Solving linear equations over polynomial semirings

Paliath Narendran*
Institute of Programming and Logics
Department of Computer Science
State University of New York at Albany
Albany, NY 12222
dran@cs.albany.edu†

Abstract

We consider the problem of solving linear equations over various semirings. In particular, solving of linear equations over polynomial rings with the additional restriction that the solutions must have only non-negative coefficients is shown to be undecidable. Applications to undecidability proofs of several unification problems are illustrated, one of which, unification modulo one associative-commutative function and one endomorphism, has been a long-standing open problem. The problem of solving multiset constraints *is also shown to be undecidable.*

1 Introduction

Equational unification is an important computational problem in automated theorem proving. Its usefulness derives from the ability to 'build in' many proof steps into the pattern matching algorithm, possibly shortening the search for a proof.

Several equational theories have been considered in the literature (see the surveys by [4, 10]) and decidability/complexity results have been obtained for many of them [12, 17]. In this paper we consider linear equations over semirings, in particular $\mathsf{N}[x_1, \ldots, x_n]$, and present an undecidability result that is relevant to several unification problems. In other words, we show that the problem of checking whether there is a solution to a set of linear equations over polynomial rings, with the additional restriction that the solutions must have only non-negative coefficients, is undecidable. This is in contrast to the case where there is no such restriction, i.e., where the solutions are over $\mathsf{Z}[x_1, \ldots, x_n]$; here variants of the Gröbner basis approach [6, 11] can be used to solve the problem.

One of the surprising consequences of our proof is that we need only *one* indeterminate for the reduction to work, i.e., the problem of solving equations over $\mathsf{N}[x]$ is itself undecidable.

This result, though negative, is useful since several unification problems can be shown to be undecidable by reduction from this. Examples are the CCC-unification problem, shown to be undecidable in [14], and unification modulo the theory AC1h, consisting of one associative-commutative function with identity and one endomorphism. The latter is a new undecidability result. We can also show that the problem of solving *multiset constraints* (which generalizes the set constraint problem) is undecidable, by straightforward reduction from AC1h-unification. With slight modifications in the arguments, ACh-unification can also be shown to be undecidable. This problem is mentioned as an open problem in [10].

It is hoped that this result will also be of interest to researchers in Computer Algebra, since the computational problem considered is a generalization of (a) solving linear equations over N (linear diophantine equations) and (b) solving linear equations over $\mathsf{Z}[x]$, both of which are known to be decidable.

2 Basic definitions

A *semiring* is an algebraic structure $< A, +, *, 0, 1 >$ consisting of a set A, binary operators $+$ and $*$, and constants 0 and 1, satisfying the properties

(a) $< A, +, 0 >$ is a commutative monoid,
(b) $< A, *, 1 >$ is a monoid,
(c) $*$ distributes over $+$, and
(d) $x * 0 \ = \ 0 * x \ = \ 0$.

In other words, a semiring is "a ring without subtraction." The most well-known semiring is the natural numbers, N, with $+$, $*$, 0 and 1 given the usual interpretation.

Given a semiring S, the semiring of polynomials

*Partially supported by the NSF grant CCR-9404930.
†Phone: (518)442-3387, Fax: (518)442-5638

$S[x_1, \ldots, x_n]$, where the x_i's are indeterminates, can be defined in the usual way: a polynomial in $S[x_1, \ldots, x_n]$ is a finite sum of monomials, where each monomial is a finite power product of the indeterminates multiplied by a coefficient $c \in S$. Thus the polynomial semiring $\mathsf{N}[x_1, \ldots, x_n]$ consists of polynomials whose coefficients are nonnegative integers.

Linear equations over a semiring R are defined as equations of the form

$$c_1 U_1 + \ldots + c_k U_k + p \;=\; d_1 V_1 + \ldots + d_m V_m + q$$

where the U_i's and the V_i's are variables, and the c_i's, the d_i's, p and q belong to R.

