CONFLUENT REDUCTIONS :

ABSTRACT PROPERTIES AND APPLICATIONS

TO TERM REWRITING SYSTEMS.

Gérard HUET

IRIA - LABORIA

Domaine de Voluceau

78150 Rocquencourt (FRANCE)

## ABSTRACT

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

Part 1 gives abstract confluence properties, depending solely on axioms for a binary relation called reduction. Results of Newman and others are presented in a unified formalism. Systematic use of a powerful induction principle permits to generalize results of Sethi on reduction modulo equivalence.

Part 2 concerns simplification systems operating on terms of a first-order logic. Results by Rosen and Knuth and Bendix are extended to give several new criteria for confluence of these systems, using the results of part 1. It is then shown how these results yield efficient methods for the mechanization of equational theories.

## I. ABSTRACT REDUCTION PROPERTIES

### 1 - Generalities

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

#### Notations

$\iota$ is the identity relation on $\mathcal{E}$ : $\iota = \{<x,x> \mid x \in \mathcal{E}\}$.

. is relation composition :

$\rightarrow_1 \cdot \rightarrow_2 = \{<x,y> \mid \exists\ z\ x \rightarrow_1 z\ \&\ z \rightarrow_2 y\}$.

$\rightarrow^{-1}$ is the inverse of relation $\rightarrow$ : $\rightarrow^{-1} = \{<x,y> \mid y \rightarrow x\}$.

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

$\overset{0}{\rightarrow} = \iota$

$\overset{\varepsilon}{\rightarrow} = \rightarrow \cup\ \iota$ reflexive closure of $\rightarrow$

$\overset{i}{\rightarrow} = \rightarrow \cdot \overset{i-1}{\rightarrow}$ $\forall\ i > 0$ i-iteration of $\rightarrow$

$\overset{+}{\rightarrow} = \bigcup\limits_{i>0} \overset{i}{\rightarrow}$ transitive closure of $\rightarrow$

$\overset{*}{\rightarrow} = \overset{+}{\rightarrow} \cup\ \iota$ transitive-reflexive closure of $\rightarrow$

$\overset{*}{\longleftrightarrow} = (\rightarrow \cup \overset{-1}{\rightarrow})^*$ equivalence closure of $\rightarrow$.

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

For a given relation $\rightarrow$, we let :

$x \downarrow y \Longleftrightarrow \exists z \quad x \overset{*}{\rightarrow} z\ \&\ y \overset{*}{\rightarrow} z$

$x \uparrow y \Longleftrightarrow \exists z \quad z \overset{*}{\rightarrow} x\ \&\ z \overset{*}{\rightarrow} y$

$\Lambda(x) = \max\{i \mid \exists\ y\ x \overset{i}{\rightarrow} y\} \in \mathbb{N} \cup \{\infty\}$

$\Delta(x) = \{y \mid x \rightarrow y\}$

$\Delta^+(x) = \{y \mid x \overset{+}{\rightarrow} y\}$, $\Delta^*(x) = \Delta^+(x) \cup \{x\}$

#### Definitions

D1 $\rightarrow$ is *inductive* iff for every sequence $x_1 \rightarrow x_2 \rightarrow \ldots \rightarrow x_n \rightarrow \ldots$ there exists y such that $\forall\ i \geq 1$ $x_i \overset{*}{\rightarrow} y$.

D2 $\to$ is *acyclic* iff $\overset{+}{\to}$ is irreflexive (and then $\overset{*}{\to}$ is a partial ordering relation).

D3 $\to$ is *noetherian* iff there is no infinite sequence $x_1 \to x_2 \to \ldots \to x_n \to \ldots$ (then $\overset{*}{\to}$ is well founded).

D4 $\to$ is *bounded* iff $\forall x\ \Lambda(x) < \infty$ (the finiteness property in [1,15]).

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

Let P be any predicate on $\mathcal{E}$ We say that P is $\to$*-complete* iff $\forall x \in \mathcal{E}\ [\forall y \in \Delta^{+}(x)\ P(y)] \Rightarrow P(x)$.

Our interest in noetherian relations stems from the following :

Principle of noetherian induction

Let $\to$ be a noetherian relation. Any $\to$ -complete predicate P is universal : $\forall x \in \mathcal{E}\ P(x)$.

This principle is as powerful as the usual forms of ordinal induction. It presents the advantage of not requiring the construction of the well ordering associated with the partial ordering $\overset{*}{\to}$.

Definitions

D5 $\to$ is *locally finite* iff $\forall x \in \mathcal{E}\ \Delta(x)$ is finite.

Let $\to$ be a locally finite relation. For every x in $\mathcal{E}$, if $\Lambda(x) = \infty$ there exists an infinite sequence $x = x_1 \to x_2 \to \ldots \to x_n \to \ldots$

Therefore a locally finite relation is bounded iff it is noetherian.

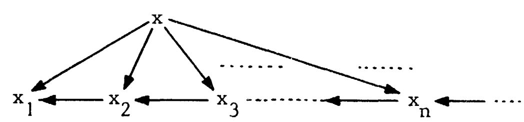
D6 $\to$ is *globally finite* iff $\forall x \in \mathcal{E}\ \Delta^{*}(x)$ is finite.

Let $\to$ be a locally finite relation. For every x in $\mathcal{E}$, if $\Delta^{*}(x)$ is infinite there exists an infinite sequence $x = x_1 \to x_2 \to \ldots \to x_n \to \ldots$

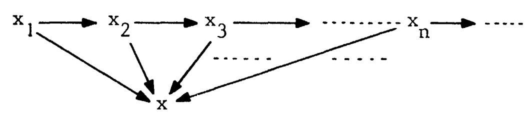
Therefore a noetherian locally finite relation is globally finite. Conversely, any acyclic globally finite relation is bounded. Combining all this, we get :

Koenig's lemma

Let $\to$ be an acyclic locally finite relation. Then $\to$ is noetherian iff it is bounded iff it is globally finite. Finally, note that acyclic and noetherian does not imply bounded, as shown by :




Also, acyclic, inductive and locally finite implies neither noetherian nor globally finite, as shown by the dual example :



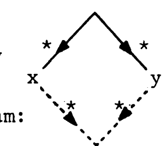

## 2 - Confluence properties

Suppose we are interested in the equivalence $\overset{*}{\leftrightarrow}$ generated by a relation $\to$. We are going to give conditions on $\to$ that permit to recognize if $x \overset{*}{\leftrightarrow} y$, when performing only reductions $(\overset{*}{\to})$ from x and y.

Definition

D7 $\to$ is *confluent* iff $\forall x\ y\ \ x \uparrow y \Rightarrow x \downarrow y$

We express this property with the diagram:




The results that follow appear in Newman [8]. They have been rediscovered by several authors in various contexts, where $\to$ is interpreted as the $\beta$-reduction relation in $\lambda$-calculus, the deduction relation in a formal system, or the operationnal semantics in a programming language.

Lemma 1 If $\to$ is confluent, then the following "Church Rosser" property holds : $\forall x\ y\ \ x \overset{*}{\leftrightarrow} y \Leftrightarrow x \downarrow y$.

Lemma 2 If $\to$ is confluent, then the normal form of any element, if it exists, is unique.

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

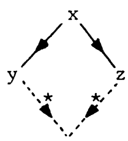
The two preceding lemmas show the interest of confluent relations. The rest of this section is devoted to finding sufficient conditions for a relation to be confluent. First, it is easy to partially localize the test for confluence :

Lemma 3 $\to$ is confluent iff $\forall x\ y\ z\ \ x \to y\ \&\ x \overset{*}{\to} z \Rightarrow y \downarrow z$.

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

Definition

D8 $\to$ is *locally confluent* iff

$\forall x\, y\, z \quad x \to y \;\&\; x \to z \Rightarrow y \downarrow z$ i.e. 


Lemma 4

A noetherian relation is confluent iff it is locally confluent.

This lemma appears in the litteraturein various places, in weaker forms : either the relation is required to be bounded (easy induction on $\Lambda(x)$) [1,15], or it is assumed to be locally finite [7], or it is proved for a specific noetherian relation [6] (ad hoc induction). Several weaker forms are given in [16]. It appears in its full generality in [8], but with an unnecessarily complex proof. Let us show how noetherian induction permits an easy and natural proof.

Proof of lemma 4

The only if part is trivial. For the if part, assume $\to$ is a noetherian locally confluent relation. We prove $P(x) : \forall y\, z \quad x \overset{*}{\to} y \;\&\; x \overset{*}{\to} z \Rightarrow y \downarrow z$ be noetherian induction, showing that P is $\to$ complete.

Let $x \overset{m}{\to} y$ and $x \overset{n}{\to} z$. We show $\exists\, t \quad y \overset{*}{\to} t$ and $z \overset{*}{\to} t$.

. if $m = 0$ we choose $t = z$, if $n = 0$ we choose $t = y$.

. otherwise, let $x \to y_1 \overset{*}{\to} y$ and $x \to z_1 \overset{*}{\to} z$.

By local confluence, $\exists\; u\; y_1 \overset{*}{\to} u$ and $z_1 \overset{*}{\to} u$. By induction hypothesis on $y_1$, $\exists\, v \quad y \overset{*}{\to} v$ and $u \overset{*}{\to} v$. By induction hypothesis on $z_1$, $\exists\, w \quad u \overset{*}{\to} w$ and $z \overset{*}{\to} w$. Finally, by induction hypothesis on u, $\exists\, t \quad v \overset{*}{\to} t$ and $w \overset{*}{\to} t$, proving P(x).

The induction step of the proof is shown in the diagram of Fig. 1. □

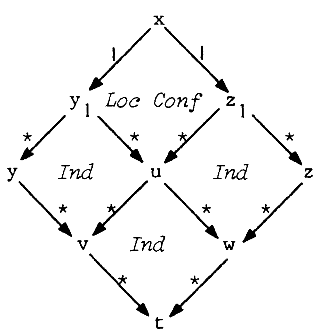



Fig. 1

Lemma 4 fails, if we suppose only $\to$ to be inductive and acyclic, as shown by the counter example in Fig. 2,due to Newman.

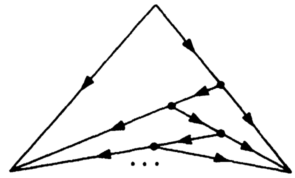


Fig. 2

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

Definition

D9 $\to$ is *strongly confluent* iff

$\forall x\, y\, z \quad x \to y \;\&\; x \to z \Rightarrow \exists u \quad y \overset{*}{\to} u \;\&\; z \overset{\varepsilon}{\to} u.$

Remark : Beware of the symmetry between y and z in the definition above. It is only slightly weaker than to require $y \overset{\varepsilon}{\to} u \;\&\; z \overset{\varepsilon}{\to} u$. For instance, $\to$ in Fig. 2 is not strongly confluent.

