Computations in Orthogonal Rewriting Systems, I

Gérard Huet and Jean-Jacques Lévy

We present in this chapter a study of derivations which formalize the computations of expressions in programming languages. Our formalism extends recursive programs with simplifications in [16, 20, 6, 27, 23, 25, 8, 2]. It permits to provide an operational semantics to programming languages such as LISP [19], LUCID [1], HOPE [5], and ML [9]. The derivations we study may also be considered as proofs in certain equational theories which are of use to study abstract data types [11, 22, 6]. Finally, our work may be used for the design of efficient simplifications in formula manipulation systems such as LCF [10].

The results of this paper may be sketched as follows: We consider finite systems of pairs of first-order terms: \( \Sigma = \{ \alpha_i \rightarrow \beta_i \mid i \leq n \} \). Computations consist of rewriting an occurrence of some instance of an \( \alpha_i \) into the corresponding instance of \( \beta_i \). We restrict every rule \( \alpha_i \rightarrow \beta_i \) so that all variables of \( \beta_i \) occur in \( \alpha_i \) and so that every variable of \( \alpha_i \) has a unique occurrence in \( \beta_i \). Furthermore, no two rules of \( \Sigma \) are nontrivially superposable. We believe that most computations in programming languages without parallelism can be formalized in this setting.

Section 1 contains the preliminary definitions. In section 2 we show how the parallel moves lemma induces a congruence ("permutation") on derivations issued from a given term. The usual notion of residuals of a redex is extended to derivations, yielding a sup-semilattice structure to the permutation classes of derivations. This generalizes Church-Rosser results from [26, 13, 24].

In section 3 we prove what is usually called the standardization theorem. The problem is to simulate any derivation by a "standard" derivation, i.e., one which computes in an outside-in way. For this we define the notion of a redex occurrence being external for a given derivation. Intuitively, an external redex is such that none of its residuals will be below any redex contracted in any permutation of the given derivation. This notion is thus invariant by permutation, and every nonempty derivation possesses at least one external redex occurrence. This allows us to define the notion of a standard derivation, and we show that every derivation class contains a unique standard derivation. We finally define the notion of a redex occurrence being external in a given term, which yields the notion of the normal derivation issued from a given term. When the term possesses a normal form, the normal derivation terminates in this normal form. This may be considered as an extension to our systems of the call by name computation rule for recursive program schemas, and of the normal derivations in \( \lambda \)-calculus. However, our formalism differs in essential ways from these two, because of the possibility of upward creation of redexes, and our call by name rule does not correspond to a simple leftmost-outermost strategy of computation. The results imply that all the nonambiguous linear term rewriting systems are d-outer in the sense of O'Donnell [24]. The existence of normal derivations entails the possibility of doing only needed computations in a top-down manner. However, it does not correspond to an effective computation rule, and at this stage the only correct effective interpreters use parallel strategies such as parallel outermost.
Part II of this paper (chapter 12) will deal with the problem of finding effective interpreters which compute in a sequential fashion.

Most of our concepts are adaptations to syntactic domains of denotational semantics notions. This algebraic approach permits us to state and prove our theorems in an abstract fashion, suggesting that our results can be extended to a more general theory of operational semantics.

1 Preliminary Definitions

We follow here the notations of Huet [13] and Berry-Lévy [2]. Let \( \mathcal{F} \) be a set of function symbols of arity \( n \), \( \mathcal{F} = \bigcup \{ \mathcal{F}_n \mid n \geq 0 \} \), and \( \mathcal{V} \) a denumerable set of variable symbols. Our expression language is the set \( \mathcal{M}(\mathcal{F}, \mathcal{V}) \) of first-order terms formed from \( \mathcal{F} \) and \( \mathcal{V} \), i.e.,

\[
\mathcal{V} \subseteq \mathcal{M}(\mathcal{F}, \mathcal{V}),
\]

\[
F \in \mathcal{F}_n \& \forall i \leq n \quad M_i \in \mathcal{M}(\mathcal{F}, \mathcal{V}) \Rightarrow F(M_1, M_2, \ldots, M_n) \in \mathcal{M}(\mathcal{F}, \mathcal{V})
\]

When \( \mathcal{F} \) and \( \mathcal{V} \) are fixed from the context, we shall usually denote \( \mathcal{M}(\mathcal{F}, \mathcal{V}) \) by \( \mathcal{M} \).

For any term \( M \) we define its set of occurrences \( \partial(M) \) as a finite subset of the set \( \mathbb{N}^* \) of finite sequences of positive integers as follows:

\[
\Lambda \in \partial(M) \quad (the \text{ empty occurrence})
\]

\[
u \in \partial(M) \Rightarrow \nu i \in \partial(F(M_1, M_2, \ldots, M_n)) \quad \text{for} \quad 1 \leq i \leq n
\]

Intuitively, an occurrence of \( M \) names a subterm of \( M \) by its access path. If \( \nu \in \partial(M) \), we define the subterm of \( M \) at \( u \) as the term \( M/\nu \), defined inductively by

\[
M/\Lambda = M,
\]

\[
F(M_1, M_2, \ldots, M_n)/\nu u = M_i/\nu.
\]

Finally, if \( \nu \in \partial(M) \), we define for every term \( N \) the replacement in \( M \) at \( u \) by \( N \) as the term \( M[\nu \leftarrow N] \), defined by

\[
M[\Lambda \leftarrow N] = M,
\]

\[
F(M_1, M_2, \ldots, M_n)[\nu \leftarrow N] = F(M_1, M_2, \ldots, M_i[\nu \leftarrow N], \ldots, M_n).
\]

We shall also use the notation \( \bar{\partial}(M) = \{ \nu \in \partial(M) \mid M/\nu \notin \mathcal{V} \} \).

Example Let \( M = F(G(x), A) \) We have \( \partial(M) = \{ \Lambda, 1, 1, 1, 2 \} \) and \( \bar{\partial}(M) = \{ \Lambda, 1, 2 \} \), \( M/1 = G(x) \), and \( M[1 \leftarrow H(B)] = F(H(B), A) \).

The set of occurrences \( \partial(M) \) is partially ordered by the prefix ordering \( u \leq v \) iff \( \exists w : uw = v \). In this case we shall define \( \nu u \) as \( w \). If \( u \not\leq v \) and \( v \not\leq u \), we say that \( u \) and \( v \) are disjoint, and write \( u|v \). Finally, \( u < v \) iff \( u \leq v \) and \( u \neq v \).
A substitution is any function $\sigma$ from $\mathcal{T}$ to $\mathcal{T}$ satisfying

$$\sigma(F(M_1, M_2, \ldots, M_n)) = F(\sigma(M_1), \sigma(M_2), \ldots, \sigma(M_n))$$

In other words, $\sigma$ is a morphism in the algebra of terms and is therefore uniquely determined from its value on variables.

We call term rewriting system (abbreviated TRS) any set $\Sigma$ of pairs of terms $a_i \rightarrow b_i$ such that $\forall_i b_i \subseteq \forall_i (a_i)$, where $\forall_i (M)$ is the set of variables appearing in $M$. We denote by $\text{red}_\Sigma$ the set of left-hand sides $a_i$ of $\Sigma$, which we call redex schemes. For any substitution $\sigma$ and $a \in \text{red}_\Sigma$, $\sigma(a)$ is called a redex of $\Sigma$. We denote by $\mathcal{P}_\Sigma(M)$ the set of redex occurrences in the term $M$. A term $M$ such that $\mathcal{P}_\Sigma(M) = \emptyset$ is called a $\Sigma$-normal form. We denote by $\mathcal{N}_\Sigma$ the set of terms in $\Sigma$-normal form. From now on, we shall assume that TRS $\Sigma$ is fixed and therefore drop the subscript $\Sigma$ except when needed.