Let E be a set of equational axioms and $=_E$ be the equational congruence generated by E. We often call such an E, along with $=_E$, an equational theory. Given an equational theory E, an *elementary term* is a term built using only the function symbols appearing in E and additional constants. Two terms s and t are said to be *unifiable modulo an equational theory E* if and only if there exists a substitution θ such that $\theta(s) =_E \theta(t)$. The *elementary unification problem* modulo an equational theory E is to determine, given a set of equations $\{s_1 = t_1, \ldots, s_n = t_n\}$, whether there exists σ such that $\sigma(s_1) =_E \sigma(t_1), \ldots, \sigma(s_n) =_E \sigma(t_n)$, where the terms ($s_i$'s and t_i's) are elementary terms[1]. This is in contrast to the *general unification problem* modulo E where the input terms may contain uninterpreted function symbols that do not occur in E.

We refer the reader to [4] and [10] for detailed surveys on unification theory.

Throughout this paper we concentrate on equational theories consisting of an operator $+$ that is associative and commutative, and one or more homomorphisms h_i over $+$. We first consider the case where $+$ also has an identity 0, with $h_i(0) = 0$ for all homorphisms h_i.

3 The main result

Lemma 3.1 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate. Then the solution set of*

$$(x-1)Y \;=\; Z - 1$$

over $\mathsf{N}[x_1, \ldots, x_n]$ is $\{< Y = x^{k-1} + x^{k-2} + \ldots + 1,\ Z = x^k > \mid k \geq 0\}$.

Sketch of proof: Let $< Y = p,\ Z = q >$ be a solution. The polynomial q must evaluate to 1 at $x = 1$. Since q cannot have any negative coefficients, the only possibility is that there is only one monomial in it, x is the only indeterminate in it, and its coefficient is 1. □

This lemma can be generalized to

Lemma 3.2 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate, and d a positive integer. Then the solution set of*

$$(x^d - 1)Y \;=\; Z - 1$$

over $\mathsf{N}[x_1, \ldots, x_n]$ is $\{< Y = x^{d(k-1)} + x^{d(k-2)} + \ldots + 1,\ Z = x^{dk} > \mid k \geq 0\}$.

Sketch of proof: By the same argument as in the above proof, Z must be of the form x^i for some $i \geq 0$. We prove the lemma by contradiction. Let r be the smallest natural number such that r is not a multiple of d and $(x^d - 1)Y = x^r - 1$ has a solution over $\mathsf{N}[x_1, \ldots, x_n]$. Y must then be of the form $x^{r-d} + Y'$ for some $Y' \in \mathsf{N}[x_1, \ldots, x_n]$. But this results in the equality

$$(x^d - 1)Y' \;=\; x^{r-d} - 1$$

with $r - d$ as a smaller counterexample. □

Lemma 3.3 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate and $v \in \mathsf{N}[x_1, \ldots, x_n]$. The equations*

$$\begin{aligned}(x-1)U_1 &= W_1 - 1\\ (x^2-1)U_2 &= W_2 - 1\\ (x-1)U_3 &= U_2 - U_1\\ (x-2)Y_1 &= U_1 - v\\ (x^2-2)Y_2 &= U_2 - v\end{aligned}$$

have a solution over $\mathsf{N}[x_1, \ldots, x_n]$ if and only if $v = 2^k - 1$ for some $k \geq 0$.

Sketch of proof: The first two equations force $U_1 = x^{k-1} + x^{k-2} + \ldots + 1$ and $U_2 = x^{2(j-1)} + x^{2(j-2)} + \ldots + 1$, for some $j, k \in \mathsf{N}$. The third forces $j = k$, since evaluating U_2 and U_1 at $x = 1$ must result in the same value.[2]

By the last two equations, evaluating v at $x = 2$ and $x = \sqrt{2}$ must result in the same value, namely $2^k - 1$. In the absence of negative coefficients, this is possible only if $v = 2^k - 1$. □

The above lemma enables us to constrain variables to be natural numbers.

