CS704: Lecture 6
The Church-Rosser Theorem

Thomas Reps

[Based on lecture of Feb. 1, 2010]

Abstract

This lecture presents the Church-Rosser Theorem (i.e., $\longrightarrow_{\alpha,\beta}$ is confluent).

1 Motivation

λ-calculus along with the encodings for basic data-types (Booleans, natural numbers, pairs, etc.) and the fixed-point combinators looks a lot like a functional programming language. Answers are normal-form terms—i.e., terms that contain no β-redexes. However, from an operational perspective, we would be in trouble if either of the following problems were to arise:

1. There is a term that has *multiple* normal forms (i.e., ones that are not α-congruent). If this were the case, which normal-form term would the system report as the answer?
2. There was not clear strategy for *finding* a normal form, given a term X that has a normal form.

However, both of the following are consequences of the Church-Rosser Theorem (CRT):

1. Normal forms are unique up to α-congruence).
2. It is sufficient to start from X and just perform *reductions* (i.e., there is never a need to guess a β-expansion step).

Items 1 and 2, together with the fact that the leftmost-outermost reduction strategy always finds a normal form if one exists, establish λ-calculus as a viable computational model (including from the operational perspective).

Remark. Leftmost-outermost (or "normal-order reduction") is just one possible reduction strategy. One can talk about a strategy S being better than strategy T:

- S always arrives at a normal-form term whenever T does, and
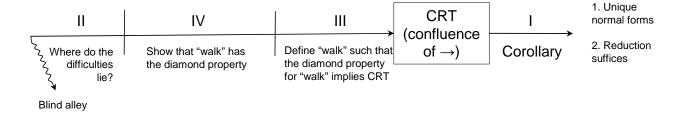- S never requires more steps than T does.

$\square$

2 Roadmap

In this lecture, we prove the Church-Rosser Theorem.

Theorem 2.1 (Church-Rosser Theorem [1]) $\longrightarrow_{\alpha,\beta}^{*}$ *has the diamond property: For all* X_0, X_1*, and* X_2 *such that* $X_0 \longrightarrow_{\alpha,\beta}^{*} X_1$ *and* $X_0 \longrightarrow_{\alpha,\beta}^{*} X_2$*, there exists* X_3 *such that* $X_1 \longrightarrow_{\alpha,\beta}^{*} X_3$ *and* $X_2 \longrightarrow_{\alpha,\beta}^{*} X_3$. $\square$

Thm. 2.1 can also be stated as "$\longrightarrow_{\alpha,\beta}$ is confluent."

Our presentation follows the proof in [1], but does not follow a linear order. Instead, it tackles the topics in the order I–IV, as shown in the diagram below:

Throughout, we use several similar notions that are related to equality and reduction:

Notation	Concept
$A \simeq B$	α-congruence
$A = B$	equality
A has a normal form B	$A = B$ and B has no β-redex
$A \longrightarrow_\alpha B$	α-reduction
$A \longrightarrow_\beta B$	β-reduction
$A \longleftarrow B$	β-expansion
$A \longrightarrow^* B$	A reduces to B
$A \Longrightarrow B$	like $A \longrightarrow^* B$, but there exists a sequence of reduction steps with a special property

(Note that "$A \longrightarrow^* B$" is denoted by "A red B" in [1].)

3 Consequences of the Church-Rosser Theorem

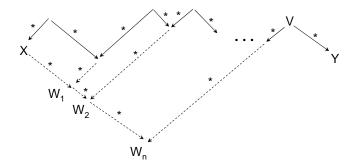(This section discusses item I from the "Roadmap Diagram".)