We say that the term $M$ reduces to $N$ at occurrence $u$ using rule $a_k \rightarrow b_k$ if there exists a substitution $\sigma$ such that $M/u = \sigma(a_k)$ and $N = M[u \leftarrow \sigma(b_k)]$. The pair $A = \langle M, u \rangle$ is called an elementary derivation, and we shall write $A: M \rightarrow_N N$. In this notation, $k, u$ or $A$ may be omitted. Note that $M, u$ and $k$ determine unambiguously $\sigma(x)$ for every $x$ in $\forall_i (a_k)$, and therefore $\sigma(b_k)$ and $N$.

A derivation is a sequence $A = A_1 A_2 \ldots A_n$ of elementary derivations $A_i: M_i \rightarrow M_{i+1}$. We use $AB$ for the concatenation of $A$ and $B$, $0$ for the empty derivation, and $|A|$ for the length of derivation $A$. We shall use the notation $A: M \rightarrow^* N$ to indicate that derivation $A$ starts in $M$ and ends in $N$.

Let $U = \{u_1, u_2, \ldots, u_n\}$ be a set of mutually disjoint redex occurrences in term $M$, and let $M/u_i = \sigma(a_i)$. We call elementary multiderivation the pair $A = \langle M, U \rangle$ and write $A: M \rightarrow_U N$, where

$$N = M[u_1 \leftarrow \sigma_1(b_1)] u_2 \leftarrow \sigma_2(b_2)] \ldots [u_n \leftarrow \sigma_n(b_n)]$$

(Of course, the order of the $u_i$'s is irrelevant.) We say that $A$ contracts the set $U$.

We define multiderivations in the same way and use the same notation as for derivations. Furthermore, if we want to emphasize the system $\Sigma$ we use, we can write $M \rightarrow^*_\Sigma N$. We denote $\mathcal{D}(M)$ the set of multiderivations issued from $M$, and $\mathcal{F}(A)$ the final term reached by the (multi)derivation $A$. We say that $A$ and $B$ are coinital if $A, B \in \mathcal{D}(M)$, cofinal if $\mathcal{F}(A) = \mathcal{F}(B)$. The notation $AB$, for the concatenation of $A$ and $B$, assumes that $B \in \mathcal{D}(\mathcal{F}(A))$. Concatenation being associative, we write $ABC$ for $ABG$ or $A(B)C$. Every set $\mathcal{D}(M)$ contains an empty multiderivation which we shall denote $0$, the term $M$ being usually understood from the context. Thus we freely write $A0 = 0A = A$.

When considering a derivation $A: M_0 \rightarrow^* M_1 \rightarrow^* M_2 \rightarrow^* \ldots \rightarrow^* M_n$, it is convenient to denote by $A[i]$ the $i$ first steps of $A$, with $0 \leq i \leq n$. The rest of $A$ is denoted $A[i, n]$. Thus $A = A[i] A[i, n]$, with $M_i$ as the final term of $A[i]$. Similarly for multiderivations.

We shall study in this paper the properties of derivations in TRSs which have two constraints:
1) Left linearity: for every $\alpha$ in red, every variable of $\alpha$ occurs only once:

$$\alpha/u = \alpha/v \in \mathcal{V} \Rightarrow u = v$$

2) Nonambiguity: if $\alpha_i, \alpha_j \in \text{red}$, for every $u$ in $\overline{\mathcal{O}}(\alpha_i)$ there are no $\sigma, \sigma'$ such that $\sigma(\alpha_i/u) = \sigma'(\alpha_j)$, except in the trivial case $i = j$ and $u = \Lambda$

We also rule out the trivial TRSs which only consist of rules $\alpha \to \beta$ with $\alpha \in \mathcal{V}$

Therefore, we have $\text{red} \cap \mathcal{V} = \emptyset$ by condition (2)

**Definition 1.1** We call orthogonal any non-trivial TRS verifying conditions 1 and 2 above.

Our TRSs are similar to the schematic tree replacement systems of Rosen [26] and O'Donnell [24]. Condition 2 is called the nonoverlapping condition in these papers. Note that 1 and 2 imply together that our systems are outer, in the terminology of [24]. In the terminology of Knuth-Bendix [17], there is no critical pair. The derivation relation $\to$ is confluent (has the Church-Rosser property) [13, 26]. We shall study in this paper some stronger properties of derivation spaces, generalizing results in Berry-Lévy [2] obtained for recursive equations.

## 2 The Derivations Space

In this section we prove an important property of derivations in TRSs, the parallel moves lemma (see Curry & Feys [7]). This allows us to define a partial ordering on derivations, inducing a semi-lattice property on derivation spaces. This useful tool generalizes the one defined in Berry-Lévy [2], which can also be defined in the $\lambda$-calculus (Lévy [18])

**Definition 2.1** Given an elementary derivation $A: M \xrightarrow{\alpha} N$ and $v \in \mathcal{R}(M)$, we define the set $v \setminus A$ of residuals of $v$ by $A$ as a subset of $\mathcal{O}(N)$ as follows:

$$v \setminus A = \begin{cases} \emptyset & \text{if } v = u, \\ \{v\} & \text{if } v|u \text{ or } v < u, \\ \{uw_1v_1 \beta_k/w_2 = x\} & \text{if } v = uwv_1 \text{ and } \alpha_k/w = x \in \mathcal{V}. \end{cases}$$

A pictorial explanation of residuals is given in figure 1. Note that all the relative positions of $u$ and $v$ have been considered because of nonambiguity. Furthermore, nonambiguity and left linearity imply that $v \setminus A \subseteq \mathcal{R}(N)$. Finally, for every $w$ in $\mathcal{R}(N)$, there is at most one $v$ such that $w \in v \setminus A$ When there is none, we say that $w$ is created by $A$. Note that such $w$s may be above $u$, as well as in the substituted right-hand side $\beta_k$.

**Example** Let $\Sigma = \{F(G(x)) \to H(x, K(x)), F(H(x, y)) \to x, K(A) \to B, C \to A\}$

We consider

$$A: M_0 = F(F(H(G(C), C))) \xrightarrow{(1)} M_1 = F(G(C)) \xrightarrow{(A)} M_2 = H(C, K(C)) \xrightarrow{1,2,1} M_3 = H(A, K(A)) \xrightarrow{(2)} H(A, B).$$
The redex occurrence 1 1 1 of $M_0$ has one residual in $M_2$, namely 1.1, and two residuals in $M_2$, namely 1 and 2.1. It has no further residuals after the second step of $A$, which reduces these two redexes. The redex occurrence 1 1 2 of $M_0$ has no residual in $M_1$. The redex occurrence 2 of $M_1$ is created (upward) by redex occurrence 2.1 of $M_2$. Finally, note that the redex occurrence $A$ of $M_2$ is created by the first step of $A$, even though the replacing term does not contribute to its redex, since it is a variable.

For any nonelementary derivation $A$, we define $v \setminus A$ by

$$v \setminus 0 = \{v\},$$

$$v \setminus (AB) = \{w \setminus B \mid w \in v \setminus A\}$$

The residual mapping is extended to sets of redex occurrences by defining

$$U \setminus A = \bigcup \{u \setminus A \mid u \in U\}.$$  

Finally, if $A$ is an elementary multiderivation $A : M \xrightarrow{U} N$ with $U = \{u_1, u_2, \ldots, u_n\}$, we define $v \setminus A$ as $v \setminus (A_1 A_2 \ldots A_n)$, where $A_i : M_{i-1} \xrightarrow{u_i} M_i$, $M_0 = M$ and $M_n = N$. Of course, $v \setminus A$ is independent of the order of the $u_i$'s. We extend $v \setminus A$ to nonelementary multiderivations and to sets of redex occurrences as above.

Let $A, B \in \mathcal{D}(M)$, with $|B| = 1$, contracting the set $U \subseteq \mathcal{R}(M)$. We define the residual $B \setminus A$ of $B$ by $A$ as the elementary derivation in $\mathcal{D}(\mathcal{F}(A))$, contracting the set $U \setminus A$. We also define $A \sqcup B = A(B \setminus A)$.

