

holpy: Interactive Theorem Proving in Python

Bohua Zhan

State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences,
Beijing, China
bzhan@ios.ac.cn

Abstract

The design of modern proof assistants is faced with several sometimes conflicting goals, including scalability, extensibility, and soundness of proof checking. In this paper, we propose a new design for proof assistants, in an attempt to address some of these difficulties. The new design is characterized by a pervasive use of macros in representing and checking proofs, and a foundational format for theory files based on JSON. We realize these ideas in a prototype proof assistant called holpy, implemented in Python. We also demonstrate how proof automation can be extended using Python under this framework. Finally, we present a case study about a simple imperative language.

2012 ACM Subject Classification Theory of computation \rightarrow Logic and verification; Theory of computation \rightarrow Higher order logic

Keywords and phrases Interactive theorem proving, Higher order logic, Python

Funding *Bohua Zhan*: [CAS Pioneer Hundred Talents Program under grant No. Y9RC585036]

Acknowledgements The author would like to thank Yi Li, Yongjian Li, Meng Sun, and Xiyue Zhang for discussions about the project, and also Jie Hou, Zhenyan Ji, Chaozhu Xiang, and Wenfan Zhou for ongoing collaboration on the user interface of the proof assistant.

1 Introduction

Proof assistants are the basic tools of interactive theorem proving. Their design therefore lies at the foundation of the subject. Decades of research has brought large improvements to the design of proof assistants. The most widely-used proof assistants today, Isabelle [17] and Coq [3], have become very mature systems capable of handling large-scale applications. However, it is unlikely that this is the end of the story. Indeed, the development of new proof assistants is still an active area of research. A well-known example is Lean [7], a recent and actively developed proof assistant based on dependent type theory.

As interactive theorem proving moves from mostly dealing with toy examples to routinely having industrial applications, the focus for the design of proof assistants has also shifted. While logical foundation used to be the main focus, today many other aspects are gaining increasing attention. In particular, we consider the following three goals to be of utmost importance in the future development of proof assistants:

- **Scalability**: the proof assistant should be able to handle very large proofs, such as those coming from industrial applications. In addition to very long hand-written proofs, this also includes proofs that involve a large amount of computation, and large proofs generated by internal tactics or external theorem provers.
- **Extensibility**: it should be easy for users to implement domain-specific proof automation for the proof assistant. Other aspects of extensibility include the ability to implement customized user interfaces, and the ability to link with other sources of automation, such as SMT solvers and computer algebra systems.
- **Soundness**: the soundness of proof-checking should be guaranteed to the highest level possible. In particular, user-specified proof automation and other extensions should never be able to compromise the proof checking kernel. Risks coming from bugs in the

kernel itself should be minimized as much as possible, for example by allowing multiple independent proof checkers.

These goals sometimes appear to be conflicting. The use of popular programming languages such as Python to implement proof automation may be convenient for users, but the lack of type or memory safety in these languages makes soundness guarantees more difficult. Generation of proof terms that can be checked by third-party tools improve soundness guarantees, but the potentially large size of proof terms makes scalability an issue.

In this paper, we propose a new design for proof assistants that aims to resolve these difficulties. The core aspects of the design is implemented in a prototype proof assistant called holpy (**h**igher-**o**rd**er** **l**ogic in **p**ython)¹. Other more advanced aspects are so far just theoretical, whose implementation is left for future work. The design includes three interconnected ideas that form the main contributions of this paper: extensive use of macros, a JSON-based format for theory files, and an API for implementing proof automation in Python. These ideas are summarized below and will be expanded upon in the body of this paper.

- Extensive use of macros: macros are abbreviations for potentially large proof terms. They have appeared in existing proof assistants before. However, as far as we know they have never been made a central part of the design of a proof assistant. In this paper, we show how a pervasive use of macros can enable proof checking that is both memory-efficient and intrinsically safe, allowing it to scale to very large proofs, and has soundness guarantees independent of the programming language used.
- JSON-based format for theory files: we propose the use of a JSON-based format as the foundational format for theory files. While in the short term it has disadvantages such as making user interfaces more difficult to implement, we believe it has long term advantages that outweigh these concerns. In particular, it allows several very different user interfaces to work together on different parts of a proof. It also simplifies implementation of third-party tools for working with theory files.
- API for implementing proof automation: we design an API for implementing proof automation in Python. We show that aspects of the language that are generally considered to make it unsuitable for this purpose: being an imperative language with weak type and memory safety enforcements, do not pose a problem in the context of the new system. In particular, we give several patterns for implementing proof automation, showing how certain common tasks can be achieved in a natural way in imperative programming.

We now clarify what are not the concerns of this paper. First, we do not propose any innovation on logical foundations for proof assistants. We continue to use higher-order logic (simply-typed lambda calculus) that has been successfully employed in HOL4, HOL-Light, and Isabelle/HOL. Compared to Isabelle/HOL, we drop the distinction between meta and object logic (e.g. \implies vs. \longrightarrow), and represent theorems as sequents with a set of antecedents and a single consequent. We also omit advanced features such as type classes and locales. The primitive deduction rules `implies_intr`, `implies_elim`, etc, are similar to that in previous HOL-based systems. By introducing the type `set`, along with axioms of ZFC set theory, it is possible to construct an environment for formalizing mathematics in set theory within higher-order logic [12, 18].

¹ available online at <https://gitee.com/bhzhan/holpy>

Second, our implementation of the proof assistant is so far just a bare prototype, with many important parts missing. This includes first of all a user interface, whose implementation is currently in progress and is not part of this paper. We also do not prove many of the theorems which we use to demonstrate the proof automation, nor do we verify the validity of inductive definitions. Techniques for foundational definition of (co)inductive datatypes and recursion is now very mature [4], and will be added in the future.

2 Macros in proof representation

The most important aspect of holpy's design is its extensive use of macros for representing proofs. Traditionally, in the context of proof terms, a macro is a special proof term that can be expanded into a larger proof term using an associated procedure, and serves as an abbreviation of the latter for efficiency purposes [7, Section 2].

In HOL-based systems, the Curry-Howard correspondence is not used explicitly, so that proofs and terms remain separate concepts. Hence, to make use of macros, it is necessary to fix a representation of proofs, and then define macros as abbreviations within this representation.

