CANONICAL FORMS AND UNIFICATION

Jean-Marie Hullot
INRIA and SRI International

Abstract

Fay has described in [2,3] a complete T-unification for equational theories T which possess a complete set of reductions as defined by Knuth & Bendix [12]. This algorithm relies essentially on using the narrowing process defined by Lankford [13]. In this paper, we first study the relations between narrowing and unification and we give a new version of Fay's algorithm. We then show how to eliminate many redundancies in this algorithm and give a sufficient condition for the termination of the algorithm. In a last part, we show how to extend the previous results to various kinds of canonical term rewriting systems.

1. Introduction.

In this paper, we are interested in unification problems arising in equational theories. More precisely, we study the case of an equational theory T which may be embedded in complete set of reductions (or canonical term rewriting system) $\mathcal{R}$ as defined by Knuth & Bendix [12]. Let us write $\rightarrow$ the reduction relation associated to $\mathcal{R}$ and $\mathcal{R}(M)$ the (unique) $\rightarrow$-normal form of any term M. A decision procedure for T-equality is known via $\rightarrow$-normal form:

$$M =_T N \Leftrightarrow \mathcal{R}(M) = \mathcal{R}(N).$$

We would like also to be able to solve equations in T, that is to T-unify two given terms; this is a quite difficult problem. Take for instance the canonical term rewriting sytem reduced to the single equation:

$$f(f(x,y),z) \rightarrow f(x,f(y,z)).$$

Solving equations in the corresponding equational theory is the problem of associative unification which has only recently shown to be decidable by Makanin [21].

A general result has been obtained by Fay who describes in [2,3] such a process to resolve equations in T. This algorithm is not in general a decision procedure for T-unification since the termination of the process is not insured. However one can organize this algorithm in such a manner that it can be used as a semi-decision procedure for T-unification in the following sense: if the two terms are unifiable, then a solution will be found in a finite time. Moreover Fay has shown that this algorithm produces a complete set of T-unifiers. Improvements over Fay's algorithm have been given by Lankford. An analogous result has been found by Huet who has given in [4] a unification algorithm for λ-calculus which relies essentially on the existence of a canonical form for λ-conversion.

In this paper we shall present a new version of Fay's algorithm. In a second step we shall eliminate many redundancies in our algorithm and sufficient conditions will be given insuring the termination of the algorithm.

New kinds of canonical term rewriting systems have been defined by Lankford & Ballantyne [16,17,18], Huet [6,7] and Peterson & Stickel [24]. Fay conjectures in [3] that his algorithm extends to the case of permutative reductions [17] and Lankford & Ballantyne use such an extension for associative and commutative theories in the appendix of [19]. We give in this paper extensions of Fay's algorithm for Huet's and Peterson & Stickel's canonical term rewriting systems.

2. An overview of first order terms.

We give a brief survey on first order terms. Our definitions and notations are consistent with those of Huet [6] and Huet & Oppen [9].

2.1. First order terms.

Let $\mathcal{V}$ be a denumerable set of elements called *variables*, and C a finite or denumerable set of elements called *constants* with $\mathcal{V} \cap C = \emptyset$. Elements in C are graded by an *arity function* α: $C \mapsto \mathcal{N}$ where $\mathcal{N}$ is the set of integers. The *set of terms* $\mathcal{T}$ is the smallest set containing $\mathcal{V}$ and closed by the operations:

$$M_1, \ldots, M_{\alpha(f)} \mapsto f(M_1, \ldots, M_{\alpha(f)})$$

for every f in C. If $\alpha(f) = 0$ we abbreviate $f()$ in f. For every M in $\mathcal{T}$, $\mathcal{V}(M)$ will denote the *set of variables of* M.

2.2. Substitutions.

Definition. A *substitution* is a mapping σ from $\mathcal{V}$ to $\mathcal{V}$ with $\sigma(x) = x$ almost everywhere. Substitutions are classically extended as morphisms of $\mathcal{T}$. For every substitution σ, we define the *set of variables affected by* σ or *domain of* σ by $\mathcal{D}(\sigma) = \{x | \sigma(x) \neq x\}$ and the *set of variables introduced by* σ by $\mathcal{I}(\sigma) = \bigcup_{x \in \mathcal{D}(\sigma)} \mathcal{V}(\sigma(x))$. For $V \subset \mathcal{V}$, we define the *restriction of* σ *to* V by $(\sigma \restriction V)(x) = \sigma(x)$ if $x \in V$ and $(\sigma \restriction V)(x) = x$ otherwise.

We define the preorder $\leq$ of *subsumption* in $\mathcal{T}$ by $M \leq N \Leftrightarrow \exists \sigma \quad \sigma(M) = N$. If such a σ exists, its restriction to $\mathcal{V}(M)$ is unique and we call it *the match of* N *by* M. Finally, we define: $M \equiv N \Leftrightarrow M \leq N \quad \& \quad N \leq M$, $\equiv$ is *variable renaming*. We extend $\leq$ to substitutions by: $\sigma \leq \sigma' \Leftrightarrow \forall x \quad \sigma(x) \leq \sigma'(x)$.

We say that two terms M and M' are *unifiable* iff $\exists \sigma \quad \sigma(M) = \sigma(M')$. Let us denote by $\mathcal{U}_\emptyset(M, M')$ the set of all unifiers of M and M'. If two terms are unifiable, then there exists a minimum unifier, that is $\exists \sigma \in \mathcal{U}_\emptyset(M, M')$, $\forall \theta \in \mathcal{U}_\emptyset(M, M')$, $\sigma \leq \theta$. This element is unique up to variable renaming and may be found by the unification algorithm [5,22,23,27]. Furthermore, note that it is always possible to impose to the minimum unifier σ the condition $\mathcal{D}(\sigma) \cap \mathcal{I}(\sigma) = \emptyset$. We will always choose such a minimum unifier.

2.3. Occurrences.

In order to have a formal way to deal with subterm of a term we define the *occurrences* that is sequences of integers denoting an access path in a term. Let N_+^* be the set of finite sequences of positive integers, Λ the empty sequence and $\cdot$ the operation of concatenation on sequences. The elements of N_+^* are called *occurrences* and we denote them by u, v, w. The set of occurrences is partially ordered by the prefix ordering: $u \preceq v \Leftrightarrow \exists w \quad v = u \cdot w$ in this case, we define $v/u = w$. If $u \not\preceq v$ and $v \not\preceq u$ we say that u and v are *disjoint*, and we write $u \mid v$. Finally, we define $u \prec v$ iff $u \preceq v$ and $u \neq v$. For any term M, we define its *set of occurrences* $\mathcal{O}(M)$ as a finite subset of N_+^* as follows:

(i) $\Lambda \in \mathcal{O}(M)$,
(ii) $u \in \mathcal{O}(M_i) \Rightarrow i \cdot u \in \mathcal{O}(F(M_1, \ldots, M_n)) \quad \forall i \quad 1 \leq i \leq n$.

If $u \in \mathcal{O}(M)$, we define the *subterm of* M *at* u as the term M/u, and for every M' the *replacement in* M *of* M' *at* u *as the term* $M[u \leftarrow M']$, by:

(i) $M/\Lambda = M$,
(ii) $F(M_1, \ldots, M_n)/i \cdot u = M_i/u$,
(iii) $M[\Lambda \leftarrow M'] = M'$,
(iv) $F(M_1, \ldots, M_n)[i \cdot u \leftarrow M'] = F(M_1, \ldots, M_i[u \leftarrow M'], \ldots, M_n)$.

In order to distinguish between variable and non-variable occurrences we define $\overline{\mathcal{O}}(M)$ as $\{u \in \mathcal{O}(M) | M/u \notin \mathcal{V}\}$, and $\mathcal{F}r(M) = \{u \in \mathcal{O}(M) | M/u \in \mathcal{V}\}$.

