Henk Barendregt

A SIMPLE PROOF OF THE CHURCH-ROSSER THEOREM.

Recd. 1975

By Martin Hyland,

Mathematical Institute,

24-29 St. Giles,

Oxford.

0. Introduction.

This paper sketches a new and simple proof of the Church-Rosser Theorem for the λ-calculus. The proof is more in the spirit of Curry-Feys [1], than of the recent proofs of Tait and Martin-Löf (see e.g. [2]). That is to say, it aims at proving Theorem 3.6 (Curry's Lemma of parallel moves), from which the Church-Rosser Theorem is a triviality. However our proof is far more direct than his, and takes into account that what has to be proved is a type of result familiar in Proof Theory, namely a Strong Normalization result.

The reader is assumed to be familiar with the basic syntax and terminology of the λ-calculus. We shall deal solely with (α- and) β-reduction. α-reduction is a matter of logical hygiene, and we shall disregard it. We adopt the following conventions: M, M', N etc. shall denote arbitrary terms of the λ-calculus; A, B, .. etc., either arbitrary terms, or arbitrary subterms of M, N etc. according to context; by a redex, we shall mean a β-redex, and R, R', S, etc shall denote arbitrary sets of subredexes of M, M'; C(D/x) shall denote the result of substituting D for all free occurences of the variable x in C. If A is a subredex of M, we shall write $M \xrightarrow{A} M'$, for M' is the result of reducing A in M. $M \rightarrow M'$ means $M \xrightarrow{A} M'$ for some A, and the relation $\succ$ is the transitive closure of $\rightarrow$. $\succcurlyeq$ is the usual relation of reduction.

1. The method of proof.

We say a relation $\succ$ between terms of the λ-calculus has the diamond property, if whenever $M \succ M_1$ and $M \succ M_2$, then there is an N such that $M_1 \succ N$ and $M_2 \succ N$. The Church-Rosser Theorem says that $\succ$ has the diamond property. If a relation has the diamond property, then so has its transitive closure; but unfortunately $\rightarrow$ does not have the diamond property. Thus the mechanism of proof of the Church-Rosser Theorem is to define a relation $\succcurlyeq_1$ such that (a) one can show relatively easily that $\succcurlyeq_1$ has the diamond property, and (b) $\succcurlyeq$ is the transitive closure of $\succcurlyeq_1$.

There appears to be just one relation $\succcurlyeq_1$ which satifies (a) and (b). The difference between our approach and that in [2], is that our problem is to show that our definition of $\succcurlyeq_1$ makes sense, while in [2], the problem is to show that $\succcurlyeq_1$ has the diamond property.

2. Ancestors and descendants.

Given any sequence, $M_0 \xrightarrow{A_1} M_1 \xrightarrow{A_2} M_2 \dots \xrightarrow{A_n} M_n$, of reductions, we will associate any subterm B of M_n, a unique subterm of M, called its ancestor in M. If for the sequences $M_i \xrightarrow{A_{i+1}} M_{i+1}$, B_{i+1} has ancestor B_i in M_i, then for the sequence, $M_0 \xrightarrow{A_1} M_1 \xrightarrow{A_2} M_2 \dots \xrightarrow{A_n} M_n$, B_n has ancestor B_0 in M_0. It remains, therefore, to say what the ancestor of a subterm E of N is, for the sequence $M \xrightarrow{A} N$. Say that A is $(\lambda x.C)D$, so $C(D/x)$ is a subterm of N; then there are four cases:

1) $C(D/x)$ is a subterm of E. Then there is a unique F, a subterm of M such that $F \xrightarrow{A} E$; this F is the ancestor of E, unless E is $C(D/x)$, when case 4) applies.

2) E is disjoint from $C(D/x)$. Then there is a corresponding subterm E, of M, and this subterm of M is the ancestor of E.

3) E is a subterm of some substitution instance of D in $C(D/x)$. Then the ancestor of E, is just E as a subterm of D, a subterm of M.

4) E is of the form $F(D/x)$, where F is not x, and is a subterm of C; this F is the ancestor of E.