We will now describe the representation of proofs used in holpy. We define a *proof rule* as a function taking as arguments the current theory, a list of input theorems, and possible additional arguments (such as terms, numbers, or strings), and outputs a new theorem. In principle, the output theorem should be derivable from the input theorems. Each of the primitive deduction rules in HOL can be expressed as proof rules. Another pre-defined proof rule is the `theorem` rule, which takes as input the name of a theorem and returns the theorem with the given name from the theory. Together, they are called *primitive* proof rules, and form the logical core of the system. Macros, to be defined below, form the second class of proof rules. Each proof rule has a name, and the theory maintains a mapping from names of proof rules to the corresponding functions.

A *proof item* specifies a step of deduction using a proof rule. It consists of an identifier, the name of the proof rule used, the argument supplied to the proof rule, and a list of identifiers of other proof items, from which the input theorems are to be obtained. A proof is represented as an ordered list of proof items. Each proof item can only refer to previous items in the list. A theorem can be associated to each proof item in the proof by invoking the proof rules in sequence. The result of the proof is the theorem associated to the last proof item.

A macro is a proof rule that, in addition to the evaluation function which produces the output theorem, also has an `expand` function which outputs the proof of the theorem. For the arguments to the `expand` function, the input theorems come with identifiers which can be referred to in the output proof. The expanded proof is allowed to refer to other macros, or even itself (presumably with different arguments). Both primitive proof rules and macros are allowed to signal exceptions if the input is improper in any way. Evaluation and expansion of macros are also allowed to run forever on certain inputs. In both cases the proof would be considered to be incorrect.

2.1 Examples of macros

Opportunity to use macros arise naturally everywhere in interactive theorem proving, unifying several existing concepts. We now give some examples.

2.1.1 Evaluation on natural numbers

The most basic use of macros is to package domain-specific proof procedures. For example, arithmetic on natural numbers can be packaged as a macro: the input is a term consisting of $+$ and \times operations on constant natural numbers, where the constants are expressed in binary form. The evaluation function returns a theorem equating the term to a single constant, where the arithmetic is performed directly using arbitrary-precision integers. The expand function justifies the equality using existing theorems about operations on binary numbers.

2.1.2 Equality between polynomials on natural numbers

Given two polynomials on natural numbers, their equality can be decided by computing the normal form of both sides. This can be packaged as a macro as follows: the input is the statement of the equality to be proved. The evaluation function computes the normal forms of both sides, which may make use of internal data structures for efficiency, e.g. representing a polynomial as a list of monomials and a monomial as a list of atoms. It returns the equality of the two sides if the normal forms are the same. The expand function produces the full deduction involving commutativity, associativity, and distributivity rules. Both signal an exception if the normal forms of the two sides are not equal.

2.1.3 Resolution and resolution chains

A resolution in propositional logic takes an atom x and two theorems $A_1 \vee A_2 \vee \dots \vee A_m$ and $B_1 \vee B_2 \vee \dots \vee B_n$, where $A_i = x$ and $B_j = \neg x$ for some i, j , and returns the theorem

$$A_1 \vee \dots \vee \hat{A}_i \vee \dots \vee A_m \vee B_1 \vee \dots \vee \hat{B}_j \vee \dots \vee B_n$$

A resolution chain is a sequence of resolutions, starting at theorem P_0 , and using theorem-variable pairs $(P_1, x_1), \dots, (P_n, x_n)$. Resolution chains arise naturally in the verification of proofs produced by SAT solvers.

A resolution can be packaged as a macro, with two theorems and a term as input. The evaluation function of the macro checks that the inputs are in the right form, and produces the output theorem. The expand function produces the full proof consisting of applications of theorems in propositional logic. A resolution chain can also be packaged as a macro, where the evaluation function repeatedly invokes the evaluation function for resolution, and where the expand function produces a proof consisting of calls to the resolution macro.

2.1.4 Simplification of definitional equalities

A major difference between systems based on dependent type theory (e.g. Coq and Lean) and those based on higher-order logic is that the former systems have a separate notion of definitional equalities, allowing some computation to be performed in the kernel. This can reduce the length of proof terms needed. The technique of reflection [3, Chapter 16] gives a systematic way to make use of this feature to speed up proof checking.

In systems based on higher-order logic, definitional equalities are generally not used. This means proof terms, if they were to be produced, can be much longer. In our framework, one way to address this problem is to maintain within the theory a list of rewriting rules acting as definitional equalities (for example, all equations in inductive definitions). Then, it is possible to define a single macro which takes a term as input, and returns an equality theorem rewriting the term according to this list of rewriting rules. The expand function

of the macro produces a proof consisting of the individual rewriting steps. This macro can then be used to abbreviate all computations involving inductive definitions.

2.1.5 Oracles

A final example of macros involves those proof procedures for which it is very difficult to generate the detailed proof. For example, the procedure may call an external SMT solver, or computer algebra systems. While producing detailed proofs for those procedures may be imaginable in the future, today it would take too much effort. Such proof procedures can be packaged as a macro where the expand function is unavailable. The proof checker is forced to trust the macro (which implies trust in the external solver, as well as any translation functions). However, this trust is explicit: the proof checking procedure can record which macros are trusted to prove which statements. The user is then free to make use of such reports, for example by re-running the statements in different solvers or computer algebra systems.

2.2 Proof checking with macros

We now consider the problem of checking a proof containing macros. We begin with the simple design where the proof checker and the expand function for all macros are contained in a single program. Then, we consider an improvement to this design.

2.2.1 Monolithic checker

The basic design calls for a single process containing both the proof checker and procedures for expanding the macros (which we call the interpreter). During proof checking, the proof is read line-by-line. Every time a macro is encountered, the interpreter for the macro is invoked, which returns the expanded proof. The expanded proof is then also read line-by-line, expanding any macros encountered recursively. When the checking of an expanded proof is finished, the proof is removed from memory, keeping only the theorem associated to the last line (which is the result of evaluating the macro). In this way, the fully expanded proof never need to be stored in memory. At any point during proof checking, only proofs for macros on the current path of expansion need to be stored. For a well-designed system of macros, where no macro expand to proofs that are too long, this means memory usage can be kept small even for very long proofs.