Lemma 5

Any strongly confluent relation is confluent.

Proof It is easy to show, by induction on n, that if $\to$ is strongly confluent then $\forall x\, y\, z \quad x \overset{\varepsilon}{\to} y \;\&\; x \overset{n}{\to} z \Rightarrow \exists u \quad y \overset{*}{\to} u \;\&\; z \overset{\varepsilon}{\to} u$. The result follows then from lemma 3. □

It may seem that the conditions in definition D9 are too restrictive to be of practical use. However, lemma 5 is the basis of a common method to prove Church Rosser results in Combinatory Logic : one usually constructs, from the reduction relation $\to$, a strongly confluent relation $\twoheadrightarrow$ with same transitive closure as $\to$ : $\overset{*}{\to} = \overset{*}{\twoheadrightarrow}$. Actually, a weaker condition is sufficient : it is enough to show that $\twoheadrightarrow$ is a compatible refinement of $\to$, in the sense of Staples [16].

Various other axiomatic conditions imply confluence, for instance using decompositions of $\to$ as the union of two or more relations. See in particular [8, 14, 16]. For instance, lemma 5 is a consequence of the commutativity lemma in Rosen [14].

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, 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 → 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 shall now model this situation by considering a reduction relation →, to which we adjoin an equivalence relation ~, in the same manner as Sethi [15].

Definition

D10 → is *confluent modulo* ~ iff

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

Remark that this condition is different from →/~ being confluent in $\mathcal{E}/\sim$ , since we do not allow ~ along the → - derivations. If → has the property of defining a normal form for every element, we get a weak form of lemma 2 :

Lemma 6

Let → normalize $\mathcal{E}$, i.e. $\forall x \in \mathcal{E} \;\; \exists y \in \mathcal{N} \;\; x \xrightarrow{*} y$. Then → is confluent modulo ~ iff

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

where $\equiv$ is $(\rightarrow \cup \xrightarrow{-1} \cup \sim)^*$.

We leave the proof of this result to the reader.
We are now going to search for sufficient conditions for → to be confluent modulo ~. The first step is to generalize lemma 4, assuming → noetherian. The lemma below generalizes th. 2.2 of Sethi [15], who requires → to be bounded. This generalization will be useful practically since one frequently proves termination results using lexicographic orderings on terms that are noetherian but not bounded [6]. But the main interest lies here in the technique of proof, based on noetherian induction.

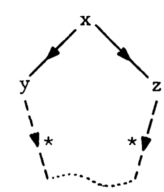
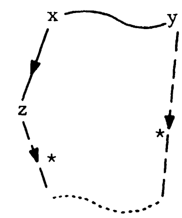
Definition

D11 → is *locally confluent modulo* ~ iff conditions α and β below are satisfied.

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

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

where $y \stackrel{\sim}{\downarrow} z \Leftrightarrow \exists u\, v \quad y \xrightarrow{*} u \;\&\; z \xrightarrow{*} v \;\&\; u \sim v$.

α :

β :


We can now state the generalization of lemma 4.

Lemma 7

Let → be a noetherian relation. For any equivalence ~, → is confluent modulo ~ iff → is locally confluent modulo ~.
Before giving the proof of this lemma, let us state a preliminary proposition.

Definition

Let → be any relation on $\mathcal{E}$. We define a relation ➞ in $\mathcal{E} \times \mathcal{E}$ by :

$$\langle x,y\rangle \twoheadrightarrow \langle x',y'\rangle \quad \text{iff :}$$

- either $x \rightarrow x'$ and $(x \rightarrow y'$ or $y = y')$ (a)
- or $y \rightarrow y'$ and $(x = x'$ or $y \rightarrow x')$ (b)

Proposition 1 if → is noetherian, then ➞ is a noetherian relation in $\mathcal{E} \times \mathcal{E}$.

Proof

Let $\langle x_i,y_i\rangle$, $i \geq 0$, be an infinite sequence in $\mathcal{E} \times \mathcal{E}$, with $\langle x_i,y_i\rangle \twoheadrightarrow \langle x_{i+1},y_{i+1}\rangle$. There are three cases :

- if from rank k we use only rules of type (a), we get an infinite sequence $x_k \rightarrow x_{k+1} \rightarrow x_{k+2} \rightarrow \cdots$
- if from rank k we use only rules of type (b) : symmetric case.
- we alternate indefinitely between rules (a) and rules (b) :
  $\langle x_o,y_o\rangle \xrightarrow[(a)]{*} \langle x_{i1},y_{i1}\rangle \xrightarrow[(b)]{+} \langle x_{j1},y_{j2}\rangle \xrightarrow[(a)]{+} \langle x_{i2},y_{i2}\rangle \cdots$

In this case we get an infinite sequence :

$y_{i1} \xrightarrow{+} x_{j1} \xrightarrow{+} y_{i2} \xrightarrow{+} x_{j2} \xrightarrow{+} \cdots$ which concludes the proof. □

Proof of lemma 7

Let → be a noetherian relation locally confluent modulo ~. We shall use noetherian induction in $\mathcal{E} \times \mathcal{E}$, applied to ➞ and to property :

$$P(x,y) : x \sim y \Rightarrow [\forall x', y' \quad x \xrightarrow{*} x' \;\&\; y \xrightarrow{*} y' \Rightarrow x' \stackrel{\sim}{\downarrow} y']$$

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

. if n = 0 and m = 0, it is trivial.

. otherwise, let us assume without loss of generality that n > 0, and let $x \to x_1 \overset{*}{\to} x'$. By applying property β to x, y, $x_1$, we get u and v such that $x_1 \overset{*}{\to} u$, $y \overset{*}{\to} v$, $u \sim v$. There are two cases :

a) m = 0. Let $\bar{x}'$, $\bar{u}$ and $\bar{v}$ be $\to$ -normal forms of respectively x',u and v.

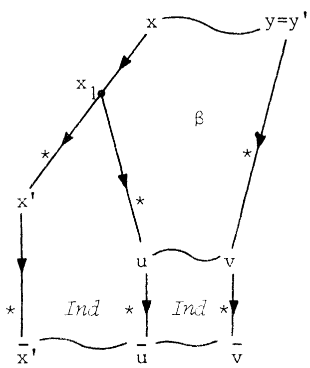
We get $\bar{x}' \sim \bar{u}$ by induction hypothesis $P(x_1,x_1)$ and $\bar{u} \sim \bar{v}$ by induction hypothesis P(u,v), completing the proof of case a) ; the diagram is shown in fig. 3a.

b) m > 0. Let $y \to y_1 \overset{*}{\to} y'$. Again there are two cases:

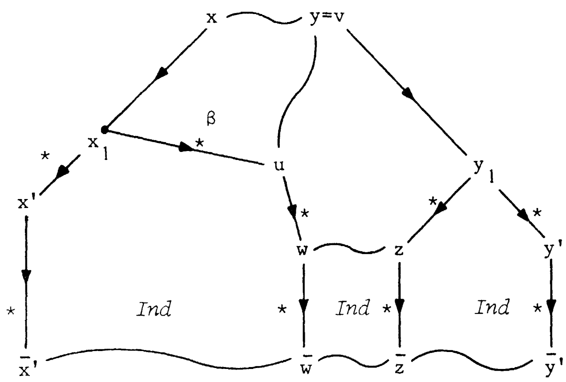
- b1) v = y. We apply again property β to y, u, $y_1$, getting w and z such that $u \overset{*}{\to} w$, $y_1 \overset{*}{\to} z$, $w \sim z$. Let $\bar{x}'$, $\bar{w}$, $\bar{z}$ and $\bar{y}'$ be $\to$ -normal forms of respectively x', w, z and y'. We get $\bar{x}' \sim \bar{w}$ by hypothesis $P(x_1,x_1)$, $\bar{w} \sim \bar{z}$ 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 fig. 3 b1.

- b2) otherwise, let $y \to t \overset{*}{\to} v$. We now apply property α to y, $y_1$, t, getting w and z such that $t \overset{*}{\to} w$, $y_1 \overset{*}{\to} z$, $w \sim z$. 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 successively $\bar{x}' \sim \bar{u}$ by 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 of this last case is shown in fig. 3 b2.

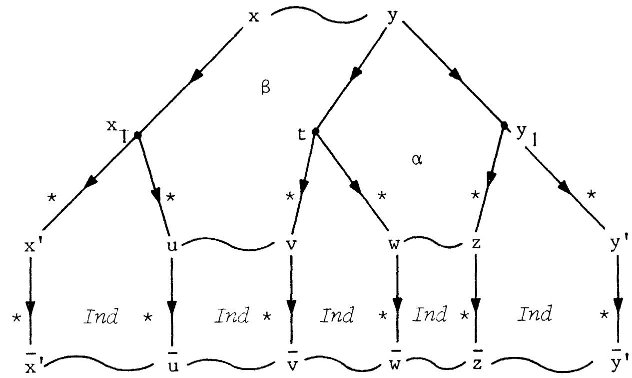
We leave it to the reader to check that we used hypothesis $P(\lambda,\mu)$ only when $\langle x,y\rangle \overset{+}{\twoheadrightarrow} \langle\lambda,\mu\rangle$. Actually, the definition of $\twoheadrightarrow$ was inspired directly from the diagrams we wished to close, which makes this method a very natural one to use for this sort of proof. □




(a)




(b1)




(b2)

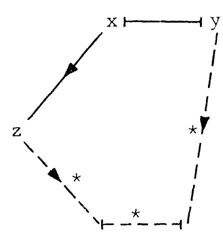
Fig. 3

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

Definition Property γ :

$\forall x\ y\ z \quad x \vdash\!\!\dashv y \ \&\ x \to z \Rightarrow y \overset{\sim}{\downarrow} z$, with $\sim\ = \overset{*}{\vdash\!\!\dashv}$ .

γ :




Definitions

If $x \sim y$, we define $\rho(x,y)$ as the smallest k such that $x \overset{k}{\vdash\!\!\dashv} y$. Similarly to above, we define a relation $\rightarrowtail$ in $\mathcal{E} \times \mathcal{E}$ by :

$\langle x,y\rangle \rightarrowtail \langle x',y'\rangle$ iff :

- either $\langle x,y\rangle \twoheadrightarrow \langle x',y'\rangle$ with same definition as above,

- or $x \sim y \sim x' \sim y'$ and $\rho(x,y) > \rho(x',y')$.

Proposition 2

if $\rightarrow.\sim$ is noetherian (or, equivalently, if $\rightarrow/\sim$ is noetherian in $\mathcal{E}/\sim$ ), then $\blacktriangleright\!\!\rightarrow$ is a noetherian relation in $\mathcal{E} \times \mathcal{E}$. The proof follows that of proposition 1, but in the quotient set $\mathcal{E}/\sim$ . Note that we need a stronger condition than for proposition 1.

