Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems

GÉRARD HUET

INRIA, Le Chesnay, France

ABSTRACT This paper gives new results, and presents old ones in a unified formalism, concerning Church-Rosser theorems for rewriting systems

Abstract confluence properties, depending solely on axioms for a binary relation called reduction, are first presented Results of Newman and others are presented in a unified formalism The systematic use of a powerful induction principle permits the generalization of results of Sethi on reduction modulo equivalence.

Simplification systems operating on terms of a first-order logic are then considered. Results by Rosen and Knuth and Bendix are extended to give several new criteria for confluence of these systems It is then shown how these criteria yield new methods for the mechanization of equational theories

KEY WORDS AND PHRASES Church-Rosser property, confluence, combinatorial theories, equational theories, operational semantics, equality theorem proving

CR CATEGORIES. 5 21, 5 24

1. *Introduction*

Term rewriting systems are an interesting model of computation. They may be used to represent abstract interpreters of programming languages and to model formula manipulating systems used in various applications, such as program optimization, program validation, and automatic theorem proving. A generalization of these systems consists in considering rewritings on equivalence classes of terms, defined by a set of equations. These equations may be used, for instance, to define abstract data types.

A fundamental property of term rewriting systems is confluence, depicted in Figure 3. In confluent systems replacements may be effected deterministically, i.e., there is no need to backtrack to consider other possible rewritings. Confluence is equivalent to the Church-Rosser property, which expresses the fact that interconvertibility of two terms can be checked by mere simplification to a common form. Confluent term rewriting systems in which every computation terminates determine a decision procedure for the corresponding equational theory, since every term possesses a unique canonical form.

We consider in this paper sufficient conditions for the confluence of a term rewriting system. The general strategy is inspired by Knuth and Bendix [16]. We show that confluence is implied by the confluence of certain special cases, the critical pairs. Critical pairs are computed by a superposition algorithm, where one attempts to match in a most general way the left-hand side of some rule with a nonvariable subterm of some other left-hand side. For instance, the two rules $F(G(x, y, A)) \to H(x, y)$ and $G(B, x, y) \to K(y, x)$ determine a critical pair $\langle F(K(A, x)), H(B, x)\rangle$. We show that various closure conditions on the critical pairs imply the closure of corresponding diagrams in the general case. The

A preliminary version of this paper was presented at the 18th IEEE Symposium on Foundations of Computer Science, Providence, R I, October 1977

Author's address: INRIA, Domaine de Voluceau-Rocquencourt, B.P. 105-78150 Le Chesnay, France.

diagrams in turn imply confluence under certain conditions. For instance, we show that a left-linear term rewriting system $\mathscr{R}$ is confluent when $P \twoheadrightarrow Q$ for every critical pair $\langle P, Q\rangle$, where $\twoheadrightarrow$ is parallel disjoint reduction by $\mathscr{R}$, generalizing a theorem of Rosen. We show how some of these results carry over to rewritings of equational classes of terms, yielding a decision procedure for the confluence of certain equational theories.

All our results are carefully partitioned between abstract diagrammatic properties that depend solely on axiomatic conditions on the reduction relation and properties depending on the term structure. The abstract confluence properties are studied separately in Section 2, which unifies and extends results of Newman [23] and Sethi [34].

2. *Abstract Reduction Properties*

2.1 GENERALITIES. Let $\mathscr{E}$ be an arbitrary set. We give in this section some more or less well-known properties of a binary relation $\rightarrow$ on $\mathscr{E}$, which we call *reduction.* These properties are abstract in the sense that they depend solely on axioms for the reduction relation.

Notation

ι is the identity relation on $\mathscr{E}$: $\iota = \{\langle x, x\rangle \mid x \in \mathscr{E}\}$.
$\cdot$ is relation composition: $\rightarrow_a \cdot \rightarrow_b = \{\langle x, y\rangle \mid \exists z\ x \rightarrow_a z\ \&\ z \rightarrow_b y\}$.
$\rightarrow^{-1}$ is the inverse of relation $\rightarrow$: $\rightarrow^{-1} = \{\langle x, y\rangle \mid y \rightarrow x\}$.

For any relation $\rightarrow$ on $\mathscr{E}$, we now define

$\xrightarrow{0} = \iota$	
$\xrightarrow{\epsilon} = \rightarrow \cup\ \iota$	reflexive closure of $\rightarrow$;
$\xrightarrow{i} = \rightarrow \cdot \xrightarrow{i-1}\ \forall i > 0$	i-fold composition of $\rightarrow$;
$\xrightarrow{+} = \bigcup_{i>0} \xrightarrow{i}$	transitive closure of $\rightarrow$;
$\xrightarrow{*} = \xrightarrow{+} \cup\ \iota$	transitive-reflexive closure of $\rightarrow$;
$\leftrightarrow\ = \rightarrow \cup \rightarrow^{-1}$	symmetric closure of $\rightarrow$.

If x is minimal with respect to $\rightarrow$, i.e., $\nexists y\ x \rightarrow y$, we say that x is a $\rightarrow$-*normal form*, and we let $\mathscr{N}$ be the set of all such elements. For $x \in \mathscr{E}$, if there exists $y \in \mathscr{N}$ such that $x \xrightarrow{*} y$, we say that y is a $\rightarrow$-*normal form of* x.

For a given relation $\rightarrow$, we let

$$
\begin{aligned}
x \downarrow y &\Leftrightarrow \exists z\ x \xrightarrow{*} z\ \&\ y \xrightarrow{*} z,\\
x \uparrow y &\Leftrightarrow \exists z\ z \xrightarrow{*} x\ \&\ z \xrightarrow{*} y,\\
\Lambda(x) &= \max\{i \mid \exists y\ x \xrightarrow{i} y\} \in N \cup \{\infty\},\\
\Delta(x) &= \{y \mid x \rightarrow y\},\\
\Delta^+(x) &= \{y \mid x \xrightarrow{+} y\},\\
\Delta^*(x) &= \Delta^+(x) \cup \{x\}.
\end{aligned}
$$

Definition. We say that relation $\rightarrow$ is

(i) *inductive* iff for every sequence $x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_n \rightarrow \cdots$, there exists y such that $\forall i \geq 1\ x_i \xrightarrow{*} y$;
(ii) *acyclic* iff $\xrightarrow{+}$ is irreflexive (and then $\xrightarrow{*}$ is a partial ordering relation);
(iii) *noetherian* iff there is no infinite sequence $x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_n \rightarrow \cdots$ (then $\xrightarrow{*}$ is well founded);
(iv) *bounded* iff $\forall x\ \Lambda(x) < \infty$ (then $\xrightarrow{*}$ is of order type ω; this is called the finiteness property in [1, 34]).

Every bounded relation is noetherian, and every noetherian relation is inductive and acyclic.

Let P be any predicate on $\mathscr{E}$. We say that P is $\rightarrow$-*complete* iff

$$\forall x \in \mathscr{E}\ [\forall y \in \Delta^+(x)\ P(y)] \Rightarrow P(x).$$

Our interest in noetherian relations stems from the following.

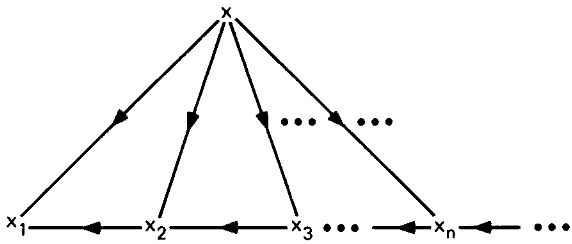


Figure 1

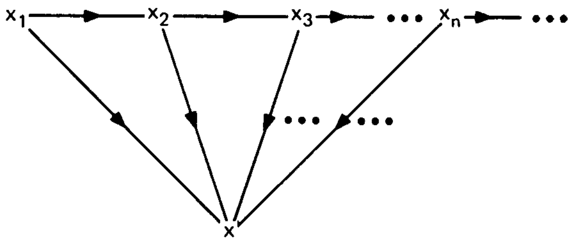


Figure 2

Principle of Noetherian Induction. Let $\rightarrow$ be a noetherian relation, and let P be a $\rightarrow$-complete predicate. Then $\forall x \in \mathscr{E}\ P(x)$.

This principle is as powerful as the usual forms of transfinite induction. It has the advantage of not requiring the construction of a (total) well ordering, using directly the partial ordering $\xrightarrow{*}$ instead. For its justification see [5], and for examples of its use see [3].

Definition. We say that relation $\rightarrow$ is *locally finite* iff $\forall x \in \mathscr{E}\ \Delta(x)$ is finite.

Let $\rightarrow$ be a locally finite relation. For every x in $\mathscr{E}$, if $\Lambda(x) = \infty$, then there exists an infinite sequence $x = x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_n \rightarrow \cdots$, using Koenig's lemma. Therefore a locally finite relation is bounded iff it is noetherian.

We say that relation $\rightarrow$ is *globally finite* iff $\forall x \in \mathscr{E}\ \Delta^*(x)$ is finite.

Let $\rightarrow$ be a locally finite relation. For every x in $\mathscr{E}$, if $\Delta^*(x)$ is infinite, then $\Lambda(x) = \infty$, and, as above, there exists an infinite sequence $x = x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_n \rightarrow \cdots$. Therefore a noetherian locally finite relation is globally finite. Conversely, any acyclic globally finite relation is bounded.

Finally, note that acyclic and noetherian does not imply bounded, as shown by Figure 1. Also, acyclic, inductive, and locally finite implies neither noetherian nor globally finite, as shown by the dual example in Figure 2.

2.2 CONFLUENCE PROPERTIES. Suppose we are interested in the equivalence $\xleftrightarrow{*}$ generated by a relation $\rightarrow$. We are going to give conditions on $\rightarrow$ that permit us to recognize if $x \xleftrightarrow{*} y$ when performing only reductions ($\xrightarrow{*}$) from x and y.

Definition. We say that the relation $\rightarrow$ is *confluent* iff $\forall xy\ x \uparrow y \Rightarrow x \downarrow y$.

We express this property with the diagram in Figure 3. In this sort of diagram, dashed arrows denote (existential) reductions depending on the (universal) reductions shown by full arrows.

The results of this section appear in Newman [23]. They have been rediscovered by several authors in various contexts, where $\rightarrow$ is interpreted as the β-reduction relation in λ-calculus [4, 6, 9], the deduction relation in a formal system, or the operational semantics in a programming language.

LEMMA 2.1 *If $\rightarrow$ is confluent, then the following "Church–Rosser" property holds*: $\forall xy$ $x \xleftrightarrow{*} y \Leftrightarrow x \downarrow y$.

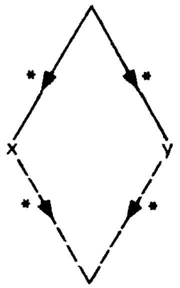


Figure 3

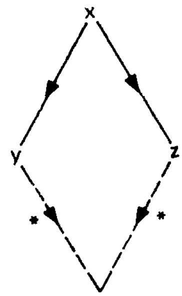


Figure 4

PROOF. By induction on n, where $x \overset{n}{\longleftrightarrow} y$. □

LEMMA 2.2 *If $\rightarrow$ is confluent, then the normal form of any element, if it exists, is unique.*

PROOF. Trivial. □

The converse of this lemma, when $\rightarrow$ is such that every element possesses a normal form, is also true. This will be the case, for instance, with acyclic inductive relations (using Zorn's lemma).

The two preceding lemmas show the interest of confluent relations. The rest of this section is devoted to finding sufficient conditions for a relation to be confluent. First, it is easy to partially localize the test for confluence.

LEMMA 2.3 *$\rightarrow$ is confluent iff $\forall xyz\ x \rightarrow y\ \&\ x \xrightarrow{*} z \Rightarrow y \downarrow z$.*

PROOF. By induction on n, where $x \xrightarrow{n} z$. □

In the case of noetherian relations it is possible to localize the confluence test completely.

Definition. We say that relation $\rightarrow$ is *locally confluent* iff

$$\forall xyz\ x \rightarrow y\ \&\ x \rightarrow z \Rightarrow y \downarrow z.$$

The corresponding diagram is shown in Figure 4.

LEMMA 2.4. *A noetherian relation is confluent iff it is locally confluent.*

This lemma appears in various places in the literature in weaker forms: either the relation is required to be bounded (easy induction on $\Lambda(x)$) [1, 34], or it is assumed to be locally finite [17], or it is proved for a specific noetherian relation [16] (ad hoc induction). Several weaker forms are given in [36]. It appears in its full generality in [23], but with an unnecessarily complex proof. Let us show how noetherian induction permits an easy and natural proof.

PROOF OF LEMMA 2.4. The "only if" part is trivial. For the "if" part, assume $\rightarrow$ is a noetherian locally confluent relation. We prove $P(x)$: $\forall yz\ x \xrightarrow{*} y\ \&\ x \xrightarrow{*} z \Rightarrow y \downarrow z$ by noetherian induction, showing that P is $\rightarrow$-complete.

Let $x \xrightarrow{m} y$ and $x \xrightarrow{n} z$. We show that $\exists t\ y \xrightarrow{*} t\ \&\ z \xrightarrow{*} t$.

(i) If $m = 0$, we choose $t = z$; if $n = 0$, we choose $t = y$.
(ii) Otherwise, let $x \rightarrow y_1 \xrightarrow{*} y\ \&\ x \rightarrow z_1 \xrightarrow{*} z$.

By local confluence, $\exists u\ y_1 \xrightarrow{*} u\ \&\ z_1 \xrightarrow{*} u$. By the induction hypothesis $P(y_1)$, $\exists v\ y \xrightarrow{*} v\ \&\ u \xrightarrow{*} v$. By the induction hypothesis $P(z_1)$, $\exists t\ v \xrightarrow{*} t\ \&\ z \xrightarrow{*} t$, proving $P(x)$.

The induction step of the proof is shown in the diagram of Figure 5. □

Lemma 2.4 fails if we just suppose $\rightarrow$ to be inductive and acyclic, as shown by the counterexample in Figure 6a, due to Newman, or inductive and finite, as shown by Figure 6b, due to Hindley. Note that the two diagrams are two projections of a 3-D object.

For the relations that are not noetherian, much stronger local hypotheses are necessary to yield confluence.

