Complete Axiomatizations of some Quotient Term Algebras*

Hubert Comon†
CNRS and LRI,
Bat. 490, Université de Paris Sud,
91405 ORSAY cedex, France.
E-mail comon@sun8.lri.fr

February 1992

Abstract

We show that $T(F)/=_E$ can be completely axiomatized when $=_E$ is a *quasi-free* theory. Quasi-free theories are a wider class of theories than *permutative theories* of [Mal71] for which Mal'cev gave decision results. As an example of application, we show that the first order theory of $T(F)/=_E$ is decidable when E is a set of ground equations. Besides, we prove that the Σ_1-fragment of the theory of $T(F)/=_E$ is decidable when E is a *compact* set of axioms. In particular, the existential fragment of the theory of associative-commutative function symbols is decidable.

Introduction

Mal'cev studied in the early sixties classes of locally free algebras that can be completely axiomatized [Mal71]. He proved in particular that what is today known as Clark's equality theory is decidable. He also studied some classes of *permutative algebras* in which, roughly, the axiom

$$f(s_1,\ldots,s_n) = f(t_1,\ldots,t_n) \Rightarrow s_1 = t_1 \wedge \ldots \wedge s_n = t_n$$

is replaced with

$$f(s_1,\ldots,s_n) = f(t_1,\ldots,t_n) \Rightarrow \bigvee_{\sigma\in\Pi} s_1 = t_{\sigma(1)} \wedge \ldots \wedge s_n = t_{\sigma(n)}$$

where Π is a subgroup of the symmetric group S_n.

Such studies were motivated by mathematical logic problems, but computer scientists are now concerned with these works because the decidability of such theories allows the use of the corresponding formulas as *constraints* in a constrained programming language. Therefore, much work has recently been devoted to considering (fragment of) first order

*This paper is an extended version of a paper which appeared in Proc. ICALP 91. It contains some slight extensions of the results of the ICALP paper.

†This work was partly supported by the *Greco de Programmation du CNRS* and partly by the Esprit Basic Research Action COMPASS

theories of some structures built on Herbrand domains. Finite trees over a finite alphabet are studied in [Mah88, CL89]; it turns out that $T(F)$, the Herbrand Universe, is completely axiomatizable. Finite trees over an infinite alphabet are also completely axiomatizable, as well as rational trees [Mah88]. Extensions to other structures have been considered: extension by adding an inequality symbol [Ven87, Com90b, Tre90, Tul91], extension with membership constraints [Com90a].

What we consider here is a simple structure: the Herbrand Universe without any predicate symbol other than equality. However, we do not assume that the model is freely generated: equality is assumed to be generated by a finite set of equations E. In other words, we are interested in the quotient $T(F)/_{=_E}$ where $=_E$ is a finitely generated congruence. This is related to [Bür88], but we consider here the full first order theory (not only a fragment) and we assume a finite alphabet F (the alphabet is assumed to be infinite in [Bür88], which is simpler in some respects).

For an arbitrary E, the first order theory of $T(F)/_{=_E}$ is of course undecidable. At least the word problem (a subset of the Π_1 fragment) and unification problem (a subset of the Σ_1 fragment) should be decidable for the congruence $=_E$. Unfortunately, this is not sufficient: the first order theory of $T(F)/_{=_E}$ has been shown undecidable when E is a set of associative-commutative axioms [Tre90]. Therefore, we have to impose strong restrictions on the set of axioms E in order to derive decidability results. Actually, we show in this paper the decidability of the first order theory of $T(F)/_{=_E}$ when $=_E$ is *quasi-free*. $=_E$ is quasi-free if E is collapse-free resolvent [Kir85, Jou90], *quasi-strict* (this notion is a new notion introduced in this paper) and if the equations in E have a depth 0 or 1. Typically, commutativity axioms are quasi-free (and more generally, permutative axioms of Mal'cev). We also show that, if E is a set of ground axioms (i.e. equations without variables), there is a conservative extension $T(F')/_{=_{E'}}$ of $T(F)/_{=_E}$ where E' is quasi-free. This shows that the first order theory of $T(F)/_{=_E}$ is decidable in this case. This should not be confused with results on the theory of ground systems [DT90]. In the latter case, the structure considered is indeed richer in one sense (there are predicate symbols other than equality), but poorer in some other respects (no function symbols, no equality predicate).

Our decidability results are proved by rewriting the formulas in equivalent formulas (quantifier elimination) until a *solved form* (which is either $\perp$ or satisfiable) is reached. Our proof also constructs an axiomatization of the model: the set of rules, viewed as logical equivalences are valid formulas. On the other hand, they generate a theory which coincides with the theory of our model because rewriting a closed formula (i.e. a formula without free variable) leads either to $\top$ or $\perp$. Therefore, the set of rules itself is a complete axiomatization of $T(F)/_{=_E}$. (This differs from other decidability techniques from which it may be more difficult to extract an axiomatization because of model-theoretic arguments in the proof.)

Actually, we use two sets of transformation rules: the first set of rules reduces every formula to a purely existential one. It is correct in $T(F)/_{=_E}$ when E is quasi-free. The second set of rules transforms any purely existential formula into a solved form. It is correct in $T(F)/_{=_E}$ when E is *compact*. (Roughly, compact equational theories are those for which the *independence of disequations lemma* holds [LMM86].) Splitting the reduction in this way allows to derive the decidability of the existential fragment of the theory of associative-commutative function symbols, since the corresponding equational theory is indeed compact.

Our results show that it is possible to use arbitrary first order formulas, interpreted in a quotient $T(F)/_{=_E}$, as a constraint language, provided that $=_E$ is quasi-free. Other applications are described in [Com91b]. For example, *complement problems* which express instances of finitely many terms which are not instances of another finite set of terms, are useful in many computational problems such as compiling pattern matching, automatic inductive proofs, logic program synthesis ...

We start in section 1 by some classical definitions, including those of equational formulas. In section 2 we introduce syntactic theories, *quasi-strict* theories and quasi-free theories. In section 3 we give a set of rules for quantifier elimination in $T(F)/_{=_E}$ when E is quasi-free. This set of rules is proved terminating. In section 4, we introduce compact theories and show that the existential fragment of the first order theory of $T(F)/_{=_E}$ is decidable in this case. Quasi-free and Associative-Commutative theories are examples of compact theories. Finally, we bring together in section 5 some results established in previous sections: we give a complete axiomatization of $T(F)/_{=_E}$ when E is quasi-free and we show that the first order theory of $T(F)/_{=_E}$ is decidable when E is a finite set of ground equations.

1 Basic Definitions

1.1 Terms and Substitutions

Most of our notations and definitions will be consistent with [DJ90]. A set of *positions* is a prefix-closed set of words over the alphabet of positive integers. The concatenation is denoted $\cdot$ and the empty word is denoted Λ. We write $p \bowtie q$ if p and q are two positions which are incomparable w.r.t. the prefix ordering. Given a set of function symbols F together with an arity function a (which associates a non-negative integer to each function symbol in F), the set of finite trees over F is the set of mappings t from a finite set of positions $Pos(t)$ into F which are consistent with the arity function a:

$p \cdot i \in Pos(t) \Leftrightarrow 1 \leq i \leq a(t(p))$. $T(F)$ is the set of finite trees over F. A tree in $T(F)$ is also called a *ground term*.

Given an infinite set of *variable symbols* X (disjoint from F), $T(F, X)$ is the set of *terms* $T(F \cup X)$ where every symbol in X is considered as having an arity 0. In the following, F is always assumed to be finite. The (syntactic) equality on terms will be denoted $\equiv$.

$t|_p$ is the subterm of t at position p and $t[u]_p$ is the term obtained by replacing $t|_p$ with u at position p. By $t[u]$ we mean that u is a subterm of t. Similar notations are also used for formulas which may be viewed as terms in some algebra.

A *substitution* is a mapping σ from a finite subset $Dom(\sigma) \subset X$ into $T(F, X)$. Every substitution σ can be extended in a unique way into an endomorphism of $T(F, X)$ which is the identity on $X - Dom(\sigma)$. As usual, we confuse the substitution and its extension. A *ground substitution* is a substitution σ such that, for every variable $x \in Dom(\sigma)$, $x\sigma \in T(F)$.

1.2 Equations and equational theory

An *equation* is a pair of terms in $T(F, X)$, denoted $s = t$. $=$ is symmetric: we make no difference between $s = t$ and $t = s$. Given a set of equations E, $=_E$ is the smallest congruence on $T(F, X)$ which contains all equations $s\sigma = t\sigma$ for any $s = t \in E$ and any substitution σ. It is confused with the equational theory of E.

The relation $\xleftrightarrow[E]{p,\sigma}$ is defined on $T(F, X)$ (as in [DJ90]) by:

$$s \xleftrightarrow[E]{p,\sigma} t \text{ iff } \exists l = r \in E,\ s|_p \equiv l\sigma \text{ and } t \equiv s[r\sigma]_p$$

Sometimes, we drop irrelevant indices. For example, $s \xleftrightarrow[l=r]{\Lambda} t$ means that $s \equiv l\sigma$ and $t \equiv r\sigma$. $s \xleftrightarrow{\neq\Lambda} t$ stands for $s \xleftrightarrow{p} t$ for some position $p \neq \Lambda$. Similarly, we use predicate on positions instead of positions themselves to indicate any position satisfying the predicate. For example, we will use $\xleftrightarrow{(>p)^*}$ for $\xleftrightarrow{p \cdot p_1} \dots \xleftrightarrow{p \cdot p_n}$ for some $p_1, \dots, p_n$.