Lemma 8

Let $\vdash\!\dashv$ be a symmetric relation, and let $\sim\ = \overset{*}{\vdash\!\dashv}$ . Let $\rightarrow$ be any relation such that $\rightarrow.\sim$ is noetherian. Then $\rightarrow$ is confluent modulo $\sim$ iff properties $\alpha$ and $\gamma$ are verified.

Proof

The only if part if obvious. For the if part, let us assume that $\rightarrow.\sim$ is noetherian, and that properties $\alpha$ and $\gamma$ hold. We shall again use noetherian induction in $\mathcal{E} \times \mathcal{E}$, applied to $\blacktriangleright\!\!\rightarrow$ and the same property P as in the proof of lemma 7.

Let $x, y, x', y' \in \mathcal{E}$ 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 :

a) $x = y$

. if $n = 0$ or $m = 0$ it is trivial.

. otherwise, let $x \rightarrow u \overset{*}{\rightarrow} x'$ and $y \rightarrow v \overset{*}{\rightarrow} y'$.

Applying property $\alpha$ to x, u, v, we get the existence of w and z such that $u \overset{*}{\rightarrow} w$, $v \overset{*}{\rightarrow} z$, $w \sim z$. Let $\bar{x}'$, $\bar{w}$, $\bar{z}$ and $\bar{y}'$ be $\rightarrow$-normal forms of respectively x', w, z and y'. We get $\bar{x}' \sim \bar{w}$ by 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 a) according to the diagram in Fig. 4a.

b) $\rho(x,y) > 0$.

. if $n = 0$ and $m = 0$ it is trivial

. 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 $\gamma$ to x, v, 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 a), applying induction hypotheses P(u,u), P(w,z) and P(v,y). Note that we always have $\langle x,y\rangle \overset{+}{\blacktriangleright\!\!\rightarrow} \langle w,z\rangle$. This concludes the proof, according to the diagram in Fig. 4b. □

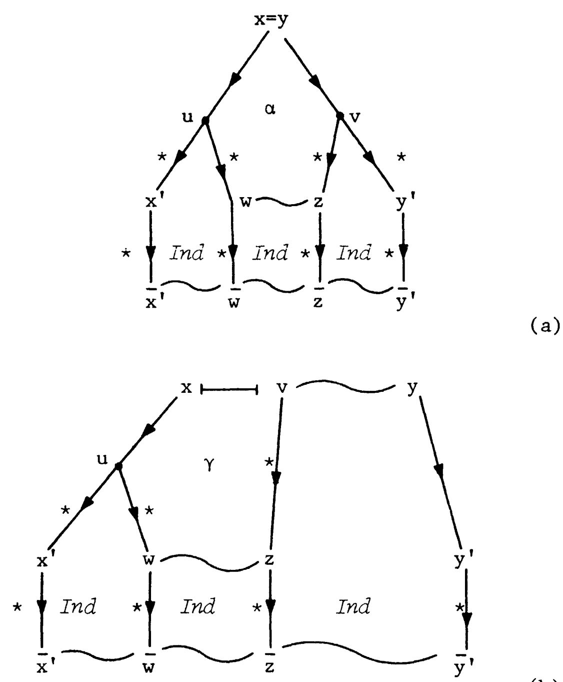



Fig. 4

Remarks Sethi's th. 2.3 [15] is similar to lemma 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 more restrictive : he demands that $\rightarrow \cup \sim$ be bounded, because he constructs explicitly the ordinal of the induction.

Nivat shows in [9] an equivalent of lemma 8, for a reduction relation defined by word rewritings in a free monoïd.

Remark the symmetry between properties $\alpha$ and $\gamma$. Both express localizing the confluence check to <u>one</u> application of the generators of respectively $\overset{*}{\rightarrow}$ and $\sim$.

The rather strong condition that $\rightarrow.\sim$ be noetherian is essential. For instance, Fig. 5 gives an example (inspired from the one in Fig. 2) where $\rightarrow$ is noetherian and $\alpha$ and $\gamma$ are verified. Still, $\rightarrow$ is not confluent modulo $\sim$. This corresponds to the infinite $\blacktriangleright\!\!\rightarrow$-sequence of pairs $\langle y,x_i\rangle$.

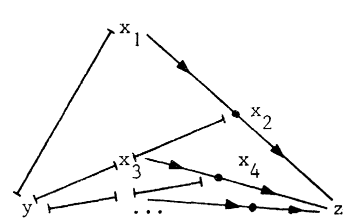



Fig. 5

## II. APPLICATIONS TO TERM REWRITING SYSTEMS

### 1 - The lattice $\mathcal{T}$ 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 [5], and related results in [10], [12] and [13].

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

Let $\Sigma = \mathcal{V} \cup \mathcal{F}$, $\Sigma^*$ the free monoïd on $\Sigma$. We define the set $\mathcal{T}$ of *terms* as the smallest subset of $\Sigma^*$ containing $\mathcal{V}$ and closed by operators : $t_1, \ldots, t_n \in \mathcal{T} \to F\, t_1 \ldots t_n \in \mathcal{T}$ for every $F \in \mathcal{F}_n$, $n \geq 0$.

$\mathcal{T}$ is thus isomorphic to the free $\alpha$-graded algebra. For $t \in \mathcal{T}$, we define :

- $\mathcal{V}(t) \subset \mathcal{V}$ : the set of variables of t by :

$$\begin{cases} \mathcal{V}(x) = \{x\} & \forall x \in \mathcal{V} \\ \mathcal{V}(F\, t_1 \ldots t_n) = \bigcup_{i=1}^{n} \mathcal{V}(t_i) & \forall F \in \mathcal{F}_n \end{cases}$$

- $\nu(t) = |\mathcal{V}(t)| \in \mathbb{N}$. If $\nu(t) = 0$ we say term t is *ground*.

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

$$\begin{cases} \lambda(x) = 1 & \forall x \in \mathcal{V} \\ \lambda(F\, t_1 \ldots t_n) = 1 + \sum_{i=1}^{n} \lambda(t_i) & \forall F \in \mathcal{F}_n \end{cases}$$

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

$$\begin{cases} \theta(x) = 0 & \forall x \in \mathcal{V} \\ \theta(F\, t_1 \ldots t_n) = 1 + \sum_{i=1}^{n} \theta(t_i) & \forall F \in \mathcal{F}_n \end{cases}$$

- $\mu(t) = \lambda(t) - \nu(t)$. It is easy to show $\mu(t) \geq \theta(t)$, which shows $\mu(t) \geq 0$, and $\mu(t) = 0 \Leftrightarrow t \in \mathcal{V}$ .

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

Let $\mathbb{N}_+^*$ be the set of sequences of positive integers, $\varepsilon$ the empty sequence in $\mathbb{N}_+^*$, . the concatenation of sequences. We shall call the members of $\mathbb{N}_+^*$ *occurrences*, and denote them u,v,w. We define the *prefix order* $\prec$ in $\mathbb{N}_+^*$ by : $u \prec v \Leftrightarrow \exists w \quad v = u.w$ ; in this case we define: $v/u = w$. Occurrences u and v are said to be *disjoint*, and we note $u|v$, iff $\neg u \prec v$ and $\neg v \prec u$.

For any $t \in \mathcal{T}$, we define its *set of occurrences* as the finite set $\mathcal{O}(t) \subset \mathbb{N}_+^*$, and for any $u \in \mathcal{O}(t)$, the *subterm of* t *at* u , $t/u \in \mathcal{T}$, as follows.

. if $t = x \in \mathcal{V}$ then $\mathcal{O}(t) = \{\varepsilon\}$, $t/\varepsilon = t$.

. if $t = F\, t_1 \ldots t_n$ then $\mathcal{O}(t) = \{\varepsilon\} \cup \{iu \mid i \leq n, u \in \mathcal{O}(t_i)\}$, $t/\varepsilon = t$, $t/iu = t_i/u$.

We say that u is an *occurrence of* t/u *in* t.
Finally, for $t \in \mathcal{T}$, $u \in \mathcal{O}(t)$ and $t' \in \mathcal{T}$, we define $t[u \leftarrow t'] \in \mathcal{T}$ by :

. $t[\varepsilon \leftarrow t'] = t'$

. $(F\, t_1 \ldots t_n)[iu \leftarrow t'] =$
$$F\, t_1 \ldots t_{i-1} (t_i[u \leftarrow t'])\, t_{i+1} \ldots t_n \quad i \leq n$$

These definitions are consistent with [14, 17], 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 [14].

**Proposition 3**

a) $\forall t_1, t_2 \in \mathcal{T}$, $u \in \mathcal{O}(t_1)$, $v \in \mathcal{O}(t_2)$ :

a-1 - $t_1[u \leftarrow t_2]/u.v = t_2/v$ embedding

a-2 - $t_1[u \leftarrow t_2[v \leftarrow t_3]] = t_1[u \leftarrow t_2][u.v \leftarrow t_3]$ associativity

b) $\forall t_1, t_2, t_3 \in \mathcal{T}$, u, $v \in \mathcal{O}(t_1)$, with $u|v$ :

b-1 - $t_1[u \leftarrow t_2]/ v = t_1/v$ persistence

b-2 - $t_1[u \leftarrow t_2][v \leftarrow t_3] = t_1[v \leftarrow t_3][u \leftarrow t_2]$ commutativity

c) $\forall t_1, t_2 \in \mathcal{T}$, u, $v \in \mathcal{O}(t_1)$, with $v \prec u$ :

c-1 - $t_1/u = (t_1/v)/(u/v)$ cancellation

c-2 - $t_1[u \leftarrow t_2]/v = (t_1/v)[u/v \leftarrow t_2]$ distributivity

**Definitions**

A *substitution* is a mapping $\sigma$ from $\mathcal{V}$ to $\mathcal{T}$ , with $\sigma(x)=x$ almost everywhere . Substitutions are noted $\sigma$, $\rho$, $\eta$. Substitutions are extended as morphisms of $\mathcal{T}$, by :

$$\sigma(F\, t_1 \ldots t_n) = F\, \sigma(t_1) \ldots \sigma(t_n).$$

The bijective morphisms are called *permutations*, and are noted $\xi$, $\xi'$, ... We call *domain* of substitution $\sigma$ the finite set $\mathcal{D}(\sigma) = \{x \in \mathcal{V} \mid \sigma(x) \neq x\} \subset \mathcal{V}$. For $V \subset \mathcal{V}$, we define the restriction $\sigma \restriction V$ of $\sigma$ to V as :

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

For all $\sigma$, t and V, $\mathcal{V}(t) \subset V \Rightarrow \sigma(t) = (\sigma \restriction V)(t)$, and $\mathcal{D}(\sigma) \cap \mathcal{V}(t) = \emptyset \Rightarrow \sigma(t) = t$.

