

Contents

1 Introduction	4
1.1 Introduction to Type Systems	4
1.1.1 Statically Typed Languages	4
1.1.2 Dynamically Typed Languages	5
1.2 The Simply Typed Lambda Calculus	6
1.2.1 Syntax	6
1.2.2 Type Checking	7
1.2.3 Example Type Derivation	7
1.3 System F	8
1.4 Improvements	10
2 Dynamically Typed Languages	10
2.1 Python	10
2.1.1 Code Example	11
2.1.2 Polymorphism	12
2.2 Runtime Errors	13
3 Statically Typed Languages	13
3.1 Java	14
3.2 Java Generics	14
3.3 Deficiencies	15
4 The Dependent Lambda Calculus	16
4.1	16
4.1.1 Syntax	16
4.1.2 Evaluation	18
4.1.3 Type Checking	18
4.1.4 Example Type Derivation in	20
4.2 Dependent Lists	20
4.2.1 Type Rules for Lists	21
4.3 An example	22
5 Implementation	23
5.1 Implementation Decisions	23
5.1.1 Abstract Syntax	23
5.1.2 Bound and Free Variables	24
5.1.3 Term Equality	24
5.2 Demo	24
5.2.1 Identity example	25
5.2.2 n_copies Example	25

5.2.3	Dependent Lists in Action	26
6	Conclusion	27
7	Future Work	

1 Introduction

Errors are the unavoidable hurdles of the computer programming experience. From forgetting a semi-colon on a first 'Hello World' program, to runtime segmentation faults caused by improper user input, computer scientists will always face the task of debugging their programs, and will never escape the suspicion that a user can make the whole program crash with one illegal command. Computer scientists are faced with the task of writing programs that perform expected computations, but what means do we have to ensure that programs actually execute accordingly to these expectations? Many people disagree on the best methods for ensuring proper program execution, whether they support unit testing, static analysis, or another technique, and programming languages themselves are designed with different strategies for handling these issues.

Type systems provide a formal framework for automating a portion of program analysis, defining typing rules for a type checking algorithm that processes a program to detect type errors. These systems associate a formal semantics with the abstract syntax of a programming language, specifying how different language constructs are allowed to interact with each other. Because this approach analyzes an intermediate representation of the program, usually in the form of an abstract syntax tree generated by parsing the program text, type checking can be performed before program execution, and even before compilation. Some languages apply this type checking algorithm and only compile programs that satisfy the type system without producing a type error, catching many errors before execution that would otherwise cause the program to terminate unexpectedly.

This thesis explores type systems in depth, with the goal of highlighting the insufficiencies of many widely used languages, and compares the costs and benefits gained from more complex type systems. Various type theories are presented and discussed, with the goal of providing enough theoretical background to make the formal theory of dependent lambda calculus accessible.

1.1 Introduction to Type Systems

1.1.1 Statically Typed Languages

Programming languages are generally classified into one of two categories, statically or dynamically typed. Languages that are statically typed, such as Java, C/C++, and ML-like languages, apply a type checking operation during the compilation process, and only compile a program if type

checking does not detect any type errors in the code. Errors such as multiplying an integer by a string, or adding an integer to an array defined to be an array of some user defined object, are caught by the type checker before compilation, whereas other languages may not detect these errors until program execution. This adds a level of safety to the programming language, as the user gains confidence that a program that passes the type checker will execute as it is expected.

However, static type checking comes with some drawbacks as well. As this process must be performed before compiling, compilation becomes more expensive. This does allow for some runtime optimizations that yield more efficient code, but it is also costly to compile and more difficult to write well-typed programs than in dynamic languages that allow much more flexibility. The added restrictions in a statically typed language occasionally rejects some programs that would execute properly occasionally fail to type check. In the case of *if*-statements in a statically typed language such as Java, the type system necessitates that the *then* and *else* clauses have the same type, but a program such as

```
if (True)
    return 1;
else
    return "This case will never happen";
```

fails to type check even though the *else* clause is never reached in execution. Many programmers begrudge these systems for this reason, but proponents of static typing think the limitations are worth the reward.

1.1.2 Dynamically Typed Languages

Often referred to as 'untyped' languages, some languages such as Python do not type check until a program is actually executed. These dynamic systems therefore do not catch type errors until runtime, as there is no static analysis of the program. Because runtime errors are typically fatal, something as easily caught as applying the '+' operator to anything other than a number can go unnoticed until suddenly causing the whole program to fail. But dynamically typed languages allow programmers much more flexibility and power in writing code, as when used properly, complex features such as polymorphism are trivially handled by the runtime system of the language.

1.2 The Simply Typed Lambda Calculus

Beyond determining when a language should handle type checking, when writing a programming language, we must also decide what forms of typing we want to allow. In a static environment, types are checked at compile time, but do programs require explicit type annotations? Should functions be passable values? There exist different theories on which to base these language designs, and this decision carries significant influence over what a programming language allows, or considers an error.

1.2.1 Syntax

The simply typed lambda calculus, λ_{ST} , is the theoretical basis for typed, functional programming languages [3]. This is typically the first formal system one learns about when studying type theory, and most typed languages handle type checking similarly to λ_{ST} , so it makes sense for us to first look at this calculus before considering more complex systems. λ_{ST} is the smallest statically typed, functional programming language we can imagine. Terms in the language can only be one of four forms: variables, constants, abstractions (anonymous functions), or applications. Types are even more simple, and can only be either a base type or a function between types.