The reflexive transitive closure of a relation R is denoted R^*, its reflexive closure is denoted $R^=$ and its transitive closure is denoted R^+. As usual, we write sometimes e.g. $\xleftrightarrow{(\neq\Lambda)^*}$ instead of $(\xleftrightarrow{\neq\Lambda})^*$.

Similar definitions are obtained, replacing E with a set of rules, in which case we use the notations $\xrightarrow[l \to r]{*}$ or $\xleftarrow[l \to r]{*}$ in order to precise in which way we used the rule.

1.3 Equational Formulas

An *equational formula* is a first order formula whose atoms are equations $s = t$. For simplicity, we assume that every variable is bound at most once and that free variables do not have bound occurrences. The set of free variables of an equational formula ϕ is denoted $Var(\phi)$ (we use a similar notation for sets of formulas). Moreover, negations are assumed to be propagated using classical rules. Then, introducing the new symbol $\neq$ (for $\neg =$), we may assume that equational formulas do not contain any occurrence of $\neg$. Finally, equational formulas are assumed to be in prenex form.

Actually, we need not consider general equational formulas in the following because we are going to use quantifier elimination techniques: we need only to consider the fragment $\exists^*\forall^*$. Indeed, we are going to prove that any formula in the fragment $\exists^*\forall^*$ is equivalent to a formula in the fragment $\exists^*$, which shows, by induction on the number of nested quantifiers and using $\forall^*\exists^* = \neg\exists^*\forall^*\neg$, that every formula is equivalent to a purely existential formula. Then, we only have to study purely existential formulas. More precisely, an *equational problem* is either $\bot$, $\top$ or a formula

$$\bigvee_{i\in I} \exists \vec{w}_i, \forall \vec{y}_i : \ P_i$$

where P_i is quantifier-free. Moreover, we assume in the following that the P_i's are conjunctions of disjunctions of atoms[1] (this choice is arbitrary).

In this paper, we only consider interpretations in quotient term algebras: let E be a set of equations. The set $\mathcal{S}(E,\phi)$ of E-solutions of an equational problem ϕ is the least set of mapping from X into $T(F)/_{=_E}$ such that

$$\begin{array}{rcl} \mathcal{S}(E,\top) & = & T(F)^X \\ \mathcal{S}(E,s=t) & = & \{\sigma \in T(F)^X \mid s\sigma =_E t\sigma\} \\ \mathcal{S}(E,\phi\wedge\psi) & = & \mathcal{S}(E,\phi) \cap \mathcal{S}(E,\psi) \\ \mathcal{S}(E,\exists x : \ \phi) & = & \bigcup_{t\in T(F)} \mathcal{S}(E,\phi\{x\mapsto t\}) \end{array}$$

The other definitions follows from the above ones.

Two formulas that have the same set of solutions are *equivalent* and we write $\phi \approx_E \psi$.

In the whole paper, we always assume that $T(F)/_{=_E}$ is infinite. (If not, everything collapses and results are straightforward).

1.4 First Order Theories

A *sentence* is a first order formula without free variables. The *(first order) theory* $Th(\mathcal{T})$ of a set of formulas $\mathcal{T}$ is the set of sentences ϕ such that $\mathcal{T} \models \phi$. A theory $\mathcal{T}$ (i.e. a set of first order formulas) is *complete* if, for every sentence ϕ, either $\mathcal{T} \models \phi$ or $\mathcal{T} \models \neg\phi$. Let us recall that a complete and recursively enumerable set of formulas has a decidable theory (see e.g. [Sho67] for more details). Finally, if $\mathcal{A}$ is an F-algebra, the *(first order) theory*

[1] We use actually a set of normalization rules (such as in [CL89, Com91b, Com90a]) and assume that the formulas are kept in normal form with respect to these rules.

$Th(\mathcal{A})$ of $\mathcal{A}$ is the set of sentences over the alphabet F of function symbols and the only predicate symbol $=$, which are true in $\mathcal{A}$. Φ is an axiomatization of $\mathcal{A}$ if $Th(\Phi) = Th(\mathcal{A})$.

1.5 Transformation Rules

We are going to use *transformation rules* on formulas. Such rules actually represent infinite sets of rewrite rules in the algebra of equational formulas. A transformation rule R is called *correct* (w.r.t. E) if

$$\phi \rightarrow_R \psi \;\Rightarrow\; \phi \approx_E \psi.$$

If a set of correct transformation rules is terminating and transforms every equational problem in a purely existential formula, then the first order theory of $T(F)/_{=_E}$ is generated by these rules (viewed as logical equivalences) and the purely existential fragment of the theory of $T(F)/_{=_E}$. We are going to construct complete (recursive) axiomatizations of $T(F)/_{=_E}$ in this way.

2 Quasi-free theories

In order to design finite terminating and complete sets of transformation rules for equational theories, a natural idea is to restrict our attention to those theories where it is possible to use a top-down strategy of paramodulation. More precisely, C. Kirchner introduced in his thesis [Kir85] *syntactic (equational) theories*. In such equational theories, every equality proof can be done with at most one inference step at the root of the tree. For such theories it is possible to design simple unification rules [Kir85, KK90, JK91, Jou90]. It is very easy to give the negative counterpart of these rules and therefore to design a set of transformation rules for equational formulas. However, unfortunately, the rules are not always terminating (this is already the case for unification). We therefore need some more restrictions on the presentation. In general, as we show in following sections, the transformation rules for solving equations may introduce "new" (i.e. existentially quantified) variables and the corresponding rules for disequations may introduce universally quantified variables. This is a problem since we aim at eliminating the quantifiers. This is why we consider *quasi-free theories*. In these theories, it is possible to design transformation rules which do not introduce any extra variable.

2.1 Syntactic Theories

Definition 2.1 *A set of equation E is* resolvent *if,*

$$s \overset{*}{\underset{E}{\longleftrightarrow}} t \;\; \textit{iff} \;\; s \overset{(\neq\Lambda)^*}{\underset{E}{\longleftrightarrow}} \overset{\Lambda^=}{\underset{E}{\longleftrightarrow}} \overset{(\neq\Lambda)^*}{\underset{E}{\longleftrightarrow}} t$$

An equational theory which can be generated by a resolvent presentation is called syntactic.

This definition is the classical one ([Kir85, Nip90]) except that we allow axioms $x = s$ where x is a variable. (This is a generalization of definitions in [Com91a].) Given a resolvent presentation, it is easy to derive correct transformation rules which decompose equations until one member is a variable (these rules are called *mutations* in [Kir85]).

The following proposition is a direct consequence of the definitions:

Proposition 2.2 *The rules given in figures 1 are correct w.r.t. E when E is a resolvent set of equations.*

Unfortunately, the mutation rules do not always terminate. Actually, they do terminate under certain syntactic restrictions on E:

Proposition 2.3 *Assume that*

- *for every equation $s = t$ in E, s and t have a depth smaller or equal to 2*
- *there is no equation $t[c]_p = c'$ in E where c and c' are constants and p has a length 2.*

Then the rules of figure 1 do terminate.

Proof

Consider the following interpretation function:

- an equation $s = t$ is interpreted as the pair $(\{d(s), d(t)\}, C(s,t))$ where $\{d(s), d(t)\}$ is the multiset of *depths* of s,t (the depth of a term is the maximal size of its positions) and $C(s,t)$ is the number of constants occurring in s,t.
- a conjunction of equations is interpreted as the multiset of interpretations of each equation
- a disjunction of conjunctions of equations is interpreted as the multiset of interpretations of each conjunction.

Pairs are ordered lexicographically and multisets are ordered using the multiset extension of their base domain (see e.g. [DM79]). Integers are ordered in the usual way.