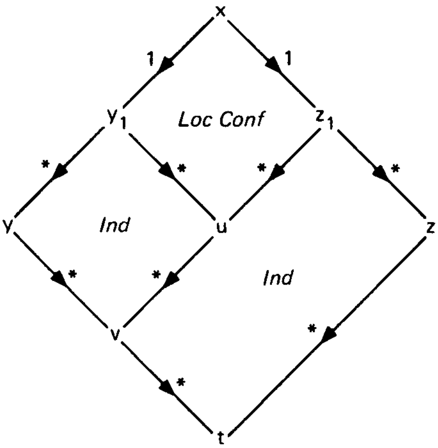
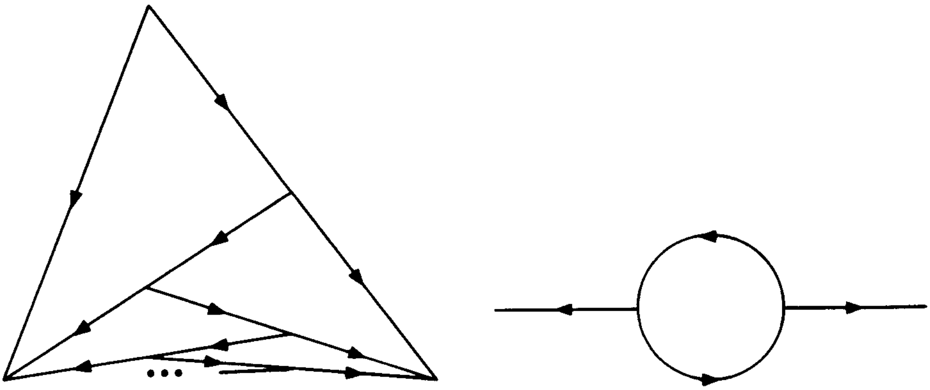


Figure 5



(a) (b)

Figure 6

Definition. We say that the relation $\rightarrow$ is *strongly confluent* iff

$$\forall xyz\ x \rightarrow y \;\&\; x \rightarrow z \Rightarrow \exists u\ y \xrightarrow{*} u \;\&\; z \xrightarrow{\varepsilon} u.$$

The corresponding diagram is shown in Figure 7.

Remark. Beware of the symmetry between y and z in the definition above. It is only slightly weaker than requiring $y \xrightarrow{\varepsilon} u \;\&\; z \xrightarrow{\varepsilon} u$. For instance, the relation $\rightarrow$ in Figure 6 is not strongly confluent.

LEMMA 2.5. *Any strongly confluent relation is confluent.*

PROOF. It is easy to show by induction on n that if $\rightarrow$ is strongly confluent, then $\forall xyz$ $x \xrightarrow{\varepsilon} y \;\&\; x \xrightarrow{n} z \Rightarrow \exists u\ y \xrightarrow{*} u \;\&\; z \xrightarrow{\varepsilon} u$. The result then follows from Lemma 2.3. □

It may seem that the condition of strong confluence is too restrictive to be of practical use. However, Lemma 2.5 can be used as follows. If we are able to define, from the reduction relation $\rightarrow$, a strongly confluent relation $\rightarrow_S$ with the same transitive closure as $\rightarrow$: $\xrightarrow{*} = \xrightarrow{*}_S$, the confluence of $\rightarrow$ follows from Lemma 2.5. This is the basis of the Tait and Martin-Löf method for proving the Church–Rosser theorem in λ-calculus [10]. Actually, a weaker condition than $\xrightarrow{*} = \xrightarrow{*}_S$ is sufficient: it is enough to show that $\rightarrow_S$ is a compatible refinement of $\rightarrow$ in the sense of Staples [36].

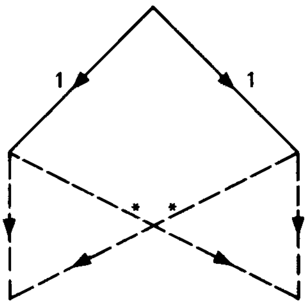


Figure 7

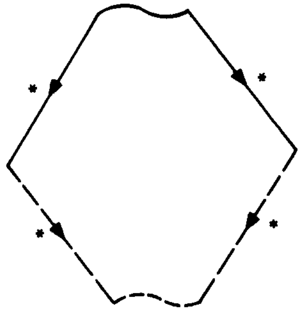


Figure 8

Various other axiomatic conditions imply confluence, for instance, using decompositions of $\rightarrow$ as the union of two or more relations. See in particular [23, 33, 36]. For instance, Lemma 2.5 is a consequence of the commutativity lemma in Rosen [33].

2.3 Reduction Modulo Equivalence. Our motivation in studying reduction relations stems from practical problems arising in formula manipulation systems such as theorem provers, program optimizers, and algebraic simplifiers. The problem is to define some efficient operational semantics for an equational theory. This theory is usually defined by axioms of two forms: "structural" axioms such as associativity and commutativity of operators, and "simplification rules" such as "**if** true **then** x **else** $y \rightarrow x$." While the latter usually define a noetherian relation on the terms of the language, the former can often be taken into account by a specific data structure used to represent these terms.

We now model this situation by considering a reduction relation $\rightarrow$, together with an equivalence relation $\sim$, in the same manner as [1, 34].

Definition. We say that the relation $\rightarrow$ is *confluent modulo* $\sim$ iff

$$\forall xyx'y'\ x \sim y \;\&\; x \xrightarrow{*} x' \;\&\; y \xrightarrow{*} y' \Rightarrow \exists \bar{x}\bar{y}\ x' \xrightarrow{*} \bar{x} \;\&\; y' \xrightarrow{*} \bar{y} \;\&\; \bar{x} \sim \bar{y}.$$

The corresponding diagram is given in Figure 8.

Note that this condition is *different* from $\rightarrow/\sim$ being confluent in $\mathscr{E}/\sim$, since we do not allow $\sim$ along the $\rightarrow$-derivations. If $\rightarrow$ has the property of defining at least one normal form for every element, we get a weak form of Lemma 2.2.

Lemma 2.6. *Let $\rightarrow$ normalize $\mathscr{E}$; i.e., $\forall x \in \mathscr{E}\ \exists y \in \mathscr{N}\ x \xrightarrow{*} y$. Then $\rightarrow$ is confluent modulo $\sim$ iff*

$$\forall xy \in \mathscr{E}\ \forall uv \in \mathscr{N}\ x \equiv y \;\&\; x \xrightarrow{*} u \;\&\; y \xrightarrow{*} v \Rightarrow u \sim v,$$

where $\equiv$ is $(\leftrightarrow \cup \sim)^*$.

Proof. The proof is trivial and is left to the reader. $\square$

We are now going to search for sufficient conditions for $\rightarrow$ to be confluent modulo $\sim$. The first step is to generalize Lemma 2.4, assuming $\rightarrow$ noetherian. Lemma 2.7 below generalizes Theorem 2.2 of Sethi [34], who requires $\rightarrow$ to be bounded. This generalization will be useful in practice, since one frequently proves termination results using lexicographic orderings on terms that are noetherian but not bounded [16]. But the main interest here lies in the technique of proof, based on noetherian induction.

Definition. We say that relation $\rightarrow$ is *locally confluent modulo* $\sim$ iff conditions α and β are satisfied:

$$\alpha: \quad \forall xyz\ x \rightarrow y \;\&\; z \rightarrow y \Rightarrow y \tilde{\downarrow} z,$$

$$\beta: \quad \forall xyz\ x \sim y \;\&\; x \rightarrow z \Rightarrow y \tilde{\downarrow} z,$$

where $y \tilde{\downarrow} z \Leftrightarrow \exists uv\ y \xrightarrow{*} u \;\&\; z \xrightarrow{*} v \;\&\; u \sim v$.

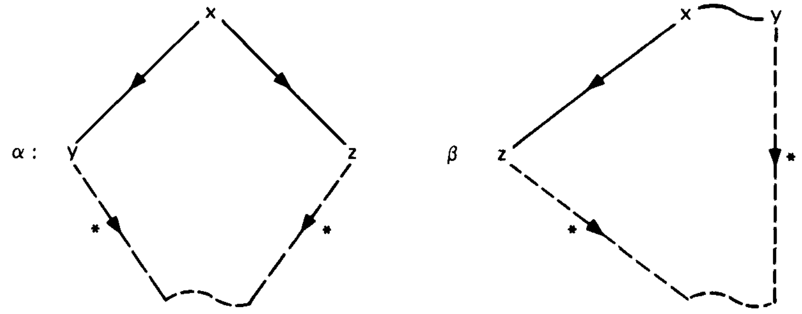


Figure 9

The corresponding diagrams are shown in Figure 9. Property α (respectively, β) is called P3 (respectively, P1) in [34].

We can now state the generalization of Lemma 2.4.

LEMMA 2.7. *Let $\rightarrow$ be a noetherian relation. For any equivalence $\sim$, $\rightarrow$ is confluent modulo $\sim$ iff $\rightarrow$ is locally confluent modulo $\sim$.*

Before giving the proof of this lemma, let us state a preliminary technical proposition.

Definition

$$\langle x, y\rangle \underset{a_1}{\rightarrow} \langle x', y'\rangle \Leftrightarrow x \rightarrow x' \;\&\; y = y',$$
$$\langle x, y\rangle \underset{a_2}{\rightarrow} \langle x', y'\rangle \Leftrightarrow x \rightarrow x' \;\&\; x \rightarrow y',$$
$$\langle x, y\rangle \underset{b_1}{\rightarrow} \langle x', y'\rangle \Leftrightarrow x = x' \;\&\; y \rightarrow y',$$
$$\langle x, y\rangle \underset{b_2}{\rightarrow} \langle x', y'\rangle \Leftrightarrow y \rightarrow x' \;\&\; y \rightarrow y',$$

$$\underset{a}{\rightarrow} = \underset{a_1}{\rightarrow} \cup \underset{a_2}{\rightarrow}, \qquad \underset{b}{\rightarrow} = \underset{b_1}{\rightarrow} \cup \underset{b_2}{\rightarrow}, \qquad \boldsymbol{\rightarrow} = \underset{a}{\rightarrow} \cup \underset{b}{\rightarrow}.$$

PROPOSITION 2.1. *If $\rightarrow$ is noetherian, then $\boldsymbol{\rightarrow}$ is a noetherian relation in $\mathscr{E}^2$.*

PROOF. Let

$$\underset{c}{\rightarrow} = \underset{a}{\rightarrow} \cup \overset{*}{\underset{b_1}{\rightarrow}}, \qquad \underset{d}{\rightarrow} = \underset{a_1}{\rightarrow} \cup \underset{b}{\rightarrow}.$$

First we show that $\underset{c}{\rightarrow}$ is noetherian. Assume the existence of an infinite $\underset{c}{\rightarrow}$-sequence. Since $\underset{b_1}{\rightarrow}$ is noetherian, it must be of the form $\overset{*}{\underset{b_1}{\rightarrow}} \underset{a}{\rightarrow} \overset{*}{\underset{b_1}{\rightarrow}} \underset{a}{\rightarrow} \cdots$, which implies the existence of an infinite $\rightarrow$-sequence of its first projections, contrary to the hypothesis that $\rightarrow$ is noetherian. Similarly, $\underset{d}{\rightarrow}$ is noetherian. Therefore, any infinite $\boldsymbol{\rightarrow}$ sequence must be of the form:

$$\overset{*}{\boldsymbol{\rightarrow}} \langle x_1, y_1\rangle \underset{a_2}{\rightarrow} \langle x_2, y_2\rangle \overset{*}{\underset{d}{\rightarrow}} \langle x_3, y_3\rangle \underset{b_2}{\rightarrow} \langle x_4, y_4\rangle \overset{*}{\underset{c}{\rightarrow}} \langle x_5, y_5\rangle \underset{a_2}{\rightarrow} \langle x_6, y_6\rangle \cdots,$$

which implies the existence of an infinite $\rightarrow$-sequence,

$$x_1 \rightarrow y_2 \overset{*}{\rightarrow} y_3 \rightarrow x_4 \overset{*}{\rightarrow} x_5 \rightarrow y_6 \rightarrow \cdots,$$

a contradiction. □

PROOF OF LEMMA 2.7. Let $\rightarrow$ be a noetherian relation locally confluent modulo $\sim$. We shall use noetherian induction in $\mathscr{E}^2$, applied to $\boldsymbol{\rightarrow}$ and to the property

$$P(x, y): \qquad x \sim y \Rightarrow [\forall x', y' \; x \overset{*}{\rightarrow} x' \;\&\; y \overset{*}{\rightarrow} y' \Rightarrow x' \tilde{\downarrow} y'].$$

Let us show that P is $\boldsymbol{\rightarrow}$-complete. For that, let $x, y, x', y' \in \mathscr{E}$ such that $x \sim y$, $x \overset{n}{\rightarrow} x'$, $y \overset{m}{\rightarrow} y'$. We show $\exists \bar{x}, \bar{y}$: $x' \overset{*}{\rightarrow} \bar{x}$, $y' \overset{*}{\rightarrow} \bar{y}$, $\bar{x} \sim \bar{y}$.

If $n = 0$ and $m = 0$, the result is trivial. Otherwise, let us assume without loss of generality that $n > 0$, and let $x \rightarrow x_1 \overset{*}{\rightarrow} x'$. By applying property β to x, y, x_1, we get u and v such that $x_1 \overset{*}{\rightarrow} u$, $y \overset{*}{\rightarrow} v$, $u \sim v$. There are two cases.

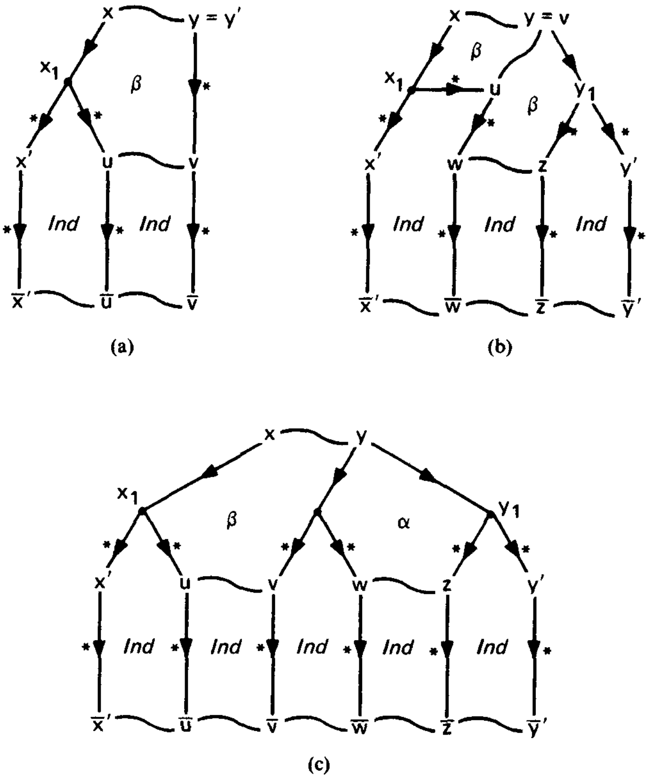


Figure 10

Case 1. $m = 0$. Let $\bar{x}'$, $\bar{u}$, and $\bar{v}$ be $\rightarrow$-normal forms of x', u, and v, respectively. We get $\bar{x}' \sim \bar{u}$ by the induction hypothesis $P(x_1, x_1)$ and $\bar{u} \sim \bar{v}$ by the induction hypothesis $P(u, v)$, completing the proof of case 1. The diagram is shown in Figure 10a.