2.2.2 Separating checking and expansion

The above proof checking mechanism addresses the memory usage problem, and mostly prevents non-hostile interference by user-defined proof automation on the proof checking process: if all the interpreter of macros do is to generate the expanded proof on their own allocated memory, no problem would occur. However, most programming languages do not possess strong guarantees of memory separation between functions. It could be possible for the interpreter of macros to modify memory held by the proof checker, hence corrupting the proof checking process.

Another problem with the monolithic design is that it is very difficult to implement third-party proof checkers. Not only do the checker need to implement a trusted kernel, it also need to re-implement the (untrusted) expand functions for all macros occurring in the proof. The cost would be prohibitive at advanced stages of development, and reduces the viability of user-defined macros.

The above problems can be solved by separating proof checking and macro expansion into two processes, called the checker and the interpreter. The two processes can run in isolated memory on the same computer, or even on different computers, with only a line of text-based communication between them. The interpreter is responsible for reading the proof line-by-line. Every time a primitive proof rule is encountered, it sends the line directly to the checker. If a macro is encountered instead, it is expanded and read line-by-line recursively. If the checking of an expanded proof is finished, the proof is deleted from interpreter's memory, and a signal is sent to also delete the proof from checker's memory. From the checker's point of view, all it receives is a stream of primitive proof steps, as well as signals saying that certain parts of the proof can be safely deleted. In this way, the entire interpreter is not part of the trusted code base. A single interpreter, which contains expand functions for all macros, can be connected to multiple third-party proof checkers, dramatically increasing confidence in the proof checking process.

2.2.3 Trust level during proof checking

As already noted in [7], it is possible to assign different trust levels to macros. In any run of proof checking, only macros with trust level higher than a pre-set number need to be expanded. The user has the flexibility to adjust this number for different stages of proof development. For example, a higher trust level is set when developing a proof, allowing rapid feedback from the proof assistant. At the end of the development, the proof is re-checked at a lower trust level, removing the need to trust most macros.

3 Foundational format for theory files

The second component of holpy's design is a foundational format for theory files based on JSON. Most existing proof assistants choose a file format that allows direct human editing, with the proof assistant acting as the interpreter of the format. While this design is certainly natural, it has the disadvantage that it is difficult for other tools to interpret the files – any such tool must re-implement a large part of the core of the proof assistant. Various proof exchange formats, such as OpenTheory [14] and Dedukti [5], have the potential to solve this problem. However, as they are developed independently, there is always difficulty translating theories between them and the major proof assistants.

In contrast, we design holpy with a foundational format for theories based on JSON. While the format is human readable and partially human editable, it is not well-suited for direct editing by users. Instead, the intention is that the file will be read and edited by other tools, including user interfaces that display the content and reflect changes onto the files. While this may make implementing a user interface more difficult, we believe it has other advantages that are more significant:

- It allows user interfaces to present the content of the files in different ways, or maintain their own file format which can be converted to the foundational format. This means user interfaces can be customized for different application domains, but still produce theory files of common format that can be checked together.
- A gap between the theory file and content displayed for the user means not all data need to be displayed. Information in the theory that are not necessarily important to the user (e.g. automatically generated proof steps) can be hidden or displayed optionally.
- The JSON format can be easily read by other tools (parser for JSON is available for most major programming languages). Extensibility of JSON means different tools can

add information to the theory files for its own use, without affecting other tools.

In this section, we describe a basic version of the file format, which is currently used in the prototype holpy system (a sample file is given at the end of Section 5). This is only intended to give an idea of the nature of the format. The format for a realistic system will certainly be more complicated, in particular involving more data fields.

3.1 JSON: a brief overview

JSON (JavaScript Object Notation) is a lightweight data-interchange format [10]. It is known for its simplicity of design. Each JSON element can be either a dictionary (with strings as keys and other JSON elements as values), an ordered list of elements, a string, a number, a boolean value, or null. Most major programming languages has tools converting between JSON format and its internal data. In particular, Python has library functions for reading a file in JSON format, resulting in a Python object where each JSON element type is converted to the corresponding Python type. Any Python object containing only dictionaries, lists, tuples, strings, numbers, and booleans can also be written as a JSON file.

3.2 Format for theory files

A theory file is stored as a dictionary with the following keys: `name` for the name of the theory, `imports` for the list of imported theories, `description` for the overall description of the theory, and `content` which is a list containing the content of the theory.

Each element in `content` is a dictionary, with key `ty` specifying the type of the element. They can be constants, definitions, axioms, theorems, datatypes, and so on (it is possible to make this list user-extensible – this is left as future work). Each type of element has its own interpretation of fields. We use theorems as an example. A theorem element contains keys `name` (name of the theorem), `vars` (dictionary mapping names of variables appearing in the theorem to its type), `prop` (statement of the theorem, as a printed string), and `proof`, containing the proof of the theorem. The proof is represented as a list of proof items, following the format given in Section 2. The theorem element can optionally contain other keys, such as `attributes` (analogous to Isabelle’s attributes, used by search tools in the user interface as well as proof automation).

3.3 Discussion

With the above format for theory files, it is immediately clear what are the theorems declared in a theory. This means different theories, and proofs of different theorems within a theory, can be checked independently of each other. In other proof assistants, such as Coq and Isabelle, this is likely to be possible after minor adjustments. In our framework, however, such opportunity for parallelism is completely transparent.

Having a universal format for theory files also means different user interfaces can be implemented for different application domains. One scenario where this is helpful is as follows. In a framework for program verification, the program logic used (syntax, semantics, and Hoare logic) may be formalized in a standard, general-purpose user interface, while actual program verification may be performed in a user interface that allows users to edit the program in its original syntax, as well as insert assertions between lines of the program in an intuitive way. The two user interfaces may have their own file formats, but both also produce files in the standard JSON format. These files can then be checked together by a proof checking kernel.

Finally, having a standard JSON format makes it easy to develop other tools to analyze theories. This includes tools for creating dependency graphs, for detection and removal of redundant content, and for extraction of training data for machine learning algorithms.