$e :=$	x	Variable
	j	Constant
	$j \quad x: .e$	Lambda Abstraction
	$j \quad e \ e$	Application
$:=$		
	j	Base Type
	$j \quad !$	Function Type

Figure 1: Abstract Syntax of λ_{ST}

As an example, we can derive the expression

$$(\lambda x:int.x) 7$$

by following the steps

$$e \neq e \neq (\lambda x: .e) e \neq (\lambda x:int:e) e \neq (\lambda x:int:x) e \neq (\lambda x:int:x) 7$$

where x is a variable, int is a base type, and 7 is a constant in this calculus.

Assuming we are within a context Γ where int is a base type, and integers are constants in the language with type int , we can derive the type of this expression as follows:

$$\begin{array}{c}
 \text{(Var)} \quad \frac{[x := int](x) = int}{[x := int] \vdash x : int} \\
 \text{(Lam)} \quad \frac{}{\vdash (x:int:x) : int \rightarrow int} \\
 \text{(App)} \quad \frac{}{\vdash (x:int:x) 7 : int}
 \end{array}
 \quad
 \begin{array}{c}
 \text{(Const)} \quad \frac{(7) = int}{\vdash 7 : int}
 \end{array}$$

In order to derive the type of the resulting expression, we first check that the applicant has a valid function type, via the **(App)** rule. We extend the context Γ to contain the domain information, that is that x has type int , and check the type of the body of the lambda expression by looking up the variable x in this new context. We confirm that the type of the applicant is $int \rightarrow int$, and then we proceed to look up the type of the operand, 7 , according to the **(Const)** rule. As 7 has the desired type int , the resulting type of the application is type int .

1.3 System F

As was mentioned in the previous section, λ_{int} restricts type expressions to only represent a specific type, meaning polymorphic code is unachievable in a language based on that formal system. In order to write reusable code that works properly over all types, we need to extend the definition of the lambda calculus to allow abstraction over types.

System F provides such a solution, allowing lambda abstractions to range over types, as well as over values [3]. For simplicity's sake, we will only discuss relevant additional features to this system instead of going into the same level of detail as with λ_{int} .

While all valid λ_{int} expressions and types are valid in System F, we also extend the abstract syntax to allow types as terms, and terms of the form

$$T : e$$

and extend the syntax of types to allow types of the form

$$T \rightarrow T$$

This extension is the basis of the form of parametric polymorphism in Java Generics and the type systems of ML-like languages such as Standard ML (SML) and Ocaml. To highlight the strength and flexibility of this formal system, we can compare the polymorphic identity function in System F to

the identity function in λ . If we have a language with *int* and *String* as base types based on the type rules of λ , we must write separate identity functions $x:int.x$ and $x:String.x$, with types $int \rightarrow int$ and $String \rightarrow String$ respectively, to operate on expressions of the two different base types. Although these are perfectly valid in λ , this creates redundant code that could be significantly condensed with a more powerful system, as the two functions perform equivalent functions.

In System F, we write the polymorphic identity function as

$$\lambda x. x$$

This allows us to abstract over the type of the input, and we supply the desired type as the first parameter when we apply the function. That is, if we desire the identity function on objects of type *int*, we simply apply $\lambda x. x$ to *int*, and replace all *x*'s in the body of the λ with *int*, yielding $int.int$. Thus the single polymorphic lambda abstraction can capture the identity function on any desired type, by simply providing the desired type as a parameter. We must adapt the type rules to allow for application of abstractions to types by the following:

$$\frac{\lambda e. e}{\lambda e. \mathbf{8} : \mathbf{!}} \text{ (T-Lam)} \quad \frac{\lambda e. \mathbf{8} : \mathbf{!} \quad \lambda : \text{Type}}{\lambda e. \mathbf{9} := \mathbf{!}} \text{ (T-App)}$$

Figure 3: Extended Type Rules for System F

where $\mathbf{9} := \mathbf{!}$ in the (T-App) rule means that we replace all occurrences of $\mathbf{!}$ in $\mathbf{8}$ with $\mathbf{!}$, and the assertion $\lambda : \text{Type}$ means that λ is a valid type in context λ . Thus we can provide a type judgement for the polymorphic identity function as follows:

$$\frac{\text{(Var)} \quad \frac{[x := \mathbf{!}](x) = \mathbf{!}}{[x := \mathbf{!}] \lambda x. \mathbf{!}}}{\text{(Lam)} \quad \lambda (x : \mathbf{!}) : \mathbf{!}} \text{ (T-Lam)} \quad \lambda (x : \mathbf{!}) : \mathbf{8} : \mathbf{!}$$

and conclude that the polymorphic identity function in System F has type $\mathbf{8} : \mathbf{!}$.

As we see in this example, System F allows programmers much more flexibility and power to write reusable, polymorphic code. This lies at the basis of polymorphic data structures, map, and fold functions that make code efficient and take advantage of properties of functional languages to their fullest.

1.4 Improvements

In languages implementing the type theories describe up to this point, type checking can catch errors at runtime such as applying a function to an input of the wrong type, or trying to append an element of the wrong type to a typed list. Static type checking provides a huge benefit to programmers by catching many mistakes before a program is ran, preventing runtime crashes. But even in languages based on the polymorphic System F, there are runtime errors we wish we could prevent through static analysis. While it is arguable that the compile-time costs and restricted freedom on the side of the programmer make type systems more of a hindrance than beneficial, we can extend these type systems further to catch even more errors before runtime, increasing the value of static analysis.