Case 2. $m > 0$. Let $y \rightarrow y_1 \xrightarrow{*} y'$. Again there are two cases.

2a. $v = y$. We again apply property β to y, u, y_1, getting w and z such that $u \xrightarrow{*} w$, $y_1 \xrightarrow{*} z$, $w \sim z$. Let $\bar{x}'$, $\bar{w}$, $\bar{z}$, and $\bar{y}'$ be $\rightarrow$-normal forms of x', w, z and y', respectively. We get $\bar{x}' \sim \bar{w}$ by the hypothesis $P(x_1, x_1)$, $\bar{w} \sim \bar{z}$ by $P(w, z)$, and $\bar{z} \sim \bar{y}'$ by $P(y_1, y_1)$, completing the proof of this case. The diagram is shown in Figure 10b.

2b. Otherwise, let $y \rightarrow t \xrightarrow{*} v$. We now apply property α to y, y_1, t, getting w and z such that $t \xrightarrow{*} w$, $y_1 \xrightarrow{*} z$, $w \sim z$. Let $\bar{x}'$, $\bar{u}$, $\bar{v}$, $\bar{w}$, $\bar{z}$, and $\bar{y}'$ be normal forms, respectively, of x', u, v, w, z, and y'. We get $\bar{x}' \sim \bar{u}$ by the induction hypothesis $P(x_1, x_1)$, $\bar{u} \sim \bar{v}$ by $P(u, v)$, $\bar{v} \sim \bar{w}$ by $P(t, t)$, $\bar{w} \sim \bar{z}$ by $P(w, z)$, and finally, $\bar{z} \sim \bar{y}'$ by $P(y_1, y_1)$, completing the proof of the lemma. The diagram is shown in Figure 10c.

We leave it to the reader to check that we used the hypothesis $P(\lambda, \mu)$ only when $\langle x, y\rangle \xrightarrow{+} \langle \lambda, \mu\rangle$. Actually, the definition of $\rightarrow$ was inspired directly by the diagrams we wished to prove, which makes this method a very natural one to use for this sort of proof. The diagrams are the same as in Sethi's proof [34]. □

Next, we further localize property β, when considering $\sim$ as generated by a symmetric relation $\vdash\!\dashv$; i.e., $\sim\ = \overset{*}{\vdash\!\dashv}$.

Definition. Property γ:

$$\forall xyz\ x \vdash\!\dashv y\ \&\ x \rightarrow z \Rightarrow y \overset{\sim}{\downarrow} z \qquad \text{with} \quad \sim\ = \overset{*}{\vdash\!\dashv}.$$

The corresponding diagram is shown in Figure 11.

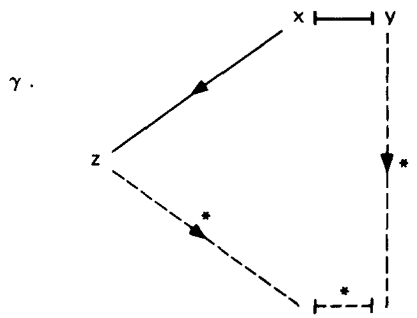


Figure 11

Definition. If $x \sim y$, we define $\rho(x, y)$ as the smallest k such that $x \overset{k}{\vdash\!\dashv} y$. In a similar way as above, we define a relation $\mapsto$ in $\mathscr{E}^2$ by

$$\langle x, y\rangle \mapsto \langle x', y'\rangle$$

iff

(i) either $\langle x, y\rangle \rightarrow \langle x', y'\rangle$ with same definition as above,
(ii) or $x \sim y \sim x' \sim y'$ and $\rho(x, y) > \rho(x', y')$.

PROPOSITION 2.2. *If $\rightarrow\cdot\sim$ is noetherian (or, equivalently, if $\rightarrow/\sim$ is noetherian in $\mathscr{E}/\sim$), then $\mapsto$ is a noetherian relation in $\mathscr{E}^2$.*

The proof follows that of Proposition 2.1, but in the quotient, set $\mathscr{E}/\sim$. Note that we need a stronger condition than for Proposition 2.1.

LEMMA 2.8. *Let $\vdash\!\dashv$ be a symmetric relation, and let $\sim\, = \overset{*}{\vdash\!\dashv}$. Let $\rightarrow$ be any relation such that $\rightarrow\cdot\sim$ is noetherian. Then $\rightarrow$ is confluent modulo $\sim$ iff properties α and γ are satisfied.*

PROOF. The "only if" part is obvious. For the "if" part, let us assume that $\rightarrow\cdot\sim$ is noetherian and that properties α and γ hold. We again use noetherian induction in $\mathscr{E}^2$, applied to $\mapsto$, and the same property P as in the proof of Lemma 2.7.

Let $x, y, x', y' \in \mathscr{E}$ be such that $x \sim y$, $x \overset{n}{\rightarrow} x'$, $y \overset{m}{\rightarrow} y'$. We show the existence of $\bar{x}$ and $\bar{y}$ such that $x' \overset{*}{\rightarrow} \bar{x}$, $y' \overset{*}{\rightarrow} \bar{y}$, and $\bar{x} \sim \bar{y}$.

There are two cases.

Case 1. $x = y$.

1a. If $n = 0$ or $m = 0$, it is trivial.

1b. Otherwise, let $x \rightarrow u \overset{*}{\rightarrow} x'$ and $y \rightarrow v \overset{*}{\rightarrow} y'$. Applying property α to x, u, and v, we get the existence of w and z such that $u \overset{*}{\rightarrow} w$, $v \overset{*}{\rightarrow} z$, and $w \sim z$. Let $\bar{x}'$, $\bar{w}$, $\bar{z}$, and $\bar{y}'$ be $\rightarrow$-normal forms of x', w, z, and y', respectively. We get $\bar{x}' \sim \bar{w}$ by the induction hypothesis $P(u, u)$, $\bar{w} \sim \bar{z}$ by hypothesis $P(w, z)$, and $\bar{z} \sim \bar{y}'$ by hypothesis $P(v, v)$, completing the proof of case 1 according to the diagram in Figure 12a.

Case 2. $\rho(x, y) > 0$.

2a. If $n = 0$ and $m = 0$, it is trivial.

2b. Otherwise, let us assume without loss of generality that $n > 0$, and let $x \rightarrow u \overset{*}{\rightarrow} x'$. Let us choose v such that $x \vdash\!\dashv v \sim y$, with $\rho(v, y) = \rho(x, y) - 1$. Applying property γ to x, v, and u, we get w and z such that $u \overset{*}{\rightarrow} w$, $v \overset{*}{\rightarrow} z$, and $w \sim z$. We complete the proof as in case 1, applying induction hypotheses $P(u, u)$, $P(w, z)$, and $P(v, y)$. Note that we always have $\langle x, y\rangle \overset{+}{\mapsto} \langle w, z\rangle$. This concludes the proof, according to the diagram in Figure 12b. □

Remarks. Sethi's Theorem 2.3 [34] is similar to Lemma 2.8 in the special case $\vdash\!\dashv\, = \sim_1 \cup \sim_2$, where $\sim_1$ and $\sim_2$ are two equivalence relations. But his conditions are significantly

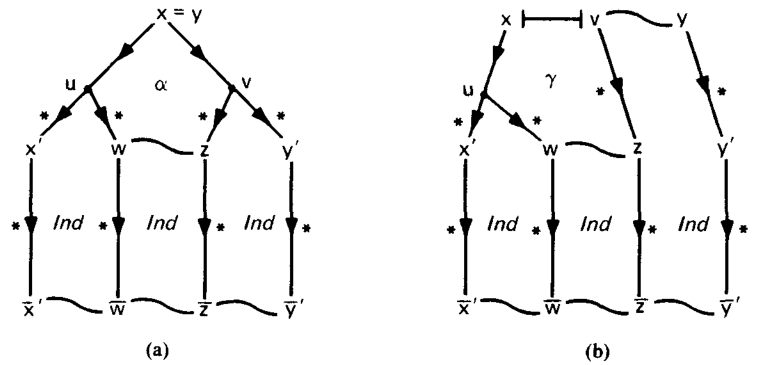


Figure 12

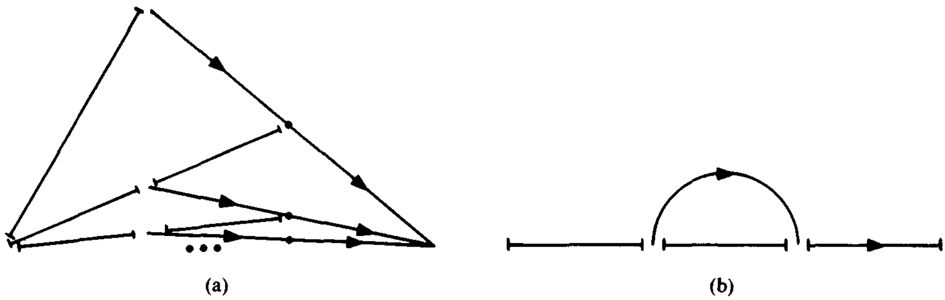


Figure 13

more restrictive: he demands that $\rightarrow \cup \sim$ be bounded, because he explicitly constructs an ordinal for the induction.

Nivat shows in [24] an equivalent of Lemma 2.8 for a reduction relation defined by word rewritings in a free monoid.

Note the symmetry between properties α and γ. Both express localizing the confluence check to *one* application of the generators of $\xrightarrow{*}$ and $\sim$, respectively.

The rather strong condition that $\rightarrow \cdot \sim$ be noetherian is essential. For instance, Figure 13 gives examples (inspired by the ones in Figure 6) where $\rightarrow$ is noetherian and α and γ are true. Still, $\rightarrow$ is not confluent modulo $\sim$.

3. *Applications to Term Rewriting Systems*

3.1 The Subsumption Lattice of First-Order Terms. We briefly survey properties of the set $\mathcal{T}$ of terms of a first-order language, ordered by substitution. Full proofs may be found in [12], and related results in [30, 31].

Let $\mathcal{V}$ be a denumerable set of elements called *variables*, denoted $x, y, z, \ldots$. Let $\mathcal{F}$ be a finite or denumerable set, with $\mathcal{F} \cap \mathcal{V} = \emptyset$, graded by an *arity* function $a : \mathcal{F} \rightarrow \mathbf{N}$. Elements in $\mathcal{F}$ are called *function symbols*, denoted $F, G, H, \ldots$. We define $\mathcal{F}_n = \{F \in \mathcal{F} \mid a(F) = n\}$.

The set $\mathcal{T}$ of *terms* is defined as the free a-graded $\mathcal{F}$-algebra generated by $\mathcal{V}$. That is, a term is either a variable or is of the form $FM_1M_2 \cdots M_n$ for some $F \in \mathcal{F}_n$ and $M_1, M_2, \ldots, M_n \in \mathcal{T}$. We denote terms by letters M, N, P, Q. We define a few functions on terms:

$\mathcal{V}(M) \subset \mathcal{V}$ (the set of variables of M):

$$\mathcal{V}(x) = \{x\} \qquad \forall x \in \mathcal{V},$$
$$\mathcal{V}(FM_1 \cdots M_n) = \bigcup_{i=1}^{n} \mathcal{V}(M_i) \qquad \forall F \in \mathcal{F}_n.$$

$\nu(M) = |\mathcal{V}(M)| \in \mathbf{N}$. If $\nu(M) = 0$ we say term M is a *closed* (or *ground*) term.

$\lambda(M) \geq 1$ (the *length* of M):

$$\lambda(x) = 1 \qquad \forall x \in \mathscr{V},$$
$$\lambda(FM_1 \cdots M_n) = 1 + \sum_{i=1}^{n} \lambda(M_i) \qquad \forall F \in \mathscr{F}_n.$$

$\theta(M) \geq 0$ (the *size* of M):

$$\theta(x) = 0 \qquad \forall x \in \mathscr{V},$$
$$\theta(FM_1 \cdots M_n) = 1 + \sum_{i=1}^{n} \theta(M_i) \qquad \forall F \in \mathscr{F}_n.$$

$\mu(M) = \lambda(M) - \nu(M)$. It is easy to show that $\mu(M) \geq \theta(M)$, which shows that $\mu(M) \geq 0$ & $\mu(M) = 0 \Leftrightarrow M \in \mathscr{V}$.

If $\mu(M) = \theta(M)$, we say that M is *linear*; this means that all variable occurrences in M are distinct.

We now formalize the notion of occurrence of a subterm in a term. Let N_+^* be the set of sequences of positive integers, Λ the empty sequence in N_+^*, and $\cdot$ the concatenation operation on sequences. We shall call the members of N_+^* *occurrences* and denote them u, v, w. We define the *prefix ordering* $\preceq$ in N_+^* by $u \preceq v \Leftrightarrow \exists w\ v = u \cdot w$; in this case we define $v/u = w$. Occurrences u and v are said to be *disjoint*, denoted $u \mid v$, iff $\neg u \preceq v$ and $\neg v \preceq u$. Finally, we let $u \prec v$ iff $u \preceq v$ and $u \neq v$.

For any $M \in \mathscr{T}$, we define its *set of occurrences* $\mathscr{O}(M) \subseteq N_+^*$ and the *subterm of M at u*, $M/u \in \mathscr{T}$, for $u \in \mathscr{O}(M)$, as follows.

(i) If $M = x \in \mathscr{V}$, then $\mathscr{O}(M) = \{\Lambda\}$ and $M/\Lambda = M$.
(ii) If $M = FM_1 \cdots M_n$, then $\mathscr{O}(M) = \{\Lambda\} \cup \{iu \mid i \leq n,\ u \in \mathscr{O}(M_i)\}$, $M/\Lambda = M$, and $M/iu = M_i/u$.

We say that u is *an occurrence of M/u in M*. (Note that our terminology extends the traditional one.)

Finally, for $M \in \mathscr{T}$, $u \in \mathscr{O}(M)$, and $N \in \mathscr{T}$, we define $M[u \leftarrow N] \in \mathscr{T}$ by

$$M[\Lambda \leftarrow N] = N,$$
$$(FM_1 \cdots M_n)[iu \leftarrow N] = FM_1 \cdots M_{i-1}(M_i[u \leftarrow N])M_{i+1} \cdots M_n, \qquad i \leq n.$$

These definitions are consistent with [33], and in the rest of the paper we shall make free use of the following proposition, which corresponds to Lemmas 4.6 and 4.7 in [33].