4 API for implementing proof automation

The third component of holpy’s design is an API (application programming interface) for implementation of proof automation in Python. Most proof assistants today support user-defined proof automation. Coq implements the Ltac language for defining tactics [8]. In Isabelle, proof automation is usually written in its implementation language Poly/ML. A new language called Eisbach [15], emulating Ltac in Coq, has also been developed. Lean develops its own metaprogramming language, based on Lean itself, for defining proof automation [9].

All of the above facilities for defining proof automation is based either on an ML-like functional programming language (e.g. Poly/ML and OCaml), or on languages defined within the proof assistant. The use of more popular imperative languages, such as C++, Java, or Python, for implementing proof automation is much less well-explored. Two aspects of these languages are generally considered to make them unsuitable for this purpose. First, the weak type and memory safety enforcements of these languages make soundness of the overall system a concern. Second, many of the existing programming paradigms for implementing proof automation, such as composition of tactics and conversions, are based on functional programming.

We have already addressed the first of these concerns in Section 2.2. The use of proof terms means the output of proof automation can be verified by independent proof checkers, and the separation of proof checking and macro expansion means there is no way for user-defined proof automation to affect the execution of the proof checker. In this section, we address the second concern, by proposing a set of programming paradigms for proof automation based on imperative programming. We show that using these paradigms, code for achieving certain common tasks can be written in a natural way.

We choose Python as the implementation language as it is known to be a very flexible language suitable for rapid prototyping. Python also has limited support for functional programming. It should be noted, however, that all of the programming paradigms discussed below can also be realized in languages such as C++ or Java (perhaps with more verbose code). All that is needed from the language itself is good support for object-oriented programming, including inheritance and polymorphism.

4.1 Construction of proof terms

In Section 2, we represented proofs as an ordered list of proof items, where each item invokes a proof rule and may depend on results from items earlier in the list. While this representation is good for visualizing the proof checking process and may be more intuitive to users, it is certainly not ideal for constructing proofs. For the latter purpose, it is useful to define the concept of a *proof term*, which represents a proof in a tree-like structure, where each node is an invocation of a proof rule, and edges denote dependencies in the proof.

In holpy, proof terms are represented by objects of the class `ProofTerm`. Each proof term contains the name of the proof rule, the argument used, and references to proof terms for the input theorems. The output theorem is also computed and stored in the object. It is simple to write a function converting a proof term into the linear representation of proofs, as required in Section 2. Note that during the conversion, branches of the proof term that

are repeated (with or without sharing memory) should be converted to the same proof item, with multiple references to the item from later in the list.

With the conversion algorithm in place, expansion of macros can be implemented by first writing a function that produces a proof term, then converting the proof term into a linear proof. As such, paradigms for implementing proof automation in Python revolves around the construction of proof terms. This produces code that has a different feel from those based on composition of tactics or conversions. In the following subsections, we show how several types of automation tasks can be achieved naturally in this way.

4.2 Conversions revisited

Conversions are functions that take a term as input, and returns an equality theorem rewriting the term to some other term (e.g. a simplification or normalization). Conversions can be composed using *combinators* to form more complex conversions. Some common combinators include `then_conv`, `else_conv`, `top_conv`, etc. Programming conversions using combinators form a big part of implementing proof automation in ML-like languages.

In holpy, conversions are realized as a Python class `Conv`. The member function `get_proof_term` takes the current theory and a term as input, and returns a proof term rewriting the input term. Combinators can be implemented as classes inheriting from `Conv`. For example, `then_conv` is implemented as follows (to save space, we omit some assertions and optimizations in the following displayed code).

```
class then_conv(Conv):
    # Applies cv1, followed by cv2.
    def __init__(self, cv1, cv2):
        self.cv1 = cv1
        self.cv2 = cv2

    def get_proof_term(self, thy, t):
        pt1 = self.cv1.get_proof_term(thy, t)
        pt2 = self.cv2.get_proof_term(thy, pt1.prop.rhs)
        return ProofTerm.transitive(pt1, pt2)
```

With definitions like these, we can proceed to program with conversions in the usual style. However, such extensive use of functional programming is not natural in Python. Instead, we propose another paradigm for programming with conversions, based on construction of proof terms.

The operation of a complex conversion can be seen as making successive changes to the right side of an equality proof term. We define a member function `on_rhs(self, thy, *cvs)` in the class `ProofTerm`, which applies the conversions in the list `cvs` in sequence to the right side of the current proof term. As an example, a conversion simplifying arithmetic on natural numbers in binary form can be implemented as follows (we assume `Suc_conv`, `add_conv`, `mult_conv` have already been implemented, for the evaluation of successor, addition, and multiplication on natural numbers).

```
class nat_conv(Conv):
    # Simplify all arithmetic operations
    def get_proof_term(self, thy, t):
        pt = refl(t)
        if is_binary(t): # t is a number in binary form
            return pt
        else:
            if t.head == Suc:
                return pt.on_rhs(thy, arg_conv(self), Suc_conv())
            elif t.head == plus:
                return pt.on_rhs(thy, binop_conv(self), add_conv())
```

```

elif t.head == times:
    return pt.on_rhs(thy, binop_conv(self), mult_conv())
else:
    raise ConvException()

```

Here we took advantage of Python's support for an arbitrary number of arguments to a function to simplify the API. Note also the use of `if` statements to replace matching in ML-like languages.

We give another illustrative example from the simplification of function updates. The function update is defined as follows.

$$(f)(a := b) = (\lambda x. \text{if } x = a \text{ then } b \text{ else } f x)$$

Some key properties of function update are:

theorem *fun_upd_upd*: $(f)(a := b, a := c) = (f)(a := c)$

theorem *fun_upd_twist*: $\neg c = a \longrightarrow (f)(a := b, c := d) = (f)(c := d, a := b)$

The aim is to convert a sequence of function updates $f(a_1 := b_1, a_2 := b_2, \dots, a_n := b_n)$ to normal form. We assume f is of type $\text{nat} \Rightarrow \text{nat}$, and all a_i, b_i are constant natural numbers in binary form. Normal form requires sorting and removing duplicates in a_i . This is used in Section 5 for the evaluation of operational semantics.