Given any sequence, $M_0 \xrightarrow{A_1} M_1 \xrightarrow{A_2} M_2 \dots \xrightarrow{A_n} M_n$, of reductions we associate with any subterm A of M_0, a (possibly empty) set of descendants, which shall be subterms of M_n, as follows. B is a descendant of A if and only if A is the ancestor of B. Observe that in $M \xrightarrow{A} N$, A has no descendants.

The concept of a descendant is central to what follows. A more formal definitiion than that above could be given, but would be less illuminating.

3. The 'strong normalization' property.

For this section we adopt the following conventions; M is a term of the λ-calculus; R is a set of subredexes of M; $A \in R$; $M \xrightarrow{A} M'$; R' is the set of descendants of elements of R; C, D are subterms of M, and C', D' are arbitrary descendants of C, D, respectively, in M'.

We define a partial order $<_R$ on subterms of M, by,

1) If D is a proper subterm of C, then $C <_R D$;

2) Otherwise, there is a unique subterm (EF) of M, with, say, C a subterm of E, and D a subterm of F. If (EF) is $(\lambda z.E')F$, a member of R, and z is free in C (being bound by the λz of $(\lambda z.E')$), then $C <_R D$;

3) If $C <_R D$ and $D <_R E$, then $C <_R E$.

We call any reduction sequence, starting with M, which procedes by reducing only descendants of elements of R, a <u>reduction of M relative to R</u>. Then the effect of our definition of $<_R$ is this: $C <_R D$ if and only if some descendant of D becomes a subterm of a descendant of C during a reduction of M relative to R.

<u>Lemma 3.1</u>. $C' <_{R'} D'$ only if $C <_R D$. (C', D', R' are descendants w.r.t. ONE contraction in R.)

Proof: It is sufficient to show the required implication in the cases,

1) $C' <_{R'} D'$ in virtue of condition 1) above. Then either D was a proper subterm of C, or D was substituted in for some variable free in C; i.e. $C <_R D$ holds by either 1) or 2).

2) $C' <_{R'} D'$ in virtue of condition 2) above. Then $(\lambda z.E')F'$ is in R', z is free in C' a subterm of E', and D' is a subterm of F'. Then $(\lambda z.E)F$ is in R, with E, F, the ancestors of E', F'. Then either z is free in C a subterm of E, and D is a subterm of F, or D has been substituted infor a free variable of F to give D'; i.e. either $C <_R D$ by 2), or $C <_R F$ by 2) and $F <_R D$ by 2) so that by 3) $C <_R D$. (Note that C could not have been substituted into E to give C', as then z could not be free in C').

For C in R, set $d(C) = \max\{d(B) \mid B \text{ is in } R \text{ and } B <_R C\} + 1$. Now define an eventually zero function u_R by $u_R(k) = \text{card}(\{C \mid C \text{ is in } R \text{ and } d(C) = k\})$. For such functions, define $u < v$ if and only if the greatest i such that $u(i) \neq v(i)$, is such that $u(i) < v(i)$. (Here i, k, denote integers and $\text{card}(X)$ is the cardinality of X).

<u>Lemma 3.2</u>. $<$ is a well-ordering of eventually zero functions.

Proof: Routine.

Lemma 3.3. $u_{R'} < u_R$.

Proof: We reduce A. If not $A <_R B$, then B has just one descendant, and $d(B) = d'(B')$. If $A <_R B$, then B has more than one descendant only if B is a proper subterm of A; for such B, since A has no descendant, we get $d'(B') < d(B)$, by induction on $<_R$ for subterms of A. For other B with $A <_R B$, we get $d'(B') \leq d(B)$. If k is the greatest $d(B)$ such that $d'(B') < d(B)$, or is $d(A)$ if there are none, then k is the greatest i such that $u_{R'}(i) \neq u_R(i)$, and $u_{R'}(k) < u_R(k)$. Hence $u_{R'} < u_R$.

Theorem 3.4. Any reduction of M relative to R must terminate.

Proof: Immediate from (3.2) and (3.3).