**Lemma 2.2: The Parallel Moves Lemma.** Let $A, B \in \mathcal{D}(M)$, with $|A| = |B| = 1$. Then $\mathcal{F}(A \sqcup B) = \mathcal{F}(B \sqcup A)$, and for all $u \in \mathcal{R}(M)$ we have $u \setminus (A \sqcup B) = u \setminus (B \sqcup A)$.

**Proof** Similar to the proof of Theorem 6.5 in [23], Lemma 11 in [17], Lemma 2.16 in [3].

The parallel moves lemma is illustrated in Figure 2.
COROLLARY: THE CHURCH-ROSSER PROPERTY  Since \(|B \setminus A| = |A \setminus B| = 1\), lemma 2.2 shows that the multiderivation relation is strongly confluent (see [13]) and therefore that the relation \(\rightarrow\) is confluent. Therefore, for every \(M\), there is at most one normal form \(N\) such that \(M \Downarrow N\).

The parallel moves lemma permits us to generalize the residual relation to arbitrary derivations, as follows.

**DEFINITION 2.3** Let \(A, B \in \mathcal{D}(M)\), with \(|B| = 1\). We define \(A \setminus B \in \mathcal{D}(\mathcal{F}(B))\) by induction on \(|A|\):

\[
0 \setminus B = 0 \tag{1}
\]

\[
(A_1 A_2) \setminus B = (A_1 \setminus B)(A_2 \setminus (B \setminus A_1)) \quad \text{with} \quad |A_1| = 1. \tag{2}
\]

Note that \(A_2 \setminus (B \setminus A_1)\) is defined by induction, since \(|B \setminus A_1| = 1\), and that it can be concatenated to \(A_1 \setminus B\), by the preceding lemma. Now for \(A, B \in \mathcal{D}(M)\) of arbitrary lengths, we define \(A \setminus B \in \mathcal{D}(\mathcal{F}(B))\) by induction on \(|B|\):

\[
A \setminus 0 = A \tag{3}
\]

\[
A \setminus (B_1 B_2) = (A \setminus B_1) \setminus B_2 \quad \text{with} \quad |B_1| = 1 \tag{4}
\]

We also extend the notation \(A \sqcup B = A(B \setminus A)\) to derivations of any length. It is easy to show by induction that \(|A \setminus B| = |A|\), that equations (1) through (4) are valid without length conditions, and to generalize the parallel moves lemma:

**LEMMA 2.4: THE GENERALIZED PARALLEL MOVES LEMMA** For all \(A, B \in \mathcal{D}(M)\) we have \(\mathcal{F}(A \sqcup B) = \mathcal{F}(\mathcal{F}(A \sqcup A))\) and for all \(u \in \mathcal{D}(M), u \setminus (A \sqcup B) = u \setminus (B \sqcup A)\)

The last part of lemma 2.4 can be generalized to an arbitrary multiderivation coinitial with \(A\) and \(B\) as follows.

**LEMMA 2.5: THE CUBE LEMMA** For all \(A, B, C \in \mathcal{D}(M)\) we have \(C \setminus (A \sqcup B) = C \setminus (B \sqcup A)\).

**Proof** By induction on \(|A| + |B| + |C|\). If \(C = 0\), use (1); otherwise, let \(C = C_1 C_2\) with \(|C_2| = 1\). We get

\[
(A \sqcup B) \setminus C_1 = (A \setminus C_1)((B \setminus A) \setminus (C_1 \setminus A)) \quad \text{by (2)}
\]

\[
= (A \setminus C_1)(B \setminus A \sqcup C_1)) \quad \text{by (4)}
\]
\[(A \backslash C_1)(B \backslash (C_1 \sqcup A)) \quad \text{by ind hyp}
\]
\[= (A \backslash C_1)((B \backslash C_1) \backslash (A \backslash C_1)) \quad \text{by (4)}
\]
\[= (A \backslash C_1) \sqcup (B \backslash C_1)
\]

Thus
\[C_2 \backslash ((A \sqcup B) \backslash C_1) = C_2 \backslash ((A \backslash C_1) \sqcup (B \backslash C_1))
\]
\[= C_2 \backslash ((B \backslash C_1) \sqcup (A \backslash C_1)) \quad \text{by lemma 2.4}
\]
\[= C_2 \backslash ((B \sqcup A) \backslash C_1) \quad \text{symmetrically}
\]

Finally, \(C_1 \backslash (A \sqcup B) = C_1 \backslash (B \sqcup A)\) by the induction hypothesis, which achieves the proof, using (2). \(\blacksquare\)

The cube lemma is illustrated in figure 3.

If we now define, for \(A, B \in D(M)\), \(A \equiv B\) iff for all \(C \in D(M)\), \(C \backslash A = C \backslash B\), we get the following corollary:

**Corollary** \(\forall A, B \in D(M), A \sqcup B \equiv B \sqcup A\)

We shall call \(\equiv\) permutation equivalence.

**Lemma 2.6:** \(\sqcup\) is associative \(\forall A, B, C \in D(M), (A \sqcup B) \sqcup C = A \sqcup (B \sqcup C)\)

**Proof**
\[(A \sqcup B) \sqcup C = (A \sqcup B)(C \backslash (A \sqcup B))
\]
\[= (A \sqcup B)(C \backslash (B \sqcup A)) \quad \text{by lemma 2.5}
\]
\[= A(B \backslash A)((C \backslash B) \backslash (A \backslash B)) \quad \text{by (4)}
\]
\[= A((B \sqcup C) \backslash A) \quad \text{by (2)}
\]
\[= A \sqcup (B \sqcup C) \quad \blacksquare
\]

The empty multiderivation 0 in \(D(M)\) should not be confused with the elementary multiderivation starting from \(M\) and contracting an empty set of redex occurrences, which we shall denote \(\emptyset\). In particular, \(|\emptyset| = 1\). However, it follows from the definition of residual that for every \(A \in D(M)\) we have \(\emptyset \backslash A = \emptyset\). By an easy induction on \(|A|\) we get that \(A \backslash \emptyset = A\), and thus \(0 \equiv \emptyset\), and also that \(A \backslash A = \emptyset^n\), with \(n = |A|\). This and lemma 2.4 easily imply that if \(A \equiv B\), then \(\mathcal{F}(A) = \mathcal{F}(B)\).
LEMMA 2.7: $\equiv$ is a congruence. Let $A, B \in \mathcal{D}(M)$, with $A \equiv B$. We have

\begin{align*}
&\forall C \in \mathcal{D}(M), A \setminus C \equiv B \setminus C \\
&\forall C \in \mathcal{D}(M), A \sqcup C \equiv B \sqcup C \\
&\forall C \in \mathcal{D}(\mathcal{F}(A)), AC \equiv BC \\
&\forall C \text{ such that } \mathcal{F}(C) = M, CA \equiv CB.
\end{align*}

**Proof** Easy consequences of the definitions.

**Corollaries** $\forall A \in \mathcal{D}(M), A \setminus A \equiv 0$. $\forall A \in \mathcal{D}(M), A \sqcup A \equiv A$.

We now define a relation $\sqsubseteq$ between coinitial multiderivations as follows:

$\forall A, B \in \mathcal{D}(M), A \sqsubseteq B \text{ iff } A \sqcup B \equiv B$

**Theorem 2.8: Lattice of Derivations Theorem** $\langle \mathcal{D}(M)/\equiv, \sqsubseteq, \sqcup \rangle$ is an upper semi-lattice.

**Proof** Easy algebraic manipulations from the preceding lemmas.

Phrased in categorical terms, this result means that the category whose objects are terms and whose morphisms are the equivalence classes of derivations admits pushout.

