542443.
- [184] Lee Naish. *Higher-Order logic programming*. Technical Report no.96/2. Dpt. of Computer Science, University of Melbourne, Australia, Feb. 1996, 15p.
- [185] Aleksandar Nanevski, Greg Morrisett, Lars Birkedal. *Polymorphism and Separation in Hoare Type Theory*. In: Proc. of the 11th ACM SIGPLAN Intl. conf. on Functional Programming. New York, USA: ACM, 2006, p.62–73. ISBN 1-59593-309-3. DOI 10.1145/1159803.1159812.
- [186] Aleksandar Nanevski, J. Gregory Morrisett, Lars Birkedal. *Hoare Type Theory, Polymorphism and Separation*. In: Journal on Functional Programming 18.5-6 (2008), p.865–911. DOI 10.1017/S0956796808006953.
- [187] Aleksandar Nanevski. *YNot: Reasoning with the awkward squad*. In: Proc. of 13th ACM SIGPLAN Intl. Conf. on Functional Programming. Victoria, British Columbia, Canada, Sep. 2008.
- [188] Charles G. Nelson, Derek C. Oppen. *A Simplifier Based on Efficient Decision Algorithms*. In: Proc. of the 5th ACM SIGSOFT-SIGPLAN symp. on Principles of Programming Languages. Jan. 1978, p.141–150. DOI 10.1145/512760.512775.
- [189] Flemming Nielson, Hanne R. Nielson, Chris Hankin. *Principles of Program Analysis*. Springer Berlin, Heidelberg, 1999, 452p. ISBN 978-3-540-65410-0.
- [190] Peter W. O’Hearn, Hongseok Yang, John C. Reynolds. *Separation and Information Hiding*. In: ACM Transactions on Programming Languages and Systems. 2004, p.268–280. DOI 10.1145/964001.964024.
- [191] Ross Overbeek. *Book Review on Larry Wos: Automated Reasoning: 33 Basic Research Problems*. In: Journal of Automated Reasoning (1988), p.233–234. DOI 10.1007/BF00244397.
- [192] Sascha A. Parduhn, Raimund Seidel, Reinhard Wilhelm. *Algorithm Visualization using Concrete and Abstract Shape Graphs*. In: Proc. of the ACM symp. on Software Visualization. 2008, p.33–36. DOI 10.1145/1409720.1409726.
- [193] Matthew J. Parkinson. *Local Reasoning for Java*. PhD thesis. . . . Cambridge University, England, 2005, 169p.
- [194] Matthew J. Parkinson. *When Separation Logic met Java*. Microsoft Research Cambridge, England, online resource from 13.08.2014. <https://www.microsoft.com/en-us/research/video/when-separation-logic-met-java>.
- [195] Matthew Parkinson, Gavin Bierman. *Separation Logic and Abstraction*. In: SIGPLAN Notes 40.1 (2005), p.247–258. DOI 10.1145/1047659.1040326.
- [196] Nick Parlante. *Linked List Basics*, document no.103 from the Stanford Computer Science Education Library, 2001. <http://cslibrary.stanford.edu/103>.
- [197] Terrence Parr. *The Definitive ANTLR 4 Reference*. The Pragmatic Programmers, 2012, 328p. ISBN 978-1-93435-699-9.
- [198] Lawrence C. Paulson. *The Foundation of a Generic Theorem Prover*. Technical Report, Computer Laboratory, University of Cambridge, England, May 1989, p.363–397. DOI 10.1007/BF00248324.
- [199] Viktor Pavlu. *Shape-Based Alias Analysis – Extracting Alias Sets from Shape Graphs for Comparison of Shape Analysis Precision*. Master thesis. . . . Vienna University of Technology, Austria, Mar. 2010, p.117.
- [200] Fernando C. N. Pereira, David H.D. Warren. *Definite Clause Grammars for Language Analysis – A Survey of the Formalism and a Comparison with Augmented Transition Networks*. In: Artificial Intelligence 13 (1980), p.231–278.
- [201] Fernando C.N. Pereira, Stuart M. Shieber. *Prolog and Natural-Language Analysis*. 3rd. Microtome Publishing, Brookline Massachusetts, 2002, 384p. ISBN 0-9719777-0-4.
- [202] Benjamin C. Pierce. *Basic Category Theory for Computer Scientists*. 1st. Cambridge, Massachusetts, USA: MIT Press, 1991, 114p. ISBN 0-262-660717-0.
- [203] Benjamin C. Pierce. *Types and Programming Languages*. Cambridge, Massachusetts, USA: MIT Press, 2002, 648p. ISBN 0-262-16209-1.
- [204] Andrew M. Pitts. *Nominal Logic: A First Order Theory of Names and Binding*. In: Information and Computation. Academic Press, 2002, p.165–193.
- [205] Andrew M. Pitts. *Relational Properties of Domains*. In: Information and Computation 127 (1996), p.66–90.
- [206] David A. Plaisted. *Theorem Proving with Abstraction, Part I+II*. Technical Report no.UUCDCS R-79-961. Dpt. of Computer Science, University of Illinois, USA, Feb. 1979.

