The Functional Correspondence Applied: An Implementation of a Semantics Transformer

(...)

Maciej Buszka

Praca magisterska

Promotor: dr hab. Dariusz Biernacki

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

23 czerwca 2020

Abstract

. . .

. . .

Contents

Chapter 1

Introduction

What is the meaning of a given computer program?

The field of formal semantics of programming languages seeks to provide tools to answer such a question. Denotational semantics [1] allow one to relate programs to mathematical objects which describe their behavior. Operational semantics provide means to characterize evaluation of programs by building a relation between terms and final values in case of natural (aka big-step) semantics [2] and pretty-big-step semantics [3]; by defining a step-by-step transition system on program terms in case of structured operational (aka small-step) semantics [4] and reduction semantics [5]; or by specifying an abstract machine with a set of states and a transition relation between those states. All of these semantic formats enable systematic definition of programming languages but differ in style and type of reasoning they allow as well as in their limitations.

Diversity of formats of operational semantics and trade-offs they impose often necessitates specifying the semantics of a calculus in more than one format, e.g., one might use natural semantics in order to show a program transformation correct but will have to also specify small-step operational semantics for proofs of type safety and characterization of non-terminating computations. Of course when multiple specifications are provided one should also prove them compatible. As it implies serious amount of work, it comes as no surprise that research has been conducted on means of mechanizing or even automating this task. In their paper [6] Poulsen and Mosses show an automatic procedure for obtaining pretty-big-step semantics from small-step ones. The most recent result is a 2019 paper by Vesely and Fisher [7] who describe an automatic transformation in other direction: from big-step semantics into its small-step counterpart.

Another line of work is that of constructing abstract machines. Starting with Landin's SECD machine [8] for λ-calculus, many abstract machines have been proposed for various evaluation strategies and with differing assumptions on capabilities of the runtime (e.g., substitution vs environments). Notable work includes: Kriv-

ine's machine [9] for call-by-name reduction, Felleisen and Friedman's CEK machine [10] and Crégut's machine [11] for normalization of λ-terms in normal order. Besides equipping existing calculi with an abstract machine, novel developments also come with both higher-level operational semantics and a machine, e.g. in the novel field of algebraic effects [12, 13]. Manual construction of an abstract machine for a given evaluation discipline can be challenging and also requires a proof of compatibility w.r.t the source semantics, therefore methods for deriving the machines have been developed. Danvy and Nielsen's refocusing framework [14] gave raise to an automatic procedure for transforming reduction semantics into an abstract machine [15, 16]. Ager shows a mechanical method of deriving abstract machines from L-attributed natural semantics [17] while Hannan and Miller present derivations of abstract machines for call-by-value and call-by-name reduction strategies [18] via program transformations. Last but not least, Danvy et al. introduced the functional correspondence between evaluators and abstract machines [19] which appears to be the most successful technique.

In order to describe the functional correspondence in greater detail let us first turn to another approach to defining a programming language: providing an interpreter for the language in question (which I will call the *object*-language) written in another language (to which I will refer as the *meta*-language). These definitional interpreters [20] can be placed on a spectrum from most abstract to most explicit. At the abstract end lie the concise meta-circular interpreters which use meta-language constructs to interpret same constructs in object-language (e.g., using anonymous functions to model functional values, using conditionals for *if* expressions). In the middle one might place various evaluators with some constructs interpreted by simpler language features (e.g., with environments represented as lists or dictionaries instead of functions) but still relying on the evaluation order of the meta-language. The explicit end is occupied by first-order machine-like interpreters which use an encoding of a stack for handling control-flow of the object-language.

In his seminal paper [20] Reynolds introduces two techniques: transformation to continuation-passing style and defunctionalization, which allow one to transform high-level definitional interpreters into lower-level ones. This connection between evaluators on different levels of abstraction has later been studied by Danvy et al.[19] who use it to relate several abstract machines for λ-calculus with interpreters embodying their evaluation strategies and called it the functional correspondence. The technique has proven to be very useful for deriving a correct-by-construction abstract machine given an evaluator in a diverse set of languages and calculi including normal and applicative order λ-calculus evaluation [19] and normalization [21], call-by-need strategy [22] and *Haskell*'s STG language [23], logic engine [24], delimited control [25], computational effects [26], object-oriented calculi [27] and *Coq*'s tactic language [28]. Besides the breadth of applications the functional correspondence proved able to relate semantic formats from opposing ends of the abstraction spectrum, e.g., a meta-circular interpreter encoding call-by-value denotational semantics for λ-calculus

with CEK machine or a normal order normalization function with a strong version of Krivine's machine [21]. Despite these successes and its mechanical nature, the functional correspondence has not yet been transformed into a working tool which would perform the derivation automatically.

Therefore it was my goal to give an algorithmic presentation of the functional correspondence and implement this algorithm in order to build a semantics transformer. In this thesis I describe all steps required to successfully convert the human-aided derivation into a computer algorithm for transforming evaluators into a representation of an abstract machine. In particular I characterize the control-flow analysis as the basis for both selective continuation-passing style transformation and partial defunctionalization. In order to obtain correct, useful and computable analysis I employ the abstracting abstract machines methodology [29] which allows for deriving the analysis from an abstract machine for the meta-language. This derivation proved very capable in handling the non-trivial language containing records, anonymous functions and pattern matching. The resulting analysis enables automatic transformation of user specified parts of the interpreter as opposed to whole-program-only transformations. I implemented the algorithm in the *Haskell* programming language giving raise to a tool — `semt` — performing the transformation. I evaluated the performance of the tool on multiple interpreters for a diverse set of programming language calculi.

The rest of this thesis is structured as follows: In the remainder of this chapter I introduce the *Interpreter Definition Language* which is the meta-language accepted by the transformer and will be used in example evaluators throughout the thesis; I also compare the semantics formats with styles of interpreters to which they correspond. In Chapter 2, I describe the functional correspondence and its constituents. In Chapter 3, I show the algorithmic characterization of the correspondence. In Chapter 4, I showcase the performance of the tool on a selection of case studies. In Chapter 5, I discuss related work, point at future avenues for improvement and conclude. Appendices contain user's and developer's manual for the semantic transformer.

I assume that the reader is familiar with λ-calculus and its semantics (both normal (call-by-name) and applicative (call-by-value) order reduction). Familiarity with formal semantics of programming languages (both denotational and operational) is also assumed although not strictly required for understanding of the main subject of this thesis. The reader should also be experienced in using a higher-order functional language with pattern matching.

1.1 Interpreter Definition Language

The *Interpreter Definition Language* or *IDL* is the meta-language used by `semt` – a semantic transformer. It is a purely functional, higher-order, dynamically (strongly)

```
(def-data Term
  String
  {Abs String Term}
  {App Term Term})

(def init (x) (error "empty environment"))

(def extend (env y v)
  (fun (x) (if (eq? x y) v (env x))))

(def eval (env term)
  (match e
    ([String x] (env x))
    ({Abs x body} (fun (v) (eval (extend env x v) body)))
    ({App fn arg} ((eval env fn) (eval env arg)))))

(def main ([Term term]) (eval init term))
```

Figure 1.1: A meta-circular interpreter for λ-calculus

typed language with strict evaluation order. It features named records and pattern matching which allow for convenient modelling of abstract syntax of the object-language as well as base types of integers, booleans and strings. The concrete syntax is in fully parenthesized form and the programs can be embedded in a `Racket` source file using the provided library with syntax definitions. A more detailed introduction along with usage instructions is available in Appendix A.

As shown in Figure 1.1 a typical interpreter definition consists of several top-level functions which may be mutually recursive. The `def-data` form introduces a datatype definition. In our case it defines a type for terms of λ-calculus – `Term`. It is a union of three types: `String`s representing variables of λ-calculus; records with label `Abs` and two fields of types `String` and `Term` representing abstractions; and records labeled `App` which contain two `Term`s and represent applications. A datatype definition may refer to itself, other previously defined datatypes and records and the base types of `String`, `Integer`, `Boolean` and `Any`. The `main` function is treated as an entry point for the evaluator and must have its arguments annotated with their type.

The `match` expression matches an expression against a list of patterns. Patterns may be variables (which will be bound to the value being matched), wildcards `_`, base type patterns, e.g., `[String x]` or record patterns, e.g., `{Abs x body}`. The `fun` form introduces anonymous function, `error "..."` stops execution and signals the error. Finally, application of a function is written as in *Scheme*, i.e., as a list of expressions (e.g., `(eval init term)`).

1.2 Semantic Formats

In this thesis I consider three widely recognized semantic formats: denotational semantics, big-step operational semantics and abstract machines. These formats make different trade-offs with respect to conciseness of definition, explicitness of specification of behavior of the object-language and power or degree of complication of the meta-language. I assume familiarity with these formats and the rest of this section should be treated as a reminder rather than an introduction. Nevertheless I will explain how these mathematical formalisms correspond to evaluators in a functional programming language.