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

$$t \leq t' \Leftrightarrow \exists \sigma \quad t' = \sigma(t)$$

It can be shown that if such a $\sigma$ exists, $\sigma\restriction\mathcal{V}(t)$ is unique. We call it the *match of* t' *by* t, and denote it $t'//t$.

We define $t \equiv t' \Leftrightarrow t \leq t'$ & $t' \leq t$ . It can be shown that $t \equiv t'$ iff there exists a permutation $\xi$ such that $t' = \xi\ t$. Remark that $\nu$, $\lambda$ and $\theta$ are preserved by $\equiv$. Finally, we define :

$$t > t' \Leftrightarrow t' \leq t \ \&\ t \not\leq t' \ .$$

Proposition 4 $>$ is a noetherian relation in $\mathcal{T}$.

The proof of this proposition is given in [5], and consists in showing $t > t' \Rightarrow \mu(t) > \mu(t')$.

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

. $F\ t_1 \ldots t_n \wedge F\ t'_1 \ldots t'_n = F(t_1 \wedge t'_1) \ldots (t_n \wedge t'_n)\ \forall F \in \mathcal{F}_n$

. $t \wedge t' = \varphi(t,t')$ in all other cases.

$t \wedge t'$ is uniquely determined from $\varphi$, and for distinct $\varphi$'s is unique up to $\equiv$.

Proposition 5 $t \wedge t'$ is a glb of t and t' under the subsumption ordering.

Let $\hat{\mathcal{T}}$ be the quotient set $\mathcal{T}/\equiv$, completed with a maximum element $\top$. From propositions 4 and 5 follows directly :

Theorem 1 $\hat{\mathcal{T}}$ is a complete lattice.

The proof of proposition 5, of theorem 1 and various other results concerning the structure of $\mathcal{T}$ and of its completion by infinite terms, may be found in [5]. See also [10] and [12] for similar constructions.

A direct consequence of theorem 1 is the existence, for any two terms t and t' that have a common instance (i.e. s.t. $\exists\ \sigma,\sigma'\ \sigma(t) = \sigma'(t')$), of an lub $t \vee t'$, most general such instance. The term $t \vee t'$ is unique modulo $\equiv$, and may be found by the *unification algorithm* [13]. Efficient ways of unifying terms are described in [5, 18]. If such an lub exists, we write $t \Delta t'$, and say that t and t' are *unifiable*.

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

Proposition 6 $\mathcal{O}(\sigma(t)) = \mathcal{O}(t) \cup \bigcup_{t/u \in \mathcal{V}} \{u.v \mid v \in \mathcal{O}(\sigma(t/u))\}$

$\forall u \in \mathcal{O}(t)$ : . if $t/u = t' \notin \mathcal{V}$ then $\sigma(t)/u = \sigma(t')$
. if $t/u = x \in \mathcal{V}$ then $\sigma(t)/u.v = \sigma(x)/v$. $\forall v \in \mathcal{O}(\sigma(x))$.

Proposition 7 $\forall t, t' \in \mathcal{T}, \forall u \in \mathcal{O}(t)\ \sigma(t)[u \leftarrow \sigma(t')] = \sigma(t[u \leftarrow t'])$.

## 2 - Term rewriting systems and critical pairs

Definition

We call *term rewriting system* any set $\mathcal{R}$ of pairs of terms $\langle\gamma,\delta\rangle$, such that $\mathcal{V}(\delta) \subset \mathcal{V}(\gamma)$.
We say that u is a *redex of* $\mathcal{R}$ *in term* t iff $u \in \mathcal{O}(t)$, and $\exists\ \langle\gamma,\delta\rangle \in \mathcal{R}$ such that $\gamma \leq t/u$. Taking $\sigma = (t/u)//\gamma$ and $t' = t\ [u \leftarrow \sigma(\delta)]$, we say that t *reduces to* t' *in* u, and we write $t \underset{\mathcal{R}}{\rightarrow} t'$ or, when we want to specify the redex, $t \xrightarrow[\mathcal{R}]{[u]} t'$.

Example Let $\mathcal{R} = \{\langle Ix,x\rangle\}$ , with $\alpha(I) = 1$.

We have $IIx \xrightarrow[\mathcal{R}]{[\varepsilon]} Ix$, and also $IIx \xrightarrow[\mathcal{R}]{[1]} Ix$.

Definition

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

- *stable* iff $\forall\sigma\ \forall t,t'\quad t \rightarrow t' \Rightarrow \sigma(t) \rightarrow \sigma(t')$.
- *compatible* iff $\forall \bar{t} \in \mathcal{T} \forall u \in \mathcal{O}(\bar{t})\ \forall t,t'\quad t \rightarrow t' \Rightarrow \bar{t}[u \leftarrow t] \rightarrow \bar{t}[u \leftarrow t']$.

It is easy to show, using propositions 3 and 6, that $\underset{\mathcal{R}}{\rightarrow}$ is the smallest compatible stable relation containing $\mathcal{R}$.

Proposition 8

Let $\rightarrow$ be any compatible relation in $\mathcal{T}$, $\sigma$ and $\sigma'$ be substitutions such that $\begin{cases} \sigma(x) \rightarrow \sigma'(x) \\ \sigma(y) = \sigma'(y) \quad \forall\ y \neq x. \end{cases}$

Let t be any term, and $u_1,\ldots,u_n \in \mathcal{O}(t)$ be all the occurrences of x in t (assumed to be distinct). Defining $t_0 = \sigma(t)$, and $t_i = t_{i-1}[u_i \leftarrow \sigma'(x)]\ \forall i\ \ 1 \leq i \leq n$, we have : $t_i \xrightarrow{n-i} \sigma'(t)\ \forall i\ \ 0 \leq i \leq n$.

We leave the proof of this easy proposition to the reader. Let us 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 [6].

Superposition algorithm

Let $<\gamma_1,\delta_1>$, $<\gamma_2,\delta_2> \in \mathcal{R}$, and $u \in \mathcal{O}(\gamma_1)$ such that $t = \gamma_1/u \notin \mathcal{V}$ and $t \,\Delta\, \gamma_2$. Let $t' \equiv t \vee \gamma_2$, such that $\mathcal{V}(t') \cap \mathcal{V}(\gamma_1) = \emptyset$. We say that the superposition of $<\gamma_2,\delta_2>$ on $<\gamma_1,\delta_1>$ in u determines the *critical pair* $<t_1, t_2>$, defined by :

$$\begin{cases} t_1 = \sigma_1(\gamma_1)\ [u \leftarrow \sigma_2(\delta_2)] \\ t_2 = \sigma_1(\delta_1) \end{cases}$$

where $\sigma_1 = t'//t$ and $\sigma_2 = t'//\gamma_2$.

Remarks : For any $<\gamma_1,\delta_1>$, $<\gamma_2,\delta_2>$ and u the critical pair is unique, up to a permutation. We may choose $<\gamma_2,\delta_2> = <\gamma_1,\delta_1>$, as in example c below. But in this case (and in this case only) we shall not consider the case $u = \varepsilon$, which gives only trivial critical pairs $<\delta,\delta>$.

Examples

For convenience, we use parentheses in our examples :

a) $\gamma_1 = F(x,G(x,A))$, $\delta_1 = H(x)$, $\gamma_2 = G(B,x)$, $\delta_2 = K(x)$ with $u = 2$ determine the pair $t_1 = F(B,K(A))$, $t_2=H(B)$.

b) $\gamma_1 = F(x,H(x'))$, $\delta_1 = P(x',x)$, $\gamma_2 = H(G(x,x'))$, $\delta_2 = Q(x,x')$ with $u = 2$ determine $t_1 = F(x,Q(y,z))$, $t_2 = P(G(y,z),x)$.

c) $\gamma_1 = \gamma_2 = H(H(x))$, $\delta_1 = \delta_2 = K(x)$ with $u = 1$ determine $t_1 = H(K(y))$, $t_2 = K(H(y))$.

Remark : The condition $\mathcal{V}(t') \cap \mathcal{V}(\gamma_1) = \emptyset$ may be replaced by the weaker condition : $\mathcal{V}(t') \cap (\mathcal{V}(\gamma_1) - \mathcal{V}(t)) = \emptyset$. The example b) shows why this condition is necessary : choosing the pair $<F(x,Q(x,x')), P(G(x,x'),x)>$ would be strictly less general than the pair $<t_1,t_2>$ . If we compute t' by unification of t and $\xi(\gamma_2)$, where $\xi$ is a permutation renaming variables in $\mathcal{V}(\gamma_1) \cap \mathcal{V}(\gamma_2)$, we get $\mathcal{V}(t') \subset (\mathcal{V}(t) \cup \mathcal{V}(\xi(\gamma_2)))$, and the condition above is thus satisfied.

Proposition 9

Let $<\gamma_1,\delta_1>$, $<\gamma_2,\delta_2> \in \mathcal{R}$ and $u \in \mathcal{O}(\gamma_1)$ such that $t = \gamma_1/u \notin \mathcal{V}$ and there exist $\sigma_1$ and $\sigma_2$ with $\sigma_1(t) = \sigma_2(\gamma_2)$. Then there exist a critical pair $<t_1,t_2>$ of $\mathcal{R}$ and a substitution $\rho$ such that $\sigma_1(\gamma_1)\ [u \leftarrow \sigma_2(\gamma_2)]=\rho(t_1)$ and $\sigma_1(\delta_1) = \rho(t_2)$.

We shall omit here, for lack of space, the proof of this proposition, which asserts the correctness of the superposition algorithm.

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

Lemma 9

$\underset{\mathcal{R}}{\rightarrow}$ is locally confluent iff for every critical pair $<t_1,t_2>$ of $\mathcal{R}$ we have $t_1 \downarrow t_2$.

Proof

We abbreviate below $\underset{\mathcal{R}}{\rightarrow}$ in $\rightarrow$ .

Using the notations of the superposition algorithm, a critical pair $<t_1, t_2>$ is such that $\sigma_1(\gamma_1) \rightarrow t_1$ and $\sigma_1(\gamma_1) \rightarrow t_2$, which shows the only if part.