Every rule transforms a problem

$$\exists \vec{x} : \ (e \wedge c) \vee c_1 \vee \ldots \vee c_n$$

(**Mutate 1**) $f(t_1, \ldots, t_n) = f(u_1, \ldots, u_n) \quad \mapsto \quad \exists Var(E) :$

$$
\begin{array}{ll}
& (t_1 = u_1 \wedge \ldots \wedge t_n = u_n) \\
\vee & \displaystyle\bigvee_{f(v_1,\ldots,v_n)=f(w_1,\ldots,w_n)\in E} (\bigwedge_{i=1}^{n} (t_i = v_i \wedge u_i = w_i)) \\
\vee & \displaystyle\bigvee_{\substack{f(v_1,\ldots,v_n)=x\in E \\ x \text{ variable}}} (x = f(t_1, \ldots, t_n) \bigwedge_{i=1}^{n} u_i = v_i) \vee (x = f(u_1, \ldots, u_n) \bigwedge_{i=1}^{n} t_i = v_i)
\end{array}
$$

(**Mutate 2**) $f(t_1, \ldots, t_n) = g(u_1, \ldots, u_m) \quad \mapsto \quad \exists Var(E) :$

$$
\begin{array}{ll}
& \displaystyle\bigvee_{f(v_1,\ldots,v_n)=g(w_1,\ldots,w_m)\in E} (\bigwedge_{i=1}^{n} (t_i = v_i) \wedge \bigwedge_{i=1}^{m} u_i = w_i)) \\
\vee & \displaystyle\bigvee_{\substack{g(v_1,\ldots,v_m)=x\in E \\ x \text{ variable}}} (x = f(t_1, \ldots, t_n) \bigwedge_{i=1}^{m} u_i = v_i) \\
\vee & \displaystyle\bigvee_{\substack{f(v_1,\ldots,v_n)=x\in E \\ x \text{ variable}}} (x = g(u_1, \ldots, u_m) \bigwedge_{i=1}^{n} t_i = v_i)
\end{array}
$$

where $\exists Var(E)$ stands for $\exists x_1, \ldots \exists x_k$ and $x_1, \ldots, x_k$ are the variables introduced by the rule. We assume moreover that there is no capture (some bound variables are renamed if necessary). Finally, empty conjunctions are identified with $\top$ and empty disjunctions are identified with $\bot$. Finally, the rule **Mutate 2** assumes that $f \neq g$.

Figure 1: Mutation rules for resolvent presentations

where e is an equation and $c, \ldots, c_n$ are conjunctions of equations into a problem

$$\exists \vec{x'} : (e_{1,1} \wedge \ldots \wedge e_{1,m_1} \wedge c) \vee \ldots \vee (e_{k,1} \wedge \ldots \wedge e_{k,m_k} \wedge c) \vee c_1 \vee \ldots \vee c_n$$

after the normalization w.r.t the distributivity of $\vee$ w.r.t. $\wedge$.

By definition of multiset orderings, we only have to show that each new equation $e_{i,j}$ is strictly smaller than e.

Assume that $e \equiv s = t$. Then, the equations introduced by a mutation rule are interpreted in one of the following ways: $(\{d(s)-1, d(t)-1\}, \alpha)$, $(\{d(s)-1, d(u)-1\}, \alpha)$, $(\{d(t)-1, d(v)-1\}, \alpha)$, $(\{d(s), 0\}, \alpha)$, $(\{d(t), 0\}, \alpha)$ where u and v are members of equations of E and α is an integer. By hypothesis, $d(u)$ and $d(v)$ are always smaller than 2. Therefore, if $d(s)$ or $d(t)$ is larger or equal to 2 and both $d(s)$ and $d(t)$ are larger or equal to 1, we have

$$\{(\{d(s)-1, d(u)-1\}, \alpha), (\{d(t)-1, d(v)-1\}, \alpha), (\{d(s), 0\}, \alpha), (\{d(t), 0\}, \alpha)\} < \{(\{d(s), d(t)\}, \beta)\}.$$

If $d(s) = d(t) = 1$, we also have the above inequality. Therefore, it only remains the cases where s or t is a constant. Assume, for example, that t is a constant. Every new equation is interpreted either as $\{d(s)-1, d(u)-1\}$ or as $\{0, 0\}$. In the latter case, s should not be a constant, and, if $d(s) \geq 2$, we obviously have $\{d(s), 0\} > \{d(s)-1, 1\}$. Therefore, we only have to consider the following case: $d(s) = 1$ and $s = f(s_1, \ldots, s_n)$, t is a constant and there is an equation $f(u_1, \ldots, u_n) = t$ in E where $d(u_i) = 1$ for some u_i. By hypothesis, $u_1, \ldots, u_n$ should not contain any constant and the second component of the interpretation is decreasing. $\Box$

The conditions of the propositions are indeed necessary, as shown in the following examples;

Example 2.4 Let $E = \{f(f(f(x_1, x_2), x_3), x_4) = f(x_1, x_4)\}$. Let us show that the mutation does not terminate, showing that it is not possible to expect termination results with axioms of depth 3:

$$f(f(z_1, z_2), z_3) = f(z_4, z_5) \mapsto_{\mathbf{Mutate1}} \mathcal{P}[f(z_1, z_2) = f(f(x_1, x_2), x_3)]$$

where $\mathcal{P}$ is an equational problem. The second equation is, up to renaming, the starting equation.

Example 2.5 Let $E = \{f(f(0)) = 0\}$. Then $f(0) = 0 \mapsto_{\mathbf{Mutate2}} f(0) = 0$. This show why the second condition is useful.

Of course, proposition 2.3 does not prove anything for unification problems: it is well-known that unification modulo associativity is not finitary (and therefore cannot be solved by a terminating finite set of transformation rules), whereas the associativity axiom is resolvent and has a depth 2.

There is another drawback of the mutation rules of figure 1. Remember that we have to put the formulas in conjunctive normal form after each transformation. On the other hand, the right hand sides of the two mutation rules are not in conjunctive normal form and the normalization can be very expensive, because of multiple duplications. Unfortunately, it is not possible to lift the disjunctions at the top of the problem on which the rule is applied, thus avoiding many duplications. More precisely, the following rule is not correct ($\mathcal{P}$ is an equational problem):

$$\textbf{(Mutate 1)}\quad \mathcal{P}[f(t_1,\ldots,t_n) = f(u_1,\ldots,u_n)] \;\mapsto\; \exists Var(E):$$

$$\begin{array}{ll} & \mathcal{P}[t_1 = u_1 \wedge \ldots \wedge t_n = u_n] \\ \vee & \displaystyle\bigvee_{f(v_1,\ldots,v_n)=f(w_1,\ldots,w_n)\in E} \exists Var(E) : \mathcal{P}[\bigwedge_{i=1}^{n} (t_i = v_i \wedge u_i = w_i)] \\ \vee & \displaystyle\bigvee_{\substack{f(v_1,\ldots,v_n) = x \in E \\ x \text{ variable}}} \exists Var(E) : \mathcal{P}[x = f(t_1,\ldots,t_n) \bigwedge_{i=1}^{n} u_i = v_i] \\ & \qquad \vee \exists Var(E) : \mathcal{P}[x = f(u_1,\ldots,u_n) \bigwedge_{i=1}^{n} t_i = v_i] \end{array}$$

For, consider the following example;

Example 2.6 $E = \{f(a,a) = a;\ f(a,f(x,y)) = a\ f(a,b) = a\}$. Let $E' = \{f(a,b) = f(a,a);\ f(a,b) = f(a,f(x,y));\ f(a,a) = f(a,f(x,y))\}$. $E \cup E'$ is resolvant, indeed, orienting the equations of E from left to right yields a canonical rewrite system $\mathcal{R}$. If $s =_E t$, assuming every strict subterm of s, t irreducible w.r.t $\mathcal{R}$, either $s \equiv t$, or s (resp. t) is reducible by $\mathcal{R}$ at the position Λ, or both are reducible at Λ by $\mathcal{R}$. In the former case, we have a rewrite proof with only one step at the root and in the latter case, we use an equation of E', yielding a proof with only one step at the root.

Assuming that $F = \{a, b, f\}$, $\sigma = \{x \mapsto a\}$ is a solution of $\forall y:\ f(x,y) = a$. But the problem

$$(\forall y:\ x = a \wedge y = a) \vee (\forall y:\ x = a \wedge y = b) \vee (\forall y:\ \exists x', y':\ x = a \wedge y = f(x', y'))$$

has no solution.

2.2 Occur Check

We need some more rules for solving equations of the form $x = t[x]$. The most simple way for handling these equations is to assume that they do not have any solutions. Equational theories in which a rule $t[x] = x \mapsto \perp$ is correct (assuming that t is a non trivial context) are called *strict theories* in [Kir85]. We do not really need such a strong condition as strictness. What we actually need is a set of rules for handling positive occur checks.

That is what we are going to propose in this section: we will consider theories in which every identity $s =_E t[s]_p$ can be proved using at least a collapsing rule at a position $q < p$.

Definition 2.7 *A rule* $f(s_1, \ldots, s_n) \to t$ *is* i-collapsing *if, for every substitution* σ, $|s_i\sigma| \geq |t\sigma|$.

$|s|$ is the *size* of the term s, i.e. the number of positions in s. This definition of a collapsing rule is more general than the classical definition which assumes t to be a variable: we do not need such a restriction here. Note that, by definition of a collapsing rule, the multiset of variables occurring in the right hand side of the rule must be included in the multiset of variables occurring in the left hand side of the rule.

For convenience, we may now view a set of equations E as a the set of rules $\bigcup_{l=r\in E}\{l \to r, r \to l\}$.

Definition 2.8 *A finite set of equations E is* quasi-strict *if , for every terms t, u, for every non-root position p of t such that $t[u]_p \overset{*}{\underset{E}{\longleftrightarrow}} u$, p can be written $q \cdot i \cdot q'$ and there is an i-collapsing rule $l \to r \in E$ such that*

$$t[u]_p \overset{(\not\leq q)^*}{\underset{E}{\longleftrightarrow}} \overset{q}{\underset{l\to r}{\longrightarrow}} \overset{*}{\underset{E}{\longleftrightarrow}} u$$

An equational theory is quasi-strict *if it can be generated by a quasi-strict set of equations.*

This definition is actually slightly more general than the one given in [Com91a].