Denotational Semantics

In this format one has to define a mapping from program terms into meta-language objects (usually functions) which *denote* those terms – that is they specify their behavior [1]. This mapping is usually required to be compositional – i.e. the denotation of complex term is a composition of denotations of its sub-terms. Denotational semantics are considered to be the most abstract way to specify behavior of programs and can lead to very concise definitions. The drawback is that interesting language features such as loops and recursion require more complex mathematical theories to describe the denotations, in particular domain theory and continuous functions. In terms of interpreters, the denotational semantics usually correspond to evaluators that heavily reuse features of the meta-language in order to define the same features of object-language, e.g., using anonymous functions to model functional values, using conditionals for if expressions, etc. This style of interpreters is sometimes called *meta-circular* due to the recursive nature of the language definition. On the one hand these definitional interpreters allow for intuitive understanding of object-language's semantics given familiarity with meta-language. On the other hand, the formal connection of such an interpreter with the denotational semantics requires formal definition of meta-language and in particular understanding of the domain in which denotations of meta-language programs live. The evaluator of Figure 1.1 is an example of the meta-circular approach. The λ-abstractions of object-language are represented directly as functions in meta-language which use denotations of lambda's bodies in extended environment. The `eval` function is compositional – the denotation of object level application is an application of denotations of function and argument expressions.

Big-step Operational Semantics

The format of big-step operational semantics [2], also known as natural semantics allows for specification of behavior of programs using inference rules. These rules usually decompose terms syntactically and give rise to a relation between programs and

```
(def-data AExpr
  String
  ...)
(def-data BExpr ...)
(def-data Cmd
  {Skip}
  {Assign String AExpr}
  {If BExpr Cmd Cmd}
  {Seq Cmd Cmd}
  {While BExpr Cmd})

(def init-state (var) 0)
(def update-state (tgt val state) ...)

(def aval (state aexpr) ...) ;; valuate arithmetic expression
(def bval (state bexpr) ...) ;; valuate boolean expression

(def eval (state cmd)
  (match cmd
    ({Skip} state)
    ({Assign var aexpr}
      (update-state var (aval state aexpr) state))
    ({If cond then else}
      (if (bval state cond)
        (eval state then)
        (eval state else)))
    ({Seq cmd1 cmd2}
      (let state (eval state cmd1))
      (eval state cmd2))
    ({While cond cmd}
      (if (bval state cond)
        (eval (eval state cmd) {While cond cmd})
        state))))

(def main ([Cmd cmd])
  (eval init-state cmd))
```

Figure 1.2: An interpreter for *IMP* in the style of natural semantics

values to which they evaluate. The fact of evaluation of a program to a value is proven by showing a derivation tree built using the inference rules. Non-terminating programs therefore have no derivation tree which makes this semantic format ill-suited

to describing divergent or infinite computations. The interpreters which correspond to big-step operational semantics usually have a form of recursive functions that are not necessarily compositional. The natural semantics may be non-deterministic and relate a program with many results. When turning nondeterministic semantics into an evaluator (in a deterministic programming language) one has to either change the formal semantics or model the nondeterminism explicitly. Let us now turn to a simple interpreter embodying the natural semantics for an imperative language *IMP* shown in Figure 1.2.

Datatypes `AExpr`, `BExpr` and `Cmd` describe abstract syntax of arithmetic expressions, boolean expressions and commands. The expressions are pure, that is, evaluating them does not affect the state. The state is a function mapping variables represented as `String`s to numbers, initially set to `0` for every variable. Functions `aval` and `bval` valuate arithmetic and boolean expressions in a given state. The function `eval` is a direct translation of big-step operational semantics for *IMP*. It is not compositional in the `While` branch, where `eval` is called recursively on the same command it received.

Abstract Machines

An abstract machine [8] is usually the most explicit definition of semantics of a language with all the details like argument evaluation order, term decomposition, environments and closures specified. It is a format of particular interest as it can very precisely specify the operational properties of the language. Therefore it provides a reasonable cost model of the evaluation and may even serve as a basis of efficient implementation [30].

A machine consists of a set of configurations (tuples), an injection of a program into the initial configuration, an extraction function of a result from the final configuration and a transition relation between configurations. The behavior of the machine then determines the behavior of the programs in object-language. As with big-step operational semantics, an abstract machine may be nondeterministic. Usually elements of the machine-state tuple are simple and first-order, e.g., terms of the object-language, numbers, lists, etc. One way of encoding a deterministic abstract machine in a programming language is to define a function for each subset of machine states with similar structure. The exact configuration is determined by the actual parameters of the function at run-time. The bodies of these (mutually recursive) functions encode the transition function.

Figure 1.3 contains an interpreter corresponding to Krivine's machine [9] performing normal order (call-by-name) reduction of λ-calculus with de Bruijn indices. It uses two stacks: `Continuation` and `Environment`. Both of them contain `Thunks` – not-yet-evaluated terms paired with their environment. The object-language functions are represented as `Closures` – function bodies paired with their environment.

The machine has two classes of states: `eval` and `continue`. The initial configuration is `(eval term {Nil}{Halt})` – i.e. eval with the term of interest and empty stacks. There are four transitions from `eval` configuration. The first two search for the `Thunk` corresponding to the variable (de Bruijn index) in the environment and then evaluate it with old stack but with restored environment. The third transition switches to `continue` configuration with the closure is created by pairing current environment with abstraction's body. The fourth transition pushes a `Thunk` onto continuation stack and begins evaluation of function expression. In `continue` configuration the machine inspects the stack. If it is empty then the computed function `fn` is the final answer which is returned. Otherwise an argument is popped from the stack and the machine switches to `eval`uating the `body` of the function in the restored environment extended with `arg`.

```
(def-data Term
  Integer
  {Abs Term}
  {App Term Term})

(def-struct {Closure body env})
(def-struct {Thunk env term})

(def-data Env
  {Nil}
  {Cons Thunk Env})

(def-data Cont
  {Push Thunk Cont}
  {Halt})

(def eval ([Term term] [Env env] cont)
  (match term
    (0 (match env
         ({Nil} (error "empty env"))
         ({Cons {Thunk env term} _} (eval term env cont))))
    ([Integer n] (eval (- n 1) env cont))
    ({Abs body} (continue cont {Closure body env}))
    ({App fn arg} (eval fn env {Push {Thunk env arg}}))))

(def continue (cont fn)
  (match cont
    ({Push arg cont}
      (let {Closure body env} fn)
      (eval body {Cons arg env} cont))
    ({Halt} fn)))

(def main ([Term term]) (eval term {Nil} {Halt}))
```

Figure 1.3: An encoding of Krivine's machine

Chapter 2

The Functional Correspondence

The functional correspondence between evaluators and abstract machines is a technique for mechanical derivation of an abstract machine from a given evaluator. The technique was first characterized and described in [19] and then later studied in context of various object-languages and their evaluators in [21, 22, 23, 24, 25, 26, 27, 28]. The input of the derivation is an evaluator written in some functional meta-language. It usually corresponds to a variant of denotational semantics (particularly in case of so-called meta-circular interpreters) or big-step operational semantics. The result of the derivation is a collection of mutually tail-recursive, first-order functions in the same meta-language. Program in such a form corresponds to an abstract machine. The different functions (with actual parameters) represent states of the machine, while the function calls specify the transition function.

The derivation consists of two program (in our case interpreter's) transformations: transformation to continuation-passing style and defunctionalization. The first one exposes the control structure of the evaluator; the second replaces function values with first-order data structures and their applications with calls to a first-order global function.

In the remainder of this chapter I will describe those transformations and illustrate their behavior using the running example of an evaluator for λ-calculus from Section 1.1. Let us recall the previously described meta-circular interpreter of Figure 1.1. The variables are represented as `String`s of characters. Since every expression in λ-calculus may only evaluate to a function, the values produced by the interpreter are represented as meta-language functions. The interpreter uses environments represented as partial functions from variables to values to handle binding of values to variables during application. The application in object-language is interpreted using application in meta-language so the defined language inherits call-by-value, left-to-right evaluation order. At the end of this chapter we shall arrive at the CEK machine.

2.1 Continuation-Passing Style

The first step towards building the abstract machine is capturing the control-flow characteristics of the defined language. We are interested in exposing the order in which the sub-expressions are evaluated and how the control is passed from function to function. Additionally, we would like the resulting program to define a transition system so we must require that every function call in the interpreter is a tail-call. It turns out that a program in continuation-passing style (CPS) exactly fits our requirements.

What does it mean for a program to be in CPS? Let us begin by classifying expressions into trivial and serious ones. An expression is trivial if evaluating it always returns a value. Since we cannot in general decide whether an arbitrary expression is trivial we will use a safe approximation: an expression is trivial if it is a variable, a function definition, a primitive operation call or a structure constructor with only trivial expressions as sub-terms. We will only allow applications, match expressions and constructors with trivial sub-expressions. Additionally we would like to consider some expressions trivial due to their interpretation (e.g., environment lookups) even though they are serious. In order to retain ability to build interesting programs, every function will accept an additional argument – a continuation which specifies what should be done next.

