

Lambda Calculus with Lifetimes and Higher Kinded Types

Final Year Project Report

Felix Bowman
Candidate Number: 122587

Supervisor: Dr. Martin Berger

University of Sussex
Department of Informatics

Contents

1	Introduction	4
1.1	Project Aims	4
1.2	Types in Programming Languages	4
1.3	Goals of This Project	5
1.4	Project Overview	5
2	Professional and Ethical Considerations	6
3	Parametric Polymorphism	7
3.1	A World Without Generics	7
3.2	Parametrizing Constructors	9
3.3	More Generic Containers	10
3.4	map and Higher Order Functions	10
3.5	Functor and Mapping over Containers	11
3.6	Higher Kinded Types	12
4	Memory Management	13
4.1	Memory Usage and Computational Effects	13
4.1.1	Stack and Heap Memory	13
4.2	Problems with Existing Memory Management Techniques	14
4.2.1	Manual Memory Management: malloc and free	14
4.2.2	Automatic Memory Management: Garbage Collection	15
4.3	A Solution in the Type System	15
4.3.1	An Introduction to Rust's Model of Memory Management	15
4.4	Representing Programs as Data Structures	16
4.5	Type checking	16
5	Formal Definitions	17
5.1	Lambda Calculus	17
5.1.1	Simple Types in the Lambda Calculus	17
5.1.2	System F	18
5.1.3	System F ω	19
5.2	Lifetimes	21
5.2.1	Adding Impurity	21
5.3	Final Typing Rules	21
6	Requirements	22
7	Implementation	23
7.1	The Haskell Language	23
7.2	Stack, Haskell's Build System	23
7.3	Parsing	24

7.4	Componests of the Type Checker	24
7.4.1	Terms	24
7.4.2	Kind Checker	24
7.4.3	Lifetime Checking	24
7.4.4	Type Checking	25
7.4.5	Error Reporting	25
7.4.6	Context Management	25
7.5	Testing	26
8	Key Tests	27
8.1	Simple Programs	27
8.1.1	Polymorphic Identity Function	27
8.1.2	Multiple Lifetimes and References	27
8.1.3	Higher Order Functions	28
8.2	Memory safety	28
8.3	Basic tests	28
9	Evaluation	29
9.1	Problems	29
10	Conclusion	30
10.1	Further Work	30

Listings

3.1	String List in Java	7
3.2	A very similar class	8
3.3	A more general approach.	8
3.4	List class with Generics	9
3.5	Binary tree with generics	10
3.6	An attempt to define Functor in Java.	11
3.7	Hypothetical type safe functor in Java	12
4.1	A C program that leaves p pointing to deallocated memory.	14
4.2	A Rust program that does not type check.	14
4.3	A C program which leaks memory.	15
7.1	Haskell representation of Terms.	24
7.2	Haskell representation of Kinds.	24
7.3	Haskell representation of Lifetimes.. . . .	24
7.4	Haskell representation of Types.	25
7.5	Partially applied error monad and language errors.	25
7.6	Record data type showing contexts.	25
7.7	Environment and error monad stack.	25
8.1	Identity function	27
8.2	Addition of two references	27
8.3	Function composition	28
8.4	Double Function application	28

8.5	Quadruple application function using double	28
-----	---	----

Chapter 1

Introduction

1.1 Project Aims

The purpose of this project is to design a type system for a programming language that incorporates Higher Kinded Types with a system that guarantees memory safety at compile time. Higher Kinded types are necessary to neatly express certain desirable programming features. Rust is a programming language that provides memory safety through compile-time checks. This aspect of Rust is known as the *ownership* model, of which *lifetimes* and *borrowing* are key concepts [9]. This project attempts to implement a type checker for this language as a Haskell program, and investigate how higher kinded types and the Rust ownership model interact.

1.2 Types in Programming Languages

Type systems are designed to help programmers reason about behaviours in the programs that they write. Types restrict the kinds of statements that may be expressed, the most obvious reason for doing this is to detect certain types of errors before a program is executed. Small, obvious errors, found in expressions such as "this sentence" * 69 are easily detected, because multiplication makes no sense when applied to a strings of characters and a number. However, modern type systems are capable of doing far more.

As programs become larger and more complex, separating parts of programs that do not need any knowledge of each other becomes more important. It is much easier to maintain a program composed of separate modules that have no knowledge of the inner workings of one another. Modules may interact through well defined interfaces and in this way may be swapped out or replaced much more easily. One may re-write code that conforms to an existing interface without knowing about another module's implementation details. A type system can be used to define this interface and to ensure that new code behaves as expected. Polymorphism, discussed in detail in Section ??, is one way of allowing more flexibility in these interfaces between parts of a program while retaining correctness.

Some programming language features may introduce whole new families of errors. Allowing a programmer to manually allocate and deallocate space for storing objects in memory is known to be a common source of bugs. Languages like C have a reputation for being difficult to write bug free programs in because of manual memory management. Memory leaks may occur if a programmer requests some storage in memory but does not deallocate it. This can lead to programs consuming unreasonably large amounts of memory. Referencing some location in memory after it has been deallocated (and possibly allocated with some new object) is another common pitfall associated with manual memory management. Garbage collection, or the automatic allocation and deallocation of objects in heap memory, may alleviate some of these issues. However, it can incur a sometimes unacceptable runtime overhead especially in software systems where responsiveness is key.

A solution can be found in the type system. Restricting where a programmer can request or reference some location in memory allows a program to be statically analysed before it is run, and any sections of code that could cause memory related issues are shown as compile time errors. A type system can form the basis of this restriction, as shown in Section 4.3.1

In studying these type systems it is often useful formalize them in a system with well known and well understood behaviour. In this case the system is the lambda calculus, which functions as a miniature programming language and as a formal model for understanding the behaviour of types. The lambda calculus and how it pertains to this project is described in Section 5.1. Higher Kinded Types, or higher order polymorphism, have been well described in System F ω , itself a typed lambda calculus [6].