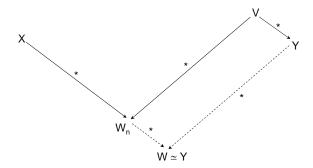**Corollary 3.1** *If X has a normal form Y, then*
1. *$X \longrightarrow^* Y$*
2. *Y is unique (up to α-congruence)*

□

Proof:

Proof of Part 1. The proof is by induction on the number of alternations of β-expansions and β-reductions used to transform X to Y. We will do a "proof by diagram":

By CRT, there exist W_1, W_2, ..., W_n as shown in the diagram above. Because $X \longrightarrow^* W_n$ by transitivity of $\longrightarrow^*$, we need only consider a "Z-like" diagram involving X, W_n, V, and Y, as shown below:

By CRT, there exists W such that $W_n \longrightarrow^* W$ and $Y \longrightarrow^* W$. However, Y is in normal form, so the transformation of Y to W can involve only α-steps. Consequently $W \simeq Y$.
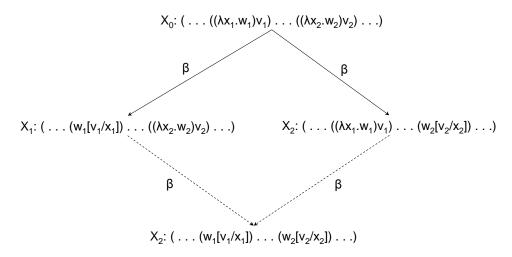
Because $X \longrightarrow^* W_n \longrightarrow^* W \simeq Y$, $X \longrightarrow^* Y$ as was to be shown.

Proof of Part 2. Suppose that Y and Z are both normal forms of X. By Part 1, $X \longrightarrow^* Y$ and $X \longrightarrow^* Z$. However, this means that Z has a normal form Y, so $Z \longrightarrow^* Y$. Because Z is a normal-form term, the reduction sequence that transforms Z to Y can involve only α-steps, and consequently $Z \simeq Y$.
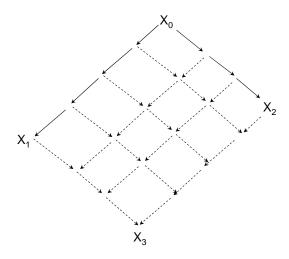
4 Where Do the Difficulties Lie? (II)

(This section discusses item II from the "Roadmap Diagram".)
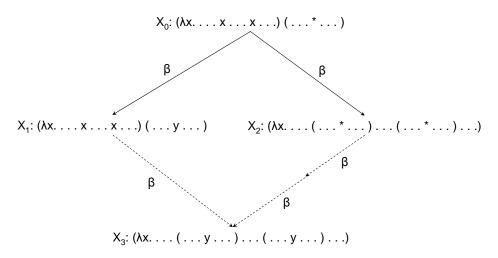
Let's examine some minimal cases, such as the term X_0 shown below:

The diamond-like shape is encouraging because it suggests that we can show the CRT by a tiling proof, as shown below:

However, this does not work because of examples like the following one (where "*" denotes a β-redex that β-reduces to y). In particular, the difficulty is that it takes *two* β-reduction steps to transform X_2 to X_3.

X_0: $(\lambda x. \ldots x \ldots x \ldots)(\ldots * \ldots)$

β β

X_1: $(\lambda x. \ldots x \ldots x \ldots)(\ldots y \ldots)$ X_2: $(\lambda x. \ldots (\ldots * \ldots) \ldots (\ldots * \ldots) \ldots)$

β β

β

X_3: $(\lambda x. \ldots (\ldots y \ldots) \ldots (\ldots y \ldots) \ldots)$

The diagram above shows that $\longrightarrow_{\alpha,\beta}$ does not have the diamond property.

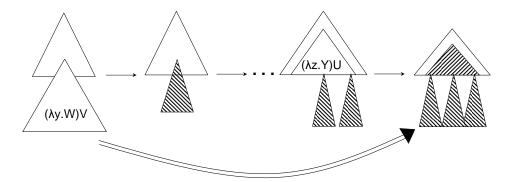## 5 Introducing "$\Longrightarrow$"

(This section discusses item III from the "Roadmap Diagram".)

Our approach to obtaining a proof of the CRT will be to identify some relation other than $\longrightarrow_{\alpha,\beta}$ or $\longrightarrow^*_{\alpha,\beta}$ that (i) has the diamond property, and (ii) implies the diamond property of $\longrightarrow^*_{\alpha,\beta}$.