Caution! The lattice structure given by the parallel moves theorem is on derivations and not on terms. For instance, if we consider the system $R$ consisting solely of the rules $I(x) \rightarrow x$ and $J(x) \rightarrow x$, figure 4 shows that the terms $I(J(K))$ and $J(I(K))$ do not possess a least upper bound. Note that this phenomenon may be traced to the existence of two non-equivalent derivations between $I(I(K))$ and $I(K)$. This shows that the categorical viewpoint is the right one here: we need to talk in terms of arrows, not just relations between terms. And now the confluence diagrams can be replaced by more informative commuting diagrams expressing permutation equivalences of derivations. For instance, in figure 4 certain sub-diagrams are confluent only for unimportant syntactic coincidences (due to the double occurrence of $I$ in $I(I(I(K))))$, but the others are commuting diagrams expressing a strong equivalence of computations.

Using all that precedes, it is easy to prove the following relations (with the appropriate conditions on initial and final terms of the following derivations):

\begin{align*}
(AB) \setminus A & \equiv B \quad (5) \\
(CA) \setminus (CB) & \equiv A \setminus B \quad (6)
\end{align*}
Commutations in Orthogonal Rewriting Systems, I

\[ A \sqsubseteq B \text{ if } A \setminus B = \emptyset^m, \text{ with } m = |A| \]  \hspace{1cm} (7)

\[ A \equiv B \text{ if } A \sqsubseteq B \sqsubseteq A \]  \hspace{1cm} (8)

\[ A \equiv \emptyset \text{ if } A = \emptyset^n \text{ for some } n \geq 0 \]  \hspace{1cm} (9)

\[ A \sqsubseteq B \text{ if } AC \equiv B \text{ for some } C \]  \hspace{1cm} (10)

\[ A \sqsubseteq B \text{ implies } A \setminus C \sqsubseteq B \setminus C \]  \hspace{1cm} (11)

\[ A \sqsubseteq B \text{ implies } CA \sqsubseteq CB \]  \hspace{1cm} (12)

Note that (7) and (8) show that \( \sqsubseteq \) and \( \equiv \) are easily decidable.

We could also have defined \( \equiv \) as the smallest congruence relation on \( \emptyset(M) \)

such that \( \emptyset \equiv 0 \) and \( A \sqcup B \equiv B \sqcup A \). This justifies our terminology of permutation equivalence.

Finally, we may extend relations \( \sqsubseteq \) and \( \equiv \) to derivations by confusing the derivation

\[ M_0 \overset{u_1}{\rightarrow} M_1 \overset{u_2}{\rightarrow} M_2 \overset{u_3}{\rightarrow} \cdots \overset{u_n}{\rightarrow} M_n \]

with the multiderivation

\[ M_0 \overset{U_1}{\rightarrow} M_1 \overset{U_2}{\rightarrow} \cdots \overset{U_n}{\rightarrow} M_n, \]

where \( \forall i \leq n, U_i = \{u_i\} \).

3 Standardization, Call by Name, Call by Need

We are going to show in this section that every derivation is equivalent by permutations to a certain derivation computing redexes in an outside-in manner. In analogy to what happens for recursive definitions or \( \lambda \)-calculus, we shall call these special derivations standard. However, it should be remarked that, unlike in these two formalisms, the leftmost outermost derivations are usually not standard in TRS. For instance, consider

\[ \Sigma = \{F(x, A) \rightarrow B, C \rightarrow C, D \rightarrow A\}. \]

The standard derivation starting from the term \( F(C, D) \) and ending in its normal form is

\[ F(C, D) \rightarrow F(C, A) \rightarrow B, \]

whereas the leftmost outermost rule leads to the infinite derivation

\[ F(C, D) \rightarrow F(C, D) \rightarrow \cdots \]

3.1 Outside-In and Standard Computations

Let us first give some preliminary definitions and technical lemmas.
DEFINITION 3.1 Let $u \in \mathcal{R}(M)$, $x$ the redex scheme at $u$ in $M$. We define the contractum in $M$ at $u$ as the set $C_M(u)$ of occurrences of $M$ that are inside $x$:

$$C_M(u) = \{uv \in \mathcal{O}(M) | \exists v \in \mathcal{O}(x)\}$$

We also define

$$C_M(u) = \{uv \in \mathcal{O}(M) | \exists v \notin \mathcal{O}(x)\}$$

Note that $u \in C_M(u)$, since $x \notin \mathcal{V}$, and thus $\forall v \in \overline{C_M(u)}, u \prec v$.

Let $u, v \in \mathcal{R}(M)$, with $u \prec v$. The nonambiguity condition imposes $v \in \overline{C_M(u)}$. Furthermore, for any elementary $A: M \rightarrow N$ such that $v \in V$, we get $u \setminus A = \{u\}$.

LEMA 3.2 Let $u, v \in \mathcal{R}(M)$. If $C_M(u) \cap \overline{C_M(v)} \neq \emptyset$, then $u \in \overline{C_M(v)}$.

Proof Easy corollary of nonambiguity.

DEFINITION 3.3 Let $A: M_0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow \cdots \rightarrow M_n$, and $u \in \mathcal{O}(M_0)$. We say that $A$ preserves $u$ if $A$ does not contract a redex above $u$, that is, $\forall i \leq n \exists v \in U_i, v \prec u$.

LEMA 3.4 Let $A \in \mathcal{R}(M)$, preserving $v$. For every $u$ in $\mathcal{R}(M)$ such that $u \prec v$, we have $u \setminus A = \{u\}$.

Proof Easy induction on $|A|$.  

We can easily refine the parallel moves lemma to derivations preserving an occurrence $u$, using:

LEMA 3.5 Let $A, B$ be coinitial, both preserving $u$. Then $A \setminus B$ preserves $u$.

Proof Easy induction on $|A| + |B|$, using the following observation. Let $A_1: P \rightarrow Q$.

For all $w \in \mathcal{R}(P)$, $w \setminus A_1$ does not contain any occurrence above both $v$ and $w$.

LEMA 3.6 Let $A, B$ be coinitial, with $A \sqsubseteq B$. If $A$ preserves $u$, then $A$ too preserves $u$.

Proof Assume that $A \sqsubseteq B$, $B$ preserves $u$, and $A$ does not preserve $u$. That is, $A = A_1 A_2 A_3$, where $A_1$ preserves $u$ and $A_2$ contracts set $W$ such that $\exists w \in W$. By lemma 3.5, $B \setminus A_1$ preserves $u$, and by lemma 3.4, $w \setminus (B \setminus A_1) = \{w\}$, whence $A \setminus B \neq 0$, contrary to hypothesis.

We are now ready to present the important definition of an occurrence being external for a (multi)derivation.

DEFINITION 3.7 Let $A \in \mathcal{R}(M)$, $u \in \mathcal{O}(M)$. We say that $u$ is external for $A$, and write $u \in \mathcal{X}(A)$, if either $A$ preserves $u$ or $A = A_1 A_2 A_3$, and there exists $v \prec u$ such that $A_1$ preserves $u$, $A_2: P \rightarrow Q$, with $v \in V$ and $u \in C_P(v)$ and $v \in \mathcal{I}(A_2)$.

Note that in the second case $v$ and the decomposition of $A$ into $A_1 A_2 A_3$ are unique: $A_2$ is the first step in $A$ that does not preserve $u$, and $v$ is the unique redex occurrence above $u$ contracted at this step. Intuitively, $u$ is external for $A$ if $A$ does not contract at some step a redex above $u$ for which the symbol at $u$ in $M$ did not contribute.
Example  Let $\Sigma = \{F(x, B) \rightarrow G(x, x), A \rightarrow B\}$ and consider

$A$: $M_0 = F(C, A) \rightarrow M_1 = F(C, B) \rightarrow M_3 = G(C, C)$

We have $\mathcal{A}(A) = \{A, 2\}$.

**Definition 3.8** Let $A: M_0 \overset{U_1}{\rightarrow} M_1 \overset{U_2}{\rightarrow} M_2 \overset{U_3}{\rightarrow} \cdots \overset{U_n}{\rightarrow} M_n$. We say that $u$ is an initial redex occurrence contributing to $A$, and write $u \in \mathcal{R}(A)$, if $\exists i \leq n \ U_i \cap (u \setminus A[i - 1]) \neq \emptyset$. Finally, we define the external redex occurrences of $A$ as $e(A) = \mathcal{R}(A) \cap \mathcal{X}(A)$

Note that outermost redex occurrences in the starting term of $A$ may be excluded from $e(A)$ either because they are not external for $A$ or else because they are not contracted in $A$.

