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

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 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, Com90c, Tre90, Tul90], extension with membership constraints [Com90b].

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

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

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 resolvent [Kir85, Jou90] 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 [Com90a]. 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.

Due to space limitations, all proofs are omitted in this paper.

1 Basic Definitions

Most of our notations and definitions will be consistent with [DJ90]. $T(F,X)$ is the set of finite terms constructed on the finite alphabet of function symbols F (together with their arity) and a set of variable symbols X. We consider only one-sorted terms and F is assumed to be finite. $t|_p$ 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. Λ is the root position. Similar notations are also used for formulas.

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 $x \in Dom(\sigma)$, $x\sigma \in T(F)$. The set of all substitutions is written Σ. 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 $t\sigma = s\sigma$ for $s = t \in E$ and $\sigma \in \Sigma$. $=_E$ is confused with the equational theory of E. The relation $\overset{p,\sigma}{\underset{E}{\longleftrightarrow}}$ is defined on $T(F,X)$ (as in [DJ90]) by:

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

Sometimes, we drop irrelevant indices. For example, $s \overset{\Lambda}{\underset{l=r}{\longleftrightarrow}} t$ means that $s \equiv l\sigma$ and $t \equiv r\sigma$. $s \overset{\neq\Lambda}{\longleftrightarrow} t$ stands for $s \overset{p}{\longleftrightarrow} t$ for some position $p \neq \Lambda$ and $\overset{(\neq\Lambda)^*}{\longleftrightarrow}$ (resp. $\overset{\Lambda^=}{\longleftrightarrow}$) is the reflexive transitive (resp. reflexive) closure of $\overset{\neq\Lambda}{\longleftrightarrow}$. Similar definitions are obtained, replacing E with a set of rules, in which case we use the notations $\overset{*}{\underset{l\to r}{\longrightarrow}}$ or $\overset{*}{\underset{l\to r}{\longleftarrow}}$ in order to precise in which way we used the rule.

An *equational formula* is a first order formula whose atoms are equations. 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 a new symbol $\neq$ (for $\neg =$), we may assume that equational formulas do not contain any occurrence of $\neg$. 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 $\exists^*\forall^*$.[1] 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 in conjunctive normal form[2] (this choice is arbitrary). Finally, every equational problem is given together with a finite set of *unknowns* $\mathcal{U}$ which contains its free variables.

In this paper, we only consider interpretations in quotient term algebras: let E be a set of equations. An E-solution of an equational problem ϕ is a ground substitution σ whose domain is $\mathcal{U}$, the set of unknowns of ϕ and such that $T(F)/_{=_E} \models \phi\sigma$. ($\bot$ and $\top$ have their usual meaning:

[1] 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.

[2] We use actually a set of normalization rules (such as in [CL89, Com90a, Com90b]) and assume that the formulas are kept in normal form with respect to these rules.

respectively no and every ground substitution is a solution of them.) 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).

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 algebra, the *(first order) theory* $Th(\mathcal{A})$ of $\mathcal{A}$ is the set of sentences which are true in $\mathcal{A}$. Φ is an axiomatization of $\mathcal{A}$ if $Th(\Phi) = Th(\mathcal{A})$.

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

$$\phi \mapsto_R \psi \ \Rightarrow\ \phi \approx_E \psi.$$

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, JK90, 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 1 *A set of equation E is* resolvent *if it does not contain any equation $x = s$ where x is a variable*[3] *and if*

$$s \xleftrightarrow[E]{*} t \ \ \textit{iff}\ \ s \xleftrightarrow[E]{(\neq\Lambda)^*} \xleftrightarrow[E]{\Lambda=} \xleftrightarrow[E]{(\neq\Lambda)^*} t$$

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

[3] Actually, this condition can be removed, see [Com91].

This definition is the classical one ([Kir85, Nip90]). Given a resolvent presentation, it is easy to derive correct transformation rules such as:

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

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

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 $\bot$.

The above rule is parametrized by the function symbol f. It is also easy to design rules for solving equations between terms whose top symbols are distinct. (Actually, we use the same rule, except that there must be one step at the root: the first conjunction is erased.)

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 $t[x] = x \mapsto \bot$ 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.

Definition 2 *A rule $f(s_1,\ldots,s_n) \to t$ is called* 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. Note that t is not necessary a variable (which differs from the classical definition). 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 3 *A finite set of equations E is* quasi-strict *if, for every terms t, u, for every position $i \cdot p$ of t such that $t[u]_{i\cdot p} \xleftrightarrow[E]{*} u$, there is an i-collapsing rule $l \to r \in E$ such that*

$$
t[u]_{i\cdot p} \xleftrightarrow[E]{(\neq\Lambda)^*} \xrightarrow[l\to r]{\Lambda} \xleftrightarrow[E]{*} u
$$

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

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

$$
\textbf{(Cycle)}\;\; f(t_1,\ldots,t_n)[x] = x \mapsto \exists Var(E): \bigvee_{f(u_1,\ldots,u_n)\to w\in E_{c,i}} (t_1 = u_1 \wedge \ldots \wedge t_n = u_n \wedge x = w)
$$

where $E_{c,i}$ is the set of i-collapsing rules in E and x is a variable occurring in t_i.