- [207] David A. Plaistead. The Undecidability of Self-Embedding for Term Rewriting Systems. In: *Information Processing Letters* 20.2 (Feb. 1985), p.61–64. DOI 10.1016/0020-0190(85)90063-8.
- [208] Gordon D. Plotkin. A Structural Approach to Operational Semantics. In: *Journal of Logic and Algebraic Programming* 60-61 (Dec. 2004), p.17–139. DOI 10.1016/j.jlap.2004.05.001.
- [209] Gordon D. Plotkin. LCF Considered as a Programming Language. In: *Theoretical Computer Science* 5.3 (1977), p.223–255. DOI 10.1016/0304-3975(77)90044-5.
- [210] Claude Pommerell, Wolfgang Fichtner. Memory Aspects and Performance of Iterative Solvers. In: *SIAM Journal on Scientific Computing* 15.2 (March 1994), p.460–473. ISSN 1064-8275. DOI 10.1137/0915031.
- [211] Francois Pottier. Hiding Local State in Direct Style: A Higher-Order Anti-Frame Rule. In: *Proc. of the 23rd Annual IEEE symp. on Logic in Computer Science*. Washington, DC, USA: IEEE Computer Society, 2008, p.331–340. DOI 10.1109/LICS.2008.16.
- [212] Anthony Preston. Book review: Automated Reasoning: 33 Basic Research Problems by Larry Wos (Prentice Hall 1988). In: *ACM SIGART Bulletin* 105 (1988), 11p. ISSN 0163-5719. DOI 10.1145/49093.1058124.
- [213] Dick Price. Pentium FDIV flaw-lessons learned. In: *IEEE Micro* 15.2 (1995), p.86–88.
- [214] Ganesan Ramanalingam. The Undecidability of Aliasing. In: *ACM Transactions on Programming Languages and Systems* 16.5 (Sep. 1994), p.1467–1471. ISSN 0164-0925. DOI 10.1145/186025.186041.
- [215] Tahina Ramananandro, Dos Gabriel Reis, Xavier Leroy. A Mechanized Semantics for C++ Object Construction and Destruction, with Applications to Resource Management. In: *39th symp. Principles of Programming Languages*. ACM Press, 2012, p.521–532. DOI 10.1145/2103656.2103718.
- [216] Tahina Ramananandro, Dos Gabriel Reis, Xavier Leroy. Formal Verification of Object Layout for C++ Multiple Inheritance. In: *38th symp. on Principles of Programming Languages*. ACM Press, 2011, p.67–79. DOI 10.1145/1926385.1926395.
- [217] John H. Reif. Code Motion. In: *SIAM Journal on Computing* 9.2 (1980), p.375–395.
- [218] Greg Restall. Introduction to Substructural Logic. Routledge Publishing, 2000, 396p. ISBN 041521534X.
- [219] Greg Restall. On Logics Without Contraction. PhD thesis . . . Department of Philosophy, University of Queensland, Australia, 1994, 292p.
- [220] Bernhard Reus. Class-Based versus Object-Based: A Denotational Comparison. In: *Algebraic Methodology and Software Technology 2422/2002* (2002), p.45–88. DOI 10.1007/3-540-45719-4.
- [221] Bernhard Reus, Jan Schwinghammer. Separation Logic for Higher-Order Store. In: *Workshop on Computer Science Logic*. 2006, p.575–590. DOI 10.1007/11874683_38.
- [222] Bernhard Reus, Thomas Streicher. About Hoare Logics for Higher-Order Store. In: *Intl. Colloquium on Automata, Languages, and Programming. Lecture Notes in Computer Science* 3580/2005 (2005), p.1337–1348. DOI 10.1007/11523468_108.
- [223] John C. Reynolds. An Introduction to Separation Logic. Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, 2009.
<http://www.cs.cmu.edu/afs/cs.cmu.edu/project/fox-19/member/jcr>.
- [224] John C. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures. In: *Proc. of the 17th Annual IEEE symp. on Logic in Computer Science*. Washington, DC, USA: IEEE Computer Society, 2002, p.55–74. DOI 10.1109/LICS.2002.1029817.
- [225] Laurence Rideau, Bernard P. Serpette, Xavier Leroy. Tilting at Windmills with Coq: Formal Verification of a Compilation Algorithm for Parallel Moves. In: *Journal of Automated Reasoning* 40.4 (2008), p.307–326. DOI 10.1007/s10817-007-9096-8.
- [226] Silvain Rideau, Xavier Leroy. Validating Register Allocation and Spilling. In: *Compiler Construction. Vol.6011. Lecture Notes in Computer Science*. Springer, 2010, p.224–243. DOI 10.1007/978-3-642-11970-5_13.
- [227] Dirk Riehle. JUnit 3.8 documented using collaborations. In: *SIGSOFT Software Engineering Notes* 33.2 (2008), p.1–28.
- [228] ROSE compiler Infrastructure project. Lawrence Livermore National Laboratory, California, USA.
<http://rosecompiler.org>.
- [229] James Rumbaugh. Object-Oriented Modeling and Design. Upper Saddle River, New Jersey, USA: Prentice-Hall, Inc., 1991, 528p. ISBN 0-13-629841-9.
- [230] Jan J. M. M. Rutten. Elements of Generalized Ultrametric Domain Theory. In: *Theoretical Computer Science* 170.1-2 (1996), p.349–381. DOI 10.1016/S0304-3975(96)80711-0.
- [231] Vladimir O. Safonov. Trustworthy Compilers. Wiley Publishing, 2010, 296p.
- [232] Mooly Sagiv, Thomas Reps, Reinhard Wilhelm. Parametric Shape Analysis via 3-valued Logic. In: *ACM Transactions on Programming Languages and Systems* 24.3 (2002), p.217–298. ISSN 0164-0925. DOI 10.1145/514188.514190.
- [233] Bernhard Scholz, Johann Blieberger, Thomas Fahringer. Symbolic Pointer Analysis for Detecting Memory Leaks. In: *SIGPLAN Notes* 34.11 (1999), p.104–113. DOI 10.1145/328691.328704.
- [234] Herbert Schorr, William M. Waite. An Efficient Machine-Independent Procedure for Garbage Collection in Various List Structures. In: *Communications of the ACM* 10.8 (1967), p.501–506. DOI 10.1145/363534.363554.
- [235] Jan Schwinghammer. Nested Hoare Triples and Frame Rules for Higher-Order Store. In: *Intl. Workshop on Computer Science Logic*. 2009, p.440–454. DOI 10.1007/978-3-642-04027-6_32.
- [236] Dana Scott. Data Types as Lattices. In: *SIAM Journal on Computing* 5.3 (May 1976), p.522–587.
- [237] Helmut Seidl, Reinhard Wilhelm, Sebastian Hack. Compiler Design — Analysis and Transformation. Saarbrücken, Munich, Germany: Springer, Nov. 2011, p.177. ISBN 978-3-642-17547-3.
- [238] Ravi Sethi. Complete Register Allocation Problems. In: *SIAM Journal on Computing* (1975), p.226–248.
- [239] Joseph Sifakis. A Framework for Component-based Construction. In: *Software Engineering and Formal Methods* (2005), p.293–299. DOI 10.1109/SEFM.2005.3.
- [240] Prokash Sinha. A Memory-Efficient Doubly Linked List, online, version from 18.11.2014.
<http://www.linuxjournal.com/article/6828>.
- [241] Daniel Dominic Sleator, Robert Endre Tarjan. Self-adjusting Heaps. In: *SIAM Journal on Computing* 15.1 (1986), p.52–69.
- [242] Amitabh Srivastava, David W. Wall. A Practical System for Intermodule Code Optimization at Link-time. Technical Report no.WRL92-6. Digital Western Research Laboratory, Palo Alto, USA, Dec. 1992.
- [243] Intl. Organization of Standardization. ISO C++ Standard, No.4296 from 2014-11-19.
<https://isocpp.org/std/the-standard>
- [244] Ryan Stansifer. Presburger’s Article on Integer Airthmetic: Remarks and Translation. Technical Report no.TR84-639. Computer Science Department, Cornell University, Sep. 1984.
<http://techreports.library.cornell.edu:8081/Dienst/UI/1.0/Display/cul.cs/TR84-639>
- [245] Static Single Assignment Book, latest from Jul. 2014.
<http://ssabook.gforge.inria.fr/latest/book.pdf>.
- [246] Bjarne Steensgaard. Points-to Analysis in Almost Linear Time. In: *Proc. of the 23rd ACM SIGPLAN-SIGACT symp. on Principles of Programming Languages*. St. Petersburg Beach, Florida, USA: ACM, Jan. 1996, p.32–41. ISBN 0-89791-769-3. DOI 10.1145/237721.237727.
- [247] Joachim Steinbach. Termination of Rewriting — Extensions, Comparison and Automatic Generation of Simplification Orderings. PhD thesis. . . . Universität Kaiserslautern, Germany, 1994, 288p.
- [248] Leon Sterling, Ehud Shapiro. The Art of Prolog: Advanced Programming Techniques. 2nd. Cambridge, MA, USA: MIT Press, 1994, 549p. ISBN 0-262-19338-8.
- [249] Norihisa Suzuki. Analysis of Pointer Rotation. In: *Communications of the ACM* 25.5 (1982), p.330–335. DOI 10.1145/358506.358513.
- [250] Robert Daniel Tennent. The Denotational Semantics of Programming Languages. In: *Communications of the*