1.3 Goals of This Project

A type checker for a language based upon the lambda calculus will be developed as a Haskell program. Haskell is described in Chapter 7 along with the reasons for choosing it. A parser, type checker, and simple interpreter will all be implemented along with a test programs demonstrating some intended behaviours. The design of the language is described in Section 5. The type-checker aspect of the program is concerned with:

- Higher Kinded types, described in Section ???. Formalised in System F ω , they allow for a neat implementation of very generic, high level programming concepts such as Monads and Functors.
- A system restricting the allocation, use, and deallocation of memory, encoded into the type system. This aspect is based on the type system of the Rust programming language, which guarantees memory safety through its lifetime and borrow checker.

The notion of an addressable area of memory, as well as mechanisms for allocating and deallocating areas of that memory, will be added to the base lambda calculus. The implementation of the type system, as well as the parser, build system, test framework, and interpreter are described in Chapter 7. A formal description of the language can be found in Chapter 5.

1.4 Project Overview

The rest of this report is divided in several chapters. Chapter 2 lists the ethical considerations of this project. Chapter 4 describes important concepts in more detail as well as describing how common tasks related to type checking are accomplished. Chapter 5 then introduces the lambda calculus as way of reasoning about type systems. The design of the language is shown including the grammar. Chapter 6 formalizes what should be accomplished by the type checker to be implemented. Software engineering issues are tackled in Chapter 7, including the test framework and build system used. Key tests demonstrating desired behaviour are given in Chapter 8. Issues about the effectiveness of this type system are described in Chapter 9. Finally, unmet requirements and further work to be done is covered in Chapter 10.

Chapter 2

Professional and Ethical Considerations

No part of this project requires human participation and as such there are no ethical considerations.

Chapter 3

Parametric Polymorphism

This section introduces Parametric Polymorphism, which is found in many programming languages. It is used to make programming languages more expressive while attempting to prevent errors from occurring at runtime. Polymorphism is one way of sticking to a core programming principle: Functionality in a program should only be implemented in one place in the source code. If different functions are meant to do very similar things, it is generally beneficial to combine them into one by parametrizing sections that differ. This allows code to be updated, maintained, and deleted more easily and so becomes very necessary in large codebases. This parametrizing of areas of code is known as abstraction. Abstraction at the levels of values is very common in the form of functions; parametric polymorphism allows for the abstraction at the level of types.

The rest of this chapter attempts to explain how polymorphism is useful, and how it is used in languages like Java to reduce code duplication and increase expressiveness. Generics, or parametric polymorphism in Java, is used extensively in Java's collections framework, which provides very general data structures for organizing data in programs. These structures are practical to implement and use partly because of Generics.

Finally, Functors are introduced as a concept that we would like to be able to represent and use in a programming language, but cannot do so in languages with the expressive power of Java. Higher Kinded Types are introduced to provide very generic solutions to programming problems, and form the basis of a large part of this project.

3.1 A World Without Generics

In software engineering one of the principles to keep in mind when attempting to write software is Don't Repeat Yourself, known as the DRY principle. If lots of similar behaviour exists in different places in a codebase, then a change to this behaviour will result in the code being modified in several places. Such changes to behaviour are common; and not applying changes to one area while applying them to another area can be a source of bugs. There are other reasons not repeat oneself in a codebase as well. Less time is spent writing code if a function only has to be written once, and lots of similar code can distract from the meaning of a program.

As an example, consider writing a list class to store some strings in a language like Java. The class may have an implementation that looks something like this:

```
class StringList {  
  
    public boolean add(String e) {  
        // implementation...  
    }  
  
    public String getAt(int index) {  
        // Get the string at position index...  
    }  
  
    public int size() {  
    }  
}
```



```

    // other sensible methods that you might want in a list...
}

```

Listing 3.1: String List in Java

This seems all very well and good. However, at a different part of the program we might want to have a list of Booleans:

```

class BoolList {

    public boolean add(Boolean e) {
        // add a boolean to the list
    }

    public Boolean getAt(int index) {
        // Get the bool at position index...
    }

    public int size() {
    }
}

```

Listing 3.2: A very similar class

The similarity between these classes is obvious: the methods that they implement are very similar except for the types in method signatures. `BoolList`'s `getAt` methods returns a `Boolean`, and `StringList`'s `getAt` returns a `String`. It is easy to see that the implementation for both of the `getAt` methods would be very similar. Now imagine if there was a bug in the implementation of this method. This bug would likely be present in both of the implementations and so a programmer would have to fix both of these implementations. It would be very possible for the programmer to forget or ignore one of these methods, leading to inconsistent behavior in the program. Even if the programmer did remember to change the codebase in two places, there would still be twice as much code to change. This becomes more of a problem for every new list type that the programmer wishes to implement.

One might be tempted to leverage Java's inheritance to solve this issue. A general list class that stores Java's `Object` class might be the answer. After all, `String` and `Boolean` both extend `Object`. At first glance this seems like a sensible solution, any changes to how lists would only have to be put into effect in this one class. This would be a vast improvement on making changes to every type of list that we implement. The class might look something like:

```

class List {

    public boolean add(Object e) {
        // add whatever you like to the list!
    }

    public Object getAt(int index) {
        // Get the whatever object is stored at index
    }

    public int size() {
    }
}

```

Listing 3.3: A more general approach.

This class looks very similar to the types of list that were implemented in Listings 3.2 and 3.1. However, in the signatures of the methods we use `Object` so we can put whatever we like in the list. The class could be used like this:

```

List list = new List();
list.add("This seems to work well!");
String firstElem = (String) list.getAt(0);

```

However, there could be a problem here. On the last line we get an element from the list, using the `getAt` method, which returns an `Object`. An instance of type `Object` is not very useful because we probably want to call some class-specific methods on our element that we pulled from the list. The example above gets around this by using casting.