Proposition 1 *If E is a quasi-strict set of equations, then the rule* **(Cycle)** *is correct.*

2.3 Quasi-free theories themselves

Definition 4 *A* quasi-free *set of equations E is a 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, 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**) and (**Cycle**) can eliminated eagerly. The rules of figure 1 are precisely those obtained after eliminating the variables introduced by (**Mutate**) and (**Cycle**) and their negation. Such rules are combined with some of the rules used for quantifier elimination in finite trees (see [CL89]) which are recalled in figure 2. In order to avoid distinguishing between $f = g$ and $f \neq g$ in the rules QF_1, QF_2, we assume that E contains the additional reflexive functional axioms $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ for every $f \in F$. The explosion rule is an expression of the *domain closure axiom*[4]:

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

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.

Definition 5 *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 2 *If any n disequations are independent w.r.t. E and if $=_E$ is decidable*[5]*, then (QE_3) is correct w.r.t. E.*

This shows by proposition 4 (which is stated in the next section) that all rules are correct when E is quasi-free.

The next result is the most difficult of the paper: it states termination of quantifier elimination.

Theorem 1 *The system of transformation rules defined in figures 1 and 2 terminates. Every irreducible equational problem is purely existential. (i.e. does not contain any universally bound variable.)*

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.

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

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

Mutations

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

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

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

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

These two rules assume that the left hand side contains at least one occurrence of a universally bound variable.

Occur-Check

$$(QF_3)\ \ x = f(t_1,\ldots,t_n) \mapsto \bigvee_{f(v_1,\ldots,v_n)\to w\in E_{c,j}} ((\bigwedge_{i=1}^{n} v_i\sigma_{v_1,\ldots,v_n} = t_i) \wedge w\sigma_{v_1,\ldots,v_n} = x$$

$$(QF_4)\ \ x \neq f(t_1,\ldots,t_n) \mapsto \bigwedge_{f(v_1,\ldots,v_n)\to w\in E_{c,j}} ((\bigvee_{i=1}^{n} v_i\sigma_{v_1,\ldots,v_n} \neq t_i) \vee w\sigma_{v_1,\ldots,v_n} \neq x$$

If x is universally bound and occurs in t_j, $E_{c,j}$ is the set of j-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 1: Quantifier Elimination in Quasi-free theories. Part I

Quantifier Elimination Rules (QE)

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

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

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, $y_i \neq_E t_i$

Explosion (E)

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

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)

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

Figure 2: Quantifier Elimination in quasi-free theories. Part II

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

Theorem 1 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[6]. 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.*[7]

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

[6] As already explained, if we are able to transform any $\exists^*\forall^*$ formula into a $\exists^*$ formula, then we are able to transform any equational formula in an $\exists^*$ formula.

[7] 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).

$$\begin{array}{llcll} (ET_1) & t = s & \mapsto & \top & \text{If } s =_E t \\ (ET_2) & t \neq s & \mapsto & \bot & \text{If } s =_E t \end{array}$$

$$(\text{Solve}) \quad t_1 = u_1 \wedge \ldots \wedge t_n = u_n \quad \mapsto \quad \mathcal{E}$$

If $\mathcal{E}$ is a completely solved form of $t_1 = u_1 \wedge \ldots \wedge t_n = u_n$.

$$(DL) \quad \exists \vec{w} : P \wedge (Q_1 \vee Q_2) \quad \mapsto \quad (\exists \vec{w} : \ P \wedge Q_1) \vee (\exists \vec{w} : \ P \wedge Q_2)$$

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

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 3: Transformation of existential formulas when E is compact

is *completely solved* if it is $\bot$ 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 problems defines in a unique way an idempotent substitution).

Definition 6 *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 $\mathcal{E}$ such that $\mathcal{P} \approx_E \mathcal{E}$.*

Definition 7 *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 criteria 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 use here the set of rules given in figure 3 (this set is actually very simple).

Proposition 3 *The rules of figure 3 define a terminating reduction relation. Moreover, if E is compact, then every irreducible formula w.r.t. the rules of figure 3 has at least one solution in $T(F)/_{=_E}$.*

Corollary 1 *If E is compact, then the Σ_1-fragment of the theory of $T(F)/_{=_E}$ is decidable.*

Indeed, we defined the compactness in order to insure this result. More interestingly, we now show how to prove compactness.