The interesting clauses of the algorithm for simple CPS translation of expressions in *IDL* are presented in Figure 2.1. The meta variables are typeset with italics (e.g., k). The pieces of syntax use typewriter font (e.g., `k'`). The function $[\![e]\!]k$ transforms an expression e to continuation-passing-style using expression k as a continuation. Whenever a new variable is introduced by the algorithm we will assume that it is fresh. The variable `x` is translated to application of continuation k to `x`. To translate an anonymous function definition, first a fresh variable `k'` is generated then the body of the function is translated with `k'` as the continuation and finally, the continuation k is applied to the transformed function expression. Function application is transformed by placing all sub-expressions in successively nested functions, with the deepest one actually performing the call with an additional argument – the continuation k. This way the evaluation of arguments is sequenced left-to-right and happens before the application. Translation of the `match` expression requires translating the scrutinee and putting the branches in the continuation. The branches are all transformed using the same continuation k. Finally, during translation of the `error` expression the continuation is discarded since the error halts the execution. The omitted rules for `if` expressions and record creation are similar to `match` expressions and applications respectively.

Figure 2.2 shows the interpreter with body of `eval` translated to CPS using the algorithm of Figure 2.1 and then hand-optimized by reducing administrative redexes. The `eval` function now takes an additional argument `k` – a continuation. The function

$$
\begin{aligned}
[\![\texttt{x}]\!]k &= (k\ \texttt{x}) \\
[\![(\texttt{fun}\ (x \ldots)\ e)]\!]k &= (k\ (\texttt{fun}\ (x \ldots \texttt{k'})\ [\![\texttt{e}]\!]\texttt{k'})) \\
[\![(e_1 \ldots e_n)]\!]k &= [\![e_1]\!]\,(\texttt{fun}\ (\texttt{v}_1)\ [\![e_2]\!]\,(\texttt{fun}\ (v_2) \ldots [\![e_n]\!]k' \ldots) \\
&\quad \text{where } k' = (\texttt{fun}\ (\texttt{v}_n)\ (\texttt{v}_1 \ldots \texttt{v}_n\ k)) \\
[\![(\texttt{match}\ e\ (p\ e) \ldots)]\!]k &= [\![e]\!](\texttt{fun}\ (\texttt{v})\ (\texttt{match}\ \texttt{v}\ ps) \\
&\quad \text{where } ps = (p\ [\![e']\!]k) \ldots
\end{aligned}
$$

Figure 2.1: A call-by-value CPS translation

denoting the object-language lambda expressions also expects a continuation. In both variable and abstraction cases the evaluator now calls the continuation `k` with the computed value: either looked up in the environment in case of a variable or freshly constructed in case of abstractions. The evaluation of applications is now explicitly sequenced. First the expression in function position will be evaluated. It is passed a continuation which will then evaluate the argument. After the argument is computed, the function value will be applied to the argument and the original continuation `k` passed by the caller. The `main` function is kept in direct style as it is the entry point of the evaluator. It calls the `eval` function which expects a continuation so it provides it the identity function. This continuation means that when evaluation is finished it will return the final value.

We can see that after the transformation the evaluation order of the meta-language does not affect the evaluation order of the object-language as every call to the only interesting function `eval` is a tail call. Therefore we have successfully captured control-flow characteristics of the object-language. The evaluator still technically depends on the order of evaluation of *IDL* as environment lookup may fail and it is in a sub-expression position but from the point of view of designing an abstract machine which works with closed terms it is not interesting.

In Section 3.3 we will see a more complex transformation which avoids creating administrative redexes and allows for user defined functions which should be considered trivial.

2.2 Defunctionalization

The second step is the elimination of higher order functions from our interpreter, transforming it into a collection of mutually (tail-)recursive functions – a state machine with the `main` function building initial configuration. There are many approaches to compiling first class functions away but of particular interest to us will

```
(def-data Term ...)

(def eval (env term k)
  (match term
    ([String x] (k (env x)))
    ({Abs x body}
      (k (fun (v k') (eval (extend env x v) body k'))))
    ({App fn arg}
      (eval env fn
        (fun (fn') (eval env arg (fun (v) (fn' v k))))))))

(def extend (env x v) ...)

(def init (x) (error "empty environment"))

(def main ([Term term]) (eval init term (fun (x) x)))
```

Figure 2.2: An interpreter for λ-calculus in CPS

be defunctionalization. It is a global program transformation that replaces each anonymous function definition with a uniquely labeled record which holds the values for function's free variables. Every application of unknown function is replaced with a specific top-level *apply* function which dispatches on the label of the passed record and evaluates the corresponding function's body.

This simple description glosses over many important details. Firstly, we must distinguish between known and unknown function calls as only unknown calls should be transformed. Secondly, we must be able to create records for top-level definitions when they are passed as a first class function, e.g., in the definition of `eval` in the branch for variables we apply an unknown function `env` which may evaluate either to an anonymous function created by `extend` or a top-level function `init`. Lastly, we must somehow know for each application point which functions may be applied. The first two challenges can be solved with a static, syntactic analysis of the interpreter. The other challenge can be solved using control-flow analysis as described in Section 3.4. For the purposes of this example we observe that there are three function spaces with anonymous functions: continuations, representation of abstractions and environments.

Figure 2.3 depicts an overview of defunctionalization procedure with *apply* functions generated according to the template in Figure 2.4. We assume that every definition and expression in program has a unique label and that all generated names and structure labels are fresh. Whenever a top-level function is called the application is transformed into top-level call with the sub-expressions transformed. Any other

$$
\begin{aligned}
[\![(\texttt{f}\ e_1 \ldots e_n)\texttt{@l}]\!] &= (\texttt{f}\ [\![e_1]\!] \ldots [\![e_n]\!]) && \text{when f is top-level} \\
[\![(\ e_1 \ldots e_n)\texttt{@l}]\!] &= (\texttt{apply-l}\ [\![e_1]\!] \ldots [\![e_n]\!]) && \text{otherwise} \\
[\![(\texttt{fun (x ...)}\ e_l)\texttt{@l}]\!] &= \{\texttt{l y ...}\} \\
[\![\texttt{f}]\!] &= \{\texttt{lf}\}
\end{aligned}
$$

Figure 2.3: Defunctionalization algorithm

```
(def apply-l (f x ...)
  (case f
    ({l-1 y-1 ...} e-1)
    ...
    ({l-n y-n ...} e-n)))
```

Figure 2.4: Apply function template

application is transformed into a call to `apply-l` where l is the application's label. Anonymous functions are transformed into a labeled record with the function's free variables as sub-expressions. Finally, references to top-level functions occurring in the program are transformed into labeled records. The template in Figure 2.4 is instantiated as follows:

- `l` is a label of application expression for which `apply-l` is generated
- `l-1` ... `l-n` are labels of functions which may be applied in `l`;
- `x ...` are variables bound by these functions (notice that it requires renaming of bound variables)
- (`y-1 ...`) ... (`y-n ...`) are free variables of these functions
- `e-1` ... `e-n` are already transformed bodies of these functions

It is worth noting that defunctionalization preserves the tail-call property of a program in CPS.

After applying the defunctionalization procedure to functions representing lambda abstractions and to continuations we obtain (again with a bit of manual cleanup) an encoding ot the CEK machine [31] in Figure 2.5. It uses a stack `Cont` (which are defunctionalized continuations) to handle the control-flow and `Closures` (which are defunctionalized lambda abstractions) to represent functions. The environment is left untouched and is still encoded as a partial function. The machine has two classes of states: `eval` and `continue`. In `eval` mode the machine dispatches on the

shape of the term and either switches to `continue` mode when it has found a value (either a variable looked up in the environment or an abstraction) or pushes a new continuation onto the stack and evaluates the expression in function position. The `continue` function is the *apply* function generated by the defunctionalization procedure. In `continue` mode the machine checks the continuation and proceeds accordingly: when it reaches the bottom of the continuation stack `Halt` it returns the final value `val`; when the continuation is `App1` it means that `val` holds the function value which will be applied once `arg` is computed; the stack frame `App2` signifies that `val` holds the computed argument and the machine calls a helper function `apply` (the second generated *apply* function) to unpack the closure in `fn` and evaluate the body of the closure in the extended environment.

```
(def-data Term ...)

(def-data Cont
  {Halt}
  {App1 arg env cont}
  {App2 fn cont})

(def-struct {Closure body env x})

(def init (x) (error "empty environment"))
(def extend (env k v) ...)

(def eval (env term cont)
  (match term
    ([String x] (continue cont (env x)))
    ({Abs x body} (continue cont {Closure body env x}))
    ({App fn arg} (eval env fn {App1 arg env cont}))))

(def apply (fn v cont)
  (let {Fun body env x} fn)
  (eval (extend env x v) body cont))

(def continue (cont val)
  (match cont
    ({Halt} val))
    ({App1 arg env cont} (eval env arg {App2 val cont}))
    ({App2 fn cont} (apply fn val cont)))

(def main ([Term term]) (eval {Init} term {Halt}))
```

Figure 2.5: An encoding of the CEK machine for λ-calculus

Chapter 3

Semantics Transformer

The adaptation of the functional correspondence into a semantics transformer was the main goal of this thesis. Although the two main transformations considered here are widely known, they are not presented in literature in a form directly applicable for the task. As the goal of the algorithm is to produce a definition of an abstract machine, to be read as a source code, care has to be taken to produce readable results. To this end I chose to allow for partial CPS translation, with functions which should be left alone marked with annotations. This approach allows one to specify helper functions whose control-flow is not particularly interesting to capture such as environment lookups. The defunctionalization is usually presented as a manual transformation with human-specified function spaces or in a type directed fashion. Neither of these approaches are satisfying for the purposes of a semantics transformer as the goal is to produce the result automatically and to uncover the operational properties of the evaluator. Additionally I wanted to allow for partial defunctionalization of programs as it permits one to keep some parts of the machine abstract (e.g., functions modelling a heap or an environment). I chose to employ the control-flow analysis to guide partitioning of function spaces as it approximates the runtime behavior of programs. This approach allows for functions of the same type to land in different spaces based on their usage and it performed satisfactory in experiments I have conducted. Finally, as the transformation generates new variables and moves code around we have to keep them readable. To this end I both allow for (optional) program annotations and employ heuristics to guide generation of names for function records, introduced variables and functions.

