

Tianlin Zhang

An Observable OCaml

Computer Science Tripos – Part II

Jesus College

May 2, 2018

Proforma

Name: **Tianlin Zhang**
College: **Jesus College**
Project Title: **An Observable OCaml**
Examination: **Computer Science Tripos – Part II**
Year: **June 2018**
Word Count: **TODO**
Project Originator: Stephen Kell
Supervisor: Stephen Kell

Original Aims of the Project

To write a backend for the OCaml compiler that allows compilation from OCaml into C in such a way that it preserves so-called “observability”, that is the ability to debug the generated C code, using GDB for example, in a similar fashion to debugging the original OCaml code. A library of test programs should be written to demonstrate the capabilities of the compiler, along with an evaluation into the performance and observability of the compiled code.

Work Completed

I have written and completed a new backend for the OCaml compiler which can compile a suitable target subset of OCaml, including a majority of the most commonly used features. A C runtime library has also been written to support the execution of the resulting C output, as well as a library of test programs which are used in testing and evaluation of the compiler. An evaluation has also been performed investigating the execution times of the compiler with respect to the OCaml native compiler, and the observability of the compiled code with the OCaml bytecode compiler.

Special Difficulties

None.

Declaration

I, Tianlin Zhang of Jesus College, being a candidate for Part II of the Computer Science Tripos, hereby declare that this dissertation and the work described in it are my own work, unaided except as may be specified below, and that the dissertation does not contain material that has already been used to any substantial extent for a comparable purpose.

Signed: Tianlin Zhang

Date: May 2, 2018

Contents

1	Introduction	7
1.1	Motivation	7
1.2	Previous Work	8
2	Preparation	9
2.1	Starting point	9
2.1.1	Intermediate representations	9
2.1.2	The <code>Lambda</code> IR	11
2.2	Extensibility of GDB	12
2.3	Target subsets	12
2.3.1	Subset 1	13
2.3.2	Subset 2	13
2.3.3	Subset 3	13
2.4	The <code>liballocs</code> library	13
2.5	The Boehm GC	14
2.6	Setting up the environment	14
2.7	Licensing of external code	15
3	Implementation	17
3.1	Obtaining types from the <code>Lambda</code> IR	17
3.1.1	<code>Lambda</code> Events	17
3.1.2	The <code>Typecollect</code> module	18
3.2	Representation of C	18
3.2.1	Expressions to statements	19
3.2.2	The <code>Ccode</code> module	19
3.2.3	The <code>Cprint</code> module	19
3.3	Compiler basics	19
3.3.1	<code>let</code> bindings	20
3.3.2	Recursive bindings with <code>let rec</code>	20
3.4	OCaml value representation	21
3.4.1	Representation requirements	21
3.4.2	Representation strategy	22
3.4.3	Representation in C	23
3.4.4	Conversion between C types	24
3.4.5	Pattern matching	25

3.5	Function compilation and closure conversion	26
3.5.1	Local functions	26
3.5.2	Function Types in C	27
3.5.3	Closure representation	27
3.5.4	Partial application compilation	28
3.5.5	Lexical closure compilation	30
3.5.6	Parametric polymorphism	30
3.6	Garbage Collection	33
4	Evaluation	35
4.1	Regression tests and feature completeness	35
4.2	Benchmarks	35
4.2.1	Sourcing Benchmarks	36
4.2.2	Investigating performance differences	38
4.3	Observability	45
4.3.1	Sample GDB session	45
4.3.2	Identifiers	46
4.3.3	Polymorphic printers	46
4.3.4	Line number matching	47
5	Conclusion	49
	Bibliography	50
A	Implementation Details	53
A.1	The <code>Ccode</code> module	53
A.2	Purpose of <code>runtime.h</code>	54
A.3	<code>#line</code> directives	54
A.4	Compilation of basic constructs	54
A.4.1	Variable scoping differences between C and OCaml	54
A.4.2	Meta-notation for compilation	55
A.4.3	<code>if-then-else</code> expressions	56
A.4.4	<code>while</code> loops	56
A.4.5	<code>for</code> loops	57
A.5	Value representation details	58
A.5.1	<code>Lstaticraise</code> and <code>Lstaticcatch</code>	58
A.6	Closure details	59
A.6.1	Functions that return other functions	59
B	Debug sessions	61
B.1	The “sum” program	61
B.2	GDB session of the “sum” program	61
B.3	Ocamldebug session of the “sum” program	62
C	Project Proposal	65

Chapter 1

Introduction

My project concerns the creation of a new compiler for OCaml, a popular statically typed functional language in the ML family, into the C language in such a way as to be able to take advantage of debugging tools provided by the C toolchain. This property, henceforth referred to as “observability”, refers to the ability to view the execution of the program through a debugger as if it was debugging a C program and to recover the program’s execution state.

I have successfully implemented a compiler for a core subset of the OCaml language in to C, which when compiled with a standard C compiler such as `gcc` or `clang` produces an executable that behaves in an identical way up to minor differences with the output of the native OCaml compiler. Additionally, when compiled with the `-g` flag, the resulting executable can be debugged under `gdb` in such a way that preserves the execution order of the original OCaml source, and allows setting breakpoints and observing values in the OCaml code in the same way as if it were debugging the original OCaml code.

1.1 Motivation

There are several motivations for this project, including:

Observability

The OCaml debugger was introduced fairly recently, and only works on compiled bytecode; in addition, since OCaml strips away type information on actual values at runtime, the debugger is unable to inspect the values of certain variables within polymorphic functions.

We can consider the following example OCaml code:

```
let id x = x
let a = id 2
```

Running this through the OCaml debugger, we see that it is unable to determine the value of the variable `x` within the `id` function.

```
(ocd) break @ Id 1
Breakpoint 1 at 10156: file id.ml, line 1, characters 12-13
(ocd) run
```

```
Time: 12 - pc: 10156 - module Id
Breakpoint: 1
1 let id x = <|b|>x
(ocd) print x
x: 'a = <poly>
```

Compiling to C could take advantage of a different data representation, and GDB extensions to customise debugger behaviour, allowing GDB to ‘see-through’ polymorphic values such as this..

Plausibility

There are many language features in OCaml which do not have similar analogues in C. Examples of these include algebraic data structures, partial application, lexical closures, and polymorphic datatypes and functions. I was interested in whether despite these differences, I could create appropriate transformations to simulate these in C but preserve observability at the same time, giving an OCaml view into what the code is doing.

Performance

By compilation to C, I can take advantage of the fact that the most popular C compilers have undergone decades of optimisation to produce very performant code. We can exploit this to obtain very fast executables without needing to perform much optimisation on the OCaml code. There will however be performance trade-offs in terms of emulating OCaml function calls in C compared to normal function calls, as OCaml functions can take advantage of features such as lexical closure and partial application, as well as being first-class allowing them to be passed as values to higher-order functions.

1.2 Previous Work

There exist prior work for compiling ML-like languages into C [1] but the approach used is to transform the program into continuation-passing style, which is not suitable for the compiler as it would interfere with the program execution and make it untenable to map OCaml source code into regions of the compiled code for debugging purposes, but shows that compilation into C from similar functional languages is feasible.

In addition, this project was also attempted in previous years by a previous student [2] under the same supervisor with a similar starting point, but my approach to the design of the compiler was not influenced and it is of my opinion that a sufficiently different approach was used for this project. A different representation of the output C code was used leading to a different compiler structure from the outset of the project, as well as completely different approaches being taken for more complex features in OCaml, such as data representation and closure conversion.

Chapter 2

Preparation

Before starting the project I have had significant experience with functional languages through the Standard ML course undertaken and also personal experience with programming in Haskell, but however I had never used OCaml at length, nor worked with the OCaml compiler codebase. While OCaml was very simple to learn from my previous experiences with functional languages, the OCaml compiler codebase much to my chagrin was large, complex, and very sparsely commented.

In this respect, a large portion of time during the starting weeks of the project was focused on reading through barely-commented source code in order to understand the different data types used by the OCaml compiler, as well as research into various options for different libraries to use.

2.1 Starting point

The starting point of this project is the existing OCaml compiler¹, as it would be too onerous to duplicate the effort of parsing and performing type inference on OCaml source code. Instead, my compiler takes the `Lambda` intermediate representation from the OCaml compiler and compiles this into C. Since the OCaml compiler backends `Asmgen` and `Bytgen`, which produce the native binaries/bytecode executables, also only take the `Lambda` IR, this approach is akin to introducing a new compiler backend or different target for compilation.

The rest of this section will address why this was chosen as the starting point, and the process during the preparation phase in which the appropriate starting point was determined.

2.1.1 Intermediate representations

The OCaml compiler processes code in the pipeline shown in figure 2.1, with the pipeline branching towards the end into two separate stages representing the targets that the OCaml compiler can compile to. Between each stage, a different intermediate representation of the code is produced.

¹<https://github.com/ocaml/ocaml>

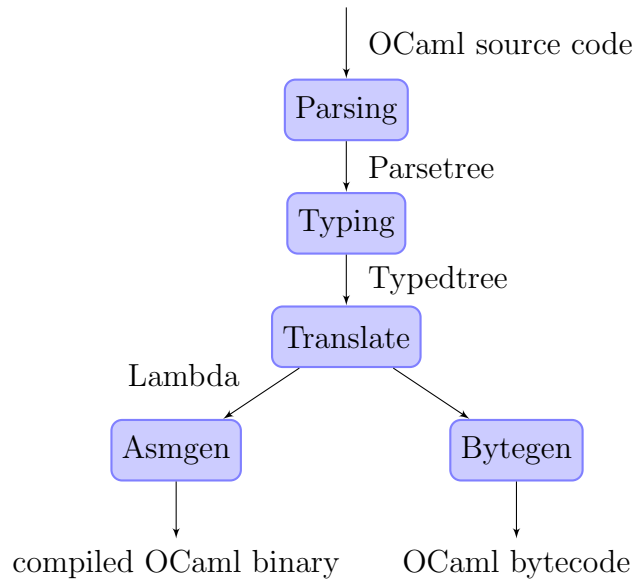


Figure 2.1: A representation of the various stages in the OCaml compiler. Adapted from [3, Chapter 22].

One of the tasks that had to be carried out during the preparation phase was to determine which intermediate representation would be most suitable for compilation into C. The requirements required for such an intermediate representation would be:

- It must be easy to recover type information from the representation. This is because the resulting C code must be statically typed also, so we need to be able to infer the types of variables and functions in order for them to be implemented in C.
- The representation must be fairly normalised, with as few as possible language constructs to simplify the translation into C. Many language features in OCaml are merely syntactically sugared versions of more primitive ones (for example, pattern matching is really a combination of branching based on the value of a variable plus some variable bindings for unpacking) which must have been desugared anyway during the compilation process, so it would be more useful if we could utilise an intermediate representation for which this has already happened.
- The representation must also allow some amount of reconstruction back to the source level, as this is important so we can map the output code to the correct sections of the source code, which is important for observability and debugging as we would like debuggers to display the correct segments of code being debugged. This does present an antagonism, where we would like the IR to be both normalised, but not enough that we cannot recover any source-level information from it.

Parsetree

Parsetree is a parsed AST representation of the source code, which essentially directly represents the original OCaml source code. No processing has occurred on any language

constructs, and type inference has not even occurred on the IR. This obviously makes this intermediate representation unsuitable as the choice of IR, since it falls down on both ability to recover type information and normalisation.

Typedtree

Typedtree is a type-annotated AST which is almost exactly identical to the **Parsetree** IR, except that expressions have been annotated with a type. This makes this IR highly desirable as the starting point for compilation into C, and was initially where the investigation for a usable intermediate representation started.

However, since **Typedtree** still almost directly represents the original source code, it suffers from the same normalisation problem as **Parsetree** does. For example, the number of different sub-expression cases that **Parsetree** represents separately is 31 — modules, classes and objects are still represented as syntactical elements; records, variants, and field accesses have not been normalised into one representation; and pattern matches have not been simplified but instead stored as association lists of raw patterns to expressions.

This makes the **Typedtree** IR very cumbersome to work with, and ultimately it was considered unsuitable for the starting point of the project.

2.1.2 The Lambda IR

The **Lambda** IR is so named because it resembles an untyped lambda calculus, and is what in fact the two existing backends of the compiler generate code from. It has a number of advantages over **Parsetree** and **Typedtree**, including:

- Variants and records have been normalised into one representation, which is referred to as a block, which are similar to tagged unions. In addition, variants without parameters are compiled into bare integers.
- Desugaring of pattern match statements. Because variants have been compiled into integers or tagged unions, the translation pass is able to optimise pattern matching into switch statements. In very simple cases, pattern matches are in fact compiled into an if-else statement instead.
- Removal of modules and functors. These values have instead been compiled into equivalent representations using blocks and functions.

In comparison to **Typedtree**'s 31 different cases for sub-expressions, the **Lambda** representation has 20 different cases, which are relatively much simpler than those in **Typedtree**. This makes the **Lambda** IR far more desirable as a starting point.

However, there are some major disadvantages of the **Lambda** IR:

- The translation pass into **Lambda** does not preserve much of the type information from **Typedtree**. This is a huge problem which is solved somewhat with the existence of **Lambda** events, which will be discussed in §3.1.

- Normalisation in the `Lambda` IR discard a lot of source-level information such as which source-level expressions `Lambda` expressions map to, as well as having very little information about the location in the source code of the current code. This is somewhat remedied with `Lambda` events, which is discussed in §A.3.
- The `Lambda` IR has not yet had closure conversion applied to it. Functions are still represented in a similar fashion to how they were in the original source code, meaning the cases of lexical closures, partial application, etc. are not handled.