Casting is a way of telling the Java compiler that one type should be treated as another. Specifically it is often used to tell the compiler that the class that is being casted from is actually a subtype of the class that is being casted to. In this case it is used to tell the Java compiler that the instance of `Object` that is being returned from the `getAt` method is actually a `String`. This is done so that we can access all of the methods that the `String` class provides, and so this object can be used where ever an instance of the `String` class is expected.

Casting from `Object` cannot be checked by the compiler. This snippet shows what could potentially go wrong in this situation:

```
List list = new List();
list.add(new Boolean(true));
String firstElem = (String) list.getAt(0);    // This line will compile
```

The above code compiles but will throw a `ClassCastException` when run because `String` is not a subclass of `Boolean`. The Java compiler cannot tell from the above that the list object is holding `Boolean` values, so cannot warn the programmer that the above code does not make sense. Any safety provided by the type system has been subverted and the code may be in production somewhere before the obvious error is detected by a human, or worse, throws a runtime exception. This is the kind of problem that Java's Generics were intended to solve.

3.2 Parametrizing Constructors

Just as methods in Java may have formal parameters that abstract values out of the method body, Generics allow types to be abstracted out of the implementation of a class. When a class is constructed a type can be passed in as an argument which can be referenced by the methods that the class provides. The type that is passed into a class is referenced with a type variable, just as arguments to methods are referenced by variables in the scope of that method. This has the benefit that code can be type-checked at compile time. Casting, as demonstrated in Section 3.1, can lead to run time errors which can be difficult to find before they cause errors.

With Generics the list example from the previous section can be implemented like this:

```
class List<T> {
    public boolean add(T e) {
        // add something of type T to the list
    }

    public T getAt(int index) {
        // Get the object of type T stored at index
    }

    public int size() {
    }
}
```

Listing 3.4: List class with Generics

Here the list is parametrized with some as yet unknown type, `T`, in the declaration `class List<T>`. When an instance of this class is created a type is passed into the constructor and the instance becomes a new, specific type of list holding objects of that type. This list can be used like this:

```
List<String> list = new List<String>();
list.add("Much better!");
String firstElem = list.getAt(0); // No casting!
```

The `String` type is passed into the `List` type constructor here. The `T` type variable in Listing 3.4 is instantiated with the `String` type and methods like `getAt` return a `String`. There is no need for casting and the type correctness of this code can be checked at compile time. If we tried to assign the result of the `getAt` method to a boolean variable here the program would not compile.

3.3 More Generic Containers

Any class that acts as a container for other types of object benefits from being parametrized with the type of object that it holds. In the list example earlier in the chapter it did not matter what kind of element the list was meant to store, all that mattered was that there was a list of them. Most data structures are this general, in that the type of element inside the structure does not matter. This is where parametric polymorphism is most useful.

Binary trees are another example of a data structure that can store any type of object. A node in a binary tree can either be empty, or hold an element and a pointer to two other nodes. The element that is held in that tree can be of any type—a perfect opportunity to use generics. The implementation could look something like this:

```
class Tree<T> {
    private Tree<T> left;      // pointer to the left branch
    private Tree<T> right;     // pointer to the right branch
    private T elem;           // Data that this node stores

    public void insert(T e) {
        // insert element into the tree
    }

    public boolean contains(T e) {
        // is e in this tree?
    }

    public int size() {
    }
}
```

Listing 3.5: Binary tree with generics

Very similarly to the list implementation, the tree class must be instantiated with some type, referred to as `T` in the body of the class. Both of these data structures act as generic containers.

This kind of abstraction, where types are parametrized in the body of classes, is known as first-order polymorphism. This notion is formalized in language called System F, described in Chapter 5. However this report attempts to explain higher-order polymorphism, a concept that cannot be expressed in languages like Java. In order to understand why higher order polymorphism is useful and why it cannot be expressed in Java it is important to understand some additional concepts.

3.4 map and Higher Order Functions

As mentioned, both the list in Listing 3.4 and the tree in Listing 3.5 can be thought of as containers that hold some type of object. It is very common in programs to apply a function to every element in collection. In Java, this is commonly expressed with a for-each loop. For example, to get a new list of integers by adding one to every element from an old list of integers one would write:

```
List<Integer> intList = new ArrayList<>();
intList.add(1);
intList.add(2);
intList.add(3);

List<Integer> outList = new ArrayList<>();

for (Integer i : intList) {
    outList.add(addOne(i));           // outList will contain [2, 3, 4]
}
```

Manipulating elements of a collection in this way is very common. However, all we are doing here is applying a function to every element in this container. It would be nice if one could apply the same kind of transformation to the binary tree that we defined, without worrying details of tree traversal in this section of program.

In functional programming this problem is solved by a specific higher-order function, commonly called `map`. A higher-order function one that takes another function as a parameter. `map` as defined for our list class would take a function as a parameter and apply that function to every element in a list. The example from above could be written as:

```
List<Integer> intList = new ArrayList<>();
intList.add(1);
intList.add(2);
intList.add(3);

List<Integer> outList = intList
    .stream()
    .map((x) -> addOne(x));    // Define an lambda function to pass to map
```

Here a lambda function is declared using Java 8 lambda syntax. The function `(x) -> addOne(x)` is declared as a without a name and passed as an argument to the higher-order function, `map`. The lambda function is then applied to every element of the list and a new list is returned.

The `map` function can be declared for any class that acts as a container holding other values. It takes a function as a parameter and applies this function to every the contents of that container. It would make sense to have a `map` function for both lists and trees. It would also make sense to try define an interface for containers that can be mapped over in this manner.

3.5 Functor and Mapping over Containers

Having an interface for containers that can be mapped over would be useful. Any time we wanted to apply a function to every element in a container we could pass a transforming function to the `map` function which the interface would provide and not have to worry about the implementation details of iterating over every single element. Even if the type of collection were to change, e.g. using a tree instead of a list, the transformation would hold because both of the classes would implement the interface. This concept of a mappable container is typically called `Functor`. We can try and write an interface for this concept in Java:

```
interface Functor<A> {
    Functor<B> map(Function<A, B> f);
}
```

Listing 3.6: An attempt to define `Functor` in Java.