The Python code for this conversion is as follows.

```

class fun_upd_norm_one_conv(Conv):
    # Normalize a function update (f)(a1 := b1, ...) (an := bn) by moving
    # the last update to the right position, combining if necessary.
    def get_proof_term(self, thy, t):
        pt = refl(t)
        if is_fun_upd(t) and is_fun_upd(t.args[0]):
            f, a, b = t.args
            f2, a2, b2 = f.args
            if nat.from_binary(a) < nat.from_binary(a2):
                neq = nat.nat_const_ineq(thy, a, a2)
                return pt.on_rhs(thy, rewr_conv("fun_upd_twist", conds=[neq]),
                                argn_conv(0, self))
            elif nat.from_binary(a) == nat.from_binary(a2):
                return pt.on_rhs(thy, rewr_conv("fun_upd_upd"))
            else:
                return pt
        else:
            return pt

class fun_upd_norm_conv(Conv):
    # Normalize a function update of the form (f)(a1 := b1, a2 := b2, ...).
    def get_proof_term(self, thy, t):
        pt = refl(t)
        if is_fun_upd(t):
            return pt.on_rhs(thy, argn_conv(0, self), fun_upd_norm_one_conv())
        else:
            return pt

```

Here `argn_conv(i, cv)` applies conversion `cv` to the i th argument of a term $f x_1 \dots x_n$, where f is not a combination, and `rewr_conv(s, conds=None)` is the rewrite conversion using the theorem with name `s`, with optional keyword argument `conds` giving a list of proof terms for discharging assumptions of the theorem.

4.3 Evaluation of inductive predicates

Another common task in proof automation is application of theorems in forward and backward directions. We illustrate this using an example about evaluation of inductive predicates.

Define a datatype for arithmetic expressions as follows:

datatype *aexp* = *N* (*n* :: *nat*) / *V* (*x* :: *nat*) / *Plus* (*a1* :: *aexp*) (*a2* :: *aexp*) /
Times (*c1* :: *aexp*) (*c2* :: *aexp*)

Evaluation of arithmetic expressions on a state *s* can be defined as an inductive predicate (see also [19, Chapter Imp]).

inductive *avalI* :: (*nat* \Rightarrow *nat*) \Rightarrow *aexp* \Rightarrow *nat* \Rightarrow *bool* **where**
avalI_const: *avalI* *s* (*N* *n*) *n*
avalI_var: *avalI* *s* (*V* *x*) (*s* *x*)
avalI_plus: *avalI* *s* *a1* *n1* \longrightarrow *avalI* *s* *a2* *n2* \longrightarrow *avalI* *s* (*Plus* *a1* *a2*) (*n1* + *n2*)
avalI_times: *avalI* *s* *a1* *n1* \longrightarrow *avalI* *s* *a2* *n2* \longrightarrow *avalI* *s* (*Times* *a1* *a2*) (*n1* * *n2*)

We now consider the following problem: given a state *s* expressed as $(\lambda x. 0)(a_1 := b_1, \dots, a_n := b_n)$ and a concrete expression *t*, prove a theorem of the form *avalI* *s* *t* *n*, where *n* is a constant. The basic idea is to “evaluate” *t* on *s* recursively, using introduction rules for *avalI* to obtain the evaluation of each construct in *aexp*, and using evaluation of function updates and arithmetic on natural numbers to simplify the results. The Python code for achieving this is as follows.

```
def get_avalI_th(self, thy, s, t):
    # Returns a proof for avalI s t n, where n is a constant.
    def helper(t):
        if t.head == N:
            n, = t.args
            return apply_theorem(thy, "avalI_const", concl=avalI(s, N(n), n))
        elif t.head == V:
            x, = t.args
            pt = apply_theorem(thy, "avalI_var", concl=avalI(s, V(x), s(x)))
            return pt.on_arg(thy, function.fun_upd_eval_conv())
        elif t.head == Plus:
            a1, a2 = t.args
            pt = apply_theorem(thy, "avalI_plus", helper(a1), helper(a2))
            return pt.on_arg(thy, nat.nat_conv())
        elif t.head == Times:
            a1, a2 = t.args
            pt = apply_theorem(thy, "avalI_times", helper(a1), helper(a2))
            return pt.on_arg(thy, nat.nat_conv())
    return helper(t)
```

This program uses the function `apply_theorem(thy, s, *prevs, concl=None)`. This function takes as arguments the current theory, the name of a theorem, and a list of proof terms discharging assumptions of the theorem. It also takes an optional keyword argument `concl` for the expected conclusion. The function performs first-order pattern matching of the inputs with the assumptions and conclusion of the theorem, and applies the theorem if the matching succeeds, returning the proof term showing the conclusion of the theorem.

A more complex situation is where the automation need to reduce the current proof goal to several other goals, to be solved by other means. A canonical example is verification condition generation. One way to realize this is to store the new goals in the antecedent part of the theorem (left of the sequent sign), using `ProofTerm.assume(A)` to generate the sequent $A \vdash A$. The example of verification condition generation is given in the next section.

5 Case study: a simple imperative language

We now put many of the ideas in previous sections together in one case study about a simple imperative language. For the basic definitions, we mostly follow the presentation in [16]. The aim of this case study is to show how user-defined proof automation, use of external SMT solvers, and custom parsing functions can be rapidly put together to build a verification tool based on holpy.

The imperative language specifies programs acting on a state of type $'a$. The syntax of the language is given as follows.

```
datatype 'a com =
  Basic (f :: 'a  $\Rightarrow$  'a)
  Seq (c1 :: 'a com) (c2 :: 'a com)
  Cond (b :: a  $\Rightarrow$  bool) (c1 :: 'a com) (c2 :: 'a com)
  While (b :: 'a  $\Rightarrow$  bool) (I :: 'a  $\Rightarrow$  bool) (c :: 'a com)
```

Here we assume the invariant is always provided for the while loop. For applications where the invariant is unnecessary, it can be set to $\lambda s. \text{true}$.