We shall first extend lemmas 3.4, 3.5 and 3.6 above to $\mathcal{X}(A)$. For lemma 3.4 we need an extra hypothesis: $v$ must be below the redex scheme at $u$.

**Lemma 3.9** Let $A \in \mathcal{R}(M), u$ in $\mathcal{R}(M)$. If $\mathcal{X}(A) \cap \overline{C_M}(u)$, we have $u \setminus A = \{u\}$

**Proof** By induction on $|A|$. Let $v \in \mathcal{X}(A) \cap \overline{C_M}(u) \neq \emptyset$. If $A$ preserves $v$, use lemma 3.4. Otherwise, $A = A_1 A_2 A_3$, and there exists $w < v$ such that the following hold:

a. $A_1$ preserves $v$, and therefore $u \setminus A_1 = \{u\}$ by lemma 3.4
b. $A_2$: $P \overset{w}{\rightarrow} Q$ with $w \in W$ and $v \in C_P(w)$. Furthermore, by (a), $v \in \overline{C_P}(u)$, and thus $w \in \overline{C_P}(u)$ by lemma 3.2. Therefore, $u \setminus A_2 = \{u\}$, and $w \in \overline{C_Q}(u)$.
c. Also, $w \in \mathcal{X}(A_3)$ and therefore, using $w \in \overline{C_Q}(u)$, we get $u \setminus A_3 = \{u\}$, by the induction hypothesis, and finally, $u \setminus A = \{u\}$.

We now extend lemma 3.5 as follows.

**Lemma 3.10** Let $A$ and $B$ be coinitial and $B$ preserve $u \in \mathcal{X}(A)$. Then $u \in \mathcal{X}(A \setminus B)$

**Proof** By induction on $|A|$.

Case 1: $A$ preserves $u$. Then by lemma 3.5, $A \setminus B$ preserves $u$, and therefore $u \in (A \setminus B)$.

Case 2: $\exists v < u$ such that $A = A_1 A_2 A_3$, as in the definition above. As $A_1$ and $B$ preserve $u$, $A_1 \setminus B$ preserves $u$, by lemma 3.5. Similarly, $B \setminus A_1$ preserves $u$, and therefore $v \setminus (B \setminus A_1) = \{v\}$, by lemma 3.4. Finally, $B \setminus A_1$ preserves $v$ (since $v < u$), $A_2$ preserves $v$ trivially, and by lemma 3.5, $B \setminus (A_1 A_2)$ preserves $v$. Now $v \in \mathcal{X}(A_3)$ implies $v \in \mathcal{X}(A_3 \setminus (B \setminus (A_1 A_2)))$, by the induction hypothesis, and therefore, $A \setminus B = (A_1 \setminus B)(A_2 \setminus (B \setminus A_1))(A_3 \setminus (B \setminus (A_1 A_2)))$ is a decomposition, which shows that $u \in \mathcal{X}(A \setminus B)$.

Note also that it follows from the definition of $\mathcal{X}$ that if $A$ preserves $u \in \mathcal{X}(B)$, we have $u \in \mathcal{X}(AB)$. We shall freely use this property below. We are now able to prove the extension of lemma 3.6.

**Lemma 3.11** Let $A$ and $B$ be coinitial, with $A \subseteq B$. We have $\mathcal{X}(B) \subseteq \mathcal{X}(A)$.
Figure 5

**Proof** Let $A \sqsubseteq B$ and $u \in \mathcal{I}(B)$. We show that $u \in \mathcal{I}(A)$ by induction on $|A|$

Case 1: $B$ preserves $u$. Then $A$ preserves $u$, by lemma 3.6, and thus $u \in \mathcal{I}(A)$.

Case 2: Otherwise, $B = B_1B_2B_3$, with $B_2 : P \Rightarrow Q$; $\exists v \in V, v < u$; $B_1$ preserves $u$; $u \in C_R(v)$; and $v \in \mathcal{I}(B_3)$. Since $A$ does not preserve $u$, we have $A = A_1A_2A_3$, where $A_1$ preserves $u$ and $A_2: R \Rightarrow S$ such that $\exists w \in W w < u$. Let $A'_1, A'_2, \ldots, A'_i, B'_i, B'_2, \ldots$ be as shown in figure 5, which expresses the parallel moves lemma for $A$ and $B$. By lemma 3.5, $A'_1$ preserves $u$ and therefore $v$, $B_2$ preserves $v$ trivially, and by lemma 3.5, again $A''_1$ preserves $v$. By lemma 3.10 we get $v \in \mathcal{I}(B'_1)$ as $A'_1$ preserves $u$, $v$ is contracted by $B'_2$, by lemma 3.4. Similarly, $A''_1$ preserves $u$ and therefore $w$, according to the relative positions of $v, w \in R(R)$.

Case 2.1: $v \neq w$. Since our systems are nonambiguos, $u \in C_R(v)$ and $w < u$ imply $v \in C_R(w)$, and thus $w \setminus B'_2 = \{w\}$. Therefore, $w \in R(S)$. Using $v \in \mathcal{I}(B'_3)$, we get by lemma 3.9 that $w \setminus B'_3 = \{w\}$, and therefore $A_2 \setminus (B'_1B'_2B'_3) \neq \emptyset$, a contradiction with $A \sqsubseteq B$.

Case 2.2: $v = w$. Since $A'_2$ and $B'_2$ preserve $v$, so do $A''_2$ and $B''_2$, by lemma 3.5. By lemma 3.10 we get $v \in \mathcal{I}(B'_2)$ as $B'_1B'_2$ preserve $v$, we have $v \in \mathcal{I}(B'_1B'_2B'_3)$. Since $A_3 \equiv B'_1B'_2B'_3$, we get $v \in \mathcal{I}(A_3)$, by the induction hypothesis, and that $A_1A_2A_3$ is a decomposition of $A$, which shows that $u \in \mathcal{I}(A)$.

**Corollary** $A \equiv B$ implies $\mathcal{I}(A) = \mathcal{I}(B)$.

External redex occurrences are their own residual until they are contracted:

**Lemma 3.12** Let $A : M \Rightarrow N$ and $u \in \mathcal{I}(A) \sqcup R(M)$. We have either $u \in \mathcal{I}(A)$ and $u \setminus A = \emptyset$ or $u \notin \mathcal{I}(A)$ and $u \setminus A = \{u\}$.

**Proof** Straightforward from the definitions of $\mathcal{I}(A)$ and $R(M)$.

**Lemma 3.13** If $A \equiv B$, we have $\mathcal{E}(A) = \mathcal{E}(B)$.

**Proof** Let $A \equiv B$ and $u \in \mathcal{E}(A)$. We get $u \in \mathcal{I}(B)$ by the corollary to lemma 3.11.
Lemma 3.12 implies \( u \setminus A = \emptyset \) and therefore, by the parallel moves lemma, \( u \setminus B = \emptyset \). Now lemma 3.12 applied to \( B \) gives \( u \in \mathcal{R}(B) \), and thus \( u \in \mathcal{E}(B) \). ■

If \( u \) is preserved by \( A \), then any prefix occurrence \( v \leq u \) is also preserved by \( A \), obviously. This property is also true of members of \( \mathcal{I}(A) \).