At first glance this interface seems to be acceptable. The interface takes a type parameter, `A`, which is the type of the element that the container holds. One method is defined, `map`, which takes a function `f` as a parameter. `f` has a generic type; it takes an object of type `A` and returns an object of type `B`. `map` itself returns an object than implements `Functor` with elements of type `B`.

However the return type of `map` is not sufficient. It may return an object of any class that implements `Functor`, which will have the correct type of elements `B`, but will not be more specific than that. Casting would be needed to use the collection again:

```
List<Integer> intList = new ArrayList<>();
intList.add(1);
intList.add(2);
intList.add(3);

// Before casting, the result of map is just Functor<Integer>
List<Integer> outList = (List<Integer>) intList.map((x) -> addOne(x));
```

This results in a similar situation to the one described in the example of the list that held only `Object` in Listing 3.3. Casting is needed to use the return value of `map` as a list, so is necessary if we wanted to use any list specific methods or pass it into a function that expects a list as an argument. Again, casting is not an ideal solution because it is susceptible to run time exceptions. In other words, this `Functor` interface cannot be used in a type safe manner.

In order to define a generic `Functor` interface, where the return type of `map` is the same as the class that implements functor, we need to reference that class that implements the interface inside the interface itself. In other words, `map`

must know that it returns a `List` when the list class implements `Functor`, or a `Tree` when the tree class implements `Functor`. Hypothetically, this interface might look something like:

```
interface Functor<F<A>> {  
    F<B> map(Function<A, B> f);  
}
```

Listing 3.7: Hypothetical type safe functor in Java

Note that this is not valid Java. In the type parameter to this version of the interface we define a generic class constructor, `F`, that itself take a single generic type parameter, `A`. The `map` function then returns the *same* generic class, but parametrized with the result type `B`. In this manner we could constrain the `map` function to return the same instance of `Functor` that it is called from.

3.6 Higher Kinded Types

define type constructors?

In order to express concepts like the `Functor` described in Listing 3.7 higher order polymorphism is needed. This means that we need the ability to pass classes that themselves have type parameters, like `List`, as type arguments in classes. Type constructors can be represented by type variables in the body of classes. This can be seen in the hypothetical Java functor example above, where the polymorphic type constructor is represented by the type variable `F`. If Java allowed for type constructors to be represented as type variables then the `Functor` syntax above might be one way of representing this.

Other generic concepts could be represented as well. Monads, a way of associating data types with specific computations, are well represented with higher order polymorphism.

Chapter 4

Memory Management

Part of this project is designing a compile time system for memory management. Before describing how this system should work, an overview of existing memory management techniques is given. Most programming languages have the ability to dynamically allocate memory on the *Heap*, which is a very useful language feature. However, the allocation, dereferencing, and freeing of heap memory is problematic and this chapter will describe some of the issues with heap allocated memory.

4.1 Memory Usage and Computational Effects

Most practical programming languages allow for storing and referencing areas in memory. When an expression is evaluated, it may have an effect on memory as well as returning a result. For example, an assignment statement in a programming does not have any obvious result, but instead operates on values in an area of memory that is accessible to other parts of the program. A language that allows for these sorts of computational effects is referred to as *impure* and one of the goals for this project is to make these features safer to use.

4.1.1 Stack and Heap Memory

There are usually two kinds of memory that may be used to store values: stack memory and heap memory. Stack memory is commonly used to store values for function calls. A function is called with parameters referred to by variables, which are in scope for the duration of the function call. These local variables hold the result of evaluating some expression, which is typically stored in stack memory. This has the advantage that memory is very predictably allocated and deallocated. However heap memory is sometimes needed when multiple functions need to refer to or mutate the same value; such as is the case with global variables. These values live longer than any individual scope and therefore it does not make sense to store them on the stack.

The basic operations needed in a system with memory allocation are:

Allocation Allocation refers to creating an area in memory to store the result of an expression. This is commonly seen in the form of variable assignment, for example `x := ref 2 + 3`; . Here the expression `2 + 3` is evaluated¹ and the result is stored in the area of memory referred to by the variable `x`. The value referred to by `x` can then be used at some later point in the program. Variables may also be reassigned, for example `y := x`. `y` would then point to the same location that `x` points to.

Dereference Once an area of memory has been allocated, and is pointed to by a variable, some way of using the expression stored at that location is needed. Dereferencing refers to getting the expression stored at a location in memory. If we wanted to use `x` at some point after the expression `x := ref 2 + 3` had been evaluated, we could write `!x`. The result of that expression would be 5, because `2 + 3` has been evaluated and the result stored in the

¹In languages with *strict* evaluation, the expression is evaluated before the result is bound to the variable. This is not the case in all programming languages.

area of memory that is pointed to by `x`. The dereference operator, `!E`, means “go to the location in memory, `E`, and get the value stored there”.

Deallocation Deallocation refers to freeing memory once it no longer needed. It is common to not want to use memory for the whole lifetime of a program. If memory was never freed programs would use far more memory than they needed, which would not be practical. In order to solve this problem memory may be deallocated once a variable goes out of scope, which is common for stack memory, or we could introduce an explicit deallocate operator, called `free`. This operator would take a memory location and mark that location as unused so that a future allocation could reuse the same space.

Garbage collection is one way of mitigating the problems induced by manual memory management. Memory is automatically deallocated at run time, and the programmer does not have to manually free memory. The freed

most programming languages. Expressions may be evaluated and stored in memory for use at a later point. This operation is called allocation. The variable may then be used in another expression at a later point. Specifically, the *heap* refers to an area of memory that is set aside for dynamic allocation. Usually areas of memory stored here can be allocated, dereferenced, and freed at any point in a program.

4.2 Problems with Existing Memory Management Techniques

Most programming languages allow for dynamic memory management where the program can request portions of memory at run time and free that memory when it is no longer required. This operation can be performed manually as in the case of languages such as C or automatically in languages with a garbage collector such as Java.

