Simply Typed $\lambda$-calculus
Lecture 4

Jeremy Dawson

The Australian National University

Semester 2, 2019
Normalisation for typed terms.

Intuitionistic logic and type theory.
Recall that computation in $\lambda$-calculus is captured by $\beta$-reduction:

$$(\lambda x. M) \ N \rightarrow_\beta M[x := N].$$

Obviously $\rightarrow_\beta$ does not apply to every term, e.g., $\lambda x. x$ cannot be reduced further.

One fundamental question is whether $\beta$-reduction terminates, when one starts with an arbitrary $\lambda$-term.

We know that the untyped $\lambda$-calculus is Turing complete, so obviously termination is not possible in all cases.

But it turns out that computation from well-typed terms always terminates.
\(\beta\)-normal form

- A \(\lambda\)-term \(M\) is said to be in \(\beta\)-normal form if \(M \not\rightarrow_\beta\), i.e., the \(\beta\)-reduction cannot be applied to \(M\).
- Terms in \(\beta\)-normal form have the following shape:

\[
\lambda x_1 \cdots \lambda x_n. x \ M_1 \cdots M_k
\]

where each \(M_i\) is itself a term in \(\beta\)-normal form.
- Example: \(\lambda x \lambda y. x (y \ x)\) is in \(\beta\)-normal form.
- Example: \(\lambda x \lambda y. x ((\lambda x. x)y)\) is not in \(\beta\)-normal form.
Weak normalisation

A term $M$ is weakly normalising if there is a $\beta$-reduction sequence from $M$ that terminates. Equivalently, $M$ is weakly normalising if it has a $\beta$-normal form.

Examples:

- $(\lambda x.x \ x) \ (\lambda x.x \ x)$ is not weakly normalising.
- $(\lambda x.\lambda y.y) \ ((\lambda x.x \ x)(\lambda x.x \ x))$ is weakly normalising. Its normal form is $\lambda y.y$. 
A term $M$ is strongly normalising if every $\beta$-reduction sequence from $M$ terminates.

Examples:

- $(\lambda x \lambda y. y) \ ((\lambda x. x \ x)(\lambda x. x \ x))$ is not strongly normalising (though it is weakly normalising).
- $(\lambda x \lambda y. y) \ (\lambda x. x \ x)$ is strongly normalising.
Normalisation of typed terms

- Turing (1942) proved that simply typed $\lambda$-terms are weakly normalising.
- Tait (1967) proposed a proof technique, called *reducibility*, to prove strong normalisation.
- The reducibility technique generalises beyond simply typed calculus, e.g., to polymorphic $\lambda$-calculus by Girard.
- Strong normalisation proofs for type systems are generally highly complex.
- For discussions on the techniques, refer to
  
Consequence of normalisation

Strong normalisation of simply typed $\lambda$-calculus, together with Church-Rosser property, implies that $\beta$-equality for typed terms is decidable.

**Theorem**

*Given two typeable terms $M$ and $N$ of the same type, the problem of determining whether $M =_\beta N$ is decidable.*

This also means that simply typed $\lambda$-calculus is not Turing complete.
Intuitionistic Logic and Type Theory
Intuitionistic Logic

- Intuitionistic logic is a branch of logic that originated from the *constructivist* approach to the foundations of mathematics in the late 19th century.
- Its conception was generally attributed to Brouwer.
- Characterised by the rejection of the principle of proof by contradiction and the *excluded middle* principle, and its insistence on constructive proofs.
- Proofs and proof constructions play a central role.
- There is a close connection between intuitionistic logic and simply typed $\lambda$-calculus: the *Curry-Howard* correspondence (next lecture).
Classical vs. intuitionistic truth

### Disjunction property
- **Classical**: $A \lor B$ ("$A$ or $B$") is true if $A$ is true or $B$ is true.
- **Intuitionistic**: $A \lor B$ is true if you can show me a *proof* of $A$ or a *proof* of $B$.

### Existential property
- **Classical**: $\exists x. A(x)$ ("there exists $x$ such that $A(x)$ holds") is true if assuming the non-existence of such an object leads to contradiction.
- **Intuitionistic**: $\exists x. A(x)$ is true if you can *construct* an object $t$ and a *proof* of $A(t)$.
Example: a non-constructive proof

**Theorem**

There are irrational numbers $a$ and $b$ such that $a^b$ is rational.

**Proof.**

Consider $\sqrt{2}^{\sqrt{2}}$. If it is rational, then we are done: let $a = b = \sqrt{2}$. (It is well-known that $\sqrt{2}$ is irrational).

Otherwise, it is irrational. Then we have

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \times \sqrt{2}} = \sqrt{2^2} = 2$$

which is certainly rational.

