

COMP3141

Software System Design and Implementation

Theory of Types

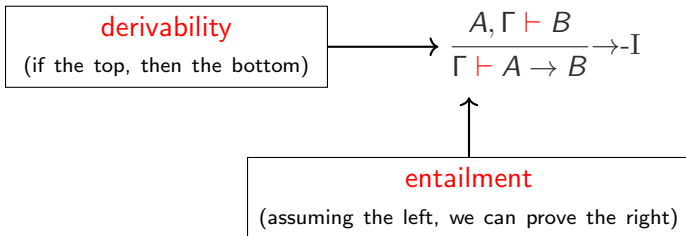
Liam O'Connor
CSE, UNSW (and data61)
Term 2 2019

Natural Deduction

Logic

We can specify a logical system as a *deductive system* by providing a set of *rules* and *axioms* that describe how to prove various connectives.

Each connective typically has *introduction* and *elimination* rules. For example, to prove an implication $A \rightarrow B$ holds, we must show that B holds assuming A . This introduction rule is written as:



More rules

Implication also has an elimination rule, that is also called *modus ponens*:

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow\text{-E}$$

Conjunction (and) has an introduction rule that follows our intuition:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-I}$$

It has *two* elimination rules:

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-E}_1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-E}_2$$

More rules

Disjunction (or) has two introduction rules:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee\text{-I}_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee\text{-I}_2$$

Disjunction elimination is a little unusual:

$$\frac{\Gamma \vdash A \vee B \quad A, \Gamma \vdash P \quad B, \Gamma \vdash P}{\Gamma \vdash P} \vee\text{-E}$$

The true literal, written \top , has only an introduction:

$$\overline{\Gamma \vdash \top}$$

And false, written \perp , has just elimination (*ex falso quodlibet*):

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash P}$$

Example Proofs

Example

Prove:

- $A \wedge B \rightarrow B \wedge A$
- $A \vee \perp \rightarrow A$

What would **negation** be equivalent to?

Typically we just define

$$\neg A \equiv (A \rightarrow \perp)$$

Example

Prove:

- $A \rightarrow (\neg\neg A)$
- $(\neg\neg A) \rightarrow A$ **We get stuck here!**

Constructive Logic

The logic we have expressed so far does **not** admit the law of the excluded middle:

$$P \vee \neg P$$

Or the equivalent double negation elimination:

$$(\neg\neg P) \rightarrow P$$

This is because it is a **constructive** logic that does not allow us to do proof by contradiction.

Boiling Haskell Down

The theoretical properties we will describe also apply to Haskell, but we need a smaller language for demonstration purposes.

- No user-defined types, just a small set of built-in types.
- No polymorphism (type variables)
- Just lambdas ($\lambda x.e$) to define functions or bind variables.

This language is a very minimal functional language, called the **simply typed lambda calculus**, originally due to Alonzo Church.

Our small set of built-in types are intended to be enough to express most of the data types we would otherwise define. We are going to use logical inference rules to specify how expressions are given types (*typing rules*).

Function Types

We create values of a function type $A \rightarrow B$ using lambda expressions:

$$\frac{x :: A, \Gamma \vdash e :: B}{\Gamma \vdash \lambda x. e :: A \rightarrow B}$$

The typing rule for function application is as follows:

$$\frac{\Gamma \vdash e_1 :: A \rightarrow B \quad \Gamma \vdash e_2 :: A}{\Gamma \vdash e_1 e_2 :: B}$$

What other types would be needed?

Composite Data Types

In addition to functions, most programming languages feature ways to *compose* types together to produce new types, such as:

Classes

Tuples

Structs

Unions

Records

Combining values conjunctively

We want to store two things in one value.