4.2.1 Manual Memory Management: `malloc` and `free`

Some languages rely on manual instructions inserted by the programmer in order to allocate and deallocate regions of memory. Most implementations of the C programming language provide a group of library functions for this purpose, which include `malloc` and `free`. As mentioned, these constructs are inserted manually by the programmer. This can lead to the issues described below.

Dangling References

Deallocating storage may lead to dangling references, where some reference exists that points to memory that has been deallocated. This is nearly always unintentional, however it is an easy for a programmer to make this mistake when writing a program. Using the value of deallocated storage can lead to nefarious bugs and most languages consider using deallocated storage to be undefined behaviour.

```
int *dangle()
{
    int i = 69;
    return &i; // Function return address of local variable!
}

int main()
{
    int *p;
    p = dangle();
}
```

Listing 4.1: A C program that leaves `p` pointing to deallocated memory.

In the Rust programming language, references to values must live longer than the resource that they refer to [7]. The same program as the C dangling pointer example (Listing 4.1) written in Rust does not compile as it does not meet this restriction.

```
fn dangle() -> &u32 {
    let i = 69;
    &i // This does not typecheck because this would be a dangling pointer
}

fn main() {
    let p = dangle();
}
```

Listing 4.2: A Rust program that does not type check.

Memory Leaks

Memory leaks occur when heap storage that is no longer usable is not deallocated. This can lead to software allocating more memory for itself and in the worst case can lead to a program consuming all available memory.

```
#include <stdlib.h>

void allocate()
{
    int* a = malloc(sizeof(int) * 100); // Allocate memory on the heap
    // Return and forget about the allocated memory!
}

int main()
{
    allocate();
    // ...
    // do more stuff, while heap space that allocate used is unreachable
}
```

Listing 4.3: A C program which leaks memory.

4.2.2 Automatic Memory Management: Garbage Collection

Techniques have been invented in order to mitigate errors related to manual memory management. Garbage collection is one such method. Garbage is a term for storage that has been allocated on the stack but is no longer reachable by the program, e.g. the storage is pointed to by a variable that has gone out of scope. Automatic garbage collection alleviates the programmer of explicitly managing memory. However there are several downsides to garbage collection. For example, the garbage collector will be invoked to collect unusable memory outside of the control of the programmer. When it is running it affects the execution of the program for an indeterminate amount of time. This hang is not acceptable in real-time systems.

4.3 A Solution in the Type System

Memory safety can still be achieved without the use of a garbage collectors. Program structure may be analysed during semantic checking and areas likely to cause issue can be identified. Here Rust’s way of performing these checks is examined.

4.3.1 An Introduction to Rust’s Model of Memory Management

Rust, a systems programming language [9] is designed to provide memory safety with no runtime overhead. Rather than relying on a garbage collector to provide run-time memory safety, Rust relies on strong compile time checks. This system of compile time checks is referred to as *ownership*, and is derived from affine type systems and unique pointers to memory locations[7] [4].

Affine types

Affine types are a development of Linear type systems. Linear type systems ensure that every variable is used exactly once. In an affine type system, a variable may be used at most once, i.e. zero or one times. This has applications for managing resources in a program that do not persist the whole time that the program is running, e.g. file handles or heap allocated memory [5] [10].

Ownership

Values in Rust are bound to a single *owner*, which is the variable to which it is bound. When the owning variable goes out of scope, the value is freed. For example:

```
{
    let x = 69;
}
```

When `x` goes out of scope the value associated with it will also be released from memory. Because there can only be a single owner associated with a value, aliasing a variable is not allowed. This prevents any two parts of a Rust program from accessing a section of heap memory at the same time.

```
{
    let x = Thing::new();
    let y = x;
    println!("{}", x);
}
```

The above code does not compile because `x` has been moved to `y`, and there is an attempt to use `x` in the print statement. Using a variable as a function argument will also make it not available for use again. If a function uses some value that has been passing in as a argument it must return that same value if the scope outside that function uses it.

```
// value is comes from outside the scope of this function
fn foo(value: Bar) -> Bar {
    // do stuff with value, returning it and hence handing back ownership
    value
}
```

This is not practical, and gets even less practical once there are more arguments that must be passed back to the caller of the function. To this end Rust allows references to a value to be created. Creating a reference to a value in Rust is called borrowing. A reference to a value may be created and passed in to a function that uses it in some way, and that function does not need to thread the ownership of that variable back to the caller.

```
// instead of passing value1 and value2 in by value, create references to values
fn foo(value1: &Bar, value2: &Bar) -> u32 {
    // do stuff with value1 and value2 and return the answer
    123
}
```

There are two kinds of borrows: immutable and mutable. There may be many immutable borrows of a resource at once or a single mutable borrow. This also prevents heap data from being accessed at the same time at different points in the program. The scope of borrow must always be shorter than that of the resource which it borrows.

This system where resources are freed after the single owner goes out of scope, as well as borrows always having shorter lifetimes than original resource mean that Rust can enforce the memory safety of programs. These concepts are built into the type system.

4.4 Representing Programs as Data Structures

talk about ASTs here

4.5 Type checking

talk about ast tree traversal

Chapter 5

Formal Definitions

This chapter attempts to formalize some of the concepts from Chapter 4. The lambda calculus is introduced as a model of computation and as a system for reasoning about features found in programming languages. Types are introduced to the lambda calculus as well as other more complex extensions relevant to this project. The higher order polymorphic lambda calculus, known as System F_ω , is included as well as a lifetime-calculus devised for this project.

5.1 Lambda Calculus

The lambda calculus is model of computation where the only behaviour is function definition and application. It is commonly used to specify programming language features and to formalize their behaviour. Specifically, it is used to reason about type systems. The lambda calculus can be viewed as a miniature programming language and a system where strict properties can be proved.

t	$::=$	x	variables
		$\lambda x . t$	function abstraction
		$t t$	function application

Figure 5.1: Grammer of the untyped lambda calculus.