Example 2.9 The following are examples of quasi-strict theories which are not strict (the last set is also resolvent):

- $\{0 + x = x\}$ (left neutral element),
- $\{x + 0 = x;\ 0 + x = x;\ x + y = y + x\}$ (commutativity plus neutral element)
- $\{x * 0 = 0;\ 0 * x = 0;\ 0 * x = x * 0\}$ (absorbing element : (EA)).

We do not prove here the quasi-strictness. Note that, with the definition of [Com91a], the quasi-strictness of these axioms only hold if there is no other function symbols; for example, $f(0 * f(0)) =_{EA} f(0)$ but this cannot be proved with a proof step at the root.

As expected, given a quasi-strict set of equations, it is easy to derive a rule for solving cyclic equations:

$$\textbf{(Cycle)}\quad t[x]_p = x \mapsto \exists Var(E) : \bigvee_{\substack{p = q\cdot i\cdot q' \\ f\in F \\ t|_q \equiv f(t_1,\ldots,t_n) \\ f(u_1,\ldots,u_n)\to w \in E_{c,i}}} (t_1 = u_1 \wedge \ldots \wedge t_n = u_n \wedge x = t[w]_q)$$

where $E_{c,i}$ is the set of i-collapsing rules in E.

Proposition 2.10 *If E is a quasi-strict set of equations, then the rule* (**Cycle**) *is correct.*

This follows from the definition of a quasi-strict set of axioms.

2.3 Quasi-free theories themselves

Definition 2.11 *A set of equations E is* collapse-free *if it does not contain any equation $s = x$ where x is a variable.*

The property of collapse-freeness is not necessary for the correctness of the rules, but we use it for the termination of the formulae-rewriting process.

Definition 2.12 *A* quasi-free *set of equations E is a collapse-free, resolvent and quasi-strict set of equations such that, for every $s = t \in E$, s and t have a depth smaller or equal to 1. An equational theory is quasi-free if it can be generated by a quasi-free set of equations.*

For example, permutative axioms of Mal'cev define quasi-free theories (this includes commutativity axioms). Also, the set (EA) defined above is quasi-free. Finally, we will see in section 5 that every set of ground equations defines an equational theory for which some conservative extension is quasi-free.

3 Quantifier Elimination

When E is quasi-free, the quantifiers that are introduced by the rules (**Mutate 1**), (**Mutate 2**) and (**Cycle**) can be eliminated eagerly. The rules of figure 2 and 3 are precisely those obtained after eliminating the variables introduced by (**Mutate 1**), (**Mutate 2**) and (**Cycle**), and their negation. From the previous section, it should be clear that these rules are correct.

Such rules are combined with some of the rules used for quantifier elimination in finite trees (see [CL89]) which are recalled in figure 4.

The explosion rule is an expression of the *domain closure axiom*[2]:

$$(DCA)\ \ \forall x \ \bigvee_{f \in F} \exists \vec{w} : \ x = f(\vec{w}).$$

The quantifier elimination rules can be easily proved to be correct, except for the rule (QE_3): its correctness w.r.t. E relies on an *independence of disequations* lemma. The following definition is inspired by [LMM86]: disequations are independent if their conjunction is solvable whenever each of them is solvable.

[2] We use here, and only here, that F is finite.

Mutations

(QF_1) $f(t_1,\ldots,t_n) = f(u_1,\ldots,u_n) \ \mapsto$

$$\begin{array}{ll} & (t_1 = u_1 \wedge \ldots \wedge t_n = u_n) \\ \vee & \displaystyle\bigvee_{f(v_1,\ldots,v_n)=f(w_1,\ldots,w_n)\in E} \Big(\big(\bigwedge_{\substack{v_i \equiv v_j \text{ and} \\ v_i \text{ variable}}} t_i = t_j \big) \wedge \big(\bigwedge_{\substack{w_i \equiv v_j \text{ and} \\ v_j \text{ variable}}} u_i = t_j \big) \\ & \quad \wedge \big(\bigwedge_{v_i \text{ constant}} t_i = v_i \big) \wedge \big(\bigwedge_{w_i \text{ constant}} u_i = w_i \big) \\ & \quad \wedge \big(\bigwedge_{w_i \equiv w_j \text{ and } w_j \text{ variable}} u_i = u_j \big) \Big) \end{array}$$

(QF_2) $f(t_1,\ldots,t_n) = g(u_1,\ldots,u_m) \ \mapsto$

$$\begin{array}{l} \displaystyle\bigvee_{f(v_1,\ldots,v_n)=g(w_1,\ldots,w_m)\in E} \Big(\big(\bigwedge_{\substack{v_i \equiv v_j \text{ and} \\ v_i \text{ variable}}} t_i = t_j \big) \wedge \big(\bigwedge_{\substack{w_i \equiv v_j \text{ and} \\ v_j \text{ variable}}} u_i = t_j \big) \\ \quad \wedge \big(\bigwedge_{v_i \text{ constant}} t_i = v_i \big) \wedge \big(\bigwedge_{w_i \text{ constant}} u_i = w_i \big) \\ \quad \wedge \big(\bigwedge_{w_i \equiv w_j \text{ and } w_j \text{ variable}} u_i = u_j \big) \Big) \end{array}$$

(QF_3) $f(t_1,\ldots,t_n) \neq f(u_1,\ldots,u_n) \ \mapsto$

$$\begin{array}{ll} & (t_1 \neq u_1 \vee \ldots \vee t_n \neq u_n) \\ \wedge & \displaystyle\bigwedge_{f(v_1,\ldots,v_n)=f(w_1,\ldots,w_n)\in E} \Big(\big(\bigvee_{\substack{v_i \equiv v_j \text{ and} \\ v_i \text{ variable}}} t_i \neq t_j \big) \vee \big(\bigvee_{\substack{w_i \equiv v_j \text{ and} \\ v_j \text{ variable}}} u_i \neq t_j \big) \\ & \quad \vee \big(\bigvee_{v_i \text{ constant}} t_i \neq v_i \big) \vee \big(\bigvee_{w_i \text{ constant}} u_i \neq w_i \big) \\ & \quad \vee \big(\bigvee_{w_i \equiv w_j \text{ and } w_j \text{ variable}} u_i \neq u_j \big) \Big) \end{array}$$

(QF_4) $f(t_1,\ldots,t_n) \neq g(u_1,\ldots,u_m) \ \mapsto$

$$\begin{array}{l} \displaystyle\bigwedge_{f(v_1,\ldots,v_n)=g(w_1,\ldots,w_m)\in E} \Big(\big(\bigvee_{\substack{v_i \equiv v_j \text{ and} \\ v_i \text{ variable}}} t_i \neq t_j \big) \vee \big(\bigvee_{\substack{w_i \equiv v_j \text{ and} \\ v_j \text{ variable}}} u_i \neq t_j \big) \\ \quad \vee \big(\bigvee_{v_i \text{ constant}} t_i \neq v_i \big) \vee \big(\bigvee_{w_i \text{ constant}} u_i \neq w_i \big) \\ \quad \vee \big(\bigvee_{w_i \equiv w_j \text{ and } w_j \text{ variable}} u_i \neq u_j \big) \Big) \end{array}$$

(QF_2) and (QF_4) assume $f \neq g$.

Figure 2: Mutation Rules in quasi-free theories.

Occur-Check

$$(QF_5)\quad t[x]_p = x \mapsto \bigvee_{\substack{p = q\cdot j\cdot q' \\ f\in F \\ t|_q \equiv f(t_1,\ldots,t_n) \\ f(v_1,\ldots,v_n)\to w \in E_{c,j}}} ((\bigwedge_{i=1}^{n} v_i\sigma_{v_1,\ldots,v_n} = t_i) \wedge t[w]_q\sigma_{v_1,\ldots,v_n} = x)$$

$$(QF_6)\quad t[x]_p \neq x \mapsto \bigwedge_{\substack{p = q\cdot j\cdot q' \\ f\in F \\ t|_q \equiv f(t_1,\ldots,t_n) \\ f(v_1,\ldots,v_n)\to w \in E_{c,j}}} ((\bigvee_{i=1}^{n} v_i\sigma_{v_1,\ldots,v_n} \neq t_i) \vee t[w]_q\sigma_{v_1,\ldots,v_n} \neq x)$$

If $p \neq \Lambda$, E_c is the set of collapsing rules in E and $\sigma_{v_1,\ldots,v_n}$ is the substitution $\{v_{i_1} \mapsto t_{i_1};\ldots;v_{i_k} \mapsto t_{i_k}\}$ where $\{v_{i_1},\ldots,v_{i_k}\} = Var(v_1,\ldots,v_n)$ is a set of distinct variables.