So in this case, let $a = \sqrt{2}^{\sqrt{2}}$ and let $b = \sqrt{2}$.  □
Example: a non-constructive definition

Suppose someone tells you that he found a number $x$ such that

\[ \text{if } x \text{ is prime then } P = NP, \text{ otherwise } P \neq NP. \]

So he has reduced the $P = NP$ problem to a prime testing problem. Great! (Whether $P = NP$ or not is a famous unsolved problem). When asked about the magic value of $x$, he tells you

\[ x \text{ is the natural number that is equal to 7 if } P = NP, \text{ and 9 otherwise.} \]

This is a non-constructive definition. But otherwise it is a perfectly good definition (classically speaking).
The syntax of intuitionistic logic

- Assume an infinite set $\text{Atm}$ of *propositional variables*:
  $\alpha, \beta, \alpha_1, \beta_1, \alpha_2, \ldots$

- The set of propositional intuitionistic formulae is given by the grammar:

  \[ \varphi ::= \alpha \mid \top \mid \bot \mid \varphi \land \varphi \mid \varphi \lor \varphi \mid \varphi \rightarrow \varphi \mid \neg \varphi \]

  where $\alpha$ is a propositional variable (also called an *atomic formula*).

- The syntax is the same as classical propositional logic; the difference is in the semantic.
Semantics of intuitionistic logic

- The meaning of intuitionistic formulae can be explained in terms of the *possible worlds* semantics. The truth value of a statement can depend on at which world the statement is made.
- Think of a mathematician whose knowledge increases over time (and never forgets anything!).
- The possible-worlds semantics was originally developed by Kripke for modal logics, and later adapted to intuitionistic logic.
A Kripke frame is a pair \((W, R)\) where \(W\) is a non-empty set of worlds and \(R\) is a binary relation on \(W\).

A Kripke model is a triple \((W, R, \vartheta)\), where

- \((W, R)\) is a Kripke frame; and
- \(\vartheta : W \times Atm \to \{t, f\}\) is a “valuation” function mapping a world and an atomic formula to true \((t)\) or false \((f)\).

Intuitively, \(\vartheta(w, \alpha) = t\) means that \(\alpha\) is true at world \(w\).
Kripke models for intuitionistic logic

- An **intuitionistic Kripke frame** is a Kripke frame \((W, R)\) such that \(R\) satisfies:
  - Reflexivity: \(aRa\), for all \(a \in W\).
  - Transitivity: for all \(a, b, c \in W\), if \(aRb\) and \(bRc\) then \(aRc\).
  - Anti-symmetry: for all \(a, b \in W\), if \(aRb\) and \(bRa\) then \(a = b\).

That is, \(R\) is a **partial order**.

- An **intuitionistic Kripke model** is a Kripke model \((W, R, \vartheta)\) where
  - \((W, R)\) is an intuitionistic Kripke frame, and
  - \(\vartheta\) satisfies the **persistency condition**:

    for every \(\alpha \in Atm\) and every \(u, v \in W\), if \(uRv\) then
    \(\vartheta(u, \alpha) = t\) implies \(\vartheta(v, \alpha) = t\).

- The persistency condition says that if an atomic formula is true in a world \(w\), then it must be true in all successor worlds of \(w\).
Kripke frames as graphs

- It is sometimes useful to draw directed graphs visualising intuitionistic Kripke frames.
- To simplify presentation, reflexivity and transitivity are implicit.
- So only draw edges between nodes that are “adjacent” (no other node in between)
- For example: If \( W = \{x, u, v, w\} \) and 
  \[ R = \{(x, x), (x, v), (x, u), (x, w), (v, v), (v, w), (u, u), (u, w), (w, w)\} \]
  then \((W, R)\) is represented by the following graph:
The semantic forcing relation

Henceforth, by a model we mean an intuitionistic Kripke model.

Given a model $\mathcal{M} = (W, R, \vartheta)$, a world $w \in W$ and a formula $\varphi$, we write $w \models \varphi$ to mean $\varphi$ is true at world $w$, and $w \not\models \varphi$ to mean $\varphi$ is false at $w$.

- $w \models \top$ (always true) and $w \not\models \bot$ (always false).
- $w \models \alpha$ iff $\vartheta(w, \alpha) = t$ (for $\alpha$ an atom).
- $w \models \varphi_1 \land \varphi_2$ iff $w \models \varphi_1$ and $w \models \varphi_2$.
- $w \models \varphi_1 \lor \varphi_2$ iff $w \models \varphi_1$ or $w \models \varphi_2$.
- $w \models \varphi_1 \rightarrow \varphi_2$ iff for all $w' \in W$ such that $wRw'$, if $w' \models \varphi_1$ then $w' \models \varphi_2$.
- $w \models \neg \varphi$ iff for all $w' \in W$ such that $wRw'$, $w' \not\models \varphi$.
  (note, $\neg \varphi$ is $\varphi \rightarrow \bot$)

Alternatively: $w \models \varphi_1 \rightarrow \varphi_2$ iff
  for all $w' \in W$ such that $wRw'$, $w' \not\models \varphi_1$ or $w' \models \varphi_2$. 
A formula $\varphi$ is **satisfiable** if there exist a model $\mathcal{M} = (W, R, \vartheta)$ and a world $w \in W$ such that $w \models \varphi$.