Accompanying this thesis is an OCaml implementation of a dependently typed, higher-order functional programming language, based on the dependently typed lambda calculus, [C_λ](#), developed from Per Martin Lof's

tions are first-class citizens, meaning they can be passed as arguments, and returned as output of other functions. Although some of these features may appear similar to the formal systems discussed, we will see how Python differs in handling program semantics and execution.

2.1.1 Code Example

As briefly presented earlier, Python allows the *then* and *else* clauses of *if*-statements to differ in their types. While programmers contend that statically typed languages may reject programs that would never fail to execute, the lack of restrictions in a language like Python could be the root of easily preventable, fatal errors at runtime.

To highlight the behavior of *if*-statements in a dynamically typed program, let's observe the following factorial function:

```
def factorial (n):
    if n < 0:
        return "Invalid Input"
    elif n == 0:
        return 1
    else :
        return n * factorial (n-1)
```

If `factorial` is called with a non-negative input, the function performs the expected factorial computation we are familiar with from mathematics. However, Python allows us to handle negative inputs in any way we want, whereas statically typed languages could only produce an exception to be handled or a runtime error. Here, the function returns a value of type *String* when called with a negative number. This does allow programmers to return meaningful information while avoiding a fatal error, but to advocates of type systems, no longer knowing how the program will execute is too dangerous a risk to take.

Additionally, nothing necessitates calling `factorial` with an integer, so we can just as easily call it with a floating-point number. Again, we do not know how the program will behave on an atypical input, as there is no standard mathematical definition of the factorial function on non-integers. In a statically typed system, type annotations can require integer inputs, and promise integer outputs, and otherwise catch these errors before execution and fail to compile.

2.1.2 Polymorphism

As was just mentioned, Python would allow us to call `factorial` on integers, floating-point numbers, or an object of any other type, without complaining until possibly producing a runtime error. For the `factorial` example, this does not make the most sense, as the factorial function is only defined in mathematics on integer values. But this does display the flexibility and freedom a programmer has working in a dynamically typed environment. Though the factorial function may not take advantage of this freedom, untyped languages make writing polymorphic code nearly effortless.

As our first example, Python allows us to write the identity function as follows:

```
def identity(x):  
    return x
```

which is polymorphic over all types of inputs. As the function's operation does not depend on any type-specific features of the input, it should naturally be polymorphic, but a language with explicit, static type declarations would require us to write nearly identical `identity` functions to operate on different types of input.

```
def n_copies(n, x):  
    return [x]*n
```

```
def length(l):  
    if l == []:  
        return 0  
    else:  
        return 1 + length(l[1:])
```

```
def reverse(l):  
    if length(l) == 0:  
        return []  
    return [l[-1]] + reverse(l[:-1])
```

Figure 4: Polymorphic Functions on Lists in Python

For a more interesting example, let us look at polymorphic operations on lists in Figure 4. Some features of lists are independent of the literal elements, or types of those elements, contained within a list. Creating a list of 'n' copies of an object, calculating the length of a list, or reversing the order of a list, are all naturally expressed as polymorphic functions.

Although these functions are polymorphic in the sense that they will properly execute on lists of any type of element, these are not type-safe according to any formal polymorphic type system. While we can reverse a list of integers, or a list of strings just as easily with this reverse function, there is nothing stopping an unknowing programmer from calling the reverse function on for example an integer or dictionary, rather than a list. The dynamic typing of Python enables these polymorphic functions to be written easily, but does nothing to ensure that they are used properly, as such a type error wouldn't be detected until runtime, crashing whatever program makes the illegal function call.

2.2 Runtime Errors

We have been discussing the shortcomings of dynamically typed programming languages for the past few sections, highlighting how errors preventable by static analysis become runtime errors that are often fatal to the program's execution. However, it is important to point out that some errors are by their nature runtime errors in most common type systems. While array or list indices, or invalid user input at runtime cannot be handled by languages like Java either, the issue with dynamic languages is that all errors become runtime errors. This puts additional pressure on programmers to write proper code, without providing any assistance to understand what the code actually does.

3 Statically Typed Languages

Now we switch our focus to statically typed languages with specific examples of Java programs. Programming takes on additional effort, however minimal, as explicit type annotations are required to satisfy the type checking algorithm, but we will see how Java's type system ensures that we are programming properly to the best of its ability.

3.1 Java

Java's type system at a basic level works in the same way as the simply typed lambda calculus. Programmers supply explicit type annotations to variables during assignment, and if the type of the expression is of anything

This straightforward implementation of a List class is a syntactically nicer version of System F, where Item takes the place of all λ in the calculus. When we instantiate a ListC of integers by declaring

```
List<Integer> list = new ListC<Integer>();
```

we replace all occurrences of Item in the class with the type Integer. Now the add function accepts an Integer as input instead of an Item, so if we try to compile the line

```
list.add("This is a String, not an Integer...");
```

we will get a type error during compilation. Python would allow such actions, as lists are general and do not restrict the types of elements allowed in a list, that is, a list could contain both an integer and a string in Python. Here, by parameterizing ListC with the type Integer, we restrict the allowed types of elements to only integers.