Figure 3: Solving Cycles in quasi-free theories

Definition 3.1 *The disequations $t_1 \neq u_1,\ldots t_n \neq u_n$ are* independent *(w.r.t. E) if*

- *either there is an index i such that $t_i =_E u_i$*
- *or else $t_1 \neq u_1 \wedge \ldots \wedge t_n \neq u_n$ has at least one solution in $T(F)/_{=_E}$.*

Proposition 3.2 *If any n disequations are independent w.r.t. E and if $=_E$ is decidable*[3], *then (QE_3) is correct w.r.t. E.*

Proof

We only have to prove that $\forall\vec{y} : y_1 = t_1 \vee \ldots \vee y_n = t_n$ has no solution under the hypotheses of (QE_3). Let σ be any ground assignment to the free variables of $\exists\vec{y} : y_1 \neq t_1 \wedge \ldots \wedge y_n \neq t_n$. Then for every i, $y_i \neq_E t_i\sigma$ since $y_i \notin Var(t_i\sigma)$ and since $T(F)/_{=_E}$ contains at least two distinct elements (it is assumed to be infinite through the whole paper). By independence of disequations again, we can conclude that $\exists\vec{y}.y_1 \neq t_1\sigma \wedge \ldots \wedge y_n \neq t_n\sigma$ is valid for any σ, hence $\forall\vec{y}.y_1 = t_1 \vee \ldots \vee y_n = t_n$ is unsatisfiable. □

Proposition 3.3 *All rules given in figures 2, 3 and 4. are correct w.r.t. E when E is quasi-free.*

[3]This condition essentially ensures the decidability of applicability of the rule.

Quantifier Elimination Rules (QE)

$$(QE_1) \quad \forall \vec{y}, y : P \ \mapsto \ \forall \vec{y} : \ P \qquad \text{If } y \notin Var(P)$$

$$(QE_2) \quad \forall \vec{y} : \ P \wedge (y \neq t \vee d) \ \mapsto \ \forall \vec{y} : \ P \wedge d\{y \mapsto t\}$$

If d is a disjunction of equations and disequations, $y \in \vec{y}$ and $y \notin Var(t)$.

$$(QE_3) \ \forall \vec{y} : P \wedge (y_1 = t_1 \vee \ldots \vee y_n = t_n \vee d) \ \mapsto \ \forall \vec{y} : P \wedge d$$

If 1. $y_1, \ldots, y_n \in \vec{y}$
2. d is a disjunction of equations and disequations without any universally quantified variable
3. For all i, $y_i \notin Var(t_i)$

Explosion (E)

$$(Ex_1) \quad \forall \vec{y} : \ P \ \mapsto \ \bigvee_{f \in F} \exists w_1, \ldots, w_p, \forall \vec{y} : \ P\{x \mapsto f(w_1, \ldots, w_p)\} \wedge x = f(w_1, \ldots, w_p)$$

This rule is applied only if
1. x is not universally bound and $\vec{w} \cap (Var(P) \cup \vec{y} \cup \mathcal{U}) = \emptyset$
2. There is an equation $x = u$ (or a disequation $x \neq u$) in P such that u is not a variable and contains at least one occurrence of a universally bound variable.
3. No other rule can be applied.

Eliminating trivial equations and trivial disequations (T)

$$\begin{array}{llll} (T_1) & s = s & \mapsto & \top \\ (T_2) & s \neq s & \mapsto & \bot \end{array}$$

Figure 4: Elimination of universally quantified variables in quasi-free theories.

Proof

For the mutation rules, this is a consequence of proposition 2.2. For the Cycle rules, this is a consequence of proposition 2.10. For other rules, except (QE_3), the correction is obvious. (The rules are consequences of the Equality axioms). The correctness of (QE_3) follows from proposition 3.2 and from the forthcoming proposition 4.6. $\square$

We assume that the rules of figures 2 are applied only if the left hand side contains an occurrence of a universally bound variable. We assume moreover that the rules of figure 3 are applied only if x is universally bound. This defines, together with the rules of figure 4, a rewrite system $\mathcal{R}$ on equational problems. The next result is the most difficult of the paper: it states termination of quantifier elimination.

Theorem 3.4 *$\mathcal{R}$ is terminating and every irreducible equational problem is purely existential. (i.e. does not contain any universally bound variable.)*

Proof

We use a proof similar to the termination proof of [CL89]; we first prove the termination of $\mathcal{R}-\{(Ex)\}$, using an interpretation Φ of the formulas in a well-founded domain D. Then, we show that, in any reduction sequence, Φ is strictly decreasing on the subproblems on which explosion is applied.

Every equational problem is a disjunction of quantified conjunctions of disjunctions of atoms. Each atom in a problem is interpreted as tuple, defined as follows:

- For every term t occurring in an equational problem ϕ, let

$$|t|_{U,\phi} = \sum_{p \in Pos(t), t(p) \in \vec{y}} |p|$$

  where $\vec{y}$ is the set of universally bound variables in ϕ and $|p|$ is the length of the position p.

- $N_1(s = t) = N_1(s \neq t)$ is the number of universally bound variables occurring in the same disjunction as the atom.

- $N_2(s = t) = N_2(s \neq t) = \max(|s|_{U,\phi}, |t|_{U,\phi})$

- each atom A is interpreted as $I_0(A) = (N_1(A), N_2(A))$.

Disjunctions of atoms are interpreted as the multiset of interpretations of each atom. Conjunctions of disjunctions are interpreted as the multiset of interpretations of disjunctions. Disjunctions of quantified conjunctions of disjunctions are interpreted as the multiset of interpretations of the conjunctions of disjunctions. These interpretations are ordered using the classical lexicographic and multiset extensions of the orderings.

As for the proof of proposition 2.3, we only have to prove that every rule (but explosion) erases an atom e and creates only atoms strictly smaller than e.

- For the rules (QF_1), (QF_2), (QF_3) and (QF_4), first note that the N_1 component cannot increase since the variables occurring in any new atomic formula also occur in the original atomic formula. On the other hand, the N_2 component is strictly decreasing: each universally bound variable occurs at a strictly smaller position in any new atom.

- For the rules (QF_5) and (QF_6), the N_1 component is not increasing, for the same reason as above. On the other hand, the N_2 component is strictly decreasing: this follows from the definition of a j-collapsing rule. Let us consider, for example, the rule (QF_5). The equations $v_i\sigma_{v_1,\ldots,v_n} = t_i$ are obviously strictly smaller than $t[x]_p = x$ since both sides are strict subterms of $t[x]_p$. Consider now the equations $t[w]_q\sigma_{v_1,\ldots,v_n} = x$. The right hand side w of a j-collapsing rule $f(v_1,\ldots,v_n) \to w$ must be (in case of a quasi-free presentation) either a constant or the variable v_j. In the former case, $|t[w]_q|_{U,\phi} < |t[x]_p|_{U,\phi}$ since an occurrence of x (which is universally bound) disappeared. In the latter case, the same inequality holds because $w\sigma_{v_1,\ldots,v_n}$ is a strict subterm of $t|_q$.

- (QE_2) and (QE_4) decrease the first component of the interpretation. The decreasingness for other rules is obvious.

Now, we have to consider the rule (Ex_1). The rule itself increases the interpretation: if $\phi \equiv \mathcal{P} \vee \mathcal{P}_1 \vee \ldots \vee \mathcal{P}_n$ where

$$\mathcal{P} \mapsto_{Ex_1} \bigvee_{f \in F} \exists \vec{w_f} : \mathcal{P}\{x \mapsto f(\vec{w_f})\} \wedge x = f(\vec{w_f})$$

Let ϕ be interpreted as

$$I(\phi) = \{\{d_1,\ldots,d_m\}, M_1,\ldots,M_n\},$$

where M_i is the interpretation of $\mathcal{P}_i$ and $\{d_1,\ldots,d_m\}$ is the interpretation of $\mathcal{P}$. Let

$$\mathcal{Q}_f \equiv \exists \vec{w_f} : \mathcal{P}\{x \mapsto f(\vec{w_f})\} \wedge x = f(\vec{w_f})$$

Each $\mathcal{Q}_f$ is interpreted as $\{\{(0,0)\}, d_1,\ldots,d_m\}$. Let ψ be the formula obtained after the application of Ex_1 on ϕ. ψ is interpreted as

$$I(\psi) = \{\{\{(0,0)\}, d_1,\ldots,d_m\},\ldots,\{\{(0,0)\}, d_1,\ldots,d_m\}, M_1,\ldots,M_n\}$$

If $\psi \mapsto^*_{\mathcal{R}-\{(Ex_1)\}} \psi' \mapsto_{(Ex_1)} \psi''$, then ψ' is a disjunction

$$\psi' \equiv \mathcal{P}_1 \vee \ldots \vee \mathcal{P}_n \vee \bigvee_{f \in F} \mathcal{Q}'_f$$

where $\mathcal{Q}'_f$ is an irreducible form w.r.t. $\mathcal{R} - \{(Ex)\}$ of $\mathcal{Q}_f$. Because of the control on (Ex_1), all problems $\mathcal{Q}_f$ contain a redex for one of the rules of figures 2, 3. Applying one of these rules to $\mathcal{Q}_f$ results in a formula whose interpretation can be written

$$\{\{(0,0)\}, d_1, \ldots, d_{i-1}, d'_1, \ldots, d'_k, d_{i+1}, \ldots, d_m\}$$

where each d'_j is strictly smaller than d_i by the first part of the proof. By the first part of the proof again, we derive the inequality

$$I(\mathcal{Q}'_f) \leq \{\{(0,0)\}, d_1, \ldots, d_{i-1}, d'_1, \ldots, d'_k, d_{i+1}, \ldots, d_m\}$$

which is strictly smaller than $\{d_1, \ldots, d_n\}$ because d_i cannot be $\{(0,0)\}$. Therefore, $I(\psi')$ is strictly smaller than $I(\phi)$. Hence, the subsequence of formulas on which (Ex_1) is applied must be finite: the system is terminating. □

The termination result might still hold if we remove the conditions on occurrences of universally bound variables, but we were unable to prove it. On the contrary, it is necessary to assume that E is collapse-free (which has been used in order to get a simple form of the rules (QF_i)), as shown by the following

Example 3.5 Let $F = \{0, f, g\}$ and $E = \{g(x) = x\}$. The theory is, of course, quasi-free. Consider now the equational problem

$$\mathcal{P} \equiv \forall y : \ x \neq f(y)$$

The only rule which can be applied is (Ex_1), leading to

$$(\forall y : \ x = 0 \wedge 0 \neq f(y)) \vee (\exists z, \forall y : \ x = f(z) \wedge f(z) \neq f(y)) \vee (\exists z, \forall y : \ x = g(z) \wedge g(z) \neq f(y))$$

The first disjunction reduces to $x = 0$, the second disjunction reduces to $\perp$ and the third disjunction reduces to $\exists z, \forall y : \ x = g(z) \wedge z \neq f(y)$ which contains a renaming of the original problem.