The big-step operational semantics of the language is specified by the following inductive predicate:

```
inductive Sem :: 'a com  $\Rightarrow$  'a  $\Rightarrow$  'a  $\Rightarrow$  bool where
  Sem_basic: Sem (Basic f) s (f s)
  Sem_seq: Sem c1 s s3  $\longrightarrow$  Sem c2 s3 s2  $\longrightarrow$  Sem (Seq c1 c2) s s2
  Sem_if1: b s  $\longrightarrow$  Sem c1 s s2  $\longrightarrow$  Sem (Cond b c1 c2) s s2
  Sem_if2:  $\neg$ b s  $\longrightarrow$  Sem c2 s s2  $\longrightarrow$  Sem (Cond b c1 c2) s s2
  Sem_while_skip:  $\neg$ b s  $\longrightarrow$  Sem (While b I c) s s
  Sem_while_loop: b s  $\longrightarrow$  Sem c s s3  $\longrightarrow$  Sem (While b I c) s3 s2  $\longrightarrow$  Sem (While b I c) s s2
```

For our case study, we will always assume the type variable $'a$ is instantiated to $\text{nat} \Rightarrow \text{nat}$. We provide two additional definitions:

```
definition Skip :: 'a com where
  Skip = Basic ( $\lambda s. s$ )
```

```
definition Assign :: 'a  $\Rightarrow$  (('a  $\Rightarrow$  'b)  $\Rightarrow$  'b)  $\Rightarrow$  ('a  $\Rightarrow$  'b) com where
  Assign a b = Basic ( $\lambda s. (s)(a := b s)$ )
```

5.1 Evaluation of operational semantics

Given the operational semantics, we would like to automatically apply the introduction rules to evaluate the result of executing a given program on a given starting state. For example, given the following program:

$$P = \text{While } (\lambda s. \neg(s\ 0 = 3))\ (\lambda s. \text{true})\ (\text{Assign } 0\ (\lambda s. s\ 0 + 1))$$

we would like to automatically prove the theorem

$$\text{Sem } P\ (\lambda x. 0)\ (\lambda x. 0)(0 := 3)$$

We implement this as a function `eval_Sem(thy, com, st)`, which takes as arguments the current theory, the program, and the starting state, and returns a theorem of the form `Sem com st st2` for some ending state `st2`.

The implementation of `eval_Sem` follows the pattern for evaluating `avalI` given in Section 4.3. It begins by finding the right introduction rule to use. If the top-level construct

of *com* is *if* or *while*, this involves evaluating the condition on the current state using an existing conversion. Next, it attempts to construct proof terms satisfying each of the assumptions, which may involve recursive calls to `eval_Sem`. Normalization of function update (defined in Section 4.2) is invoked at appropriate parts of the program. We omit the detailed code for the lack of space.

Note this function is possibly non-terminating (it does not terminate exactly when the given program does not terminate on the given input). However, this is not an issue for us, as this is just a regular Python function with no requirement on termination. Any proof that invokes this function in a non-terminating case would simply cause the proof checker to run forever or run out of memory.

5.2 Program verification using SMT solvers

We now consider Hoare logic and verification condition generation for the language. The basic definitions and theorem are as follows. For reason of space, we only show the case of *Assign*, *Seq*, and *While* commands.

definition $\text{Entail } P \ Q = (\forall s. P \ s \longrightarrow Q \ s)$

definition $\text{Valid } P \ c \ Q = (\forall s. \forall s2. P \ s \longrightarrow \text{Sem } c \ s \ s2 \longrightarrow Q \ s2)$

theorem $\text{pre_rule: Entail } P \ Q \longrightarrow \text{Valid } Q \ c \ R \longrightarrow \text{Valid } P \ c \ R$

theorem $\text{assign_rule: Valid } (\lambda s. P \ ((s)(a := b \ s))) \ (\text{Assign } a \ b) \ P$

theorem $\text{seq_rule: Valid } P \ c1 \ Q \longrightarrow \text{Valid } Q \ c2 \ R \longrightarrow \text{Valid } P \ (\text{Seq } c1 \ c2) \ R$

theorem while_rule:

$\text{Entail } (\lambda s. I \ s \wedge \neg b \ s) \ Q \longrightarrow \text{Valid } (\lambda s. I \ s \wedge b \ s) \ c \ I \longrightarrow \text{Valid } I \ (\text{While } b \ I \ c) \ Q$

The implementation of verification condition generation follows the strategy described at the end of Section 4.3. We write two mutually-recursive functions. For both functions, `thy` is the current theory and `T` is the type '*a*'. The function `compute_wp(thy, T, c, Q)` finds the weakest-precondition *P* of program *c* with postcondition *Q*, and returns a proof term showing $\text{Valid } P \ c \ Q$, possibly with verification conditions in the antecedent of the theorem. The function `vcg(thy, T, goal)` takes a goal of the form $\text{Valid } P \ c \ Q$, and returns a proof term showing the goal, again with verification conditions in the antecedent. The detailed code is as follows.

```
def compute_wp(thy, T, c, Q):
    # Compute the weakest precondition for the given command
    # and postcondition. Returns the validity theorem.
    if c.head.is_const_name("Assign"): # Assign a b
        a, b = c.args
        s = Var("s", T)
        P2 = Term.mk_abs(s, Q(function.mk_fun_upd(s, a, b(s).beta_conv())))
        return apply_theorem(thy, "assign_rule", inst={"b": b},
                              concl=Valid(T)(P2, c, Q))
    elif c.head.is_const_name("Seq"): # Seq c1 c2
        c1, c2 = c.args
        wp1 = compute_wp(thy, T, c2, Q) # Valid Q' c2 Q
        wp2 = compute_wp(thy, T, c1, wp1.prop.args[0]) # Valid Q'' c1 Q'
        return apply_theorem(thy, "seq_rule", wp2, wp1)
    elif c.head.is_const_name("While"): # While b I c
        _, I, _ = c.args
        pt = apply_theorem(thy, "while_rule", concl=Valid(T)(I, c, Q))
        pt0 = ProofTerm.assume(pt.assums[0])
        pt1 = vcg(thy, T, pt.assums[1])
        return ProofTerm.implies_elim(pt, pt0, pt1)

def vcg(thy, T, goal):
    # Compute the verification conditions for the goal.
```

```

P, c, Q = goal.args
pt = compute_wp(thy, T, c, Q)
entail_P = ProofTerm.assume(Entail(T)(P, pt.prop.args[0]))
return apply_theorem(thy, "pre_rule", entail_P, pt)