5.1.1 Simple Types in the Lambda Calculus

The lambda calculus can be extended with the most simple of typing systems. In order to demonstrate how the lambda calculus can be used to reason about type systems, some additional constructs added. If Boolean literals some other concepts are added it becomes more clear how types are useful in programming languages.

Terms		
$t ::=$	x	variables
	$\lambda x : T . t$	function abstraction, with type annotations
	$true$	true literal
	$false$	false literal
	$\text{if } t \text{ then } t \text{ else } t$	if-then-else expression
	$t \ t$	function application

Values		
$v ::=$	$\lambda x : T . t$	lambda value
	$true$	true literal value
	$false$	false literal value

Types		
$T ::=$	$T \rightarrow T$	type of functions
	$Bool$	type of boolean literals

Figure 5.2: Lambda calculus extended with simple types and booleans.

Programs can be constructed using the language defined in Figure 5.1.1 that do not make any sense. For example:

```
baddef = if  $\lambda x : Bool.x$  then false else true
```

This program is constructed according to the grammar of terms. However, is not well typed according to the typing rules in Figure ???. Specifically, the type of the term found in the guard of the if-expression, $\lambda x : Bool.x$ has type $Bool \rightarrow Bool$ but has to be $Bool$ for the term to be considered well typed. It makes sense to restrict the sorts of values found in the guard of an if-then-else expression. Anything other than a boolean value in that place may indicate programmer error, which could be as simple as a spelling mistake or a fundamental misunderstanding of what they are trying to express. Type systems help catch these kind of mistakes before program execution. Specifying these rules on top of the lambda calculus can be a very informative way of looking at programming language features. The rest of this chapter describes other extensions to the lambda calculus that model some of the programming concepts investigated in this report.

5.1.2 System F

System F is an extension of the simply typed lambda calculus [6] that allows for quantification over types as well as terms. In doing this it formalizes the notion of polymorphism in programming languages, as described in Section ???. It is used to study implementations of polymorphism in programming languages.

As the simply typed lambda calculus allows for abstraction of terms outside of terms through function definitions, System F introduces abstractions at the level of types. The system also allows for application of type level expressions. This system can be used to reason about first order polymorphism, however more extensions to talk about higher order polymorphism. These extensions are introduced in Section 5.1.3.

Terms		
t	$::=$	x variables
		$\lambda x : T . t$ function abstraction, with type annotations
		$t\ t$ function application
		$\lambda X . t$ type abstraction
		$t\ [T]$ type application
Values		
v	$::=$	$\lambda x : T . t$ lambda value
		$\lambda X . t$ type abstraction value
Types		
T	$::=$	$T \rightarrow T$ type of functions
		X type variables
		$\forall X . T$ universal type

Figure 5.3: System F

Examples

System F models first order polymorphism in programming languages, such as aspect of the generics found in Java. Some examples of how System F can be used are given below:

```
id =  $\lambda X . \lambda x : X . x$ 
boolId = id [Bool]
```

This example shows type level lambdas, where X is a type variable that has been abstracted out of the function definition. The term level lambda abstracts x which has the type X . Applying `id` to a type maybe be written as `id [Bool]`, which yields $\lambda x : Bool . x$, or the identify function over boolean values. Here X in the original definition of `id` has been instantiated with the type of Booleans.

5.1.3 System F ω

System F ω is also known as the higher order polymorphic lambda calculus. It takes concepts from the polymorphic lambda calculus, or System F, and combines these with type constructors described in Section 5.1.3. From a programming point of view, System F ω allows us to write polymorphic functions not only at the level of types, but also in type constructors.

Most usefully System F ω can be used to build type safe abstractions around traditionally impure forms of computation; typically in the form of a *monad*. Not only is higher order polymorphism very good at formalizing monads, but also very good at combining them. *Monad transformers* are a key example, but outside the scope of this paper. An example of monad transformers in use can be found in Section 7.4.6. Haskell uses the concepts to great effect.

Type Operators

Type constructors were mentioned in Section ?? and this section attempts to frame this idea within the lambda calculus. As mentioned previously, type constructors can be thought of functions from types to new types. Application and abstraction at the level of types can be modelled as a type system for the lambda calculus.

Terms		
t	$::=$	x variables
	$ $	$\lambda x : T . t$ function abstraction, with type annotations
	$ $	$t \ t$ function application
Values		
v	$::=$	$\lambda x : T . t$ lambda value
Types		
T	$::=$	$T \rightarrow T$ type of functions
	$ $	$\lambda X :: K . T$ operator lambda
	$ $	$T \ T$ operator application
	$ $	X type variables
Kinds		
K	$::=$	$*$ kind of concrete types
	$ $	$K \rightarrow K$ kind of type operators

Figure 5.4: Type operators and Kinding

Kinds play a key role here. Just as types enforce well-formed expressions at the level of terms, Kinds are needed to check that expressions at the level of types are well formed. In other words, Kinds do not allow non-sensicle expressions like `Bool Int`, because `Bool` is not a type constructor. Concrete types, also called base types, have Kind $*$. These are the types that may be the type of terms in the language like `false`. Type constructors, like `List` have kind $* \rightarrow *$. They need to be parametrized with a type that had kind $*$.

Type operators combined with System F forms the basis of System F ω . In effect System F ω turns type constructors into first class values of the language. Kind annotations are carried over from the lambda calculus with type constructors.