The abstract syntax of *IDL* is presented in Figure 3.1. The meta-variables x, y, z denote variables; r denote structure (aka record) names; s is used to denote string literals and b is used for all literal values – strings, integers and booleans. The meta-variable tp is used in pattern matches which check whether a value is one of the primitive types. The patterns are referred to with variable p and may be a variable, a literal value, a wildcard, a record pattern or a type test. Terms are denoted with variable t and are one of variable, literal value, anonymous function, application,

$$
\begin{array}{rcl}
x, y, z \in Var & r \in StructName \quad s \in String & b \in Int \cup Boolean \cup String \\
Tp \ni tp & ::= & \texttt{String} \mid \texttt{Integer} \mid \texttt{Boolean} \\
Pattern \ni p & ::= & x \mid b \mid \_ \mid \{r\ p \ldots\} \mid [tp\ x] \\
Term \ni t & ::= & x \mid b \mid (\texttt{fun}\ (x \ldots)\ t) \mid (t\ t \ldots) \mid \{r\ t \ldots\} \\
 & & \mid (\texttt{let}\ p\ t\ t) \mid (\texttt{match}\ t\ (p\ t) \ldots) \mid (\texttt{error}\ s) \\
FunDef \ni fd & ::= & (\texttt{def}\ x\ (x \ldots)\ t) \\
StructDef \ni sd & ::= & (\texttt{def-struct}\ \{r\ x \ldots\})
\end{array}
$$

Figure 3.1: Abstract syntax of *IDL*

record constructor, let binding (which may destructure bound term with a pattern), pattern match or an error expression.

The transformation described in this chapter consists of three main stages: translation to administrative normal form, selective translation to continuation-passing style and selective defunctionalization. After defunctionalization the program is in the desired form of an abstract machine. The last step taken by the transformer is inlining of administrative let-bindings introduced by previous steps in order to obtain more readable results. In the remainder of this chapter I will describe the three main stages of the transformation and the algorithm used to compute the control-flow analysis.

3.1 Administrative Normal Form

The administrative normal form (ANF) [32] is an intermediate representation for functional languages in which all intermediate results are let-bound to names. This shape greatly simplifies later transformations as programs do not have complicated sub-expressions. From operational point of view, the only place where a continuation is grown when evaluating program in ANF is a let-binding. This property ensures that a program in ANF is also much easier to evaluate using an abstract machine which will be taken advantage of in Section 3.2. The abstract syntax of terms in ANF and an algorithm for transforming *IDL* programs into such form is presented in Figure 3.2. The terms are partitioned into three levels: variables, commands and expressions. Commands c extend variables with values – base literals, record constructors (with variables as sub-terms) and abstractions (whose bodies are in ANF); and with redexes like applications of variables and match expressions (which match on variable and have branches in ANF). Expressions e in ANF have the shape of a possibly empty sequence of let-bindings ending with either an error term or a command.

The $[\![\cdot]\!]\,\cdot$ function, written in CPS, is the main transformation function. Its arguments are term to be transformed and a meta-continuation (i.e. a continuation in meta-language) which will be called to obtain the term for the rest of transformed

$$
\begin{array}{rl}
\mathit{Command} \ni c & ::= x \mid b \mid (\texttt{fun}\ (x \ldots)\ e) \mid (x\ x \ldots) \\
 & \mid \{r\ x \ldots\} \mid (\texttt{match}\ x\ (p\ e) \ldots) \\
\mathit{Expression} \ni e & ::= c \mid (\texttt{let}\ p\ c\ e) \mid (\texttt{error}\ s)
\end{array}
$$

$$
\begin{array}{rl}
[\![\cdot]\!]\ \cdot & : \mathit{Expr} \times (\mathit{Com} \to \mathit{Anf}) \to \mathit{Anf} \\
[\![a]\!]\ k & = k\, a \\
[\![(\texttt{fun}\ (x \ldots) e)]\!]\ k & = k\, (\texttt{fun}\ (x \ldots)\ [\![e]\!]\, id) \\
[\![(e_f\ e_{arg} \ldots)]\!]\ k & = [\![e_f]\!]\, [\lambda a_f.\, [\![e_{arg} \ldots]\!]_s\, \lambda(a_{arg} \ldots).k\, (a_f\ a_{arg} \ldots)]_a \\
[\![(\texttt{let}\ x\ e_1\ e_2)]\!]\ k & = [\![e_1]\!]\, \lambda e_1'.(\texttt{let}\ x\ e_1\ [\![e_2]\!]\, k) \\
[\![\{r\ e \ldots\}]\!]\ k & = [\![e \ldots]\!]_s\, \lambda(a \ldots).k\, \{r\ a \ldots\} \\
[\![(\texttt{match}\ e (p\ e_b))]\!]\ k & = [\![e]\!]\, [\lambda e'.k\, (\texttt{match}\ e\ (p\ [\![e_b]\!]\, id)]_a \\
[\![(\texttt{error}\ s)]\!]\ \_ & = (\texttt{error}\ s)
\end{array}
$$

$$
\begin{array}{rl}
[\cdot]_a\ \cdot & : (\mathit{Atomic} \to \mathit{Anf}) \to \mathit{Com} \to \mathit{Anf} \\
[k]_a\ a & = k\, a \\
[k]_a\ c & = (\texttt{let}\ x\ c\ (k\, x))
\end{array}
$$

$$
\begin{array}{rl}
[\![\cdot]\!]_s\ \cdot & : \mathit{Expr}^* \times (\mathit{Atomic}^* \to \mathit{Anf}) \to \mathit{Anf} \\
[\![e \ldots]\!]_s\ k & = [\![e \ldots]\!]_s^{\epsilon} \\
[\![\epsilon]\!]_s^{a \ldots}\ k & = k\, (a \ldots) \\
[\![e\, e_r \ldots]\!]_s^{a_{acc} \ldots}\ k & = [\![e]\!]\, [\lambda a.\, [\![e_r \ldots]\!]_s^{a_{acc} \ldots a}]_a
\end{array}
$$

Figure 3.2: ANF transformation for *IDL*

input. This function decomposes the term according to the evaluation rules and uses two helper functions. Function $[\cdot]_a$ transforms a continuation expecting an atomic expression (which are created when transforming commands) into one accepting any command by let-binding passed argument c when necessary. Function $[\![\cdot]\!]_s\ \cdot$ sequences computation of multiple expressions by creating a chain of let-bindings (using $[\cdot]_a$) and then calling the continuation with created variables.

3.2 Control-Flow Analysis

The analysis most relevant to the task of deriving abstract machines from interpreters is the control-flow analysis. Its objective is to find for each expression in a program an over-approximation of a set of functions it may evaluate to [33]. This information can be used in two places: when determining whether a function and applications should be CPS transformed and for checking which functions an expression in operator position may evaluate to. There are a couple of different approaches to performing this analysis available in the literature: abstract interpretation [33], (annotated) type systems [33] and abstract abstract machines [29]. I chose to employ the last approach as it allows for derivation of the control-flow analysis from an abstract machine for

IDL. The derivation technique guarantees correctness of the resulting interpreter and hence provides high confidence in the actual implementation of the machine. I will present the template for acquiring both concrete and abstract versions of the abstract machine for *IDL* but refrain from stepping through the whole derivation. An interested reader should definitely acquaint themselves with the original work in [29] to understand the reasoning and insights behind the technique.

A Machine Template

We will begin with a template of a machine for *IDL* terms in A-normal form presented in Figure 3.3. It is a CEK-style machine modified to explicitly allocate memory for values and continuations in an abstract store. The template is parameterized by: implementation of the store σ along with five operations: $alloc_v$, $alloc_k$, $deref_v$, $deref_k$ and $copy_v$; interpretation of primitive operations δ and implementation of *match* function which interprets pattern matching. The store maps value addresses ν to values v and continuation addresses κ to continuations k. The environment maps program variables to value locations. The values on which machine operates are the following: base values b, primitive operations δ, records with addresses as fields, closures and top-level functions. Thanks to terms being in A-normal form, there are only two kinds of continuations which form a stack. The stack frames $\langle \rho, p, e, \kappa \rangle$ are introduced by let-bindings. They hold an environment ρ, a pattern p to use for destructuring of a value, the body e of a let expression and a pointer to the next continuation κ. The bottom of the stack is marked by the empty continuation $\langle\rangle$. We assume that every term has a unique label l which will be used in abstract version of the machine to implement store addresses.

The machine configurations are pairs of a store σ and a partial configuration γ. This split of configuration into two parts will prove beneficial when we will be instantiating the template to obtain an abstract interpreter. There are two classes of partial configurations. An evaluation configuration contains an environment ρ, an expression e and a continuation pointer κ. A continuation configuration holds an address ν of a value that has been computed so far and a pointer κ to a resumption which should be applied next.