**Lemma 3.14**  If \( u \in \mathcal{I}(A) \), then \( \forall v \leq u \ v \in \mathcal{I}(A) \).

**Proof**  Induction on \(|A|\).

Case 1: \( A \) preserves \( u \) Then \( A \) preserves \( v \), and \( uw \in \mathcal{I}(A) \)

Case 2: \( A = A_1 A_2 A_3 \) with \( A_2: P \xrightarrow{w} Q \) and \( \exists w < u \) such that \( w \in W \), \( u \in C_P(w) \) and \( w \in \mathcal{I}(A_3) \). Moreover, \( A_1 \) preserves \( u \) and therefore \( v \)

Case 2.1: \( u \leq w \) Then \( v \in \mathcal{I}(A_3) \) by the induction hypothesis, and therefore, since \( A_1, A_2 \) preserve \( u \), we get \( v \in \mathcal{I}(A) \).

Case 2.2: \( w < v \leq u \) Then \( v \in C_P(w) \), and therefore the decomposition \( A_1 A_2 A_3 \) shows that \( v \in \mathcal{I}(A) \)

The set \( \mathcal{I}(A) \) is therefore closed by prefix. When it contains some \( u \in \mathcal{I}(M) \), with \( A \in \mathcal{C}(M) \), is also contains all the members of \( C_M(u) \) \( \mathcal{I}(A) \) is obviously non-empty, since it always contains \( \Lambda \), preserved by every derivation. We shall now show that \( \mathcal{E}(A) \) is also non-empty whenever \( A \neq \emptyset \).

**Lemma 3.15**  If \( A \neq 0 \), we have \( \mathcal{E}(A) \neq \emptyset \)

**Proof**  By induction on \(|A|\). If \( A = 0 \), the proof is trivial. Otherwise, let \( A = A_1 A_2 \), with \( A_1: M \xrightarrow{\gamma} N \) elementary If \( A_2 \equiv 0 \), then \( U \neq \emptyset \), and any member of \( U \) is obviously in \( \mathcal{E}(A) \). Otherwise, let us consider \( v \in \mathcal{E}(A) \), which exists by the induction hypothesis.

Case 1: There exists \( u \) in \( U \) such that \( u \leq v \) Then \( u \in \mathcal{I}(A_2) \) by lemma 3.14 and thus \( u \in \mathcal{I}(A) \) since \( A_1 \) preserves \( u \). Therefore, \( u \in \mathcal{E}(A) \)

Case 2: Otherwise, \( v \) is preserved by \( A_1 \), and therefore \( v \in \mathcal{I}(A) \).

Case 2.1: There exists \( u \) in \( U \cap C_M(v) \). Then by definition, \( u \in \mathcal{I}(A) \), and therefore \( u \in \mathcal{E}(A) \).

Case 2.2: Otherwise, \( v \in \mathcal{E}(A) \), and therefore \( v \in \mathcal{E}(A) \) ■

We are now ready to use \( \mathcal{E}(A) \) to construct an outside-in equivalent of \( A \) The following lemma is useful to show that this construction will always terminate.

**Lemma 3.16**  There is no infinite chain \( A_1 \Rightarrow A_2 \Rightarrow A_3 \Rightarrow \cdots \), where \( A \Rightarrow B \) iff \( A \equiv B \) and \( B = A \setminus \{u\} \), with \( u \in \mathcal{E}(A) \)

**Proof**  Let \( A: M_0 \xrightarrow{u_1} M_1 \xrightarrow{u_2} M_2 \xrightarrow{u_3} \cdots \xrightarrow{u_n} M_n \). If \( A \equiv 0 \), there is no \( B \) such that \( A \Rightarrow B \). Otherwise, let \( u \in \mathcal{E}(A) \). According to lemma 3.12, there exists \( k \leq n \) such that \( u \setminus A[k-1] = \{u\} \) and \( u \in U_k \). Therefore, \( (A \setminus u)[k-1,n] = A[k-1,n] \setminus u \) contracts the sets \( U_k, U_{k+1}, \ldots, U_n \). Thus \( A \setminus u \) is less than \( A \) in the lexicographic ordering on the tuples \( \langle|U_n|,|U_{n-1}|,\ldots,|U_1|\rangle \) ■
DEFINITION 3.17  The derivation $A$ is said to be outside-in iff either $A = 0$ or $A = A_1 A_2$, where $A_1$ is the elementary derivation contracting some $u$ in $\mathcal{E}(A)$ and $A_2$ is outside-in.

In other words, in an outside-in derivation, we contract at every step some redex occurrence external for the rest of the derivation.

Let $A$ be any multiderivation. We construct an outside-in equivalent $B$ of $A$ as follows. If $A \equiv 0$, we stop with $B = 0$. Otherwise, let us pick some $u$ in $\mathcal{E}(A)$. We define $B$ as the elementary derivation contracting $u$, followed by an outside-in equivalent of $A \setminus u$. By Noetherian induction, using lemma 3.16, the construction always terminates. By construction, $B \sqsubseteq A$. But according to lemma 3.15, the construction can only stop when $A \sqsubseteq B$, and therefore $B \equiv A$, which justifies our terminology. The construction is illustrated in figure 6.

DEFINITION 3.18  Let $A$ be any derivation. We say that $A$ is standard iff $A$ is outside-in and at every step the redex occurrence $u$ is the leftmost in $\mathcal{E}(A)$.

Similarly to the above, we define the standard derivation $B$ in the class of $A$, and write $B = \text{st}(A)$. Using lemma 3.13, we easily get by Noetherian induction that $\text{st}(A_1) = \text{st}(A_2)$ whenever $A_1 \equiv A_2$.

To conclude, we have shown the following:

THEOREM 3.19: STANDARDIZATION THEOREM  Every derivation class contains a unique standard derivation.

Note that the leftmost condition is unimportant here: any choice function over sets of disjoint occurrences would guarantee the uniqueness of the standard derivation.

Example  Let $\Sigma = \{ F(x, B) \rightarrow G(x, x), A \rightarrow B, C \rightarrow D \}$. Among the derivations starting at $F(C, A)$, all the ones that do not use the reductions marked with an $X$ in figure 7 are standard.

Finally, we remark that it is possible to express standard derivations in terms of residuals, because $\mathcal{E}(A)$ can be characterized as the set of redex occurrences of $A$ that stay outermost modulo permutations in the following sense.
DEFINITION 3.20 Let \( A : M_0 \overset{u_1}{\rightarrow} M_1 \overset{u_2}{\rightarrow} M_2 \overset{u_3}{\rightarrow} \cdots \overset{u_n}{\rightarrow} M_n \) and \( u \in \mathcal{R}(A) \). We say that \( u \) is outermost in \( A \), and write \( u \in \text{Out}(A) \), if \( \forall i \leq n \ \forall v \in u \backslash A[i-1] \ \exists u_i \in U_i \ u_i < v \)

In other words, \( u \in \text{Out}(A) \) iff \( u \in U \) for some \( i \leq n \), and \( \forall j < i \ \exists u_j \in U_j \ u_j \leq u \) Therefore, \( \forall j < i \ u \backslash A[j] = \{ u \} \) and \( u \backslash A[i] = u \backslash A = \emptyset \). Note that lemma 3.12 implies that \( \mathcal{E}(A) \subseteq \text{Out}(A) \). The converse is true for outside-in derivations.

LEMMA 3.21 If \( A \) is outside-in, we have \( \mathcal{E}(A) = \text{Out}(A) \)

**Proof** Let \( A : M_0 \overset{u_1}{\rightarrow} M_1 \overset{u_2}{\rightarrow} M_2 \overset{u_3}{\rightarrow} \cdots \overset{u_n}{\rightarrow} M_n \) be an outside-in derivation and \( u \in \text{Out}(A) \). By definition, \( \exists i \leq n \ u_i = u \) and \( \forall j < i \ u_j \leq u \). Since \( A \) is outside-in, we have \( u \in \mathcal{E}(A[i-1, n]) \) and, since \( A[i-1] \) preserves \( u \), we get \( u \in \mathcal{E}(A) \). The converse follows from lemma 3.12.

LEMMA 3.22 \( \mathcal{E}(A) = \bigcap_{B=\Delta} \text{Out}(B) \).