4 Decidability of the Existential Fragment of the Theory of $T(F)/_{=_E}$ when E is Compact

Theorem 3.4 shows that every equational formula is equivalent (w.r.t. $\approx_E$) to a purely existential one when E is a quasi-free set of equations. In order to show the decidability of the first order theory of $T(F)/_{=_E}$, it only remains to solve purely existential formulas. But, for this latter problem, we do not need the theory to be quasi-free: we relax this condition to the weaker assumption that E is *compact.*[4]

4.1 Definition of compact theories

Compact theories are particular cases of *finitary equational theories* (as defined in e.g. [BHSS87]). Let us first recall what are finitary theories. A *Unification problem* is a purely existential equational problem which does not involve negation (i.e. no disequation). A unification problem is *completely solved* if it is $\perp$ or $\top$ or else of the form

$$\exists \vec{w} : \; x_1 = t_1 \wedge \ldots \wedge x_n = t_n$$

where $\mathcal{U} = \{x_1, \ldots, x_n\}$ and $\mathcal{U} \cap Var(\vec{w}, t_1, \ldots, t_n) = \emptyset$. (In other words, a completely solved unification problem defines in a unique way an idempotent substitution).

Definition 4.1 *A finite set of equations is* finitary *if there is a terminating algorithm which transforms any unification problem $\mathcal{P}$ into a finite disjunction of completely solved unification problems $\mathcal{SF}(\mathcal{P})$ such that* $\mathcal{P} \approx_E \bigvee_{\mathcal{E} \in \mathcal{SF}(\mathcal{P})} \mathcal{E}$.

Definition 4.2 *A set of equations E is* compact *if it is finitary and $=_E$ is decidable and any n disequations are independent (w.r.t. E).*

We will see in section 4.3 a general sufficient criterion for compactness of a set of equations, but note already that an empty set of equations is compact by the independence of disequations lemma [LMM86].

4.2 Transformation rules, solved forms and completeness

We assume that the formulas are disjunctions of simple formulas. We use here the set of rules given in figure 5 (this set is actually very simple).

Proposition 4.3 *The rules of figure 5 define a terminating reduction relation. Moreover, if E is compact, then every irreducible formula w.r.t. the rules of figure 5 is either $\perp$ or has at least one solution in $T(F)/_{=_E}$.*

Proof

Let us prove first termination. We consider the following interpretation:

[4] Actually, the main result of this section is very similar to [Bür88]. The only difference is the domain of interpretation: we consider $T(F)/_{=_E}$ whereas H.-J. Bürckert considers $T(F, X)/_{=_E}$. In other words, we assume a finite alphabet, whereas he considered an infinite one. However, as shown for finite trees [Mah88], the cases F finite and F infinite are very different ($T(F)$ is not axiomatized in the same way).

$$(ET_1) \quad t = s \quad \mapsto \quad \top \qquad \text{If } s =_E t$$
$$(ET_2) \quad t \neq s \quad \mapsto \quad \bot \qquad \text{If } s =_E t$$

$$\text{(Solve)} \quad \exists \vec{x} : \; t_1 = u_1 \wedge \ldots \wedge t_n = u_n \wedge d_1 \wedge \ldots \wedge d_m \; \mapsto \bigvee_{\mathcal{E} \in \mathcal{SF}(t_1 = u_1 \wedge \ldots \wedge t_n = u_n)} \exists \vec{x} : \mathcal{E} \wedge d_1 \wedge \ldots \wedge d_m$$

If $\mathcal{SF}(c)$ is a set of completely solved forms of c and $d_1, \ldots d_m$ are disequations.

$$(VE) \quad \exists \vec{w} : \; x = t \wedge P \quad \mapsto \quad \exists \vec{w} : \; x = t \wedge P\{x \mapsto t\}$$

If $x \notin Var(t)$, $x \in Var(P)$ and, when t is a variable, $t \in Var(P)$.

$$(EQE) \quad \exists w : P \wedge w = t \quad \mapsto \quad P \qquad \text{If } w \notin Var(P, t).$$

Figure 5: Transformation of existential formulas when E is compact

- Each disjunction of simple formulas is interpreted as the multiset of interpretations of each simple formula

- $\exists \vec{z} : s_1 = t_1 \wedge \ldots \wedge \ldots s_n = t_n \wedge u_1 \neq v_1 \wedge \ldots \wedge u_m \neq v_m$ is interpreted as the triple (M, N, n) where

  - $M = 1$ if $s_1 = t_1 \wedge \ldots \wedge s_n = t_n$ is not completely solved and $M = 0$ otherwise the number of
  - N is the number of variables in the formula that have more than one occurrence in it

By (Solve), a triple $(1, N, n)$ is replaced with finitely many triples $(0, M, k)$ (and the interpretation is decreasing). By (VE), a triple (M, N, n) is replaced with a triple $(M', N-1, n)$ where $M' \leq M$. By (EQE), a triple (M, N, n) is replaced with a triple $(M, N, n-1)$. By (ET_i) all three components are decreasing. The third one is strictly decreasing.

Since the interpretation is strictly decreasing by application of any rule, the system is terminating. We have now to prove that every irreducible formula which is distinct from $\perp$ has a solution. For, we only have to consider simple formulas.

Let $P \equiv \exists \vec{z} : x_1 = t_1 \wedge \ldots \wedge x_n = t_n \wedge u_1 \neq v_1 \wedge \ldots \wedge u_m \neq v_m$ be an irreducible simple formula. Since P is irreducible, for every i, $u_i \neq_E v_i$. Therefore, by definition 3.1, there is a solution σ to $u_1 \neq v_1 \wedge \ldots \wedge u_n \neq v_n$. Let now $\theta = \{x_1 \mapsto t_1\sigma; \ldots; x_n \mapsto t_n\sigma\}\sigma$. θ is a solution of P since $x_1, \ldots, x_n$ are variables and they occur only once in P. $\square$

Corollary 4.4 *If E is compact, then the Σ_1-fragment of the theory of $T(F)/_{=_E}$ is decidable.*

This is a consequence of proposition 4.3 since the rules of figure 5 are correct w.r.t. E when E is compact.

More interestingly, we now show how to prove compactness.

4.3 Examples of compact theories

The following lemma gives a sufficient criteria for compactness:

Lemma 4.5 *If*

- *E is finitary,*
- *$=_E$ is decidable,*
- *for every set of new constants F', for every equation $s = t$ such that*

- $s, t \in T(F \cup F')$
- $Var(s,t) = \{x\}$
- $s \neq_E t$,

the set $\{u \in T(F \cup F') \mid s\{x \mapsto u\} =_E t\{x \mapsto u\}\}$ *contains finitely many classes,*

then E *is compact.*

Proof

The proof is actually a generalization of the independence of disequations lemma. Consider a conjunction

$$s_1 \neq t_1 \wedge \ldots \wedge s_n \neq t_n$$

where, for every i, $s_i \neq_E t_i$. We are going to prove, by induction on $N = Var(s_1, t_1, \ldots, s_n, t_n)$ that this system has a solution[5] (as soon as $T(F)/_{=_E}$ is infinite, which was assumed through the whole paper).

If the formula does not involve any variable, then it is a valid formula because, by hypothesis, $s_i \neq_E t_i$. Thus, the property holds when $N = 0$.