The first case of the transition relation $\Rightarrow$ looks up a pointer for the variable x in the environment ρ and switches to the continuation mode. It modifies the store via *copy* function which ensures that every occurrence of a variable has a corresponding binding in the store. The next three cases deal with values by *alloc*ating them in the store and switching to the continuation mode. When the machine encounters a let-binding it allocates a continuation for the body e of the expression and proceeds to evaluate the bound command c with the new pointer κ'. In case of applications and match expressions the resulting configuration is decided using auxiliary functions *apply* and *match* respectively. Finally, in continuation mode, may transition if the continuation loaded from address κ is a frame. In such a case the machine matches

the stored pattern against the value pointed-to by ν. Otherwise κ points to a $\langle\rangle$ instead and the machine has reached the final state. The auxiliary function *apply* checks what kind of function is referenced by ν and proceeds accordingly.

$$
\begin{array}{rl}
\nu \in \mathit{VAddr} & \kappa \in \mathit{KAddr} \quad l \in \mathit{Label} \quad \sigma \in \mathit{Store} \\
\delta \in \mathit{PrimOp} & \subseteq \mathit{Val}^* \to \mathit{Val} \\
\rho \in \mathit{Env} & = \mathit{Var} \to \mathit{VAddr} \\
\mathit{Val} \ni v & ::= b \mid \delta \mid \{r\ \nu \ldots\} \mid \langle \rho, x \ldots, e \rangle \mid (\texttt{def}\ x\ (x \ldots)\ e) \\
\mathit{Cont} \ni k & ::= \langle \rho, p, e, \kappa \rangle \mid \langle\rangle \\
\mathit{PartialConf} \ni \gamma & ::= \langle \rho, e, \kappa \rangle_e \mid \langle \nu, \kappa \rangle_c \\
\mathit{Conf} \ni \varsigma & ::= \langle \sigma, \gamma \rangle
\end{array}
$$

$$
\begin{array}{rl}
\langle \sigma, \langle \rho, x, \kappa \rangle_e \rangle & \Rightarrow \langle \mathit{copy}_v(\rho(x), l, \sigma), \langle \rho(x), \kappa \rangle_c \rangle \\
\langle \sigma, \langle \rho, b^l, \kappa \rangle_e \rangle & \Rightarrow \langle \sigma', \langle \nu, \kappa \rangle_c \rangle \\
 & \text{where } \langle \sigma', \nu \rangle = \mathit{alloc}_v(b, l, \sigma) \\
\langle \sigma, \langle \rho, \{r\ x \ldots\}^l, \kappa \rangle_e \rangle & \Rightarrow \langle \sigma', \langle \nu, \kappa \rangle_c \rangle \\
 & \text{where } \langle \sigma', \nu \rangle = \mathit{alloc}_v(\{r\ \rho(x) \ldots\}, l, \sigma) \\
\langle \sigma, \langle \rho, (\texttt{fun}\ (x \ldots) e)^l, \kappa \rangle_e \rangle & \Rightarrow \langle \sigma', \langle \nu, \kappa \rangle_c \rangle \\
 & \text{where } \langle \sigma', \nu \rangle = \mathit{alloc}_v(\langle \rho, x \ldots, e \rangle, l, \sigma) \\
\langle \sigma, \langle \rho, (\texttt{let}\ p\ c^l\ e), \kappa \rangle_e \rangle & \Rightarrow \langle \sigma', \langle \rho, c, \kappa' \rangle_e \rangle \\
 & \text{where } \langle \sigma', \kappa' \rangle = \mathit{alloc}_k(\langle \rho, p, e, \kappa \rangle, l, \sigma) \\
\langle \sigma, \langle \rho, (x\ y \ldots), \kappa \rangle_e \rangle & \Rightarrow \mathit{apply}(\sigma, \rho(x), \rho(y) \ldots, l) \\
\langle \sigma, \langle \rho, (\texttt{match}\ x\ (p\ e) \ldots), \kappa \rangle_e \rangle & \Rightarrow \mathit{match}(\sigma, \rho, \rho(x), \langle p, e \rangle \ldots) \\
\langle \sigma, \langle \nu, \kappa \rangle_c \rangle & \Rightarrow \mathit{match}(\sigma, \rho, \nu, \kappa', \langle p, e \rangle) \\
 & \text{where } \langle \rho, p, e, \kappa' \rangle = \mathit{deref}_k(\sigma, \kappa)
\end{array}
$$

$$
\mathit{apply}(\sigma, \nu, \nu' \ldots, \kappa, l) = \begin{cases}
\langle \sigma, \langle \rho[(x \mapsto \nu') \ldots], e, \kappa \rangle_e \rangle \\
\quad \text{when } \mathit{deref}_v(\sigma, \nu) = \langle \rho, x \ldots, e \rangle \\
\langle \sigma, \langle \rho_0[(x \mapsto \nu') \ldots], e, \kappa \rangle_e \rangle \\
\quad \text{when } \mathit{deref}_v(\sigma, \nu) = (\texttt{def}\ y\ (x \ldots)\ e) \\
\langle \sigma', \langle \nu'', \kappa \rangle_c \rangle \\
\quad \text{when } \mathit{deref}_v(\sigma, \nu) = \delta \\
\quad \text{and } \langle \sigma', \nu'' \rangle = \mathit{alloc}_v(\delta(\sigma(\nu') \ldots), l, \sigma)
\end{cases}
$$

$$
\mathit{match}(\sigma, \rho, \nu, \kappa, \langle p, e \rangle \ldots) = \langle \sigma, \langle \rho', e', \kappa \rangle_e \rangle \text{ where } \rho' \text{ is the environment for the first matching branch with body } e'
$$

Figure 3.3: An abstract machine for *IDL* terms in ANF

A Concrete Abstract Machine

The machine template can now be instantiated with a store, a *match* implementation which finds the first matching branch and interpretation for primitive operations in order to obtain an abstract machine. By choosing *Store* to be a mapping with infinite

domain we can ensure that *alloc* can always return a fresh address. In this setting the store-allocated continuations are just an implementation of a stack. The extra layer of indirection introduced by storing values in a store can also be disregarded as the machine operates on persistent values. Therefore the machine corresponds to a CEK-style abstract machine which is a natural [19] formulation for call-by-value functional calculi.

An Abstract Abstract Machine

Let us now turn to a different instantiation of the template. Figure 3.4 shows the missing pieces of an abstract abstract machine for *IDL*. The abstract values use base type names *tp* to represent any value of that type, abstract versions of primitive operations, records, closures and top-level functions. The interpretation of primitive operations must approximate their concrete counterparts.

The store is represented as a pair of finite mappings from labels to sets of abstract values and continuations respectively. This bounding of store domain and range ensures that the state-space of the machine becomes finite and therefore can be used for computing an analysis. To retain soundness w.r.t. the concrete abstract machine the store must map a single address to multiple values to account for address reuse. This style of abstraction is fairly straightforward as noted by [29] and used in textbooks [33]. When instantiated with this store, the transition relation $\Rightarrow$ becomes nondeterministic as pointer *deref*erencing nondeterministically returns one of the values available in the store. Additionally the implementation of *match* function is also nondeterministic in choice of a branch to match against. This machine is not yet suitable for computing the analysis as the state space is still too large since every machine configuration has its own copy of the store. To circumvent this problem a standard technique of widening [33] can be employed. In particular, following [29], we will use a global store. The abstract configuration $\tilde{\varsigma}$ is a pair of a store and a set of partial configurations. The abstract transition $\Rightarrow_a$ performs one step of computation using $\Rightarrow$ on the global store σ paired with every partial configuration γ. The resulting stores σ' are merged together and with the original store to create a new, extended global store. The partial configurations C' are added to the initial set of configurations C. The transition relation $\Rightarrow_a$ is deterministic so it can be treated as a function. This function is monotone on a finite lattice and therefore is amenable to fixed-point iteration.