PROPOSITION 3.1

(1) $\forall M, N, P \in \mathscr{T}, u \in \mathscr{O}(M), v \in \mathscr{O}(N)$:

(a) $M[u \leftarrow N]/u \cdot v = N/v$, *embedding*;
(b) $M[u \leftarrow N][u \cdot v \leftarrow P] = M[u \leftarrow N[v \leftarrow P]]$, *associativity*.

(2) $\forall M, N, P \in \mathscr{T}, u, v \in \mathscr{O}(M)$, with $u \mid v$:

(a) $M[u \leftarrow N]/v = M/v$, *persistence*;
(b) $M[u \leftarrow N][v \leftarrow P] = M[v \leftarrow P][u \leftarrow N]$, *commutativity*.

(3) $\forall M, N, P \in \mathscr{T}, u, v \in \mathscr{O}(M)$, with $v \preceq u$:

(a) $M[u \leftarrow N]/v = (M/v)[u/v \leftarrow N]$, *distributivity*;
(b) $M[u \leftarrow N][v \leftarrow P] = M[v \leftarrow P]$, *dominance*.

Definitions. A *substitution* is a mapping σ from $\mathscr{V}$ to $\mathscr{T}$, with $\sigma(x) = x$ almost everywhere. Substitutions are denoted by σ, ρ, η. Substitutions are extended as morphisms of $\mathscr{T}$ by

$$\sigma(FM_1 \cdots M_n) = F\sigma(M_1) \cdots \sigma(M_n).$$

Bijective morphisms are called *permutations* and are denoted by ξ, ξ', ... Given a substitution σ, the finite set $\mathscr{D}(\sigma) = \{x \in \mathscr{V} \mid \sigma(x) \neq x\} \subset \mathscr{V}$ is called the *domain* of σ.

For $V \subset \mathscr{V}$, we define the restriction $\sigma \restriction V$ of σ to V as

$$(\sigma \restriction V)(x) = \begin{cases} \sigma(x) & \text{if } x \in V, \\ x & \text{otherwise.} \end{cases}$$

For all σ, M, and V,

$$\mathscr{V}(M) \subseteq V \Rightarrow \sigma(t) = (\sigma \restriction V)(M),$$

and $\mathscr{D}(\sigma) \cap \mathscr{V}(M) = \emptyset \Rightarrow \sigma(M) = M$.

We define the quasi-ordering $\leq$ of *subsumption* in $\mathscr{T}$ by

$$M \leq N \Leftrightarrow \exists \sigma\ N = \sigma(M).$$

It can be shown that if such a σ exists, $\sigma \restriction \mathscr{V}(M)$ is unique. We call it the *match of N by M*, and denote it by $N :: M$.

We define $M \equiv N \Leftrightarrow M \leq N \;\&\; N \leq M$. It can be shown that $M \equiv N$ iff there exists a permutation ξ such that $N = \xi(M)$. Note that ν, λ, and θ are preserved by $\equiv$. Finally, we define

$$M > N \Leftrightarrow N \leq M \;\&\; M \not\leq N.$$

PROPOSITION 3.2. *$>$ is a noetherian relation in $\mathscr{T}$.*

The proof of this proposition is given in [12] and consists in showing that $M > N \Rightarrow \mu(M) > \mu(N)$.

Let ϕ be any bijection between $\mathscr{T} \times \mathscr{T}$ and $\mathscr{V}$. We define a binary operation $\wedge$ in $\mathscr{T}$ inductively by

(i) $FM_1 \cdots M_n \wedge FN_1 \cdots N_n = F(M_1 \wedge N_1) \cdots (M_n \wedge N_n)\ \forall F \in \mathscr{F}_n$.
(ii) $M \wedge N = \phi(M, N)$ in all other cases.

$M \wedge N$ is uniquely determined from ϕ and, for distinct ϕ's, is unique up to $\equiv$.

PROPOSITION 3.3. *$M \wedge N$ is a g.l.b. of M and N under the subsumption quasi-ordering.*

Let $\hat{\mathscr{T}}$ be the quotient set $\mathscr{T}/\equiv$, completed with a maximum element $\top$. From Propositions 3.2 and 3.3 there follows directly:

THEOREM 3.1. *$\hat{\mathscr{T}}$ is a complete lattice.*

The proof of Proposition 3.3, of Theorem 3.1 and various other results concerning the structure of $\mathscr{T}$, and of its completion by infinite terms, may be found in [12]. See also [29] and [31] for similar constructions.

A direct consequence of Theorem 3.1 is the existence, for any two terms M and N that have a common instance (i.e., such that $\exists \sigma, \sigma'\ \sigma(M) = \sigma'(N)$) of an l.u.b. $M \vee N$, which is a most general such instance. The term $M \vee N$ is unique modulo $\equiv$ and may be found by the *unification algorithm* [32]. Efficient ways of unifying terms are described in [12, 25]. If such an l.u.b. exists, we write $M \nabla N$ and say that M and N are *unifiable*.

We shall need in the next sections the following propositions, whose proofs are omitted here.

PROPOSITION 3.4. $\mathscr{O}(\sigma(M)) = \mathscr{O}(M) \cup \bigcup_{M/u=x} \{u \cdot v \mid v \in \mathscr{O}(\sigma(x))\}$.

$$\forall u \in \mathscr{O}(M), \quad \begin{cases} \textit{if}\ \ M/u = N \notin \mathscr{V}, & \textit{then}\ \ \sigma(M)/u = \sigma(N), \\ \textit{if}\ \ M/u = x \in \mathscr{V}, & \textit{then}\ \ \sigma(M)/u \cdot v = \sigma(x)/v \quad \forall v \in \mathscr{O}(\sigma(x)). \end{cases}$$

PROPOSITION 3.5. $\forall M, N \in \mathscr{T}, \forall u \in \mathscr{O}(M), \sigma(M)[u \leftarrow \sigma(N)] = \sigma(M[u \leftarrow N])$.

3.2 TERM REWRITING SYSTEMS AND CRITICAL PAIRS

Definition. We call *a term rewriting system* any set $\mathscr{R}$ of pairs of terms $\langle \alpha \rightarrow \beta \rangle$, such that $\mathscr{V}(\beta) \subseteq \mathscr{V}(\alpha)$.

We say that u is a *redex occurrence of $\mathscr{R}$ in term M* iff $u \in \mathscr{O}(M)$ and $\exists \langle \alpha \rightarrow \beta \rangle \in \mathscr{R}$

such that $\alpha \le M/u$. Taking $\sigma = (M/u)::\alpha$ and $N = M[u \leftarrow \sigma(\beta)]$, we say that M *reduces to* N *in* u, and we write $M \underset{\mathscr{R}}{\rightarrow} N$.

Example. Let $\mathscr{R} = \{\langle Ix \rightarrow x\rangle\}$, with $a(I) = 1$. We have $IIx \underset{\mathscr{R}}{\rightarrow} Ix$ in two possible ways, with redex occurrence Λ or 1.

Definition. Let $\rightarrow$ be a relation over $\mathscr{T}$. We say that $\rightarrow$ is

(i) *stable* iff $\forall\sigma, \forall M, N, M \rightarrow N \Rightarrow \sigma(M) \rightarrow \sigma(N)$;
(ii) *compatible* iff $\forall P \in \mathscr{T}, \forall u \in \mathscr{O}(P), \forall M, N, M \rightarrow N \Rightarrow P[u \leftarrow M] \rightarrow P[u \leftarrow N]$.

It is easy to show, using Propositions 3.1 and 3.4, that $\underset{\mathscr{R}}{\rightarrow}$ is the smallest compatible stable relation containing $\mathscr{R}$.

Term rewriting systems are a general model of computation. They generalize to arbitrary algebras the semi-Thue systems in free monoids.

PROPOSITION 3.6. *Let $\rightarrow$ be any compatible relation in $\mathscr{T}$, and let σ and σ' be substitutions such that*

$$\sigma(x) \rightarrow \sigma'(x),$$
$$\sigma(y) = \sigma'(y) \qquad \forall y \ne x.$$

Let M be any term, and let $u_1, \ldots, u_n \in \mathscr{O}(M)$ be all the occurrences of x in M (assumed to be distinct). Defining $M_0 = \sigma(M)$ and $M_i = M_{i-1}[u_i \leftarrow \sigma'(x)]$ $(1 \le i \le n)$, we have

$$M_i \xrightarrow{n-1} \sigma'(M) \ (0 \le i \le n).$$

PROOF. Using Proposition 3.4 we show that $M_i/u_i = \sigma(x)$, and therefore $\forall i\ 0 \le i \le n$ $M_i \rightarrow M_{i+1}$. We then show that $M_n = \sigma'(M)$ by an induction on M, using the compatibility of $\rightarrow$. $\square$

We now describe a superposition algorithm, used to define critical pairs of terms in a term rewriting system. This algorithm is taken from Knuth and Bendix [16].

Superposition Algorithm. Let $\langle\alpha_1 \rightarrow \beta_1\rangle, \langle\alpha_2 \rightarrow \beta_2\rangle \in \mathscr{R}$ and $u \in \mathscr{O}(\alpha_1)$ such that $M = \alpha_1/u \notin \mathscr{V}$ and $M \nabla \alpha_2$. Let $N \equiv M \vee \alpha_2$ such that $\mathscr{V}(N) \cap \mathscr{V}(\alpha_1) = \varnothing$. We say that the superposition of $\langle\alpha_2 \rightarrow \beta_2\rangle$ on $\langle\alpha_1 \rightarrow \beta_1\rangle$ in u determines the *critical pair* $\langle P, Q\rangle$, defined by

$$P = \sigma_1(\alpha_1)[u \leftarrow \sigma_2(\beta_2)],$$
$$Q = \sigma_1(\beta_1),$$

where $\sigma_1 = N::M$ and $\sigma_2 = N::\alpha_2$. In words, this means that we match in the most general way the left-hand side of some rule with a nonvariable subterm of another (or the same) left-hand side. The critical pair consists of the two ways in which the common instance reduces by the two rules.

Remark. For any $\langle\alpha_1 \rightarrow \beta_1\rangle$, $\langle\alpha_2 \rightarrow \beta_2\rangle$, and u, the critical pair is unique up to a permutation. We may choose $\langle\alpha_2 \rightarrow \beta_2\rangle = \langle\alpha_1 \rightarrow \beta_1\rangle$, as in Example (c) below, but in this case (and in this case only) we shall not consider the case $u = \Lambda$, which gives only trivial critical pairs $\langle P, P\rangle$.

Examples. For convenience we use parentheses in the terms of our examples.

(a) $\alpha_1 = F(x, G(x, A))$, $\beta_1 = H(x)$, $\alpha_2 = G(B, x)$, $\beta_2 = K(x)$ with $u = 2$ determine the pair $P = F(B, K(A))$, $Q = H(B)$.
(b) $\alpha_1 = F(x, H(x'))$, $\beta_1 = K(x', x)$, $\alpha_2 = H(G(x, x'))$, $\beta_2 = L(x, x')$ with $u = 2$ determine $P = F(x, L(y, z))$, $Q = K(G(y, z), x)$.
(c) $\alpha_1 = \alpha_2 = H(H(x))$, $\beta_1 = \beta_2 = K(x)$ with $u = 1$ determine $P = H(K(y))$, $Q = K(H(y))$.

Remark. The condition $\mathscr{V}(N) \cap \mathscr{V}(\alpha_1) = \varnothing$ may be replaced by the weaker condition $\mathscr{V}(N) \cap (\mathscr{V}(\alpha_1) - \mathscr{V}(M)) = \varnothing$. Example (b) shows why this condition is necessary: choosing the pair $\langle F(x, L(x, x')), K(G(x, x'), x)\rangle$ would be strictly less general than the pair $\langle P, Q\rangle$. If we compute N by unification of M and $\xi(\alpha_2)$, where ξ is a permutation renaming variables in $\mathscr{V}(\alpha_1) \cap \mathscr{V}(\alpha_2)$, we get $\mathscr{V}(N) \subseteq (\mathscr{V}(M) \cup \mathscr{V}(\xi(\alpha_2)))$, and the condition above is thus satisfied.

PROPOSITION 3.7. *Let $\langle \alpha_1 \to \beta_1\rangle$, $\langle \alpha_2 \to \beta_2\rangle \in \mathscr{R}$ and $u \in \mathcal{O}(\alpha_1)$ such that $M = \alpha_1/u \notin \mathscr{V}$ and there exist σ_1 and σ_2 such that $\sigma_1(M) = \sigma_2(\alpha_2)$. Then there exist a critical pair $\langle P, Q\rangle$ of $\mathscr{R}$ and a substitution ρ such that $\sigma_1(\alpha_1)[u \leftarrow \sigma_2(\beta_2)] = \rho(P)$ and $\sigma_1(\beta_1) = \rho(Q)$.*

PROOF. We know that $M \nabla \alpha_2$. Let $N \equiv M \vee \alpha_2$ such that $\mathscr{V}(N) \cap \mathscr{V}(\alpha_1) = \varnothing$, and let $\sigma = N::M$, $\sigma' = N::\alpha_2$, as determined by the superposition algorithm, which constructs a critical pair $\langle P, Q\rangle$ with $P = \sigma(\alpha_1)[u \leftarrow \sigma'(\beta_2)]$ and $Q = \sigma(\beta_1)$.

We consider substitutions $\eta = \sigma_2(\alpha_2)::N = \sigma_1(M)::N$ and $\rho = [\eta \restriction \mathscr{V}(N)] \cup [\sigma_1 \restriction \mathscr{V}(\alpha_1)]$. (This is meaningful, since $\mathscr{V}(N) \cap \mathscr{V}(\alpha_1) = \varnothing$.) By construction we have $\sigma_1(M) = \eta(\sigma(M))$, and therefore

(i) $\forall x \in \mathscr{V}(M)\ \sigma_1(x) = \eta(\sigma(x)) = \rho(\sigma(x))$ because $\mathscr{V}(\sigma(x)) \subseteq \mathscr{V}(N)$.

(ii) $\forall x \in \mathscr{V}(\alpha_1) - \mathscr{V}(M)\ \sigma(x) = x$ because $\mathscr{D}(\sigma) \subseteq \mathscr{V}(M)$, and $\rho(x) = \sigma_1(x)$ by definition of ρ.

Therefore

$$\forall x \in \mathscr{V}(\alpha_1)\ \sigma_1(x) = \rho(\sigma(x)). \tag{1}$$

Similarly, $\sigma_2(\alpha_2) = \eta(\sigma'(\alpha_2))$ gives

$$\forall x \in \mathscr{V}(\alpha_2)\ \sigma_2(x) = \eta(\sigma'(x)) = \rho(\sigma'(x)). \tag{2}$$

Since $\mathscr{V}(\beta_1) \subseteq \mathscr{V}(\alpha_1)$ and $\mathscr{V}(\beta_2) \subseteq \mathscr{V}(\alpha_2)$, we get

$$\begin{aligned} \sigma_1(\beta_1) &= \rho(\sigma(\beta_1)) && \text{by (1)} \\ &= \rho(Q), \end{aligned}$$

and

$$\begin{aligned} \sigma_1(\alpha_1)[u \leftarrow \sigma_2(\beta_2)] &= \rho(\sigma(\alpha_1))[u \leftarrow \rho(\sigma'(\beta_2)) && \text{by (1) and (2)} \\ &= \rho(P) && \text{by Proposition 3.5.} \end{aligned}$$ □

We are interested in critical pairs because of the next lemma, which shows that the test for local confluence may be restricted to critical pairs.