It was determined that while the `Lambda` IR does not fully satisfy the typing and source reconstruction requirements, enough type and source information was recoverable that it was deemed acceptable as a starting point. Thus, my project starts compilation by obtaining the `Lambda` representation by passing the source code through part of the compilation pipeline, and then translates the resulting IR into C from that point onwards.

2.2 Extensibility of GDB

Part of the project requirements dictate that the resulting code be “observable”, and it was quickly identified that if GDB is to be used as the primary debugger it may be necessary to extend GDB in order to handle the compiled OCaml code correctly and display recursive OCaml values. Thus, a brief investigation into GDB was carried out in the preparation phase to investigate its extensibility.

One of the experiments which was carried out was to see if GDB could display code from other files, and associate parts of compiled C code with instead parts of code from another file. This is a necessary part of the compilation process, as the resulting debuggable executable must display code and symbols from the original OCaml file from which it was compiled from via my compiler, not the C file that my compiler produces. With some investigation it was found that this was possible with the `#line` directive, which is explored in §A.3.

Another feature which is required for observability is the ability to display OCaml values at least recursively, if not formatted in the same way as the OCaml compiler does. This is because many OCaml values are recursive (for example, the list type is a recursive type which refers back to itself as one of its parameters) so it must be possible to extend GDB with some way to recursively print values whenever it finds a pointer. It was found that GDB does support extensions to itself via custom macros, and also supports custom pretty-printers (via, for example, Python) for different types. Either of these features would allow GDB to display OCaml values correctly.

2.3 Target subsets

During the write-up of the project proposal, three expanding subsets of OCaml were identified in order to structure the creation of the compiler around. These subsets represent a grouping of similar constructs and features together such that each subset focuses on a similar theme in the new features it introduces.

Identification of these subsets firstly has the benefit of providing a clear structure to the project, and greatly influenced the order in which features were implemented. Optimistically, it was expected that at the end of proposed deadlines a compiler would be completed that could compile the associated Subset – unfortunately, due to interdependence between a lot of the features a working compiler was not produced until towards the end of implementing features for Subset 2.

These subsets also serve to identify what the minimum viable product of the project is, as it was determined on project conception compilation of the entire OCaml language would be far too ambitious. As such, Subset 3 represents the subset of the language that the final product should at minimum be able to compile correctly.

Despite the fact that the subsets ultimately did not produce distinct and recognisable milestones for compilers that could operate on the appropriate subsets of the language, it is still worth describing the subsets for the effect they had on the planning for the rest of the project.

2.3.1 Subset 1

Subset 1 is a very simple language with only a limited number of types and language constructs. This subset contains only basic boolean, integer, floating point, and `unit` types, only basic string support (for input/output), top level function declarations with `let` and `let rec`, and basic language constructs such as `if`, `for`, and `while`.

2.3.2 Subset 2

Subset 2 expands on Subset 1 by introducing custom types and polymorphism. This includes tuples, lists, variant types via algebraic data types, record types, match expressions and function parametric polymorphism. This subset is aimed towards designing and implementing an appropriate representation of OCaml values in C, as well as a way of representing polymorphic values both as values in user-defined types and as parameters to functions.

2.3.3 Subset 3

Subset 3 expands further on Subset 2 by adding treatment of functions as first class values, plus closure conversion features, which would entail compilation of lexical closures, partial application, anonymous functions, etc. The focus of this subset is intended towards the design and implementation of closures in C, and correctly compiling the more difficult features of OCaml functions into C.

2.4 The liballocs library

`liballocs`[4] is a library that is able to track all allocations in memory and their associated types with no extra required effort. It exposes an interface that, when given an

arbitrary pointer, is able to return information about the type of the value in the allocated memory. This was identified to be extremely useful for implementing observability features, as it could be used within polymorphic functions to determine the type of certain values whilst debugging at runtime, which would be an advantage over the OCaml bytecode debugger, which due to the untagged nature of OCaml values cannot determine the type of polymorphic values at runtime.

Unfortunately, it was deemed that explicit tagging of types was easier to implement than inclusion of the `liballocs` library, but future extensions to the compiler may incorporate it to provide more detailed typing information.

2.5 The Boehm GC

Since the target subset aims to include a significant portion of OCaml including parts which allow for data structures and closures to be created. It is necessary that the runtime would require some sort of garbage collection. For reference, the OCaml native compiler includes as part of its runtime a specialised garbage collector written specifically for OCaml programs.

Writing a new garbage collector would be very complex and heavily outside the scope of the project, so we would like to make use of a pre-existing solution for garbage collection in C. Fortunately, many garbage collectors exist, and the Boehm GC² was selected and used.

The Boehm GC is a garbage collector for C and C++, which exposes a function `GC_MALLOC` which can work as a replacement for `malloc`. Whenever `GC_MALLOC` is called, it runs the garbage collector by scanning the stack for values that could potentially look like pointers and so performing garbage collection. This means that in simple cases, it can be used as a drop-in solution for GC without extra configuration.

2.6 Setting up the environment

The source code of the compiler was managed using `git`, the repository of which was backed up by publishing to GitHub³. Development initially took place on the master branch, but once the compiler approached feature completeness new features in the compiler would be developed in a forked branch, worked on until they pass the regression tests, and then merged into the master branch.

In addition, a copy of the source code was continuously backed up using Dropbox, which was synced between two local copies of the code, on two separate machines. In this way, the code had four points of redundancy in the case of any computer failures.

²<http://www.hboehm.info/gc/>

³<https://github.com/t-veor/observable-ocaml>

2.7 Licensing of external code

The principal body of code being used is the OCaml core system⁴, which is released under LGPL v2.1. LGPL is a more permissive version of the GPL license, intended for use for libraries rather than full pieces of software. The LGPL license puts restrictions on what it calls “derivative works of the Library”, which are either modifications of the library or other software that includes the library or statically link to it, requiring that these derivative works are open source and also released with either the LGPL or the GPL library.

However, software that is designed to work with the library by linking against it but does not actually contain any portion of the library fall outside the scope of the license, which is the case with my compiler. As I am only releasing the source code of the compiler, which do not contain parts of the OCaml core system but link against it, the LGPL terms do not apply to the source code. They would however apply if I decided to release a compiled executable which has statically linked in the OCaml core system, but in fact a special exemption in the OCaml’s core system also covers this, allowing works which statically or dynamically link with a publicly distributed version of the OCaml core system to be exempt from the clauses of LGPL.

The other main library used is the Boehm GC⁵, which uses a custom permissive free software license, allowing for distribution and modification as long as a copy of the license is distributed with the library. This means in fact that my code is not within the scope of the license, since I do not distribute any part of the Boehm GC, but merely link against it in the compilation process. I have included the license within my repository nonetheless.

⁴<https://github.com/ocaml/ocaml/blob/4.05/LICENSE>

⁵<http://www.hboehm.info/gc/license.txt>

Chapter 3

Implementation

In the implementation, several modules were written in OCaml for implementing different parts of the compiler. The most significant modules were:

- `Typecollect`, for obtaining types from the `Lambda IR`;
- `Ccode`, for representation of C compilation target;
- `Ccompile`, for the actual compilation process from the `Lambda IR` to C.

3.1 Obtaining types from the Lambda IR

The `Lambda IR` does not have any type information associated with it, as within the OCaml compiler, `Lambda` was intended as the last representation before compilation into actual machine code, so all type information was erased from the underlying data.

While not having types isn't such a big problem for the compilation into C, one of the goals of the project was to have the resulting code be “observable”, which means where possible variables should be of a meaningful type in order to be displayed correctly in GDB.

3.1.1 Lambda Events

The OCaml compiler inserts `Lambda` events into the `Lambda IR` when the debug flag is set. A `Lambda` event is simply a wrapper around another `Lambda` expression that carries some

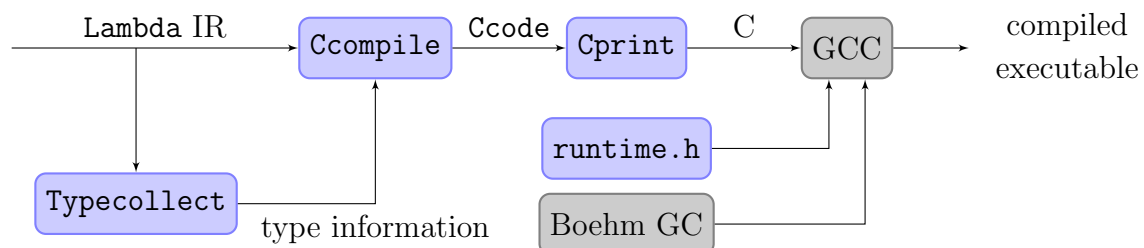


Figure 3.1: A representation of the stages in producing an executable output from my compiler, starting from the `Lambda IR`.

extra information, which includes the potential type of an expression and the current location in the source code.

Within the OCaml compiler, the purpose of a `Lambda` event is to mark where an interesting expression may be, so that the debugger may stop execution and inspect the state of the program just before the evaluation of the expression, or just after. This gives `Lambda` events two main useful properties, which are:

- `Lambda` events provide information about the current source code location of the expressions being currently compiled, which will be useful in for specifying source location (see §A.3);
- `Lambda` events provide type information about types of certain expressions.

Unfortunately, the compiler does not insert events that give types for every expression, nor is there a one-to-one correspondence between `Lambda` expressions and source-code expressions, since the `Lambda` IR may simplify certain expressions or insert new ones. However, every source-code variable was associated with at least one `Lambda` event describing its type. Therefore, determining types of variables used the `Lambda` events, and types of compound expressions were determined with very basic type- inference.

3.1.2 The `Typecollect` module

The `Typecollect` module therefore has a function `scrape` which does the following:

1. Initialise a hash table of variable identifiers to types (this is safe as the `Lambda` IR already assigns a different identifier to every variable)
2. Walk recursively down the `Lambda` tree:
 3. Upon encountering a `Lambda` event surrounding a variable:
 4. Set the variable and its type in the hash table
5. Return the now-filled hash table.

This preliminary pass over the `Lambda` IR passes the inferred types to the `Ccompile` module.

3.2 Representation of C

Before compilation can start, an appropriate representation of C must be chosen as the compilation target for the compiler.

3.2.1 Expressions to statements

OCaml is what is known as an expression-oriented programming language, where every syntactical construct is actually an expression of some kind. This is in contrast to C, which is statement-oriented. Contrast for example the following (slightly contrived) piece of code in OCaml and C:

```
let sq_max_plus_one x y =
  (let m = if x > y then x else y in m * m) + 1

int sq_max_plus_one(int x, int y) {
  int m;
  if (x > y) {
    m = x;
  } else {
    m = y;
  }
  return m * m + 1;
}
```

To solve this problem, my compiler assigns every sub-expression in the program to a separate variable. This means that if an expression consists of just a variable, use the variable name directly; otherwise, create and assign the result of each sub-expression to a new temporary variable.

By setting up a variable for each sub-expression, this creates an equivalence between variables and sub-expressions. The compilation of any expression therefore generates some sequence of statements, by the end of which the value of the expression is assigned to a variable. The compilation function therefore adds the statements to the current context, and returns the variable.

3.2.2 The Ccode module

The `Ccode` module is a module of the compiler that simply stores the type declarations for the internal representation of C. More details is given in the appendix at §A.1.

3.2.3 The Cprint module

The `Cprint` module is another module that's fairly straightforward – it contains functions for printing types from `Ccode` to an output stream, most likely a file. Its functions simply recursively traverse down the `Ccode` representation and prints out the corresponding C as it goes along.

3.3 Compiler basics

Structures from Subset 1 were implemented first, which included basic structures, some of which are included below. In the interest of brevity other more trivial structures are described in the appendix at §A.4.

3.3.1 let bindings

When compiling let bindings, special attention needs to be paid to the variable scoping (see §A.4.1). In OCaml, a `let` binding has the structure:

$$\text{let } x = \text{expr} \text{ in } \text{body}$$

Note that x is not a free variable of expr but is one in body , and also that the value of the overall expression is the evaluated value of body . Thus, a block is required to emulate the scoping correctly.

We therefore define the compilation of `let` bindings like thus, using the notation defined in §A.4.2:

```
comp<let x = expr in body> :=

declare result;

comp<expr>;
declare temp = var<temp>;
{
  declare x;
  x = temp;

  comp<body>;
  result = var<body>;
}
```

expr must be evaluated outside of the inner scope, where x is visible, and body must be evaluated inside the inner scope. We declare and assign the value of x only inside the inner scope. In addition, the actual value of expr must then be available outside the inner scope, so we propagate it outwards by declaring a variable `result` in the outer scope and performing its actual assignment in the inner scope.

OCaml also allows `let` bindings to be a shorthand for function declaration; function compilation will be discussed in §3.5.

3.3.2 Recursive bindings with `let rec`

Normally in a `let` binding, the variable being bound is not in scope for the expression being bound. This however makes it difficult to define recursive functions, so OCaml supplies the `let rec` binding which is useful for creating recursive functions, or sets of mutually recursive functions. For example, consider the following functions:

```
let rec add x y =
  if x = 0 then y else add (x - 1) (y + 1)

let rec even n =
  if n = 0 then true else odd (n - 1)
and odd n =
  if n = 0 then false else even (n - 1)
```

However OCaml allows `let rec` bindings to be used for creating a restricted class of non-functional recursive values. The typical example given is:

```
let rec x = 1::y and y = 1::x in expr
```

This binds `x` to the infinite list `1::2::1::2::...`, which is accomplished by making the list cyclical. Unsurprisingly, this is very rarely used feature within OCaml, but in the interest of fully supporting all features within our OCaml subset we would also like to compile expressions like this correctly.