To portray the polymorphism of Generics, we could just as easily instantiate a list strings by declaring

```
List<String> list_2 = new ListC<Integer>();
```

in which case we could add the string from before without producing a type error at compile time.

Java Generics allow programmers to write polymorphic, reusable code that ranges over all types of objects, and adds an additional level of type-safety for such programs that languages like Python cannot capture. This polymorphism is based on λ of the formal System F, and adheres to its theoretical type rules.

3.3 De ciencias

Even with a more robust type system (or the mere existence of a static type system as compared to dynamically typed languages), languages such as Java cannot capture all errors during compilation. Notably, Java has no way of statically detecting illegal access of list or array indices until runtime.

Imagine having the two lists of Integer elements:

```
List<Integer> list_1 = new ListC<Integer>();  
List<Integer> list_2 = new ListC<Integer>();
```

where the two lists are defined to be [1, 2, 3, 4, 5] and

4.1.2 Evaluation

While we did not discuss evaluation in simply-typed or polymorphic contexts, type-checking in λ is a form of evaluation. We will see what this means shortly, but here we present the evaluation rules and discuss their meanings.

$$\begin{array}{c}
 \frac{}{? \rightarrow ?} \quad \frac{}{8x \rightarrow 8x} \quad \frac{}{x \rightarrow x} \\
 \frac{e \rightarrow e' \quad x : \tau}{e[x] \rightarrow e'[x]} \quad \frac{}{x : \tau \rightarrow x : \tau}
 \end{array}$$

Figure 7: Evaluation Rules for λ [1]

When we evaluate the $? \rightarrow ?$ term, it simply evaluates to the $?$ value.

When evaluating a dependent function space, we evaluate the domain τ , and the codomain σ to evaluate the whole term.

Evaluating applications, we first evaluate the operator term to a lambda abstraction value. We then replace all x in the body of the lambda abstraction with e^0 , and evaluate this substituted body to w .

thus typing involves evaluating the input, and type checking the type of the codomain of the dependent function space in a context, extended with the newly evaluated input.

$$\begin{array}{c}
 \frac{}{\Gamma \vdash ? : ?} \text{ (Star)} \\
 \\
 \frac{\Gamma \vdash ? : ? \quad + \quad \Gamma [x := ?] \vdash e^0 : ?}{\Gamma (x : ?) \vdash ? : ?} \text{ (Pi)} \\
 \\
 \frac{\Gamma \vdash ? : ? \quad + \quad \Gamma [x := ?] \vdash e : ?^0}{\Gamma (x : ?) \vdash \lambda x. e : ?^0} \text{ (Lam)} \\
 \\
 \frac{\Gamma \vdash e : ?^0 \quad \Gamma \vdash e^0 : ?^0 \quad + \quad \Gamma [x := e^0] \vdash ?^0}{\Gamma \vdash e e^0 : ?^0} \text{ (App)}
 \end{array}$$

Figure 8: Type Rules for λ [1]

The Star term type checks as the type ?

the intention is to gain additional capabilities through the more complex type system. To take full advantage of λ , we introduce dependent list types. We want them to be polymorphic, so that we can declare a list of integers, a list of strings, or even a list of types, and to be able to statically ensure that we do not violate the prescribed type of a list by trying to insert an element of an improper type. Additionally, we include the length of a list in its type, thus we the type $list(x)$, where λ has kind $?$ and x is an integer. In concrete instances, this allows us to construct objects of such types as $int\ list(3)$, or $?\ list(5)$ (read int list of length 3 and star list of length 5, that is a list of types of length 5).

To allow for such constructs in the abstract syntax, we allow a term to be of the forms:

$stop[\]$	Nil of type
$more[e; \]\ e^0\ e^{00}$	Cons of length e , type λ , element e^0 , and rest e^{00}
$list(e)$	List of type

$$\begin{array}{c}
\frac{\text{` } : ? \quad +}{\text{` stop[] : list(0)} \text{ (Nil)}} \\
\frac{\text{` } e + v \quad + \quad \text{` } : ? \quad \text{` } e^0 : \quad \text{` } e^{00} : \text{list}(v \ 1)}{\text{` more[e;] } e^0 e^{00} : \text{list}(v)} \text{ (Cons)} \\
\frac{\text{` } : ? \quad \text{` } e : \text{int}}{\text{` list}(e) : ?} \text{ (List)}
\end{array}$$

Figure 9: Type Rules for List Constructs in

To type check a Nil list, we first check that `stop` has kind `?`, and then evaluate `stop` to determine the type of the elements of the list.

Type checking a Cons cell is the most computationally expensive portion of type checking in our language. As shown in the type rule above, type checking involves evaluation of terms. We first ensure that the provided length term is of type `int`, and evaluate it to `vto`

We can apply the same type rule to derive the type of the tail in expression (1), and then apply the Nil type rule to derive the type of the end of the list. This displays that even for a simple, explicitly declared list of length 2, type checking is expensive, so why do we go through all of this effort?

abstraction obfuscates the underlying semantics of `let` more than I wanted to allow.

5.1.2 Bound and Free Variables

The tutorial implementation utilizes de Bruijn indices to maintain bound variables and their scopes throughout the intermediate representation of the language [1]. Again, though this may be the standard implementation practice, I chose to instead implement direct substitution of variables bound to symbols. To avoid name capture, I maintained a context containing information of types and values for both type checking and evaluation.