Assume that the property holds for $N-1$ variables ($N \geq 1$). Let $x \in Var(s_1, t_1 \ldots, s_n, t_n)$ and $X_0 = Var(s_1, t_1, \ldots, s_n, t_n) - \{x\}$. Each equation $s_i = t_i$ has finitely many (maybe 0) solutions in $T(F \cup X_0)$. For each i, let S_i be the set of solutions of $s_i = t_i$. In particular, there is a term t_0 in $T(F \cup X_0)$ which is not equal (modulo $=_E$) to any term in $S_1 \cup \ldots \cup S_n$. Consider now the system

$$s_1\{x \mapsto t_0\} \neq t_1\{x \mapsto t_0\} \wedge \ldots \wedge s_n\{x \mapsto t_0\} \neq t_n\{x \mapsto t_0\}.$$

For every index i, $s_i\{x \mapsto t_0\} \neq_E t_i\{x \mapsto t_0\}$ by construction. By induction hypothesis, this system has a solution σ in $T(F)$. Then $\{x \mapsto t_0\sigma\}\sigma$ is a solution of P. $\square$

It is possible to use this criteria in order to find a number of compact sets of axioms:

Proposition 4.6 *Quasi-free sets of axioms are compact.*

Proof

To prove this property, we use the lemma 4.5. For, we are going to exhibit a unification algorithm which will also decide $=_E$ and prove that any equation with one variable has finitely many solutions.

[5] Actually, it has infinitely many solutions.

Let the rules (QF_1), (QF_2), (QF_5), (T_1) and (VE) form a system $\mathcal{R}'$ which is applied on disjunctions of conjunctions of equations. (Such systems are assumed to be kept in disjunctive normal form.) $\mathcal{R}'$ is terminating. Indeed, consider the following interpretation:

- each equation $s = t$ is interpreted as the sum of the sizes of its members
- each conjunction of equations is interpreted as the pair (n, M) where n is the number of unsolved variables (i.e. variables that have more than one occurrence in the conjunction) and M is the multiset of interpretations of each equation in the conjunction
- disjunctions of conjunctions are interpreted as the multiset of interpretations of each conjunction.

As in the proof of theorem 3.4, it is easy to prove that this interpretation is strictly decreasing by application of the rules, which show their termination. Now, irreducible formulas are finite disjunctions of conjunctions of completely solved forms: unification in quasi-free theories is finitary. Moreover, since we did not introduce any variable, completely solved forms of an equation containing only one variable x can only be $\bot$, $\top$ or $x = t$. Finally, starting with an equation without variables, the result is $\top$ or $\bot$, which decides equality between two terms (variables have to be considered as new constants in such a proof). □

Proposition 4.7 *The sets of equations consisting of associativity and commutativity of function symbols are compact.*

Proof

Here, we use again lemma 4.5: we prove that every non-trivial equation involving only one variable has finitely many ground solutions in the AC case. (It is well known that AC theories are finitary and that $=_{AC}$ is decidable).

Let s, t be two terms such that $Var(s,t) = \{x\}$ and F_{AC} be the subset of F of associative-commutative function symbols. Assume moreover that $s \neq_{AC} t$. We prove by induction on $|s| + |t|$ that $s = t$ as finitely many solutions in $T(F \cup F')$. (For simplicity, we call here "solution" a substitution $\{x \mapsto u\}$ where $u \in T(F \cup F')$.)

if $|s| + |t| = 2$, then s (or t) must be the variable x and t be a constant: there is only one solution to this equation.

assume that the property holds, up to the size $|s| + |t| - 1$. Consider the top symbols of s, t:

- If s (or t) is the variable x, then $s = t$ has either no solution (if x occurs in the other side) or one solution.
- If $s(\Lambda) \neq t(\Lambda)$, then the equation cannot have any solution because AC axioms do not change the top symbol
- If $s(\Lambda) = t(\Lambda) \notin F_{AC}$, then $s \equiv f(s_1, \ldots, s_n)$, $t \equiv f(t_1, \ldots, t_n)$ and $s\sigma =_{AC} t\sigma$ iff, for all i, $s_i\sigma =_{AC} t_i\sigma$. Since $s \neq_{AC} t$, there is at least one index i such that $s_i \neq_{AC} t_i$. Moreover, by induction hypothesis, such an equation has only finitely many solutions.
- If $s(\Lambda) = t(\Lambda) = + \in F_{AC}$. Let $s \equiv n_1x + s_1 + \ldots + s_k$ and $t \equiv n_2x + t_1 + \ldots + t_m$ where nx stands for $\underbrace{x + \ldots + x}_{n \text{ times}}$ and $s_1, \ldots, s_k, t_1, \ldots, t_m$ are terms whose top symbols are distinct from $+$. (We use here the so-called "flatten" representation of AC terms.) The equation $s = t$ can be first simplified, cancelling the smallest number of x's: we may assume (say) that $n_2 = 0$, removing n_2x from both sides. There are now two cases:
  - if $n_1 = 0$, then me must have $k = m$ and, for every solution σ of $s = t$, there is a permutation $\pi \in S_k$ such that, for all i, $s_i\sigma =_{AC} t_{\pi(i)}\sigma$. Since $s \neq_{AC} t$, for every permutation π, there is (at least) one index i such that $s_i \neq_{AC} t_{\pi(i)}$. Thus, by induction hypothesis, for every permutation π, there are finitely many solutions to $s_1 = t_{\pi(1)} \wedge \ldots \wedge s_k = t_{\pi(k)}$. If follows that $s = t$ has finitely many solutions, since there are only finitely many permutations.
  - if $n_1 \neq 0$ then any solution of $s = t$ must map x to $t_{i_1} + \ldots + t_{i_q}$ for some sub-multiset $\{t_{i_1}, \ldots, t_{i_q}\} \subseteq \{t_1, \ldots, t_n\}$. Which proves again the finiteness of the set of solutions. □

5 Decidability of the First Order Theory of $T(F)/_{=_E}$

5.1 E is a quasi-free set of equations

Combining theorem 3.4 with propositions 4.4 and 4.6, we get the decidability of the first order theory of $T(F)/_{=_E}$. Looking more closely at the rules which are used in the transformations, we extract the equality axioms E_{eq} of figure 6. The domain closure axiom (DCA) and the axioms for quasi-free quotients E_{QF} of figure 7.

Theorem 5.1 *$E_{eq} \cup E_{QF} \cup \{DCA\}$ is a complete axiomatization of $T(F)/_{=_E}$ when E is quasi-free.*

Equality axioms

Reflexivity

$$\forall s,\ s = s$$

Symmetry

$$\forall s, t,\ s = t \Leftrightarrow t = s$$

Transitivity

$$\forall s, t, u,\ s = t \wedge s = u \Rightarrow t = u$$

Compatibility

$$\forall t_1, \ldots, t_n, u_1, \ldots, u_n,\ \ t_1 = u_1 \wedge \ldots \wedge t_n = u_n \ \Rightarrow\ f(t_1, \ldots, t_n) = f(u_1, \ldots, u_n)$$

Figure 6: Equality axioms

Mutations

$$\begin{array}{l}\forall x_1, \ldots, x_n, y_1, \ldots, y_m \quad [f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \Longleftrightarrow \\ \qquad (t_1 = u_1 \wedge \ldots \wedge t_n = u_n) \\ \qquad \vee \exists \vec{x} : \bigvee_{f(v_1,\ldots,v_n)=f(w_1,\ldots,w_n)\in E} (\bigwedge_{i=1}^{n} (t_i = v_i \wedge u_i = w_i))\end{array}$$

For every $f \in F$. $\vec{x}$ is assume to contain all variables distinct from $x_1, \ldots, x_n, y_1, \ldots, y_n$.

$$\begin{array}{l}\forall x_1, \ldots, x_n, y_1, \ldots, y_m \quad [f(x_1, \ldots, x_n) = g(y_1, \ldots, y_m) \Longleftrightarrow \\ \qquad \exists \vec{x} : \bigvee_{f(v_1,\ldots,v_n)=g(w_1,\ldots,w_m)\in E} (\bigwedge_{i=1}^{n} (t_i = v_i) \wedge \bigwedge_{i=1}^{m} u_i = w_i))\end{array}$$

For all distinct function symbols $f, g \in F$. $\vec{x}$ is the set of variables which are not in $\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$.

Occur checks

$$\forall x \quad [f(t_1, \ldots t_i[x], \ldots, t_n) = x \Longleftrightarrow \ \exists \vec{z} \bigvee_{f(v_1,\ldots,v_n)\to w\in E_{c,i}} \bigwedge_{j=1}^{n} t_j = v_j \wedge x = w]$$

For each function symbol $f \in F$, each $i \leq a(f)$, each terms $t_1, \ldots, t_n$ and if $E_{c,i}$ is the subset of E containing all i-collapsing rules.

Figure 7: Axioms for "quasi-free" quotients

This theorem is actually a generalization of some Mal'cev results [Mal71]. It implies, of course, the decidability of the first order theory of $T(F)/_{=_E}$.

5.2 E is a finite set of ground equations

Let F_0 be a set of function symbols and E_0 be a set of ground equations. A *conservative extension* of E_0 is a set of equations E, built on a set $F \supseteq F_0$ of function symbols and such that

$$\begin{cases} \forall s, t \in T(F_0),\ s =_{E_0} t \Leftrightarrow s =_E t \\ \forall s \in T(F),\ \exists t \in T(F_0),\ s =_E t \end{cases}$$

In such a case, $Th(T(F_0)/_{=_{E_0}})$ is the subset of formulas in $Th(T(F)/_{=_E})$ which only involve symbols in F_0 (see e.g. [Sho67])

Theorem 5.2 *Let E_0 be a set of ground equations. There is a (computable) conservative extension (F, E) of (F_0, E_0) which is quasi-free.*

<u>Proof</u>

The construction of F, E consist in three steps.