Informally, the class of values that are allowed to be used as the right-hand side of a `let rec` binding are those where the recursively bound names occur only within a function, or a data constructor. This means that to preserve the semantics in C, the compiler therefore compiles `let rec` in two phases:

The compiler thus splits compilation of `let rec` into two phases:

- Variables are declared. If the associated expression has no free variables that are bound as part of the same `let rec`, evaluation can happen immediately; otherwise, its size is determined and then space for them is allocated with `malloc`, issuing them addresses in the process.
- Once all addresses are known, evaluation proceeds using the obtained addresses in place of variables which reference a value bound in the `let rec`.

3.4 OCaml value representation

This section largely details work undertaken to implement Subset 2, which deals with data representation and the language structures surrounding them.

3.4.1 Representation requirements

Before discussing the strategy for representing OCaml values, it is useful to discuss the problems that the value representation needs to solve.

Polymorphic types

Polymorphic code does not know the precise type of values it is manipulating, so cannot deal with variable size data as they may not copy polymorphic values correctly.

OCaml blocks

More complex types such as tuples and records are represented by a construct known as an OCaml block, which is a variable length array of values with a header containing its length and an integer tag value.

The Lambda IR in fact normalises all data structures into blocks, including references (they're a mutable singleton block), arrays, modules etc. which is rather convenient as we can implement all of these data types for free by implementing blocks.

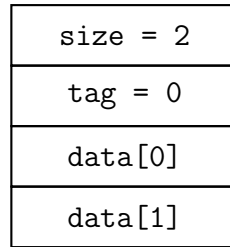


Figure 3.2: Example OCaml block containing two values with tag 0.

Algebraic Data Types

A major feature in OCaml is the ADT, which combines elements of both enums and record types. As an example, consider the following type declaration:

```
type color =
  | Red
  | Green
  | Blue
  | Gray of int
  | RGB of int * int * int
```

The data constructors (`Red`, `Green`, `Blue`, `Gray`, and `RGB`) within an ADT declaration are referred to as variants, and the type is a union of all of these types together. In the `Lambda IR`, data constructors that do not have any parameters are represented as integers starting from 0 (so `Red` is 0, `Green` is 1, and `Blue` is 2), and data constructors that do are represented using OCaml blocks, with tag values starting from 0 (so `Gray` is an OCaml block of size 1 with tag 0, and `RGB` is an OCaml block of size 3 with tag 1). This is the significance of the tag values – they differentiate between different variants in ADTs.

3.4.2 Representation strategy

As a consequence of the fact that we want the resulting C code to be observable, whenever there is an exact primitive type the C code should attempt to use the equivalent type in C as much as possible.

Representation for non-primitive types however is more complex. Integer types and OCaml blocks must be unified in representation, because variants that don't have any parameters and variants that do can be of the same type.

Tagged pointers

OCaml blocks must be allocated on the heap since they are of variable size, so have to be referenced using a pointer. This means that we need a type that can either be a pointer or an integer, which is what tagged pointers provide.

Tagged pointers are just a union type between pointers and integers. On most architectures, pointers are word-aligned, meaning that the lower bits of a pointer are always 0. The tagged pointer approach employed in this compiler is to use the least significant bit

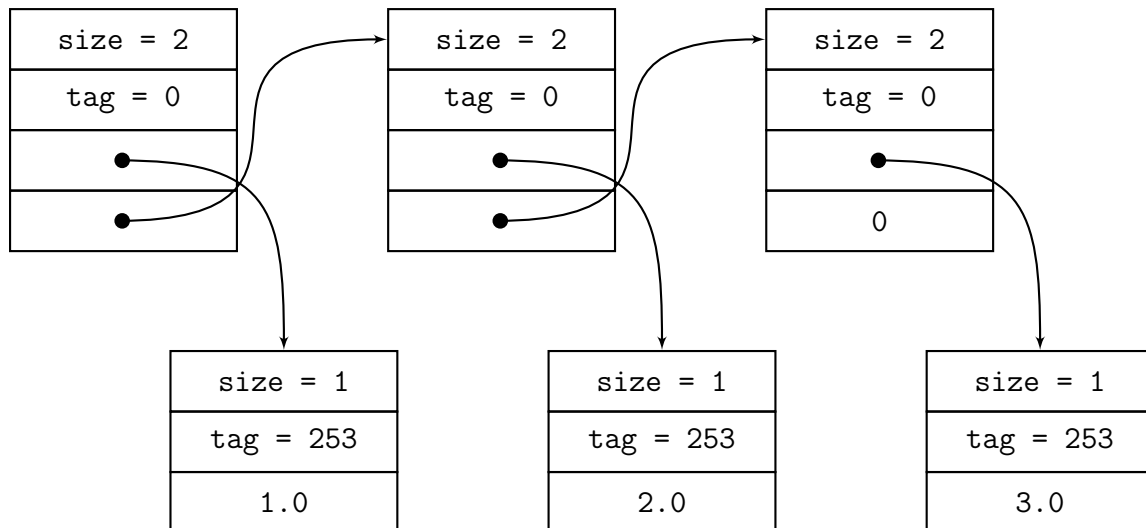


Figure 3.3: Example box-and-pointer diagram for the list `[1.0; 2.0; 3.0]`. Floating point numbers must be boxed to be stored in a block, so a special block is created for each one with the special tag 253.

of an 8-byte word as the tag bit to differentiate between pointers and integers, and the remaining 63 bits to store the integer or pointer.

There is a choice as to which way round the tag bit should be – should 0 represent integers or pointers? I chose to use 0 for pointers, and 1 for integers, which means that the “boxed” version of a pointer is identical to the pointer in memory. This has the effect that dereferencing pointers is cheap and we can use a conservative GC with no modification – see §3.6.

Polymorphic values

We can use the tagged pointer representation to represent polymorphic values as well, by boxing all non-integer values into a block. To disambiguate these blocks from other normal blocks so that at runtime, the debugger is able to see what type they really are, we assign a special tag to them which for example marks the block as containing only floats or strings.

3.4.3 Representation in C

By taking advantage of flexible array members, it is easy to implement an OCaml block in C.

```

typedef struct _block {
    uintptr_t size : 56;
    uintptr_t tag : 8;
    any_type data[];
} block;

```

Recall that a block needs to store its size, an integer tag, and any number of other OCaml values. Since OCaml tags only range between 0-255¹, and 45 bits are sufficient for storing the size of a block in words, we can reduce the amount of space used for the header using C bit-fields. This means the header only needs to be one word long.

We can now implement actual OCaml values as a union type:

```
typedef union _value_type {
    intptr_t i;
    block* block;
} value_type;

#define BOX_INT(v) ((value_type){.i = (intptr_t)(v) << 1 | 1})
#define UNBOX_INT(v) ((v).i >> 1)

#define BOX_BLOCK ((value_type){.block = (v)})
#define UNBOX_BLOCK ((v).block)

#define IS_INT(v) ((v).i & 1)
```

BOX_INT and UNBOX_INT demonstrate how to box integers into a `value_type`, and likewise for block pointers. We also have a special macro IS_INT, which checks if a `value_type` is holding an integer or a pointer – it simply checks the last bit, returning 1 if the last bit is also a 1.

Type-punning with any_type

While blocks normally hold an array of other `value_types`, we would like to have special blocks that represent the result of boxing certain other primitive types, such as floats and strings. To do this, we declare a union type `any_type`²:

```
typedef union {
    double fl;
    char* str;
    value_type value;
} any_type;
```

block therefore declares a `any_type` array to support both storing `value_types` as well as special blocks that store doubles and char*s.

3.4.4 Conversion between C types

Despite the Lambda IR having already gone through type inferencing, there are still a few cases in which “casting” is necessary. This is because, for example, the C types for polymorphic types and monomorphic types in OCaml are different, so a C cast is necessary when passing a value of a known type to a polymorphic function.

¹In fact, the native OCaml runtime restricts the number of possible variants to 246, using the tags 0-245 for variants. It uses the last 10 possible tags for special tags.

²For clarity, we ignore the problems associated with recursive type definitions in C, assuming the correct forward declarations.

In general, there are several cases where we need to perform a conversion operation in C. These cases are:

- A conversion from an integer to an OCaml value is required, because the **Lambda** IR uses integers for representing certain non-integer OCaml values.
- A conversion from any other type to an OCaml value, because a variable is being passed into a polymorphic function, or being placed into a block.
- An actual conversion between types, such as from integers to floating point numbers.

The cases all involve a mismatch between the C types of two expressions, so are handled using a function that does the following:

1. If the source and target types are the same, do nothing.
2. If either type is **any_type**, pack or unpack the value as appropriate.
3. If either type is **value_type**, box or unbox the value as appropriate.
4. Otherwise, perform a C cast between source type and target type.

3.4.5 Pattern matching

OCaml employs pattern matching in many constructs of the language, particularly in its **match** expressions. Fortunately, the **Lambda** IR usually compiles these down to an equivalent set of **if** expressions and **let** bindings. In the case of variants however, pattern matching typically compiles down into a **Lswitch** expression.

Lswitch expressions

Lswitch expressions correspond to match statements on a variant expression. For an example, consider the type and match expression:

```
type color =
  | Red
  | Green
  | Blue
  | Gray of int
  | RGB of int * int * int
```

```
match c with
  | Red -> 0
  | Green -> 1
  | Blue -> 2
  | Gray x -> 3
  | RGB (r, g, b) -> 4
```

This match statement is compiled into the following **Lambda** expression:

```
(switch* c/xxxx
  case int 0: 0
  case int 1: 1
  case int 2: 2
  case tag 0: 3
  case tag 1: 4)
```

There's one important difference between this and a C switch statement: each of the cases predicate on both whether the value is an integer or a block in addition to its value or tag.

One `Lswitch` statement therefore compiles into two switch statements in C, one for the integers and one for the tags, which are the two branches of an if statement that checks if the value being switched on is an integer or a value using the tagged pointer check.

3.5 Function compilation and closure conversion

Functions and closures are the final major feature required to compile the target subset of OCaml into C. The following sections will discuss the motivations for a closure representation and the implementation of such a representation, which is the majority of work undertaken in the implementation of Subset 3.

3.5.1 Local functions

All functions in C are required to be defined at top-level, which means that nested function declarations are not possible. This is in contrast to OCaml, where function definitions are simply expressions like any other, and thus can be defined locally and passed as values. In order to emulate this behaviour in C, whenever we come across a function definition we lift the function definition to the toplevel scope, compile the function there, and then return its function pointer when we come back.³

We can write the compilation of a local function like thus, using the notation from §A.4.2:

```
comp<fun args... -> body> :=

/* in top-level */
return_type local_function(args...) {
  comp<body>;
  return var<body>;
}

/* in current context */
declare result = &local_function;
```

³This clearly does not deal with lexical closures, so we actually return a pointer to a closure object instead of a function pointer, but the idea is the same.

3.5.2 Function Types in C

In OCaml, one way of viewing functions is always as functions of one argument, which can return other functions. As an example, the function type `int -> float -> int` represents a function that takes an integer and returns a `float -> int`, which is a function that takes a floating point number and returns an integer.

While this is a correct high-level view of functions, this is not suitable for a low-level implementation at all, since it is much more efficient for functions to actually accept multiple arguments instead of taking one argument at a time.

In C by contrast, a function declaration consists of a return type, and a list of input arguments. We therefore need a consistent conversion between OCaml function types and C function types, so we pick the most obvious one – all the types in the OCaml function type are the arguments to the C function, and the final type is the return type of the C function.

For example, a function of type `int -> float -> str` is compiled to `char* (*)(int, double)` in C.

3.5.3 Closure representation

Closures are, implementation-wise, a structure that stores both a function pointer and an environment, containing values required for the execution of the function.

Our closure representation essentially requires storing a function pointer and some list of values, so taking advantage of flexible array members again we arrive at the following definition:

```
typedef struct _closure_type {
    void* (*f)();
    struct _closure_type* next;
    any_type4 args[];
}
```

As you can see, this definition contains a function pointer, and a variably-sized array of arguments, which we reused `any_type` from §3.4.3 to implement. Closures also have a `next` field which points to another `closure_type`, allowing them to act like a linked list. The motivation of this is discussed in partial application compilation, in §3.5.4.

Using closure objects

In order to make the closure object useful, we modify all functions to instead take an extra parameter, `closure_type* closure_obj`, which stores the pointer to the current closure object. From there, the function is able to access closure values by indexing `closure_obj->args`.

Calling a closure can be done by invoking the function pointer with the required arguments, passing in the closure pointer as the last argument.

⁴Note that we are reusing `any_type`, which means we need to extend its definition and the casting rules to accept more types, such as integers, function pointers, and closure types.

```
cl->f(args..., cl);
```

Promoting ordinary functions to closures

This necessitates some sort of promotion process where functions that do not require environment capture are promoted to closures. This is done by creating another function which takes all the same arguments as the original function plus the closure object. This function just passes the arguments along to the original function.

```
return_type promoted_closure(args..., closure_type* closure_obj) {
    return f(args...);
}
```

```
closure_type* cl = MALLOC(sizeof(closure_type));
cl->f = (void*(*)(()))&promoted_closure;
cl->next = NULL;
```

Unification of closures and functions

For ease of representation, it was decided to unify functions and closures in C as well. This means that all functions are promoted to closures, and all function applications in OCaml are compiled into closure calls in C, simplifying the implementation at the cost of possible performance losses.

3.5.4 Partial application compilation

Partial application is one of the major use-cases for closures, and is modelled in my compiler using a closure object. Whenever there is a partial application, a function is created instead that takes the remaining parameters, and a closure object is created to store the partially-applied arguments. The newly created function simply obtains the previously partially applied arguments from the closure object and passes them along with its own arguments to reconstruct the original function call.