3. Reduction, narrowing and unification.

We call an *equation* any pair of terms. An equation will be denoted by $M = N$. Let T be any finite set of equations. We define the relation $\doteq_T$ on $\mathcal{T}$ as the compatible, stable, symmetric closure of T. We define the equality in the *equational theory* T or *T-equality* to be the congruence generated by T, that is $\doteq_T^*$. It will be denoted by $=_T$.
Example. The equational theory of groups is generated by the set of equations:

$$x + 0 = x;$$
$$x + (-x) = 0;$$
$$(x + y) + z = x + (y + z).$$

We are interested in *unifying terms in the equational theory* T; given two terms M and M', we shall say that a substitution σ is a T-unifier of M and M' iff $\sigma(M) =_T \sigma(M')$. $\mathcal{U}_T(M, M')$ will denote the set of all T-unifiers of M and M'. When dealing with ordinary unification, we have seen that two unifiable terms have a minimum unifier. This is no longer the case with T-unification. However, this notion generalizes to the one of *complete set of T-unifiers* [4,5,25].

Definition. Let M and M' be two terms and W be a finite set of variables containing $V = \mathcal{V}(M) \cup \mathcal{V}(M')$. We say that a set of substitutions Σ is a *complete set of unifiers of M and M' away from W* iff:

(i) $\forall \sigma \in \Sigma \quad \mathcal{D}(\sigma) \subset V \quad \& \quad \mathcal{I}(\sigma) \cap W = \emptyset,$
(ii) $\Sigma \subset \mathcal{U}_T(M, M'),$
(iii) $\forall \sigma \in \mathcal{U}_T(M, M') \quad \exists \theta \in \Sigma \quad \theta \leq_T \sigma \; [\![V]\!].$

where $\leq_T$ is the preorder defined on $\mathcal{T}$ by $M \leq_T M'$ iff $M' =_T \sigma(M)$ and $\leq_T \; [\![V]\!]$ is the following extension of $\leq_T$ to substitutions: $\sigma \leq \sigma' \; [\![V]\!]$ iff there exists a substitution ρ such that $\sigma'(x) =_T \rho(\sigma(x))$ for all x in V. $CSU_T(M, M', W)$ will denote the set of all such Σ's. In addition Σ is said to be *minimal* iff it satisfies the further condition:

(iv) $\forall \sigma, \sigma' \in \Sigma \quad \sigma \neq \sigma' \Rightarrow \sigma \not\leq_T \sigma' \; [\![V]\!].$

A discussion of general properties of complete set of unifiers may be found in [5]. Remark that the introduction of the set W is motivated by technical reasons: it is a way to avoid conflicts when choosing new variables.

A T-unification algorithm is *complete* if it generates a complete set of T-unifiers for all T-unifiable input terms. Complete unification algorithm are known for various theories including commutativity, associativity [25], idempotence [26], associativity and commutativity [29], associativity commutativity and idempotence [20] and abelian group theory [14]. Note that we do not require any termination property.

A very general result on T-unification problems has been obtained by Fay who describes in [2,3] such a T-unification algorithm in the case where the equational theory T may be described by a *complete set of reductions* as defined by Knuth & Bendix [12]. We recall that a *term rewriting system* $\mathcal{R}$ is a set of pairs of terms $\gamma_k \to \delta_k$, such that $\mathcal{V}(\gamma_k) \subseteq \mathcal{V}(\delta_k)$. We say that term $M \to_{\mathcal{R}}$-reduces to term N at occurrence u and we write $M \to_{\mathcal{R}} N$ iff:

$$\exists \gamma_k \to \delta_k \in \mathcal{R} \quad \exists \sigma \quad \exists u \in \mathcal{O}(M) \quad M/u = \sigma(\gamma_k) \quad \& \quad N = M[u \leftarrow \sigma(\delta_k)].$$

Sometimes we will write: $M \to_{[u,k]} N$. We say that a term M is in *$\to_{\mathcal{R}}$-normal form* iff $\not\exists N$, $M \to_{\mathcal{R}} N$. If $M \to_{\mathcal{R}}^* N$ and N is in $\to_{\mathcal{R}}$-normal form, we say that N is a *$\to_{\mathcal{R}}$-normal form of M*. We say that a substitution σ is in *$\to_{\mathcal{R}}$-normal form* iff $\forall x \in \mathcal{D}(\sigma)$, $\sigma(x)$ is in $\to_{\mathcal{R}}$-normal form.

A term rewriting system $\mathcal{R}$ is said to be a *complete set of reductions* or a *canonical term rewriting system* iff:

(a) $\rightarrow_{\mathcal{R}}$ is nœtherian, that is, there does not exist infinite derivation $M_1 \rightarrow M_2 \cdots$

(b) $\rightarrow_{\mathcal{R}}$ is confluent, that is $\forall M, M_1, M_2$, such that $M \rightarrow^*_{\mathcal{R}} M_1$ and $M \rightarrow^*_{\mathcal{R}} M_2$ then $\exists M'$ such that $M_1 \rightarrow^*_{\mathcal{R}} M'$ and $M_2 \rightarrow^*_{\mathcal{R}} M'$.

Note that if $\mathcal{R}$ is a canonical term rewriting system, each term M admits a unique $\rightarrow_{\mathcal{R}}$-normal form we shall denote by $\mathcal{R}(M)$. Thus a decision procedure for T-equality is known via this normal form. More precisely, we have:

$$M =_T N \Leftrightarrow \mathcal{R}(M) = \mathcal{R}(N).$$

Knuth & Bendix give in [12] a way to decide if a finite and nœtherian term rewriting system $\mathcal{R}$ is canonical. A detailed study may be found also in [6].

It is not possible to define a canonical term rewriting system for a theory T which includes for instance a commutativity axiom (condition (a) never holds with such an axiom). Differents ways have been proposed to extend the notion of canonical term rewriting systems as we shall see in section 5.

Our aim in this section is to give a new version of Fay's algorithm.

Notation. $\rightarrow$ will be $\rightarrow_{\mathcal{R}}$ where $\mathcal{R}$ is any canonical term rewriting system defining an equational theory T.

3.1. Narrowing.

The basic idea in Fay's algorithm is to combine ordinary unification and "narrowing". Informally narrowing a term is applying to it the minimum substitution such that the resulting term is not in $\rightarrow$-normal form and then reducing it one step. Slagle [28] has first noticed the difficulties arising when working with terms which are "narrowable" and thus considered in its work only sets of clauses which are fully "narrowed". Lankford in [13] was first to show the interest of the iteration of narrowing and to give applications of such a "narrowing procedure". We define below a relation on $\mathcal{T}$ we call the *narrowing relation*. A step of derivation using this relation is very close to the notion of *immediate narrowing* of Lankford.

Definition. Let M be a term and V be a finite set of variables containing $\mathcal{V}(M)$. Assume there exists a non-variable subterm of M, say M_1, which is unifiable with the left part of some rule $\gamma_k \rightarrow \delta_k$ in $\mathcal{R}$. More formally:

$$\exists u \in \overline{O}(M), \quad \exists \gamma_k \rightarrow \delta_k \in \mathcal{R}, \quad U_\emptyset(M/u, \gamma_k) \neq \emptyset,$$

where we assume $\gamma_k \rightarrow \delta_k$ is renamed so that $\mathcal{V}(\gamma_k) \cap V = \emptyset$.
Let σ the minimum unifier of $M_1 = M/u$ and γ_k. We say that σ is a *narrowing substitution of M away from V*. $NS(M, V)$ will denote the finite set of such substitutions.
Let us now consider the term M obtained from $\sigma(M)$ in replacing $\sigma(M_1)$ by $\sigma(\delta_k)$, that is:

$$M' = \sigma(M)[u \leftarrow \sigma(\delta_k)] = \sigma(M[u \leftarrow \delta_k]).$$

We say that M *is narrowable in M' at occurrence u using rule* $\gamma_k \rightarrow \delta_k$ and we write:

$$M \mathrel{\wr\!\!\rightarrow}_{[u,k,\sigma]} M'.$$

$\wr\!\!\rightarrow$ is called *the narrowing relation on T*.

Notations. Sometimes we will abbreviate $\wr\!\!\rightarrow_{[u,k,\sigma]}$ in $\wr\!\!\rightarrow_{[u,k]}$ or $\wr\!\!\rightarrow_{[\sigma]}$.

Remark 1. Note that our definition is not exactly the one used by Lankford, Fay or Slagle. More precisely, we do not assume that M is normalized and we do not normalize M', so that we have:

$$\rightarrow \subseteq \overset{\wedge}{\rightarrow}.$$

The motivation behind this modification is that we want to express very precisely correspondances between reduction and narrowing in order to find sufficient conditions insuring the termination of the narrowing process.