Terms

$t ::=$	x	variables
	$\lambda x : T . t$	function abstraction, with type annotations
	$t \ t$	function application
	$\lambda X :: K . t$	type abstraction
	$t \ [T]$	type application

Values

$v ::=$	$\lambda x : T . t$	lambda value
	$\lambda X :: K . t$	type abstraction value

Types

$T ::=$	$T \rightarrow T$	type of functions
	$\lambda X :: K . T$	operator lambda
	$T \ T$	operator application
	X	type variables
	$\forall X :: K . t$	universal type

Kinds

$K ::=$	$*$	kind of concrete types
	$K \rightarrow K$	kind of type operators

Figure 5.5: System $F \omega$ **Examples**

examples of programming in System $F \omega$

5.2 Lifetimes

syntax of lifetimes

5.2.1 Adding Impurity

var references, borrow types, etc

5.3 Final Typing Rules

final grammar and typing derivations for the language

Chapter 6

Requirements

Chapter 7

Implementation

This chapter describes how the ideas and type system described in Chapter 5 will be implemented. As stated in Chapter 6, one of the goals for this project is to build a program that will be able to parse, type check, and evaluate a language based on the lambda calculus. The most involved phase of implementation and the focus of this project involves the type checking phase, which includes lifetime checking of pointers and references, polymorphic type checking, and checking that the language of types themselves is well formed, or kind checking.

The requirements of this project influence the choice of the language of implementation. Haskell was chosen as it is well suited to the tasks of parsing, abstract syntax tree declaration, and is in general a practical language to work with.

7.1 The Haskell Language

Haskell is a general purpose, statically typed, functional language [3]. It has several desirable features for a language implementation language. These include:

- Algebraic data types, which are very good at representing abstract syntax trees, used to describe programming languages.
- Pattern matching, which is useful for deconstructing abstract syntax trees.
- A wealth of effective parsing libraries, convening several paradigms.
- Idiomatic monadic programming, which can be used to reduce error handling and state threading boilerplate out of the logic of the program.

It also has the benefit of having higher kinded types built into the language, making it ideal for testing potential features of the implemented language. The language described in Chapter 5 has been implemented as a Haskell program. The rest of this chapter describes how this was accomplished in more specific detail.

7.2 Stack, Haskell's Build System

Stack was used as the build tool for this project [8]. This made it easy to compile and test the project as well as managing libraries. Several commands were very useful in managing the project, including `stack build` to compile all changes to the project and `stack test` which ran all of the tests for the project. The lexer and parser generator source files were not Haskell source files but instead specify how Haskell source files should be built. These tools are described in detail in later sections but Stack was used to automate the building of these tools as well. Finally, Stack provides an interface to an interactive interpreter for Haskell, GHCi. This tool was used extensively to test parts of the project as they were being developed.

7.3 Parsing

A lexer generator, Alex [1], and parser generator, Happy [2], were used in this project. Using these tools in combination made parsing the language into the Haskell representation of the abstract syntax simple. The grammars provided for the parser generator are a very close approximation of Haskell data type. Both Alex and Happy generate Haskell files when run which implement the specified grammars.

7.4 Components of the Type Checker

7.4.1 Terms

The Haskell representation of terms of the language are given in Listing 7.1. Type lambdas and Lifetime lambdas can be seen as first class citizens here.

```
data Term
  = Var String
  | Lit Int
  | Lam String (Lifetime, Type) Term
  | App Term Term
  | TyLam String Kind Term
  | TyApp Term Type
  | LiLam String Term
  | LiApp Term Term
  | Lt Lifetime
  deriving (Eq, Show)
```

Listing 7.1: Haskell representation of Terms.

7.4.2 Kind Checker

The kind checker makes sure that the type expressions in a supplied program are well-formed. The Haskell abstract data type that represents kind expression is show in Listing 7.2.

```
data Kind
  = KnStar
  | KnArr Kind Kind
  deriving (Eq, Show)
```

Listing 7.2: Haskell representation of Kinds.

7.4.3 Lifetime Checking

The syntax of lifetime is show in Listing 7.3.

```
data Lifetime
  = LiVar String
  | LiLit Int
  | LiStatic
  | LiDummy
  deriving (Eq, Show)
```

Listing 7.3: Haskell representation of Lifetimes..

LiDummy is used here as a dummy place holder for occurrences of lifetime literals during parsing, as lifetimes are associated with the scope of terms. An initial walk of the tree replaces dummy values with the LiLit value that represents the depth of the scope that the lifetime value is found in.

7.4.4 Type Checking

Type checking is rather involved in this language as the type system almost contains the lambda calculus itself.

```
data Type
= TyVar String
| TyInt
| TyArr Type Type
| Forall String Kind Type
| OpLam String Kind Type
| OpApp Type Type
deriving (Eq, Show)
```

Listing 7.4: Haskell representation of Types.

7.4.5 Error Reporting

Any part of the program that may result in some kind of error is wrapped in a partial application of Haskell's error monad, Except, to a custom error data type:

```
type ThrowsError = Except LangErr

data LangErr
= ParseError
| NoMain
| VarNotFound String
| WrongKind Kind Kind
| NotKnArr Kind
| WrongType Type Type
| NotTyArr Type
| NotForall Type
deriving (Eq, Show)
```

Listing 7.5: Partially applied error monad and language errors.

This has the advantage of being very composeable and also of reducing error handling boilerplate in the program.

7.4.6 Context Management

The lifetime checker, kind checker, and type checker all rely on a variable typing context. These contexts are threaded through the program using Haskell's environment monad, also known as the Reader monad. The record type holding these contexts is shown in Listing 7.6. Contexts are represented as a map from variable names are strings to some value, using Haskell's own built in strict map data structure.

```
type Ctx = Map.Map String

data Env = Env
{ _typeCtx :: Ctx (Type, Lifetime)
, _kindCtx :: Ctx Kind
, _ltCtx :: Ctx Lifetime
} deriving (Show, Eq)
```

Listing 7.6: Record data type showing contexts.

The monad transformer stack where parsing, lifetime checking, kind checking, and type checking take place is therefore:

```
type Typing = ReaderT Env ThrowsError
```

Listing 7.7: Environment and error monad stack.

7.5 Testing

The testing aspect of this project was very important, and was the only way to have some idea that the program worked as expected. Specifically, these tests needed to be automated so that any changes in the behaviour of the program could be checked to make sure that they did not break any previous behaviours. Test programs were manually written, and then loaded from file.