As an example, observe the following C-style pseudocode, where a closure `cl_f` (which requires three integer arguments and returns an integer) is partially applied with two integers, `a` and `b`, and another closure `cl_g` is returned⁵.

```
int g(int c, closure_type* closure_obj) {
    int arg_0 = closure_obj->data[0];
    int arg_1 = closure_obj->data[1];

    closure_type* cl = closure_obj->next;
    cl->f(arg_0, arg_1, c, cl);
}

closure_type* cl_g = MALLOC(sizeof(closure_type) + sizeof(any_type)*2);
```

⁵Cast operators have been omitted for simplicity.

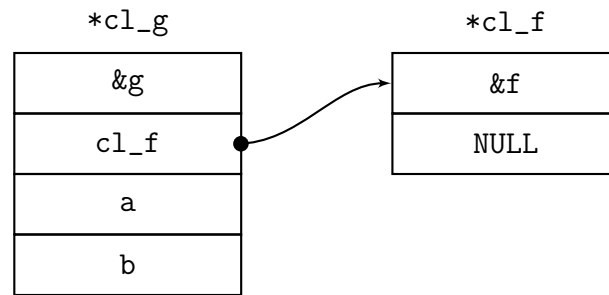


Figure 3.4: Example result of a partial application of a function `f(a, b, c)` with the arguments `(a, b)`. The arguments `a` and `b` are pushed onto a new closure object, which contains a function pointer to `g` and a pointer to the previous closure object. When `cl_g` is called with an argument `c`, `g` will obtain `a` and `b` from the closure object and pass them together with `c` to `f`.

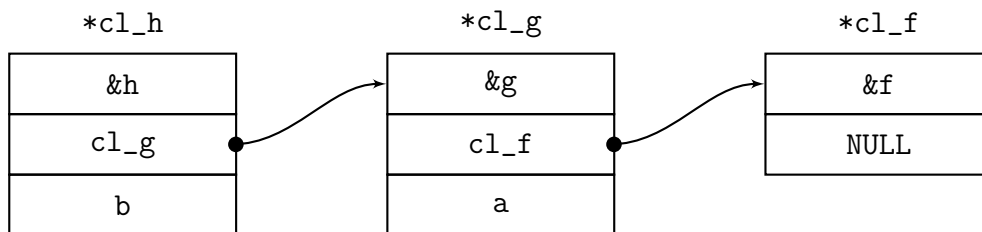


Figure 3.5: Example of a chained double application. In this case, the function `f(a, b, c)` has been applied with `a` and `b` separately, creating two closure objects, `cl_g` in the first application, and `cl_h` in the second. Here, `h` translates a call `h(c)` into `g(b, c)`, which in turn translates that call into `f(a, b, c)`.

```
cl_g->f = &g;
cl_g->next = cl_f;
cl_g->data[0] = a;
cl_g->data[1] = b;
```

Chaining partial applications

An important requirement is that a partially applied closure needs to act the same as an unapplied closure, as in we must be able to partially apply it again. This requirement is the justification for why closures are implemented as a linked list – each closure needs to know the function pointer of the next function they need to invoke, but that isn't always possible to determine statically⁶.

Thus, each closure resulting from partial application points to the closure from which it was derived from so their function can figure out what function pointer to invoke (see figure 3.4).

⁶As an example, consider a partially applied function which is passed as an argument to a higher-order function, which further partially applies the function.

3.5.5 Lexical closure compilation

Lexical closures are another common use of closures, and occur when a function refers to values in an enclosing scope. This presents a problem in C, as it does not allow nesting functions.

Because our closure representation allows storing arbitrary data already, this is simple to implement using closure objects. When compiling any local function, first check if the function contains any free variables. If it does, take the value of all the free variables at that point and push them onto the closure object, and when compiling the function body, before compiling re-assign all lexically bound variables to values from the closure object.

As an example, consider the compilation of the following OCaml code:⁷

```
let f x y =
  let g z = x + y + z in g
```

This is compiled into the following C-style pseudocode:

```
int f(int x, int y, closure_type* closure_obj) {
  closure_type* cl_g = MALLOC(sizeof(closure_type) + sizeof(any_type)*2);
  cl_g->f = &g;
  cl_g->next = NULL;
  cl_g->data[0] = x;
  cl_g->data[1] = y;

  return cl_g;
}

int g(int z, closure_type* closure_obj) {
  int x = closure_obj->data[0];
  int y = closure_obj->data[1];

  return x + y + z;
}
```

3.5.6 Parametric polymorphism

Parametric polymorphism is an important feature in OCaml, allowing programmers to write general code without knowing the type of its arguments in advance. As discussed in §3.4 we use the `value_type` representation of polymorphic values when defining polymorphic functions.

This works fine for passing simple values and polymorphic datatypes, as long as we remember to cast values to `value_type` when passing values to polymorphic functions, and cast back to their actual types when receiving values from function calls.

However, passing other functions (closures) into polymorphic functions is more problematic.

⁷In an actual compilation, this will get eta-expanded to make the function types consistent (see §A.6.1) but we suppose this doesn't happen in this example for simplicity.

Erasing function types

When passing a non-polymorphic function, e.g. `float -> float`, to polymorphic function expecting an `'a -> 'b` requires a cast between the two types. This is because the polymorphic function is representing `'a` as `value_type`, and so will attempt to pass data of the type `value_type` into the function, and will expect a return type also of `value_type`. Thus in order to cast `float -> float` we will need to add a wrapper function which performs the casts.

```
value_type g(value_type x, closure_type* closure_obj) {
    double new_x = UNBOX_FLOAT(x);

    closure_type* cl = closure_obj->next;
    double result = cl->f(new_x, cl);

    value_type new_result = BOX_FLOAT(result);
    return new_result;
}

closure_type* cl_g = MALLOC(sizeof(closure_type));
cl_g->f = &g;
cl_g->next = cl_f;
```

This in fact needs to happen any time it's possible to “lose track” of the actual type of a function, i.e. it's possible the function will be used in a situation where its type has been generalised away. This includes adding functions to an OCaml block (because the data structure may be passed to a function polymorphic in a subtype of the data structure), or accessing functions from an OCaml block⁸, or storing and retrieving functions from closure data.

Thus, the casting rules from §3.4.4 need to be modified.

1. If the source type is `value_type` or `any_type`, when casting back assume all of its argument and return types are `value_type`, and then cast it back to the expected type using the technique from the previous section.
2. If the target type is `value_type` or `any_type` and the source type is a function, first erase types from that function by rewriting all its argument and return types to `value_type` using the technique from the previous section before proceeding with the cast.

“Upcasting” functions

Another case when dealing with polymorphic functions is when the expected type of a function has fewer parameters than the actual type, e.g. passing a function of type `float`

⁸It's not safe to simply remove the head from the closure chain to undo this cast, as there's no guarantee the last transformation applied to a closure will be the cast – the closure may have been partially applied or cast again to something else.

`-> float -> float` to a higher-order function that is expecting a `'a -> 'b`. This poses a problem for the type system for functions we decided on in §3.5.2.

To see why, consider a polymorphic function which receives a function `'a -> 'b`, and needs to apply it to something of type `'a`. How does it know whether to treat this as a full application, where it needs to invoke the function as a closure, or a partial application, where it needs to create a new closure object?

One solution is to solve this on the caller's side. Essentially, we want to transform a C function signature from:

```
value_type f(value_type x, value_type y, closure_type* closure_obj);

into9:
```

```
closure_type* g(value_type x, closure_type* closure_obj);
// where the returned value points to the function
value_type h(value_type y, closure_type& closure_obj);
```

This is to ensure that from the point of view of a polymorphic function, if the same number of elements is applied to the function type, then it can be considered fully applied.

This transformation can be modelled using the current closure representation, using a process I refer to as “upcasting”. In this process of upcasting a function `f`, two more functions are created, which are `g` and `h`.

`g`'s role is to act as the resulting function that will be passed into whatever polymorphic function. It's essentially a wrapper around a partial application.

```
closure_type* g(value_type x, closure_type* closure_obj) {
    closure_type* cl = MALLOC(sizeof(closure_type) + sizeof(any_type));
    cl->f = &h;
    cl->next = closure_obj;
    cl->data[0] = x;

    return cl;
}
```

`h` acts as the counterpart function to a polymorphic function, which takes the data that `g` has set up for it and applies it to `f`.

```
value_type h(value_type y, closure_type* closure_obj) {
    value_type x = closure_obj->data[0];

    closure_type* cl = closure_obj->next;
    value_type result = cl->f(x, y, cl);

    return result;
}
```

The surrounding code adds `g` as a closure onto `f`'s closure.

⁹The `closure_type*` is actually also cast into a `value_type`, to match the type the polymorphic function is expecting.


```
closure_type* cl_g = MALLOC(sizeof(closure_type));  
cl_g->f = &g;  
cl_g->next = cl_f;
```

By tracing through the executions, it can be seen that an application by x followed by an application by y gives the correct function call $f(x, y)$.

3.6 Garbage Collection

We can use the Boehm GC to implement a garbage collector without needing to write one ourselves. Because of the way we have defined the implementation of OCaml values, all values potentially representing pointers will be unchanged in their actual binary value. This means that we can simply “drop-in” the Boehm GC by including the following in our runtime:

```
#include "gc.h"  
#define MALLOC(v) GC_MALLOC(v)
```


Chapter 4

Evaluation

The resulting compiler was evaluated in two key aspects, which are the resulting speed of the produced executables and the observability of the debug output.

4.1 Regression tests and feature completeness

To test the correctness of the compilation, over the course of the project 21 different regression tests were written to test different features of the language were being compiled correctly. They include simple tests which test one feature each, to more complex tests which test multiple features combined in different variations.

With every iteration of the compiler, regression tests are run against it to ensure that the output of the compiler remains correct. To do this, a simple regression test script was written which compiles the same OCaml program against the OCaml native compiler and my compiler, and asserts that the output of both executables match.

One of the most complex regression tests is one which reimplements many of the list processing functions in the OCaml standard library. These functions use many advanced features of the language, including recursion, pattern matching, parametric and datatype polymorphism, and closure creation.

4.2 Benchmarks

A most natural way to evaluate the compiler is to compare the execution times of the output, and the most natural metric to compare the compiler against is the existing OCaml compiler. The basic idea of all the benchmarks is simple – it’s to compile the same program under the OCaml standard compilers and under my compiler, and compare the execution speed of their outputs.

Several different configurations for comparisons can be attempted. OCaml supplies two compiler backends, the OCaml native compiler (`ocamlopt`) and the OCaml bytecode compiler (`ocamlc`). For our purposes, we will be mostly considering the output of the native compiler, as the bytecode interpreter unsurprisingly is at least one order of magnitude slower than the native compiler.

In addition, since my compiler only produces C code, we have a choice as to which compiler to compile the C code with, and under which configurations. I chose the most popular C compilers, `gcc` and `clang`, and compiled the code under the four optimisation levels provided (`-O0`, `-O1`, `-O2`, and `-O3`).

To simplify the process of running the many benchmarks against the configurations, a script `run_benchmarks.py` was written, and the results were plotted using Python and `matplotlib`.

4.2.1 Sourcing Benchmarks

Benchmarks programs were taken from the Computer Language Benchmarks Game (CLBG)[5], the `operf-micro`[6] OCaml library, and the rest were written by me.

These programs were chosen to exemplify a wide range of features within the OCaml language, particularly to exercise the more advanced features of the subset of OCaml which I am targeting.

Benchmarks were adjusted to take between 0.5 to 2.0 seconds to run so that the timer does not significantly affect the running time, and were run 50 times each on an idle Linux laptop.

On the whole, C compilers do quite well in comparison to the OCaml native compiler being only a small constant factor time slower in most cases and matching and outperforming the native compiler in select cases. Also of note was that in all benchmarks, the C compilers outperformed the OCaml bytecode compiler, which is surprising since no significant effort was made into optimisation of the C output.

A breakdown of the benchmarks is included below:

- `binary-trees` is adapted directly from the CLBG, and is a benchmark for garbage collection.
- `collatz` is a benchmark written by me, where the longest Collatz chain is found between 0 and an upper limit using a tail-recursive function.
- `even_fib` and is composed of mainly a simple tail-recursive function.
- `fibonacci` is a benchmark written by me, and performs non-tail-recursive recursion.
- `lens` is a benchmark adapted from the `operf-micro` library, and uses Haskell-like lens objects to perform calculations on a rectangle record type. This benchmark performs plenty of closure operations and therefore is a test of the speed of closures.
- `mandelbrot` is adapted directly from the CLBG, and is a benchmark for imperative-style floating point manipulation.
- `n-body` is adapted from the CLBG with minor changes as it requires arrays, which were not part of the target subset for my compiler. It is a test for floating point operations in a more functional style.
- `rule30` is a benchmark written by me, the focus of this benchmark being list manipulation and allocation and deallocation of lists.