5.1.3 Term Equality

Because of the previous choices made in the tutorial paper, checking equality of terms became non-trivial. While it would be easy to assert that the `int` type is equal to the `int` type, but not equal to the `bool` type, the higher-order abstract syntax makes certain cases more difficult to compare. Because functions are used to define language constructs for dependent function spaces and lambda abstractions, we cannot simply ask if two OCaml functions are equal to determine the equality of the term itself. We would need to assert that the two OCaml functions produced the same output on every given input, a task that sounds too complicated to even attempt to address.

A technique called 'quotation' was used to handle this issue, effectively reverting higher-order abstract syntactic representations of values to first-order terms that can be syntactically checked for equality [1]. Once again, this did not uphold my expectations of clarity and simplicity in my own implementation, and fortunately by avoiding a higher-order abstract syntax altogether, I was able to implement a straightforward syntactic comparison to determine equality.

5.2 Demo

To test my implementation of the language and confirm it properly adheres to the semantics of `let`, I implemented a read-eval-print-loop interpreter to demo some code written in my language. It is important to realize that this interpreter conflates type checking and evaluation of terms into a single process, and so appears to behave as a dynamically typed interactive language. Although these errors seem to occur only during program

execution, type checking and evaluation are actually implemented as separate processes, that in a compiler would be separated into pre-compile type checking that produces a compiled executable of the program if type checking is satisfied, and evaluation of this already statically analyzed executable program.

5.2.1 Identity example

To introduce the syntax of my implementation, we begin with a presentation of the polymorphic identity function we have previously shown the typing rules for in .

```
let id: pi x: . pi y: x. x =  
      fn x: . fn y: x. y;;  
  
id int 8;; (*Evaluates to 8*)  
id (pi x: . pi y: x. x) id;; (*Evaluates to 'id' function*)  
id int id;; (*Fails to type check*)
```

Function declarations mimic the syntax of a lambda abstraction, and a let

When we componentwise multiply two integer lists of length 1, the application passes the type checking process, so compilation would continue and we can expect the program to execute properly and return the list [25]. If we try to componentwise multiply lists on elements that are of non-integer type, then the type system catches a type error during compilation, just as we would expect in a statically typed language such as Java. Finally, we see the power of λ_{dep} as a type system. When we try to componentwise multiply two integer lists of different lengths, type checking fails, as we require both lists input to be of length 1.

6 Conclusion

These examples show how λ_{dep} effectively handles the same typed situations as less expressive type theories. Simply-typed and polymorphic terms remain well-typed in λ_{dep} , and we have introduced more information to the type system to capture more understanding during static analysis. Dependent lists are a powerful extension of the dependently typed lambda calculus; they maintain the flexibility of polymorphic lists and express more about the

certain errors during static analysis, but catch all that would be caught in simple type systems, and additional errors that are beyond their scope.

7 Future Work

Hopefully the usefulness of dependent types is made clear from the previous discussions, but there is more work to be done in creating highly expressive type systems to ensure additional safety of program execution. It seems that the more expressive the type system, the more errors we are capable of catching during static analysis, so naturally we want to extend further to reap its full benefits.

Though my current implementation introduces some extensions of `Agda` to incorporate assignments, conditionals, arithmetic, boolean logic, and dependent lists, much is lacking compared to what most immediately think of as a general programming language. Extending the core type system further to allow dependent abstract data types, other dependent data structures, and a core API strengthened by the theoretical foundation of `Agda` would be the next natural step in further developing this implementation.

Despite the expressive power of such a complex, but useful type theory, requiring types to contain such additional information inevitably clutters the syntax of a language. Not only do we have explicit type annotations, but these type annotations depend on evaluation of terms. Of course, it would be helpful to clean up the syntax of my implementation to improve ease of use, but this would also further dispel the notion that dependently typed languages are not suited for general programming. The highly expressive type systems based on an encoding of predicate logic in language make for extremely powerful logic-based proof systems, but it is often thought that the complexity of dependent types is too high for common purposes. Hopefully a straightforward implementation and more succinct syntax will help discourage this belief.

Although `Agda` has deficiencies, the most notable of which is probably the computational cost of type checking a dependent language, it is important to recognize the usefulness we can gain from such additional security. While static typing will never even be universally accepted due to the restrictions it places on the programmer, we should still acknowledge the importance and practicality of more rigid formal systems thanks to their increased assurance of proper execution.

References

- [1] Andres Löh , Conor McBride , Wouter Swierstra, **A Tutorial Implementation of a Dependently Typed Lambda Calculus** *Fundamenta Informaticae*, v.102 n.2, p.177-207, April 2010
- [2] Norell, Ulf. **Dependently typed programming in Agda** *Advanced Functional Programming*. Springer Berlin Heidelberg, 2009. 230-266.
- [3] Benjamin C. Pierce. **Types and Programming Languages** MIT Press, 2002.