We call a reduction of M relative to R which terminates (i.e. the final term, N, of the reduction sequence has no descendants of elements of R as subterms), complete. (3.4) says that however we reduce M relative to R, eventually we come to such an N, that is , eventually we have performed a complete reduction.

Hence forth, we will often use the obvious fact that if the elements of a set T, of subredexes of M are disjoint, then there is a unique N such that M completely reduces to N, relative to T.

For the next lemma we adopt the following further conventions; $S \subseteq R$ is such that any two distinct members of S are incomparable with respect to $<_R$; S' is the set of descendants of elements of S in M'; let M completely reduce to M_S relative to S; T is the set of descendants of A in M_S. (3.1) shows that if B,C are distinct members of S', then they are incomparable with respect to $<_{R'}$.

Lemma 3.5. Inthe above situation, there is a unique N such that M' and M_S completely reduce to N, relative to S' and T, respectively.

Proof: There are three cases.

1) A is disjoint from all the elements of S, and the result is plain.

2) A is a subterm of $C \in S$. Let $M \xrightarrow{C} M_1$, and an inspection of cases shows that there is a unique N_1, such that $M' \xrightarrow{C'} N_1$, and M_1 reduces to N_1, relative to the descendants of A in M_1. Then in M_1, the descendants of elements of $S \cup \{A\}$ are disjoint, so there is a unique N terminating any complete reduction of M_1 relative to that set. But then, M_S reduces to N relative to T, while N_1 reduces to N relative to the descendants of elements of S, i.e. M' reduces to N relative to S'.

3) $C_1 \ldots C_r \in S$ are (disjoint) subterms of A. Let $M \xrightarrow{C_1} M_1 \ldots \xrightarrow{C_r} M_r$, and let A_i be the

(only) descendant of A in M_i. Let $M_i \xrightarrow{A_i} N_i$. Again, an inspection of cases shows that M' reduces to N_1 relative to the descendants of C_1, and so by induction, M' reduces to N_r relative to the descendants of $\{C_1 \ldots C_r\}$. Now in M_r, the descendants of $S \cup \{A\}$ are disjoint, and we procede as in case 2).

We are now in a position to prove our strong normalization property for reductions of M relative to R.

Theorem 3.6. Any reduction of M relative to R terminates; and all complete reductions terminate in the same N.

Proof: By (3.4), it is sufficient to show that given a complete reduction of M to N relative to R, then there is a complete reduction of M' to N relative to R' (recall the conventions introduced at the beginning of this section). Let the complete reduction be $M=M_0 \xrightarrow{A_1} M_1 \ldots \xrightarrow{A_n} M_n=N$. For each i, let R_i be the set of descendants of elements of R and S_i the set of descendants of A, in M_i. Then M_i, R_i, S_i, A_{i+1}, are in exactly the position of M, R,S, A, in (3.5), so applying (3.5) we obtain : let N_i be the result of completely reducing M_i relative to S_i; then each N_i completely reduces to N_{i+1} relative to the descendants of A_{i+1} in N_i. Since plainly N_n is N, we now have a complete reduction of M' to N relative to R'.

4. The Church-Rosser Theorem.

Let $M \geqslant_1 N$ if and only if N is the unique result of completely reducing M relative to some set R of subredexes of M. Section 3 established that this is a sensible definition.

Theorem 4.1. $\geqslant_1$ has the diamond property.

Proof: Suppose M completely reduces to M_1, M_2, relative to R_1, R_2, respectively; let N be the result of completely reducing M relative to $R_1 \cup R_2$; then by (3.6), M_1, M_2, completely reduce to N relative to the descendants of elements of R_2, R_1, respectively.

Theorem 4.2. (Church-Rosser) $\geqslant$ has the diamond property.

Proof: This is immediate on (4.1), as $\geqslant$ is the transitive closure of $\geqslant_1$.

References:

[1] Curry, H.B. and Feys, R. Combinatory Logic I (North-Holland 1958)

[2] Hindley, J.R. , Lercher, B. and Seldin, J.P. Introduction to Combinatory Logic (L.M.S. lecture Note Series 7, CUP 1972)