**Proof** Let \( B \equiv A \). We have, by lemma 3.13, \( \mathcal{E}(A) = \mathcal{E}(B) \subseteq \text{Out}(B) \), which shows that \( \mathcal{E}(A) \subseteq \bigcap_{B=\Delta} \text{Out}(B) \). For the converse, take \( B = \text{st}(A) \) and use the preceding lemma.

That is, \( \mathcal{E}(A) \) is the set of redex occurrences which are outermost in every permutation of \( A \), or equivalently, which are outermost in some outside-in equivalent of \( A \).

The results obtained so far do not allow us to say how to compute in a standard way, since \( \mathcal{E}(A) \) may depend on the whole of \( A \). We are now going to relativize these notions to the starting term of derivation \( A \), so that we may define an outside-in computation rule, generalizing the call-by-name computation rule for recursive program schemes.

### 3.2 Normal Derivation, Call by Name

**DEFINITION 3.23** We define the set of external occurrences in term \( M \) as \( \mathcal{X}(M) = \bigcap_{A \in \mathcal{R}(M)} \mathcal{X}(A) \). Similarly to above, we define the set of external redex occurrences in \( M \) as \( \mathcal{E}(M) = \mathcal{R}(M) \cap \mathcal{X}(M) \), or equivalently, \( \mathcal{E}(M) = \bigcap_{A \in \mathcal{R}(M)} \mathcal{E}'(A) \), where for \( A \) in \( \mathcal{D}(M) \) we define \( \mathcal{E}'(A) = \mathcal{X}(A) \cap \mathcal{R}(M) \).
It is easy to show, similarly to lemma 3.22, that $\mathcal{E}(A) = \bigcap_{B = A} \text{Out}'(B)$, where

$$\text{Out}'(A) = \{ u \in \mathcal{R}(M_0) | \forall i \leq n \forall v \in u \setminus A[i - 1] \exists u_i \in U_i u_i < v \}$$

with $A: M_0 \xrightarrow{u_1} M_1 \xrightarrow{u_2} \cdots \xrightarrow{u_{n-1}} M_{n-1} \xrightarrow{u_n} M_n$

We may therefore characterize alternatively $\mathcal{E}(M)$ as the set of redex occurrences of $M$ which are outermost in every derivation issued from $M$:

$$\mathcal{E}(M) = \bigcap_{A \in \mathcal{D}(M)} \text{Out}'(A).$$

We shall now show that $\mathcal{E}(M)$ is not empty if $M$ is not a normal form. But first we need a technical lemma.

**Notation** We write $\rightarrow_{\text{int}}$ for $\rightarrow$ (internal reduction). We say that derivation $A$ is internal iff it is composed of internal reductions. That is, $A$ in $\mathcal{D}(M)$ is internal iff $M = F M_1 \cdots M_p$ and $A$ preserves $1, 2, \ldots, p$ (and therefore $\mathcal{F}(A) = F N_1 \cdots N_p$). Of course, if $A$ is internal, every permutation of $A$ is internal.

**Lemma 3.24** Let $A: M \xrightarrow{\rightarrow_{\text{int}}}^* A N$. For any $B$ in $\mathcal{D}(N)$ we have $\mathcal{I}(A B) = \mathcal{I}(A)$

**Proof** Obvious from definitions, since $A \in \mathcal{I}(B)$

**Lemma 3.25** $M \in \mathcal{N}\mathcal{F}$ iff $\mathcal{E}(M) = \emptyset$.

**Proof** If $M$ is a normal form, $\mathcal{R}(M) = \emptyset$ and thus $\mathcal{E}(M) = \emptyset$. Conversely, by induction on $M$. Assume $M \in \mathcal{N}\mathcal{F}$. We show $\mathcal{E}(M) \neq \emptyset$.

Case 1: Every $A$ in $\mathcal{R}(M)$ is internal. Thus $M = F(M_1, \ldots, M_p)$ and for some $k \leq p$, $M_k \notin \mathcal{N}\mathcal{F}$. By induction hypothesis there exists $u_k \in \delta(M_k)$, and therefore $ku_k$ is in $\mathcal{E}(M)$.

Case 2: There is some $A: M \xrightarrow{\rightarrow_{\text{int}}} A N$. Let us show that $\mathcal{E}(A) \subseteq \mathcal{E}(M)$. Contrariwise, assume that there exists $B$ in $\mathcal{R}(M)$ and $u$ in $\mathcal{E}(A) - \mathcal{I}(B)$. Since $B \sqsubseteq A \sqcup B$, we have $u \notin \mathcal{I}(A \sqcup B)$ by lemma 3.11. But $\mathcal{I}(A \sqcup B) = \mathcal{I}(A)$ by lemma 3.24, a contradiction with $u \in \mathcal{E}(A)$. Therefore, $\mathcal{E}(A) \subseteq \mathcal{E}(M)$, and since $A \neq 0$, we get $\mathcal{E}(M) \neq \emptyset$ by lemma 3.15.

This permits us to define the notion of normal derivation issued from a term $M$, similarly to what happens in λ-calculus:

**Definition** If $M \in \mathcal{N}\mathcal{F}$, the normal derivation issued from $M$ is 0. Otherwise, let $u$ be the leftmost occurrence in $\mathcal{E}(M)$ and $A$ the elementary derivation: $M \xrightarrow{u} N$. The normal derivation issued from $M$ is $A$ followed by the normal derivation issued from $N$.

**Theorem 3.26** Normal Derivation Theorem If $M$ admits a normal form $N$, the normal derivation issued from $M$ will end in $N$; it is the standard in the class of all derivations going from $M$ to $N$. 
Proof Let $M$ be a term admitting a normal form $N$ and $A$ be some derivation from $M$ to $N$. Let now $B$ be any derivation issued from $M$. We have $B \sqsubseteq A$ and thus $\mathcal{R}(A) \subseteq \mathcal{R}(B)$ by lemma 3.11. This shows that $\mathcal{R}(M) = \mathcal{R}(A)$: the external occurrences of a term admitting a normal form are the occurrences external for any derivation going to this normal form. Assume now there is some $u$ in $(\mathcal{R}(A) \cap \mathcal{R}(M)) - \mathcal{R}(A)$, i.e., $u$ is a redex occurrence in $M$ external to $A$ but not contributing to $A$. According to lemma 3.12 we have $u \setminus A = \{u\}$, contrary to the hypothesis that $N$ is in normal form. This shows that $\mathcal{S}(M) = \mathcal{S}(A)$. With a simple induction on $|A|$, it is now easy to show that $\text{st}(A)$ is the normal derivation issued from $M$.

The notion of normal derivation may be considered as the generalisation to term rewriting systems of the call by name computation rule for recursive equations [2, 6, 8, 27]. In the terminology of [24], we have that all our systems are $d$-outer, using the dominance ordering $d$ defined by $u(dM)v$ iff either $u \leq v$ or $u|v$, $u \in \mathcal{R}(M)$, and $v \notin \mathcal{R}(M)$.

In the next section, we are going to extend these results to define a call-by-need computation rule for terms possessing a normal form. Before that, let us remark that it is possible to extend lemma 3.24 to external redex occurrences, yielding a canonical form for the standard of external derivations issued from a given term.

**Lemma 3.27** Let $A: M \rightarrow^* \rightarrow_N A$. For any $B$ in $\mathcal{S}(N)$ we have $\mathcal{S}(AB) = \mathcal{S}(A)$.

**Proof** Let $u \in \mathcal{S}(AB) - \mathcal{S}(A)$. We have $u \notin \text{Out}(AB)$ and therefore $u \notin \mathcal{S}(AB)$.

**Lemma 3.28** Let $A: M \rightarrow^* \rightarrow_N A$. For any $B$ in $\mathcal{S}(N)$, $AB$ is standard iff $A$ and $B$ are standard.

**Proof** An easy induction on $|A|$, using lemma 3.27 above.

**Corollary** Let $A: M \rightarrow^* \rightarrow_N A$ be standard. For every noninternal $B$ in $\mathcal{S}(N)$ we have $\text{st}(B) = AC$, with $C = \text{st}(B \setminus A)$.