Corollary 3.4 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate and $v_1 \in \mathsf{N}[x_1, \ldots, x_n]$. The equations*

$$\begin{aligned}(x-1)U_1 &= W_1 - 1\\ (x^2-1)U_2 &= W_2 - 1\\ (x-1)U_3 &= U_2 - U_1\\ (x-2)Y_1 &= U_1 - V\\ (x^2-2)Y_2 &= U_2 - V\\ v_1 + V_2 &= V\end{aligned}$$

[1] This is called *unification with constants* in [4]

[2] Strictly speaking, we do not have to constrain U_3, Y_1 and Y_2 to be from $\mathsf{N}[x_1, \ldots, x_n]$. We could let them be from $\mathsf{Z}[x_1, \ldots, x_n]$, since only divisibility by the polynomial on the left is needed.

have a solution over $\mathsf{N}[x_1, \ldots, x_n]$ *if and only if* v_1 *is a natural number.*

Lemma 3.5 *Let* $x \in \{x_1, \ldots, x_n\}$ *be an indeterminate and* v_1 *and* v_2 *be non-negative integers. The equations*

$$\begin{aligned}(x-1)Y_1 &= Z-1\\(x-1)Y_2 &= Y_1 - v_1\\(x-1)Y_3 &= Y_2 - v_2\end{aligned}$$

have a solution over $\mathsf{N}[x_1, \ldots, x_n]$ *if and only if* $v_2 = v_1(v_1-1)/2$. *(Thus* $2v_2 + v_1 = {v_1}^2$.*)*

Sketch of proof: By Lemma 3.1, the first equation forces Z to be of the form x^k for some k. We consider the case where $k \geq 3$. Y_1 has to be $x^{k-1} + \ldots + 1$, again by Lemma 3.1. Since Y_1 evaluates to k at $x = 1$, it must be that $v_1 = k$. Now dividing $x^{k-1} + \ldots + 1 - k$ by $x - 1$ gives $Y_2 = x^{k-2} + 2x^{k-3} + \ldots + jx^{k-j-1} + \ldots + (k-2)x + k - 1$. Y_2 evaluates to $\sum_{i=1}^{k-1} i = k(k-1)/2$ at $x = 1$, which, by the third equation, is the value of v_2.

The cases $k = 0, 1, 2$ can be done by computation. □

4 Reduction from Hilbert's tenth problem

We use the formulation of Hilbert's tenth problem where every equation is of one of the following forms: $y_i = m$, $y_i + y_j = y_k$, or $y_i y_j = y_k$, where m is a natural number. Since squaring is available to us by Lemma 3.5, we can simulate the product using the identity $(u+v)^2 = u^2 + v^2 + 2uv$. Thus the following can be easily shown:

Lemma 4.1 *The following problem is undecidable:*

INSTANCE: A set of diophantine equations S *where each equation is either a linear equation or an equation of the form* $y_i = {y_j}^2$.
QUESTION: Does S *have a solution over* N*?*

Theorem 4.2 *Solvability of linear equations over the ring* $\mathsf{N}[x_1, \ldots, x_n]$ *is undecidable for all* $n \geq 1$.

Proof: Consider a set of diophantine equations satisfying the conditions mentioned in Lemma 4.1, i.e., each equation is either a linear equation or one of the form $x = y^2$. Let $z_1, \ldots, z_m$ be the variables of S.

The modus operandi is as follows:

(a) Impose the condition that $z_1, \ldots, z_m$ are natural numbers using Corollary 3.4.

In fact, the following equations are sufficient:

$$\begin{aligned}(x-1)U_1 &= W_1 - 1\\(x^2-1)U_2 &= W_2 - 1\\(x-1)U_3 &= U_2 - U_1\\(x-2)Y_1 &= U_1 - V\\(x^2-2)Y_2 &= U_2 - V\\z_1 + \ldots + z_m + V_2 &= V\end{aligned}$$

where $W_1, W_2, U_1, U_2, U_3, V$ and V_2 are new variables.