For the if part, assume that for every critical pair $<t_1,t_2>$ of $\mathcal{R}$ we have $t_1 \downarrow t_2$. Let t be an arbitrary term, t and t' such that $t \xrightarrow{[u_1]} t'$ and $t \xrightarrow{[u2]} t''$ ; i.e., there exists $<\gamma_1,\delta_1>$, $<\gamma_2,\delta_2>$ in $\mathcal{R}$ and substitutions $\sigma_1$ and $\sigma_2$, with :

$$t/u_1 = \sigma_1(\gamma_1), t/u_2 = \sigma_2(\gamma_2),\ t' = t[u_1 \leftarrow \sigma_1(\delta_1)],$$
$$t'' = t[u_2 \leftarrow \sigma_2(\delta_2)].$$

There are two cases, according to the relative positions of the two redexes :

a) disjoint redexes : $u_1 | u_2$

We have then $t'/u_2 = \sigma_2(\gamma_2)$ by persistence, and similarly $t''/u_1 = \sigma_1(\gamma_1)$. Furthermore, we have $\bar{t} = t'[u_2 \leftarrow \sigma_2(\delta_2)] = t''[u_1 \leftarrow \sigma_1(\delta_1)]$ by commutativity, and therefore $t' \rightarrow \bar{t}$ and $t'' \rightarrow \bar{t}$.

b) prefix redexes.

Let us assume, without loss of generality, that $u_1 \prec u_2$. Let $v = u_2/u_1$. By cancellation, we get $\sigma_1(\gamma_1)/v = \sigma_2(\gamma_2)$ and by distributivity : $t''/u_1 = \sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)]$.

Let us show that there exists $\bar{t}$ such that $\sigma_1(\delta_1) \overset{*}{\rightarrow} \bar{t}$ and $t''/u_1 \overset{*}{\rightarrow} \bar{t}$. It will then follow that $t' \downarrow t''$, by compatibility of $\rightarrow$. According to proposition 6, there are two cases :

b1) $v = v_1.v_2 \quad \gamma_1/v_1 = x \in \mathcal{V}\ \sigma_2(\gamma_2) = \sigma_1(x)/v_2$.

Let us consider substitution $\sigma'_1$ defined by :

$$\begin{cases} \sigma'_1(x) = \sigma_1(x)[v_2 \leftarrow \sigma_2(\delta_2)] \\ \sigma'_1(y) = \sigma_1(y)\ \forall\, y \neq x. \end{cases} \quad \text{and let } \bar{t} = \sigma'_1(\delta_1).$$

We have $\sigma_1(x) \rightarrow \sigma'_1(x)$, and by proposition 8 we get $\sigma_1(\delta_1) \overset{*}{\rightarrow} \bar{t}$ and $\sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)] \overset{*}{\rightarrow} \sigma'_1(\gamma_1)$. Since $\rightarrow$ is stable we get $\sigma'_1(\gamma_1) \rightarrow \bar{t}$, which concludes the proof of b1.

b2) $\exists \gamma \notin \mathcal{V}\ \gamma = \gamma_1/v,\ \sigma_2(\gamma_2) = \sigma_1(\gamma)$.

Using proposition 9, there exists a critical pair $\langle t_1, t_2\rangle$ and a substitution $\rho$ such that $\sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)] = \rho(t_1)$ and $\sigma_1(\delta_1) = \rho(t_2)$. By hypothesis, there exists $t_3$ such that $t_1 \overset{*}{\rightarrow} t_3$ and $t_2 \overset{*}{\rightarrow} t_3$. We may choose $\bar{t} = \rho(t_3)$, and the result follows by stability of $\rightarrow$. □

Remark : Lemma 9 is inspired from Knuth & Bendix [6]. But our proof, contrarily to theirs, does not require $\rightarrow$ to be noetherian. The corollary to th. 5 in [6] is essentially th.2 below.

### Theorem 2

Let $\mathfrak{R}$ be a term rewriting system such that $\underset{\mathfrak{R}}{\rightarrow}$ is noetherian. Let $\hat{t}$ denote an arbitrary $\underset{\mathfrak{R}}{\rightarrow}$-normal form of $t$, for $t \in \mathfrak{T}$. Then $\underset{\mathfrak{R}}{\rightarrow}$ is confluent iff for every critical pair $\langle t_1, t_2\rangle$ of $\mathfrak{R}$ we have $\hat{t}_1 = \hat{t}_2$.

### Proof

$\Rightarrow$ For any critical pair $\langle t_1, t_2\rangle$ of $\mathfrak{R}$, $\exists t\ t \underset{\mathfrak{R}}{\rightarrow} t_1$ & $t \underset{\mathfrak{R}}{\rightarrow} t_2$. If $\underset{\mathfrak{R}}{\rightarrow}$ is confluent, then by lemma 2 $t$ admits a unique $\underset{\mathfrak{R}}{\rightarrow}$-normal form $\hat{t}_1 = \hat{t}_2$. $\Leftarrow$ $\hat{t}_1 = \hat{t}_2$ implies $t_1 \downarrow t_2$, and $\underset{\mathfrak{R}}{\rightarrow}$ is locally confluent by lemma 9, and therefore confluent by lemma 4. □

Remarks : If $\underset{\mathfrak{R}}{\rightarrow}$ is noetherian, we may get $\hat{t}$ by an arbitrary sequence of rewritings using rules of $\mathfrak{R}$ to $t$, termination being guaranteed. Theorem 2 gives us in this case an effective way of testing the confluence of $\underset{\mathfrak{R}}{\rightarrow}$ provided we have only a finite number of critical pairs $\langle t_1, t_2\rangle$. This will happen in particular if $\mathfrak{R}$ is finite.

Theorem 2 gives also hints on how to complete $\mathfrak{R}$ to a confluent system, when it is not : the idea is to include in $\mathfrak{R}$, for every $\langle t_1, t_2\rangle$ such that $\hat{t}_1 \neq \hat{t}_2$, either $\langle t_1, t_2\rangle$, or $\langle t_2, t_1\rangle$, or $\langle t_1, t\rangle$ and $\langle t_2, t\rangle$ for some term $t$. See [6] and [7]. Of course one must show that the new pairs preserve termination, and there is no guarantee that the "completing" process will terminate. We shall come back to this in section 4.

The main difficulty in using th.2 consists in showing $\underset{\mathfrak{R}}{\rightarrow}$ noetherian. For that, one must find a noetherian, stable, compatible strict partial order $\rhd$ such that $\gamma \rhd \delta$ for every $\langle \gamma, \delta\rangle$ in $\mathfrak{R}$. Knuth & Bendix propose in [6] a tricky lexicographic ordering for this purpose. A somewhat more general method consists in defining an interpretation $\chi$ of terms over $\mathbb{N}$. To be effective, each $F$ in $\mathfrak{F}_n$ will be interpreted as a recursive total function of n arguments $\chi(F)$. Interpretations being morphisms, compatibility is insured. To prove $\underset{\mathfrak{R}}{\rightarrow}$ noetherian, it suffices to show that, for every $\langle \gamma, \delta\rangle$ in $\mathfrak{R}$, $\chi(\gamma) > \chi(\delta)$ is identically true for all values of $\chi(x_i)$. This is essentially the method (with $\chi(F)$ being polynomials) used by Lankford in [7]. For instance, the ten group reduction rules of Knuth & Bendix may be shown to define a noetherian rewriting system, using the interpretation :

$$\begin{cases} \chi(.) = \lambda\ x\ y.\ x(1+2y) \\ \chi(-) = \lambda\ x.\ x^2 \\ \chi(e) = 2 \qquad\qquad \text{over integers} > 1. \end{cases}$$

## 3 - Free 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 $\langle t_1, t_2\rangle$ of $\mathfrak{R}$ a condition stronger than $t_1 \downarrow t_2$, inspired from the strong confluency condition.

### Definition

A term rewriting system $\mathfrak{R}$ is $\varepsilon$-$\varepsilon$ *closed* iff, for every critical pair $\langle t_1, t_2\rangle$ of $\mathfrak{R}$, there exists $t_3$ such that $t_1 \overset{\varepsilon}{\underset{\mathfrak{R}}{\rightarrow}} t_3$ and $t_2 \overset{\varepsilon}{\underset{\mathfrak{R}}{\rightarrow}} t_3$.

Remark that this condition alone is not sufficient to ensure confluence, as shown by the counter-example :

$$\mathfrak{R} = \{\langle F(x,x),A\rangle,\ \langle F(x,G(x)),B\rangle,\ \langle C,G(C)\rangle\}$$

since the term F(C,C) possesses two distinct normal forms A and B. Note that $\mathfrak{R}$ has no critical pair.

### Definition

$\mathfrak{R}$ is *left-free* iff $\forall \langle \gamma, \delta\rangle \in \mathfrak{R}$ $\gamma$ is free.
$\mathfrak{R}$ is *right-free* iff $\forall \langle \gamma, \delta\rangle \in \mathfrak{R}$ $\delta$ is free.

### Lemma 10

If $\mathfrak{R}$ is a left and right-free $\varepsilon$-$\varepsilon$ closed term rewriting system, $\underset{\mathfrak{R}}{\rightarrow}$ is strongly confluent.

### Proof

Let us assume $\mathfrak{R}$ is left and right free and $\varepsilon$-$\varepsilon$ closed, and let us abbreviate $\underset{\mathfrak{R}}{\rightarrow}$ in $\rightarrow$. Let $t \xrightarrow{[u_1]} t'$ and $t \xrightarrow{[u_2]} t''$; i.e., $\exists \langle \gamma_1, \delta_1\rangle, \langle \gamma_2, \delta_2\rangle \in \mathfrak{R}$, and substitutions $\sigma_1$ and $\sigma_2$ such that $t/u_1 = \sigma_1(\gamma_1)$, $t' = t[u_1 \leftarrow \sigma_1(\delta_1)]$, $t/u_2 = \sigma_2(\gamma_2)$, and $t'' = t[u_2 \leftarrow \sigma_2(\delta_2)]$. We show there exists $\bar{t}$ such that $t' \overset{\varepsilon}{\rightarrow} \bar{t}$ and $t'' \overset{\varepsilon}{\rightarrow} \bar{t}$.

There are two cases, according to the relative positions of redexes $u_1$ and $u_2$ ; the proof is similar to that of lemma 9.

a) disjoint redexes : $u_1 | u_2$

We take $\bar{t} = t'[u_2 \leftarrow \sigma_2(\delta_2)] = t''[u_1 \leftarrow \sigma_1(\delta_1)]$.

b) prefix redexes ; let us assume, without loss of generality, that $u_1 \prec u_2$.

Let $v = u_2/u_1$. We have $\sigma_2(\gamma_2) = \sigma_1(\delta_1)/v$ and $t'' = t[u_1 \leftarrow \sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)]]$.

b1) $\sigma_2(\gamma_2)$ is completely introduced by $\sigma_1$ :

$\exists\, v_1, v_2 \quad v = v_1.v_2,\ \gamma_1/v_1 = x \in \mathcal{V},\ \sigma_1(x)/v_2 = \sigma_2(\gamma_2)$.