Remark 2. The condition $\mathcal{V}(\gamma_k) \cap V = \emptyset$ insures that $\sigma(M)$ is reducible by $\rightarrow$ using $\gamma_k \rightarrow \delta_k$. Note that M' may contain variables which are not in V; these variables come from $\mathcal{V}(\gamma_k)$. In the next section, when we shall study the iteration of the narrowing process we will have to make explicit the renaming of variables of the γ_k's at each step of the iteration in order to avoid conflict between the names of all these "new" variables. In practice the problem is simplified in using the GENSYM operator of LISP for instance.

Example. Let us consider the following canonical term rewriting system $\mathcal{R}$:

$$\mathcal{R} = \{f(x, x) \rightarrow x\},$$

and the term $M = f(x_1, f(y_1, z_1))$. M is narrowable at occurrence Λ since it is unifiable with $f(x, x)$:

$$M \overset{\wedge}{\rightarrow}_{[\Lambda]} f(y_1, z_1), \quad \sigma = \{(x \leftarrow f(y_1, z_1)), (x_1 \leftarrow f(y_1, z_1))\},$$

and at occurrence 1 for the subterm $f(y_1, z_1)$ is unifiable with $f(x, x)$:

$$M \overset{\wedge}{\rightarrow}_{[1]} f(x_1, x), \quad \sigma = \{(y_1 \leftarrow x), (z_1 \leftarrow x)\}.$$

Remark 3. Let us now have a look back to the initial problem we were interested in: given two terms P and Q, find a substitution σ such that:

$$\sigma(P) =_T \sigma(Q), \tag{1}$$

or equivalently:

$$\mathcal{R}(\sigma(P)) = \mathcal{R}(\sigma(Q)). \tag{2}$$

Assume the problem has a solution, say σ, then there are two cases: either σ is a unifier of P and Q in the usual sense in which case one can find a minimum unifier of P and Q in using the unification algorithm. Or σ does not unify P and Q, in which case at least one of $\sigma(P)$ and $\sigma(Q)$ is $\rightarrow$-reducible, since otherwise it would be impossible to have (2). In this case at least one of P and Q is narrowable.

3.2. Narrowing and reduction.

Using the notations of remark 3 of the previous section, the equivalence between (1) and (2) gives a particular interest in the study of $\rightarrow$-derivation issuing from $\sigma(M)$ where σ is any substitution and M is any term. The aim of the following theorem is to show how one can make correspond any such derivation to a $\overset{\wedge}{\rightarrow}$-derivation and conversely. In other words, we shall show that any $\rightarrow$-derivation issuing from $\sigma(M)$ may be "projected" on a $\overset{\wedge}{\rightarrow}$-derivation issuing from M. And conversely any $\overset{\wedge}{\rightarrow}$-derivation issuing from M may be considered as the "projection" of a certain class of $\rightarrow$-derivations.

Theorem 1. *Let M be any term, V be a finite set of variables containing $\mathcal{V}(M)$, and η be a normalized substitution with $\mathcal{D}(\eta) \subseteq \mathcal{V}(M)$. Consider any $\rightarrow$-derivation issuing from $\eta(M)$:*

$$\eta(M) = N_0 \rightarrow_{[u_0,k_0]} N_1 \rightarrow_{[u_1,k_1]} N_2 \rightarrow \cdots \rightarrow_{[u_{n-1},k_{n-1}]} N_n. \tag{1}$$

There exists an associated $\leadsto$-derivation issuing from M:

$$M = M_0 \leadsto_{[u_0,k_0,\sigma_0]} M_1 \leadsto_{[u_1,k_1,\sigma_1]} M_2 \leadsto \cdots \leadsto_{[u_{n-1},k_{n-1},\sigma_{n-1}]} M_n, \tag{2}$$

and for each i, $0 \leq i \leq n$, a substitution η_i and a finite set of variables V_i such that:

(i) $\mathcal{D}(\eta_i) \subseteq V_i$,
(ii) η_i *is normalized,*
(iii) $(\eta \uparrow V) = (\eta_i\theta_i \uparrow V)$,
(iv) $\eta_i(M_i) = N_i$,

where $\theta_0 = \epsilon$ and $\theta_{i+1} = \sigma_{i+1}\theta_i$.

Conversely, to each $\leadsto$-derivation (2) and every η such that $\theta_n \leq \eta[\![V]\!]$, we can associate a $\rightarrow$-derivation (1).

As usual the motivation behind the introduction of the V_i is technical: it is a way to avoid conflicts between "new" and initial variables. As one can see in the following proof, it is not totally trivial to deal in a mathematical way with this problem of renaming. In a certain way we have to give all the details of a "garbage collecting" process.

Proof. $\Rightarrow$ By induction on i. For $i = 0$ it is obvious, taking $\eta_0 = \eta$ and $V_0 = V \cup \mathcal{D}(\eta)$. Let us assume (i) to (iv) hold for i.
Since $M_i \leadsto_{[u_i,k_i]} M_{i+1}$, we have:

$$\exists\sigma \quad \sigma(\gamma_{k_i}) = M_i/u_i,$$

where γ_{k_i} is renamed so that $\mathcal{D}(\sigma) \cap V_i = \emptyset$.
From assumptions (ii) and (iv) for i, we get $u_i \in \overline{\mathcal{O}}(M_i)$ and therefore:

$$\eta_i(M_i/u_i) = \sigma(\gamma_{k_i}).$$

Let us consider $\rho = \eta_i \cup \sigma$. We have:

$$\rho(M_i/u_i) = \rho(\gamma_{k_i}),$$

and thus:

$$M_i \leadsto_{[u_i,k_i,\sigma_i]} M_{i+1},$$

where σ_i is the minimum unifier of M_i/u_{i+1} and γ_{k_i}. We have $\sigma_i \leq \rho$, and thus there exists a substitution η' such that $\rho = \eta'\sigma_i$. Therefore:

$$\eta_i = ((\eta'\sigma_i) \uparrow V_i).$$

Now, let:

$$V_{i+1} = (V_i \cup \mathcal{I}(\sigma_i)) - \mathcal{D}(\sigma_i),$$

and:

$$\eta_{i+1} = \eta' \uparrow V_{i+1}.$$

We get (i) and:

$$\eta_i = (\eta_{i+1}\sigma_i) \uparrow V_i. \tag{*}$$

(remember that we impose $\mathcal{D}(\sigma_i) \cap \mathcal{I}(\sigma_i) = \emptyset$).
Now, let us consider x in V_{i+1}. There are two cases:

a) $x \in \mathcal{I}(\sigma_i)$; then $\exists y \in \mathcal{D}(\eta_i)$ such that $x \in \mathcal{V}(\sigma_i(y))$, and $\eta_i(y) = \eta_{i+1}(\sigma_i(y))$ normalized implies $\eta_{i+1}(x)$ normalized.

b) otherwise $\sigma_i(x) = x$ since $x \notin \mathcal{D}(\sigma_{i+1})$ and therefore $\eta_{i+1}(x) = \eta_i(x)$ is normalized, which proves (ii).

We now assume (iii) for i:

$$\eta \uparrow V = \eta_i\theta_i \uparrow V,$$

and show it fo $i+1$. From (*) above, we get:

$$(\eta_i\theta_i) \uparrow V = (((\eta_{i+1}\sigma_i) \uparrow V_i)\theta_i) \uparrow V.$$

From the definition of θ_i, we get $I(\theta_i) \subseteq V_i$ and $V \subseteq V_i \cup D(\theta_i)$. The above expression simplifies therefore to:

$$(\eta_{i+1}\sigma_i\theta_i) \uparrow V = (\eta_{i+1}\sigma_i) \uparrow V,$$

proving (iii).

Finally we get easily $\mathcal{V}(M_i) \subseteq V_i$, from which we get:

$$\eta_{i+1}(M_{i+1}) = \eta_{i+1}\sigma_i(M_i[u_i \leftarrow \delta_{k_i}]) = \eta_i(M_i[u_{i+1} \leftarrow \delta_{k_{i+1}}) = N_{i+1},$$

proving (iv).

Note that because of (iii) every $\theta_i \uparrow V$ is normalized.