- ACM 19.8 (Aug. 1976), p.437–453. ISSN 0001-0782. DOI 10.1145/360303.360308.
- [251] The Clang Project, University of Illinois, USA. <http://clang.llvm.org>.
- [252] The GNU Compiler Collection. <http://gcc.gnu.org>.
- [253] The LLVM Project, University of Illinois, USA. <http://llvm.org>.
- [254] The Valgrind Project. <http://www.valgrind.org>.
- [255] Simon Thompson. Haskell: The Craft of Functional Programming. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1997, 528p. ISBN 0-201-40357-9.
- [256] Simon Thompson. Type Theory and Functional Programming. Intl. Computer Science Series. Wokingham, England: Addison-Wesley, 1991, 388p. ISBN 0-201-41667-0.
- [257] Mads Tofte, Jean-Pierre Talpin. Implementation of the Typed Call-by-Value λ -Calculus using a Stack of Regions. In: Proc. of the 21st ACM SIGPLAN-SIGACT symp. on Principles of Programming Languages. POPL'94. Portland, Oregon, USA: ACM, 1994, p.188–201. DOI 10.1145/174675.177855.
- [258] Mads Tofte, Jean-Pierre Talpin. Region-based Memory Management. In: Information and Computation 132.2 (1997), p.109–176.
- [259] Paolo Tonella. Concept Analysis for Module Restructuring. In: IEEE Transactions on Software Engineering 27.4 (2001), p.351–363. DOI 10.1109/32.917524.
- [260] Jean-Baptiste Tristan, Xavier Leroy. Formal Verification of Translation Validators: A Case Study on Instruction Scheduling Optimizations. In: 35th symp. Principles of Programming Languages. ACM Press, 2008, p.17–27.
- [261] Jean-Baptiste Tristan, Xavier Leroy. Verified Validation of Lazy Code Motion. In: Programming Language Design and Implementation. ACM Press, 2009, p.316–326.
- [262] Anne Sjerp Troelstra, Helmut Schwichtenberg. Basic Proof Theory. 2nd. New-York, USA: Cambridge University Press, 2000, 417p. ISBN 0-521-77911-1.
- [263] Stanford University. Gottlob Frege. Stanford Encyclopedia of Philosophy. <http://plato.stanford.edu>.
- [264] Robert A. Wagner, Michael J. Fischer. The String-to-String Correction Problem. In: Journal of the ACM 21.1 (Jan. 1974), p.168–173. ISSN 0004-5411. DOI 10.1145/321796.321811.
- [265] Mitchell Wand. A New Incompleteness Result for Hoare's System. In: Proc. of 8th ACM symp. on Theory of Computing. 1976, p.87–91. DOI 10.1145/800113. 803635.
- [266] David H.D. Warren. Applied Logic — Its Use and Implementation as a Programming Tool (also passed as PhD-thesis same year to Edinburgh University, Scotland). Technical Report. no.290. Menlo Park, California, USA: SRI International, Jun. 1983.
- [267] David Scott Warren. Efficient Prolog Memory Management for Flexible Control Strategies. In: Intl. symp. on Logic Programming, New Generation Computing (reprint). Vol.2. 4. Atlantic City, New York, USA, Dec. 1984, p.361–369.
- [268] David Scott Warren. Programming in Tabled Prolog (Draft), Dpt. of Computer Science, Stony Brook, New York, USA, from 31th July 1999. <http://www3.cs.stonybrook.edu/~warren/xsbbook/book.html>.
- [269] William E. Weihl. Interprocedural Data Flow Analysis in the Presence of Pointers, Procedure Variables and Label Variables. In: Proc. of the 7th ACM SIGPLAN-SIGACT symp. on Principles of Programming Languages. eds. Paul W. Abrahams, Richard J. Lipton, Stephen R. Bourne. ACM Press, 1980, p.83–94. ISBN 0-89791-011-7.
- [270] Georg Weissenbacher. Abstrakte Kunst: Fehler finden durch Model Checker. In: Magazin für professionelle Informationstechnik, iX 5 (2004), p.116–118. http://www.heise.de/artikel-archiv/ix/2004/05/116_-Abstrakte-Kunst
- [271] Georg Weissenbacher. Ohne Beweis — VDM++ Lightweight Formal Methods. In: Magazin für professionelle Informationstechnik, iX 3 (2001), p.157–161. http://www.heise.de/artikel-archiv/ix/2001/03/157_-Ohne-Beweis
- [272] Why3 Platform for Verification Systems, Project. <http://why3.lri.fr>.
- [273] Wikipedia. Funarg Problem. http://en.wikipedia.org/wiki/Funarg_problem.
- [274] Wikipedia. Region-based Memory Management. https://en.wikipedia.org/wiki/Region-based_memory_management.
- [275] Wikipedia. Shape Analysis. [https://en.wikipedia.org/wiki/Shape_analysis_\(program_analysis\)](https://en.wikipedia.org/wiki/Shape_analysis_(program_analysis)).
- [276] Glynn Winskel. The Formal Semantics of Programming Languages: An Introduction. Cambridge, Massachusetts, USA: MIT Press, Apr. 1993, 384p. ISBN 0-262-23169-7.
- [277] Paul Tucker Withington. How Real is "Real-Time" GC? In: Proc. of 6th annual Object-Oriented Programming Systems, Languages and Applications Workshop: Garbage Collection in Object-Oriented Systems. Phoenix, Arizona, USA, Oct. 1991, p.1–8.
- [278] Stephen Wolfram. A New Kind of Science. Champaign, Illinois, US, United States: Wolfram Media Inc., 2002, 1197p. ISBN 1-57955-008-8.
- [279] Larry Wos. Automated Reasoning: 33 BASIC Research Problems. Prentice-Hall, Inc., 1988, 319p. ISBN 0-13-054552-X.
- [280] Larry Wos. The Problem of Finding a Restriction Strategy more effective than the Set of Support Strategy. In: Journal of Automated Reasoning 7.1 (1991), p.105–107.
- [281] Hongseok Yang, Peter W. O'Hearn. A Semantic Basis for Local Reasoning. In: Foundations of Software Science and Computation Structures. 2002, p.402–416.
- [282] Ilya S. Zakharov. Configurable Toolset for Static Verification of Operating Systems Kernel Modules. In: Programming and Computer Software. Vol.41. Proc. of the Institute for System Programming of Russian Academy of Science. Pleiades Publishing, 2015, p.49–64.
- [283] Karen Zee, Viktor Kuncak, Martin C. Rinard. Full Functional Verification of Linked Data Structures. In: Programming Language Design and Implementation. 2008, p.349–361. DOI 10.1145/1375581.1375624.
- [284] Kaizhong Zhang, Dennis Shasha. Simple Fast Algorithms for the Editing Distance between Trees and Related Problems. In: SIAM Journal on Computing 18.6 (1989), p.1245–1262.
- [285] Кулик, В.А. Логика естественных рассуждений / В.А. Дюк – Санкт-Петербург. Невский Диалект, 2001. – 128с. ISBN 5-7940-0080-5
- [286] Калинина, Т. В. Абстрактные методы повышения эффективности логического вывода: дис. ... канд. физ.-мат.наук:05.13.18/ Калинина Татьяна Владимировна. — Санкт-Петербург, 2001. — 185с.
- [287] Левенштейн, В.И. Двоичные коды с исправлением выпадений, вставок, замещений символов / В.И. Левенштейн // Докл. АН СССР. – 1965. №4(163). С.845–848.
- [288] Братчиков, И. Л. Формально-грамматическая интерпретация метода резолюции / Братчиков Игорь Леонидович // Вестник СПбГУ, труды XXIV-ых научн. конференции процесса управления, устойчивости, Санкт-Петербург. – 1998. №1. p.197-202.
- [289] Верт, Т., Крикуна, Т., Глухих, М. Обнаружение дефектов работы с указателями в программах на языках Си, Си++ с использованием статического анализа, логического вывода / Верт Татьяна // Инструменты, методы анализа программ (ТМРА 2013), Кострома. – 2013.
- [290] Лавров, С.С. Программирование — Математические основы, средства, теория. / С. Лавров // Санкт-Петербург: БХВ-Петербург, 2001 - 320с. ISBN 5-94157-069-4
- [291] Опалева, Э.А. Самойленко В.П. Языки Программирование, Методы Трансляции. / Э.А. Опалева // Санкт-Петербург: БХВ-Петербург, 2005 - 480с. ISBN 5-94157-327-8
- [292] René Haberland. Using Prolog for Transforming XML-Documents. In: arXiv:1912.10817[cs.PL]
- [293] René Haberland. Narrowing Down XML Template Expansion and Schema Validation. In: arXiv:1912.10816[cs.LO]