(might want to use non-compact slides for this one)

Has

type Point

midpoint (

= ((x1+x2

type

float

float

} poi

point }

poi

mid

mid

ret

}

C Structs

Java

"Better" Java

```
class Point {  
    private float x;  
    private float y;  
    public Point (float x, float y) {  
        this.x = x; this.y = y;  
    }  
    public float getX() {return this.x;}  
    public float getY() {return this.y;}  
    public float setX(float x) {this.x=x;}  
    public float setY(float y) {this.y=y;}  
}  
  
Point midPoint (Point p1, Point p2) {  
    return new Point((p1.getX() + p2.getX()) / 2.0,  
                     (p2.getY() + p2.getY()) / 2.0);  
}
```

Product Types

For simply typed lambda calculus, we will accomplish this with tuples, also called *product types*.

$$(A, B)$$

We won't have type declarations, named fields or anything like that. More than two values can be combined by nesting products, for example a three dimensional vector:

$$(\text{Int}, (\text{Int}, \text{Int}))$$

Constructors and Eliminators

We can **construct** a product type the same as Haskell tuples:

$$\frac{\Gamma \vdash e_1 :: A \quad \Gamma \vdash e_2 :: B}{\Gamma \vdash (e_1, e_2) :: (A, B)}$$

The only way to extract each component of the product is to use the `fst` and `snd` eliminators:

$$\frac{\Gamma \vdash e :: (A, B)}{\Gamma \vdash \text{fst } e :: A} \quad \frac{\Gamma \vdash e :: (A, B)}{\Gamma \vdash \text{snd } e :: B}$$

Unit Types

Currently, we have no way to express a type with just **one** value. This may seem useless at first, but it becomes useful in combination with other types.

We'll introduce the **unit** type from Haskell, written `()`, which has exactly one inhabitant, also written `()`:

$$\Gamma \vdash () :: ()$$


Disjunctive Composition

We can't, with the types we have, express a type with exactly **three** values.

Example (Trivalued type)

```
data TrafficLight = Red | Amber | Green
```

In general we want to express data that can be **one** of multiple **alternatives**, that contain different bits of data.

Example (More elaborate alternatives)

```
type Length = Int
type Angle = Int
data Shape = Rect Length Length
           | Circle Length | Point
           | Triangle Angle Length Length
```

This is awkward in many languages. In Java we'd have to use inheritance. In C we'd have to use unions.

Sum Types

We'll build in the Haskell `Either` type to express the possibility that data may be one of two forms.

`Either A B`

These types are also called *sum types*.

Our `TrafficLight` type can be expressed (grotesquely) as a sum of units:

$$\text{TrafficLight} \simeq \text{Either } () (\text{Either } () ())$$

Constructors and Elimimators for Sums

To make a value of type `Either A B`, we invoke one of the two **constructors**:

$$\frac{\Gamma \vdash e :: A}{\Gamma \vdash \text{Left } e :: \text{Either } A \ B}$$

$$\frac{\Gamma \vdash e :: B}{\Gamma \vdash \text{Right } e :: \text{Either } A \ B}$$

We can branch based on which alternative is used using **pattern matching**:

$$\frac{\Gamma \vdash e :: \text{Either } A \ B \quad x :: A, \Gamma \vdash e_1 :: P \quad y :: B, \Gamma \vdash e_2 :: P}{\Gamma \vdash (\text{case } e \text{ of Left } x \rightarrow e_1; \text{Right } y \rightarrow e_2) :: P}$$

Examples

Example (Traffic Lights)

Our traffic light type has three values as required:

$$\text{TrafficLight} \simeq \text{Either } () (\text{Either } () ())$$

$$\text{Red} \simeq \text{Left } ()$$

$$\text{Amber} \simeq \text{Right } (\text{Left } ())$$

$$\text{Green} \simeq \text{Right } (\text{Right } (\text{Left } ()))$$

The Empty Type

We add another type, called `Void`, that has **no** inhabitants.

Because it is empty, there is no way to construct it.

We do have a way to eliminate it, however:

$$\frac{\Gamma \vdash e :: \text{Void}}{\Gamma \vdash \text{absurd } e :: P}$$



If I have a variable of the **empty** type in scope, we must be looking at an expression that will **never** be evaluated. Therefore, we can assign any type we like to this expression, because it will never be executed.