$\Leftarrow$ Conversely, let us consider any $\curlywedge\!\!\rightarrow$-derivation (2) and any substitution η such that $\theta_n \leq \eta[\![V]\!]$. Let ρ be such that $\eta \uparrow V = (\rho\theta_n) \uparrow V$. We define substitutions η_i for $0 \leq i \leq n-1$ by:

$$\eta_i = \rho\sigma_n\sigma_{n-1}\cdots\sigma_i,$$

and substitution η_n as being ρ. With $N_i = \eta_i(M_i)$, it is easy to show by induction on i, that:

$$\eta(M) = N_0 \rightarrow_{[u_0,k_0]} N_1 \rightarrow_{[u_1,k_1]} N_2 \rightarrow \cdots \rightarrow_{[u_{n-1},k_{n-1}]} N_n.$$

Now:

$$N_0 = \eta_0(M_0) = \eta_0(M) = \eta_n\theta_n(M) = \eta(M),$$

since $\mathcal{V}(M) \subseteq V$, which establishes the $\Leftarrow$-part. ∎

3.3. Narrowing and unification.

In this section we will describe a non-deterministic T-unification algorithm. Before giving this algorithm we prove two key lemmas about the connection between narrowing and T-unification.

Let us consider two terms P and Q. In order to find T-unifiability properties of these two terms we will have to iterate the narrowing process on both P and Q in parallel. It will simplify matters to iterate the narrowing process on the single term $M = H(P,Q)$ where H is a "new" function symbol, that is $H \notin C$, playing the rôle of cartesian product.

In lemma 1, we show how to combine narrowing and ordinary unification to build T-unifiers. This lemma will show the correctness of the unification algorithm.

Lemma 1. *Let us consider any $\curlywedge\!\!\rightarrow$-derivation:*

$$M = H(P,Q) = M_0 \curlywedge\!\!\rightarrow M_1 = H(P_1,Q_1) \curlywedge\!\!\rightarrow \cdots \curlywedge\!\!\rightarrow M_n = H(P_n,Q_n),$$

such that P_n and Q_n are unifiable say by substitution σ. Then $\sigma\theta_n$ is a T-unifier of P and Q, where θ_n is the composition of substitutions along the derivation, as defined in theorem 1.

Proof. Using the $\Leftarrow$ part of the previous theorem with $\eta = \rho_n$, we can associate to this $\curlywedge\!\!\rightarrow$-derivation the following $\rightarrow$-derivation:

$$\theta_n(M) = N_0 \rightarrow N_1 \rightarrow N_2 \rightarrow \cdots \rightarrow N_n = H(N_n^P, N_n^Q),$$

and thus, we have:

$$\theta_n(P) \rightarrow^* N_n^P \quad \& \quad \theta_n(Q) \rightarrow^* N_n^Q.$$

Moreover, since $\eta_n = \epsilon$ in this case, we have:

$$N_n^P = P_n \quad \& \quad N_n^Q = Q_n,$$

thus:

$$\sigma\theta_n(P) =_T \sigma\theta_n(Q),$$

since these two terms are $\rightarrow$-reducible to the same term. ∎

In lemma 2 we show that any T-unifier may be reached in such a way. This lemma will be used when showing the completeness of the T-unification algorithm.

Lemma 2. *Let P and Q be two terms which are T-unifiable, ρ be any T-unifier and V be a finite set of variables containing $\mathcal{V}(P) \cup \mathcal{V}(Q)$. Then there exists a $\leftsquigarrow$-derivation:*

$$M = H(P,Q) = M_0 \leftsquigarrow M_1 = H(P_1,Q_1) \leftsquigarrow \cdots \leftsquigarrow M_n = H(P_n,Q_n),$$

such that P_n and Q_n are unifiable. Let μ be the minimum unifier of P_n and Q_n we have:

$$\mu\theta_n \leq_T \rho\ [\![V]\!].$$

Moreover we are allowed to restrict our attention to $\leftsquigarrow$-derivations such that: $\forall i$, $0 \leq i \leq n$, $\theta_i \uparrow V$ is normalized.

Proof. We have $\rho(P) =_T \rho(Q)$ thus with $\eta = \mathcal{R}(\rho)$, where $(\mathcal{R}(\rho))(x) = \mathcal{R}(\rho(x))$, $\eta(P) =_T \eta(Q)$ that is these two terms have a same normal form which we call R. Then we have:

$$\eta(M) = H(\eta(P),\eta(Q)) = N_0 \to \cdots \to N_n = H(R,R).$$

The corresponding $\leftsquigarrow$-derivation is such that:

$$\eta_n(M_n) = H(\eta_n(P_n),\eta_n(Q_n)) = N_n = H(R,R).$$

Thus η_n is a unifier of P_n and Q_n. Let μ be the minimum unifier, we have: $\exists \xi \quad \xi\mu = \eta_n$, therefore:

$$(\xi\mu\theta_n \uparrow V) = (\eta_n\theta_n \uparrow V) = (\eta \uparrow V) =_T (\rho \uparrow V),$$

that is:

$$\mu\theta_n \leq_T \rho\ [\![V]\!],$$

which proves the lemma. ∎

We are now ready to describe how to build a complete set of T-unifiers for two terms.

Theorem 2. *Let T be the equational theory defined by a canonical term rewriting system $\mathcal{R}$. Let P and Q be two terms, M be $H(P,Q)$ where H is a new function symbol ($H \notin C$), and V be a finite set of variables containing $\mathcal{V}(M)$. Let Σ be the set of all substitutions σ such that σ is in Σ iff there exists a $\leftsquigarrow$-derivation:*

$$M = H(P,Q) = M_0 \leftsquigarrow M_1 = H(P_1,Q_1) \leftsquigarrow \cdots \leftsquigarrow M_n = H(P_n,Q_n),$$

such that P_n and Q_n are unifiable, θ_n is normalized and $\sigma = \mu\theta_n$ where μ is the minimum unifier of P_n and Q_n. Then Σ is a complete set of T-unifiers of P and Q away from V.

Proof. Lemma 1 proves consistency and lemma 2 proves completeness. ∎

A T-unification algorithm follows from the construction of theorem 2: enumerate all elements of Σ. Essentially this algorithm is the same as Fay's; however we do not normalize terms at each step. Note that, althougt this set may be infinite, one can organize the enumeration in such a way that if two terms P and Q are T-unifiable, then a T-unifier will be produced in a finite number of steps. Thus this algorithm gives a semi-decision procedure for T-unifiability. In the following section we shall study how to refine this algorithm in order to eliminate some redundancies. Moreover a sufficient condition for the termination of the construction will be given.

Note also that this algorithm does not enumerate a minimal set of unifiers (even when such a set exists as one can see in the example of associativity). We will give an example in section 5 where a complete and finite T-unification algorithm is known and the algorithm described here does not even terminate.

4. Elimination of redundancies.

In this section we are interested in eliminating some redundancies in the construction of theorem 2. To achieve this aim we shall restrict our attention to special $\leftsquigarrow$-derivations. Since we have seen in theorem 1 that any $\leftsquigarrow$-derivation issuing from M is the "projection" of a $\to$-derivation issuing from $\eta(M)$ such that η is normalized, we shall first give a particular property verified by all such $\to$-derivations.