Remark. The final diagram in §4 suggests that $\longrightarrow_{\alpha,\beta}$ might be weakly confluent. However, it would not help to know that $\longrightarrow_{\alpha,\beta}$ is weakly confluent because, as we saw on the first homework problem, one can have a relation that is weakly confluent but not confluent. That is, weak confluence does not imply confluence, so establishing that $\longrightarrow_{\alpha,\beta}$ is weakly confluent does not provide a way to prove the CRT. □
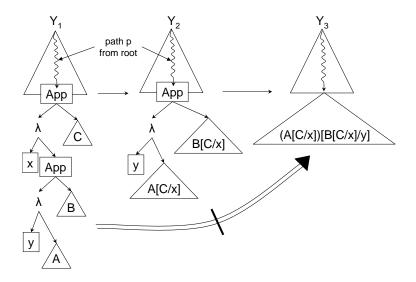
Definition 5.1 (Walk Relation on λ-Terms.) *We say that A walk B holds iff there is a sequence of 0 or more $\longrightarrow_{\alpha,\beta}$ steps that (i) transforms A to B, and (ii) the sequence of β-reduction steps are performed bottom-up. "A walk B" is denoted by $A \Longrightarrow B$.*

A reduction-sequence that demonstrates that $A \Longrightarrow B$ holds is called a walk-sequence. □

Pictorially, a walk looks something like the following, where at each step the shaded regions are off-limits for additional β-reductions:

The following diagram tries to show more about what it means for a sub-term to be off-limits in a walk sequence. In particular, the sequence $[Y_1, Y_2, Y_3]$ shown below is not a walk. (In fact, the relation $Y_1 \implies Y_3$ does hold; however, it justified by a different sequence from the one shown below.)

One way to formalize the notion of "off-limits" is in terms of *director-strings*, such as "LRRLLR", which represent how to navigate down from the root of a tree to a particular node (e.g., see path p in Y_1 and Y_2). At each stage in the walk, there is a set OffLimits $= \{p_1, p_2, \ldots, p_n\}$. Initially, OffLimits $= \emptyset$. A β-reduction is permitted at position p if for all $1 \leq i \leq |\text{OffLimits}|$, p_i is not a prefix of p.[1] Because the off-limits subtrees can change position relative to the root during a β-reduction, the set OffLimits should be updated as follows with each β-reduction:

$$\text{OffLimits} := (\text{OffLimits} - \{p_i \in \text{OffLimits} \mid p \text{ is a prefix of } p_i\}) \cup \{p\}. \qquad (1)$$

The director-strings $\{p_i \in \text{OffLimits} \mid p \text{ is a prefix of } p_i\}$ can be removed from OffLimits in Eqn. (1) because the director-string p added to OffLimits serves to block all β-reductions at or below the position specified by p.

---

[1]A director-string is considered to be a prefix of itself. Thus, the set of prefixes of LRRLLR is $\{\epsilon, \text{L}, \text{LR}, \text{LRR},$ LRRL, LRRLL, LRRLLR$\}$.
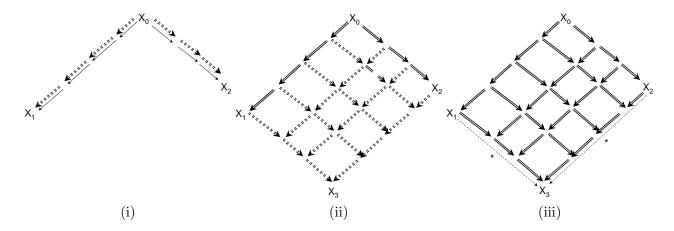
Observation 5.2 *Given two reduction-sequences S_1 and S_2 such that (i) each qualify as walk-sequences, and (ii) the last term of S_1 is the first term of S_2, their concatenation $S_1 || S_2$ does not necessarily qualify as a walk sequence.* □

In several places in the proof given in §6, we need to construct a walk-sequence by concatenating two known walk-sequences. The consequence of Obs. 5.2 is that at each such point in the proof, we will need to argue that the walk-sequences can, indeed, be concatenated to form a valid walk-sequence.