Appendix

```
1 (
2   file: ast.ml
3   author: Sam Baxter
4
5   This file lays out the abstract syntax of the language.
6   A substitution function is implemented to handle
7   substitution of types and values in type checking and
8   the evaluation process.
9   A toString function is provided for the interactive display.
10  )
11
12  type variable =
13    j String of string
14    j Symbol of string int
15    j Dummy
16
17  type term =
18    j Var of variable
19    j Star
20    j Pi of abstraction
21    j Lambda of abstraction
22    j App of term term
23    j Int of int
24    j Bool of int
25    j Ann of term term
26    j If of term term term
27    j And of term term
28    j Or of term term
29    j Op of term term list
30    j Let of abstraction
31    j IntType
32    j BoolType
33  )
```



```
139 |
140 | and toStringList = function
141 |   j [] > ""
142 |   j [only] > toString only
143 |   j x::xs > (toString x) ^ ", " ^ (toStringList xs)
144 |
145 | and toStringVar = function
146 |   j String s > s
147 |   j Symbol (s, i) > s
148 |
149 | and toStringAbs (x, t, e) = "(" ^ (toStringVar x) ^ ", " ^ (
    toString t) ^ ", " ^ (toString e) ^ ")"
```

10 interpreter.ml The apply functions can be used to actually
put a type checker for (or
12 implementation of) a primitive to use.

To extend the basis with new primitives, the list primNames
14 must be
extended with an appropriate identifier.
16)

open Environment;;

(
20 This is the master list of names of primitive operators.

22 NB: THESE NAMES ARE LAYED OUT IN A FIXED ORDER!

24 let primOpNames = ["+"; " "; " "; " "; " "; "/"; "%"; " "; "<"; "<="; "="
"; "<"; ">"; " 333.G ET q 2359 ref Q 0 g 0 G 1 6 1 G q 1 0 0 1 7 122.61 549.34 c319.10F6d0 J 0.398 w 0 6


```

100 (fun (Ast.Int(v1),
101       Ast.Int(v2)) > ( / )
102   Ast.Int (v1 / v2));

104 (fun (Ast.Int(v1),
105       Ast.Int(v2)) > ( % )
106   Ast.Int (v1 mod v2));

108 (fun (Ast.Int(v1),
109       Ast.Int(v2)) > ( )
110   let v1' = float_of_int v1 in
111     let v2' = float_of_int v2 in
112     Ast.Int(int_of_float(v1' / v2')));

114 (fun (Ast.Int(v1),
115       Ast.Int(v2)) > ( < )
116   Ast.Bool(if v1 < v2 then 1 else 0));

118 (fun (Ast.Int(v1),
119       Ast.Int(v2)) > ( <= )
120   Ast.Bool(if v1 <= v2 then 1 else 0));

122 (function
123   j (Ast.Int(v1),
124     Ast.Int(v2)) > ( = )
125     Ast.Bool(if v1 = v2 then 1 else 0)
126     j(a,b) >
127     Ast.Op(Ast.Var(Ast.String("=")), [a;b]));

128
129 (function
130   j (Ast.Int(v1),
131     Ast.Int(v2)) > ( < )
132     Ast.Bool(if v1 < v2 then 1 else 0)
133     j (a,b) >
134     Ast.Op(Ast.Var(Ast.String "<"), [a;b]));

136
137 (function
138   j (Ast.Int(v1),
139     Ast.Int(v2)) > ( >= )
140     Ast.Bool(if v1 >= v2 then 1 else 0)
141     j (a, b) >
142     Ast.Op(Ast.Var(Ast.String ">="), [a;b]));

144
145 (function
146   j (Ast.Int(v1),
147     Ast.Int(v2)) > ( > )
148     Ast.Bool(if v1 > v2 then 1 else 0)
149     j (a,b) >

```

```
Ast.Op(Ast.Var(Ast.String(">")), [a;b]);
```

```

8   formal rules of the dependent type system. The equal function
9   compares the equality of terms/types.
10  )
12  open Ast
13  open Environment
14
15  let rec normalize env = function
16  j Var x >
17      (match
18          (try lookup _value x !env
19           with Not_found > raise (Failure "unknow identifier nn
20          "))
21      with
22          j None > (Var x, env)
23          j Some e > (fst(normalize env e), env))
24  j Star >
25      (Star, env)
26  j Pi a >
27      (Pi (normalize _abs env a), env)
28  j Lambda a >
29      (Lambda (normalize _abs env a), env)
30  j App(e1, e2) >
31      let e2' = fst (normalize env e2) in
32      (match fst (normalize env e1) with
33          j Lambda (x, _, e1') >
34              (fst (normalize env (subst [(x, e2')] e1')), env)
35          j e1 >
36              (App(e1, e2)), env)