Definition. Let us consider a term N and a set of occurrences U of a proper prefix of N (e.g. $U = \overline{O}(M)$, for some $M \leq N$). We define by induction what it means for a derivation:

$$N = N_0 \to_{[u_0,k_0]} N_1 \to_{[u_1,k_1]} \cdots \to_{[u_{i-1},k_{i-1}]} N_i,$$

to be *based on* U, and we construct sets of occurrences $U_i \subset O(N_i)$, $0 \leq i \leq n$, as follows:

- the empty derivation is based on U, and $U_0 = U$,
- if the derivation above is based on U, then the derivation obtained from it by adding one step $N_i \to_{[u_i,k_i]} N_{i+1}$ is based on U iff $u_i \in U_i$, and in this case we take:

$$U_{i+1} = (U_i - \{v \in U_i | u_i \preceq v\}) \cup \{u_i \cdot v | v \in \overline{O}(\delta_{k_i})\}.$$

This definition is quite technical, but the practical meaning is easy to understand. Consider for instance the following term rewriting system:

$$f(h(x)) \to h(x); \tag{r1}$$

$$h(h(x)) \to x; \tag{r2}$$

$$h(a) \to a. \tag{r3}$$

We consider terms $M = h(f(x))$ and $N = h(f(h(a)))$ that is $N = \sigma(M)$ with $\sigma(x) = h(a)$. Note that σ is not normalized (see lemma 3 below). In order to be based on $\overline{O}(M)$ a derivation issuing from N must not affect $\sigma(x)$. For instance the following derivation using rule (r3) is not based on $\overline{O}(M)$:

$$N = h(f(h(a))) \to h(f(a)).$$

Thus it must affect a subterm which has a prefix in M, for instance the following step of reduction using rule (r1):

$$N = h(f(h(a))) \to h(h(a)).$$

Since the affected subterm was $f(h(a))$ the definition says that we can iterate these considerations with $M_1 = h(x)$, $N_1 = h(h(a))$ and $\sigma_1(x) = h(a)$. Thus the only way to go on is:

$$h(h(a)) \to a.$$

Let us now give a lemma which shows our interest in derivations based on a set of occurrences.

Lemma 3. *Let $N = \eta(M)$, with η normalized. Every $\to$-derivation from N is based on $\overline{O}(M)$.*

Proof. Obvious. ∎

Definition. A $\leadsto$-derivation:

$$M = M_0 \leadsto_{[u_0,k_0]} M_1 \leadsto_{[u_1,k_1]} M_2 \leadsto \cdots \leadsto_{[u_{i-1},k_{i-1}]} M_i,$$

is said to be *basic* iff it is based on $\overline{O}(M)$ (in the same sense as in the previous definition for $\to$-derivation).

Let us now consider the $\leadsto$-derivation:

$$M = M_0 \leadsto_{[u_0,k_0,\sigma_0]} M_1 \leadsto_{[u_1,k_1,\sigma_1]} M_2 \cdots \leadsto_{[u_{n-1},k_{n-1},\sigma_{n-1}]} M_n,$$

associated by theorem 1 to any $\to$-derivation:

$$\eta(M) = N_0 \to_{[u_0,k_0]} N_1 \to_{[u_1,k_1]} N_2 \to \cdots \to_{[u_{n-1},k_{n-1}]} N_n,$$

such that η is normalized. Because of lemma 3 this $\to$-derivation is based on $\overline{O}(M)$, and since the sets U_i are the same for the $\to$-derivation and the $\leadsto$-derivation it follows easily that the considered $\leadsto$-derivation is basic. Thus, we have:

Theorem 3. *The $\wedge\!\!\rightarrow$-derivations constructed in the $\Rightarrow$-part of theorem 1 are all basic.*
As a corollary of theorem 3 we can now give a refined version of theorem 2:

Theorem 4. *Theorem 2 holds if we consider only basic $\wedge\!\!\rightarrow$-derivations.*

The main interest of this theorem is that we can give a sufficient condition for the termination of the narrowing process when we consider only basic $\wedge\!\!\rightarrow$-derivations and therefore for the termination of the corresponding T-unification algorithm.

Proposition 1. *Let $\mathcal{R} = \{\gamma_k \rightarrow \delta_k\}$ be a canonical term rewriting system such that any basic $\wedge\!\!\rightarrow$-derivation issuing from any of the δ_k's terminates. Then any $\wedge\!\!\rightarrow$-derivation issuing from any term terminates.*

Proof. Let us consider any basic $\wedge\!\!\rightarrow$-derivation:

$$M = M_0 \wedge\!\!\rightarrow_{[u_0]} M_1 \wedge\!\!\rightarrow \cdots \wedge\!\!\rightarrow_{[u_{i-1}]} M_i \wedge\!\!\rightarrow_{[u_i]} M_{i+1} \wedge\!\!\rightarrow \cdots;$$

The basic idea underlying the proof is the following: at each step of the derivation, either u_i comes from $\overline{O}(M)$ and such an occurrence may be used only one time, or this step of derivation "is part" of some $\wedge\!\!\rightarrow$-derivation issuing from a δ_k. More formally, we define sets of occurrences $\mathcal{G}_i$ by:

- $\mathcal{G}_0 = \overline{O}(M_0)$,
- $\mathcal{G}_{i+1} = (\mathcal{G}_i - \{u | u \in \mathcal{G}_i \quad \& \quad u_i \preceq u\})$ if $u_i \in \mathcal{G}_i$ and $\mathcal{G}_{i+1} = \mathcal{G}_i$ otherwise.

We define also sets $\mathcal{H}_i$. Each element of a $\mathcal{H}_i$ will be a pair which left part is an occurrence u and which right part is an integer $n(u)$. For each $\gamma_k \rightarrow \delta_k \in \mathcal{R}$ we define integer n_k to be the maximal length of a derivation issuing from δ_k.

- $\mathcal{H}_0 = \emptyset$.
- if $u_i \in \mathcal{G}_i$, $\mathcal{H}_{i+1} = (\mathcal{H}_i - \{(u, n(u)) | u \in \mathcal{H}_i \quad \& \quad u_i \prec u\} \cup \{(u_i, n_{k_i})\}$,
- otherwise let us consider the following sequence of occurrences in N_i:

$$v_0 = \Lambda, v_1, \ldots, v_p = u_i.$$

Since $u_i \not\in \mathcal{G}_i$, there exists an integer q such that $v_q \in \mathcal{G}_i$ and $v_{q+1} \not\in \mathcal{G}_i$. In this case, we define: $\mathcal{H}_{i+1} = (\mathcal{H}_i - \{(v_{q+1}, n(v_{q+1}))\}) \cup \{(v_{q+1}, n(v_{q+1}) - 1)\}$ (note that v_{q+1} is an u_j with $j \leq i$).

Along the lines of the definition of basic $\wedge\!\!\rightarrow$-derivation, it is easy to prove that, if a right part of a couple in one $\mathcal{H}_i$ reaches value 0, then no more narrowing will be possible under the corresponding left part occurrence. Moreover, one of the two following situations occurs:

(a) either $|\mathcal{G}_{i+1}| < |\mathcal{G}_i|$, $|\mathcal{H}_{i+1}| \leq |\mathcal{H}_i| + 1$,

(b) or $|\mathcal{G}_{i+1}| = |\mathcal{G}_i|$, $|\mathcal{H}_{i+1}| = |\mathcal{H}_i|$, and the right part of one of the elements of $\mathcal{H}_i$ has decreased from 1.

Thus situation (a) may occur only $|\mathcal{G}_0|$ times in the derivation. Then we have $\forall i$, $|\mathcal{H}_i| \leq |\mathcal{G}_0|$. It is then easy to prove the termination, using the decreasing of the integers in situation (b). ∎

Proposition 2. *If the hypothesis of proposition 1 holds, the construction of theorem 4 leads to a complete and finite T-unification algorithm.*

Example 1. In the case where all right parts of the rules of a canonical term rewriting system are variables, the previous proposition obviously applies. This is the case for idempotency law alone. However, in this case, a more powerful (for minimal) complete and finite T-unification algorithm is known [26].

Example 2. Another example is quasi-group theory, which can be defined by the following set of equations:

$$x * (x \setminus y) = y; \tag{a1}$$
$$(x / y) * y = x; \tag{a2}$$
$$x \setminus (x * y) = y; \tag{a3}$$
$$(x * y) / y = x. \tag{a4}$$

This set of equations can be embedded in a canonical term rewriting system $\mathcal{R}$, as shown in [11]:

$$x * (x \setminus y) \to y; \tag{r1}$$
$$(x / y) * y \to x; \tag{r2}$$
$$x \setminus (x * y) \to y; \tag{r3}$$
$$(x * y) / y \to x; \tag{r4}$$
$$(x / y) \setminus x \to y; \tag{r5}$$
$$x / (y \setminus x) \to y. \tag{r6}$$

Thus we obtain the first known complete and finite T-unification algorithm for quasi-group theory. Note that our result applies in the same way to all particular quasi-group with identities studied by Hullot in [11].

Example 3. This example is from Lankford [15]. Let us consider a theory T defined by a finite set of ground equations. In this case, using a lexicographic ordering to show the finite termination property, it is always possible to build a canonical term rewriting system from the equations. Moreover, since the right parts of the resulting rewrite rules are ground, no $\overset{\wedge}{\to}$-derivation is possible from these terms. Thus the narrowing process is finite and the construction of theorems 2 & 3 gives a quite elegant way to solve equations in such theories. We have implemented this equation solver as a LISP program.