A formula $\varphi$ is **valid** if for every model $\mathcal{M} = (W, R, \vartheta)$ and for every $w \in W$, $w \models \varphi$.

The concepts of **falsifiability** and **unsatisfiability** are defined dually (w.r.t, validity and satisfiability).
Persistency for all formulae

Lemma

In an intuitionistic Kripke model, for every formula \( \varphi \) and every \( u, v \in W \), if \( uRv \) then \( u \models \varphi \) implies \( v \models \varphi \)

Proof.

By induction on the structure of the formula \( \varphi \).

- For an atom \( \alpha \), this is the persistency condition of the intuitionistic Kripke model.
- For \( \varphi = \top \) or \( \varphi = \bot \) it follows directly from the definition.
- For \( \varphi = \varphi_1 \land \varphi_2 \) or \( \varphi = \varphi_1 \lor \varphi_2 \), it follows from the persistency of truth of \( \varphi_1 \) and/or \( \varphi_2 \).
- For \( \varphi = \varphi_1 \to \varphi_2 \) (and for \( \varphi = \neg \varphi_1 \), use \( \neg \varphi_1 = \varphi_1 \to \bot \)):
  assuming \( u \models \varphi \), to show \( v \models \varphi \), let \( w \) be given such that \( vRw \). Then \( uRw \) (by transitivity of a Kripke frame), so \( w \not\models \varphi_1 \) or \( w \models \varphi_2 \) (as \( u \models \varphi \)). As this holds for all \( w \) such that \( vRw \), we have \( v \models \varphi \).
Relation to classical logic

- The classical semantic (i.e., the truth table) is a degenerate form of intuitionistic semantic, i.e., with only one world.
- Every theorem of intuitionistic logic is also a theorem of classical logic.
- This gives us a simple (but incomplete) way of testing falsifiability of an intuitionistic formula $\varphi$:

  \[
  \text{If } \varphi \text{ is not valid classically, then it is not valid intuitionistically.}
  \]

- The converse, i.e., whether classical validity implies intuitionistic validity, is not true.
- Hint: if $\varphi$ is valid classically, but not intuitionistically, then to show it is not valid intuitionistically, you need to use a frame with more than one world, and the valuation function $\vartheta$ must not be the same on all worlds.
Example: a non-tautology

Consider the following formula (also called *Peirce’s law*):

\[ \varphi = ((P \rightarrow Q) \rightarrow P) \rightarrow P. \]

It is valid in classical logic, but not in intuitionistic logic.

Let \((W, R)\) be a Kripke frame consisting of two worlds (say, \(w_1\) and \(w_2\)),

\[
\begin{align*}
    v(w_1, P) &= f, \\
    v(w_2, P) &= t, \\
    v(w_1, Q) &= f, \\
    v(w_2, Q) &= f.
\end{align*}
\]

and let \(\mathcal{M} = (W, R, v)\).

1. From \(w_2 \models P\) and \(w_2 \not\models Q\), we have \(w_1 \not\models P \rightarrow Q\) and \(w_2 \not\models P \rightarrow Q\).
2. From \(w_1 \not\models (P \rightarrow Q)\) and \(w_2 \not\models (P \rightarrow Q)\), we have \(w_1 \not\models (P \rightarrow Q) \rightarrow P\).
3. From \(w_1 \models (P \rightarrow Q) \rightarrow P\) and \(w_1 \not\models P\), we have \(w_1 \not\models \varphi\).
Example: a valid formula

Show that $\varphi = P \rightarrow ((P \rightarrow Q) \rightarrow Q)$ is valid.

Proof.

By contradiction. Suppose $\varphi$ is falsifiable, i.e., there exists a model $\mathcal{M} = (W, R, \vartheta)$ and $w \in W$ such that

$$w \not\models P \rightarrow ((P \rightarrow Q) \rightarrow Q).$$

This means, there exists $u$, s.t. $wRu$ and $u \models P$ but $u \not\models (P \rightarrow Q) \rightarrow Q$. The latter means there exists $v$ such that $uRv$ and

\begin{align*}
(1) & \quad v \models P \rightarrow Q \\
(2) & \quad v \not\models Q.
\end{align*}

By the persistency condition, $v \models P$, and by reflexivity of $R$, $vRv$. These, together with (1), imply that $v \models Q$. But this contradicts (2). So $\varphi$ must be valid.