- [294] René Haberland, Igor L. Bratchikov. Transformation of XML Documents with Prolog. In: Advances in Methods of Information and Communication Technology. Vol. 10. 2008, p.99–111. ISBN 978-5-8021-1020-1, УДК 519.1+681.3.
- [295] René Haberland, Kirill Krinkin. A Non-repetitive Logic for Verification of Dynamic Memory with Explicit Heap Conjunction and Disjunction. In: International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP). Ed. University of Venice, Italy. Oct. 2016, p.1–9. ISBN 978-1-61208-506-7, ISSN 2308–4498, IARIA XPS Press/-ThinkMind.
- [296] René Haberland, Kirill Krinkin, Sergey Ivanovskiy. Abstract Predicate Entailment over Points-To Heaplets is Syntax Recognition. In: 18th Conference of Open Innovations (FRUCT), ISSN 2305-7254, ISBN 978-952-68397-3-8. Ed. By T. Tyutina S., Balandin A., Levina. 2016, p.66–74. DOI 10.1109/FRUCT-ISPIT.2016.7561510.
- [297] René Haberland. A Stricter Heap Separating Points-To Logic. In: 3rd Intl. Scientific Symposium Sense Enable (SPITSE2016). Ed. by Russia National Research University Moscow. June 2016, p.103–104. РИНЦ 26444969.
- [298] René Haberland, Sergey Ivanovskiy. Dynamically Allocated Memory Verification in Object-Oriented Programs using Prolog. In: Proc. of the 8th Spring/Summer Young Researchers' Colloquium on Software Engineering (SYRCoSE 2014). Ed. by Alexander Kamkin, Alexander Petrenko, and Andrey Terekhov. 2014, p.46–50. ISBN 978-5-91474-020-4, ISSN 2311–7230, DOI 10.15514/SYRCoSE-2014-8-7.
- [299] René Haberland. Unification of Template-Expansion and XML-Validation. In: Proc. of Intl. Conf. on Control Processes and Stability. Vol. 34. Saint Petersburg State University, 2008, p.389–394. ISBN 978-5-288-04680-3, ISSN 2313–7304, РИНЦ, УДК 517.51:517.9:518.9.
- [300] Хаберланд, Р. Верификация корректности динамической памяти с помощью логического языка программирования. / Р. Хаберланд // Конференция EMC^2 «Технологии Майкрософт в Теории, на Практике Программирования. Серия: Новые подходы к разработке программного обеспечения», Санкт-Петербургский Политехнический Университет, Санкт-Петербург. – 2014. №3. С.56–57.
- [301] Хаберланд, Р. Расширяемый Фреймворк для верификации статически типизированных объектно-ориентированных программ, использующих динамическую память. / Р. Хаберланд // Санкт-Петербургский Электротехнический Университет «ЛЭТИ» (ПИС ЛЭТИ), Санкт-Петербург. – дек. 2015. №5. УДК 004.052.2.
- [302] Хаберланд, Р., Ивановский, С. А., Кринкин, К. В. Верификация Объектно-ориентированных программ с динамической памятью на основе ссылочной модели с помощью Пролога. / Р. Хаберланд // Известия ЛЭТИ, Санкт-Петербургский Электротехнический Университет, Санкт-Петербург. – 2016. №1. С.14–18. ISSN 2017–8985, УДК 004.052.2.
- [303] Хаберланд, Р. Сравнительный анализ статических методов верификации динамической памяти. / Р. Хаберланд // Компьютерные инструменты в образовании, Санкт-Петербург. – 2019. №2. С.5–30. DOI 10.32603/2071-2340-2019-2-5-30, УДК 004.052.2.
- [304] Haberland, R. Universal direct project building tool. Saint Petersburg State Electrotechnical University (LETI) — ROSPATENT, granted on 18.12.2018, registration no. 2019610438
- [305] Haberland, R. Universal program slicing tool. Saint Petersburg State Electrotechnical University (LETI) — ROSPATENT, granted on 18.12.2018, registration no. 2018664644
- [306] Haberland, R. Program for verifying dynamic memory (ProLogika). Saint Petersburg State Electrotechnical University (LETI) — ROSPATENT, granted on 18.12.2018, registration no. 2019610339
- [307] René Haberland. Recent Techniques Review on Heap Verification with Class Objects. St. Petersburg Electrotechnical University (unpublished), 2016
- [308] René Haberland. Tutorials and Examples. St.

Petersburg Electrotechnical University, 2016.
<https://bitbucket.org/reneH123/tutorials>.

List of Theorems

1.1	Definition (Hoare Triple)	4	5.1	Observation (Operator Overloading)	62
1.2	Definition (Input Programming Language)	6	5.2	Thesis (Strengthening Expressibility of Ambiguous Spatial Operation)	62
1.3	Definition (Specification Language)	6	5.3	Thesis (Simplification by Differentiating Heaps)	62
1.4	Definition (Logical Consequence)	7	5.4	Thesis (Complete Heap Rules by Incomplete Specifiers)	62
1.5	Observation (Proving as Searching)	7	5.5	Corollary (Strengthening Modelling)	62
1.6	Definition (Soundness of a Hoare Calculus)	7	5.6	Definition (Observable Heap by Reynolds)	64
1.7	Definition (Completeness of a Hoare Calculus)	8	5.7	Definition (Heap Conjunction)	65
1.8	Definition (Logical Formulae in the First-Order Predicate Logic)	10	5.8	Theorem (Conjunction of Generalised Heaps)	65
1.9	Definition (Terms T_{λ_2})	11	5.9	Convention (Locations)	66
1.10	Definition (Set of $\Lambda_{T_{\lambda_2}}$ terms)	11	5.10	Lemma (Monoid over Conjunction)	66
1.11	Definition (Type Checking)	11	5.11	Theorem (Abelian Group over Conjunction)	66
1.12	Definition (Formal Proof)	12	5.12	Convention (Heap Invertibility)	67
1.13	Observation (Verification Model of Computation)	12	5.13	Lemma (Homomorphism over Simple Heaps)	68
1.14	Observation (Phase Type Checking)	16	5.14	Definition (Heap Disjunction)	68
1.15	Observation (Verification Non-Reducibility towards Typing)	16	5.15	Lemma (Monoid over Disjunction)	68
3.1	Observation (Organised Memory and Fresh Context)	36	5.16	Theorem (Distributivity)	68
3.2	Observation (Unorganised Memory and Unique Context)	36	5.17	Convention (Modelling of Object Instances)	69
3.3	Observation (Phenomenon of Remote Manipulation)	36	5.18	Convention (Object Fields)	70
3.4	Observation (Variable Visibility Scope)	36	5.19	Definition (Incomplete Predicate)	71
3.5	Observation (Graph-based Representation of Dynamic Memory)	38	5.20	Example (Incomplete Predicate no.1)	71
3.6	Theorem (Reynolds' Spatial Properties)	41	5.21	Example (Incomplete Predicate no.2)	71
3.7	Definition (Heap Satisfaction Relation)	42	6.1	Definition (Heap Assertion)	73
3.8	Definition (Finite Heap Graph)	43	6.2	Corollary (Heap Soundness)	74
3.9	Definition (Heap Term)	43	6.3	Definition (Informal Heap Graph sketch)	74
3.10	Definition (Heap Term Extension)	43	6.4	Definition (Predicate Rule)	75
4.1	Definition (Generic Prolog-term)	45	6.5	Definition (Predicate Rule Set)	75
4.2	Definition (Horn Rule)	45	6.6	Corollary (Predicates Environment)	76
4.3	Definition (A Query in Prolog)	46	6.7	Lemma (Predicate Completeness regarding Expressibility)	76
4.4	Definition (Cutting Solutions)	47	6.8	Lemma (Higher-order Predicate Expressibility)	76
4.5	Thesis (Proof over Heaps is equivalent to Syntax Analysis)	49	6.9	Definition (Predicate Folding)	77
4.6	Lemma (The Double-Semantics of Prolog Predicates)	50	6.10	Observation (Narrowing down with Formal Languages)	77
4.7	Observation (Equality of Proof Elements)	51	6.11	Thesis (Syntax Recognition is Proving)	77
4.8	Observation (Deduction with Backtracking)	52	6.12	Corollary (Context-Freeness of Heap Expressions)	77
4.9	Observation (Stack-based Predicate Calls)	52	6.13	Observation (Heap Reduction)	78
4.10	Thesis (Expressibility of Relations in Prolog)	54	6.14	Lemma (Heap as Word)	78
4.11	Thesis (Simplification using Term IR)	55	6.15	Theorem (Transduction into Attributed Grammar)	78
4.12	Observation (Comparison of Declarative Paradigms)	56	6.16	Theorem (Inverted Transduction from Attributed Grammar)	79
4.13	Observation (Simplification of Inductive Proof Primitives by Generalisation)	56	6.17	Corollary (Transducer Termination)	79
4.14	Corollary (Minimisation of Differences between Generational and Checking Languages)	56	6.18	Corollary (Soundness and Completeness of Transductions)	79
4.15	Observation (Language Confluency upon Verification)	57	6.19	Definition (Abstract Sentence)	79
4.16	Corollary (Minimisation of Incoming Program)	60	6.20	Definition (First-Set of Non-Terminals)	80
			6.21	Definition (Set of Following Terminals)	81
			6.22	Example (Rules Ambiguity)	81
			6.23	Example (Example for Word Correctness)	81