Testing code goes here, unit tests etc

The correctness of the parser, type checker, and evaluator was tested with the HUnit testing framework for Haskell. This tool integrates with the stack build tool so that all tests can be run with a single command. Tests themselves were small programs— these small programs were loaded from file, parsed, and then type checked. The resulting type was then validated against the expected type that was associated with each test file. This system had the advantage that the whole process was checked any time that changes were made to the behaviour of the type checker.

Certain tests were simply to test the parser aspect of the program but others demonstrated key behavior expected from the language. These tests are covered in more detail in Chapter 8.

Chapter 8

Key Tests

This section describes key test programs that demonstrate programming with higher kinded types and lifetimes. The syntax the language is described in Chapter 5. Additional constructs have been added for clarity, such as allowing a term to be defined with a name.

8.1 Simple Programs

The programs in this section serve as an introduction to the language syntax and style, without introducing more advanced features. Some of the examples are polymorphic in their type.

8.1.1 Polymorphic Identity Function

This example shows the polymorphic identity function:

```
id: (X, 'a) → (X, 'a)
id = λx::* . λ'a . λx: (X, 'a) . x
```

Listing 8.1: Identity function

Above, the type of the function is give. All function parameters are associated with a lifetime as well as a type. This is what is meant by the pair $(X, 'a)$. Here X is a type parameter which is introduced starting in the scope of the function $\lambda x::* ..$. The while id term must be applied to type first, as the type lambda expression is outermost. The type that the expression is applied to must be of kind $*$, like Int or $X \rightarrow X$. For example, $id [Int]$ is type correct.

The term $\lambda 'a ..$ is a lifetime lambda. This term must be applied to some lifetime expression, such as another lifetime variable or a static lifetime.

8.1.2 Multiple Lifetimes and References

More concepts are introduced in this example:

```
add: (&Int, 'a) → (&Int, 'b) → (Int, min('a, 'b))
add = λ'a . λ'b . λx: (&Int, 'a) . λy: (&Int, 'b) . !x + !y
```

Listing 8.2: Addition of two references

Here the dereference operator is used to get the values in the locations held by x and y . Both of these variables have the type of references of Int , demonstrated in the type, $\&Int$. These values have an associated lifetime, or the length that they will exist in memory for. The lifetime of the whole resulting expression is the either $'a$ or $'b$, whichever exists for the shortest length of time. In other words, whichever lifetime is at the top of the stack.

It is quite useful to have multiple lifetimes bound here. x may exist for a different length of time then y . A common real world example would be searching for some value in a larger data structure; the value to search for would only

need to exist for the length of the search function, whereas the structure being search might need to exist for a much longer time.

8.1.3 Higher Order Functions

This example shows functions being used as first class values in the language, which is not very interesting in itself, but the type signatures of the functions are of note. In the simply typed lambda calculus, functions may have type $X \rightarrow X$. Here, functions must annotate the variable that they bind with a lifetime as well as a type. Hence, a function might have the signature $(X, 'a) \rightarrow (X, 'a)$, meaning that a function takes a value of type X that lives for $'a$ and return a value of the same type and lifetime.

```
compose: ((B, 'a) → (C, 'a)) → ((A, 'a) → (B, 'a)) → (A, 'a) → (C, 'a)
compose = λA:: * . λB:: * . λC:: * .
    λ'a .
        λf: (B, 'a) → (C, 'a) .
            λg: (A, 'a) → (B, 'a) .
                λx: (A, 'a) . f (g x)
```

Listing 8.3: Function composition

The signatures of f and g show that they may return values with different types, but the same lifetimes. In fact, all values in this version of `compose` must live for the same length of time.

8.2 Memory safety

The intention of this section is to show how programs written in an unsafe language, like C, can be transformed into a language with memory safety. Specifically, problems in C programs will be highlighted and an equivalent program will be shown that does not compile.

dangle example, calc example that does not typecheck, explain why

8.3 Basic tests

Here basic aspects such as definition

```
double:
double = λX:: * . λa' . λf: (X, 'a) → (X, 'a) . λx:(X, 'a) . f (f x)
```

Listing 8.4: Double Function application

```
quad:
quad = λX:: * . λ'a . double [X → X] a' (double [X] 'a)
```

Listing 8.5: Quadruple application function using double

Chapter 9

Evaluation

9.1 Problems

Chapter 10

Conclusion

10.1 Further Work

Bibliography

- [1] *Alex: A lexical analyser generator for Haskell*. <https://www.haskell.org/alex/>. Accessed: 2016-10-18.
- [2] *Happy: The Parser Generator for Haskell*. <https://www.haskell.org/happy/>. Accessed: 2016-10-18.
- [3] *Haskell: An advanced, purely functional programming language*. <https://www.haskell.org/>. Accessed: 2016-10-18.
- [4] Amit Levy et al. “Ownership is theft: experiences building an embedded OS in rust”. In: *Proceedings of the 8th Workshop on Programming Languages and Operating Systems*. ACM. 2015, pp. 21–26.
- [5] Benjamin C. Pierce. *Advanced Topics in Types and Programming Languages*. The MIT Press, 2004. ISBN: 0262162288.
- [6] Benjamin C. Pierce. *Types and Programming Languages*. 1st. The MIT Press, 2002. ISBN: 0262162091, 9780262162098.
- [7] *References and Borrowing*. <https://doc.rust-lang.org/book/references-and-borrowing.html>. Accessed: 2016-10-18.
- [8] *The Haskell Tool Stack*. <https://docs.haskellstack.org/en/stable/README/>. Accessed: 2016-10-18.
- [9] *The Rust Programming Language*. <https://www.rust-lang.org/en-US/>. Accessed: 2016-10-18.
- [10] Jesse A. Tov and Riccardo Pucella. “Practical Affine Types”. In: *SIGPLAN Not.* 46.1 (Jan. 2011), pp. 447–458. ISSN: 0362-1340. DOI: 10.1145/1925844.1926436. URL: <http://doi.acm.org/10.1145/1925844.1926436>.