An Introduction to untyped λ-calculus, and the Church-Rosser Theorem

Will Troiani

August 2019

1 Introduction

The execution of a computation is a process of allowed transformations to a term in some language which either continues indefinitely or terminates after a finite number of steps. If termination occurs, then the term which is "left at the end" is special in that it is the term where the computation ended. For example,

$$1 + 2 + 3 \tag{1}$$

is not *computed* yet, as it may be transformed to

$$3 + 3$$

which can then be transformed to 6. Of course, there is another route of computation which could have been taken, performing the second addition of (1) first obtains $1 + 5$, which then yields 6. The property that there exists the term 6 which both computation paths $1 + 2 + 3 \to 3 + 3$ and $1 + 2 + 3 \to 1 + 5$ can be computed to is the property of *confluence* of natural number addition.

The goal of this note is to introduce a system of computation, the *untyped λ-calculus*, and prove the Church-Rosser theorem which states that the untyped λ-calculus is *confluent.*

2 The Untyped λ-Calculus

The untyped λ-calculus sits among a collection of *type theories* which have been used as a foundation for mathematics [7], a foundation for logic [1], (although it was later found to be inconsistent [2]), and a foundation of certain programming languages such as AGDA, Lisp, Haskell, Coq, COC, etc. The untyped λ-calculus is the simplest of these theories, and although is rarely used in its original form, is a good entry point to many of the important ideas concerning the more modern type theories.

The main reference for this section is [4, §3.3].

Definition 1. *Let $\mathscr{V}$ be a (countably) infinite set of variables, and let $\mathscr{L}$ be the language consisting of $\mathscr{V}$ along with the special symbols*

$$\lambda \qquad . \qquad (\qquad)$$

Let $\mathscr{L}^*$ be the set of words of $\mathscr{L}$, more precisely, an element $w \in \mathscr{L}^*$ is a finite sequence $(w_1, ..., w_n)$ where each w_i is in $\mathscr{L}$, for convenience, such an element will be written as $w_1...w_n$. Now let Λ_p denote the smallest subset of $\mathscr{L}^*$ such that

- *if $x \in \mathscr{V}$ then $x \in \Lambda_p$,*
- *if $M, N \in \Lambda_p$ then $(MN) \in \Lambda_p$,*
- *if $x \in \mathscr{V}$ and $M \in \Lambda_p$ then $(\lambda x.M) \in \Lambda_p$*

Λ_p is the set of ***preterms****. A preterm M such that $M \in \mathscr{V}$ is a* ***variable****, if $M = (M_1 M_2)$ for some preterms M_1, M_2, then M is an* ***application****, and if $M = (\lambda x, M')$ for some $x \in \mathscr{V}$ and $M' \in \Lambda_p$ then M is an* ***abstraction****.*

In practice, it becomes unwieldy to use this notation for the preterms exactly, and so the following notation is adopted:

Definition 2.

- *For preterms M_1, M_2, M_3, the preterm $M_1 M_2 M_3$ means $((M_1 M_2) M_3))$,*
- *For variables x, y and a preterm M, the preterm $\lambda xy.M$ means $(\lambda x.(\lambda y.M))$.*

The variables x which appear in the subpreterm M of a preterm $\lambda x.M$ are viewed as "markers for substitution", (see Remark 3). For this reason, a distinction is made between the variable x and the variable y in, for example, the preterm $\lambda x.xy$:

Definition 3. *Given a preterm M, let $FV(M)$ be the following set of variables, defined recursively*

- *if $M = x$ where x is a variable then $FV(M) = \{x\}$,*
- *if $M = M_1 M_2$ then $FV(M) = FV(M_1) \cup FV(M_2)$,*
- *if $M = \lambda x.M'$ then $FV(M) = FV(M') \setminus \{x\}$.*

A variable $x \in FV(M)$ is a ***free variable*** *of M, a variable x which appears in M but is not a free variable is a* ***bound variable****.*

As mentioned, bound variables will be viewed as "markers for substitution", so we define the following equivalence relation on Λ_p which relates a preterm M to M' if M can be obtained by replacing every bound occurrence of a variable x in M' with another variable y:

Definition 4. *For any term M, let $M[x := y]$ be the preterm given by replacing every bound occurrence of x in M with y. Define the following equivalence relation on Λ_p: $M \sim_\alpha M'$ if there exists $x, y \in \mathscr{V}$ such that $M[x := y] = M'$, where no free variable of M becomes bound in $M[x := y]$. In such a case, we say that M is **α-equivalent** to M'.*

Remark 1. *The reason why we need to let x and y be such that no free variable of M becomes bound in $M[x := y]$ is so that a preterm such as $\lambda x.y$ does not get identified with the preterm $\lambda y.y$.*

We are now in a position to define the underlying language of λ-calculus:

Definition 5. *Let $\Lambda = {}^{\Lambda_p}/_{\sim_\alpha}$ be the set of **λ-terms**. The set of **free variables** of a λ-term $[M]$ is $FV(M)$, which can be shown to be well defined. For convenience, M will be written instead of $[M]$.*

Now the dynamics of the computation of λ-terms will be defined.

Definition 6. ***Single step β-reduction** $\to_\beta$ is the smallest relation on Λ satisfying:*

- *the **reduction axiom**:*
  - *for all variables x and λ-terms M, M', $(\lambda x.M)M' \to_\beta M[x := M']$, where $M[x := M']$ is the term given by replacing every free occurrence of x in M with M',*
- *the following **compatibility axioms**:*
  - *if $M \to_\beta M'$ then $(MN) \to_\beta (M'N)$ and $(NM) \to_\beta (NM')$,*
  - *if $M \to_\beta M'$ then for any variable x, $\lambda x.M \to_\beta \lambda x M'$.*

*A subterm of the form $(\lambda x.M)M'$ is a **β-redex**, and $(\lambda x.M)M'$ **single step β-reduces** to M'.*

Remark 2. *Strictly, single step β reduction should be defined on preterms and then shown that a well defined relation is induced on terms, but this level of detail has been omitted for the sake of clarity.*

Remark 3. *The reducition axiom shows precisely in what sense a bound variable is a "marker for substitution". For example, $(\lambda x.x)M \to_\beta M$ and $(\lambda y.y)M \to_\beta M$, which is why $\lambda x.x$ is identified with $\lambda y.y$.*

It is through single step β-reduction that computation may be performed. In fact, λ-calculus is capable of performing natural number addition:

Example 1. *Define the following λ-terms:*

- *ONE* $:= \lambda fx.fx$,

- $TWO := \lambda fx.ffx$,
- $THREE := \lambda fx.fffx$,
- $PLUS := \lambda mnfx.mf(nfx)$

then

$$\begin{aligned}
PLUS\ ONE\ TWO &= (\lambda mnfx.\underline{m}f(nfx))\underline{(\lambda fx.fx)}(\lambda fx.ffx) \\
&\to_\beta (\lambda nfx.(\lambda fx.\underline{f}x)\underline{f}(nfx))(\lambda fx.ffx) \\
&\to_\beta (\lambda nfx.(\lambda x.f\underline{x})\underline{(nfx)})(\lambda fx.ffx) \\
&\to_\beta (\lambda nfx.f\underline{n}fx)\underline{(\lambda fx.ffx)} \\
&\to_\beta (\lambda fx.f(\lambda fx.\underline{f}\underline{f}x)\underline{f}x) \\
&\to_\beta (\lambda fx.f(\lambda x.ff\underline{x})\underline{x}) \\
&\to_\beta (\lambda fx.fffx) = THREE
\end{aligned}$$

where each step is obtained by substituting the right most underlined λ-term inplace of the left most underlined variable.

Historically, is this how Church first defined computable functions.