Gathering Rules

$$\Gamma \vdash e :: \text{Void}$$

$$\Gamma \vdash \text{absurd } e :: P$$

$$\Gamma \vdash () :: ()$$

$$\Gamma \vdash e :: A$$

$$\Gamma \vdash e :: B$$

$$\Gamma \vdash \text{Left } e :: \text{Either } A \ B$$

$$\Gamma \vdash \text{Right } e :: \text{Either } A \ B$$

$$\Gamma \vdash e :: \text{Either } A \ B$$

$$x :: A, \Gamma \vdash e_1 :: P$$

$$y :: B, \Gamma \vdash e_2 :: P$$

$$\Gamma \vdash (\text{case } e \text{ of Left } x \rightarrow e_1; \text{Right } y \rightarrow e_2) :: P$$

$$\Gamma \vdash e_1 :: A$$

$$\Gamma \vdash e_2 :: B$$

$$\Gamma \vdash e :: (A, B)$$

$$\Gamma \vdash e :: (A, B)$$

$$\Gamma \vdash (e_1, e_2) :: (A, B)$$

$$\Gamma \vdash \text{fst } e :: A$$

$$\Gamma \vdash \text{snd } e :: B$$

$$\Gamma \vdash e_1 :: A \rightarrow B$$

$$\Gamma \vdash e_2 :: A$$

$$x :: A, \Gamma \vdash e :: B$$

$$\Gamma \vdash e_1 \ e_2 :: B$$

$$\Gamma \vdash \lambda x. e :: A \rightarrow B$$

Removing Terms...

$$\begin{array}{c}
 \frac{\Gamma \vdash \text{Void}}{\Gamma \vdash P} \qquad \frac{}{\Gamma \vdash ()} \\
 \\
 \frac{\Gamma \vdash A}{\Gamma \vdash \text{Either } A \ B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash \text{Either } A \ B} \\
 \\
 \frac{\Gamma \vdash \text{Either } A \ B \quad A, \Gamma \vdash P \quad B, \Gamma \vdash P}{\Gamma \vdash P} \\
 \\
 \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash (A, B)} \qquad \frac{\Gamma \vdash (A, B)}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash (A, B)}{\Gamma \vdash B} \\
 \\
 \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \rightarrow B}
 \end{array}$$

This looks exactly like **constructive logic!**

If we can construct a **program** of a certain **type**, we have also created a **proof** of a certain **proposition**.

The Curry-Howard Correspondence

This correspondence goes by many names, but is usually attributed to **Haskell Curry** and **William Howard**.

It is a **very deep** result:

Programming	Logic
Types	Propositions
Programs	Proofs
Evaluation	Proof Simplification

It turns out, no matter what logic you want to define, there is always a corresponding λ -calculus, and vice versa.

Constructive Logic	Typed λ -Calculus
Classical Logic	Continuations
Modal Logic	Monads
Linear Logic	Linear Types, Session Types
Separation Logic	Region Types

Examples

Example (Commutativity of Conjunction)

andComm :: $(A, B) \rightarrow (B, A)$

andComm *p* = (snd *p*, fst *p*)

This proves $A \wedge B \rightarrow B \wedge A$.

Example (Transitivity of Implication)

transitive :: $(A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow (A \rightarrow C)$

transitive *f g x* = *g* (*f x*)

Transitivity of implication is just **function composition**.

Translating

We can translate logical connectives to types and back:

Conjunction (\wedge)	Tuples
Disjunction (\vee)	Either
Implication	Functions
True	()
False	Void

We can also translate our *equational reasoning* on programs into *proof simplification* on proofs!

Proof Simplification

Assuming $A \wedge B$, we want to prove $B \wedge A$.