From now on we shall generally abbreviate $\underset{\mathscr{R}}{\to}$ by $\to$. As in Section 2, we use the notation $M \downarrow N$ for $\exists P\ M \xrightarrow{*} P\ \&\ N \xrightarrow{*} P$.

LEMMA 3.1. *The relation $\underset{\mathscr{R}}{\to}$ is locally confluent iff for every critical pair $\langle P, Q\rangle$ of $\mathscr{R}$* we have $P \downarrow Q$.

PROOF. Using the notation of the superposition algorithm, a critical pair $\langle P, Q\rangle$ is such that $\sigma_1(\alpha_1) \to P$ and $\sigma_1(\alpha_1) \to Q$, which shows the "only if" part.

For the "if" part, assume that for every critical pair $\langle P, Q\rangle$ of $\mathscr{R}$ we have $P \downarrow Q$. Let M be an arbitrary term, with $M \to N_1$ and $M \to N_2$; i.e., $\exists u_1, u_2 \in \mathcal{O}(M)$, $\exists \langle \alpha_1 \to \beta_1\rangle$, $\langle \alpha_2 \to \beta_2\rangle \in \mathscr{R}$, and $\exists \sigma_1, \sigma_2$ such that $M/u_1 = \sigma_1(\alpha_1)$, $M/u_2 = \sigma_2(\alpha_2)$, $N_1 = M[u_1 \leftarrow \sigma_1(\beta_1)]$, and $N_2 = M[u_2 \leftarrow \sigma_2(\beta_2)]$.

There are two cases, according to the relative positions of the two redex occurrences.

Case 1. Disjoint redexes: $u_1 | u_2$. We then have $N_1/u_2 = \sigma_2(\alpha_2)$ by persistence, and similarly, $N_2/u_1 = \sigma_1(\alpha_1)$. Furthermore, we have $\bar{M} = N_1[u_2 \leftarrow \sigma_2(\beta_2)] = N_2[u_1 \leftarrow \sigma_1(\beta_1)]$ by commutativity, and therefore $N_1 \to \bar{M}$ and $N_2 \to \bar{M}$.

Case 2. Prefix redexes. Let us assume, without loss of generality, that $u_1 \leq u_2$. Let $v = u_2/u_1$. By cancellation we get $\sigma_1(\alpha_1)/v = \sigma_2(\alpha_2)$, and by distributivity we get $N_2/u_1 = \sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)]$.

Let us show that there exists $\bar{M}$ such that $\sigma_1(\beta_1) \xrightarrow{*} \bar{M}$ and $N_2/u_1 \xrightarrow{*} \bar{M}$. It will then follow that $N_1 \downarrow N_2$, by compatibility of $\to$.

According to Proposition 3.4, there are two cases.

2a. $\nu = \nu_1 \cdot \nu_2$, $\alpha_1/\nu_1 = x \in \mathscr{V}$, $\sigma_2(\alpha_2) = \sigma_1(x)/\nu_2$. Let us consider the substitution σ_1' defined by

$$\sigma_1'(x) = \sigma_1(x)[\nu_2 \leftarrow \sigma_2(\beta_2)],$$
$$\sigma_1'(y) = \sigma_1(y) \qquad \forall y \neq x,$$

and let $\bar{M} = \sigma_1'(\beta_1)$. We have $\sigma_1(x) \rightarrow \sigma_1'(x)$, and by Proposition 3.6 we get $\sigma_1(\beta_1) \xrightarrow{*} \bar{M}$ and $\sigma_1(\alpha_1)[\nu \leftarrow \sigma_2(\beta_2)] \xrightarrow{*} \sigma_1'(\alpha_1)$. Since $\rightarrow$ is stable, we get $\sigma_1'(\alpha_1) \rightarrow \bar{M}$, which concludes the proof of case 2a.

2b. $\alpha_1/\nu \notin \mathscr{V}$, $\sigma_2(\alpha_2) = \sigma(\alpha_1/\nu)$. Using Proposition 3.7, there exist a critical pair $\langle P, Q\rangle$ and a substitution ρ such that

$$\sigma_1(\alpha_1)[\nu \leftarrow \sigma_2(\beta_2)] = \rho(P) \qquad \text{and} \qquad \sigma_1(\beta_1) = \rho(Q).$$

By hypothesis, there exists R such that $P \xrightarrow{*} R$ and $Q \xrightarrow{*} R$. We may choose $\bar{M} = \rho(R)$, and the result follows by the stability of $\rightarrow$. $\square$

Remark. Lemma 3.1 is inspired by Knuth and Bendix [16], but our proof, unlike theirs, does not require $\rightarrow$ to be noetherian.

Example. Let $\mathscr{R}$ be $\{\langle F(x) \rightarrow A\rangle, \langle F(x) \rightarrow G(F(x))\rangle, \langle G(F(x)) \rightarrow F(H(x))\rangle, \langle G(F(x)) \rightarrow B\rangle\}$. We leave it to the reader to check that for every critical pair $\langle P, Q\rangle$ of $\mathscr{R}$ we have $P \downarrow Q$. Therefore $\rightarrow$ is locally confluent. However, $\rightarrow$ is not confluent, since it is not noetherian. Actually, note that the diagram of reductions from $F(x)$ using $\mathscr{R}$ is identical to Figure 6a. In the case of noetherian relations we get the following theorem, essentially identical to the corollary to Theorem 5 of [16].

THEOREM 3.2. *Let $\mathscr{R}$ be a term rewriting system such that $\xrightarrow[\mathscr{R}]{}$ is noetherian. Let $\hat{M}$ denote an arbitrary $\xrightarrow[\mathscr{R}]{}$-normal form of M, for $M \in \mathscr{T}$. Then $\xrightarrow[\mathscr{R}]{}$ is confluent iff for every critical pair $\langle P, Q\rangle$ of $\mathscr{R}$ we have $\hat{P} = \hat{Q}$.*

PROOF

$\Rightarrow$. For any critical pair $\langle P, Q\rangle$ of $\mathscr{R}$, $\exists M\ M \rightarrow P \ \&\ M \rightarrow Q$. If $\rightarrow$ is confluent, then by Lemma 2.2 the term M admits a unique $\rightarrow$-normal form $\hat{P} = \hat{Q}$.

$\Leftarrow$. $\hat{P} = \hat{Q}$ implies $P \downarrow Q$, and $\rightarrow$ is locally confluent by Lemma 3.1 and therefore confluent by Lemma 3.4. $\square$

Remark. If $\rightarrow$ is noetherian, we may get $\hat{M}$ from M by an arbitrary sequence of rewritings using rules in $\mathscr{R}$, termination being guaranteed. Theorem 3.2 gives us in this case an effective way of testing the confluence of $\rightarrow$, provided we have only a finite number of critical pairs $\langle P, Q\rangle$. This will happen in particular when $\mathscr{R}$ is finite.

Examples

(a) Let $\mathscr{R} = \{\langle H(H(x)) \rightarrow K(x)\rangle\}$. As we saw in Example (c) above, we have a critical pair $P = H(K(y))$, $Q = K(H(y))$. Since P and Q are distinct $\rightarrow$-normal forms, $\mathscr{R}$ is not a confluent system.

(b) If we form $\mathscr{R}'$ by adding to $\mathscr{R}$ above the rule $\langle H(K(x)) \rightarrow K(H(x))\rangle$, we now have $\hat{P} = \hat{Q} = K(H(y))$. A new critical pair appears by superposition of the two rules $P' = H(K(H(y)))$ and $Q' = K(K(y))$. But $P' \rightarrow K(H(H(y))) \rightarrow K(K(y)) = Q'$. $\mathscr{R}'$ being noetherian (we shall discuss this problem below), we have shown that it is confluent.

(c) Group theory. Let

$$\begin{aligned}\mathscr{R} = \{&\langle F(E, x) \rightarrow x\rangle, \langle F(I(x), x) \rightarrow E\rangle, \langle I(E) \rightarrow E\rangle,\\ &\langle F(F(x, y), z) \rightarrow F(x, F(y, z))\rangle, \langle F(I(x), F(x, y)) \rightarrow y\rangle,\\ &\langle F(x, E) \rightarrow x\rangle, \langle I(I(x)) \rightarrow x\rangle, \langle F(x, I(x)) \rightarrow E\rangle,\\ &\langle F(x, F(I(x), y)) \rightarrow y\rangle, \langle I(F(x, y)) \rightarrow F(I(y), I(x))\rangle\}.\end{aligned}$$

We leave it to the reader to show that for all critical pairs $\langle P, Q\rangle$ we have $\hat{P} = \hat{Q}$. We show below that $\mathscr{R}$ is noetherian. $\mathscr{R}$ is therefore a confluent system. This example is taken from [16].

Proving $\mathscr{R}$ Noetherian. The main difficulty in using Theorem 3.2 consists in showing $\rightarrow$ to be noetherian. For that one must find a noetherian, stable, compatible strict partial order $\rhd$ such $\alpha \rhd \beta$ for every $\langle \alpha \rightarrow \beta\rangle$ in $\mathscr{R}$. Knuth and Bendix [16] propose a tricky lexicographic ordering for this purpose. Providing the user specifies integer weights to the function symbols, this test can be completely mechanized. Further studies of these orderings are given in [2, 7, 27, 28].

More generally, this problem is equivalent to finding some interpretation χ of our term language over some well-founded domain $\langle \mathscr{D}, <_{\mathscr{D}}\rangle$, such that for every F in $\mathscr{F}$, $\chi(F)$ is monotone increasing in each of its arguments. To prove $\rightarrow$ noetherian, we have to show that for every $\langle \alpha \rightarrow \beta\rangle$ in $\mathscr{R}$, $\chi(\beta) <_{\mathscr{D}} \chi(\alpha)$ is identically true for every assignment of $\chi(x_i)$ in $\mathscr{D}$. This method was proposed by Manna and Ness in [22] and used by Lankford in [17] (where $\chi(F)$ were polynomials over $\mathbf{N}$). For instance, the ten group reductions of Example (c) above may be shown to be noetherian using the interpretation

$$\begin{aligned} \chi(F) &= \lambda xy \cdot x(1 + 2y), \\ \chi(I) &= \lambda x \cdot x^2, \\ \chi(E) &= 2, \end{aligned}$$

over integers greater than 1.

Another method is given in [21]. The general problem of showing that $\mathscr{R}$ is noetherian is shown in [13] to be undecidable of order O'', even for terms restricted to monadic function symbols, but to be decidable for ground systems (i.e., such that $\mathscr{V}(\alpha) = \mathscr{V}(\beta) = \varnothing$ for every $\langle \alpha \rightarrow \beta\rangle$ in $\mathscr{R}$).

Completing $\mathscr{R}$ to a Confluent System. Theorem 3.2 also gives hints on how to complete $\mathscr{R}$ to a confluent system when it is not: the idea is to include in $\mathscr{R}$, for every $\langle P, Q\rangle$ such that $\hat{P} \neq \hat{Q}$, either $\langle P \rightarrow Q\rangle$, $\langle Q \rightarrow P\rangle$, or $\langle P \rightarrow M\rangle$ and $\langle Q \rightarrow M\rangle$ for some term M. Of course, one must show that the new pairs preserve termination, and there is no guarantee that the "completing" process will terminate. We shall not explain further the details of the method, which is explained in [16] and illustrated by numerous examples. Note that if we consider $\mathscr{R}$ as an equational theory, the critical pairs are consequences of the original axioms. Moreover, they usually turn out to be very useful lemmas. For instance, note that in Example (a) above we know in one step that H and K must commute, from the assumption that K is the square of H. This makes this completing procedure a very efficient semidecision procedure for equational theories in the cases where it applies. If the procedure terminates, it may be viewed as the compilation of a decision procedure from the axioms of an equational theory. For instance, Knuth and Bendix mechanically generate the set $\mathscr{R}$ of Example (c) above from the three group axioms $F(E, x) = x$, $F(I(x), x) = E$, and $F(F(x, y), z) = F(x, F(y, z))$. Now $M = N$ is a consequence of these axioms if and only if $\hat{M}$ is identical to $\hat{N}$, where $\hat{M}$ is obtained from M by an arbitrary sequence of rewritings using rules of $\mathscr{R}$, until none applies.

This method may be considered as the theoretical justification of earlier methods for mechanizing equality theorem proving [8, 11]. It is further explored in [2, 17], and related methods are considered in [35]. We give an extension of this method in Section 3.4.

3.3 Linear Term Rewriting Systems. We are now going to give sufficient conditions for confluence that do not depend on termination conditions. The idea is to impose on critical pairs $\langle P, Q\rangle$ of $\mathscr{R}$ a condition stronger than $P \downarrow Q$, inspired by the strong confluency condition.

Definition. A term rewriting system $\mathscr{R}$ is *strongly closed* iff, for every critical pair $\langle P, Q\rangle$ of $\mathscr{R}$, there exist R and S such that $P \xrightarrow[\mathscr{R}]{*} R \xleftarrow[\mathscr{R}]{\epsilon} Q$ and $P \xrightarrow[\mathscr{R}]{\epsilon} S \xleftarrow[\mathscr{R}]{*} Q$. Note that this condition alone is not sufficient to ensure confluence, as shown by the counterexample

$\mathscr{R} = \{\langle F(x, x) \to A\rangle, \langle F(x, G(x)) \to B\rangle, \langle C \to G(C)\rangle\}$, since the term $F(C, C)$ possesses two distinct normal forms A and B. Note that $\mathscr{R}$ has no critical pair, since $F(x, x) \not\uparrow F(x, G(x))$. Note that the diagram of reductions of $F(C, C)$ is identical to Figure 6a. Another interesting counterexample is due to Barendregt, simplifying a result of Klop [15], namely, $\mathscr{R} = \{\langle F(x, x) \to A\rangle, \langle G(x) \to F(x, G(x))\rangle, \langle C \to G(C)\rangle\}$, since $G(C) \xrightarrow{*} A$ and $G(C) \xrightarrow{*} G(A)$, but $A \not\downarrow G(A)$, although here the normal form of every term, when it exists, is unique.

Both of these systems contain nonlinear terms, which motivates the following definition.