The Idea Behind the Proof. The idea behind the introduction of $\Longrightarrow$ is that it provides extra structure that allows a modified "tiling" argument to be pushed through. In particular, $\Longrightarrow$ has three properties:

1. If $X \longrightarrow Y$, then $X \Longrightarrow Y$.
2. If $X \Longrightarrow Y$, then $X \longrightarrow^* Y$. Moreover, if $X \Longrightarrow^* Z$, then $X \longrightarrow^* Z$.
3. As will be shown in §6, $\Longrightarrow$ has the diamond property.

Assuming that $\Longrightarrow$ has the diamond property (which will be demonstrated in §6), the proof of the CRT is an inductive tiling argument that follows the diagrams given below, where in each step the solid arrows are assumed and the dashed arrows are deduced:

(i)   (ii)   (iii)

The argument goes as follows:

(i) Using property 1 above, each individual reduction step of the reduction sequences $X_0 \longrightarrow^* X_1$ and $X_0 \longrightarrow^* X_2$ is identified as a walk (consisting of a single α-step or β-step).

(ii) Using property 3 above, the diamond property is repeatedly applied to tile the graph and to identify λ-term X_3.

(iii) Using property 2 above, the sequences of walk steps along the southwest and southeast edges are each identified as reduction sequences ($\longrightarrow^*$).

Consequently, there exists a λ-term X_3 such that $X_1 \longrightarrow^* X_3$ and $X_2 \longrightarrow^* X_3$, as was to be shown.

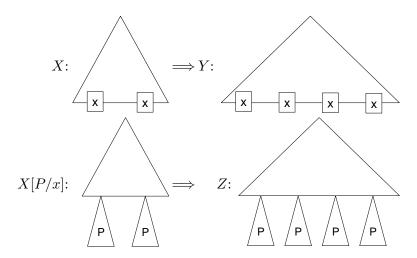# 6 $\Longrightarrow$ has the Diamond Property

(This section discusses item IV from the "Roadmap Diagram".)

What remains to be shown is that $\Longrightarrow$ has the Diamond Property. At certain points, the proof given by Rosser [1] gets caught up in the minutiae of α-reductions. However, if one uses the De Bruijn representation of λ-terms, we never perform α-reductions. Thus, whenever I want to finesse a point involving α-reductions in Rosser's proof, I merely have to appeal to the De Bruijn representation, and the problem disappears.

We will also use the following lemma:

Lemma 6.1 (Walks and Substitutions) *If $X \Longrightarrow Y$ then $X[P/x] \Longrightarrow Z$, where $Z \simeq Y[P/x]$.*
□

Sketch of Proof: The idea behind the proof is captured in the following diagram:
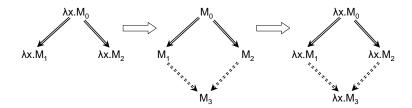

In essence, the Ps move around just like the xs as you do the same steps of the walk-sequence that justifies $X \Longrightarrow Y$.

Lemma 6.2 *The $\Longrightarrow$ relation has the diamond property: For all X_0, X_1, and X_2 such that $X_0 \Longrightarrow X_1$ and $X_0 \Longrightarrow X_2$, there exists X_3 such that $X_1 \Longrightarrow X_3$ and $X_2 \Longrightarrow X_3$.* □

Proof: The proof is by induction on the size of the term X_0 (at the apex of the diamond). In particular, we are permitted to assume that the property holds for all diamonds whose apex is a proper subterm of X_0. The proof is structured according to the operator at the root of X_0.

Case 1: X_0 is a variable. The proposition is immediate because both $X_0 \Longrightarrow X_1$ and $X_0 \Longrightarrow X_2$ must be empty walks. Therefore, $X_1 \equiv X_0 \equiv X_2$ and we can choose $X_3 \stackrel{\text{def}}{=} X_0$.