Mutations

$\forall x_1,\dots,x_n,y_1,\dots,y_m$

$$[f(x_1,\dots,x_n)=g(y_1,\dots,y_m) \iff \bigvee_{f(v_1,\dots,v_n)=g(w_1,\dots,w_m)\in E} \exists\vec{z} \bigwedge_{i=1}^{n} x_i = v_i \bigwedge_{j=1}^{m} y_i = w_i]$$

where $f \in F$, E is assumed to contain the reflexive functional axioms and $\vec{z} = Var(f(v_1,\dots,v_n),g(w_1,\dots,w_m))$.

Occur checks

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

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

Figure 4: Axioms for "quasi-free" quotients

4.3 Examples of compact theories

The following lemma gives a sufficient criteria for compactness:

Lemma 1 *If E is finitary, $=_E$ is decidable and if every equation $s = t$ such that $Var(s,t) = \{x\}$ and $s \neq_E t$ has finitely many solutions in $T(F \cup F')/_{=_E}$, where F' is an infinite set of constants, then E is compact.*

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

Proposition 4 *Quasi-free sets of axioms are compact.*

To prove this property, we use the lemma 1, showing that the rules (QF_1), (QF_3), (T_1) (without the condition on occurrences of universally bound variables), together with the variable elimination rule (VE) indeed defines a unification algorithm in quasi-free theories (it is also a decision procedure for $=_E$).

Proposition 5 *The sets of equations consisting of associativity and commutativity of function symbols are compact.*

Here, we use again lemma 1: we prove that every non-trivial equation involving only one variable has finitely many ground solutions in the AC case.

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

5.1 E is a quasi-free set of equations

Combining theorem 1 with propositions 1 and 4, 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} (reflexivity, symmetry ,transitivity and compatibility), the domain closure axiom (DCA) and the axioms for quasi-free quotients E_{QF} of figure 4.

Theorem 2 *$E_{eq} \cup E_{QF} \cup \{DCA\}$ is a complete axiomatization of $T(F)/_{=_E}$ when E is quasi-free.*

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 3 *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.*

Roughly, the construction of E consist of the following steps:

1. Label the nodes of the congruence closure graph (see [NO80]) with new constant symbols: this amounts to add some new ground equations.

2. Use the Knuth-Bendix completion procedure (see [DJ90]) with a lexicographic path ordering extending a total precedence in which constants are smaller than other symbols. The result is a finite set of ground equations whose depth is at most 1.

3. For every pair $u = t, v = t$ where $u > t$ and $v > t$, add the equation $u = v$.

The result is a quasi-free set of equations.

As a consequence of theorem 1 and theorem 3, we get:

Theorem 4 *The first order theory of $T(F)/_{=_E}$ is decidable when E is a finite set of ground equations.*

References

[BHSS87] H. J. Bürckert, A. Herold, and Manfred Schmidt-Schauß. On equational theories, unification and decidability. In *Proc. Rewriting Techniques and Applications 87, Bordeaux, LNCS 256*, pages 204–215. Springer-Verlag, May 1987. Also in C. Kirchner ed. *Unification*, Academic Press, 1990.

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

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

[Com90a] Hubert Comon. Disunification: a survey. In Jean-Louis Lassez and Gordon Plötkin, editors, *Computational Logic: Essays in Honor of Alan Robinson*. MIT Press, 1990. to appear.

[Com90b] Hubert Comon. Equational formulas in order-sorted algebras. In *Proc. ICALP, Warwick*. Springer-Verlag, July 1990.

[Com90c] Hubert Comon. Solving inequations in term algebras. In *Proc. 5th IEEE Symposium on Logic in Computer Science, Philadelphia*, June 1990.

[Com91] H. Comon. Complete axiomatizations of some quotient term algebras. Research report, LRI and CNRS, Univ. Paris-Sud, 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.

[DT90] M. Dauchet and S. 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.

[JK90] Jean-Pierre Jouannaud and Claude Kirchner. Solving equations in abstract algebras: A rule-based survey of unification. In Jean-Louis Lassez and Gordon Plötkin, editors, *Computational Logic: Essays in Honor of Alan Robinson.* MIT-Press, 1990. to appear.

[Jou90] Jean-Pierre Jouannaud. Syntactic theories. In B. Rovan, editor, *Proc. MFCS 90, Banskà Bystrica, LNCS 452*, 1990.

[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 F. Klay. Syntactic theories and unification. In *Proc. 5th IEEE Symp. Logic in Computer Science, Philadelphia*, June 1990.

[LMM86] J.-L. 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] Tobias Nipkow. Proof transformations for equational theories. In *Proc. 5th IEEE Symp. Logic in Computer Science, Philadelphia*, June 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] R. Treinen. A new method for undecidability proofs of first order theories. Tech. Report A-09/90, Universität des Saarladandes, Saarbrücken, May 1990.

[Tul90] Sauro Tulipani. Decidability of the existential theory of infinite terms with subterm relation. Unpublished Draft, October 1990.

[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.