Definition. We say that $\mathscr{R}$ is *left linear* (respectively, *right linear*) iff $\forall\langle\alpha \to \beta\rangle \in \mathscr{R}$ α (respectively, β) is linear.

LEMMA 3.2. *If $\mathscr{R}$ is a left- and right-linear strongly closed term rewriting system, $\xrightarrow[\mathscr{R}]{}$ is strongly confluent.*

PROOF. Let us assume that $\mathscr{R}$ is left and right linear and strongly closed, and let us abbreviate $\xrightarrow[\mathscr{R}]{}$ by $\to$.

Let $M \xrightarrow[\mathscr{R}]{} N_1$ and $M \to N_2$; i.e., $\exists u_1, u_2 \in \mathcal{O}(M)$, $\langle\alpha_1 \to \beta_1\rangle$, $\langle\alpha_2 \to \beta_2\rangle \in \mathscr{R}$, and substitutions σ_1 and σ_2 such that $M/u_1 = \sigma_1(\alpha_1)$, $N_1 = M[u_1 \leftarrow \sigma_1(\beta_1)]$, $M/u_2 = \sigma_2(\alpha_2)$, and $N_2 = M[u_2 \leftarrow \sigma_2(\beta_2)]$. We show that there exist N_3 and N_4 such that $N_1 \xrightarrow{*} N_3 \xleftarrow{\epsilon} N_2$ and $N_1 \xrightarrow{\epsilon} N_4 \xleftarrow{*} N_2$.

There are two cases, according to the relative positions of redex occurrences u_1 and u_2; the proof is similar to that of Lemma 3.1.

Case 1. Disjoint redexes: $u_1 | u_2$. We take

$$N_3 = N_4 = N_1[u_2 \leftarrow \sigma_2(\beta_2)] = N_2[u_1 \leftarrow \sigma_1(\beta_1)].$$

Case 2. Prefix redexes. Let us assume, without loss of generality, that $u_1 \leq u_2$. Let $v = u_2/u_1$. We have $\sigma_2(\alpha_2) = \sigma_1(\alpha_1)/v$ and $N_2 = M[u_1 \leftarrow \sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)]]$.

2a. $\sigma_2(\alpha_2)$ is completely introduced by σ_1; *i.e.*, $\exists v_1, v_2$ $v = v_1 \cdot v_2$, $\alpha_1/v_1 = x \in \mathscr{V}$, $\sigma_1(x)/v_2 = \sigma_2(\alpha_2)$. We define a substitution σ_3 by

$$\sigma_3(x) = \sigma_1(x)[v_2 \leftarrow \sigma_2(\beta_2)],$$
$$\sigma_3(y) = \sigma_1(y) \qquad \forall y \neq x,$$

and we take $N_3 = N_4 = M[u_1 \leftarrow \sigma_3(\beta_1)]$.

Since $\mathscr{R}$ is left linear, x occurs in α_1 only in occurrence v_1, and we get

$$\begin{aligned}\sigma_3(\alpha_1) &= \sigma_1(\alpha_1)[v_1 \leftarrow \sigma_3(x)] = \sigma_1(\alpha_1)[v_1 \leftarrow \sigma_1(x)[v_2 \leftarrow \sigma_2(\beta_2)]] \\ &= \sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)],\end{aligned}$$

whence $N_2 = M[u_1 \leftarrow \sigma_3(\alpha_1)]$, which shows $N_2 \to N_3$. There are again two cases.

(i) $x \notin \mathscr{V}(\beta_1)$. Then trivially $\sigma_3(\beta_1) = \sigma_1(\beta_1)$, and therefore $N_3 = N_1$.
(ii) $\exists w \in \mathcal{O}(\beta_1)$ $\beta_1/w = x$. Since $\mathscr{R}$ is right linear, w is the unique occurrence of x in β_1, and we get

$$\sigma_3(\beta_1) = \sigma_1(\beta_1)[w \leftarrow \sigma_1(x)[v_2 \leftarrow \sigma_2(\beta_2)]] = \sigma_1(\beta_1)[w \cdot v_2 \leftarrow \sigma_2(\beta_2)].$$

Since $\sigma_1(\beta_1)/w \cdot v_2 = \sigma_2(\alpha_2)$, we get $N_1 \to N_3$ using redex occurrence $u \cdot w \cdot v_2$.

2b. $\sigma_2(\alpha_2)$ partially exists in α_1; *i.e.*, $v \in \mathcal{O}(\alpha_1)$, $\alpha_1/v \notin \mathscr{V}$, $\sigma_1(\alpha_1/v) = \sigma_2(\alpha_2)$.

According to Proposition 3.7, there exist a critical pair $\langle P, Q\rangle$ and a substitution ρ such that

$$\rho(P) = \sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)] \qquad \text{and} \qquad \rho(Q) = \sigma_1(\beta_1),$$

and thus

$$N_1 = M[u_1 \leftarrow \rho(Q)] \qquad \text{and} \qquad N_2 = M[u_1 \leftarrow \rho(P)].$$

By the closure hypothesis, there exist R and S such that $P \xrightarrow{*} R \xleftarrow{\epsilon} Q$ and $P \xrightarrow{\epsilon} S \xleftarrow{*} Q$, and therefore we can take $N_3 = M[u_1 \leftarrow \rho(P)]$ and $N_4 = M[u_1 \leftarrow \rho(Q)]$. $\square$

Using Lemma 2.5, we get

COROLLARY. *If $\mathscr{R}$ is a left- and right-linear strongly closed system, $\underset{\mathscr{R}}{\rightarrow}$ is confluent.*

Example. Let

$$\mathscr{R} = \{\langle H(F(x, y)) \rightarrow F(H(R(x)), y)\rangle, \\ \langle F(x, K(y, z)) \rightarrow G(P(y), Q(z, x))\rangle, \\ \langle H(Q(x, y)) \rightarrow Q(x, H(R(y)))\rangle, \\ \langle Q(x, H(R(y))) \rightarrow H(Q(x, y))\rangle, \\ \langle H(G(x, y)) \rightarrow G(x, H(y))\rangle\}.$$

We have two critical pairs. First between the first two rules,

$$P = H(G(P(y), Q(z, x))), \qquad Q = F(H(R(x)), K(y, z)).$$

But, taking $R = G(P(y), H(Q(z, x)))$ and $S = G(P(y), Q(z, H(R(x))))$, we check that $P \rightarrow R \rightleftarrows S \leftarrow Q$.

Finally, between the next two rules we get

$$P' = H(H(Q(x, y))), \qquad Q' = Q(x, H(R(H(R(y))))),$$

and taking $T = H(Q(x, H(R(y))))$, we check that $P' \rightarrow T \leftarrow Q'$. This shows that $\mathscr{R}$ is strongly closed and therefore confluent. Note that it is not noetherian, since the rules 3 and 4 form a loop.

If $\mathscr{R}$ is only left linear, the condition "strongly closed" is not sufficient to ensure the confluence, as shown by the following counterexample due to J.J. Lévy:

$$\mathscr{R} = \{\langle F(A, A) \rightarrow G(B, B)\rangle, \langle A \rightarrow A'\rangle, \langle F(A', x) \rightarrow F(x, x)\rangle, \\ \langle F(x, A') \rightarrow F(x, x)\rangle, \langle G(B, B) \rightarrow F(A, A)\rangle, \langle B \rightarrow B'\rangle, \\ \langle G(B', x) \rightarrow G(x, x)\rangle, \langle G(x, B') \rightarrow G(x, x)\rangle\},$$

since $F(A', A') \overset{*}{\leftrightarrow} G(B', B')$ and $F(A', A') \downarrow G(B', B')$ is still false.

Still, it is very desirable to find sufficient conditions for a term rewriting system to be confluent that do not depend on right linearity, a rather unnatural condition. One way to do this is to change the closure condition, as we shall see. Let us first give some new definitions.

Definition. For any term rewriting system $\mathscr{R}$, we define a relation $\underset{\mathscr{R}}{\twoheadrightarrow}$ (parallel–disjoint reduction) as follows. Let $M \in \mathscr{T}$, and let $U = \{u_1, \ldots, u_n\}$ be a set of mutually disjoint redex occurrences of $\mathscr{R}$ in M: $\forall i \leq n\ M/u_i = \sigma_i(\alpha_i)$, $\langle \alpha_i \rightarrow \beta_i \rangle \in \mathscr{R}$, and $i \neq j \Rightarrow u_i | u_j$.

We define $N = M[u_i \leftarrow \sigma_i(\beta_i) | i \leq n]$ as the term $M[u_1 \leftarrow \sigma_1(\beta_1)] \cdots [u_n \leftarrow \sigma_n(\beta_n)]$. It is easy to show by commutativity that the order in which we reduce redexes is irrelevant. We say that *M reduces in parallel* to N, which we write $M \underset{\mathscr{R}}{\twoheadrightarrow} N$. It is easy to show that $\underset{\mathscr{R}}{\twoheadrightarrow}$ is the smallest reflexive relation containing $\underset{\mathscr{R}}{\rightarrow}$ and verifying

$$(*) \qquad M_1 \twoheadrightarrow N_1 \;\&\; \cdots \;\&\; M_n \twoheadrightarrow N_n \Rightarrow FM_1 \cdots M_n \twoheadrightarrow FN_1 \cdots N_n \quad \forall F \in \mathscr{F}_n.$$

Also $\twoheadrightarrow$ is stable, and $\underset{\mathscr{R}}{\overset{*}{\twoheadrightarrow}} = \underset{\mathscr{R}}{\overset{*}{\rightarrow}}$.

Let us now give two technical propositions.

PROPOSITION 3.8. *For any substitution σ and term M,*

$$\sigma(M) = M[u \leftarrow \sigma(x) | M/u = x \in \mathscr{V}].$$

PROPOSITION 3.9. *Let $\twoheadrightarrow$ be any reflexive relation verifying $(*)$. Let U be a set of disjoint occurrences in term M. Then*

$$\forall u \in U\ P_u \twoheadrightarrow Q_u \Rightarrow M[u \leftarrow P_u | u \in U] \twoheadrightarrow M[u \leftarrow Q_u | u \in U].$$

Propositions 3.8 and 3.9 are easily proved by induction on M.

Definition. A term rewriting system $\mathscr{R}$ is *parallel closed* iff for every critical pair $\langle P, Q\rangle$ of $\mathscr{R}$ we have $P \underset{\#}{\twoheadrightarrow} Q$.

LEMMA 3.3 *If $\mathscr{R}$ is a left-linear parallel closed term rewriting system, $\underset{\#}{\twoheadrightarrow}$ is strongly confluent.*

PROOF. We abbreviate $\underset{\#}{\twoheadrightarrow}$ as $\twoheadrightarrow$. Let $M \twoheadrightarrow N_1$ with set of redex occurrences U, and $M \twoheadrightarrow N_2$ with set V. Let $\bar{W} = \{u \in U | \exists v \in V\ v \leq u\} \cup \{v \in V | \exists u \in U\ u \leq v\}$ and $\bar{W} = [(U \cup V) - W] \cup (U \cap V)$.

W and $\bar{W}$ are two sets of mutually disjoint occurrences of M. We prove $\exists N\ N_1 \twoheadrightarrow N\ \&\ N_2 \twoheadrightarrow N$ by complete induction on $p(M, U, V) = \sum_{w \in W} \lambda(M/w)$. (We recall that $\lambda(M)$ is the length of M, as defined in Section 3.1.)

Part 1. Let u be any redex occurrence in $\bar{W}$. We may assume, without loss of generality, that $u \in U$. Let $V_u = \{u \in V | u \leq v\}$. We shall now show the existence of a term M_u such that $N_1/u \twoheadrightarrow M_u$ and $N_2/u \twoheadrightarrow M_u$.

Let $\langle \alpha \rightarrow \beta\rangle$ be the rule of $\mathscr{R}$ used in u in the parallel reduction U, with substitution σ: $M/u = \sigma(\alpha)$ and $N_1/u = \sigma(\beta)$. There are two cases.

Case 1. No v is critical in u; i.e., for all v in V_u we have $v/u = w \cdot w'$ with $\alpha/w = x \in \mathscr{V}$. (This covers the case $V_u = \varnothing$.) This case is illustrated in Figure 14.

Let x be any variable of α. Since the term α is linear by hypothesis, there is a unique $w \in \mathscr{O}(\alpha)$ such that $\alpha/w = x$. Let W' be the set of occurrences in $\sigma(x)$ of redex occurrences of V: $W' = \{v/u \cdot w | u \cdot w \leq v \in V_u\}$. Let $\langle \alpha_i, \beta_i\rangle$ be the rule of $\mathscr{R}$ corresponding to w_i' in the reduction V, with substitution σ_i: $\sigma(x)/w_i' = \sigma_i(\alpha_i)$.

We define the term $S_x = \sigma(x)[w_i' \leftarrow \sigma_i(\beta_i) | w_i' \in W']$. Doing this for every x in α, we now define a substitution σ' of domain $\mathscr{V}(\alpha)$ by $\sigma'(x) = S_x\ \forall x \in \mathscr{V}(\alpha)$. By construction we have $\sigma(x) \twoheadrightarrow S_x$, and therefore $\sigma(\beta) \twoheadrightarrow \sigma'(\beta)$, using Propositions 3.8 and 3.9. Also, using Proposition 3.8, we have $N_2/u = \sigma'(\beta)$. We may therefore choose $M_u = \sigma'(\beta)$.

Case 2. Let v_1 in V_u be critical in u; i.e., $\alpha/w \notin \mathscr{V}$, with $w = v_1/u$. Let $\langle \alpha_1 \rightarrow \beta_1\rangle$ be the rule of $\mathscr{R}$ corresponding to v_1 in the reduction V, with substitution σ_1. Using Proposition 3.7, there exist a critical pair $\langle P, Q\rangle$ of $\mathscr{R}$ and a substitution ρ such that $N_1/u = \rho(Q)$ and $\hat{M} = M/u[w \leftarrow \sigma_1(\beta_1)] = \rho(P)$.

By the closure hypothesis $P \twoheadrightarrow Q$ and by the stability of $\twoheadrightarrow$ we get $\hat{M} \twoheadrightarrow N_1/u$. Let $\hat{W}$ be the set of redex occurrences of $\hat{M}$ in this reduction. We have also $\hat{M} \twoheadrightarrow N_2/u$, using the set of redex occurrences $V' = \{v/u | v \in V_u - \{v_1\}\}$.

Now let $p' = \sum_{v' \in V'} \lambda(M/u \cdot v')$ We have $p(\hat{M}, V', \hat{W}) \leq p'$ by cases on the relative positions of occurrences in V' and $\hat{W}$. The four cases are shown in Figure 15, where the contribution to $p(\hat{M}, V', \hat{W})$ (respectively, p') is the shaded surface in Figure 15a (respectively, 15b).