We have this unpleasant proof:

$$\frac{\frac{A \wedge B}{B} \quad \frac{\frac{\frac{A \wedge B}{A} \quad \frac{A \wedge B}{A}}{A \wedge A}}{A}}{B \wedge A}$$

Proof Simplification

Translating to types, we get:

Assuming $x :: (A, B)$, we want to construct (B, A) .

$$\begin{array}{c}
 \frac{x :: (A, B)}{\text{fst } x :: A} \quad \frac{x :: (A, B)}{\text{fst } x :: A} \\
 \hline
 \frac{x :: (A, B)}{\text{snd } x :: B} \quad \frac{(\text{fst } x, \text{fst } x) :: (A, A)}{\text{snd } (\text{fst } x, \text{fst } x) :: A} \\
 \hline
 (\text{snd } x, \text{snd } (\text{fst } x, \text{fst } x)) :: (B, A)
 \end{array}$$

We know that

$$(\text{snd } x, \text{snd } (\text{fst } x, \text{fst } x)) = (\text{snd } x, \text{fst } x)$$

Lets apply this simplification to our proof!

Proof Simplification

Assuming $x :: (A, B)$, we want to construct (B, A) .

$$\frac{\frac{x :: (A, B)}{\text{snd } x :: B} \quad \frac{x :: (A, B)}{\text{fst } x :: A}}{(\text{snd } x, \text{fst } x) :: (B, A)}$$

Back to logic:

$$\frac{\frac{A \wedge B}{B} \quad \frac{A \wedge B}{A}}{B \wedge A}$$

Applications

As mentioned before, in **dependently typed languages** such as Agda and Idris, the distinction between value-level and type-level languages is removed, allowing us to refer to our program in types (i.e. propositions) and then construct programs of those types (i.e. proofs).

Peano Arithmetic

If there's time, Liam will demo how to prove some basic facts of natural numbers in Agda, a dependently typed language.

Generally, dependent types allow us to use rich types not just for programming, but also for verification via the Curry-Howard correspondence.

Caveats

All functions we define have to be **total and terminating**.
Otherwise we get an **inconsistent** logic that lets us prove false things:

$$\begin{aligned} proof_1 &:: P = NP \\ proof_1 &= proof_1 \end{aligned}$$

$$\begin{aligned} proof_2 &:: P \neq NP \\ proof_2 &= proof_2 \end{aligned}$$

Most common calculi correspond to **constructive** logic, not **classical** ones, so principles like the **law of excluded middle** or **double negation elimination** do not hold:

$$\neg\neg P \rightarrow P$$



Semiring Structure

These types we have defined form an algebraic structure called a *commutative semiring*.

Laws for Either and Void:

- Associativity:
 $\text{Either } (\text{Either } A \ B) \ C \simeq \text{Either } A \ (\text{Either } B \ C)$
- Identity: $\text{Either } \text{Void } A \simeq A$
- Commutativity: $\text{Either } A \ B \simeq \text{Either } B \ A$

Laws for tuples and 1

- Associativity: $((A, B), C) \simeq (A, (B, C))$
- Identity: $((), A) \simeq A$
- Commutativity: $(A, B) \simeq (B, A)$

Combining the two:

- Distributivity: $(A, \text{Either } B \ C) \simeq \text{Either } (A, B) \ (A, C)$
- Absorption: $(\text{Void}, A) \simeq \text{Void}$

What does \simeq mean here? It's more than logical equivalence.

Isomorphism

Two types A and B are *isomorphic*, written $A \simeq B$, if there exists a *bijection* between them. This means that for each value in A we can find a unique value in B and vice versa.

Example (Refactoring)

We can use this reasoning to simplify type definitions. For example:

```
data Switch = On Name Int
           | Off Name
```

Can be simplified to the isomorphic $(\text{Name}, \text{Maybe Int})$.

Generic Programming

Representing data types generically as sums and products is the foundation for *generic programming* libraries such as GHC generics. This allows us to define algorithms that work on arbitrary data structures.

Type Quantifiers

Consider the type of `fst`:

`fst :: (a,b) -> a`

This can be written more verbosely as:

`fst :: forall a b. (a,b) -> a`

Or, in a more mathematical notation:

$$\text{fst} :: \forall a\ b. (a, b) \rightarrow a$$

This kind of quantification over type variables is called **parametric polymorphism** or just **polymorphism** for short.

(It's also called **generics** in some languages, but this terminology is bad)

What is the analogue of \forall in logic? (via Curry-Howard)?