	List of Figures	49	Unifications for the proof tree from fig.48 . .	47
1	Prioritised quality ladder	3	Example code for the factorials in Prolog . .	48
2	Logical rules in Hoare's calculus	3	Counter-example code on factorial in Prolog .	48
3	An incomplete rule set for verification	5	Characterisations of typings from points 2,3 .	50
4	Loop rules replacing while	5	Calling subgoals	51
5	Code example for the remainder of two integers	6	Example of stack windows and related subgoal	
6	Example of a proof refutation	6	references with ingoing and outgoing terms .	51
7	Church-Rosser theorem applied to Hoare triples	7	Relational model over Prolog predicates . . .	54
8	Example of a complete and sound rule set		Pipeline architecture for the prover and syn-	
	taken from [67]	10	tax processors	56
9	Peirce's theorem about the excluded third in		Roles in the Model-View-Controller meta-	
	Coq	11	pattern applied to heap verification	57
10	Inductive Coq definition of Church's numbers	12	Quantitative analysis using Hälstead metrics	
11	CFG with assigned intervals	14	[112]	58
12	Phases until code generation	16	CFG on heap verification	59
13	Comparison between type checking and Hoare		Isomorphic 3-regular heaps with objects . . .	63
	calculus	16	Example of a connected heap graph	63
14	Object calculi	17	Example of a disconnected heap graph	64
15	x points to an object which points to y . .	19	Example of a possible heap dissection	64
16	Specifiable life-cycle of an object	19	Heap graph before and after conjunction . . .	65
17	Definition of object terms after Abadi-Leino .	20	Heap graph before and after inversion	67
18	Example of unsound rule set	20	Poset over heap graph inclusion	69
19	Simplified Abadi-Leino object definition . . .	21	Shapes of object assignments	69
20	A possible definition of subclassing	21	Transformation of schematic heap graph . . .	70
21	Proof tree example for an object-based calculus	22	Example of compound heaps	74
22	Example rule set for an object calculus	22	EBNF for logical rules	75
23	Code example for a pointer rotation after		Functional map/3	76
	Suzuki (in Pascal)	24	Example of a heap configuration	81
24	Dynamic Memory whilst rotating pointers . .	25	Graphical user interface	83
25	A typical memory layout for a Linux process	29	Programmer's view (UML use case)	83
26	Example for a stack	30	Specifier's view (UML use case)	84
27	Example for a heap	30	Verifier's view (UML use case)	84
28	Example for classically instantiated objects .	32	Example of a simply-linked list no.1	84
29	Example for an incorrect assignment of an		Example of a simply-linked list no.2	85
	object pointer	32	Layered architecture of verifier "ProLogika" .	86
30	Examples of bit/byte ordering	33	ProLogika components	86
31	Example of an incorrectly linked pointer and		Package alice.tuProlog	87
	non-terminating program	33	Package parsers	87
32	Example CFG.	35	Package core	87
33	Example of SSA-placements by basic blocks .	35	Packages internal.checkers	88
34	Visibility of locals in a),b) and dynamically		Packages internal.aps	88
	allocated variable in c)	36	Class Main	88
35	Example finite automaton \mathcal{A}_1	37	Class Parser	89
36	Example finite automaton \mathcal{A}_2	37	Class SyntaxAnalyzer	89
37	Example finite automaton \mathcal{A}_3	37	Package frontend	90
38	Equalities describing the automaton	38	Package parsers.incoming	90
39	C code example for list inversion	38	Package parsers	91
40	Example heap trace for list inversion	38	Package frontend	91
41	Example heap with pointers x,u,y	41	Package internal.core	92
42	Example cactus in dynamic memory	41	Package layers frontend, internal.core, inter-	
43	Example of schematic separability of heap . .	42	nal.aps	92
44	Formal heap definition according to SL	42	Package internal.aps	93
45	Example on Prolog rules and facts	46	Package internal.ht	93
46	Example code on occurs-checks	47	Package prolog	94
47	Example code on list unification	47		
48	Derivation tree for the Ackermann-predicate .	47		

- >:, 61
- α -conversion, 21, 41
- λ -calculus, 5, 11, 16, 18, 41, 58, 59
- λ -expression, 10
- λ -term, 9, 18, 23, 57
- \mapsto -assertion, 80, 83
- μ -recursive predicate, 77
- μ -recursive schema, 20
- μ -recursive scheme, 71
- ϕ -function, 35
- \star , 42, 72, 73, 77
- (3-)SAT-problem, 53
- (CPU) word, 32, 39, 42
- (sub-)expression, 53
- \cdot -operator, 42
- \cdot -operator, 42, 45, 61, 66
- .bss, 29, 32
- .ctor, 19
- .dtor, 19
- =.., 46
- _, 45, 50
- union, 187
- Proof, 11
- Qed, 12
- atom, 46
- calloc, 18
- compound, 46
- concatMap, 49
- concat, 50, 51, 58
- foldl, 49
- is, 46
- list, 46
- malloc, 18
- new, 18, 19
- number, 46
- register, 34
- self, 19
- super, 19
- take, 9, 53
- tauto, 12
- unify_with_check, 58
- union, 30, 33, 69
- var, 46

- Abadi-Cardelli calculus, 17–19, 60
- Abadi-Leino calculus, 17, 19, 21, 60
- abduction, 4, 24, 28, 58
- ABI, 18, 26, 34
- absorption, 69
- abstract interpretation, 13, 58
- abstract machine, 55, 93
- abstract predicate, 28, 44, 55, 60, 61, 63, 66, 71–74, 81
- abstract predicate family, 28, 76
- abstract sentence, 81

Index

- abstraction, 10, 12, 21, 22, 33, 41, 50, 72
- Ackermann function, 46, 47, 51, 58
- ACL2, 45
- actor, 18, 22
- address space, 64
- addressation, 29, 39, 42
- adjoint-trees, 73
- Adren’s lemma, 37
- ADT, 15, 17, 22, 23
- algebra
 - formal, 12
 - initial, 76
 - relational, 53
- algebraic field, 68
- alias, 8, 21, 23–26, 30, 33, 36, 37, 44, 54, 55, 59, 65, 70, 72, 74
- alias analysis, 3, 24–26, 30, 34, 59
- alignment, 15, 33
- allegory of the cave, 40
- ambiguity, 40, 73, 81
- ambiguous operation, 62
- anonymous function, 20, 21, 44
- antecedent, 3, 27
- ANTLR, 82, 83
- approximation, 13, 24, 56
- Arden’s lemma, 38
- arising chain, 48
- Aristotle, 40, 45
- arithmetic, 61, 71
 - Church, 44, 45
 - Peano, 13
 - pointer, 27
 - Presburger, 13
- arithmetic expression, 75
- arity, 45, 46, 51, 52, 58, 72
- ARM, 33
- array, 18, 27, 29, 30, 70
- artificial intelligence, 49
- assembler, 19
- assembly, 55
- assembly line, 56, 59
- assertion, 13, 21, 41, 42, 45, 46, 48, 56, 59–61
 - base, 78
- assertion negation, 48, 49, 74
- assignment, 21, 24
- associativity, 54, 66, 68
- AST, 55, 59
- atom, 58, 83
- atomic assertion, 44
- atomism, 18, 57
- attribute, 70
- automated proof, 59
- automated testing, 14
- automated verification, 10, 49

- automaton
 - abstract, 7
 - finite, 37, 54, 73, 94
 - partial-derivatives, 73
- auxiliary predicate, 57
- axiom, 3
- axiomatic semantics, 57

- B-tree, 53
- Baby Modula 3, 20
- backtracking, 52
- base case, 48
- basically stable, 3
- bigraph, 64
 - maximal matching, 64
- binary operator, 61, 64
- binary tree, 39, 42
- bipartite graph, 64
- BISON, 82
- bitfield, 25, 36
- block, 35
- boolean denotation, 9, 10, 27, 43
- boolean set, 49, 74
- bottom-up, 52
- branch and bound, 75
- builder, 16
- built-in command, 73
- byte, 30