```

In this example, we used `is_const_name` followed by Python’s multiple assignment syntax to emulate pattern matching in ML-like languages, with little loss in readability. Verification condition generation can be packaged into a macro, which performs some cleanup after calling `vcg`, including moving antecedents (`pt.hyps`) to the right of the sequent as implications, and simplifying the verification conditions.

```

class vcg_macro(ProofTermMacro):
    # Compute the verification conditions for a hoare triple, then
    # normalizes the verification conditions.
    def get_proof_term(self, thy, goal, pts):
        f, (P, c, Q) = goal.strip_comb()
        T = Q.get_type().domain_type()
        pt = vcg(thy, T, goal)
        for A in reversed(pt.hyps):
            pt = ProofTerm.implies_intr(A, pt)
        return pt.on_assums(thy, rew_conv("Entail_def"),
                           top_conv(beta_conv()),
                           top_conv(function.fun_upd_eval_conv()))

```

In many program verification tools, verification condition generation is followed immediately by solving the verification conditions using SMT solvers. This is simple to implement within our framework. We use the Python frontend [2] for the SMT solver Z3 [6]. Calls to Z3 is packaged as the macro `z3`. This macro takes a goal statement as the argument (with no input theorems). If Z3 is able to solve the goal, the macro succeeds with the goal as the output theorem. Otherwise the macro raises an exception. The following function combines verification condition generation with solving by Z3, returning a proof term for the input Hoare triple.

```

def vcg_solve(thy, goal):
    # Compute the verification conditions for a hoare triple, then
    # solves the verification conditions using Z3.
    pt = ProofTermDeriv("vcg", thy, goal, [])
    vc_pt = [ProofTermDeriv("z3", thy, vc, []) for vc in pt.assums]
    return ProofTerm.implies_elim(pt, *vc_pt)

```

5.3 Parsing input problems

For realistic applications, we would like to work with programs in its original syntax, rather than the converted HOL terms. Proof assistants such as Isabelle allow the definition of custom parsers in the ML language. For our system, we can directly use parser libraries in Python to implement this functionality. For the parsing of programs written in our imperative language, we use the Lark parser [2], a standalone parsing library in Python. The same parser is also used in our project to parse the HOL terms.

Lark is a parser-generator. Given the syntax of the language written in BNF form, it produces the parsing function for the language. The parsing function produces the abstract syntax tree, which can be further processed into the target data type. This allows parsers to be implemented rapidly for a wide range of languages. For example, with a standard definition of the syntax of the language, the generated function is able to parse the string

```
while (a != 3) {b := b + 5; a := a + 1}
```

into the HOL term

While ($\lambda s. \neg s\ 0 = 3$) ($\lambda s. \text{true}$) (*Seq* (*Assign 1* ($\lambda s. s\ 1 + 5$)) (*Assign 0* ($\lambda s. s\ 0 + 1$)))

where a and b are considered to be shorthand for $s\ 0$ and $s\ 1$, respectively.

The parser, evaluation of operational semantics, and program verification using SMT solvers can be combined together into a small application based on holpy. This application reads input problems stored in a JSON format (different from the JSON format for theory files), and outputs solutions in the format for theory files. For example, the following input contains one problem on checking the evaluation of operational semantics, and one problem on program verification.

```
{
  "name": "test",
  "content": [
    {
      "ty": "eval",
      "com": "while (a != 3) {b := b + 5; a := a + 1}",
      "init": {},
      "final": {"a": 3, "b": 15}
    },
    {
      "ty": "vcg",
      "com": "while (a != A) [b == a * B] {b := b + B; a := a + 1}",
      "pre": "a == 0 & b == 0",
      "post": "b == A * B"
    }
  ]
}
```

From this input, the application invokes the corresponding proof automation, and outputs the following theory file (some details are omitted):

```
{
  "name": "hoare_test_output"
  "imports": ["hoare"],
  "content": [
    {
      "name": "eval0", "ty": "thm",
      "prop": "Sem ... (%x. 0) ((%x. 0) (0 := 3, 1 := 15))",
      "proof": [{"id": "0", "rule": "eval_Sem", "prevs": [], ...}],
      ...
    },
    {
      "name": "vcg0", "ty": "thm",
      "prop": "Valid (%s. s 0 = 0 & s 1 = 0) ... (%s. s 1 = A * B)",
      "proof": [
        {"id": "0", "rule": "vcg", ...},
        {"id": "1", "rule": "z3", ...},
        {"id": "2", "rule": "implies_elim", ...},
        {"id": "3", "rule": "z3", ...},
        {"id": "4", "rule": "implies_elim", ...},
        {"id": "5", "rule": "z3", ...},
        {"id": "6", "rule": "implies_elim", ...}
      ],
      ...
    }
  ],
}
```

This theory file can then be checked by a proof checker just like any other theory (with `z3` as a trusted macro). Note the file imports the theory `hoare`, and the proofs in the theory, once expanded, do involve theorems in `hoare` (as well as earlier imported theories). Hence, the proof checker is able to check the connection between the two theories, and verify the proof as a whole.

6 Related work

Apart from the new concepts proposed in this paper, the design of holpy is largely based on that of Isabelle [17]. Many choices in the design, including the use of higher-order logic, structure of terms, syntax for inductive definitions, conversion combinators, or even the typesetting of HOL terms used in this paper, are taken from there. In addition, the author examined the design of HOL Light [13] and HOL4 [1] during this research.

Lean [7] already proposed the use of macros to shorten proof terms. However, this functionality does not appear to be widely used in user-defined theories. The virtual machine for Lean evaluates operations on natural numbers, integers, and arrays directly using C++ functions, rather than within the logic, resulting in a large speedup in many applications [9]. The main difference in our work is that definition of macros is easily accessible and widely applied at the user level. We also demonstrate the use of macros in logical foundations without explicit Curry-Howard correspondence.

OpenTheory [14] and Dedukti [5] both provide a universal language for representing theories in a very general logic, at least in part with the aim to allow communication between different proof assistants. While we also provide a common format for theories, our aim is different. Our common format is based on a relatively simple logic. Rather than aiming for interoperability with other proof assistants, we aim to allow many different applications, including user interfaces, to work on the same base library. In this way, we do not have to worry about compatibility of definitions of basic concepts. The use of macros also mean that the common format is able to scale to very large proofs.