3 The Church-Rosser Theorem

Example 1 shows one possible sequence of β-reductions which reduces PLUS ONE TWO to THREE, however, different valid sequences exist. Moreover, no matter what path is taken, one can always find a path to THREE. The following theorem, which is the main point of this note, states that such a term always exists:

Definition 7. ***Multi step*** β***-reduction*** $\twoheadrightarrow$ *(or simply* β***-reduction****) is the smallest relation on* Λ *satisfying*

- *the* ***reduction axiom****:*
  - *if* $M \to_\beta M'$ *then* $M \twoheadrightarrow M'$,
- ***reflexivity****:*
  - *if* $M = M'$ *then* $M \twoheadrightarrow M'$,
- ***transitivity****:*
  - *if* $M_1 \twoheadrightarrow M_2$ *and* $M_2 \twoheadrightarrow M_3$ *then* $M_1 \twoheadrightarrow M_3$

If $M \twoheadrightarrow M'$*, then* M ***multistep*** β***-reduces*** *to* M'.

Theorem 1 (The Church Rosser Theorem)**.** *If $M_1 \twoheadrightarrow M_2$ and $M_1 \twoheadrightarrow M_3$ then there exists a term M_4 such that the diagram*

$$\begin{array}{ccc} M_1 & \twoheadrightarrow & M_2 \\ \downarrow\!\!\!\downarrow & & \downarrow\!\!\!\downarrow \\ M_3 & \twoheadrightarrow & M_4 \end{array}$$

commutes. That is, multi step β reduction is ***confluent****.*

Proof. The proof will proceed by introducing a new relation $\Rightarrow$ on Λ which satisfies the following:

- if $M \to_\beta M'$ then $M \Rightarrow M'$,
- if $M \Rightarrow M'$ then $M \twoheadrightarrow M'$,
- if $M_1 \Rightarrow M_2$ and $M_1 \Rightarrow M_3$ then there exists $M_4 \in \Lambda$ which makes the following diagram commute

$$\begin{array}{ccc} M_1 & \Longrightarrow & M_2 \\ \Downarrow & & \Downarrow \\ M_3 & \Longrightarrow & M_4 \end{array}$$

This is sufficient as if $M_1 = M^{11}, ..., M^{1m}$ and $M_1 = M^{11}, ..., M^{n1}$ are sequences of λ-terms such that

$$M^{11} \to_\beta M^{12} \to_\beta \ldots \to_\beta M^{1m}$$

and

$$M^{11} \to_\beta M^{21} \to_\beta \ldots \to_\beta M^{n1}$$

then the diagram

$$\begin{array}{ccccccc} M_1 = M^{11} & \Longrightarrow & M^{12} & \Longrightarrow & \ldots & \Longrightarrow & M^{1m} = M_2 \\ \Downarrow & & & & & & \\ M^{21} & & & & & & \\ \Downarrow & & & & & & \\ \vdots & & & & & & \\ \Downarrow & & & & & & \\ M_3 = M^{n1} & & & & & & \end{array}$$

can be completed to the following commuting diagram

$$\begin{array}{ccccccc}
M_1 = M^{11} & \Longrightarrow & M^{12} & \Longrightarrow & \dots & \Longrightarrow & M^{1m} = M_2 \\
\Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\
M^{21} & \Longrightarrow & M^{22} & \Longrightarrow & \dots & \Longrightarrow & M^{2m} \\
\Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\
\vdots & \Longrightarrow & \vdots & \Longrightarrow & \ddots & \Longrightarrow & \vdots \\
\Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\
M_3 = M^{n1} & \Longrightarrow & M^{n2} & \Longrightarrow & \dots & \Longrightarrow & M^{nm}
\end{array}$$

from which it follows that M^{nm} satisfies the required properties of M_4.

Towards this end, define the following relation on Λ:

Definition 8. ***Parallel*** β ***reduction*** $\Rightarrow$ *is the smallest relation on* Λ *satisfying*

- *the* ***reduction axiom****:*
  - *if* $M \Rightarrow M'$ *and* $N \Rightarrow N'$ *then* $(\lambda x.M)N \Rightarrow M'[x := N']$*,*
- ***reflexivity****:*
  - *if* $M = M'$ *then* $M \Rightarrow M'$*,*
- *the following* ***compatibility axioms****:*
  - *if* $M \Rightarrow M'$ *and* $N \Rightarrow N'$ *then* $(MN) \Rightarrow (M'N')$*,*
  - *if* $M \Rightarrow M'$ *then* $\lambda x.M \Rightarrow \lambda x.M'$*.*