- C, 9, 25, 28, 30, 32, 34, 38, 59
- C++, 6, 18, 19, 23, 27
- caching, 26, 54, 71, 81
- cactus, 41, 42
- calculation ordering, 76
- calculation state, 3, 4, 16, 56, 59
- call by value, 29, 35, 59
- callee, 47
- caller, 34, 47
- can-alias, 34
- canonisation, 54, 63, 83
- Cantor set, 11, 53
- carrier set, 17, 66, 68, 76
- CF, 78
- CFG, 4, 9, 14, 22, 25, 35, 59
- Church arithmetics, 44, 45
- Church typing, 9
- Church's calculus, 16
- Church-Rosser theorem, 7
- CLANG, 55
- class, 19, 20
- class instance, 23, 69
- class type, 20
- class-based calculus, 59
- closure, 9, 66
- co-domain, 58, 79
- co-procedure, 8

- code generation, 34, 42, 55, 59
- code size, 29
- code transformation, 55
- collaborations, 23
- compacting GC, 26
- compactness, 41
- comparison, 60
- compilation, 60
- completely stable, 3
- completeness, 3, 6, 8, 9, 11, 13, 14, 44, 61, 62
- complex numbers, 66
- complexity, 22
- component algebra, 23
- computability, 55
- conclusion
 - logical, 73
 - semi-automated, 73
- concretisation, 5, 70
- conditional branch, 5, 9, 21, 29, 35
- confluency, 4, 7, 9, 13, 65–67
- conjunct, 64, 70, 71
- conjunction, 10, 43, 64, 66–69, 71
- connected graph, 74, 75
- connectionism, 18
- connotation, 40
- consequent, 3, 48
- const, 34
- constant function, 43–45, 71, 74
- constraint programming, 59
- constructor, 19
- context-free, 50, 62, 78
- context-sensitive, 49, 61
- continuation, 36, 52
- Cook's completeness, 9
- copying GC, 26
- copying memory, 52
- Coq, 10, 73
- counter-example, 4, 8, 12, 23, 58, 59, 78, 93
- Cousout's method, 13
- Curry's calculus, 16
- Curry-Howard isomorphism, 73
- cut, 46–48, 51, 52, 54
- Cyclone, 28

- dangling pointer, 22, 33, 36
- data dependency, 5, 15, 34, 35, 43, 53, 78
- data structure, 39, 40, 42, 46, 58
- DCG, 59, 73
- decidability, 13
- deduction, 4, 34, 52, 59
- delegation, 19
- denotational semantics, 20, 36, 43, 57
- depedent type, 21
- dependency graph, 24, 60
- dependent type, 58
- derivable result, 51

- derivation tree, 6, 47, 50, 52
- descending chain, 7, 8
- design by contract, 22
- destructor, 29
- determinism, 48
- diamond property, 7, 9
- difference lists, 73
- disjunction, 10, 41, 42, 67, 68, 71
- distributivity, 68
- division, 6
- domain, 7, 58, 64, 76
- domain as relations, 54
- DOT, 58, 59, 83–85, 91
- doubly-connected edge list, 72
- doubly-linked list, 26, 72
- dual operation, 68
- duality, 70
- duplicate, 33, 39, 48, 55
- dynamic memory, 3, 4, 16, 24, 27–29, 31, 32, 34, 36–41, 43, 49, 52, 55–57, 59–61, 64, 74
- dynamic parameters, 23
- eager evaluation, 58
- Earley recogniser, 79
- EBNF, 45, 61, 75
- edit distance, 94
- ElectricFence, 28
- embedded device, 31
- equivalency relationship, 44
- error localisation, 14, 34
- error production rules, 79
- evaluation ordering, 4, 8, 18, 44, 53, 71
- exception, 10, 51
- excluded third, 11
- exclusive or, 29
- expressibility, 8, 9, 21, 33, 38, 42–44, 50, 52, 54–56, 62, 63, 76
- expression, 36, 46
- expression negation, 5, 48
- extensibility, 51, 53, 55, 59
- fact, 45, 48, 51, 52, 57, 75
- factorial, 48
- fail, 49
- false, 74
- falsification, 52
- Fibonacci heap, 39
- field, 22, 24, 71
 - arithmetic, 66
 - assignment, 65
 - attribute, 18
 - Galois, 68
 - real numbers, 66
- field accessor, 75
- first set, 80
- first-terminals set, 78
- fix-point combinator, 5
- fixpoint combinator, 20, 48
- flash memory, 30
- floating approach, 26
- fold, 24, 73, 75, 76, 80, 92
- follow-set, 78
- follow-terminals set, 81
- footprint, 60
- formal algebra, 12
- formal logic, 7, 12
- formal method, 8, 13, 14, 22
- formal theory, 10, 14, 34, 51, 57, 59, 62, 65
- formal verification, 4
- formula interpretation, 59, 61
- frame, 27, 28, 43, 60
- framework, 23, 34, 36
- full abstraction, 20
- full definition, 40
- full specification, 23
- function inversion, 71
- function invertibility, 58
- functional, 7, 9, 16, 23
- functor, 10, 44, 46, 47, 50, 58, 59, 61, 75
- Gallina, 10
- gaps, 54
- garbage, 26, 39, 64
- GC, 3, 22, 23, 26, 27, 30, 31, 50, 59
- GCC, 18, 25, 31, 55
- generalisation, 5
- generalised assertion, 34
- generational GC, 30
- geometry, computational, 72
- GIMPLE, 28, 55, 96, 97
- global invariant, 22
- GNU, 30, 51
- GNU Linux, 35
- GNU make, 16
- GNU Prolog, 82
- grammar
 - attributed, 78, 93
 - context-free, 50
 - formal, 45, 50, 73, 75, 77, 78, 82
 - mutation, 73
 - sub-, 79
- grap vertex, 39
- graph
 - bridge, 67
 - full, 39, 69
 - merge, 66
 - relation, 69
 - simple, 66
 - vertex, 39, 40, 44, 72
 - vertex degree, 39
- graph abstraction, 24
- graph concretisation, 24

- graph edge, 37, 39, 41, 44, 60, 72
- graph isomorphism, 81
- graph transformation, 15, 22, 38
- green cut, 48, 71
- group, 67, 68
 - Abelian, 66
 - inverse element, 66–69
 - neutral element, 66, 68
 - sub-, 66
- Halting-problem, 44, 48, 59, 76
- hardware architecture, 18
- Haskell, 8, 9
- Hasse diagram, 69
- heap, 24, 26, 29, 30, 36, 39–44, 51, 53, 54, 56, 61, 62, 64, 65, 68, 69
 - assertion, 73
 - base, 52, 54, 72, 73
 - canonisation, 74
 - cell, 29
 - complex, 69, 72, 74
 - connected, 33, 41, 44
 - empty, 67, 69, 71, 73, 81
 - finite, 68
 - generalisation, 67
 - generalised, 70
 - incomplete, 62
 - independent, 73
 - interpretation, 37, 60, 74
 - inverse, 66
 - inversion, 66–69
 - isomorphism, 63
 - merge, 64
 - modality, 41
 - negative, 67
 - normalisation, 67
 - separation, 41, 64
 - simple, 70
 - specification, 63
 - state, 36
 - sub-, 64
 - subtraction, 48
 - with symbols, 75
- heap copy, 72
- heap edge, 38
- heap formula, 74
- heap graph, 36, 37, 39–41, 43, 44, 57, 60, 61, 63, 65–68, 74
- heap instance, 51
- heap separation, 24
- heap state, 30
- heap verification, 55
- heuristics, 28, 44
- hierarchical specification, 8
- higher-order logic, 9, 57, 76
- Hindley-Milner calculus, 16
- Hoare calculus, 8, 10, 12, 16, 189
- Hoare triple, 4, 6, 14, 16, 52, 56
- Hoare-rule, 45
- homomorphism, 67, 71
- Horn-rule, 45, 49, 57–59, 71, 73
- hypothesis, 12
- implication, 5, 12
- incremental approximation, 13, 60
- induction, 4, 8, 41, 66
- inductive definition, 8, 12, 49
- inductive structure, 10, 44, 48
- infimum, 18, 19
- infinite data structure, 9, 53, 60
- infix notation, 46
- Information Hiding Principle, 184
- inheritance hierarchy, 19, 61, 69
- inherited class, 69
- initial algebra, 76
- initial stack, 21
- injection, 13
- inner class, 28
- inner object, 69
- inner procedure, 9
- input program, 56, 59, 60
- integers, 44, 48, 61, 64
- Intel, 33
- intellectual language level, 58
- intellectual level, 54
- interpretation, 57
- intra-procedural alias analysis, 24
- introspection, 3, 28, 31, 46
- intuitionistic judgement, 11
- invalid access, 30–32
- invariant, 8, 9, 17, 24, 54, 66
- inverse mapping, 44
- inversion of control, 28
- invertible function, 52
- IR, 28, 49, 53, 55–57, 59, 60, 82
- ISO-C++, 30
- isomorphic mapping, 13, 44, 50, 58
- Java, 18, 28, 30, 58
- JIMPLE, 28
- join, 69
- jStar, 28, 55
- judgement, 3, 4, 21
- jump field, 29
- KeY, 28
- Kleene’s star, 75
- knowledge base, 45, 46, 73
- Knuth-Bendix algorithm, 13
- LALR-recogniser, 44, 79
- language