Languages for defining proof automation is an active area of research. Lean’s metaprogramming language [9] allows users to define automation in Lean itself. Another research direction is to add typing to tactic languages [22, 24]. Recent efforts to implement proof assistants in imperative languages include Lean (implemented in C++), and Platzer’s work on Orbital [20] and KeYmaera/KeYmaera X [21, 11] for reasoning about hybrid systems (implemented in Java/Scala).

Many of the ideas in the current work arose from the author’s previous work on the auto2 prover [23]. In particular, the definition of macros is similar to that of proof steps in the earlier work. The style of programming proof automation based on building proof terms is also already present there.

7 Conclusion

In this paper, we presented three inter-connected ideas for the design of proof assistants: pervasive use of macros to limit the size of proof terms, a foundational format for theory files, and programming paradigms for implementing proof automation in an imperative language. The core ideas are implemented in a prototype proof assistant called holpy. We used this prototype to demonstrate our API for implementing proof automation in Python, and to present a case study about a simple imperative language.

In the immediate future, we plan to finish some left-over tasks from developing the proof assistant. This includes a standard, general-purpose user interface, foundational definition of inductive datatypes, and a library of basic concepts in mathematics. After this, we plan to explore applications in program verification, as well as verified computation in calculus and linear algebra, taking advantage of the extensibility of the system in terms of the design of user interface and proof automation.

References

- 1 The HOL 4 system. <http://hol.sourceforge.net/>.
- 2 z3-solver. <https://pypi.org/project/z3-solver/>.
- 3 Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development - Coq'Art: The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.
- 4 Julian Biendarra, Jasmin Christian Blanchette, Aymeric Bouzy, Martin Desharnais, Mathias Fleury, Johannes Hölzl, Ondrej Kuncar, Andreas Lochbihler, Fabian Meier, Lorenz Panny, Andrei Popescu, Christian Sternagel, René Thiemann, and Dmitriy Traytel. Foundational (co)datatypes and (co)recursion for higher-order logic. In *Frontiers of Combining Systems - 11th International Symposium, FroCoS 2017, Brasília, Brazil, September 27-29, 2017, Proceedings*, pages 3–21, 2017.
- 5 Raphaël Cauderlier and Catherine Dubois. FoCaLiZe and Dedukti to the rescue for proof interoperability. In *Interactive Theorem Proving - 8th International Conference, ITP 2017, Brasília, Brazil, September 26-29, 2017, Proceedings*, pages 131–147, 2017.
- 6 Leonardo Mendonça de Moura and Nikolaj Bjørner. Z3: an efficient SMT solver. In *Tools and Algorithms for the Construction and Analysis of Systems, 14th International Conference, TACAS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008. Proceedings*, pages 337–340, 2008.
- 7 Leonardo Mendonça de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. The Lean theorem prover (system description). In *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*, pages 378–388, 2015.
- 8 David Delahaye. A tactic language for the system Coq. In *Logic for Programming and Automated Reasoning, 7th International Conference, LPAR 2000, Reunion Island, France, November 11-12, 2000, Proceedings*, pages 85–95, 2000.
- 9 Gabriel Ebner, Sebastian Ullrich, Jared Roesch, Jeremy Avigad, and Leonardo de Moura. A metaprogramming framework for formal verification. *PACMPL*, 1(ICFP):34:1–34:29, 2017.
- 10 The JSON data interchange syntax. <http://ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf>, 12 2017.
- 11 Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völpl, and André Platzer. KeYmaera X: an axiomatic tactical theorem prover for hybrid systems. In *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*, pages 527–538, 2015.
- 12 Michael J. C. Gordon. Set theory, higher order logic or both? In *Theorem Proving in Higher Order Logics, 9th International Conference, TPHOLs'96, Turku, Finland, August 26-30, 1996, Proceedings*, pages 191–201, 1996.
- 13 John Harrison. HOL light: An overview. In *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17-20, 2009. Proceedings*, pages 60–66, 2009.
- 14 Joe Hurd. The OpenTheory standard theory library. In *NASA Formal Methods - Third International Symposium, NFM 2011, Pasadena, CA, USA, April 18-20, 2011. Proceedings*, pages 177–191, 2011.
- 15 Daniel Matichuk, Toby C. Murray, and Makarius Wenzel. Eisbach: A proof method language for Isabelle. *J. Autom. Reasoning*, 56(3):261–282, 2016.
- 16 Tobias Nipkow and Gerwin Klein. *Concrete Semantics: With Isabelle/HOL*. Springer, 2014.
- 17 Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer, 2002.
- 18 Steven Obua. Partizan games in Isabelle/HOLZF. In *Theoretical Aspects of Computing - ICTAC 2006, Third International Colloquium, Tunis, Tunisia, November 20-24, 2006, Proceedings*, pages 272–286, 2006.

- 19 Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hrițcu, Vilhelm Sjöberg, and Brent Yorgey. Software foundations volume 1: Logical foundations. URL: <https://softwarefoundations.cis.upenn.edu/lf-current/index.html>.
- 20 André Platzer. Orbital library. <http://symbolaris.com/orbital/>.
- 21 André Platzer and Jan-David Quesel. KeYmaera: A hybrid theorem prover for hybrid systems (system description). In *Automated Reasoning, 4th International Joint Conference, IJCAR 2008, Sydney, Australia, August 12-15, 2008, Proceedings*, pages 171–178, 2008.
- 22 Antonis Stampoulis and Zhong Shao. VeriML: typed computation of logical terms inside a language with effects. In *Proceeding of the 15th ACM SIGPLAN international conference on Functional programming, ICFP 2010, Baltimore, Maryland, USA, September 27-29, 2010*, pages 333–344, 2010.
- 23 Bohua Zhan. Auto2, A saturation-based heuristic prover for higher-order logic. In *Interactive Theorem Proving - 7th International Conference, ITP 2016, Nancy, France, August 22-25, 2016, Proceedings*, pages 441–456, 2016.
- 24 Beta Ziliani, Derek Dreyer, Neelakantan R. Krishnaswami, Aleksandar Nanevski, and Viktor Vafeiadis. Mtac: A monad for typed tactic programming in Coq. *J. Funct. Program.*, 25, 2015.