Computing the Analysis

With the abstract transition function in hand we can now specify the algorithm for obtaining the analysis. To start the abstract interpreter we must provide it with an initial configuration: a store, an environment, a term and a continuation pointer. The store will be assembled from datatype and structure definitions of the program as well

$$
\begin{array}{rl}
\mathit{VAddr} & = \mathit{KAddr} = \mathit{Label} \\
\widetilde{\mathit{Val}} \ni v & ::= tp \mid \widetilde{\delta} \mid \{r\ \nu \ldots\} \mid \langle \rho, x \ldots, e \rangle \mid (\texttt{def}\ x\ (x \ldots)\ e) \\
\sigma \in \mathit{Store} & = (\mathit{VAddr} \to \mathbb{P}(\widetilde{\mathit{Val}})) \times (\mathit{KAddr} \to \mathbb{P}(\mathit{Cont})) \\
\mathit{alloc}_v(v, l, \langle \sigma_v, \sigma_k \rangle) & = \langle \langle \sigma_v[l \mapsto \sigma_v(l) \cup \{v\}], \sigma_k \rangle, l \rangle \\
\mathit{alloc}_k(v, l, \langle \sigma_v, \sigma_k \rangle) & = \langle \langle \sigma_v, \sigma_k[l \mapsto \sigma_k(l) \cup \{k\}] \rangle, l \rangle \\
\mathit{copy}_v(\nu, l, \langle \sigma_v, \sigma_k \rangle) & = \langle \sigma_v[l \mapsto \sigma_v(l) \cup \sigma_v(\nu)], \sigma_k \rangle \\
\mathit{deref}_v(l, \langle \sigma_v, \sigma_k \rangle) & = \sigma_v \\
\tilde{\varsigma} \in \widetilde{\mathit{Conf}} & = \mathit{Store} \times \mathbb{P}(\mathit{PartialConf}) \\
\hline
\langle \sigma, C \rangle & \Rightarrow_a \langle \sigma' \sqcup \sigma, C \cup C' \rangle \\
 & \text{where } \sigma' = \bigsqcup \{\sigma' \mid \exists \gamma \in C.\, \langle \sigma, \gamma \rangle \Rightarrow \langle \sigma', \gamma' \rangle\} \\
 & \text{and } C' = \{\gamma' \mid \exists \gamma \in C.\, \langle \sigma, \gamma \rangle \Rightarrow \langle \sigma', \gamma' \rangle\}
\end{array}
$$

Figure 3.4: An abstract abstract machine for *IDL*

as base types. The initial term is the body of the `main` function of the interpreter and the environment is the global environment extended with `main`'s parameters bound to pointers to datatypes in the above-built store. The initial continuation is of course $\langle\rangle$ and the pointer is the label of the `main`'s body. The analysis is computed by performing fixed-point iteration of $\Rightarrow_a$. The resulting store will contain a set of functions to which every variable (the only allowed term) in function position may evaluate to (ensured by the use of copy_v function). This result will be used in Sections 3.3 and 3.4.

3.3 Selective CPS

In this section we will formulate an algorithm for selectively transforming the program into continuation-passing style. All functions (anonymous and top-level) marked `#:atomic` by the user will be kept in direct style. The `main` function is implicitly marked as atomic since its interface should be preserved as it is an entry point of the interpreter. Primitive operations are treated as atomic at call-site. Atomic functions may call non-atomic ones by providing the called function an identity continuation. The algorithm uses the results of control-flow analysis to determine whether all functions to which a variable labeled l in function position may evaluate are atomic – denoted $\mathit{allAtomic}(l)$ or none of them are atomic – $\mathit{noneAtomic}(l)$. When both atomic and non-atomic functions may be called the algorithm cannot proceed and signals an error in the source program.

The algorithm consists of two mutually recursive transformations: $[\![e]\!]_c\, k$ in Figure 3.5 transforming a term e into CPS with a program variable k as a continuation and $[\![e]\!]_d$ in Figure 3.6 transforming a term e which should be kept in direct style.

The first five clauses of CPS translation deal with values. When a variable is encountered it may be immediately returned by applying continuation. In other

$$
\begin{aligned}
[\![x]\!]_c\, k &= (k\ x) \\
[\![b]\!]_c\, k &= (\texttt{let}\ x\ b\ (k\ x)) \\
[\![\{r\ x\ldots\}]\!]_c\, k &= (\texttt{let}\ y\ \{r\ x\ldots\}\ (k\ y)) \\
[\![(\texttt{fun}\ \texttt{\#:atomic}\ (x\ldots) e)]\!]_c\, k &= (\texttt{let}\ y\ (\texttt{fun}\ (x\ldots)\ [\![e]\!]_d)\ (k\ y)) \\
[\![(\texttt{fun}\ (x\ldots) e)]\!]_c\, k &= (\texttt{let}\ y\ (\texttt{fun}\ (x\ldots k')\ [\![e]\!]_c\, k')\ (k\ y)) \\
[\![(f^l\ x\ldots)]\!]_c\, k &= \begin{cases} (f\ x\ldots\ k) & \text{when } \mathit{noneAtomic}(l) \\ (\texttt{let}\ y\ (f\ x\ldots)\ (k\ y)) & \text{when } \mathit{allAtomic}(l) \end{cases} \\
[\![(\texttt{match}\ x\ (p\ e)\ldots)]\!]_c\, k &= (\texttt{match}\ x\ (p\ [\![e]\!]_c\, k)\ldots) \\
[\![(\texttt{let}\ x\ c\ e)]\!]_c\, k &= \begin{cases} (\texttt{let}\ x\ [\![d]\!]_d\ [\![e]\!]_c\, k) & \text{when } \mathit{trivial}(c) \\ (\texttt{let}\ k'\ (\texttt{fun}\ (x)\ [\![e]\!]_c\, k)\ [\![c]\!]_c\, k') & \text{otherwise} \end{cases} \\
[\![(\texttt{error}\ s)]\!]_c\, k &= (\texttt{error}\ s)
\end{aligned}
$$

Figure 3.5: A translation for CPS terms

$$
\begin{aligned}
[\![x]\!]_d &= x \\
[\![b]\!]_d &= b \\
[\![\{r\ x\ldots\}]\!]_d &= \{r\ x\ldots\} \\
[\![(\texttt{fun}\ \texttt{\#:atomic}\ (x\ldots) e)]\!]_d &= (\texttt{fun}\ (x\ldots)\ [\![e]\!]_d) \\
[\![(\texttt{fun}\ (x\ldots) e)]\!]_d &= (\texttt{fun}\ (x\ldots k')\ [\![e]\!]_c\, k') \\
[\![(f^l\ x\ldots)]\!]_d &= \begin{cases} (f\ x\ldots) & \text{when } \mathit{allAtomic}(l) \\ (\texttt{let}\ k\ (\texttt{fun}\ (y)\ y)\ (f\ x\ldots\ k)) & \text{when } \mathit{noneAtomic}(l) \end{cases} \\
[\![(\texttt{match}\ x\ (p\ e)\ldots)]\!]_d &= (\texttt{match}\ x\ (p\ [\![e]\!]_d)\ldots) \\
[\![(\texttt{let}\ x\ (f^l\ y\ldots)\ e)]\!]_d &= \begin{array}{l} (\texttt{let}\ k\ (\texttt{fun}\ (z)\ z) \\ \quad (\texttt{let}\ x\ (f\ y\ldots\ k)) \\ \qquad [\![e]\!]_d) \end{array} \quad \text{when } \mathit{noneAtomic}(l) \\
[\![(\texttt{let}\ x\ c\ e)]\!]_d &= (\texttt{let}\ x\ [\![c]\!]_d\ [\![e]\!]_d) \\
[\![(\texttt{error}\ s)]\!]_d &= (\texttt{error}\ s)
\end{aligned}
$$

Figure 3.6: A translation for direct style terms

cases the value must be let-bound in order to preserve the A-normal form of the term and then the continuation is applied to the introduced variable. The body e of an anonymous function is translated using $[\![e]\!]_d$ when the function is marked atomic. When the function is not atomic a new variable k' is appended to its parameter list and its body is translated using $[\![e]\!]_c\, k'$. The form of an application depends on atomicity of functions which may be applied. When none of them are atomic the continuation k is passed to the function. When all of them are atomic the result of the call is let-bound and returned by applying the continuation k. Match expression is transformed by recursing on its branches. Since the continuation is always a program variable no code gets duplicated. When transforming a let expression the algorithm checks whether the bound command c is *trivial* – meaning it will only call atomic functions when evaluated (defined in Figure 3.7). If it is then it can

$$
\begin{aligned}
\mathit{trivial}(x) \quad & \mathit{trivial}(b) \\
\mathit{trivial}(\texttt{(\{}r\ x \ldots\texttt{\})}) \quad & \mathit{trivial}(\texttt{(fun (}x \ldots\texttt{)}e\texttt{)}) \\
\mathit{trivial}(\texttt{(}f^l\ x \ldots\texttt{)}) & \iff \mathit{allAtomic}(l) \\
\mathit{trivial}(\texttt{(match }x\texttt{ (}b\ e\texttt{)}\ldots\texttt{)}) & \iff \bigwedge \mathit{trivial}(e) \ldots \\
\mathit{trivial}(\texttt{(let }x\ c\ e\texttt{)}) & \iff \mathit{trivial}(c) \wedge \mathit{trivial}(e)
\end{aligned}
$$

Figure 3.7: The *trivial* predicate

remain in direct style $[\![c]\!]_d$, no new continuation has to be introduced and the body can be transformed by $[\![e]\!]_c\, k$. If the command is non-trivial then a new continuation is created and bound to k'. This continuation uses the variable x as its argument and its body is the body of let-expression e transformed with the input continuation k. The bound command is transformed with the newly introduced continuation k'. Finally, the translation of `error` throws out the continuation.

The direct style transformation begins similarly to CPS one – with five clauses for values. In case of an application the algorithm is symmetric: when all functions are atomic the call remains in direct style, when none of them are atomic a new identity continuation k is constructed and is passed to the called function. A match expression is again transformed recursively. A let binding of a call to cps function gets special treatment to preserve A-normal by chaining allocation of identity continuation with the call. In other cases a let binding is transformed recursively. An `error` expression is left untouched.

Each top-level function definition in a program is transformed in the same fashion as anonymous functions. After the transformation the program is still in ANF and can be again analyzed by the abstract abstract machine of previous section.