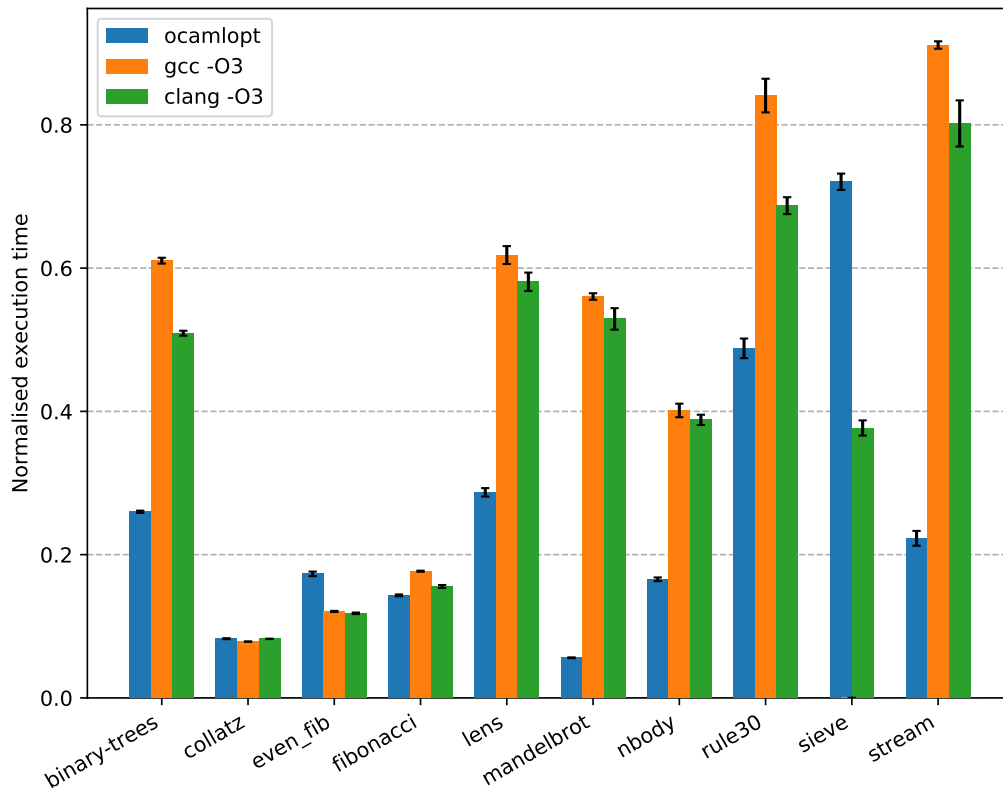


Figure 4.1: Execution times for comparison between the OCaml native compiler (`ocamlpt`), and the C compilers at the highest optimisation level. Execution times were normalised with respect to the OCaml bytecode compiler, setting the execution time of the compiled bytecode to be 1.0. Error bars represent 1 standard deviation in the execution time.

- **sieve** is a benchmark taken from **operf-micro**, and performs list manipulation via a tail-recursive function.
- **stream** is a benchmark written by me, and is heavy in both custom in data manipulation, and closure creation and application.

Notable results from the benchmark include:

- The drop-in garbage collection is unsurprisingly much slower than the OCaml GC, as it is a conservative GC and does not have any domain-specific knowledge. This can be best seen in the **n-body** benchmark.
- The C compilers perform extremely well on benchmarks that involve few allocations and straightforward tail-recursive code, often beating even the OCaml native compiler. This is seen in the **collatz**, **even_fib**, and **sieve** benchmarks.
- Strangely, the C compilers perform exceptionally bad in benchmarks involving floating point manipulations, as can be seen in **mandelbrot** and **nbody** benchmarks.
- Benchmarks which involve lots of closure creation and application are also slower relative to the OCaml native compiler, as can be seen in the **lens** and **stream** benchmarks.
- In the **sieve** benchmark, the executable compiled with **gcc** actually segfaults, the cause of which is a failure to perform a tail-call optimisation.

4.2.2 Investigating performance differences

Instrumentation

Having obtained execution times for the different benchmarks, a natural question to ask is why the the OCaml and C compilers perform the way that they do; we would like some way of profiling the code to see what parts of the code take longer to run.

Fortunately, a key consequence of the compiler being from OCaml to C is that standard C tools will work on the resulting code, including Gprof, a profiler which can be enabled in **gcc** with the **-pg** flag. Gprof can provide information as to how much time is spent in each function via the flat profile, as well as information about how the call graph, or which functions called what other functions and how many times.

It turns out that OCaml also supports using Gprof to profile its native code output simply by adding the **-p** flag to **ocamlopt**, giving us a convenient way to compare the execution of the C executable and the OCaml native executable. We can therefore use this profiler to investigate performance differences between the OCaml native compiler and the C compiler.

% time	cumulative seconds	self seconds	calls	self ms/call	total ms/call	name
100.00	0.93	0.93	1	930.03	930.03	camlTest__entry
0.00	0.93	0.00	1125001	0.00	0.00	caml_ml_output_char
0.00	0.93	0.00	1125000	0.00	0.00	camlTest__print_byte_1232
0.00	0.93	0.00	1489	0.00	0.00	caml_page_table_modify
0.00	0.93	0.00	28	0.00	0.00	caml_stat_alloc
...						

% time	cumulative seconds	self seconds	calls	self ms/call	total ms/call	name
44.37	7.00	7.00				main
10.65	8.68	1.68	676990954	0.00	0.00	BOX_GEN
8.71	10.06	1.38				GC_malloc_kind
8.24	11.36	1.30				GC_build_fl
7.16	12.49	1.13				GC_apply_to_all_blocks
3.55	13.05	0.56				GC_mark_from
2.66	13.47	0.42				GC_allochblk_nth
2.28	13.83	0.36				GC_clear_stack_inner
1.77	14.11	0.28				frame_dummy
1.71	14.38	0.27				GC_reclaim_clear
1.05	14.54	0.17				GC_malloc
0.76	14.66	0.12				GC_find_header
0.63	14.76	0.10				GC_clear_hdr_marks
0.63	14.86	0.10				GC_finish_collection
0.48	14.94	0.08				GC_generic_malloc_inner
...						

Figure 4.2: Truncated Gprof outputs for the OCaml native executable and the C executable, which has been highlighted with the roles of each function. Functions highlighted green are logical functions for the execution of the program, functions highlighted red are to do with allocating blocks on the heap, and functions highlighted blue are functions used by the garbage collector. Note that compiling with profiling information inserts extra instructions and function calls for instrumentation purposes so the times shown are not indicative of how fast the benchmarks execute otherwise.

Floating point and polymorphic structures

For example, one discrepancy which we may wish to investigate is the `mandelbrot` benchmark, which C compilers perform much worse on despite having been written in imperative-style code.

I collected profiling information using Gprof from both the native and C executables, a truncated version of which can be seen in figure 4.2. As shown below, the OCaml executable spends almost 100% of its execution time in the main logic of the program (which is the `entry` function), in comparison to the C executable, which only spends 44.37% of the execution time in the main logic. Instead, the majority of the time spent during execution is allocating new blocks and garbage collecting old ones.

Upon further investigation, it was found that the `mandelbrot` benchmark stored floats inside `float refs`, and the `Lambda` representation normalises references into singleton OCaml blocks. This means that according to the casting rules as described in §3.4.4, whenever a `float` needs to be stored inside a `float ref` a new tagged OCaml block is allocated on the heap and then the pointer is stored in the `float ref`. This means that mutable floating point fields within OCaml blocks are in fact incredibly slow, as each store necessitates creating a new block on the heap, and needing to GC the block that was replaced.

The same is true for the `nbody` benchmark, which uses mutable float fields in a record to store the position, velocity, mass etc. of the different celestial bodies.

“Reduced allocations” mode

This problem means that floating point operations become incredibly slow, but it is necessary for observability, as non-integral or pointer types may be tagged with their type within polymorphic structures so that a debugger is able to infer their types. If we relax this requirement however, since the OCaml runtime does not require data to be tagged with their type (as the code has already been type-checked), we can store floating point numbers (and other types, such as closures and strings) directly within OCaml blocks without needing to make a separate object on the heap to tag their types.

I implemented this mode which is accessible via a C compiler flag, and obtained results which demonstrated far more favourable execution times especially for the `mandelbrot` and `nbody` benchmarks, as can be seen in figure 4.3.

While this change does increase the performance of the compiler, it is worth noting that this means that polymorphic structures are no longer observable as a debugger cannot determine all the types at runtime, as well as meaning that functions that require some degree of runtime reflection such as OCaml’s polymorphic comparisons do not function. This means that while the results provided by this mode are interesting and represent the performance of the compiler under perhaps a better representation of polymorphic data, it is not suitable for use generally.

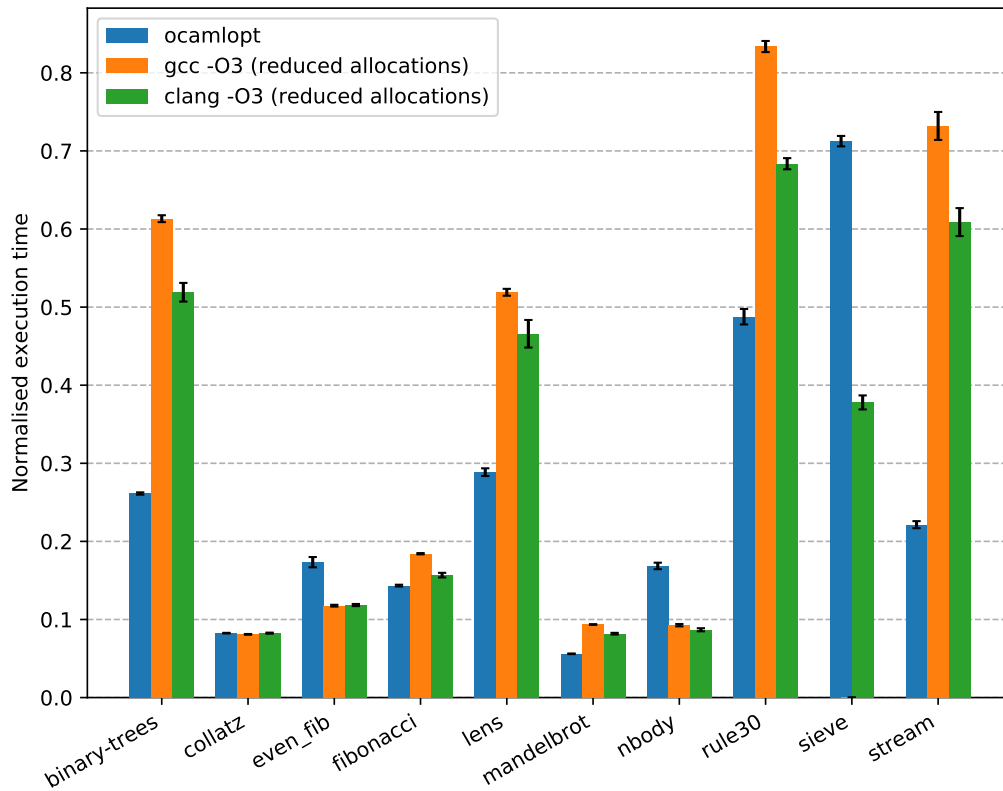


Figure 4.3: Execution times for comparison between the OCaml native compiler (`ocamlpt`), and the C compilers at the highest optimisation level, but with the reduced allocations flag enabled. While most of the benchmarks do not change much, note that the execution times for `mandelbrot` and `nbody` decrease significantly.

```

0000000000400fe0 <local_func_1215>:
 400fe0:    48 85 f6                test    rsi,rsi
 400fe3:    75 0b                   jne     400ff0 <local_func_1215+0x10>
 400fe5:    48 89 f8                mov     rax,rdi
 400fe8:    c3                      ret
 400fe9:    0f 1f 80 00 00 00 00    nop     DWORD PTR [rax+0x0]
 400ff0:    48 8b 52 10             mov     rdx,QWORD PTR [rdx+0x10]
 400ff4:    48 83 c7 01             add     rdi,0x1
 400ff8:    48 83 ee 01             sub     rsi,0x1
 400ffc:    48 8b 02                mov     rax,QWORD PTR [rdx]
 400fff:    ff e0                   jmp     rax
 401001:    0f 1f 44 00 00          nop     DWORD PTR [rax+rax*1+0x0]
 401006:    66 2e 0f 1f 84 00 00    nop     WORD PTR cs:[rax+rax*1+0x0]
 40100d:    00 00 00

```

Figure 4.4: Disassembly of the the function `let rec add x y = if y = 0 then x else add (x - 1) (y + 1)` compiled using my compiler and then using `gcc -O3`. The compiler is able to optimise the tail call, but is not able to see through the closure representation to optimise into a loop, instead jumping to a function pointer obtained via the closure object (the pointer to which is initially stored in the `rdx` register).

Tail recursion

Another interesting question to ask is if the C compilers can see through the closure representation to perform tail-call optimisation, since it is far more idiomatic to write tail-recursive functions in OCaml than it is to write explicit iteration. It is therefore important for performance that the C compilers can do tail-call optimisation to avoid the extra overheads of function calls as well as avoiding stack overflows.

To do this, we can use the `objdump` Linux utility, which can “disassemble” the executable, printing out the assembly mnemonics corresponding to the machine code. Figure 4.4 shows the disassembly of the following simple tail-recursive function:

```

let rec add x y =
  if y = 0 then
    x
  else
    add (x - 1) (y + 1)

```

As can be seen, the C compiler is able to infer that the closure application is equivalent to a function call in tail-call position, despite not being able to see through the closure representation explicitly, and has therefore compiled the closure application into a single `jmp` instruction. This means that tail-recursive functions do not incur the full penalties from a function call, but a small amount of overhead from needing to load in an address

Stack overflow

On the `sieve` benchmark, the `gcc` executable compiled under all optimisation levels segfaults, which is because of a stack overflow. This is particularly confusing because the `sieve` benchmark was written to be tail-recursive, and also the executable produced

by `clang` does not segfault, indicating that `clang` must have been able to perform the tail-call recursion.

After some investigation, the offending code was found to be this:

```
typedef union {
    void* ptr;
} val;

void* g(val);

val f(val x) {
    return {.ptr = g(x)};
}
```

When compiled with `gcc`, this produces the rather confusing output:

0000000000400590 <f>:			
400590:	48 83 ec 08	sub	rsp,0x8
400594:	e8 57 ff ff ff	call	4004f0 <g>
400599:	48 83 c4 08	add	rsp,0x8
40059d:	c3	ret	
40059e:	66 90	xchg	ax,ax

Somehow, the cast back into the union type prevents `gcc` from detecting the function call is in tail-call position in this specific case, despite the fact that the resulting machine code could obviously be optimised and the function call be put in tail-call position.