We define a substitution $\sigma_3$ by :

$$\begin{cases} \sigma_3(x) = \sigma_1(x)[v_2 \leftarrow \sigma_2(\delta_2)]. \\ \sigma_3(y) = \sigma_1(y) \qquad \forall\, y \neq x. \end{cases}$$

and we take $\bar{t} = t[u_1 \leftarrow \sigma_3(\delta_1)]$.

$\mathfrak{R}$ being left-free, x occurs in $\gamma_1$ only in occurrence $v_1$, and we get :

$$\sigma_3(\gamma_1) = \sigma_1(\gamma_1)[v_1 \leftarrow \sigma_3(x)] = \sigma_1(\gamma_1)[v_1 \leftarrow \sigma_1(x)[v_2 \leftarrow \sigma_2(\delta_2)]]$$
$$= \sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)] \text{ , whence } t'' = t[u_1 \leftarrow \sigma_3(\gamma_1)],$$

which shows $t'' \rightarrow \bar{t}$. There are again two cases :

b1-i ) $x \notin \mathcal{V}(\delta_1)$

Then trivially $\sigma_3(\delta_1) = \sigma_1(\delta_1)$ and therefore $\bar{t} = t'$.

b1-ii) $\exists\, w \in \mathcal{O}(\delta_1) \quad \delta_1/w = x$.

$\mathfrak{R}$ being right-free, w is the unique occurrence of x in $\delta_1$, and we get :

$$\sigma_3(\delta_1) = \sigma_1(\delta_1)[w \leftarrow \sigma_1(x)[v_2 \leftarrow \sigma_2(\delta_2)]] =$$
$$= \sigma_1(\delta_1)[w.v_2 \leftarrow \sigma_2(\delta_2)].$$

Since $\sigma_1(\delta_1)/w.v_2 = \sigma_2(\gamma_2)$, we get $t' \rightarrow \bar{t}$, using redex $u.w.v_2$.

b2) $\sigma_2(\gamma_2)$ partially exists in $\gamma_1$ :

$v \in \mathcal{O}(\gamma_1), \gamma = \gamma_1/v \notin \mathcal{V},\ \sigma_1(\gamma) = \sigma_2(\gamma_2)$.

According to proposition 9, there exists a critical pair $<t_1,t_2>$ and a substitution $\rho$ such that: $\rho(t_1) = \sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)]$ and $\rho(t_2) = \sigma_1(\delta_1)$, and thus $t' = t[u_1 \leftarrow \rho(t_2)]$ and $t'' = t[u_1 \leftarrow \rho(t_1)]$.

By closure hypothesis, there exists $t_3$ such that $t_1 \overset{\varepsilon}{\rightarrow} t_3$ and $t_2 \overset{\varepsilon}{\rightarrow} t_3$, and therefore $t' \overset{\varepsilon}{\rightarrow} \bar{t}$ and $t'' \overset{\varepsilon}{\rightarrow} \bar{t}$, with $\bar{t} = t[u_1 \leftarrow \rho(t_3)]$. □

Using lemma 5 we get :

<u>Corollary</u> : If $\mathfrak{R}$ is a left and right free ε-ε closed system, $\underset{\mathfrak{R}}{\rightarrow}$ is confluent.

<u>Remarks</u> : Without change to the proof above, we could replace the condition "ε-ε closed" by the slightly more general condition : "for every critical pair $<t_1,t_2>$ of $\mathfrak{R}$, there exist $t_3$ and $t_4$ such that $t_1 \underset{\mathfrak{R}}{\overset{*}{\rightarrow}} t_3$, $t_2 \underset{\mathfrak{R}}{\overset{\varepsilon}{\rightarrow}} t_3$, $t_1 \underset{\mathfrak{R}}{\overset{\varepsilon}{\rightarrow}} t_4$ and $t_2 \underset{\mathfrak{R}}{\overset{*}{\rightarrow}} t_4$".

If $\mathfrak{R}$ is only left-free and ε-ε closed, $\underset{\mathfrak{R}}{\rightarrow}$ is not necessarily confluent, as shown by the following counter-example :

$\mathfrak{R}$ = {<F(A,A), G(B,B)>, <A,A'>, <F(A',x),F(x,x)>, <F(x,A'),F(x,x)>, <G(B,B),F(A,A)>, <B,B'>, <G(B',x),G(x,x)>, <G(x,B'),G(x,x)>}

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

Still, it is very desirable to find sufficient conditions for a term rewriting system to be confluent that do not depend on right-freeness, 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.

A reduction relation $\twoheadrightarrow$ over $\mathcal{T}$ is said to be a *congruence* iff it is reflexive and it verifies :

$$t_1 \twoheadrightarrow t_1' \ \&\ \ldots\ \&\ t_n \twoheadrightarrow t_n' \Rightarrow F\ t_1 \ldots t_n \twoheadrightarrow F\ t_1' \ldots t_n' \qquad \forall\, F \in \mathcal{F}_n.$$

For any term rewriting $\mathfrak{R}$, we define a relation $\underset{\mathfrak{R}}{\twoheadrightarrow}$ (parallel reduction) as follows.

Let $t \in \mathcal{T}$, and $U = \{u_1,\ldots,u_n\}$ be a set of mutually disjoint redexes of $\mathfrak{R}$ in t : $\forall\, i \leq n \quad t/u_i = \sigma_i(\gamma_i)$, with $<\gamma_i,\delta_i> \in \mathfrak{R}$. We define $t' = t[u_i \leftarrow \sigma_i(\delta_i) | i \leq n]$ as the term $t[u_1 \leftarrow \sigma_1(\delta_1)]\ldots[u_n \leftarrow \sigma_n(\delta_n)]$. It is easy to show, by commutativity, that the order in which we reduce redexes is irrelevant. We say that t *reduces in parallel* to t', which we write $t \underset{\mathfrak{R}}{\twoheadrightarrow} t'$. It is easy to show that $\underset{\mathfrak{R}}{\twoheadrightarrow}$ is the smallest congruence containing $\underset{\mathfrak{R}}{\rightarrow}$, and that it is stable.

Proposition 10

For any substitution $\sigma$ and term t :

$$\sigma(t) = t[u \leftarrow \sigma(x) \mid t/u = x \in \mathcal{V}] .$$

Proposition 11 Let $\nrightarrow\!\!\!\!\rightarrow$ be any congruence.

Let U be a set of disjoint occurrences in term t. Then $\forall\, u \in U \; t'_u \twoheadrightarrow t''_u \Rightarrow t[u \leftarrow t'_u \mid u \in U] \twoheadrightarrow t[u \leftarrow t''_u \mid u \in U]$.

Propositions 10 and 11 are easily proved by induction on t.

Definition

A term rewriting system $\mathfrak{R}$ is *parallel-0 closed* iff, for every critical pair $<t_1,t_2>$ of $\mathfrak{R}$ we have $t_1 \underset{\mathfrak{R}}{\twoheadrightarrow} t_2$.

Lemma 11

If $\mathfrak{R}$ is a left-free parallel-0 closed term rewriting system, $\underset{\mathfrak{R}}{\twoheadrightarrow}$ is strongly confluent.

Proof We abbreviate $\underset{\mathfrak{R}}{\twoheadrightarrow}$ in $\twoheadrightarrow$.

Let $t \twoheadrightarrow t'$ with set of redexes U, and $t \twoheadrightarrow t''$ with set V.

Let $P = \{u \in U \mid \exists\, v \in V \;\; v \prec u\} \cup \{v \in V \mid \exists\, u \in U \;\; u \prec v\}$ and $Q = [(U \cup V) - P] \cup (U \cap V)$.

P and Q are two sets of mutually disjoint occurrences of t. We prove $\exists\, \bar{t} \;\; t' \twoheadrightarrow \bar{t} \;\; \& \; t'' \twoheadrightarrow \bar{t}$ by complete induction on $p(t,U,V) = \sum_{w \in P} \lambda(t/w)$.

1) Let u be any redex in Q. We may assume, without loss of generality, that $u \in U$. Let $V_u = \{v \in V \mid u \prec v\}$. We shall now show the existence of a term $t_u$ such that $t'/u \twoheadrightarrow t_u$ and $t''/u \twoheadrightarrow t_u$.

Let $<\gamma,\delta>$ be the rule of $\mathfrak{R}$ used in u in the parallel reduction U, with substitution $\sigma$ : $t/u = \sigma(\gamma)$ and $t'/u = \sigma(\delta)$.

There are two cases :

a) No v is critical in u, i.e. for all v in $V_u$, we have $v/u = w.w'$ with $\gamma/w = x \in \mathcal{V}$. (This covers the case $V_u = \emptyset$).

Conversely, let x be any variable of $\gamma$. $\gamma$ being free by hypothesis, there is a unique $w \in \mathcal{O}(\gamma)$ such that $\gamma/w = x$. Let W' be the set of occurrences in $\sigma(x)$ of redexes of V : $W' = \{v/u.w \mid u.w \prec v \in V_u\}$. Let $<\gamma_i,\delta_i>$ be the rule of $\mathfrak{R}$ corresponding to $w'_i$ in the reduction V, with substitution $\sigma_i$ : $\gamma/w.w'_i = \sigma_i(\gamma_i)$. Let us construct a substitution $\sigma'$ by defining $\sigma'(x) = \sigma(x)[w'_i \leftarrow \sigma_i(\delta_i) \mid w'_i \in W']$, for every x in $\gamma$.

We have $\sigma(x) \twoheadrightarrow \sigma'(x)$, and therefore $\sigma(\delta) \twoheadrightarrow \sigma'(\delta)$, using propositions 10 and 11. But also $t''/u = \sigma'(\gamma)$ by construction, using propositions 3 and 10. We may therefore choose $t_u = \sigma'(\delta)$.

b) Let $v_1$ in $V_u$ be critical in u, i.e. $\gamma/w \notin \mathcal{V}$, with $w = v_1/u$.

Let $<\gamma_1,\delta_1>$ be the rule of $\mathfrak{R}$ corresponding to $v_1$ in the reduction V, with substitution $\sigma_1$. Using proposition 9, there exists a critical pair $<t_1,t_2>$ of $\mathfrak{R}$ and a substitution $\rho$ such that $t'/u = \rho(t_2)$ and $\hat{t} = t/u[w \leftarrow \sigma_1(\delta_1)] = \rho(t_1)$. By closure hypothesis $t_1 \twoheadrightarrow t_2$, and by stability of $\twoheadrightarrow$ we get $\hat{t} \twoheadrightarrow t'/u$. Let $\hat{W}$ be the set of redexes of $\hat{t}$ in this reduction.

We have also $\hat{t} \twoheadrightarrow t''/u$, using the set of redexes $V' = \{v/u \mid v \in V_u - \{v_1\}\}$. Furthermore, $p(\hat{t},V',\hat{W}) \leq \sum_{v' \in V'} \lambda(t/u.v') < \sum_{v \in V} \lambda(t/v) \leq p(t,U,V)$ (by cases according to the position of v' relatively to the family $\hat{W}$). We may therefore use the induction hypothesis, showing the existence of $t_u$.