**Proof** If $B$ is not internal, it is easy to show that $A \sqsubseteq B$. Consider $C = \text{st}(B \setminus A)$. Since $A$ is standard, $AC$ is standard by lemma 3.28. But $C \equiv B \setminus A$ implies then that $AC \equiv B$. By unicity of standard derivations, we get $\text{st}(B) = AC$.

### 3.3 Call by Need

We are interested in defining an interpreter for any TRS $\Sigma$ in our class. Such an interpreter will be defined by a computation rule, where we choose in any term $M$ some redex occurrence to contract next. The interpreter will compute correctly if, started on any term $M$ possessing a normal form $N$, it defines a derivation that terminates in $N$ after a finite number of steps.

Note that this question is non-trivial only if for some rule $\alpha \rightarrow \beta$ in $\Sigma$ we have $\nu(\alpha) - \nu(\beta) \neq \emptyset$, since otherwise any computation rule is correct; we leave this easy proof to the reader.
In the general case, we saw in the last section that the normal computation rule (leftmost of $\mathcal{E}(M)$) is correct. Actually, with the help of lemma 3.16 we could easily have proven correct a more general computation rule: contract any redex occurrence in $\mathcal{E}(M)$. Intuitively, the redexes named by $\mathcal{E}(M)$ need to be contracted in order to get to the normal form of $M$. We shall here formalize this concept, and generalize the results of 3.2 by defining precisely what is a correct call-by-need interpreter.

**Definition 3.29** If $M$ admits a normal form $N$, then $u \in \mathcal{R}(M)$ is a redex occurrence needed for the normal form, in symbols $u \in \mathcal{N}(M)$ iff $u \in \mathcal{R}(A)$ for every $A : M \rightarrow N$.

In order to prove further properties of needed redexes, consider first a few technical lemmas about outside-in derivations. In the following, we abbreviate outside-in as "oi".

**Lemma 3.30** If $A \equiv B$ with $A$ oi, then $\mathcal{R}(A) \subseteq \mathcal{R}(B)$.

*Proof* Let $A = A_1 A_2$ with $A_1 : M \rightarrow M'$. Then $u \in \mathcal{E}(A) = \mathcal{E}(B)$. Thus $u \in \mathcal{R}(B)$. Furthermore, $\mathcal{R}(A_2) \subseteq \mathcal{R}(B \setminus A_1)$, by the induction hypothesis. Therefore, $\mathcal{R}(A) \subseteq \mathcal{R}(B)$.

**Corollary** If $M$ has the normal form $N$, then $\mathcal{N}(M) = \mathcal{R}(A)$, where $A$ is any oi derivation from $M$ to $N$.

**Lemma 3.31** If $A$ is oi and $B \subseteq A$, then $A \setminus B$ is oi (except for some empty steps).

*Proof* By induction on $|A|$. Let $A = A_1 A_2$, with $A_1 : M \rightarrow N$. By the induction hypothesis, we already know that $A_2 \setminus (B \setminus A_1)$ is oi. Consider now $A_1 \setminus B$, i.e., $u \setminus B$. If $u \setminus B = \emptyset$, then $A_1 \setminus B$ is obviously oi. Suppose now $u \setminus B \neq \emptyset$. Since $A$ is oi and $A \equiv B \cup A$, we know that $u \in \mathcal{E}(A) = \mathcal{E}(A \setminus B)$. Thus $u \in \text{Out}(B \cup A)$, by lemma 3.22, and $u \setminus B = \{u\}$. Now for all $C \equiv A \setminus B$, one has $u \in \text{Out}(C)$, since $BC \equiv A$ and $u \in \mathcal{E}(A)$. Again by lemma 3.22, one has $u \in \mathcal{E}(A \setminus B)$.

**Lemma 3.32** If $A, B$ are oi and $A \equiv B$, then $|A| = |B|$.

*Proof* If $|A| = 0$, then $B = 0$ and $B = 0$, since $B$ is oi. Similarly if $|B| = 0$. Now let $A = A_1 A_2$ and $B = B_1 B_2$ with $A_1 : M \rightarrow N$ and $B_1 : M \rightarrow P$. Denote temporarily by $C$ the derivation $C$, where the empty steps are suppressed. As $\mathcal{E}(A) = \mathcal{E}(B)$ and $u \in \mathcal{E}(A)$, we have $u$ and $v$ disjoint. Thus if $B_3 = B_1 \setminus A_1$ and $A_3 = A_1 \setminus B_1$, one has $B_3 : N \rightarrow Q$ and $A_3 : P \rightarrow Q$. Therefore, using the previous lemma and an induction on $|A| + |B|$, we get $|A| = 1 + |A_2| = 1 + |(B_2 \setminus A_2')|$. Again by induction, $|A_2 \setminus B_2'| = |A_2 \setminus A_3'|$. But one also has $|B| = 2 + |A_3 \setminus B_3'|$.

**Notation** Let $d(A) = |\text{st}(A)|$.

By the previous lemma, since $\text{st}(A)$ is oi, one has $d(A) = |B|$ for any $B$ oi such that $B \equiv A$. The fact that external redexes are preserved until they are reduced gives us properties of this notion of distance.

**Lemma 3.33** If $A \equiv B$, then $d(A) \geq d(A \setminus B)$.
\[ d(M') = d(M_1) > d(M_2) = d(M_3) > d(M_4) > d(M_5) = d(M_6) > d(M_7) = 0 \]

Figure 8

**Proof** Obvious from the two previous lemmas.

**Lemma 3.34** If \( A \sqsupseteq B \) and \( |B| = 1 \), then \( d(A) > d(A \setminus B) \) iff \( \mathcal{R}(\text{st}(A)) \cap \mathcal{R}(B) \neq \emptyset \).

**Proof** Let \( C = \text{st}(A) \) and \( C = C_1 \sqcup C_2 \), with \( C_1 : M \rightarrow N \). Let \( B = M \rightarrow P \). Then with \( C \equiv A \sqsupseteq B \), we get \( C \equiv B \sqcup C \) and \( u \in \text{Out}(B \sqcup C) \), since \( u \in \mathcal{E}(C) = \mathcal{E}(B \sqcup C) \). This means that \( u \setminus B = \emptyset \) iff \( u \in V \). Now the lemma follows by induction on \( |C| \), since \( A \setminus B \equiv C \setminus B \) and by lemma 3.31 and lemma 3.32.

For the following corollary we denote by \( d(M) \) the length of the standard derivation of \( M \) to its normal form when it exists.

**Corollary** Let \( M \) have the normal form \( N \). Then \( d(M) = 0 \) iff \( M = N \). In addition, let \( M \xrightarrow{U} M' \) Then if \( U \cap \mathcal{N}(M) = \emptyset \), one has \( d(M) = d(M') \). Otherwise, \( d(M) > d(M') \).

This is summarized in figure 8, where the slanted steps are needed and the vertical derivations are standard.

This concludes the proof of the correctness of the call-by-need computation rule. Actually, any interpreter which is fair for needed redexes, in the sense that it will never postpone forever the contraction of needed redexes, is correct for computing normal forms. Note that the standard derivation is the longest derivation contracting only needed redexes.

The next problem we shall tackle is how to effectively compute a needed redex in a given term. We know from the corollary to lemma 3.30 that \( \mathcal{N}(M) = \mathcal{R}(A) \) for \( A \) any outside-in derivation going from \( M \) to its normal form. But this is useless practically. Intuitively we want our interpreter to compute an element of \( \mathcal{N}(M) \) without looking ahead. This problem will be stated precisely and solved in part II of this paper (chapter 12).

**References**


[21] R. Milner. Implementation and application of Scott's logic for computable functions *Proc ACM Conf. on Proving Assertions about Programs* SIGPLAN notices 71, Las Cruces, Jan 1972


[26] B. K. Rosen. Tree manipulation systems and Church-Rosser theorems *JACM* 20, no. 1, 1973