Closure creation

For a lot of benchmarks the C compilers perform far worse than the OCaml native compiler which is likely to be due to the fact that the closure operations in C are far slower than the OCaml native compiler can compile them.

To confirm this, I collected profiling information from the `lens` benchmark, which is perhaps the most heavy benchmark in terms of closure creation and application. The truncated flat profiles can be seen in figure 4.5.

As can be seen by the results, the execution time of the C executable is strongly dominated by the garbage collector and functions used in the process of closure creation and application, with functions implementing logic actually being a small fraction of the execution time. This is in strong contrast to the OCaml code, where the run time is dominated instead by the actual logic of the program and the printing functions.

This suggests that in certain workloads the closure representation can degrade the performance significantly, resulting in unnecessary amounts of work being put into closure operations as compared to if the compiler was able to see through them. Furthermore, since the closure operation necessitates allocating new blocks onto the heap, creation of lots of closures can put much more extra stress onto the garbage collector.

These problems may be allayed with a better closure representation, for example turning partial application into generating function stubs which push the correct arguments into the correct registers before jumping to the function body. Unfortunately, there was insufficient time to investigate more performant closure representations.

% time	cumulative seconds	self seconds	calls	self ms/call	total ms/call	name
18.87	0.10	0.10	20000004	0.00	0.00	camlTest_std__compose_1267
9.43	0.15	0.05	5000001	0.00	0.00	camlTest_std__lens_rect_area_1376
9.43	0.20	0.05	5000001	0.00	0.00	caml_ml_output_bytes
5.66	0.23	0.03	10000002	0.00	0.00	camlCamlinternalFormat__output_acc_64856
5.66	0.26	0.03	5000005	0.00	0.00	caml_alloc_string
5.66	0.29	0.03	5000001	0.00	0.00	camlCamlinternalFormat__fun_84305
3.77	0.31	0.02	10000003	0.00	0.00	camlCamlinternalFormat__make_printf_62490
3.77	0.33	0.02	10000002	0.00	0.00	camlPrintf__fun_1347
3.77	0.35	0.02	5000001	0.00	0.00	caml_format_int
3.77	0.37	0.02	5000001	0.00	0.00	parse_format
2.83	0.39	0.02	20000004	0.00	0.00	camlTest_std__fun_1501
1.89	0.40	0.01	15000003	0.00	0.00	caml_apply2
1.89	0.41	0.01	10000002	0.00	0.00	camlTest_std__fun_1631
1.89	0.42	0.01	10000002	0.00	0.00	camlTest_std__fun_1635
1.89	0.43	0.01	5000611	0.00	0.00	caml_putblock
1.89	0.44	0.01	5000002	0.00	0.00	camlPrintf__fprintf_1294
1.89	0.45	0.01	5000002	0.00	0.00	camlPrintf__kfprintf_1255
1.89	0.46	0.01	5000001	0.00	0.00	caml_alloc_sprintf
1.89	0.47	0.01	5000001	0.00	0.00	caml_ml_output_char
1.89	0.48	0.01	5000001	0.00	0.00	caml_string_length
1.89	0.49	0.01	11067	0.00	0.00	caml_oldify_one
1.89	0.50	0.01	2060	0.00	0.01	caml_oldify_local_roots
...						

% time	cumulative seconds	self seconds	calls	self ns/call	total ns/call	name
13.17	0.32	0.32				GC_build_fl
12.96	0.64	0.32	20000004	15.75	15.75	closure_promote_1636
12.76	0.95	0.31				GC_malloc_kind
10.29	1.20	0.25				GC_mark_from
9.47	1.43	0.23				GC_apply_to_all_blocks
6.38	1.58	0.16				GC_allochblk_nth
4.94	1.70	0.12				closure_promote_2347
3.70	1.79	0.09				GC_clear_stack_inner
2.26	1.85	0.06				GC_malloc
1.65	1.89	0.04	20000004	2.00	5.00	closure_promote_1504
1.65	1.93	0.04				GC_clear_hdr_marks
1.23	1.96	0.03				GC_finish_collection
1.23	1.99	0.03				func_2301
1.03	2.01	0.03	20000004	1.25	6.25	closure_2_1588
0.82	2.03	0.02	10000002	2.00	2.00	local_func_2208
0.82	2.05	0.02				GC_allochblk
0.82	2.07	0.02				GC_generic_malloc
0.82	2.09	0.02				GC_generic_malloc_inner
0.82	2.11	0.02				GC_install_header
0.82	2.13	0.02				GC_push_next_marked_uncollectable
0.82	2.15	0.02				GC_reclaim_clear
0.82	2.17	0.02				get_index
0.62	2.19	0.02	10000002	1.50	1.50	local_func_2144
0.62	2.20	0.02	10000002	1.50	1.50	local_func_2240
0.62	2.22	0.02				GC_free_block_ending_at
0.41	2.23	0.01	20000004	0.50	6.75	closure_promote_1542
0.41	2.24	0.01	10000002	1.00	1.00	local_func_2176
0.41	2.25	0.01				GC_add_to_black_list_stack
0.41	2.26	0.01				GC_clear_fl_links
0.41	2.27	0.01				GC_clear_fl_marks
0.41	2.28	0.01				GC_clear_stack
0.41	2.29	0.01				GC_continue_reclaim
0.41	2.30	0.01				GC_find_header
...						

Figure 4.5: Truncated Gprof outputs from the lens benchmark, coloured using the same scheme as before in figure 4.2, with the addition of yellow functions being related to the closure creation/application process.

benchmark	ocamlc		ocamlopt		gcc -O3		clang -O3		reduced allocations			
									gcc -O3		clang -O3	
	mean	std	mean	std	mean	std	mean	std	mean	std	mean	std
binary-trees	7.959	0.088	2.068	0.012	4.858	0.032	4.052	0.027	4.864	0.035	4.117	0.095
collatz	28.437	0.055	2.351	0.019	2.236	0.006	2.344	0.008	2.305	0.013	2.348	0.019
even_fib	8.218	0.066	1.423	0.026	0.992	0.007	0.971	0.009	0.964	0.009	0.971	0.011
fibonacci	7.211	0.190	1.032	0.009	1.275	0.006	1.122	0.015	1.321	0.006	1.124	0.021
lens	4.510	0.120	1.294	0.027	2.788	0.056	2.620	0.058	2.322	0.020	2.084	0.079
mandelbrot	16.609	0.151	0.931	0.009	9.307	0.076	8.788	0.249	1.548	0.007	1.354	0.018
nbody	8.251	0.133	1.366	0.021	3.311	0.078	3.203	0.059	0.764	0.013	0.716	0.016
rule30	2.311	0.030	1.128	0.032	1.943	0.054	1.588	0.027	1.923	0.016	1.577	0.016
sieve	2.341	0.021	1.687	0.027	N/A	N/A	0.882	0.025	N/A	N/A	0.880	0.021
stream	3.966	0.022	0.884	0.041	3.614	0.021	3.180	0.128	2.896	0.071	2.409	0.071

Figure 4.6: Summary results of benchmark results. All figures given in seconds.

4.3 Observability

The other way to evaluate the the compiler is to determine the observability of the compiled output, or how much information we are able to recover about the internal state of the program as it is executing.

The OCaml native code compiler can be said to be not observable at all, since the native executables do not support debugging. Instead, comparisons will be made with the OCaml bytecode debugger.

4.3.1 Sample GDB session

We consider the following simple program, for summing a list of numbers using a generic fold function.

```

1 external print_int : int -> unit = "print_int"
2 external newline : unit -> unit = "newline"
3
4 let rec foldl f acc = function
5   | x :: xs -> foldl f (f acc x) xs
6   | [] -> acc
7
8 let sum = foldl (+) 0
9
10 let a = sum [1; 2; 3]
11 let _ = print_int a; newline ()

```

Debug sessions when debugging using both GDB and `ocamldebug` can be found in appendix §B, with equivalent commands entered for both sessions. There are some minor differences with regards to which locations the debuggers stop at, and the commands have been altered slightly to reflect this.

By loading in a script which enables custom pretty-printers, we are able to observe OCaml values in a nicer representation than printing out raw pointers. In addition, the use of `#line` directives has meant that that GDB can display correctly the lines of OCaml

code the code it is currently debugging correspond to, allowing breakpoints to be set. Since what is being debugged underneath is essentially just a C program, the full power of GDB's tools can be utilised, including breakpoints, backtraces, watchpoints, etc.

4.3.2 Identifiers

In the C code, in order to avoid ambiguity we suffix identifier names with their unique 'stamp' in order to avoid naming conflicts. Practically, this is more of an annoyance than a problem. As GDB allows tab completion in order to reference variable names, to obtain the name of a variable in the C code one only needs to type the name followed by an underscore, then press tab to tab-complete the appropriate stamp.

This does however mean that debugging is a worse experience in comparison to `ocamldebug`, where typing the name of a variable automatically refers to the variable with that name which is currently in scope. Because of the precautions outlined earlier in §A.4.1, it should not be theoretically difficult to erase these 'stamps' from variable names, but practically there are a few problems with this:

- The `Lambda` IR introduces new variables in certain cases, but does not care about naming conflicts as its transformation is post-source-code level where identifiers are compared using their stamps only. This means that erasing stamps naively would cause naming conflicts.
- There is no equivalent way to deal with this for top-level identifiers, as we cannot have shadowing in the top-level scope in C.

4.3.3 Polymorphic printers

The `debug/pprint.py` script is a script written to enable printing of OCaml values within GDB, as otherwise many values will only be displayed as pointers otherwise.

This is a point where my implementation performs better than `ocamldebug`. Because of the representation strategy described in section 3.4, we can determine the types of values at runtime even if the code we're debugging does not know the types themselves.

We can see this at lines 24-31 in the GDB output (B.2), and lines 10-15 in the `ocamldebug` output (B.3). The pretty printers which I have loaded into GDB are correctly able to infer that the values being printed are integers and an integer list, but `ocamldebug` cannot, and instead can only print the polymorphic values as `<poly>`.

One limitation of this however is that when printing data structures, I print the in-memory representation of the structure instead of how it would be represented in OCaml. Had I more time this could be remedied by also outputting a lookup table for the pretty printers to use to find out what type a data structure is and how it should be formatted. As of currently, OCaml blocks are printed with the tag first, a colon, and then the data within the block; this results in the list `[1; 2; 3]` being printed as `[0: 1 [0: 2 [0: 3 0]]]`.

4.3.4 Line number matching

While the line number matching between the C code and the OCaml code is acceptably good for debugging, there are certain cases which it does fall down, due to a fundamental difference in the way GDB and `ocamldebug` treats points where the debugger may pause execution.

`ocamldebug` notably only pauses at `Lambda` events, which are described in §3.1.1, but GDB only pauses on lines of code. Since `Lambda` events are inserted directly before or after certain expressions, `ocamldebug` is able to pinpoint exactly where in the evaluation of the code it has stopped, but GDB is unable to do this, only printing the line of code where it stops at.

This is especially confusing for sometimes for local anonymous functions. For example, in the `sum` example from earlier, stepping inside the `(f acc x)` expression on line 5 steps you back to the line 8 `(let sum = foldl (+) 0)`, because we are stepping inside the implicitly defined `(+)` function, which was defined on line 8.

Chapter 5

Conclusion

Overall, the project was largely successful as I had accomplished my goal of compiling the target subset of OCaml correctly into C, as well as providing facilities under which the resulting C code could be “observed” by a debugger as if it was OCaml code.

Translations of technically challenging features of the languages such as data representation and closure represented were attempted, and largely successful. My implementation also leaves room for further additions to the compiler to add support for the remaining features of OCaml which were not included in the target subset if more time was to be dedicated.

We can see that the motivations of the project have been largely fulfilled, including:

Observability

The work into making the code observable has largely held up, with GDB being able to display the current location of the code and observe OCaml values, even polymorphic values that the `ocamldebug` debugger could not discern. It is a weak point however that GDB is unable to print out OCaml data structures using OCaml’s notations for them, but this is very possible with an extension to the compiler that generated debug information for the types of objects within the executable being debugged.

Plausibility

The completion of the compiler is a proof that my approach to compiling OCaml and other similar languages into C works, and it is possible to represent even complex closure structures and OCaml’s algebraic data types within C, as well as a debugger being able to “see through” parametric polymorphism to determine the types of the values being manipulated.

Performance

Despite no heavy efforts being paid to make the resulting code performant, under all tested workloads my compiler outperforms the OCaml bytecode compiler and matches or is sometimes even faster than the OCaml native compiler in select workloads.

My project leaves plenty of room for future extension work, and there are things that I would've done differently had I started the project again. These include:

- Support for OCaml's module system, allowing multi-file programs to be compiled correctly. Currently the compiler is only capable of compiling one file at a time, but it should not be difficult extend this support;
- Support for more of OCaml's standard library, allowing standard library modules to be compiled and used;
- Support for a larger subset of OCaml's core language, including array types and a better support for floating point values, in order to make them more performant;
- A key assumption of the code is that all primitive types needed are 8 bytes long, or word-sized on a 64-bit system. It would be nice if less reliance was depended on this so the compiler was more portable to other systems than 64-bit Linux;
- More performant closures, such as generating function stubs at runtime to implement closure operations, or using a closure implementation from a popular library such as `libffi`;
- More time spent with libraries, such as my supervisor's `liballocs`, in order to make it possible to have runtime reflection without resorting to less performant means of storing values.