2) We now consider $\bar{t} = t[u \leftarrow t_u \mid u \in Q]$. Since Q dominates all the redexes in U, we have $t' = t[u \leftarrow t'/u \mid u \in Q]$ and similarly for t". Using proposition 11, we get $t' \twoheadrightarrow \bar{t}$ and $t'' \twoheadrightarrow \bar{t}$, which concludes the proof. □

Using lemma 5 and the fact that $\overset{*}{\twoheadrightarrow} = \overset{*}{\longrightarrow}$, we get :

Corollary Any left-free parallel-0 closed term rewriting system is confluent.

This result is important in practice. It can be used for instance to show the consistence of operational semantics for recursive programming languages. It is the generalization to schemas of the main theorem of Rosen [14], which applies only to ground terms, and which requires 1-0 closure. Notice that Rosen's theorem 6.5 gives only a very particular case of lemma 11 (no critical pairs).

## 4 - Confluent equational theories

We shall now use the results of I-3 to extend the applicability of lemma 9.

We suppose that we are interested in an equational first-order theory $\mathcal{X}$. We assume that the rules of inference of substitution of terms for free variables and of replacement of equals are valid.

Suppose we partition $\mathcal{X}$ in $\mathcal{R} \cup \mathcal{E}$, where $\mathcal{R}$ is a term rewriting system and $\mathcal{E}$ is a set of equations. We assume that $\forall\ \langle\gamma,\delta\rangle \in \mathcal{R}\ \mathcal{V}(\delta) \subset \mathcal{V}(\gamma)$, and furthermore

$\forall\ \gamma=\delta\ \in \mathcal{E}\ \mathcal{V}(\delta) = \mathcal{V}(\gamma)$.

As before, $\underset{\mathcal{R}}{\rightarrow}$ (abbreviated below $\rightarrow$) will denote the smallest compatible stable relation containing $\mathcal{R}$. We also define $\underset{\mathcal{E}}{\longmapsto}$ (abbreviated below $\longmapsto$) as the smallest compatible stable symmetric relation containing $\mathcal{E}$. Note that $\mathcal{X} \vdash t = t' \iff t(\rightarrow \cup \overset{-1}{\rightarrow} \cup \longmapsto)^{*} t'$.

We say that $\mathcal{X}$ is a *confluent equational theory* iff $\rightarrow$ is confluent modulo $\overset{*}{\longmapsto}$. In this case, provided $\rightarrow$ normalizes $\mathcal{T}$, lemma 6 gives us a way of reducing the problem $\mathcal{X} \vdash t = t'$ to the problem $\hat{t} \sim \hat{t}'$, where $\hat{t}$ and $\hat{t}'$ are $\rightarrow$-normal forms of respectively t and t', and $\sim\ = \overset{*}{\longmapsto}$.

We shall now show how lemma 9 can be generalized to confluent equational theories, which will give sufficient conditions for an equational theory to be confluent, using lemma 8.

Let us recall property $\alpha$ of definition D11 :

$\alpha : \forall\ t, t', t''\quad t \rightarrow t'\ \&\ t \rightarrow t'' \Rightarrow t' \overset{\sim}{\downarrow} t''$

where $t' \overset{\sim}{\downarrow} t'' \iff \exists\ \bar{t}', \bar{t}''\quad t' \overset{*}{\rightarrow} \bar{t}'\ \&\ t'' \overset{*}{\rightarrow} \bar{t}''\ \&$
$\bar{t}' \sim \bar{t}''$.

### Lemma 12

$\langle\mathcal{R},\mathcal{E}\rangle$ verifies property $\alpha$ iff for every critical pair $\langle t_1,t_2\rangle$ of $\mathcal{R}$ we have $t_1 \overset{\sim}{\downarrow} t_2$.

### Proof

The proof follows closely that of lemma 9. We use the same notation and indicate here only the points that differ.

Parts a and b1 are kept unchanged.
For part b2, let $\langle t_1,t_2\rangle$ be the critical pair of $\mathcal{R}$ involved.

By hypothesis, there exist $t_3$ and $t_4$ such that $t_1 \overset{*}{\rightarrow} t_3$, $t_2 \overset{*}{\rightarrow} t_4$ and $t_3 \sim t_4$. Let us consider $\bar{t}_1 = \rho(t_3)$ and $\bar{t}_2 = \rho(t_4)$.

We get here $\sigma_1(\delta_1) = \rho(t_2) \overset{*}{\rightarrow} \bar{t}_2$ since $\rightarrow$ is stable and $t''/u_1 = \rho(t_1) \overset{*}{\rightarrow} \bar{t}_3$ since $\rightarrow$ is stable. Therefore $\sigma_1(\delta_1) \overset{\sim}{\downarrow} t''/u_1$, and thus $t' \overset{\sim}{\downarrow} t''$ since $\rightarrow$ and $\longmapsto$ are compatible, which concludes the proof. □

We want now to get a similar result for property $\gamma$, which we recall here : $\gamma : \forall\ t, t', t''\quad t \rightarrow t'\ \&\ t \longmapsto t'' \Rightarrow t' \overset{\sim}{\downarrow} t''$.

### Definition

Let $\langle\mathcal{R},\mathcal{E}\rangle$ be an equational theory. We call *critical pair of* $\mathcal{E}/\mathcal{R}$ any pair $\langle t_1,t_2\rangle$ as constructed by the superposition algorithm, but now applied to $\gamma_1$, $\delta_1$, $\gamma_2$, $\delta_2$ such that :

. either $\gamma_1 = \delta_1 \in \mathcal{E}$ or $\delta_1 = \gamma_1 \in \mathcal{E}$, and $\langle\gamma_2,\delta_2\rangle \in \mathcal{R}$

. or $\langle\gamma_1,\delta_1\rangle \in \mathcal{R}$ and $\gamma_2 = \delta_2 \in \mathcal{E}$ or $\delta_2 = \gamma_2 \in \mathcal{E}$.

### Lemma 13

Let $\langle\mathcal{R},\mathcal{E}\rangle$ be an equational theory such that $\mathcal{R}$ is left-free. Then property $\gamma$ holds iff for every critical pair $\langle t_1,t_2\rangle$ of $\mathcal{E}/\mathcal{R}$ we have $t_1 \overset{\sim}{\downarrow} t_2$.

### Proof

The proof follows the same general pattern as that of lemma 9.
Using the notations of the superposition algorithm, a critical pair $\langle t_1,t_2\rangle$ of $\mathcal{E}/\mathcal{R}$ is such that $\sigma_1(\gamma_1) \rightarrow t_1$ and $\sigma_1(\gamma_1) \longmapsto t_2$, which shows the only if part.

For the if part, assume that for every critical pair $\langle t_1,t_2\rangle$ of $\mathcal{E}/\mathcal{R}$ : $t_1 \overset{\sim}{\downarrow} t_2$.
Let t be an arbitrary term, t' and t'' such that :

$$t \xrightarrow{[u_1]} t' \text{ and } t \overset{[u_2]}{\longmapsto} t'' ;$$

i.e. $\exists \langle\gamma_1,\delta_1\rangle \in \mathcal{R}$, $\gamma_2 = \delta_2 \in \mathcal{E}$, and substitutions $\sigma_1$, $\sigma_2$ such that $t/u_1 = \sigma_1(\gamma_1), t/u_2 = \sigma_2(\gamma_2)$, $t' = t[u_1 \leftarrow \sigma_1(\delta_1)]$, $t'' = t[u_2 \leftarrow \sigma_2(\delta_2)]$ (the symmetric case is obtained in replacing below $\gamma_2$ by $\delta_2$ and conversely throughout).

There are here three cases, according to the relative positions of the two redexes :

a) disjoint redexes : $u_1 | u_2$

With $\bar{t} = t'[u_2 \leftarrow \sigma_2(\delta_2)] = t''[u_1 \leftarrow \sigma_1(\delta_1)]$ we get $t' \longmapsto \bar{t}$ and $t'' \rightarrow \bar{t}$, and therefore $t' \overset{\sim}{\downarrow} t''$.

b) $u_1 \prec u_2$ - Let $v = u_2/u_1$.

We have $\sigma_1(\gamma_1)/v = \sigma_2(\gamma_2)$, and $t''/u_1 = \sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)]$ There are two cases :

b1) $v = v_1.v_2$, $\gamma_1/v_1 = x \in \mathcal{V}$, $\sigma_2(\gamma_2) = \sigma_1(x)/v_2$.

Let us consider substitution $\sigma'_1$ defined by :

$$\begin{cases} \sigma'_1(x) = \sigma_1(x)\ [v_2 \leftarrow \sigma_2(\delta_2)] \\ \sigma'_1(y) = \sigma_1(y) \quad \forall\ y \neq x \end{cases}$$

and let $\bar{t} = \sigma'_1(\delta_1)$.

We have $\sigma_1(\delta_1) \overset{*}{\vdash\!\dashv} \bar{t}$ by the analogue of proposition 8.

Also $\sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)] = \sigma'_1(\gamma_1)$, since $v_1$ is the only occurrence of x in $\gamma_1$, $\mathcal{R}$ being left-free by hypothesis.

$\sigma'_1(\gamma_1) \rightarrow \bar{t}$ by stability of $\rightarrow$, and thus, taking $\hat{t} = t[u_1 \leftarrow \bar{t}]$, we get $t' \overset{*}{\vdash\!\dashv} \hat{t}$ and $t'' \rightarrow \hat{t}$, by compatibility of $\rightarrow$ and $\vdash\!\dashv$.

b2) $\exists\ \gamma \notin \mathcal{V}$ $\gamma = \gamma_1/v$ $\sigma_2(\gamma_2) = \sigma_1(\gamma)$.

Similarly to proposition 9, there exists a critical pair $<t_1,t_2>$ of $\mathcal{E}/\mathcal{R}$ and a substitution $\rho$ such that :

$\sigma_1(\delta_1) = \rho(t_2)$ and $\sigma_1(\gamma_1)[v \leftarrow \sigma_2(\delta_2)] = \rho(t_1)$.

By hypothesis, $t_1 \overset{\sim}{\downarrow} t_2$, whence $\rho(t_2) \overset{\sim}{\downarrow} \rho(t_1)$ by stability, and $t' \overset{\sim}{\downarrow} t''$ by compatibility. This concludes case b.

c) $u_2 \prec u_1$ - Let $v = u_1/u_2$.

Similarly to b, there are two cases :

c1) $v = v_1.v_2$, $\gamma_2/v_1 = x \in \mathcal{V}$, $\sigma_1(\gamma_1) = \sigma_2(x)/v_2$.