Curry-Howard

The type quantifier \forall corresponds to a universal quantifier \forall , but it is **not** the same as the \forall from first-order logic. What's the difference?

First-order logic quantifiers range over a set of *individuals* or values, for example the natural numbers:

$$\forall x. x + 1 > x$$

These quantifiers range over *propositions* (types) themselves. It is analogous to *second-order logic*, not first-order:

$$\forall A. \forall B. A \wedge B \rightarrow B \wedge A$$

$$\forall A. \forall B. (A, B) \rightarrow (B, A)$$

The first-order quantifier has a type-theoretic analogue too (type indices), but this is not nearly as common as polymorphism.

Generality

If we need a function of type $\text{Int} \rightarrow \text{Int}$, a polymorphic function of type $\forall a. a \rightarrow a$ will do just fine, we can just instantiate the type variable to Int . But the reverse is not true. This gives rise to an ordering.

Generality

A type A is *more general* than a type B , often written $A \sqsubseteq B$, if type variables in A can be instantiated to give the type B .

Example (Functions)

$$\text{Int} \rightarrow \text{Int} \quad \sqsubseteq \quad \forall z. z \rightarrow z \quad \sqsubseteq \quad \forall x y. x \rightarrow y \quad \sqsubseteq \quad \forall a. a$$

Constraining Implementations

How many possible total, terminating implementations are there of a function of the following type?

$$\text{Int} \rightarrow \text{Int}$$

How about this type?

$$\forall a. a \rightarrow a$$

Polymorphic type signatures constrain implementations.

Parametricity

Definition

The principle of **parametricity** states that the result of polymorphic functions cannot depend on **values** of an abstracted type. More formally, suppose I have a polymorphic function g that is polymorphic on type a . If run any arbitrary function $f :: a \rightarrow a$ on all the a values in the input of g , that will give the same results as running g first, then f on all the a values of the output.

Example

$$foo :: \forall a. [a] \rightarrow [a]$$

We know that **every** element of the output occurs in the input. The parametricity theorem we get is, for all f :

$$foo \circ (map\ f) = (map\ f) \circ foo$$

More Examples

$$\text{head} :: \forall a. [a] \rightarrow a$$

What's the parametricity theorems?

Example (Answer)



For any f :

$$f (\text{head } \ell) = \text{head } (\text{map } f \ell)$$

More Examples

$$(++) :: \forall a. [a] \rightarrow [a] \rightarrow [a]$$

What's the parametricity theorem?

Example (Answer)

$$\text{map } f (a ++ b) = \text{map } f a ++ \text{map } f b$$

More Examples

$concat :: \forall a. [[a]] \rightarrow [a]$

What's the parametricity theorem?

Example (Answer)

$$map\ f\ (concat\ ls) = concat\ (map\ (map\ f)\ ls)$$

Higher Order Functions

$$\text{filter} :: \forall a. (a \rightarrow \text{Bool}) \rightarrow [a] \rightarrow [a]$$

What's the parametricity theorem?

Example (Answer)

$$\text{filter } p (\text{map } f \text{ } l s) = \text{map } f (\text{filter } (p \circ f) \text{ } l s)$$

Parametricity Theorems

Follow a similar structure. In fact it can be mechanically derived, using the *relational parametricity* framework invented by John C. Reynolds, and popularised by Wadler in the famous paper, “Theorems for Free!”¹.

Upshot: We can ask `lambdabot` on the Haskell IRC channel for these theorems.

¹<https://people.mpi-sws.org/~dreyer/tor/papers/wadler.pdf>

Wrap-up

- 1 That's the entirety of the assessable course content for COMP3141.
- 2 Assignment 2 is due in just over a week.
- 3 There is a quiz for this week, but no exercise.
- 4 Next week's lectures consist of a **guest lecture** on Tuesday, from **Dr. Hira Taqdees Syeda** of the Trustworthy Systems group at data61 (CSIRO), and a **revision lecture** on Wednesday.
- 5 Please come up with **questions** to ask us for the revision lecture! It will be over very quickly otherwise.