Bibliography

- [1] D. Tarditi, A. Acharya, P. Lee, *No Assembly Required: compiling Standard ML to C*, November 1990.
<http://repository.cmu.edu/cgi/viewcontent.cgi?article=3011&context=compsci>
- [2] C. Sun, *An Observable OCaml with liballocs and C*, May 2017.
- [3] A. Madhavapeddy, J. Hickey, Y. Minsky, *Real World OCaml*, O'Reilly Media, November 2013.
- [4] S. Kell, *Towards a Dynamic Object Model within Unix Processes*, October 2015.
- [5] CLBG, *The Computer Language Benchmarks Game*, last accessed at 2018-03-26.
<https://benchmarksgame.alioth.debian.org>
- [6] OCamlPro, *A set of micro-benchmarks for OCaml compiler*, last accessed at 2018-03-26.
<https://github.com/OCamlPro/operf-micro/>

Appendix A

Implementation Details

This appendix chapter provides some more details about finer implementation details that could not fit within the implementation chapter.

A.1 The Ccode module

The `Ccode` module stores the OCaml representation of the target C subset. It is specially chosen to be a subset of C, and only contain the necessary types to represent the compilation target. There are four main datatypes in the module, and a quick summary of them is given here:

- `Ccode.cident`, for representing identifiers (variable names, macro names, function names etc.) in C. This is largely a wrapper over the `Ident.t` type the OCaml compiler uses to represent identifiers, which is the string name along with a unique integer ID to disambiguate it from other identifiers with the same name.
- `Ccode.cexpr`, for representing expressions in C. These include a wrapper around `cidents`, literals, and operations (such as unary operations, binary operations, function calls etc.) on other `cexprs`.
- `Ccode.cstatement`, for representing statements in C. Most data constructors in this type take a `cexpr` or a block of other `cstatements`, and include if statements, while statements, switch statements etc. Notably a `cexpr` can be promoted to a `cstatement`, but not the other way around.
- `Ccode.ctype`, for representing types in C. This is an auxiliary type used by the casting operator in `cexpr` and the variable declaration statement in `cstatement`. A more in-depth discussion of the types used to represent OCaml values is at §3.4.

In addition, the `Ccode` module contains some special record types:

- `Ccode.cfunc`, which is a record type holding information about the return type of the function, the names and types of its arguments, its name, its body of code, and its location in the source.

- `Ccode.ccode`, which is the record struct that is finally passed into `Cprint` to print the code. It is composed of three lists: the block of statements that forms the preamble (which is things like `#include` directives and global variable declarations), the list of functions, and the block of code representing the `main` function.

A.2 Purpose of `runtime.h`

`runtime.h` is a special header file which needs to be included in the compilation of the output C file to produce executables from my compiler. It contains the type declarations mentioned in the implementation chapter, as well as helper functions and macros useful for implementing certain structures and observability features.

A.3 `#line` directives

A key observability feature is for the debugger to associate the currently executing machine code with the relevant line from the source.

C compilers support controlling the line and source file of your code with use of the `#line` directive. This means the compiler can put all statements associated with one line of source on the same line¹, interspersed with a `#line` directive whenever the source code line actually changes.

To actually obtain information about which line we're on, we again use `Lambda` events (§3.1.1), as they carry information about the current file and line. Since they also represent places where the OCaml bytecode debugger `ocamldebug` may pause execution, this gives us a pleasing way to treat them: `Lambda` events simply compile directly into `#line` directives.

A.4 Compilation of basic constructs

This section gives an overview of other common basic syntactical structures in OCaml are compiled into C.

A.4.1 Variable scoping differences between C and OCaml

In OCaml, each variable is only visible in the body of the expression where it is bound, whether if that's in a `let`-binding or a function declaration. This is in contrast to variable scope in C, where a variable is visible for the entirety of the rest of the block it is in.

Furthermore, while OCaml does not allow reassignments (of variables, not references), it does allow you to bind another variable with the same name:

```
let x = 1 in
let x = 2 in
print_int x
```

¹the line number changes whenever there is a new line, even after being specified with `#line`.

Here the second binding is not reassigning the value of `x`, rather it's creating another variable with the same name. The first variable still exists, but it's been shadowed by the second variable making it inaccessible. Note that after leaving the body of the second `let` binding the second variable goes out of scope and the first variable is accessible again.

This behaviour can be approximated using C99's block-scoping:

```
int x = 1;
{
    int x = 2;
    print_int(x);
}
```

Here we see that within the inner block, the second declaration of `x` has shadowed the first declaration of `x`, but the original declaration of `x` is still accessible once we leave the inner block (which is also the behaviour in OCaml). Therefore, we have to pay careful attention to inserting variable scopes to correctly mirror the shadowing effects in OCaml².

A.4.2 Meta-notation for compilation

To describe the compilation process from OCaml expressions into C we use a C-like meta-notation. Recall from §3.2.1, each OCaml expression compiles to a set of C statements and a variable, which the C statements will have assigned the correct value to after their execution. We therefore denote the set of C statements an expression `e` compiles into as `comp<e>`, and the variable it is associated with with `var<e>`. This gives a way of recursively defining the compilation process by defining `comp<e>` for all possible OCaml expressions. In the actual compiler, the `comp<>` functions are implemented within the `Ccompile` module, which outputs an equivalent representation of C using the types in the `Ccode` module.

As an example, consider the OCaml expression `e1 + e2`. We therefore define:

```
comp<e1 + e2> :=
```

```
declare3 result;
comp<e1>; // var<e1> now contains the correct value
comp<e2>; // var<e2> now contains the correct value
result = var<e1> + var<e2>;
```

`result` refers to some temporary variable name which we assign to this expression, and we define `var<e1 + e2> := result`. Note that this is a common pattern so we will implicitly assume that when defining the compilation of an expression `e`, `var<e>` will be the variable named `result` within `comp<e>`.

²Note however we cannot apply this process for variable declarations at the top-level, since you cannot insert block-scopes at the top level in C. Unfortunately this requires top-level variables to be renamed.

³`declare` here stands for the type of the result of the expression which is required for variable declarations in C. In general, this type is not known generally and depends on the specific types of the subexpressions, so we use `declare` to stand in for this.

A.4.3 if-then-else expressions

OCaml does not have if-statements but if-expressions, which are of the form:

`if cond then A else B`

Using the same notational conventions as in §A.4.2:

```
comp<if cond then A else B> :=
```

```
declare result;
```

```
comp<cond>;
if (var<cond>) {
  comp<A>;
  result = var<A>;
} else {
  comp<B>;
  result = var<B>;
}
```

The same trick to propagate results outwards from inner scopes has been employed here also.

A.4.4 while loops

While loops are fairly simple in OCaml – they simply repeatedly evaluate their body while the condition evaluates to true. There are no break nor continue statements, so there is not a concept of breaking out of a loop early with the exception of setting the condition to false. They have the syntax:

`while cond do body done`

In addition, the overall return value of the loop is `unit`. The compilation for them is therefore:

```
comp<while cond do body done> :=
```

```
comp<cond>;
declare temp = var<cond>;
while (temp) {
  comp<body>;
  comp<cond>;
}
```

```
declare result = make_unit();
```

There is one interesting thing of note here: *cond* does need to be evaluated twice, once before the loop, and once at the end of the loop. This is because the OCaml while loop re-evaluates *cond* at the beginning of each iteration, but since OCaml expressions turn

into a list of statements in C, we cannot fit this re-evaluation into the head of the while statement – instead, a simple and equivalent way around this is to simply re-evaluate *cond* at the end of the loop.

A.4.5 for loops

For loops in OCaml are extremely limited. They permit only iteration over a fixed range of integers, and also only allow increments in steps of 1. Like with while loops, there are no break nor continue statements in OCaml and so there is no possibility of exiting a loop early. They have two forms, which are:

```
for x = start to end do body done
for x = start downto end do body done
```

These two versions simply iterate up to or down to a certain number (inclusive). Since for loops are so incredibly limited, it was decided that rather than including for loops in the targeted subset of C, it would be easier to also compile these into while loops in C.

```
comp<for x = start to end do body done> :=
```

```
comp<start>;
comp<end>;
int temp1 = var<start>;
int temp2 = var<end>;

{
  decl x = temp1;
  while (x <= temp2) {
    comp<body>;
    x++;
  }
}
```

```
decl result = make_unit();
```

(Replace <= for >= and *x*++ for *x*-- for *downto*.)

There are a few things about this compilation that warrant elaboration:

- *x* again needs to be declared in its own scope, as the for loop acts as another variable binding site. Thus, the entirety of the for loop is wrapped in another block.
- Note the use of *temp1* and *temp2*, which are necessary because *var<start>* and *var<end>* may collide with the name of the variable *x* and cause it to be shadowed in the inner scope.
- *start* and *end* are only evaluated once at the start of the loop – after some quick experiments it could be shown that OCaml does this as well, i.e. the limits of the iteration range do not change while the loop is running.

- x is mutated through the iteration of the loop. This is fine, as OCaml for loops only operate on integers, which are copied instead of referenced by other constructs in the target subset of C; thus the mutation of x cannot affect the behaviour of the program.

A.5 Value representation details

This section deals with details related to the value representation used in the compiler.

A.5.1 Lstaticraise and Lstaticcatch

The Lambda IR also has support for static exceptions, which are exceptions that can only occur across a local scope⁴. This is similar to the behaviour of a `goto` statement in C. In particular, the OCaml pattern-match compiler may opt to use a static exception to avoid duplication of code for certain branches. For example, consider this match expression:

```
type color =
  | Red
  | Green
  | Blue
  | Gray of int
  | RGB of int * int * int

match c with
  | Red -> 0
  | Green -> 1
  | Gray x -> 2
  | _ -> 3
```

This match expression contains a wildcard expression which matches both `Blue`, which is an integer, and `RGB`, which is a block. The OCaml pattern-match compiler thus compiles it into the following Lambda expression:

```
(catch
  (switch* c/xxxx
    case int 0: 0
    case int 1: 1
    case int 2: (exit 1)
    case tag 0: 2
    case tag 1: (exit 1))
  with (1) 3)
```

The branches for `Blue` and `RGB` have been compiled into a static exception (the `exit` expression), to avoid duplicating the expression in the branch. This behaviour can be emulated with `gotos` in C. `Lstaticcatch` expressions can be compiled simply into an `if(0)` and a label, and `Lstaticraise` expressions are simply compiled into a `goto`.

⁴In contrast to normal exceptions, which unwind the stack and can jump to an error handler in an enclosing scope.

A.6 Closure details

This section deals with details related to the compilation of functions and closures.

A.6.1 Functions that return other functions

§3.5.2 provides a scheme for converting between function types in OCaml to function types in C, but this conversion doesn't always make sense. In OCaml, it is possible and often useful to define functions that return other functions. As a simple example, consider the function:

```
let f x = (fun y -> x + y)
```

The type of `f` is `int -> int -> int`, but it's obvious that this isn't translatable into a C function `int f(int x, int y)` – the body of the function would return a closure, and not an integer.

Since the type of `f` is known, this is a rather simple problem to fix via a technique known as eta-expansion, and can be done at the source code level. Simply add extra parameters to match the number of parameters in the type, and apply them to the old result of the function.

```
let f x y = (fun y -> x + y) y
```


Appendix B

Debug sessions

B.1 The “sum” program

```
1 external print_int : int -> unit = "print_int"
2 external newline : unit -> unit = "newline"
3
4 let rec foldl f acc = function
5   | x :: xs -> foldl f (f acc x) xs
6   | [] -> acc
7
8 let sum = foldl (+) 0
9
10 let a = sum [1; 2; 3]
11 let _ = print_int a; newline ()
```

B.2 GDB session of the “sum” program

```
1 GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
2 Copyright (C) 2016 Free Software Foundation, Inc.
3 License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
4 This is free software: you are free to change and redistribute it.
5 There is NO WARRANTY, to the extent permitted by law. Type "show copying"
6 and "show warranty" for details.
7 This GDB was configured as "x86_64-linux-gnu".
8 Type "show configuration" for configuration details.
9 For bug reporting instructions, please see:
10 <http://www.gnu.org/software/gdb/bugs/>.
11 Find the GDB manual and other documentation resources online at:
12 <http://www.gnu.org/software/gdb/documentation/>.
13 For help, type "help".
14 Type "apropos word" to search for commands related to "word"...
15 Reading symbols from test_gdb...done.
16 (gdb) source ../../../../debug/pprint.py
17 (gdb) break 4
18 Breakpoint 1 at 0x400fdc: file test.ml, line 4.
19 (gdb) run
20 Starting program: /home/tyler/Code/Coursework/observable-ocaml/tests/observability/sum
   /test_gdb
21
22 Breakpoint 1, local_func_1222 (f_1207=<closure>, acc_1208=0, param_1211=[0: 1 [0: 2
   [0: 3 0]]], closure_obj_1221=<closure>) at test.ml:4
23 4      let rec foldl f acc = function
24 (gdb) print acc_1208
```

```

25 $1 = 0
26 (gdb) step
27 5 | x :: xs -> foldl f (f acc x) xs
28 (gdb) print x_1209
29 $2 = 1
30 (gdb) print xs_1210
31 $3 = [0: 2 [0: 3 0]]
32 (gdb) continue
33 Continuing.
34
35 Breakpoint 1, local_func_1222 (f_1207=<closure>, acc_1208=1, param_1211=[0: 2 [0: 3
    0]], closure_obj_1221=<closure>) at test.ml:4
36 4 | let rec foldl f acc = function
37 (gdb) print acc_1208
38 $4 = 1
39 (gdb) step
40 5 | x :: xs -> foldl f (f acc x) xs
41 (gdb) print x_1209
42 $5 = 2
43 (gdb) print xs_1210
44 $6 = [0: 3 0]
45 (gdb) continue
46 Continuing.
47
48 Breakpoint 1, local_func_1222 (f_1207=<closure>, acc_1208=3, param_1211=[0: 3 0],
    closure_obj_1221=<closure>) at test.ml:4
49 4 | let rec foldl f acc = function
50 (gdb) continue
51 Continuing.
52
53 Breakpoint 1, local_func_1222 (f_1207=<closure>, acc_1208=6, param_1211=0,
    closure_obj_1221=<closure>) at test.ml:4
54 4 | let rec foldl f acc = function
55 (gdb) step
56 6 | [] -> acc
57 (gdb) p acc_1208
58 $7 = 6
59 (gdb) step
60 main () at test.ml:11
61 11 | let _ = print_int a; newline ()
62 (gdb) print a_1213
63 $8 = 6
64 (gdb) continue
65 Continuing.
66 6
67 [Inferior 1 (process 32184) exited normally]
68 (gdb)