5. Extensions.

Under certain conditions it is possible to define canonical term rewriting systems on equivalence classes of terms modulo permutations. This has been done for commutativity by Lankford & Ballantyne [16], for associativity and commutativity by Lankford & Ballantyne [18] and Peterson & Stickel [24]. In the case where the term rewriting sytem is left linear Huet [6,7] has given general results. We are interested in this section to extend the results of sections 3 & 4 to all these cases.

Let T be the equational theory defined by $T = \mathcal{E} \cup \mathcal{R}$ where $\mathcal{R}$ is a term rewriting system and $\mathcal{E}$ is a set of equations verifying:

$$\forall \langle \gamma, \delta \rangle \in \mathcal{E} \qquad \mathcal{V}(\gamma) = \mathcal{V}(\delta).$$

In all this section, we assume the existence of a complete $\mathcal{E}$-unification algorithm. We shall study three cases according to the three methods known to extend Knuth & Bendix's results.

First we shall study the case where $\mathcal{R}$ is a canonical term rewriting system modulo $=_{\mathcal{E}}$ (Huet [6]), that is $\to_{\mathcal{R}}$ is nœtherian in the quotient structure by $=_{\mathcal{E}}$, and $\to_{\mathcal{R}}$ is *confluent modulo* $=_{\mathcal{E}}$, e.g. $\forall M_1, M_2, M'_1, M'_2$, such that $M_1 =_{\mathcal{E}} M_2$ and $M_1 \to^*_{\mathcal{R}} M'_1$ and $M_2 \to^*_{\mathcal{R}} M'_2$, then $\exists M''_1$, M''_2 such that $M'_2 \to^*_{\mathcal{R}} M''_2$ and $M''_1 =_{\mathcal{E}} M''_2$. Note that if $\mathcal{E}$-equality is decidable, a decision procedure for T-equality is known: $M =_T M'$ iff $\mathcal{R}(M) =_{\mathcal{E}} \mathcal{R}(M')$.

For the two other cases, we have to define a new relation on T:

$$\to_{\approx} = =_{\mathcal{E}} \cdot \to_{\mathcal{R}},$$

that is: to achieve one step of $\rightarrow_{\approx}$ to a term M, one has to find any term $\mathcal{E}$-equivalent to M which is $\rightarrow_{\mathcal{R}}$-simplifiable and then to achieve one step of $\rightarrow_{\mathcal{R}}$-reduction. We define also a new notion of canonical term rewriting system: we say that $\mathcal{R}$ is a *canonical term rewriting system over* $\mathcal{E}$ iff $\rightarrow_{\approx}$ is nœtherian and $\rightarrow_{\mathcal{R}}$ is *confluent over* $=_{\mathcal{E}}$, that is $\forall M, M_1, M_2$, such that $M \rightarrow^*_{\approx} M_1$ and $M \rightarrow^*_{\approx} M_2$, then $\exists M'_1, M'_2$ such that $M_1 \rightarrow^*_{\approx} M'_1$ and $M_2 \rightarrow^*_{\approx} M'_2$ and $M'_1 =_{\mathcal{E}} M'_2$. Note that in the case where $\mathcal{E}$-equality is decidable and $\rightarrow_{\approx}$-simplifiability is decidable and $\mathcal{R}$ is a canonical term rewriting system over $=_{\mathcal{E}}$, we have a decision procedure for T-equality: $M =_T M'$ iff $\mathcal{R}_{\approx}(M) =_{\mathcal{E}} \mathcal{R}_{\approx}(M')$ where $\mathcal{R}_{\approx}(M)$ is a $\rightarrow_{\approx}$-normal form of M which is unique modulo $=_{\mathcal{E}}$.

One difficulty with this approch is the need of a decision procedure for $\rightarrow_{\approx}$-simplifiability. In the case where all equivalences classes under $=_{\mathcal{E}}$ are finite, such a decision procedure is easily obtained by generating the equivalence class of a term and by checking $\rightarrow_{\mathcal{R}}$-simplifiability on each element of this class. This is the way used by Lankford & Ballantyne when dealing with permutative reductions [16,17,18].

Another way is given by Huet in [7]. We first give a definition.

Definition. $\rightarrow_{\mathcal{R}}$ is said to be $=_{\mathcal{E}}$-uniform iff:

$$M \rightarrow_{\mathcal{R}} N \quad \& \quad M \doteq_{\mathcal{E}} M' \Rightarrow \exists N' \quad M' \rightarrow_{\mathcal{R}} N'.$$

Proposition. *Assume $\rightarrow_{\mathcal{R}}$ is $\doteq_{\mathcal{E}}$-uniform, then for any term M, M is $\rightarrow_{\approx}$-reductible iff M is $\rightarrow_{\mathcal{R}}$-reductible.*

Proof. Obvious ∎

Huet gives in [7] a way to decide, for any finite left linear term rewriting system $\mathcal{R}$ and any finite set of equations $\mathcal{E}$ having decidable $\mathcal{E}$-equality if $\mathcal{R}$ is a canonical term rewriting system over $=_{\mathcal{E}}$.

Another way has been introduced by Peterson & Stickel [24]. The idea is to extend $\rightarrow_{\mathcal{R}}$ in a new relation $\rightarrow_{\mathcal{R},\mathcal{E}}$.

Definition. We say that $M \rightarrow_{\mathcal{R},\mathcal{E}} N$ iff:

$$\exists \gamma \rightarrow \delta \in \mathcal{R} \quad \exists \sigma \quad \exists u \in \mathcal{O}(M) \quad M/u =_{\mathcal{E}} \sigma(\gamma) \quad N = M[u \leftarrow \sigma(\delta)]$$

Remark that $\rightarrow_{\mathcal{R},\mathcal{E}}$-simplifiability is decidable, when $\mathcal{R}$ is finite, if T-matching is decidable. We define now a new notion of uniformity.

Definition. $\rightarrow_{\mathcal{R},\mathcal{E}}$ is said to be $\mathcal{E}$-uniform iff:

$$\forall M, N \quad M \rightarrow_{\approx} N \Rightarrow \exists P \quad M \rightarrow_{\mathcal{R},T} P.$$

Proposition. *Assume $\rightarrow_{\mathcal{R},\mathcal{E}}$ is $\mathcal{E}$-uniform, then for any term M, $M \rightarrow_{\approx}$-simplifiable iff $M \rightarrow_{\mathcal{R},\mathcal{E}}$-simplifiable.*

Proof. Obvious ∎

Peterson & Stickel give in [24] a way to decide if $\mathcal{R}$ is a canonical term rewriting system over $\mathcal{E}$ in the case where there exists a complete $\mathcal{E}$-unification algorithm and $\mathcal{R}$ is "$\mathcal{E}$-compatible" which condition is stronger that $\mathcal{E}$-uniform.

We shall extend our results to the three following cases:

(1) $\mathcal{R}$ is a canonical term rewriting system modulo $=_{\mathcal{E}}$.

(2) $\mathcal{R}$ is a canonical term rewriting system over $=_{\mathcal{E}}$ and $\rightarrow_{\mathcal{R}}$ is $=_{\mathcal{E}}$-uniform.

(3) $\mathcal{R}$ is a canonical term rewriting system over $=_{\mathcal{E}}$ and $\rightarrow_{\mathcal{R},\mathcal{E}}$ is $\mathcal{E}$-uniform.

For cases (1) and (2) we will use the same notion of narrowing as in previous section. For case (3) we shall define a new definition of narrowing using $\rightarrow_{\mathcal{R},\mathcal{E}}$ instead of $\rightarrow_{\mathcal{R}}$. Note that this notion of extended narrowing has been introduced by Lankford & Ballantyne [19] in the case of associative commutative derivations. We generalize the result to all cases covered by Peterson & Stickel's paper [23] and prove the correctness of this new T-unification process.

Note that we extend theorems 1 & 2; however it is possible to extend results of section 4 as well.

5.1. Extension to cases (1) & (2).

Lemma 4 (resp. 5) is an analogue of lemma 1 (resp.2). We use the same notations: P and Q are two terms, H is a "new" function symbol and M is $H(P,Q)$.