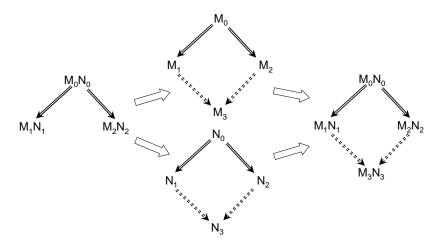**Case 2:** X_0 is of the form $\lambda x.M_0$. The argument follows the following diagram:

X_1 must be of the form $\lambda x.M_1$; similarly, X_2 must be of the form $\lambda x.M_2$. Moreover, we have $M_0 \Longrightarrow M_1$ and $M_0 \Longrightarrow M_2$.[2] M_0 is a proper subterm of X_0; thus, by the induction hypothesis there is an M_3 such that $M_1 \Longrightarrow M_3$ and $M_2 \Longrightarrow M_3$.

We choose $X_3 \stackrel{\text{def}}{=} \lambda x.M_3$ and transform the walk-sequences that justify $M_1 \Longrightarrow M_3$ and $M_2 \Longrightarrow M_3$ into ones that justify $X_1 \Longrightarrow X_3$ and $X_2 \Longrightarrow X_3$, respectively.

---

[2]For instance, to create the director-strings for a walk-sequence that justifies $M_0 \Longrightarrow M_1$, we merely have to remove the first letter from each director-string S in the walk-sequence that justifies $\lambda x.M_0 \Longrightarrow \lambda x.M_1$. The first letter of S is always "R" to move into the body of a λ-abstraction at the root; however, in each term in the walk sequence that justifies $M_0 \Longrightarrow M_1$, the outermost λ-abstraction has been stripped off.

Case 3: X_0 is of the form $(M_0 N_0)$. The proof splits into four sub-cases.

Case 3.1: Assume that there was no β-reduction performed at the root in either $X_0 \Longrightarrow X_1$ or $X_0 \Longrightarrow X_2$. The argument follows the following diagram:
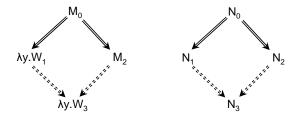

Because there is an application at the root of each of X_0, X_1, and X_2, and no β-reduction was performed at the root, it must be that (i) $M_0 \Longrightarrow M_1$ and $M_0 \Longrightarrow M_2$, and (ii) $N_0 \Longrightarrow N_1$ and $N_0 \Longrightarrow N_2$. M_0 and N_0 are both proper subterms of X_0; thus, by the induction hypothesis there exist (i) M_3 such that $M_1 \Longrightarrow M_3$ and $M_2 \Longrightarrow M_3$, and (ii) N_3 such that $N_1 \Longrightarrow N_3$ and $N_2 \Longrightarrow N_3$.

We choose $X_3 \stackrel{\text{def}}{=} (M_3 N_3)$ and, by adjusting director-strings appropriately, can use the walk-sequences that justify (a) $M_1 \Longrightarrow M_3$ and $N_1 \Longrightarrow N_3$, and (b) $M_2 \Longrightarrow M_3$ and $N_2 \Longrightarrow N_3$ to create walk-sequences that justify (a) $X_1 \equiv (M_1 N_1) \Longrightarrow (M_3 N_3) \equiv X_3$, and (b) $X_2 \equiv (M_2 N_2) \Longrightarrow (M_3 N_3) \equiv X_3$, respectively.

Case 3.2: Assume that there was a β-reduction performed at the root in $X_0 \Longrightarrow X_1$, but there was no β-reduction performed at the root in $X_0 \Longrightarrow X_2$. Because of the constraint on the order of β-reductions in walk-sequences, the fact that $X_0 \Longrightarrow X_1$ involves a β-reduction at the root means that the β-reduction at the root was the *last* β-reduction in the walk. In particular, $X_0 \Longrightarrow X_1$ can be decomposed as follows:

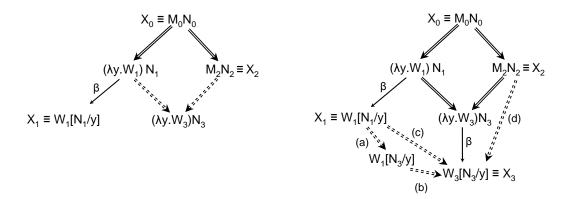$$X_0 \Longrightarrow (\lambda y.W_1)N_1 \longrightarrow_\beta X_1.$$

M_0 and N_0 are both proper subterms of X_0; thus, by the induction hypothesis we have the situation depicted below:

(i) From $M_0 \Longrightarrow \lambda y.W_1$ and $M_0 \Longrightarrow M_2$, we deduce the existence of a term $\lambda y.W_3$ such that $\lambda y.W_1 \Longrightarrow \lambda y.W_3$ and $M_2 \Longrightarrow \lambda y.W_3$.