```

B.3 Ocamldebug session of the “sum” program

```

1      OCaml Debugger version 4.05.0
2
3 (ocd) break @ Test_ocaml 4
4 Loading program... done.
5 Breakpoint 1 at 106800: file test_ocaml.ml, line 4, characters 15-81
6 (ocd) run
7 Time: 24 - pc: 106832 - module Test_ocaml
8 Breakpoint: 1
9 5 | x :: xs -> <|b|>foldl f (f acc x) xs
10 (ocd) print acc
11 acc: 'a = <poly>
12 (ocd) print x
13 x: 'a = <poly>
14 (ocd) print xs
15 xs: 'a list = [<poly>; <poly>]
16 (ocd) run
17 Time: 26 - pc: 106832 - module Test_ocaml

```

```
18 Breakpoint: 1
19 5 | x :: xs -> <|b|>foldl f (f acc x) xs
20 (ocd) print x
21 x: 'a = <poly>
22 (ocd) print xs
23 xs: 'a list = [<poly>]
24 (ocd) run
25 Time: 28 - pc: 106832 - module Test_ocaml
26 Breakpoint: 1
27 5 | x :: xs -> <|b|>foldl f (f acc x) xs
28 (ocd) run
29 Time: 30 - pc: 106864 - module Test_ocaml
30 Breakpoint: 1
31 6 | [] -> <|b|>acc
32 (ocd) print acc
33 acc: 'a = <poly>
34 (ocd) step
35 Time: 31 - pc: 107040 - module Test_ocaml
36 10 let a = sum [1; 2; 3]<|a|>
37 (ocd) next
38 Time: 47 - pc: 107052 - module Test_ocaml
39 11 let _ = print_int a<|a|>; newline ()
40 (ocd) print a
41 a: int = 6
42 (ocd) run
43 6
44 Time: 79
45 Program exit.
46 (ocd)
```


Appendix C

Project Proposal

Introduction and Description of the Work

This project involves the implementation of a compiler from OCaml to C in such a way that will allow the resulting executable to be compatible with DWARF-based debugging tools, such as `gdb`. This project will use the existing front-end of the OCaml compiler, but implement a very different back-end which outputs valid C code that can be compiled using a tool such as `gcc` into a debuggable executable. The focus of the compiler is to optimise for debuggability, or “observability”, by taking advantage of the numerous debugging tools available of the C compilation toolchain.

Since the implementation of the full OCaml language is likely too ambitious for one project, the core project will instead revolve around the implementation of an interesting subset of OCaml which still provides technically interesting challenges in its implementation, while extension tasks may extend the implementation to cover a wider subset of the entire language. An informal description of said subset will be given in the Substance and Structure section.

The “observability” of the compiler means that where possible the debugger should behave *as if* it was debugging the OCaml code. This means that the debugger should consider sections of the compiled machine code to be mapped to the appropriate lines of code in OCaml. Furthermore, locally bound variables should be visible from the debugger when execution has reached the relevant point, meaning that local variables in the C code should mirror the variables in the OCaml code.

In addition, features such as closures and parametric polymorphism must be implemented carefully since these features don’t have any similar structures in C for which they could’ve been mapped to, but also to maintain “observability” these must be “transparent” to the debugger (for example, a polymorphic function of the type `'a -> 'a` that has been instantiated as the type `int -> int` should have this quality be visible from the debugger). These qualities can be implemented using user-defined commands for `gdb`.

The resulting compiler can be evaluated in mainly two contexts. One of these is a straightforward performance comparison, where a testbed of OCaml programs are benchmarked across the OCaml native compiler, the OCaml bytecode compiler, and this project. The other context is the “observability” of the compiler; where programs are stopped at a certain point of their execution and inspected, to see how much of the internal state of the

stack is recoverable. This can be made in comparison with OCaml’s bytecode debugger, `ocamldebug`.

Resources Required

No special resources are required that are not open source and freely available for download.

Starting Point

The project, at least initially, will be a fork of the OCaml compiler obtainable at `github.com/ocaml/ocaml` which will take the same front-end as the existing compiler, but will implement a new back-end for compilation into C. The work may use other libraries such as `libffi` and `liballocs` but no work of similar scope to the project.

Substance and Structure of the Project

The core of the project will be devoted into the implementation of three incrementally expanding subsets of OCaml. These subsets have been identified such that each is sufficient to write nontrivial programs in, and features have been grouped by relation to each other. In this manner work can be easily split into 3 discrete blocks, each of which will support a new collection of programs by their completion.

Subset 1

Subset 1 will be a very simple language with only a limited number of types and language constructs. The subset will contain only the basic boolean, integer, floating point and `unit` types, basic string support (for input/output), top level function declarations with `let` and `let rec`, which only accept one argument (so as to sidestep the problem of partial application and closures), `if`, `for`, `while`, `ref`, as well as basic arithmetic and boolean operations.

These features were chosen because they very easily make for a small minimalist language, and all constructs more or less have direct analogues in C meaning translation from AST to C code should be fairly easy. Nonetheless, this small subset is sufficient to write simple programs.

Subset 2

Subset 2 will focus on the implementation of types and polymorphism, and will support tuples, lists, parametric polymorphism, algebraic data types, record types, and `match` expressions.

The implementation of this subset will require the design of an object representation for OCaml values. Tuples and record types map easily to structs in C, while a tagged union can be used for OCaml’s “sum of products” approach to algebraic data types. On

the first pass, it is quite likely that a naive “tagged pointer” type will be used for support for polymorphism, but extension tasks may experiment with eliminating this need via some method.

The addition of algebraic data types greatly increases the scope of supported programs, and allows for functions taking multiple arguments (via tuples), list processing functions, and more complex data structures such as binary trees.

Subset 3

Subset 3 will finally add treatment of functions as first-class values. This will include lambdas, lexical closures, and partial application of functions.

The implementation of this subset will require some representation of closures. While C does support function pointers, it has no lexical closures and as such a representation where closures are function pointers with an extra `void *` pointer that refers to data in the closure is likely to be the implementation on the first pass. As an extension task, more performant ways of implementing closures may be investigated, such as potentially dynamically generating entry points that push the required arguments before jumping to the body of the function.

The addition of these features will make higher-order functions representable, and make available functions such as `map`, `filter`, function composition etc. At this point subset 3 can be considered a fairly minimal but full-featured functional language.

Evaluation

Evaluation will require the creation of a small library of test programs. These programs should be novel and exhibit the full range of language features supported by the subsets.

Two main methods will then be used to evaluate the compiler. One is benchmarking performance of the test programs with the existing OCaml native compiler and the OCaml bytecode compiler. While it is not expected that the C compiler will match the performance of OCaml official compilers, the goal is to be within a reasonable margin so that the performance of compiled C code is comparable. The performance evaluation will be a simple measurement of the runtime of the compiled executable in relation to the running time of the executable produced by the OCaml native compiler and the running time of the interpreter on the bytecode produced by the OCaml bytecode compiler. The test suite for the performance evaluation will have to be partly written as part of the project, and partly adapted from the existing OCaml compiler test suite (github.com/ocaml/ocaml/tree/trunk/testsuite) or possibly the Computer Language Benchmarks Game (benchmarksgame.alioth.debian.org). Since the compilation source is only a subset of OCaml, not all of the existing test suite programs will be relevant, and others will require some adaptation for them to work for the project.

The other method will be the evaluation of the “observability” of the C code. This will take place in two parts: firstly, we can do a test for “observability”: this will entail a minimum list of requirements, such as ability to step through OCaml code, ability to print locally bound values, ability to print types of locally bound variables, and ability to show

instantiation of polymorphic functions into specific types. The second is to compare the debug outputs of the C code and the OCaml code. The native OCaml compiler does not allow observation of locally bound values at all, so our C compiler should beat this easily; although a more interesting comparison would be with the OCaml bytecode debugger. Breakpoints could be set at randomly chosen call sites, and the stack traces, visible locals etc. could be compared between `ocamldebug` and the debug output of the C code.

Extension Tasks

This project leaves a lot of room for extension tasks. An obvious extension is to extend the subset to be a more complete subset of OCaml. The next steps taken would likely be module and exception support, although both are far more complex features to attempt for implementation in C.

More realistic extension tasks would be changes to the existing code in order to make it more performant. This would involve improvements to the implementation of polymorphic functions and closures, as described in their respective sections prior.

Another plausible extension task is to improve the debug output of OCaml values. Since C does not have an exact analogue for all OCaml values the debug output from `gdb` for example will not look exactly like their OCaml representation. However, `gdb` supports the use of custom formatters written in Python for types and a task to implement a way to generate formatters to print OCaml values correctly is a suitable extension task.

Success Criteria

The following criteria should be achieved at the completion of the project:

- A working compiler, that is able to compile the language as described in Subset 3 into C code correctly;
- An evaluation of performance between the output of the compiler and the OCaml native and bytecode compilers;
- An evaluation of “observability” in the compiled executable with tools such as `gdb`.

The evaluation should focus on the following:

- Ability to set breakpoints and step through the compiled executable as if it was OCaml code;
- Ability to view locally bound variables, and their types, although perhaps only as a C “version” of the resulting data;
- Ability to print more complex data structures, such as ADTs, record types and lists;
- Similar and comparable output between the debug output and the same code running in `ocamldebug`.

Further success criteria, which are not expected to be achieved through the core project, but interesting as extension tasks may be:

- Ability to view the instantiated types of polymorphic functions;
- Ability to view data formatted as OCaml values, using specially written formatters for `gdb`;
- Any number of optimisations on the generated code, resulting in better performance benchmarks.

Timetable and Milestones

20 October — 3 November

Initial experiments and reading. Familiarise with the OCaml compiler source code and obtain typed AST. Set up development environment. Write testbed of evaluation programs so that features can be tested and evaluated immediately after their implementation.

Milestones: A completed small library of OCaml programs, plus a way of obtaining the typed AST from the OCaml compiler.

4 November — 17 November

Implementation of Subset 1. Evaluation of Subset 1 performance with respect to the OCaml native and bytecode compilers.

Milestones: A collection of programs now compileable by the Subset 1 compiler, along with their running times collected in comparison with the OCaml compilers.

18 November — 15 December

Implementation of Subset 2. This is expected to take longer than the implementation of Subset 1 to take into account that special care needs to be taken when designing object representations of OCaml values and implementation of parametric polymorphism. Evaluation of Subset 2 performance with respect to OCaml compilers.

Milestones: A larger collection of programs now compileable by the Subset 2 compiler, along with their performance results in comparison with the OCaml compilers.

16 December — 29 December

(Two week break for Christmas)

30 December — 12 January

Implementation of Subset 3. Evaluation of Subset 3 performance, as well as comparison between the debug output of the compiled code with `ocamldebug`.

Milestones: Completion of core project with the implementation of Subset 3. Some evaluation results (although perhaps not complete) for the core project.

13 January — 26 January

Write up of the Progress Report. Perform any new evaluation tasks that were missed but become apparent in the write up of the Progress Report. Review the remainder of the project in context with the existing work and determine which extension tasks are best to pursue.

Milestones: Completed core project with evaluation, with a completed Progress Report ready for submission. Entire project reviewed with supervisor and overseers.

27 January — 9 February

Submission of Progress Report. Revise evaluation tasks with feedback from Progress Report. Prepare Progress Report presentation.

10 February — 23 February

Start work on dissertation, as well as the implementation of ways of making the compiled code more performant. Investigation and use of perhaps `libffi` and `liballocs` to improve performance and observability.

Milestones: The introduction and preparation sections of the dissertation complete. Improvements on the compiler made, with evaluation results to show improvements in performance of the compiled output.

24 February — 9 March

Start writing the implementation section of dissertation. Implementation of the generation of custom formatters for `gdb`, which will make the debug output easier to read and interpret as OCaml values.

Milestones: Implementation section of the dissertation at least half complete. Improvements to debug output of debuggers run on the compiled executables.

10 March — 22 March

Finish writing implementation section of dissertation. Start evaluation section. Pick up any further evaluation tasks at this point that become apparent.

Milestones: Finished implementation section, evaluation section at least half complete. Revised evaluation tasks in accordance with the write up of the evaluation section.

23 March — 5 April

Finish evaluation and conclusion sections of the dissertation. Deliver draft dissertation to supervisor and director of studies for feedback. Spend time working on whatever is in greatest need of attention.

Milestones: Submit a complete draft of the dissertation for review to supervisor and director of studies.

6 April — 19 April

Revise dissertation based on feedback received. Finish any last tasks that require performing, which are hopefully minor at this point in time. Send revised drafts for further rounds of review.

20 April —

Final adjustments and revisions to dissertation and the body of code. Prepare for submission of dissertation.

Milestone: Submission of dissertation.

Resource Declaration

No special resources are required for this project other than those that are not already available as open source code.