Lemma 4. *Let us consider any $\mathcal{R}$-derivation:*

$$M = H(P,Q) = M_0 \mathcal{R} M_1 = H(P_1,Q_1) \mathcal{R} \cdots M_n = H(P_n,Q_n),$$

such that P_n and Q_n are $\mathcal{E}$-unifiable, say by substitution σ. Then $\sigma\theta_n$ is a T-unifier of P and Q.

Proof. The proof closely follows that of lemma 1. ∎

Lemma 5. *Let P and Q be two terms which are T-unifiable, ρ be any T-unifier and V be a finite set of variables containing $\mathcal{V}(P) \cup \mathcal{V}(Q)$. Then there exists a $\mathcal{R}$-derivation:*

$$M = H(P,Q) = M_0 \mathcal{R} M_1 = H(P_1,Q_1) \mathcal{R} \cdots \mathcal{R} M_n = H(P_n,Q_n),$$

such that P_n and Q_n are $\mathcal{E}$-unifiable. Let Σ be any complete set of $\mathcal{E}$-unifiers of P_n and Q_n away from $V \cup V_n$. We have:

$$\exists \mu \in \Sigma \quad \mu\theta_n \leq_T \rho[\![V]\!].$$

Moreover we are allowed to restrict our attention to $\mathcal{R}$-derivations such that: $\forall i$, $0 \leq i \leq n$, $\theta_i \uparrow V$ is normalized.

Proof. We have $\rho(P) =_T \rho(Q)$ thus with $\eta = \mathcal{R}(\rho)$, $\eta(P) =_T \eta(Q)$. Let us consider a derivation from $\eta(M)$ to one of its normal form:

$$\eta(M) = H(\eta(P),\eta(Q)) = N_0 \rightarrow \cdots \rightarrow N_n = H(N_P,N_Q),$$

where N_P is a $\rightarrow$-normal form of $\eta(P)$ and N_Q is a $\rightarrow$-normal form of $\eta(Q)$. In the two cases we are studying, we have then $N_P =_{\mathcal{E}} N_Q$. For the corresponding $\mathcal{R}$-derivation we have:

$$\eta_n(M_n) = H(\eta_n(P_n),\eta_n(Q_n)) = N_n = H(N_P,N_Q).$$

Thus η_n is a $\mathcal{E}$-unifier of P_n and Q_n. Let Σ be any complete set of $\mathcal{E}$-unifiers away from $V \cup V_n$. We have:

$$\exists \mu \in \Sigma \quad \mu \uparrow (V \cup V_n) \leq_{\mathcal{E}} \eta_n \uparrow (V \cup V_n),$$

then:

$$\exists \xi \quad (\xi\mu) \uparrow (V \cup V_n) =_{\mathcal{E}} \eta_n \uparrow (V \cup V_n),$$

thus:

$$(\xi\mu\theta_n) \uparrow V = ((\xi\mu) \uparrow (V \cup V_n))(\theta_n \uparrow V) =_{\mathcal{E}} ((\eta_n \uparrow (V \cup V_n))(\theta_n \uparrow V) = (\eta_n\theta_n \uparrow V)$$

and:

$$(\eta_n\theta_n \uparrow V) = (\eta \uparrow V) =_T (\rho \uparrow V),$$

that is:

$$\mu\theta_n \leq_T \rho[\![V]\!],$$

which proves the lemma. ∎

We can now give an analogue of theorem 2:

Theorem 5. *Let T be the equational theory defined by $T = \mathcal{R} \cup \mathcal{E}$ where $\mathcal{R}$ is:*

- *either a canonical term rewriting system modulo $=_{\mathcal{E}}$,*
- *or a canonical term rewriting system over $=_{\mathcal{E}}$ such that $\rightarrow_{\mathcal{R}}$ is $\doteq_{\mathcal{E}}$-uniform,*

and $\mathcal{E}$ is a set of equations defining an equational theory in which a complete $\mathcal{E}$-unification algorithm is known.

Let P and Q be two terms, M be $H(P,Q)$ where H is a new function symbol ($H \notin C$), V be a finite set of variables containing $\mathcal{V}(M)$. Let Σ be the set of all substitutions σ such that σ is in Σ iff there exists a $\mathcal{R}$-derivation:

$$M = H(P,Q) = M_0 \mathcal{R} M_1 = H(P_1,Q_1) \mathcal{R} M_n = H(P_n,Q_n),$$

such that P_n and Q_n are $\mathcal{E}$-unifiable, θ_n is normalized and $\sigma = \mu\theta_n$ where μ is any element in a complete set of $\mathcal{E}$-unifiers of P_n and Q_n. Then Σ is a complete set of T-unifiers of P and Q away from V.

Proof. Lemma 3 proves consistency and lemma 4 proves completeness. ∎

5.2. Extension to case (3).

$\mathcal{R}$ is a canonical term rewriting system over $=_{\mathcal{E}}$ and $\rightarrow_{\mathcal{R},\mathcal{E}}$ is $\mathcal{E}$-uniform. In this case, we need to define a new notion of narrowing.

Definition. Let M be a term and V be a finite set of variables containing $\mathcal{V}(M)$. Assume the following situation holds:

$$\exists u \in \overline{O}(M) \quad \exists \gamma_k \rightarrow \delta_k \in \mathcal{R} \quad \mathcal{U}_{\mathcal{E}}(M/u, \gamma_k, W_k) \neq \emptyset,$$

where we assume $\gamma_k \rightarrow \delta_k$ is renamed so that $\mathcal{V}(\gamma_k) \cap V = \emptyset$ and W_k is a finite set of variables containing $\mathcal{V}(\gamma_k) \cup V$.

Let Σ be any complete set of $\mathcal{E}$-unifiers of M/u and γ_k away from W_k, then each element of Σ will be called *$\mathcal{E}$-narrowing substitution of M away from V*. $NS_{\mathcal{E}}(M,V)$ will denote the set of all such substitutions.

Let N be the term $\sigma(M[u \leftarrow \delta_k])$ where σ is any substitution in Σ. We say that M is *$\mathcal{E}$-narrowable in M at occurrence u using rule $\gamma_k \rightarrow \delta_k$* and we write:

$$M \mathcal{R}_{\mathcal{E},[u,k,\sigma]} N.$$

$\mathcal{R}_{\mathcal{E}}$ is called *$\mathcal{E}$-narrowing relation on T*.

Notations. We will use all notations of section 3. In particular $\mathcal{R}_{\mathcal{E}}$-derivations are defined in an obvious way.

Theorem 6. *Theorem 1 holds if we replace $\rightarrow$-derivation by $\rightarrow_{\mathcal{R},\mathcal{E}}$-derivation and $\mathcal{R}$-derivation by $\mathcal{R}_{\mathcal{E}}$-derivation.*

Proof. The proof follows closely the one of theorem 1, we do not give it. ∎

It is now easy to prove lemma 4 & 5 where narrowing is replaced by $\mathcal{E}$-narrowing. Finally we give an analogue of theorems 1 & 2.

Theorem 7. *Let T be the equational theory defined by $T = \mathcal{R} \cup \mathcal{E}$. $\mathcal{E}$ is a set of equations defining an equational theory in which a complete $\mathcal{E}$-unification algorithm is known. $\mathcal{R}$ is a canonical term rewriting system over $=_{\mathcal{E}}$ such that $\rightarrow_{\mathcal{R},\mathcal{E}}$ is $\mathcal{E}$-uniform. Then the result of theorem 5 holds where $\mathcal{E}$-narrowing is used instead of narrowing.*

Example. We give an example in abelian group theory. In this case $\mathcal{E}$ will be the set of two equations defining the associativity and commutativity of $+$. We list below a canonical term rewriting system for abelian group theory :

$$x + 0 \to x; \tag{r1}$$
$$x + (-x) \to 0; \tag{r2}$$
$$-0 \to 0; \tag{r3}$$
$$-(-x) \to x; \tag{r4}$$
$$-(x + y) \to (-x) + (-y). \tag{r5}$$

which appears in [24,18]. Note that we need to consider extended rules only for rule $(r2)$:

$$x + (-x) + y \to y. \tag{er2}$$

With this rule $\mathcal{E}$-compatibility is insured (see [23]), and $\mathcal{E}$-uniformity follows.