- assertion, 9, 73, 93
- extension, 62
- formal, 6, 40, 49, 50, 73
- functional, 14, 43, 49
- imperative, 4, 43, 49, 52, 74
- input, 42, 56, 60
- logical, 41, 43, 51
- natural, 40, 49, 50, 73
- processor, 78
- programming, 4, 6, 18, 23, 73
- regular, 73
- specification, 6, 42, 56, 63, 74
- validation, 54
- verification, 56, 93
- language abstraction, 58
- language extension, 31, 53
- late binding, 70
- lattice, 13, 18, 35
- lazy evaluation, 8, 11, 12
- left folding, 76
- lemma, 12, 16, 59, 60
- Levenshtein's algorithm, 94
- lexeme, 73
- lexical analysis, 49
- lexicographical ordering, 58, 61, 77
- limit, 13, 14, 16, 18, 34, 35
- linear list, 9, 33, 34, 38, 39, 41–43, 45, 46, 50, 53
- linux, 25, 35
- Liskov's principle, 22
- LISP, 36
- list inversion, 33, 34, 38
- literal, 48
- LL(k)-recogniser, 81
- LL-analyser, 49, 79
- LLVM, 28, 31, 55, 96
- LLVM-bitcode, 55
- localisation of errors, 19
- locality, 23, 44, 47, 50, 64, 69, 93
- location, 43, 66, 67, 72, 73, 76
- logical derivation, 4
- logical formula, 10, 74
- logical operator, 41
- logical predicate, 56
- logical programming, 50
- logical reasoning, 51, 52, 56, 71
- logical rule, 75
- logics, 12
- mapping, 13, 44, 53
- may-alias, 30, 34
- memoisation, 71
- memoiser, 81
- memory allocation, 35, 36, 39
- memory cell, 37, 39, 40, 43
- memory deallocation, 19, 29, 32, 33, 35, 36, 39
- memory fragmentation, 69
- memory leak, 30–32
- memory model
 - Burstall, 41, 64
 - Reynolds, 42, 64, 73
- memory region, 26, 38, 40, 42, 43, 61
- memory state, 6, 21
- mesh, 72
- meta-physics, 12
- method, 22
- metrics, 22, 49, 54, 58
- minimalistic program, 60
- minimality, 60
- model checking, 14, 15
- model of computation, 9
- model transformation, 23, 54
- Modula-2, 20
- modular algebra, 23
- modular programming, 12
- modularity, 75
- monad, 72
- monoid, 66, 68
- morpheme, 73
- multi-paradigm, 51, 53
- multi-paradigm programming, 78
- multi-target paradigm, 82
- must-alias, 30, 34
- name clashing, 6, 76
- name mangling, 83
- natural deduction, 4, 13
- natural numbers, 12, 13, 45, 46, 71
- natural speech recognition, 49
- non-ambiguous operator, 61
- non-decidable, 16
- non-determinism, 43, 44
- non-repetitiveness, 41, 66, 71
- non-strict, 9
- non-terminal, 77, 78
- non-termination, 9
- normal vector, 72
- normalisation, 56
- NP-hard problem, 30
- numeral logic, 5
- object, 22
 - field, 18, 19, 65, 69
 - state, 19
- object calculus, 17–19, 23
- Object Constraint Language, 23
- object field, 9, 37, 39, 41, 42, 61, 67
- object instance, 18, 19, 21, 39, 41–43, 50, 54, 58, 61, 65, 81
- object invariant, 22
- object orientation, 3
- object type, 18, 21
- observed behaviour, 17

- OCaml, 8, 28
- occurs-check, 80
- OCL, 23, 62
- offset, 26, 27
- one-time function, 49
- one-way function, 71
- ontology, 22
- openness, 59
- operational semantics, 7, 9, 20, 53, 71
- optimal stable, 3
- organised memory, 29
- OS, 31, 32, 39, 74
- overloaded definition, 51
- paradigm, 9, 17, 35, 49, 56, 74
 - declarative, 47
 - declarative, 4, 6, 50, 52, 53, 56, 57, 74
 - functional, 9, 23, 36, 49, 57
 - imperative, 4, 35, 74
 - object-oriented, 17
- paradox, 44, 58, 61
- parameter
 - by call, 7
 - by reference, 7
 - formal, 9
 - incoming, 9, 51, 57
 - incorrect, 9
 - outgoing, 51
- parameter by call, 71
- parameter cutting, 9
- parameters by reference, 50
- Parnas' principle, 22
- partial correctness, 9
- partial derivatives, 55
- partial specification, 94
- Pascal, 20
- path accessor, 39, 42, 65
- pattern, 15, 18, 28, 76, 82
- pattern matching, 9, 45, 51, 60, 184
- PCF, 59
- Peano arithmetics, 71
- Peano's arithmetics, 13
- Peirce's theorem, 11, 52
- performance, 29, 30, 52, 53
- permanent memory, 31
- platform, 30
- Plato, 40, 45
- plausibility, 59
- pointer, 8, 18, 23, 24, 27, 29, 30, 32, 36–42, 44, 58, 62, 64, 65, 67, 69, 70, 72, 74
- pointer approximation, 25
- pointer content, 34, 61
- pointer rotation, 24, 33
- polish-inverse notation, 55
- polyhedron mesh, 72
- polymorphism, 18, 51, 60, 61, 72
- polynomial rank, 62
- Popper's method, 4
- poset, 7, 19, 20, 39, 69
- Post's problem, 78
- postcondition, 60
- PowerPC, 33
- pragmatics, 12
- pragmatism, 18
- precondition, 5, 13, 60
- predicate, 40–43, 45, 46, 48, 49, 51–53, 55, 74
 - assertion, 10, 36
 - auxiliary, 34
 - auxiliary, 42, 71
 - body, 45, 75
 - built-in, 28, 46, 49, 51, 76
 - call, 46–48, 50, 51, 60
 - contradiction, 74
 - first-order, 4, 52
 - head, 45, 48, 51, 58, 78
 - higher-order, 36, 44, 45, 49, 50, 76
 - negation, 41
 - parameterisation, 42, 44, 58, 72
 - quantified, 9
 - semantics, 48, 75
- predicate call, 77
- predicate environment, 76
- predicate logic, 10, 13, 18, 63, 72
- predicate negation, 74
- prefix, 77
- prenex-normal-form, 44
- Presburger's arithmetics, 13
- Principle Data Independence, 36
- prioritisation issue, 48
- priority queue, 39
- process, 29, 57
- production rules, 81
- program length, 58
- program simplification, 16
- program slicing, 16
- program statement, 4, 6, 9, 10, 13, 14, 16, 33, 36, 38, 40, 41, 51, 55, 60, 61, 64
- programming by proving, 73
- programming idiom, 18
- programs statement, 39
- projective geometry, 5
- Prolog, 45, 46, 48–55, 57, 59–61, 71, 73, 79
 - Definite Clause Grammars, 73
 - disjunction, 74
 - query, 44, 46, 74
- Prolog rule, 50, 59, 78
- Prolog theory, 51
- proof
 - automation, 59, 61
 - hint, 73
 - refutation, 52
 - search, 47