3.4 Selective Defunctionalization

The second step of the functional correspondence and the last stage of the transformation is selective defunctionalization. The goal is to defunctionalize function spaces deemed interesting by the author of the program. To this end top-level and anonymous functions may be annotated with `#:no-defun` to skip defunctionalization of function spaces they belong to. In the algorithm of Figure 3.8 the predicate *defun* specifies whether a function should be transformed. Predicates *primOp* and *topLevel* specify whether a variable refers to (taking into account the scoping rules) primitive operation or top-level function respectively. For each application point l in the program we can utilize the results of control-flow analysis to obtain the set of functions which may be applied. If all of them should be defunctionalized (*allDefun*) then a call to the generated apply function is introduced, when none of them should

$$
\begin{aligned}
[\![x]\!] &= \begin{cases} \{\texttt{Prim}_x\} & \text{when } primOp(x) \\ \{\texttt{Top}_x\} & \text{when } topLevel(x) \\ x & \text{otherwise} \end{cases} \\
[\![b]\!] &= b \\
[\![\{r\ x \ldots\}]\!] &= \{\texttt{r}\ [\![x]\!] \ldots\} \\
[\![(\texttt{fun}\ (x \ldots) e)^l]\!] &= \begin{cases} \{\texttt{Fun}_l\ fvs(e)\} & \text{when } defun(l) \\ (\texttt{fun}\ (x \ldots)\ [\![e]\!]) & \text{otherwise} \end{cases} \\
[\![(f^{l'}\ x \ldots)^l]\!] &= \begin{cases} (\texttt{apply}_l\ f\ [\![x]\!] \ldots) & \text{when } allDefun(l') \\ (f\ [\![x]\!] \ldots) & \text{when } noneDefun(l') \end{cases} \\
[\![(\texttt{match}\ x\ (p\ e) \ldots)]\!] &= (\texttt{match}\ x\ (p\ [\![e]\!]) \ldots) \\
[\![(\texttt{let}\ x\ c\ e)]\!] &= (\texttt{let}\ x\ [\![c]\!]\ [\![e]\!]) \\
[\![(\texttt{error}\ s)]\!] &= (\texttt{error}\ s)
\end{aligned}
$$

Figure 3.8: Selective defunctionalization algorithm for *IDL*

$$
\begin{aligned}
mkBranch(x \ldots, \qquad\qquad \delta) &= (\{\texttt{Prim}_\delta\}\ (\delta\ x \ldots)) \\
mkBranch(x \ldots, (\texttt{def}\ f\ (y \ldots)\ \texttt{e})) &= (\{\texttt{Top}_f\}\ (f\ x \ldots)) \\
mkBranch(x \ldots, \quad (\texttt{fun}\ (y \ldots)\ e)^l) &= (\{\texttt{Fun}_l\ fvs(e)\}\ [\![e]\!]\,[y \mapsto x])
\end{aligned}
$$

$$
\begin{aligned}
mkApply(l, fn \ldots) = \quad & (\texttt{def}\ \texttt{apply}_l\ (f\ x \ldots) \\
& \quad (\texttt{match}\ f \\
& \qquad mkBranch(x \ldots, fn) \ldots))
\end{aligned}
$$

Figure 3.9: Top-level apply function generation

(*noneDefun*) then the application is left as is, if neither condition holds then an error in the source program is signaled. The apply functions are generated using *mkApply* as specified in Figure 3.9 where the *fn* ... is a list of functions which may be applied. After the transformation the program is no longer in A-normal form since variables referencing top-level functions may have been transformed into records. However it does not pose a problem since the majority of work has already been done and the last step – let-inlining does not require the program to be in ANF.

Chapter 4

Case Studies

I studied the performance of the algorithm and the implementation on a number of programming language calculi. Figure 4.1 shows a summary of interpreters on which I tested the transformer. The first group of interpreters is denotational (mostly meta-circular) in style and covers various extensions of the base λ-calculus with call-by-value evaluation order. The additions I tested include: integers with addition, recursive let-bindings, delimited control operators – *shift* and *reset* with CPS interpreter based on [25] and exceptions in two styles: monadic with exceptions as values (functions return either value or an exception) and in CPS with success and error continuations. The last interpreter for call-by-value in Figure 4.1 is a normalization function based on normalization by evaluation technique transcribed from [34]. The next three interpreters correspond to big-step operational semantics for call-by-name λ-calculus, call-by-need (call-by-name with memoization) and a simple imperative language respectively.

Language	Interpreter style	Lang. Features	Result
call-by-value λ-calculus	denotational	·	CEK machine
	denotational	integers with add	CEK with add
	denotational, recursion via environment	integers, recursive let-bindings	similar to Reynold's first-order interpreter
	denotational with conts.	shift and reset	two layers of conts.
	denotational, monadic	exceptions with handlers	explicit stack unwinding
	denotational, CPS		pointer to exception handler
	normalization by evaluation	·	strong CEK machine
call-by-name λ-calculus	big-step	·	Krivine machine
call-by-need λ-calculus	big-step (state passing)	memoization	lazy Krivine machine
simple imperative	big-step (state passing)	conditionals, while, assignment	·

Figure 4.1: Summary of tested interpreters

Chapter 5

Conclusions

In the thesis I described an algorithm allowing for automatic derivation of an abstract machine given an interpreter which usually corresponds to denotational or natural semantics. The algorithm allows for specification of functions which should be considered atomic from the point of view of control-flow and function spaces which treated as abstract (i.e. left in the higher-order form) in the resulting machine. In order to enable the transformation I derived the control-flow analysis for *IDL* using the abstracting abstract machines methodology. I implemented the algorithm in the *Haskell* programming language and used this tool to transform a selection of interpreters.

The correctness of the tool has been established experimentally by running the interpreters after every intermediate step of transformation. The next logical step is a formalization of the algorithm using a proof assistant (e.g., Coq) to obtain a powerful and correct method of deriving abstract machines.

In order to extend capabilities of `semt` as a practical tool for semantics engineering the future work could include extending the set of primitive operations and adding the ability to import arbitrary *Racket* functions and provide their abstract specification. Another important matter is the performance (i.e., speed) of the tool. To this end a thorough investigation of cost and complexity of computing the control-flow analysis is required.

Other avenue for improvement lies in extensions of the meta-language capabilities. Investigation of additions such as control operators, nondeterministic choice and concurrency could yield many opportunities for diversifying the set of interpreters (and languages) that may be encoded in the *IDL*. In particular control operators could allow for expressing the interpreter for a language with delimited control (or algebraic effects) in direct style.

Appendix A

User's Manual

Installation

The semantic transformer – `semt` is built from source using `cabal` – a *Haskell* package manager. To build the binary use `cabal build` and to install the resulting binary use `cabal install` in the root of the project.

Tool usage

The basic mode of usage is to transform a `file.rkt` containing an interpreter into `out/file.rkt` which is a source file containing the transformed interpreter i.e. an abstract machine using the command `semt file.rkt`. The options modifying the behavior of the tool can be displayed with the command `semt --help`:

```
Usage: semt FILE [-o|--output DIR] [-i|--intermediate]
            [-d|--debug] [-t|--self-test]
  Transform an interpreter into an abstract machine.

Available options:
  FILE                     Source file with the interpreter.
  -o,--output DIR          Output directory for generated
                            files, defaults to ./out/
  -i,--intermediate        Emit executable source files for
                            each stage.
  -d,--debug               Emit labeled source files for
                            each stage.
  -t,--self-test           Run raco test on each
                            intermediate file; implies
                            --intermediate
  -h,--help                Show this help text
```

```
data-def    ::= (def-data tp-name tp-elem ...)
tp-elem     ::= tp | record
record      ::= {tp-name record-field ...}
record-field ::= tp | var | [tp var]
record-def  ::= (def-struct record)
base-tp     ::= String | Integer | Boolean
tp          ::= Any | base-tp | tp-name
fun-def     ::= (def var annot ... (arg ...) term)
annot       ::= #:no-defun | #:atomic | #:name tp-name | #:apply var
arg         ::= var | [tp var]
term        ::= var | (fun annot ... (arg ...) term) | (term term ...)
              | {tp-name term ...}
```

Source File Format

The tool assumes that the source file with an interpreter is a *Racket* program. The interpreter itself (line 6) has to be placed between two comments (lines 4 and 8):

```
1  #racket
2  ...
3
4  ; begin interpreter
5
6  ;; interpreter goes here
7
8  ; end interpreter
9
10 ...
```

The interpreter consists of a sequence of datatype, record and function definitions. One of the functions must be named `main` and will serve as an entry point of the interpreter. The syntax of top-level definitions is given in Figure ???

Appendix B

Developer's Manual

Bibliography

[1] Dana Scott. Data Types as Lattices. In: *SIAM Journal on Computing* 5.3 (1976), pp. 522–587. DOI: 10.1137/0205037. eprint: https://doi.org/10.1137/0205037. URL: https://doi.org/10.1137/0205037.

[2] G. Kahn. Natural semantics. In: *STACS 87*. Ed. by Franz J. Brandenburg, Guy Vidal-Naquet, and Martin Wirsing. Berlin, Heidelberg: Springer Berlin Heidelberg, 1987, pp. 22–39. ISBN: 978-3-540-47419-7.