Lankford has proposed to orient rule $(r5)$ from right to left. In this case we obtain another complete set of reductions for abelian groups. Rules $(r1)$ to $(r4)$ are the same, the others are:

$$(-x) + (-y) \to -(x + y); \tag{r5'}$$
$$-((-x) + y) \to x + (-y); \tag{r6'}$$
$$x + -(y + x) \to (-y). \tag{r7'}$$

in this case we need to consider extended rules for rules $(r5')$ & $(r7')$, that is:

$$(-x) + (-y) + z \to -(x + y) + z; \tag{er5'}$$
$$x + -(y + x) + z \to (-y) + z. \tag{er7'}$$

As in the previous example $\mathcal{E}$-compatibility and $\mathcal{E}$-uniformity are then insured.

Let us now consider term $M_1 = -x_1$ (this example is from Lankford). We show that there exists an infinite $\mathcal{E}$-derivation issuing from M_1, even if we restrict ourself to basic $\mathcal{E}$-reduction, as one can define in the same way as basic -reductions. We begin with the first term rewriting system . M_1 is $\mathcal{E}$-unifiable with the left part of rule $(r5)$, $\sigma = \{(x_1 \leftarrow x + y)\}$ being a unifier. Thus, we have (after renaming):

$$M_1 = -x_1 \mathcal{E} M_2 = (-x_2) + (-y_1).$$

In the same way, using subterm $-x_2$ we have:

$$M_2 = (-x_2) + (-y_1) \mathcal{E} M_3 = (-x_3) + (-y_1) + (-y_2),$$

and more generally:

$$M_n = (-x_n) + (-y_1) + \cdots + (-y_{n-1}) \mathcal{E} M_{n+1},$$

showing the existence of an infinite $\mathcal{E}$-derivation. Note that we have used only basic $\mathcal{E}$-derivations.

When dealing with the second term rewriting system, consider rule $(r6')$. We build the infinite derivation:

$$M_1 = -x_1 \mathcal{E} M_2' = (-x_2) + y_1 \mathcal{E} \cdots \mathcal{E} M_n' = (-x_n) + y_1 + \cdots + y_{n-1}.$$

Thus, none of these two canonical term rewriting systems leads to a finite T-unification algorithm with the methods described in this paper. However, there exists a complete and finite T-unification algorithm for abelian group theory as shown by Lankford [14].

Remark. Ballantyne & Lankford have shown in [1] how to solve the word problem for finitely presented commutative semigroups in using associative and commutative term rewriting systems. Thus one could be interested in solving equations in commutative semigroups in using the way described in this section. However note that we cannot expect to show the termination of the algorithm since some of these equations have infinite set of independent unifiers. Let us for instance consider the equational theory defined by $ab = a$ and let us try to unify ax and a where x is a variable. It is easy to show that $x \leftarrow b$, $x \leftarrow bb$, $x \leftarrow bbb$, ... are independent unifiers. (This example was communicated to the author by A.M. Ballantyne).

6. Conclusion.

We have shown in this paper how to improve over Fay's T-unification algorithm. In particular we have given a sufficient condition for the termination of this algorithm, proving a refined version of a conjecture by Lankford. Furthermore we have shown how to extend Fay's algorithm to equational theories defined by various kinds of canonical term rewriting systems.

7. Acknowledgments.

We thank G. Huet for his help in writing this paper and R. Shostak for his many helpful comments.

8. References.

1. Ballantyne A.M. and Lankford D.S., *New Decision Algorithms for Finitely Presented Commutative Semigroups.* Report MTP-4, Department of Mathematics, Louisiana Tech. U., May 1979.
2. Fay M., *First-order Unification in an Equational Theory.* Master Thesis, U. of California at Santa Cruz. Tech. Report 78-5-002, May 1978.
3. Fay M., *First-order Unification in an Equational Theory.* 4th Workshop on Automated Deduction, Austin, Texas, Feb. 1979, 161–167.
4. Huet G., *A Unification Algorithm for Typed Lambda Calculus.* Theoretical Computer Science, 1,1 (1975), 27–57.
5. Huet G., *Résolution d'équations dans des langages d'ordre* $1, 2, \ldots, \omega$. Thèse d'Etat, Université de Paris VII, 1976.
6. Huet G., *Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems.* 18th IEEE Symposium on Foundations of Computer Science (1977), 30–45.
7. Huet G., *Embedding Equational Theories in Complete Sets of Reductions.* Unpublished manuscript, 1979.
8. Huet G. and Lévy J.J., *Call by Need Computations in Non-Ambiguous Linear Term Rewriting Systems.* Rapport Laboria 359, IRIA, Août 1979.
9. Huet G. and Oppen D.C., *Equations and Rewrite Rules: a Survey.* In "Formal Languages: Perspectives and Open Problems". Ed. Book R., Academic press 1980.
10. Hullot J.M., *Associative-Commutative Pattern Matching.* Fifth International Joint Conference on Artificial Intelligence, Tokyo, 1979.
11. Hullot J.M., *A Catalogue of Canonical Term Rewriting Systems.* Unpublished manuscript, March 1980.
12. Knuth D. and Bendix P., *Simple Word Problems in Universal Algebras.* "Computational Problems in Abstract Algebra". Ed. Leech J., Pergamon Press, 1970, 263–297.
13. Lankford D.S., *Canonical Inference.* Report ATP-32, Departments of Mathematics and Computer Sciences, University of Texas at Austin, Dec. 1975.

14. Lankford D.S., *A Unification Algorithm for Abelian Group Theory.* Report MTP-1, Math. Dept., Louisiana Tech. U., Jan. 1979.

15. Lankford D.S., *Private Communication.* 1980.

16. Lankford D.S. and Ballantyne A.M., *Decision Procedures for Simple Equational Theories With Commutative Axioms: Complete Sets of Commutative Reductions.* Report ATP-35, Departments of Mathematics and Computer Sciences, U. of Texas at Austin, March 1977.

17. Lankford D.S. and Ballantyne A.M., *Decision Procedures for Simple Equational Theories With Permutative Axioms: Complete Sets of Permutative Reductions.* Report ATP-37, Departments of Mathematics and Computer Sciences, U. of Texas at Austin, April 1977.

18. Lankford D.S. and Ballantyne A.M., *Decision Procedures for Simple Equational Theories With Commutative-Associative Axioms: Complete Sets of Commutative-Associative Reductions.* Report ATP-39, Departments of Mathematics and Computer Sciences, U. of Texas at Austin, Aug. 1977.

19. Lankford D.S. and Ballantyne A.M., *The Refutation Completeness of Blocked Permutative Narrowing and Resolution.* Fourth Conference on Automated Deduction, Austin, Feb. 1979, 53–59.

20. Livesey M. and Siekmann J., *Unification of Sets.* Internal Report 3/76, Institut fur Informatik I, U. Karlsruhe, 1977.

21. Makanin G.S., *The Problem of Solvability of Equations in a Free Semigroup.* Akad. Nauk. SSSR, TOM 233,2 (1977).

22. Martelli A. and Montanari U., *An Efficient Unification Algorithm.* Unpublished manuscript, 1979.

23. Paterson M.S. and Wegman M.N., *Linear Unification.* J. of Computer and Systems Sciences 16 (1978), 158–167.

24. Peterson G.E. and Stickel M.E., *Complete Sets of Reductions for Equational Theories With Complete Unification Algorithms.* Tech. Report, Dept. of Computer Science, U. of Arizona, Tucson, Sept. 1977.

25. Plotkin G., *Building-in Equational Theories.* Machine Intelligence 7 (1972), 73–90.

26. Raulefs P. and Siekmann J., *Unification of Idempotent Functions.* Unpublished manuscript, 1978.

27. Robinson J.A., *A Machine-Oriented Logic Based on the Resolution Principle.* JACM 12 (1965), 32–41.

28. Slagle J.R., *Automated Theorem-Proving for Theories with Simplifiers, Commutativity and Associativity.* JACM 21 (1974), 622–642.

29. Stickel M.E., *A Complete Unification Algorithm for Associative-Commutative Functions.* 4th International Joint Conference on Artificial Intelligence, Tbilisi, 1975.