Because $\lambda(M/v_1) > 0$, we have $p' < \sum_{v \in V_u} \lambda(M/v) \leq p(M, U, V)$, since $V_u \subseteq W$. Therefore $p(\hat{M}, V', \hat{W}) < p(M, U, V)$, and we may use the induction hypothesis, showing the existence of M_u.

Part 2. We now consider $\bar{M} = M[u \leftarrow M_u | u \in \bar{W}]$. Since $\bar{W}$ dominates all the occurrences in U, we have $N_1 = M[u \leftarrow N_1/u | u \in \bar{W}]$, and similarly for N_2. Using Proposition 3.9 we get $N_1 \twoheadrightarrow \bar{M}$ and $N_2 \twoheadrightarrow \bar{M}$, which concludes the proof $\square$

Using Lemma 2.5 and the fact that $\overset{*}{\twoheadrightarrow} = \overset{*}{\rightarrow}$, we get

COROLLARY. *Any left-linear parallel closed term rewriting system is confluent.*

This result is important in practice. It can be used, for instance, to show the consistency of operational semantics for recursive programming languages. It is the generalization to schemata of the main theorem of Rosen [33], which applies only to ground terms (no variables), and which requires the stronger closure condition $\langle P \rightarrow Q\rangle \in \mathscr{R}$. Note that

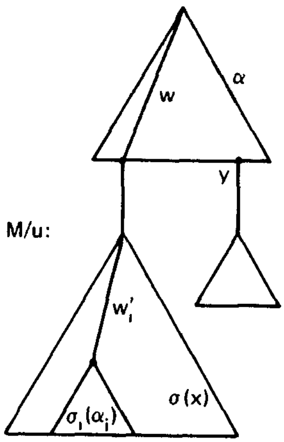


Figure 14

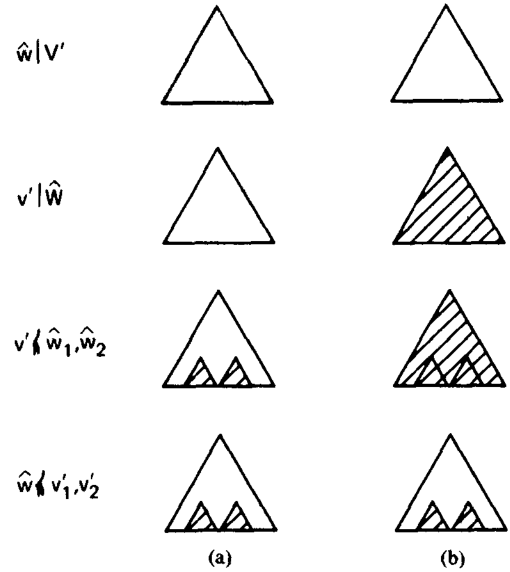


Figure 15

Rosen's Theorem 6.5 gives only a very particular case of Lemma 3.3 (no critical pairs). Computations in left-linear term rewriting systems with no critical pairs are further studied in [14].

Examples

(a) Combinatory logic. The reduction rules of the combinators S and K may be expressed by the following term rewriting system, with A denoting the application operator:

$$\begin{aligned}\mathscr{R} = \{&\langle A(A(A(S, x), y), z)) \to A(A(x, y), A(y, z))\rangle, \\ &\langle A(A(K, x), y) \to x\rangle\}.\end{aligned}$$

Because of the first rule, $\mathscr{R}$ is neither right linear nor noetherian (for instance, the term $A(A(M, M), M)$, with $M = A(A(S, S), S)$ does not admit a normal form). Still, the confluence of $\mathscr{R}$ is immediate, since it is left linear and there are no critical pairs.

The same argument applies to show the consistency of operational semantics for recursive program schemes.

(b) Let

$$\begin{aligned}\mathscr{R} = \{&\langle F(G(x, A, B)) \to x\rangle, \\ &\langle G(F(H(C, D)), x, y) \to H(K_1(x), K_2(y))\rangle, \\ &\langle K_1(A) \to C\rangle, \langle K_2(B) \to D\rangle\}.\end{aligned}$$

The system $\mathscr{R}$ is left linear, and there is only one critical pair $\langle P, Q\rangle$, with $P = F(H(K_1(A), K_2(B)))$ and $Q = F(H(C, D))$. Since $P \twoheadrightarrow Q$, the system $\mathscr{R}$ is confluent.

3.4 CONFLUENT EQUATIONAL THEORIES. We shall now use the results of Section 2.3 to extend the applicability of Lemma 3.1.

We suppose that we are interested in an equational first-order theory defined by a set of equational axioms $\mathscr{A} \subset \mathscr{T}^2$. We assume that the rules of inference of substitution of terms for free variables and of replacement of equals are valid. We write $\mathscr{A} \vdash M = N$ iff $M = N$ can be deduced from $\mathscr{A}$ using these rules.

Let us now partition $\mathscr{A}$ into $\mathscr{R} \cup \mathscr{E}$, where $\mathscr{R}$ and $\mathscr{E}$ verify

$$\begin{aligned}&\forall\langle\alpha \to \beta\rangle \in \mathscr{R} \quad \mathscr{V}(\beta) \subseteq \mathscr{V}(\alpha), \\ &\forall\langle\alpha = \beta\rangle \in \mathscr{E} \quad \mathscr{V}(\beta) = \mathscr{V}(\alpha).\end{aligned}$$

We shall use $\mathcal{R}$ as a term rewriting system, defining $\underset{\mathcal{R}}{\rightarrow}$ as above, and $\mathcal{E}$ as a *symmetric* term rewriting system, defining the symmetric relation $\underset{\mathcal{E}}{\vdash\!\dashv} = \underset{\mathcal{E}}{\rightarrow} \cup \underset{\mathcal{E}}{\rightarrow}^{-1}$. Note that because of the condition on variables in equations of $\mathcal{E}$, we have $\underset{\mathcal{E}}{\rightarrow}^{-1} = \underset{\mathcal{E}^{-1}}{\longrightarrow}$; i.e., the only substitutions considered are those obtained by matching. From now on we shall abbreviate $\underset{\mathcal{R}}{\rightarrow}$ as $\rightarrow$ and $\underset{\mathcal{E}}{\vdash\!\dashv}$ as $\vdash\!\dashv$. Note that $\mathcal{A} \vdash M = N \Leftrightarrow M(\leftrightarrow \cup \vdash\!\dashv)^*N$.

We say that $\langle \mathcal{R}, \mathcal{E} \rangle$ is a *confluent equational theory* iff $\rightarrow$ is confluent modulo $\sim$, where $\sim\, = \overset{*}{\vdash\!\dashv}$. In this case, provided $\rightarrow$ normalizes $\mathcal{T}$, Lemma 2.6 gives us a way of reducing the problem $\mathcal{A} \vdash M = N$ to the problem $\hat{M} \sim \hat{N}$, where $\hat{M}$ and $\hat{N}$ are $\rightarrow$-normal forms of M and N, respectively.

We now show how Lemma 3.1 can be generalized to equational theories which will give sufficient conditions for an equational theory to be confluent, using Lemma 2.8.

Let us recall property α of Figure 9:

$$\alpha: \quad \forall M, N_1, N_2 \quad M \rightarrow N_1 \;\&\; M \rightarrow N_2 \Rightarrow N_1 \tilde{\downarrow} N_2,$$

where $M \tilde{\downarrow} N \Leftrightarrow \exists M', N' \quad M \overset{*}{\rightarrow} M' \;\&\; N \overset{*}{\rightarrow} N' \;\&\; M' \sim N'$.

LEMMA 3.4. *$\langle \mathcal{R}, \mathcal{E} \rangle$ verifies property α iff for every critical pair $\langle P, Q \rangle$ of $\mathcal{R}$, we have $P \tilde{\downarrow} Q$.*

PROOF. The proof follows closely that of Lemma 3.1. We use the same notation and indicate here only the points that differ.

Cases 1 and 2a are kept unchanged. For case 2b let $\langle P, Q \rangle$ be the critical pair of $\mathcal{R}$ involved.

By hypothesis, there exist R and S such that $P \overset{*}{\rightarrow} R$, $Q \overset{*}{\rightarrow} S$, and $R \sim S$. Let us consider $\bar{R} = \rho(R)$ and $\bar{S} = \rho(S)$. We get $\sigma_1(\beta_1) = \rho(Q) \overset{*}{\rightarrow} \bar{S}$, since $\rightarrow$ is stable and $N_2/u_1 = \rho(P) \overset{*}{\rightarrow} \bar{R}$ as well. Therefore $\sigma_1(\beta_1) \tilde{\downarrow} N_2/u_1$, and thus $N_1 \tilde{\downarrow} N_2$ since $\rightarrow$ and $\vdash\!\dashv$ are compatible, which concludes the proof. $\square$

We want now to get a similar result for property γ, which we recall here:

$$\gamma: \quad \forall M, N, P \quad M \rightarrow N \;\&\; M \vdash\!\dashv P \Rightarrow N \tilde{\downarrow} P.$$

Definition. Let $\langle \mathcal{R}, \mathcal{E} \rangle$ be an equational theory. We call a *critical pair of $\mathcal{E}/\mathcal{R}$* any pair $\langle P, Q \rangle$ constructed by the superposition algorithm, but now applied to α_1, β_1, α_2, β_2 such that either

$$\langle \alpha_1 = \beta_1 \rangle \in \mathcal{E} \cup \mathcal{E}^{-1} \qquad \text{and} \qquad \langle \alpha_2 \rightarrow \beta_2 \rangle \in \mathcal{R}$$

or

$$\langle \alpha_1 \rightarrow \beta_1 \rangle \in \mathcal{R} \qquad \text{and} \qquad \langle \alpha_2 = \beta_2 \rangle \in \mathcal{E} \cup \mathcal{E}^{-1}.$$

LEMMA 3.5. *Let $\langle \mathcal{R}, \mathcal{E} \rangle$ be an equational theory such that $\mathcal{R}$ is left linear. Then property γ holds iff for every critical pair $\langle P, Q \rangle$ of $\mathcal{E}/\mathcal{R}$, we have $P \tilde{\downarrow} Q$.*

PROOF. The proof follows the same general pattern as that of Lemma 3.1. Using the notation of the superposition algorithm, a critical pair $\langle P, Q \rangle$ of $\mathcal{E}/\mathcal{R}$ is such that $\sigma_1(\alpha_1) \rightarrow P$ and $\sigma_1(\alpha_1) \vdash\!\dashv Q$, which shows the "only if" part.

For the "if" part, assume that for every critical pair $\langle P, Q \rangle$ of $\mathcal{E}/\mathcal{R}$, $P \tilde{\downarrow} Q$. Let M be an arbitrary term, and N_1 and N_2 be such that $M \rightarrow N_1$ and $M \vdash\!\dashv N_2$; i.e., $\exists u_1, u_2 \in \mathcal{O}(M)$, $\langle \alpha_1 \rightarrow \beta_1 \rangle \in \mathcal{R}$, $\langle \alpha_2 = \beta_2 \rangle \in \mathcal{E}$, and substitutions σ_1 and σ_2 such that $M/u_1 = \sigma_1(\alpha_1)$, $M/u_2 = \sigma_2(\alpha_2)$, $N_1 = M[u_1 \leftarrow \sigma_1(\beta_1)]$, and $N_2 = M[u_2 \leftarrow \sigma_2(\beta_2)]$ (the symmetric case is obtained in interchanging α_2 and β_2 below throughout).

There are here three cases, according to the relative positions of the occurrences u_1 and u_2.

Case 1. $u_1 | u_2$. With $\bar{M} = N_1[u_2 \leftarrow \sigma_2(\beta_2)] = N_2[u_1 \leftarrow \sigma_1(\beta_1)]$, we get $N_1 \vdash\!\dashv \bar{M}$ and $N_2 \rightarrow \bar{M}$, and therefore $N_1 \tilde{\downarrow} N_2$.

Case 2. $u_1 \le u_2$. Let $v = u_2/u_1$. We have $\sigma_1(\alpha_1)/v = \sigma_2(\alpha_2)$ and $N_2/u_1 = \sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)]$. There are two cases.

2a. $v = v_1 \cdot v_2$, $\alpha_1/v_1 = x \in \mathscr{V}$, $\sigma_2(\alpha_2) = \sigma_1(x)/v_2$. Let us consider substitution σ_1' defined by

$$\sigma_1'(x) = \sigma_1(x)[v_2 \leftarrow \sigma_2(\beta_2)],$$
$$\sigma_1'(y) = \sigma_1(y) \qquad \forall y \neq x,$$

and let $\bar{M} = \sigma_1'(\beta_1)$.

We have $\sigma_1(\beta_1) \sim \bar{M}$ by Proposition 3.6. Also, $\sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)] = \sigma_1'(\alpha_1)$, since v_1 is the only occurrence of x in α_1, $\mathscr{R}$ being left linear by hypothesis.

$\sigma_1'(\alpha_1) \rightarrow \bar{M}$ by the stability of $\rightarrow$, and thus, taking $\hat{M} = M[u_1 \leftarrow \bar{M}]$, we get $N_1 \sim \hat{M}$ and $N_2 \rightarrow \hat{M}$ by the compatibility of $\rightarrow$ and $\vdash\!\dashv$.

2b. $\alpha_1/v \notin \mathscr{V}$, $\sigma_2(\alpha_2) = \sigma_1(\alpha_1/v)$. By Proposition 3.7 there exist a critical pair $\langle P, Q\rangle$ of $\mathscr{E}/\mathscr{R}$ and a substitution ρ such that

$$\sigma_1(\beta_1) = \rho(Q) \qquad \text{and} \qquad \sigma_1(\alpha_1)[v \leftarrow \sigma_2(\beta_2)] = \rho(P).$$

By hypothesis, $P \tilde{\downarrow} Q$, whence $\rho(P) \tilde{\downarrow} \rho(Q)$ by stability, and $N_1 \tilde{\downarrow} N_2$ by compatibility. This concludes case 2.

Case 3. $u_2 \le u_1$. Let $v = u_1/u_2$. As in case 2, there are two cases.

3a. $v = v_1 \cdot v_2$, $\alpha_2/v_1 = x \in \mathscr{V}$, $\sigma_1(\alpha_1) = \sigma_2(x)/v_2$. We define substitution σ_2' by

$$\sigma_2'(x) = \sigma_1(x)[v_2 \leftarrow \sigma_1(\beta_1)],$$
$$\sigma_2'(y) = \sigma_2(y) \qquad \forall y \neq x,$$

and we consider $\bar{M} = \sigma_2'(\beta_2)$.

We have $\sigma_2(\beta_2) \xrightarrow{*} \bar{M}$ by Proposition 3.6, and also $N_1/u_2 = \sigma_2(\alpha_2)[v \leftarrow \sigma_1(\beta_1)] \xrightarrow{*} \sigma_2'(\alpha_2) \vdash\!\dashv \bar{M}$, which shows $N_1 \tilde{\downarrow} N_2$.