[3] Arthur Charguéraud. Pretty-Big-Step Semantics. In: *Programming Languages and Systems*. Ed. by Matthias Felleisen and Philippa Gardner. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 41–60. ISBN: 978-3-642-37036-6.

[4] Gordon Plotkin. A Structural Approach to Operational Semantics. In: *J. Log. Algebr. Program.* 60-61 (July 2004), pp. 17–139. DOI: 10.1016/j.jlap.2004.05.001.

[5] Matthias Felleisen, Robert Bruce Findler, and Matthew Flatt. Semantics engineering with PLT Redex. Mit Press, 2009.

[6] Casper Bach Poulsen and Peter D. Mosses. Deriving Pretty-Big-Step Semantics from Small-Step Semantics. In: *Programming Languages and Systems*. Ed. by Zhong Shao. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 270–289. ISBN: 978-3-642-54833-8.

[7] Ferdinand Vesely and Kathleen Fisher. One Step at a Time. In: *Programming Languages and Systems*. Ed. by Luís Caires. Cham: Springer International Publishing, 2019, pp. 205–231. ISBN: 978-3-030-17184-1.

[8] Peter J Landin. The mechanical evaluation of expressions. In: *The computer journal* 6.4 (1964), pp. 308–320.

[9] Jean-Louis Krivine. A Call-by-Name Lambda-Calculus Machine. In: *Higher Order Symbol. Comput.* 20.3 (Sept. 2007), pp. 199–207. ISSN: 1388-3690. DOI: 10.1007/s10990-007-9018-9. URL: https://doi.org/10.1007/s10990-007-9018-9.

[10] Matthias Felleisen and Daniel P. Friedman. Control operators, the SECD-machine, and the λ-calculus. In: *Formal Description of Programming Concepts*. 1987.

[11] P. Crégut. An Abstract Machine for Lambda-Terms Normalization. In: *Proceedings of the 1990 ACM Conference on LISP and Functional Programming*. LFP '90. Nice, France: Association for Computing Machinery, 1990, pp. 333–340. ISBN: 089791368X. DOI: 10.1145/91556.91681. URL: https://doi.org/10.1145/91556.91681.

[12] Dariusz Biernacki et al. Abstracting Algebraic Effects. In: *Proc. ACM Program. Lang.* 3.POPL (Jan. 2019). DOI: 10.1145/3290319. URL: https://doi.org/10.1145/3290319.

[13] Daniel Hillerström and Sam Lindley. Liberating Effects with Rows and Handlers. In: *Proceedings of the 1st International Workshop on Type-Driven Development*. TyDe 2016. Nara, Japan: Association for Computing Machinery, 2016, pp. 15–27. ISBN: 9781450344357. DOI: 10.1145/2976022.2976033. URL: https://doi.org/10.1145/2976022.2976033.

[14] Olivier Danvy and Lasse R Nielsen. Refocusing in reduction semantics. In: *BRICS Report Series* 11.26 (2004).

[15] Filip Sieczkowski, Małgorzata Biernacka, and Dariusz Biernacki. Automating Derivations of Abstract Machines from Reduction Semantics: A Generic Formalization of Refocusing in Coq. In: *Proceedings of the 22nd International Conference on Implementation and Application of Functional Languages*. IFL'10. Alphen aan den Rijn, The Netherlands: Springer-Verlag, 2010, pp. 72–88. ISBN: 9783642242755.

[16] Malgorzata Biernacka, Witold Charatonik, and Klara Zielinska. Generalized Refocusing: From Hybrid Strategies to Abstract Machines. In: *2nd International Conference on Formal Structures for Computation and Deduction (FSCD 2017)*. Ed. by Dale Miller. Vol. 84. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017, 10:1–10:17. ISBN: 978-3-95977-047-7. DOI: 10.4230/LIPIcs.FSCD.2017.10. URL: http://drops.dagstuhl.de/opus/volltexte/2017/7718.

[17] Mads Ager. From Natural Semantics to Abstract Machines. In: vol. 3573. Aug. 2004, pp. 245–261. DOI: 10.1007/11506676_16.

[18] John Hannan and Dale Miller. From operational semantics to abstract machines. In: *Mathematical Structures in Computer Science* 2.4 (1992), pp. 415–459.

[19] Mads Sig Ager et al. A Functional Correspondence between Evaluators and Abstract Machines. In: *Proceedings of the 5th ACM SIGPLAN International Conference on Principles and Practice of Declaritive Programming*. PPDP '03. Uppsala, Sweden: Association for Computing Machinery, 2003, pp. 8–19. ISBN: 1581137052. DOI: 10.1145/888251.888254. URL: https://doi.org/10.1145/888251.888254.

[20] John C. Reynolds. Definitional Interpreters for Higher-Order Programming Languages. In: *Proceedings of the ACM Annual Conference - Volume 2*. ACM '72. Boston, Massachusetts, USA: Association for Computing Machinery, 1972, pp. 717–740. ISBN: 9781450374927. DOI: 10.1145/800194.805852. URL: https://doi.org/10.1145/800194.805852.

[21] Mads Sig Ager et al. From interpreter to compiler and virtual machine: a functional derivation. In: *BRICS Report Series* 10.14 (2003).

[22] Mads Sig Ager, Olivier Danvy, and Jan Midtgaard. A functional correspondence between call-by-need evaluators and lazy abstract machines. In: *Information Processing Letters* 90.5 (2004), pp. 223–232. ISSN: 0020-0190. DOI: https://doi.org/10.1016/j.ipl.2004.02.012. URL: http://www.sciencedirect.com/science/article/pii/S0020019004000638.

[23] Maciej Pirog and Dariusz Biernacki. A Systematic Derivation of the STG Machine Verified in Coq. In: *Proceedings of the Third ACM Haskell Symposium on Haskell*. Haskell '10. Baltimore, Maryland, USA: Association for Computing Machinery, 2010, pp. 25–36. ISBN: 9781450302524. DOI: 10.1145/1863523.1863528. URL: https://doi.org/10.1145/1863523.1863528.

[24] Dariusz Biernacki and Olivier Danvy. From Interpreter to Logic Engine by Defunctionalization. In: *Logic Based Program Synthesis and Transformation*. Ed. by Maurice Bruynooghe. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 143–159. ISBN: 978-3-540-25938-1.

[25] Malgorzata Biernacka, Dariusz Biernacki, and Olivier Danvy. An Operational Foundation for Delimited Continuations in the CPS Hierarchy. In: *Logical Methods in Computer Science* 1.2 (Nov. 2005). Ed. by Philip Wadler. ISSN: 1860-5974. DOI: 10.2168/lmcs-1(2:5)2005. URL: http://dx.doi.org/10.2168/LMCS-1(2:5)2005.

[26] Mads Sig Ager, Olivier Danvy, and Jan Midtgaard. A functional correspondence between monadic evaluators and abstract machines for languages with computational effects. In: *Theoretical Computer Science* 342.1 (2005). Applied Semantics: Selected Topics, pp. 149–172. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2005.06.008. URL: http://www.sciencedirect.com/science/article/pii/S0304397505003439.

[27] Olivier Danvy and Jacob Johannsen. Inter-deriving semantic artifacts for object-oriented programming. In: *Journal of Computer and System Sciences* 76.5 (2010). Workshop on Logic, Language, Information and Computation, pp. 302–323. ISSN: 0022-0000. DOI: https://doi.org/10.1016/j.jcss.2009.10.004. URL: http://www.sciencedirect.com/science/article/pii/S0022000009000932.

[28] Wojciech Jedynak, Małgorzata Biernacka, and Dariusz Biernacki. An Operational Foundation for the Tactic Language of Coq. In: *Proceedings of the 15th Symposium on Principles and Practice of Declarative Programming*. PPDP '13. Madrid, Spain: Association for Computing Machinery, 2013, pp. 25–36. ISBN:

9781450321549. DOI: 10.1145/2505879.2505890. URL: https://doi.org/10.1145/2505879.2505890.

[29] David Van Horn and Matthew Might. Abstracting Abstract Machines. In: *SIGPLAN Not.* 45.9 (Sept. 2010), pp. 51–62. ISSN: 0362-1340. DOI: 10.1145/1932681.1863553. URL: https://doi.org/10.1145/1932681.1863553.

[30] Xavier Leroy. The ZINC experiment: an economical implementation of the ML language. In: (1990).

[31] Mattias Felleisen and D. P. Friedman. A Calculus for Assignments in Higher-Order Languages. In: *Proceedings of the 14th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*. POPL '87. Munich, West Germany: Association for Computing Machinery, 1987, p. 314. ISBN: 0897912152. DOI: 10.1145/41625.41654. URL: https://doi.org/10.1145/41625.41654.

[32] Cormac Flanagan et al. The Essence of Compiling with Continuations. In: *SIGPLAN Not.* 28.6 (June 1993), pp. 237–247. ISSN: 0362-1340. DOI: 10.1145/173262.155113. URL: https://doi.org/10.1145/173262.155113.

[33] Flemming Nielson, Hanne Nielson, and Chris Hankin. Principles of Program Analysis. Jan. 1999. DOI: 10.1007/978-3-662-03811-6.

[34] Andreas Abel. Normalization by Evaluation: Dependent Types and Impredicativity. In: (2013).