- solution, 47
 - strategy, 26
 - tree, 21, 50
 - unfolding, 6
- prototyping, 72
- quality criteria, 3
- quality ladder, 3, 6, 23, 34, 45
- RAM, 4, 18, 29, 39
- rapid prototyping, 72
- RC, 3, 28, 38
- real numbers, 10, 45
- recogniser, 55
 - recursive, 73
 - top-down, 73
- record, 16, 21
- recursion, 8, 9, 46, 48, 52
 - arise, 48
 - left, 48, 73
 - mutual, 46
 - primitive, 9
 - right, 78
 - schema, 46, 52, 53
 - unbound, 80
- recursive scheme, 71
- recursive type, 18, 44
- red cut, 48, 71
- redex, 11, 73
- REDUCE, 79
- reduction, 16
- reduction over records, 22
- register, 4, 18, 34
 - special purpose, 19
- register allocation, 18, 30
- regular expression, 37, 38, 40, 49, 55, 83
- regular graph, 39
- reification, 40
- relation, 10, 51, 53–55, 57
 - minus, 54
 - product, 54
 - projection, 54
 - renaming, 54
 - selection, 54
 - union, 54
- relational algebra, 53
- remainder, 6
- remote manipulation, 36
- renaming, 21
- resolution, 4
- resolution method, 13
- return on fail, 52
- Reynolds' algorithm, 34
- rule
 - alternative, 47, 58
 - assignment, 5, 6
 - contraction, 27
 - frame, 28
 - logical consequence, 5
 - loop, 5
 - object constructor, 21
 - sequential, 5
 - substitution, 27
 - syntax error, 93
 - thinning, 27, 73
 - verification, 3
- rule body, 48, 58
- rule canonisation, 76
- rule factorisation, 77
- rule normalisation, 59
- rules overloading, 58
- Russel's paradox, 11
- SA, 3, 38
- safe pointer operations, 33
- SAFECode, 28
- SAT-problem, 9, 51
- SATlrE, 28
- scope visibility, 45, 74
- security breach, 32
- self-inverse operation, 68
- semantic analysis, 18, 37, 59, 61
- semantic field, 55, 56
- semantic function, 71
- semantic web, 50
- semantics, 12, 13, 40, 49
 - operational, 73
- semi-structured data, 28, 45, 57
- semiotics, 12, 40
- separation of concerns, 22, 75
- sequence operator, 77
- sequentialiser, 16, 42
- shape analysis, 28
- shape graph, 24
- shared vertex, 68
- SHIFT, 79
- shift-reduce, 82
- shrinker, 17
- side-effect, 56, 81
- sign, 12
- signature, 19
- simply-linked list, 38
- Skolem normal-form, 12
- SL, 27, 28, 41, 42, 61, 65, 93
- SLR-recogniser, 79
- Smallfoot, 28, 41
- SMT-solver, 14, 28, 44, 50, 62, 66, 67
- soundness, 3, 5, 8, 9, 20, 21, 24, 30, 34, 48, 61, 62
- SpaceInvader, 28
- spatial operator, 43, 61
- specification, 19, 21, 23, 33, 39, 43, 53–56, 60
 - full, 60

- modularity, 60
- undetermined, 11
- SSA-form, 25, 35, 43
- stack, 4, 21, 22, 26, 29, 36, 37, 41, 42, 50–53, 69
 - architecture, 71
 - overflow, 34
 - pop, 31
 - popping, 29
 - push, 9, 23, 31
 - pushing, 29, 46
 - rewinding, 10
 - window, 8, 23, 29, 35, 47, 50, 51, 53, 71
- stack, pushing into, 53
- static, 19
- static analysis, 70
- static analysis, 13–15, 55, 56, 59, 60
- static field, 28
- stderr, 17
- stdout, 17
- stepwise graph construction, 65
- stepwise verification, 51, 69
- stereotype, 18, 22
- Stratego XT, 15
- strategy, 13, 26, 47
- stratification, 47, 50
- strengthening, 43, 62
- strict evaluation, 9
- strict operator, 65
- structuralism, 40, 65
- subclass, 18, 61
- subgoal, 45–48, 50, 51, 56, 75, 77, 79, 80
- subgraph, 24
- subprocedure, 43
- substructural logic, 27, 66, 73
- subtype, 20
- supremum, 14, 18
- surjection, 13
- Suzuki’s memory model, 33
- syllogism, 40
- symbol, 6, 15, 40–43, 45, 46, 50, 52–54, 56, 58, 61, 66, 74, 93
- symbols environment, 75
- synchronisation point, 79
- syntactic sugar, 21, 48, 72
- syntax, 12, 21, 38, 40, 50, 57
- syntax analysis, 49, 50, 55, 59–61, 63, 73, 79, 81, 92
- syntax tree, 73
- synthesised attribute, 83
- Tableaux method, 4, 11
- tactics, 10, 12, 57, 59, 73
- tautology, 43, 76
- temporal assertion, 22, 23
- term, 43, 45–48, 53, 55, 57–60, 74
 - algebra, 65
 - expression, 61
 - incoming, 43, 48, 49, 52, 59, 71, 76
 - incoming/outgoing, 71
 - normalisation, 54
 - outgoing, 43, 48, 49, 59, 71, 76
 - self-applicable, 7, 11, 58
 - self-containing, 80
 - sub-, 58
 - tree, 54
- term normalisation, 12
- term reduction, 11
- term rewriting system, 7, 15
- term unification, 43, 45–48, 50, 54, 57, 58, 77, 80
- term vector, 45, 75
- terminal, 77, 81
- termination, 8, 9, 13, 31, 33
- test, 14
- test coverage, 30
- testing, 14
- tetrades, 55
- tetrads, 55
- theorem, 12, 31, 34, 49, 50, 59
 - Gödel’s, 8
 - Birkhoff, 54
- theory of integers, 8, 12
- theory of objects, 3, 17
- thesis-antithesis-synthesis, 40
- thread, 10
- thread blocking, 22
- token, 78
 - predecessor, 73
- token stream, 79
- totality, 9, 45, 46, 61
- transducer, 33, 78, 79
- transfer function, 24
- translating rule, 83
- triads, 55
- triangle, 72, 81
- triangulation, 72
- true, 74
- trustworthy compilation, 23
- truth, 3
- tuple, 18, 61
- Turing machine, 4
- Turing-computability, 19, 49
- type, 16, 43, 46, 58, 60, 61
- type calculus
 - Church, 42
 - Curry, 42
- type cast, 32
- type checking, 11, 13–16, 20, 21
- type compatibility, 20, 69
- type ideal, 21
- type relationship, 21
- type variable, 74
- typing, 8, 11, 16, 18, 20, 27, 32, 43, 45, 59
 - higher-order, 21

- typing paradox, 11
- UML, 15, 23, 28, 62
- unconditional branch, 55
- unfold, 12, 24, 75, 80, 92
- unification, 26, 56, 72
- uninitialised, 9, 18, 38
- uninitialised value, 32
- union, 26
- universe, 4
- Unix, 30
- unorganised memory, 29
- untypable term, 11
- untyped term, 16
- utilitarian approach, 63
- Valgrind, 28
- variability, 51, 53, 55
- variable
 - automated, 8, 35
 - boolean, 10
 - dynamic, 8, 29, 35, 41
 - free, 7, 41, 46
 - global, 7, 24, 29, 43, 56
 - local, 10, 18, 21, 22, 28, 29, 35, 38, 41, 45, 74, 75
 - logical, 36
 - quantified, 58, 72
 - static, 8, 36
 - symbolic, 42, 45, 46, 56
 - typed, 74
 - uninitialised, 30
- VDM++, 15, 28
- Verifast, 28, 73
- verification, 3, 6, 14, 31, 51, 54, 56, 59, 60, 63
- verification assistant, 10, 28
- verification automation, 92
- verification core, 10
- verification platform, 10
- verification result, 6
- Vernacular, 10
- virtual machine, 30
- virtual memory, 29, 31
- virtual register, 21
- visibility scope, 6, 23, 29, 35, 56, 59
- WAM, 46, 49, 52, 53, 71, 75, 93
- weak typing, 46
- weakly typed, 30
- White-Schorr's algorithm, 34
- Why, 14
- Windows, 32
- word, 6
- wrong, 20
- XML, 25, 54
- xor, 26
- XSL-T, 25, 57
- Y-not, 14, 28
- YACC, 82