Remark 4. *β-reduction might introduce new β-redexes which are not "visible" in the original term. For example*

$$(\lambda x.xxx)(\lambda x.x) \twoheadrightarrow (\lambda x.x)(\lambda x.x)(\lambda x.x)$$

By transitivity, $(\lambda x.xxx)(\lambda x.x) \twoheadrightarrow \lambda x.x$. However, parallel β-reduction is not transitive, so $(\lambda x.xxx)(\lambda x.x) \not\Rightarrow \lambda x.x$. So $M \Rightarrow N$ only if N is obtained from M by reducing a collection of the β redexes in M and not ones which are introduced by this reduction process.

Clearly, if $M \to_\beta M'$ then $M \Rightarrow M'$ and if $M \Rightarrow M'$ then $M \twoheadrightarrow M'$. It remains to show that parallel β reduction is confluent.

First, we claim that if $M_1 \Rightarrow M_2$ and $N_1 \Rightarrow N_2$ then $M_1[x := N_1] \Rightarrow M_2[x := N_2]$. To prove this claim, we proceed by inducting on the "minimum number of usages of the axioms of parallel β reduction required to prove that $M_1 \Rightarrow M_2$". More precisely, let

$$S_0 := \{(M, M) \mid M \in \Lambda\}$$

and for $i > 0$, let S_i be the smallest set such that

- $S_{i-1} \subseteq S_i$,
- if $(M_1, M_2), (N_1, N_2) \in S_{i-1}$ then $((M_1 N_1), (M_2 N_2)) \in S_i$,
- if $(M, N) \in S_{i-1}$ then $(\lambda x.M, \lambda x.N) \in S_i$,
- if $(M_1, M_2), (N_1, N_2) \in S_{i-1}$ then $((\lambda x.M_1)N_1, N_2[x := M_2]) \in S_i$

Clearly, $M \Rightarrow N$ if and only if $(M, N) \in S := \cup_{i=0}^{\infty} S_i$. Define the following function:

$$\begin{aligned} \varphi : S &\to \mathbb{N} \\ (M, N) &\mapsto \min\{i \in \mathbb{N} \mid (M, N) \in S_i\} \end{aligned}$$

we proceed by (strong) induction on $\varphi(M_1, M_2)$. If $\varphi(M_1, M_2) = 0$ then $M_1 = M_2$ from which it follows that $M_1[x := N_1] \Rightarrow M_2[x := N_2]$. Say the result holds true for $\varphi(M_1, M_2) < k$. Then there are three cases, corresponding to M_1 being a variable, an application, or an abstraction (see Definition 1). If M_1 is a variable, then $\varphi(M_1, M_2) = 0$ and we have reduced to the base case. If $M_1 = \lambda y.M_1'$ then $M_1 \Rightarrow M_2$ implies that $M_2 = \lambda x.M_2'$. By the inductive hypothesis $M_1'[x := N_1] \Rightarrow M_2'[x := N_2]$ which implies

$$\begin{aligned} \lambda y.(M_1'[x := N_1]) &\Rightarrow \lambda y.(M_2'[x := N_2]) \\ \text{so, } (\lambda y.M_1')[x := N_1] &\Rightarrow (\lambda y.M_2')[x := N_2] \\ \text{so, } M_1[x := N_1] &\Rightarrow M_2[x := N_2] \end{aligned}$$