```

```

56     (match rator', rands with
57       j BinaryOp f, [a;b] >
58         (f (fst (normalize env a), fst (normalize env b)),
env)
59       j UnaryOp f, [a] >
60         (f (fst (normalize env a))), env)
61 j Prod x >
62   (Prod (List.map fst (List.map (normalize env) x)), env)
63 j Let (x, t, e) >
64   let t' = fst (normalize env t) in
65   let e' = fst (normalize env e) in
66   extend x t' ~value:e' env;
67   (Let (x, t', e'), env)
68 j IntType >
69   (IntType, env)
70 j BoolType >
71   (BoolType, env)
72 j BinaryOp f as x > (x, env)
73 j UnaryOp f as x > (x, env)
74 j List(typ, len) >
75   (List(fst (normalize env typ), fst (normalize env len)),
env)
76 j Nil e > (Nil (fst (normalize env e)), env)
77 j Cons(len, typ, el, rest) >
78   (Cons(fst (normalize env len), fst (normalize env typ),
fst (normalize env el), fst (normalize env rest)), env)
79 j lsNil e >
80   (match fst (normalize env e) with
81     j Nil a as t > (Bool(1), env)
82     j Cons(_, -, -, _) > (Bool(0), env)
83     j _ > raise (Failure "Input cannot normalize nn"))
84 j Head e >
85   (match fst (normalize env e) with
86     j Cons(_, -, e, _) > (e, env)
87     j _ > raise (Failure "Cannot normalize head of anything
other than non empty list nn"))
88 j Tail e >
89   (match fst (normalize env e) with
90     j Cons(_, -, -, e) > (e, env)
91     j Nil e > (Nil e, env)
92     j _ > raise (Failure "Cannot normalize tail of anything
other than a list nn"))
93 j _ > raise (Failure "Input cannot normalize nn")
94
95 and normalize_abs env (x, t, e) =
96   let t' = fst (normalize env t) in
97   (x, t', e)
98
99 let rec all_true l = (match l with

```

```

100 j [] > true
101 j [x] > x
102 j x::xs > x && all _true xs)

104 let rec apply_list fs ls =
  (match fs, ls with
106   j [], [] > []
107   j [f], [x] > [f x]
108   j x::xs, y::ys > (x y)::(apply_list xs ys))

110 let equal env e1 e2 =
  let rec equal' e1 e2 = (match e1, e2 with
112   j Var x1, Var x2 > x1 = x2
113   j App(d1, d2), App(f1, f2) > equal' d1 f1 && equal' d2 f2
114   j Star, Star > true
115   j Pi a1, Pi a2 > equal_abs a1 a2
116   j Lambda a1, Lambda a2 > equal_abs a1 a2
117   j Int i, Int j > i = j
118   j Bool b, Bool b' > b = b'
119   j Ann(d1, d2), Ann(f1, f2) >
120     equal' d1 f1 && equal' d2 f2
121   j Op(r, rands), Op(r', rands') >
122     equal' r r' && all _true (apply_list (List.map equal'
123     rands) rands'))
124   j Let a1, Let a2 >
125     equal_abs a1 a2
126   j IntType, IntType > true
127   j BoolType, BoolType > true
128   j Prod a, Prod b >
129     (match a, b with
130      j [], [] > true
131      j [x], [y] > equal' x y
132      j x::xs, y::ys > equal' (Prod xs) (Prod ys))
133   j List(a, b), List(x, y) >
134     equal' a x && equal' b y
135   j Nil a, Nil b >
136     equal' a b
137   j Cons(a1, b1, c1, d1), Cons(a2, b2, c2, d2) >
138     equal' a1 a2 && equal' b1 b2 && equal' c1 c2 && equal'
139     d1 d2
140   j IsNil a, IsNil b >
141     equal' a b
142   j Head a, Head b >
143     equal' a b
144   j Tail a, Tail b >
145     equal' a b
146   j -

```



```

    equal' t t' && (equal' (subst [(x, z)] e1) (subst [(x', z)]
148   e2))
  in
    equal' (fst (normalize env e1)) (fst (normalize env e2))
150
let rec infer env = function
152   j Var x >
      (try lookup _typ x !env
154     with Not_found > raise (Failure "unknown identifier nn"))
  j Star > Star
156   j Pi (x, t, e) >
      let t' = infer env t in
158     let temp = !env in
      extend x t env;
160     let e' = infer env e in
      env := temp;
162     (match t', e' with
      Star, Star > Star
164     j -, - > raise (Failure "invalid type in dependent
function spacenn"))
  j Lambda (x, t, e) >
166     let t' = infer env t in
      let temp = !env in
168     extend x t env;
      let e' =
170       (try infer env e
        with Failure s >
172         env := temp;
          raise (Failure ("Input doeise ((1)]410.959 ref Q 0 g 0 G 1 g 1 G q 1 0 0 1 487.641 341.121 cm

```

```

194         (match (infer env e2), (infer env e3) with
195             j List(t, a), List(t', b) >
196                 check_equal env t t';
197                 List(t', b)
198             j List(_, Int i), List(_, Int j) > raise (Failure "If
199 statement on lists does not type checknn")
200             j _, _ > raise (Failure ("If statement does not type
201 checknn" ^ (toString (infer env e2)) ^ " <> " ^ (toString (
202 infer env e3))))))
203 j And(e1, e2) >
204     let e1' = infer env e1 in
205     let e2' = infer env e2 in
206     check_equal env e1' e2';
207     check_equal env e1' BoolType;
208     BoolType
209 j Or(e1, e2) >
210     let [e1'; e2'] = List.map (infer env) [e1; e2] in
211     check_equal env e1' e2';
212     check_equal env e1' BoolType;
213     BoolType
214 j Op(rator, rands) >
215     let (x, Prod(s), t) = infer _pi env rator in
216     let e = List.map (infer env) rands in
217     apply_list (List.map (check_equal env) s) e;
218     subst [(x, Prod(rands))] t
219 j Prod x > Prod (List.map (infer env) x)
220 j Let(x, typ, e) >
221     let temp = !env in
222     extend x typ env;
223     let t = infer env e in
224     (try check_equal env t typ
225      with Failure s >
226         env := temp;
227         raise (Failure ("Let binding does not type checknn" ^ (
228 s)))));
229     env := temp;
230     t
231 j IntType >
232     Star
233 j BoolType >
234     Star
235 j List(typ, len) >
236     (match infer env typ, infer env len with
237         j Star, IntType > Star
238         j _ > raise (Failure "Input does not type check as list
239 nn"))
240 j Nil e >
241     let t = fst (normalize env e) in
242     check_equal env (infer env t) Star;