We define substitution $\sigma'_2$ by :

$$\begin{cases} \sigma'_2(x) = \sigma_2(x)[v_2 \leftarrow \sigma_1(\delta_1)] \\ \sigma'_2(y) = \sigma_2(y) \quad \forall\ y \neq x \end{cases}$$

and consider $\bar{t} = \sigma'_2(\delta_2)$.

We have $\sigma_2(\delta_2) \overset{*}{\rightarrow} \bar{t}$ by proposition 11, and also $t'/u_2 = \sigma_2(\gamma_2)[v \leftarrow \sigma_1(\delta_1)] \overset{*}{\rightarrow} \sigma'_2(\gamma_2) \vdash\!\dashv \bar{t}$, which shows $t' \overset{\sim}{\downarrow} t''$.

c2) $\exists\ \gamma \notin \mathcal{V}$ $\gamma = \gamma_2/v$, $\sigma_1(\gamma_1) = \sigma_2(\gamma)$.

Again there exists a critical pair $<t_1,t_2>$ of $\mathcal{E}/\mathcal{R}$ and a substitution $\rho$ such that :

$\sigma_2(\gamma_2)[v \leftarrow \sigma_1(\delta_1)] = \rho(t_1)$ and $\sigma_2(\delta_2) = \rho(t_2)$.

By hypothesis, $t_1 \overset{\sim}{\downarrow} t_2$, and therefore $t' \overset{\sim}{\downarrow} t''$, which concludes the proof. □

<u>Remarks</u> : The condition $\mathcal{R}$ left-free is essential, and cannot be removed. For instance, with $\mathcal{R}=\{<F(x,x),G(x)>\}$ and $\mathcal{E} = \{A = B\}$, taking $t = F(A,A)$, $t' = G(A)$ and $t'' = F(A,B)$, we do not have $t' \overset{\sim}{\downarrow} t''$. Note that there are no such restrictions for the equations in $\mathcal{E}$.

We have imposed here a condition $\mathcal{V}(\delta) \subset \mathcal{V}(\gamma)$ for all simplification rules $<\gamma,\delta>$ in $\mathcal{R}$, essentially because it made the definition of $\underset{\mathcal{R}}{\rightarrow}$ simpler. If we get rid of this condition, the definition of $\underset{\mathcal{R}}{\rightarrow}$ will rely on unification, rather than on the simpler pattern-matching operation of subsumption. But this has some undesirable consequences ; suppose $\mathcal{R}$ contains a rule <A, Fx>. Then, since $\underset{\mathcal{R}}{\rightarrow}$ is compatible and stable, we must have :

$A \underset{\mathcal{R}}{\rightarrow} F(A) \underset{\mathcal{R}}{\rightarrow} F(F(A)) \underset{\mathcal{R}}{\rightarrow} \ldots$ which shows that $\underset{\mathcal{R}}{\rightarrow}$ is not noetherian. Furthermore, since $A \underset{\mathcal{R}}{\rightarrow} F(t)$ $\forall\ t \in \mathcal{T}$, $\underset{\mathcal{R}}{\rightarrow}$ is not locally finite, even if $\mathcal{R}$ is finite. For these reasons, we keep requesting $\mathcal{V}(\delta) \subset \mathcal{V}(\gamma)$ for all $<\gamma,\delta>$ in $\mathcal{R}$.

For $\mathcal{E}$, the situation is analogous. In the case where $\mathcal{V}(\gamma) = \mathcal{V}(\delta)$ for all $\gamma = \delta$ in $\mathcal{E}$, we have simply defined the relation $\underset{\mathcal{E}}{\vdash\!\dashv}$ as $\underset{\mathcal{E}_1}{\rightarrow} \cup \underset{\mathcal{E}_2}{\rightarrow}$, where $\mathcal{E}_1 = \{<\gamma,\delta> \mid \gamma=\delta \in \mathcal{E}\}$ and $\mathcal{E}_2 = \{<\delta,\gamma> \mid \gamma=\delta \in \mathcal{E}\}$. Using the property $\mathcal{D}(\sigma) \subset \mathcal{V}(t) \Rightarrow \sigma(t)//t = \sigma$, it is easy to show that $\underset{\mathcal{E}_2}{\rightarrow} = \underset{\mathcal{E}_1}{\rightarrow}^{-1}$, and therefore that $\underset{\mathcal{E}_1}{\rightarrow} \cup \underset{\mathcal{E}_2}{\rightarrow}$ is the smallest compatible stable symmetric relation containing the pairs in $\mathcal{E}$. If on the contrary there exists in $\mathcal{E}$ an equation $\gamma = \delta$ with $\mathcal{V}(\gamma) \neq \mathcal{V}(\delta)$, then the definition of $\underset{\mathcal{E}}{\vdash\!\dashv}$ is more complicated, and has the drawbacks mentioned for $\underset{\mathcal{R}}{\rightarrow}$. However here this restriction is more debatable, since we do not use $\underset{\mathcal{E}}{\vdash\!\dashv}$ as a computation rule, and therefore do not care about termination or local finiteness. Furthermore, all our results remain true if we remove this condition, using the same definition of critical pairs. In automatic theorem proving terminology, $\underset{\mathcal{E}}{\vdash\!\dashv}$ is called paramodulation in non-variable positions. We shall not develop this further in this paper.

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

<u>Theorem 3</u>

Let $<\mathcal{R},\mathcal{E}>$ be an equational theory such that $\mathcal{R}$ is left-free and $\rightarrow.\sim$ is noetherian, with $\rightarrow = \underset{\mathcal{R}}{\rightarrow}$ and $\sim = \underset{\mathcal{E}}{\overset{*}{\vdash\!\dashv}}$. Then $<\mathcal{R},\mathcal{E}>$ is confluent iff for all its critical pairs $<t_1,t_2>$ we have $t_1 \overset{\sim}{\downarrow} t_2$, which may be checked as $\hat{t}_1 \sim \hat{t}_2$, where $\hat{t}$ is an arbitrary $\rightarrow$-normal form of t.

<u>Proof</u> Directly from lemmas 6, 8, 12 and 13. □

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

Remark that for any equational theory $\mathcal{T}$ theorem 3 is trivially applicable with $\mathcal{E} = \mathcal{T}$ and $\mathcal{R} = \emptyset$. This suggests to try to build up $\mathcal{R}$ progressively, removing equations in $\mathcal{E}$ one at a time, checking the termination condition, then generating a set $\mathcal{C}$ of critical pairs. All pairs $<t_1,t_2>$ in $\mathcal{C}$ that do not verify $t_1 \overset{\sim}{\downarrow} t_2$ are then added to $\mathcal{E}$, and the process is iterated. Of course there may be several ways of choosing the candidate simplifications, and the whole process may not terminate. But this kind of algorithm seems a promising way of mechanizing equational theories, compatible with other rules of inference such as resolution. A similar approach is currently being pursued, in particular by Lankford [7], who has already obtained good experimental evidence of its success.

To check the termination condition : $\rightarrow.\sim$ noetherian, the method given in section 2 is still valid, provided the interpretation $\chi$ chosen is such that $\chi(\gamma) = \chi(\delta)$ is identically true for every equation $\gamma = \delta$ in $\mathcal{E}$.

Remark that it is important to get termination criteria as general as possible in lemmas 4, 7 and 8. For instance, the conditions of [15] are too restrictive to be used with Knuth & Bendix's lexicographic ordering [6].

## CONCLUSION

We have presented in this paper general axiomatic properties that are sufficient to prove the confluence of a reduction relation. These results are then applied to term rewriting systems to provide systematic ways of mechanizing an equational theory, favoring simplifications over arbitrary equality replacements. This method, a generalization of early results by Knuth & Bendix, has important applications in formula manipulation systems : program optimization, program validation, automatic theorem proving, operational semantics of programming languages and semantics of parallelism.

## ACKNOWLEDGEMENTS

I wish to thank J.J. Levy and B. Rosen for their helpful remarks.

## REFERENCES

[1] A. Aho, R. Sethi & J. Ullman
Code optimization and finite Church-Rosser systems
Proceedings of Courant Computer Science Symposium
5 Ed. R. Rustin, Prentice Hall 1972.

[2] A. Church & J.B. Rosser
Some properties of conversion
Transactions of AMS Vol 39
(1936) pp 472-482

[3] H.B. Curry & R. Feys
Combinatory Logic, Vol 1
North Holland, 1958.

[4] R. Hindley
An abstract Church-Rosser theorem
part 1 Journal of Symbolic Logic Vol 34 (1969) pp 545-560
part 2 Journal of Symbolic Logic Vol 39 (1974) pp 1-21

[5] G. Huet
Résolution d'équations dans des langages d'ordre 1, 2, ... ω.
Thèse d'Etat, Université Paris VII, sept. 1976.

[6] D. Knuth & P. Bendix
Simple word problems in universal algebras
Computational problems in abstract algebra
Ed. J. Leech, Pergamon Press 1970, pp 263-297.

[7] D. Lankford
Canonical inference
Report ATP-25, Dec 1975
Departments of mathematics and computer sciences
University of Texas at Austin

[8] M.H.A. Newman
On theories with a combinatorial definition of "equivalence". Annals of Maths, vol 43 (1942) pp 223-243.

[9] M. Nivat
Congruences parfaites et quasi-parfaites
Séminaire Dubreil, 1971-72, n° 7.

[10] G. Plotkin
Lattice-theoretic properties of subsumption
Memorandum MIP - R - 77
University of Edinburgh, 1970

[11] G. Plotkin
Building-in equational theories
in Machine Intelligence 7, 1972, pp 73-90
American Elsevier

[12] J. Reynolds
Transformational systems and the algebraic structure of atomic formulas
in Machine Intelligence 5, 1970, pp 135-152
American Elsevier

[13] J.A. Robinson
A machine-oriented logic based on the resolution principle
J. ACM Vol 12 (1965) pp 23-41.

[14] B. Rosen
Tree-manipulating systems and Church-Rosser theorems
J. ACM Vol 20 (1973) pp 160-187

[15] R. Sethi
Testing for the Church-Rosser property
J. ACM Vol 21 (1974) pp 671-679
Erratum Vol 22 (1975) p 424.

[16] J. Staples
Church-Rosser theorems for replacement systems
in Algebra and Logic,
Ed. J. Crossley, pp 291-307.
Lecture Notes in Maths n° 450, Springer-Verlag, 1975.

[17] M. O'Donnell
Subtree Replacement Systems : A Unifying Theory for Recursive Equations, LISP, Lucid and Combinatory Logic.
Proc. 9 th Ann. ACM Symp. on Theory of Computing (1977), pp 295-305.

[18] M.S. Paterson & M.N. Wegman
Linear unification
Proc. 8 th. Ann. ACM Symp. on Theory of Computing (1976), pp 181-186.