Lastly, say $M_1 = (M_1^1 M_1^2)$. Then either M_1^1 is an abstraction or it is not. If it is not then the proof is similar to the case where M_1 is an abstraction. Say $M_1^1 = (\lambda x.M_1^{1'})$. Now, either $M_2 = (\lambda x.M_2^{1'})M_2^2$, in which case the proof is similar to the case when M_1 is an abstraction, or $M_2 = M_2^{1'}[x := M_2^2]$. In this case, by the inductive hypothesis we have

$$M_1^{1'}[x = N_1] \Rightarrow M_2^{1'}[x = N_2]$$

and

$$M_1^2[x = N_1] \Rightarrow M_2^2[x = N_2]$$

from which it follows that

$$(\lambda x.M_1^{1'}[x := N_1])(M_1^2[x := N_1]) \Rightarrow (\lambda x.M_2^{1'}[x := N_2])(M_2^2[x := N_2])$$

which implies

$$M_1[x := N_1] = \big((\lambda x.M_1^{1'})M_1^2\big)[x := N_1] \Rightarrow \big((\lambda x.M_2^{1'})M_2^2\big)[x := N_2] = M_2[x := N_2]$$

which establishes the claim.

To finish the proof, say $M_1 \Rightarrow M_2$ and $M_1 \Rightarrow M_3$, we will show that there exists an appropriate term M_4 by induction on $l(M_1)$, the length of M_1. This is broken up into cases in a similar way to the proof of the claim above, the only non-trivial case is when

$$M_1 = (\lambda x.M_1^{1'})M_1^2, \qquad M_2 = M_2^{1'}[x := M_2^2], \qquad M_3 = M_3^{1'}[x := M_3^2]$$

By the inductive hypothesis, there exists $M_4^{1'}$ and M_4^2 such that the diagrams

$$\begin{array}{ccc} M_1^{1'} & \Longrightarrow & M_2^{1'} \\ \Downarrow & & \Downarrow \\ M_3^{1'} & \Longrightarrow & M_4^{1'} \end{array} \qquad \begin{array}{ccc} M_1^{2} & \Longrightarrow & M_2^{2} \\ \Downarrow & & \Downarrow \\ M_3^{2} & \Longrightarrow & M_4^{2} \end{array}$$

both commute. Now, by the claim proved above,

$$M_2^{1'}[x := M_2^2] \Rightarrow M_4^{1'}[x := M_4^2] \qquad M_3^{1'}[x := M_3^2] \Rightarrow M_4^{1'}[x := M_4^2]$$

and so,

$$(\lambda x.M_2^{1'})M_2^2 \Rightarrow (\lambda x.M_4^{1'})M_4^2 \qquad (\lambda x.M_3^{1'})M_3^2 \Rightarrow (\lambda x.M_4^{1'})M_4^2$$

ie, the diagram

$$\begin{array}{ccc} M_1 & \Longrightarrow & M_2 \\ \Downarrow & & \Downarrow \\ M_3 & \Longrightarrow & M_4 \end{array}$$

commutes, as required. $\square$

References

[1] A. Church, *An Unsolvable Problem of Elementary Number Theory*, American Journal of Mathematics, Vol. 58, No. 2. (Apr., 1936), pp. 345-363.

[2] A. Church, *A Set of Postulates for the Foundation of Logic* Annals of Mathematics Second Series, Vol. 33, No. 2 (Apr., 1932), pp. 346-366

[3] A. Church, *A Set of Postulates for the Foundation of Logic (Second Paper)*, Annals of Mathematics Vol. 34, No. 4 (Oct., 1933), pp. 839-864

[4] M. Sørensen, P. Urzyczyn, *Lectures on the Curry-Howard Isomorphism*, Studies in Logic and the Foundations of Mathematics, 4th July 2006.

[5] A. Turing, [Delivered to the Society November 1936], "On Computable Numbers, with an Application to the Entscheidungsproblem" (PDF), Proceedings of the London Mathematical Society, 2, 42, pp. 230–65, doi:10.1112/plms/s2-42.1.230 and Turing, A.M. (1938). "On Computable Numbers, with an Application to the Entscheidungsproblem: A correction". Proceedings of the London Mathematical Society. 2. 43 (published 1937). pp. 544–6, 1937

[6] K. Gödel "On Undecidable Propositions of Formal Mathematical Systems". In Davis, Martin (ed.). The Undecidable. Kleene and Rosser (lecture note-takers); Institute for Advanced Study (lecture sponsor). New York: Raven Press, 1934.

[7] J. Lambek, P.J. Scott, *Introduction to Higher Order Categorical Logic*, Cambridge University Press, New York, 1986.