```

```

238     List(t, Int 0)
j Cons(len, typ, el, rest) >
240     let len' = fst (normalize env len) in
242     let typ' = fst (normalize env typ) in
244     check_equal env (infer env typ') Star;
246     check_equal env (infer env len') IntType;
248     let el' = infer env el in
250     check_equal env typ' el';
252     (match len', infer env rest with
254     j Int i, List(t, Int j) >
256         check_equal env t typ';
258         (try assert (i = j+1)
260         with Assert_failure s > raise (Failure "List
lengths do not type checknn"));
262         List(typ', len')
264     j -, List(t, _) >
266         List(typ', len')
268     j - > raise (Failure "Cons does not type checknn"))
j IsNil e >
270     (match infer env e with
272     j List(_, Int i) > BoolType
274     j - > raise (Failure "Input does not type checknn"))
j Head e >
276     (match infer env e with
278     j List(t, _) >
280         t
282     j - > raise (Failure "Head does not type checknn"))
j Tail e >
284     (match infer env e with
286     j List(t, Int i) as t' >
288         if i = 0 then t'
290         else List(t, Int (i - 1))
292     j List(t, a) >
294         List(t, Op(Var(String(" ")), [a; Int 1]))
296     j - > raise (Failure "Tail does not type checknn"))
j - >
298     raise (Failure "General input does not type checknn")
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999

```

```

284 if not (equal env x y) then raise (Failure ("Expressions are
      not equivalentnn" ^ (Ast.toString x) ^ " <> " ^ (Ast.toString
      y)))

```

Listing 4: ../../Final/staticsemantics.ml

```

( file: lexer.mll )
2 ( Lexical analyzer returns one of the tokens:
  the token NUM of integer,
  4 operators (PLUS, MINUS, MULTIPLY, DIVIDE, CARET),
  or EOF. It skips all blanks and tabs, unknown characters. )
6 f
  open Parser ( Assumes the parser file is "parser.mly". )
8 g
  let digit = ['0' '9']
10 let word = ['a' 'z' 'A' 'Z']
  rule token = parse
12 j [' ' '\n' '\r'] f token lexbuf g
  j ',' f COMMA g
14 j digit+
  j "." digit+
16 j digit+ "." digit as num
      f NUM (int_of_string num) g
18 j '+' f PLUS g
  j '-' f MINUS g
20 j '*' f MULTIPLY g
  j '/' f DIVIDE g
22 j '%' f MOD g
  j ':' f COLON g
24 j ';' f SEMI g
  j ">" f ARROW g
26 j "fn" f FUN g
  j "pi" f PI g
28 j "~" f STAR g
  j '.' f DOT g
30 j "int

```

```
44 j "!=" f NEALT g
j ">=" f GE g
46 j ">" f GT g
j "true" f TRUE g
48 j "false" f FALSE g
j "let" f LET g
50 j "in" f IN g
j "if" f IF g
52 j "else" f ELSE g
j "then" f THEN g
54 j "and" f AND g
j "or" f OR g
56 j "not" f NOT g
j word+ as string f ID string g
58 j '(' f LPA'
```



```

j exp LT exp          f let id = told("<") in Ast.Op(id,[ $1; $3
  ) g
69 j exp LE exp        f let id = told("<=") in Ast.Op(id,[ $1; $3
  ) g
j exp CMPEQ exp       f let id = told("==") in Ast.Op(id,[ $1; $3
  ) g
71 j exp NE exp        f let id = told(">") in Ast.Op(id,[ $1; $3
  ) g
j exp NEALT exp       f let id = told(">") in Ast.Op(id,[ $1; $3
  ) g
73 j exp GT exp        f let id = told(">") in Ast.Op(id,[ $1; $3
  ) g
j exp GE exp          f let id = told(">=") in Ast.Op(id,[ $1; $3
  ) g
75 j NOT exp           f let id = told("not") in Ast.Op(id,[ $2])
  g
j MINUS exp           f let id = told("-") in Ast.Op(id,[ Ast.Int
  (0); $2]) g
77 j LPAREN exp RPAREN f $2 g
j IF exp THEN exp ELSE exp f Ast.If($2,$4,$6) g
79 j exp AND exp        f Ast.And($1, $3) g
j exp OR exp           f Ast.Or($1, $3) g
81 j LET ID COLON tyterm EQ exp f Ast.Let(Ast.String($2), $4
  , $6) g
;
83
list:
85 NIL LBRACKET tyterm RBRACKET f Ast.Nil($3) g
j CONS LBRACKET term COMMA tyterm RBRACKET exp term f Ast.Cons(
  $3, $5, $7, $8) g
87
tyterm:
89 INTTYPE             f Ast.IntType g
j BOOLTYPE             f Ast.BoolType g
91 j PI ID COLON tyterm DOT tyterm f Ast.Pi(Ast.String($2), $4, $6
  ) g

```



```
52         )  
53     )  
54     with Parsing.Parse_error >  
55     (   output_string stdout "Input string does not parse  
...nn";
```