(ii) From $N_0 \Longrightarrow N_1$ and $N_0 \Longrightarrow N_2$, we deduce the existence of a term N_3 such that $N_1 \Longrightarrow N_3$ and $N_2 \Longrightarrow N_3$.

Moreover, similar to the situation that arose in Case 2, from $\lambda y.W_1 \Longrightarrow \lambda y.W_3$ we can deduce that $W_1 \Longrightarrow W_3$ holds.

The remainder of the proof follows the two diagrams shown below:

As indicated on the left, we can construct walk-sequences $(\lambda y.W_1)N_1 \Longrightarrow (\lambda y.W_3)N_3$ and $M_2N_2 \Longrightarrow (\lambda y.W_3)N_3$.
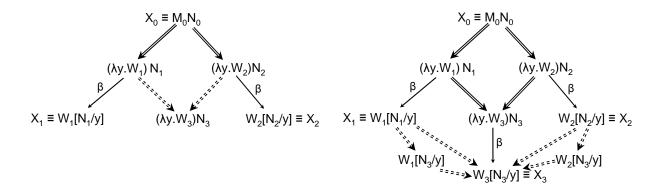
As indicated on the right, we choose X_3 to be the term $W_3[N_3/y]$ (obtained from $(\lambda y.W_3)N_3$ by a β-reduction). The remaining observations concern the existence of the walks labeled (a), (b), (c), and (d) in the right-hand diagram above.

(a) From $N_1 \Longrightarrow N_3$ we can construct a walk-sequence that justifies $W_1[N_1/y] \Longrightarrow W_1[N_3/y]$. ($W_1[N_1/y]$ may have many copies of N_1, but they occur in disjoint parts of the term—hence their walk-sequences can be interleaved in any order to construct a walk-sequence that justifies $W_1[N_1/y] \Longrightarrow W_1[N_3/y]$.)

(b) Earlier, we observed that $W_1 \Longrightarrow W_3$. Consequently, by Lem. 6.1, $W_1[N_3/y] \Longrightarrow W_3[N_3/y]$.

(c) Because the β-reductions in the walk-sequence that justifies $W_1[N_1/y] \Longrightarrow W_1[N_3/y]$ are entirely in the "N_1-parts", and the β-reductions in the walk-sequence that justifies $W_1[N_3/y] \Longrightarrow W_3[N_3/y]$ are entirely in the "W_1-parts", we can concatenate the two walk-sequences to create a walk-sequence that justifies $W_1[N_1/y] \Longrightarrow W_3[N_3/y]$.

(d) The walk-sequence that justifies $M_2N_2 \Longrightarrow (\lambda y.W_3)N_3$ has no β-reduction at the root. Consequently, we can extend the walk-sequence with $(\lambda y.W_3)N_3 \longrightarrow_\beta W_3[N_3/y]$ to create a walk-sequence that justifies $M_2N_2 \Longrightarrow W_3[N_3/y]$.

Case 3.3: Symmetric to Case 3.2.

Case 3.4: Assume that there was a β-reduction performed at the root in both $X_0 \Longrightarrow X_1$ and $X_0 \Longrightarrow X_2$.

The proof is similar to that of Case 3.2: the argument used to justify $X_1 \Longrightarrow W_3[N_3/y]$ in Case 3.2 are now used to justify both $X_1 \Longrightarrow W_3[N_3/y]$ and symmetrically $X_2 \Longrightarrow W_3[N_3/y]$, as indicated by the diagram below:

□

References

[1] J.B. Rosser. Highlights of the history of the lambda-calculus. *Annals of the History of Computing*, 6(4):337–349, October 1984.