1. Label the nodes of the congruence closure graph (see [NO80]) with new constant symbols. More precisely, we use the following inference rule on pairs (F, E):

   $$F, E \cup \{t[u]_p = s\} \ \vdash\ F \cup \{a\}, E \cup \{t[a]_p = s;\ a = u\}$$

   if $|p| \geq 1$ and $|u| \geq 1$. a is assumed to be distinct from all symbols in F.

   Of course, this rule terminates and the result is a conservative extension of F_1, E_1 of F_0, E_0. Moreover, for every $s = t \in E_1$, the depth of s and t is smaller or equal to 1.

2. We complete E_1, using the Knuth-Bendix completion procedure (see [DJ90]). Let $\geq_{lpo}$ be the lexicographic path ordering extending a total precedence in which constants are smaller than other symbols. $\geq_{lpo}$ is total on ground terms. Therefore, each non trivial ground equation can be viewed as a rule $l \to r$ where $l >_{lpo} r$. The completion consists in applying the following rules:

   $$\begin{array}{rcll} E \cup \{l \to r;\ l \to r'\} & \vdash & E \cup \{l \to r;\ r' \to r\} & \text{If } r' >_{lpo} r \\ E \cup \{l \to r;\ r \to r'\} & \vdash & E \cup \{l \to r';\ r \to r'\} & \\ E \cup \{l[a]_i = r\} & \vdash & l[b]_i = r & \text{If } a \text{ is a constant and } a \to_E b \\ E \cup \{l = l\} & \vdash & E & \end{array}$$

   These rules preserve the property on the depth of terms occurring as a member of an equation of E. The rules also terminate, yielding a canonical rewrite system (this is a classical result). Let E_2 be the resulting set of equations.

3. For every pair $u = t, v = t \in E_2$ where $u >_{lpo} t$ and $v >_{lpo} t$, add the equation $u = v$.

The result is a quasi-free set of equations. Indeed, the property on the depth of members of equations is satisfied; we only have to prove that E is resolvent and quasi-free.

Let s, t be two terms such that $s =_E t$. Since $E_2 \subseteq E$ is convergent and defines the same equational theory as E, there is a rewrite proof $s \xrightarrow[E_2]{*} u \xleftarrow[E_2]{*} t$. E_2 only contains equations between ground terms of depth 0 or 1. Therefore, $s' \xrightarrow[l \to r]{\Lambda} u'$ implies that $s' \equiv l$. Now, E_2 is canonical, which means that every right hand side is irreducible. Hence, if there is a proof step at the root along the proof $s \xrightarrow[E_2]{*} u$, this must be the last step: $s \xrightarrow[E_2]{*} l \xrightarrow[E_2]{\Lambda} u$. Moreover, $l \to u \in E_2$.

It follows that the proof $s \xrightarrow[E_2]{*} u \xleftarrow[E_2]{*} t$ contains at most two steps at the root and that, in such a case the proof can be written

$$s \xrightarrow[E_2]{(\neq\Lambda)^*} l_1 \xrightarrow[l_1 \to u]{\Lambda} u \xleftarrow[l_2 \to u]{\Lambda} l_2 \xleftarrow[E_2]{(\neq\Lambda)^*} t$$

Now, by construction of E, $l_1 = l_2 \in E$: there is a proof of $s =_E t$ involving at most one step at the root.

Let s, t be two terms and p be a non-root position such that $s[t]_p =_E t$. Let t' be the irreducible form of t (w.r.t. E_2). Then $s[t']_p =_E t'$. As above, there is a rewrite proof of this equality: $s[t']_p \xrightarrow[E_2]{*} t'$. Moreover, there should be at least one step in this proof which takes place at a position $q < p$. Since every left hand side of E_2 is ground and has a depth smaller than 1, this means that t' must be a constant. Therefore, the rewrite proof must contain a step at the root. As above, the proof contains actually exactly one step at the root and this is the last rewrite step: $s[t']_p \xrightarrow[E_2]{(\neq\Lambda)^*} u \xrightarrow[E_2]{\Lambda} t'$. $u \to t'$ is an i-collapsing rule of E_2 since, actually, every rule whose right hand side is a constant is i-collapsing. Now, we have a proof

$$s[t]_p \xleftrightarrow[E]{(\neq\Lambda)^*} u \xrightarrow[u \to t']{\Lambda} t' \xleftarrow[E_2]{*} t$$

which means that the theory is quasi-strict[6].

We are now able to conclude that E is quasi-free. □

As a consequence of theorem 3.4 and theorem 5.2, we get:

Theorem 5.3 *The first order theory of $T(F)/_{=_E}$ is decidable when E is a finite set of ground equations.*

[6]We actually proved a stronger property since, in the case of ground axioms, it is always possible to choose $q = \Lambda$. This corresponds to the notion of quasi-freeness of [Com91a].

References

[BHSS87] H. J. Bürckert, A. Herold, and Manfred Schmidt-Schauß. On equational theories, unification and decidability. In *Proc. 2nd Rewriting Techniques and Applications, Bordeaux, LNCS 256*, pages 204–215. Springer-Verlag, May 1987. Also in Claude Kirchner ed. *Unification*, Academic Press, 1990.

[Bür88] H. J. Bürckert. Solving disequations in equational theories. In *Proc. 9th Int. Conf. on Automated Deduction, Argonne, IL, LNCS 310*. Springer-Verlag, May 1988.

[CL89] Hubert Comon and Pierre Lescanne. Equational problems and disunification. *Journal of Symbolic Computation*, 7:371–425, 1989.

[Com90a] Hubert Comon. Equational formulas in order-sorted algebras. In *Proc. 17th Int. Coll. on Automata, Languages and Programming, Warwick, LNCS 443*, Warwick, July 1990. Springer-Verlag.

[Com90b] Hubert Comon. Solving inequations in term algebras. In *Proc. 5th IEEE Symposium on Logic in Computer Science, Philadelphia*, June 1990.

[Com91a] Hubert Comon. Complete axiomatizations of some quotient term algebras. In *Proc. 18th Int. Coll. on Automata, Languages and Programming, Madrid, LNCS 510*, July 1991.

[Com91b] Hubert Comon. Disunification: a survey. In Jean-Louis Lassez and Gordon Plotkin, editors, *Computational Logic: Essays in Honor of Alan Robinson.* MIT Press, 1991.

[DJ90] Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 243–309. North-Holland, 1990.

[DM79] Nachum Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, August 1979.

[DT90] Max Dauchet and Sophie Tison. The theory of ground rewrite systems is decidable. Research Report IT 182, Laboratoire d'Informatique Fondamentale de Lille, Université des Sciences et Techniques de Lille Flandres Artois, France, March 1990. Also in Proc. 5th IEEE LICS, Philadelphia.

[JK91] Jean-Pierre Jouannaud and Claude Kirchner. Solving equations in abstract algebras: A rule-based survey of unification. In Jean-Louis Lassez and Gordon

Plotkin, editors, *Computational Logic: Essays in Honor of Alan Robinson.* MIT-Press, 1991.

[Jou90] Jean-Pierre Jouannaud. Syntactic theories. In B. Rovan, editor, *Proc. 15th Mathematical Foundations of Computer Science, Banskà Bystrica*, 1990. LNCS 452.

[Kir85] Claude Kirchner. Méthodes et outils de conception systématique d'algorithmes d'unification dans les théories equationnelles. Thèse d'Etat, Univ. Nancy, France, 1985.

[KK90] Claude Kirchner and Francis Klay. Syntactic theories and unification. In *Proc. 5th IEEE Symp. Logic in Computer Science, Philadelphia*, June 1990.

[LMM86] Jean-Louis Lassez, M. J. Maher, and K. G. Marriot. Unification revisited. In *Proc. Workshop on Found. of Logic and Functional Programming, Trento, LNCS 306*. Springer-Verlag, December 1986.

[Mah88] M. J. Maher. Complete axiomatizations of the algebras of finite, rational and infinite trees. In *Proc. 3rd IEEE Symp. Logic in Computer Science, Edinburgh*, pages 348–357, July 1988.

[Mal71] A. I. Mal'cev. Axiomatizable classes of locally free algebras of various types. In *The Metamathematics of Algebraic Systems. Collected Papers. 1936-1967*, pages 262–289. North-Holland, 1971.

[Nip90] T. Nipkow. Higher-order unification, polymorphism and subsorts. Tech. Report 210, University of Cambridge, Computer laboratory, November 1990.

[NO80] G. Nelson and D. C. Oppen. Fast decision procedures based on congruence closure. *Journal of the ACM*, 27:356–364, 1980.

[Sho67] J. R. Shoenfield. *Mathematical Logic.* Addison-Wesley, 1967.

[Tre90] Ralf Treinen. A new method for undecidability proofs of first order theories. Tech. Report A-09/90, Universität des Saarladandes, Saarbrücken, May 1990.

[Tul91] Sauro Tulipani. Decidability of the existential theory of infinite terms with subterm relation. To appear in *Information and Computation*, 1991.

[Ven87] K. N. Venkataraman. Decidability of the purely existential fragment of the theory of term algebras. *Journal of the ACM*, 34(2):492–510, 1987.