3b. $\alpha_2/v \notin \mathscr{V}$, $\sigma_1(\alpha_1) = \sigma_2(\alpha_2/v)$. Again there exist a critical pair $\langle P, Q\rangle$ of $\mathscr{E}/\mathscr{R}$ and a substitution ρ such that $\sigma_2(\beta_2) = \rho(Q)$ and $\sigma_2(\alpha_2)[v \leftarrow \sigma_1(\beta_1)] = \rho(P)$. By hypothesis, $P \tilde{\downarrow} Q$, and therefore $N_1 \tilde{\downarrow} N_2$, which concludes the proof. □

Remark. The condition $\mathscr{R}$ left linear is essential and cannot be removed. For instance, with $\mathscr{R} = \{\langle F(x, x) \rightarrow G(x)\rangle\}$ and $\mathscr{E} = \{\langle A = B\rangle\}$, and taking $M = F(A, A)$, $N_1 = G(A)$, and $N_2 = F(A, B)$, we do not have $N_1 \tilde{\downarrow} N_2$. Note that there are no such restrictions for the equations in $\mathscr{E}$.

We are now able to state our main result. Let us define the set of *critical pairs of an equational theory* $\langle \mathscr{R}, \mathscr{E}\rangle$ as the set of all critical pairs of $\mathscr{R}$ and critical pairs of $\mathscr{E}/\mathscr{R}$, as defined above.

THEOREM 3.3. *Let* $\langle \mathscr{R}, \mathscr{E}\rangle$ *be an equational theory such that*

(1) $\forall \langle \alpha \rightarrow \beta\rangle \in \mathscr{R}$ $\;\mathscr{V}(\beta) \subseteq \mathscr{V}(\alpha)$ *and* α *is linear;*
(2) $\forall \langle \alpha = \beta\rangle \in \mathscr{E}$ $\;\mathscr{V}(\beta) = \mathscr{V}(\alpha)$;
(3) $\rightarrow \cdot \sim$ *is noetherian with* $\rightarrow\; = \underset{\mathscr{R}}{\rightarrow}$ *and* $\sim\; = \underset{\mathscr{E}}{\overset{*}{\vdash\!\dashv}}$.

Let $\hat{M}$ *denote any* $\rightarrow$*-normal form of* M*, obtained by any sequence of reductions of* $\mathscr{R}$*, for any* $M \in \mathscr{T}$*. The theory* $\langle \mathscr{R}, \mathscr{E}\rangle$ *is confluent iff for all its critical pairs* $\langle P, Q\rangle$ *we have* $\hat{P} \sim \hat{Q}$*, and then* $\langle \mathscr{R}, \mathscr{E}\rangle \vdash M = N$ *iff* $\hat{M} \sim \hat{N}$.

PROOF. Directly from Lemmas 2.6, 2.8, 3.4, and 3.5. □

Remarks. The notion of critical pair of $\langle \mathscr{R}, \mathscr{E}\rangle$ involves trying all superpositions of equations in $\mathscr{E}$ with simplifications in $\mathscr{R}$, and conversely, and mutual superpositions of simplifications in $\mathscr{R}$. But there is no need to superpose two equations in $\mathscr{E}$.

To check the termination condition $\rightarrow \cdot \sim$ noetherian, the method given in Section 3.2 is still valid, provided the interpretation χ chosen is such that $\chi(\alpha) = \chi(\beta)$ is identically true for every equation $\langle \alpha = \beta \rangle$ in $\mathscr{E}$.

Note that it is important to get termination criteria as general as possible in Lemmas 2.4, 2.7, and 2.8. For instance, the conditions of [34] are too restrictive to be used with Knuth and Bendix's lexicographic ordering [16].

When $\mathscr{R}$ and $\mathscr{E}$ are finite, Theorem 3.3 gives us a decision procedure for the confluence of $\langle \mathscr{R}, \mathscr{E} \rangle$, since there is a finite number of critical pairs. Furthermore, it is possible to extend the Knuth and Bendix method, to attempt to complete a theory to a confluent one, as follows. We start from $\mathscr{R}$ and $\mathscr{E}$ satisfying conditions 1, 2, and 3 of Theorem 3.3. We generate the set $\mathscr{C}$ of critical pairs. For every $\langle P, Q \rangle$ in $\mathscr{C}$ such that $\hat{P} \not\sim \hat{Q}$, we either add $\langle \hat{P} = \hat{Q} \rangle$ to $\mathscr{E}$ or one of the rules $\langle \hat{P} \rightarrow \hat{Q} \rangle$ and $\langle \hat{Q} \rightarrow \hat{P} \rangle$ to $\mathscr{R}$. Of course we must check that all the conditions of Theorem 3.3 are still valid. If this completion succeeds for every element of $\mathscr{C}$, we iterate the process with the new critical pairs that may have been created. The whole process may stop with success, resulting in a confluent equational theory equivalent to the initial one (i.e., with same deducibility relation $\vdash$); this may be considered as compiling axioms into simplification rules, replacing deduction by computation. The process may also fail or loop forever, generating progressively an infinite confluent equational theory.

A generalization of the Knuth and Bendix completion algorithm for handling commutative axioms is given in [18] and extended in [19] to a class of axioms called permutative axioms. This approach is different from ours: first because the condition checked in these papers is the confluence of $\rightarrow/\sim$, rather than the confluence of $\rightarrow$ modulo $\sim$; second, because they consider arbitrary simplifications, but the equations must be such that the equivalence classes of $\sim$ are finite, whereas our equations are arbitrary, but our simplifications must be left linear.

Another approach to the generalization of [16] consists in embedding equations into specialized unification algorithms, in the manner of [30]. This method may be used for commutative and associative axioms, as shown in [20, 26] for Abelian groups, commutative rings, and distributive lattices.

Let us end this section with an example of the use of Theorem 3.3.

Example. We use the binary symbols + and $\cdot$ in infix notation. Let

$$\begin{aligned}\mathscr{R} = \{&\langle E(x+y) \rightarrow E(x)\cdot E(y)\rangle, \langle E(0) \rightarrow 1\rangle,\\ &\langle x+0 \rightarrow x\rangle, \langle 0+x \rightarrow x\rangle, \langle x\cdot 1 \rightarrow x\rangle, \langle 1\cdot x \rightarrow x\rangle\}\end{aligned}$$

and

$$\begin{aligned}\mathscr{E} = \{&\langle x+y = y+x\rangle, \langle (x+y)+z = x+(y+z)\rangle, \langle x\cdot y = y\cdot x\rangle,\\ &\langle (x\cdot y)z = x(y\cdot z)\rangle\}.\end{aligned}$$

We leave it to the reader to check that conditions 1, 2, and 3 of Theorem 3.3 are fulfilled and that for every critical pair $\langle P, Q \rangle$ we have $\hat{P} \sim \hat{Q}$, proving that $\langle \mathscr{R}, \mathscr{E} \rangle$ is a confluent equational theory. This example suggests the use of Theorem 3.3 for the study of operational semantics of recursive programs operating on abstract data types, with $\mathscr{R}$ modeling the computation rules, and $\mathscr{E}$ the axiomatic definition of the data type.

4. *Conclusion*

We have presented in Section 2 of this paper general axiomatic properties that are sufficient to prove the confluence of a reduction relation. These results permit us, under certain conditions, to *localize* the confluence test to simpler diagrams. We consider in Section 3 term rewriting systems and show that many closure conditions expressed by these diagrams can be *specialized* to the critical pairs. These methods give us systematic ways of mechanizing an equational theory, favoring simplifications over arbitrary equality replacements. This problem arises in formula manipulating systems for various applications: program optimization, program validation, automatic theorem proving, operational semantics of programming languages, and semantics of parallel systems.

ACKNOWLEDGMENTS. I wish to thank J.J. Levy, B. Rosen, and R. Sethi for their helpful remarks.

REFERENCES

1. AHO, A., SETHI, R., AND ULLMAN, J. Code optimization and finite Church-Rosser systems In *Proceedings of Courant Computer Science Symposium 5*, R Rustin, Ed., Prentice Hall, Englewood Cliffs, N.J, 1972, pp 89-105
2. BROWN, T A structured design method for specialized proof procedures Ph D Thesis, California Institute of Technology, Pasadena, Calif., 1975
3 BURSTALL, R Proving properties of programs by structural induction *Comput J. 12* (1969), 41-48
4. CHURCH, A., AND ROSSER, J.B. Some properties of conversion. *Trans. AMS 39* (1936), 472-482.
5. COHN, P M *Universal algebra.* Harper and Row, New York, 1965.
6 CURRY, H B., AND FEYS, R *Combinatory Logic*, Vol 1 North Holland, Amsterdam, 1958
7. DERSHOWITZ, N, AND MANNA, Z Proving termination with multiset orderings *Commun ACM 22*, 8 (Aug. 1979), 465-476
8 GUARD, J R, OGLESBY, F.C, BENNETT, J.H., AND SETTLE, L.G. Semi-automated mathematics *J. ACM 16* (1969), 49-62.
9. HINDLEY, R An abstract Church-Rosser theorem Pt 1, *J Symbolic Logic 34* (1969), 545-560, Pt 2, *J Symbolic Logic 39* (1974), 1-21.
10 HINDLEY, R, LERCHER, B., AND SELDIN, J.P. Introduction to combinatory logic In *London Mathematical Society Lecture Notes 7*, Cambridge University Press, Cambridge, England, 1972
11. HUET, G. Experiments with an interactive prover for logic with equality Rep. 1106, Jennings Computing Center, Case Western Reserve Univ, Cleveland, Ohio, 1970.
12 HUET, G Résolution d'équations dans des langages d'ordre 1, 2, .. , ω Thèse d'Etat, Univ Paris VII, Paris, Sept 1976.
13 HUET, G, AND LANKFORD, D.S On the uniform halting problem for term rewriting systems Lab Rep No 283, INRIA, Le Chesnay, France, March 1978
14. HUET, G., AND LÉVY, J J. Call by need computations in non-ambiguous linear term rewriting systems. Lab. Rep. No. 359, INRIA, Le Chesnay, France, Aug. 1979
15. KLOP, J W A counter example to the Church-Rosser property for lambda calculus with subjective pairing Preprint No 102, Dep of Mathematics, Univ. of Utrecht, Utrecht, The Netherlands, 1978.
16. KNUTH, D., AND BENDIX, P. Simple word problems in universal algebras In *Computational Problems in Abstract Algebra*, J Leech, Ed., Pergamon Press, Elmsford, N.Y, 1970, pp. 263-297
17. LANKFORD, D S. Canonical inference Rep ATP-25, Dep. Mathematics and Computer Sciences, Univ. of Texas, Austin, Texas, Dec 1975
18. LANKFORD, D S., AND BALLANTYNE, A.M Decision procedures for simple equational theories with commutative axioms: Complete sets of commutative reductions. Rep. ATP-35, Dep. Mathematics and Computer Sciences, Univ of Texas, Austin, Texas, March 1977
19. LANKFORD, D.S, AND BALLANTYNE, A M. Decision procedures for simple equational theories with permutative axioms: Complete sets of permutative reductions Rep. ATP-37, Dep. of Mathematics and Computer Sciences, Univ of Texas, Austin, Texas, April 1977
20 LANKFORD, D.S, AND BALLANTYNE, A.M Decision procedures for simple equational theories with commutative-associative axioms: Complete sets of commutative-associative reductions Rep ATP-39, Dep Mathematics and Computer Sciences, Univ. of Texas, Austin, Texas, Aug. 1977.
21. LIPTON, R.J, AND SNYDER, L On the halting of tree replacement systems Proc of Waterloo Conf. on Theoretical Computer Science, Univ of Waterloo, Waterloo, Ontario, Aug 1977, pp 43-46
22. MANNA, Z., AND NESS, S. On the termination of Markov algorithms. Proc 3rd Hawaii Int. Conf. on System Sciences, Jan. 1970, pp. 789-792.
23. NEWMAN, M.H A On theories with a combinatorial definition of "equivalence" *Ann Math*, *43* (1942), 223-243
24. NIVAT, M. Congruences parfaites et quasi-parfaites *Séminaire Dubreuil 7*, 1971-72, see also preliminary version: On some families of languages related to the Dyck language. Proc 2nd Ann. ACM Symp on Theory of Computing, Northampton, Mass., May 1970, pp. 221-225
25 PATERSON, M.S., AND WEGMAN, M N Linear unification Proc 8th Ann ACM Symp. on Theory of Computing, Hershey, Pa, May 1976, pp. 181-186.
26. PETERSON, G E, AND STICKEL, M E Complete sets of reductions for equational theories with complete unification algorithms Tech. Rep., Dep. of Computer Science, Univ. of Arizona, Tucson, Ariz., Sept 1977.
27 PLAISTED, D. Well-founded orderings for proving termination of systems of rewrite rules Tech Rep. 78-932, Dep. of Computer Science, Univ. of Illinois, Urbana-Champaign, Ill, July 1978.
28. PLAISTED, D. A recursively defined ordering for proving termination of term rewriting systems Tech. Rep 78-943, Dep of Computer Science, Univ of Illinois, Urbana-Champaign, Ill, Sept 1978

29 PLOTKIN, G Lattice-theoretic properties of subsumption Memo MIP-R77, Univ. of Edinburgh, Edinburgh, Scotland, 1970

30 PLOTKIN G. Building-in equational theories In *Machine Intelligence 7*, B. Meltzer and D. Michie, Eds., American Elsevier, New York, 1972, pp 73–90

31. REYNOLDS, J Transformational systems and the algebraic structure of atomic formulas. In *Machine Intelligence 5*, B Meltzer and D Michie, Eds, American Elsevier, New York, 1970, pp. 135–152.

32 ROBINSON, J. A. A machine-oriented logic based on the resolution principle *J. ACM 12*, 1 (Jan. 1965), 23–41

33 ROSEN, B K. Tree-manipulating systems and Church–Rosser theorems *J. ACM 20*, 1 (Jan. 1973), 160–187

34. SETHI, R Testing for the Church–Rosser property *J ACM 21*, 4 (Oct 1974), 671–679, Errata, *J. ACM 22*, 3 (July 1975), 424

35 SLAGLE, J R Automated theorem-proving for theories with simplifiers, commutativity, and associativity. *J ACM 21*, 4 (Oct 1974), 622–642

36 STAPLES, J Church–Rosser theorems for replacement systems In *Algebra and Logic*, J. Crossley, Ed., Lecture Notes in Mathematics No 450, Springer-Verlag, 1975

RECEIVED FEBRUARY 1978; REVISED SEPTEMBER 1979; ACCEPTED JANUARY 1980