(b) Take the linear equations as they are.

(c) Simulate equations of the form $z_i = {z_j}^2$ using Lemma 3.5.

Let $k = m * i + j$. We form the equations

$$\begin{aligned}(x-1)Y_{k,1} &= Z_k - 1\\(x-1)Y_{k,2} &= Y_{k,1} - z_j\\(x-1)Y_{k,3} &= Y_{k,2} - V_k\\z_i &= 2V_k + z_j\end{aligned}$$

(Note that the last equation forces V_k to be a natural number, since z_i and z_j are already forced to be natural numbers.)

Let T be the set of linear equations over $\mathsf{N}[x_1, \ldots, x_n]$ obtained this way. It is clear that T has a solution over $\mathsf{N}[x_1, \ldots, x_n]$ if and only if S has a solution over the natural numbers. □

5 Reductions

5.1 AC1 + a homomorphism

The theory AC1h consists of the equations

$$\begin{aligned}x + (y+z) &= (x+y)+z\\x+y &= y+x\\x+0 &= x\\h(0) &= 0\\h(x+y) &= h(x)+h(y)\end{aligned}$$

The connection between the (elementary) unification problems of such theories—with one AC1 operator and several homomorphisms—and solving linear equations over $\mathsf{N}[x_1, \ldots, x_n]$ was first observed by Nutt [15] (see also [2]).

Theorem 5.1 [15] *Solvability of linear equations over* $\mathsf{N}[x]$ *is reducible to the unifiability problem for AC1h.*

Corollary 5.2 *AC1h-unification is undecidable.*

It was already shown by Baader [2] that the apparent simplicity of the the theory *AC1h* is deceptive, because the unification problem is of type 0; in other words, complete, minimal sets of unifiers may not always exist. The present result complements this, by showing that even computationally this theory is quite nasty.

5.2 CCC-unification

The CCC-unification problem [14] is the equational unification problem for the theory

$$\begin{array}{rcl} x \times (y \times z) & = & (x \times y) \times z \\ x \times y & = & y \times x \\ x \times 1 & = & x \\ 1 \Rightarrow x & = & x \\ x \Rightarrow 1 & = & 1 \\ x \Rightarrow (y \Rightarrow z) & = & (x \times y) \Rightarrow z \\ x \Rightarrow (y \times z) & = & (x \Rightarrow y) \times (x \Rightarrow z) \end{array}$$

Our result also gives us an alternative undecidability proof for this problem. To see that AC1h-unification can be reduced to CCC-unification observe that if a is a constant, then $\lambda x.a \Rightarrow x$ behaves like a homomorphism (with 1 as the unity of the operator $\times$).

Alternatively, we could directly reduce from the solvability problem. This reduction was first outlined in [13]. Since the published proof in [14] does not use this reduction, we briefly sketch it here.

First of all, note that we can view $\times$ as $*$ (multiplication) and $\Rightarrow$ as $\uparrow$ (exponentiation). We use $+$ and the natural numbers merely for abbreviation; e.g., a^{x+y} is the abbreviation of $a^x * a^y$, and $2x$ is the (further) abbreviation of $x + x$. Thus for any polynomial p with positive integral coefficients, x^p is a valid term in our algebra, where x is a variable. So also is a^p, where a is a constant. Now any polynomial q from $\mathsf{Z}[x_1, \ldots, x_n]$ can be written as $q' - q''$ where q' and q'' have only positive coefficients. (Think of these as the "positive" and "negative" parts of the polynomial.) Hence it should not be too difficult to see that solving the linear equation

$$p_1 Y_1 + \ldots + p_m Y_m = p$$

over $\mathsf{N}[x_1, \ldots, x_n]$ where $p_1, \ldots, p_m, p \in \mathsf{Z}[x_1, \ldots, x_n]$, is equivalent to unifying the terms $y_1{}^{p_1{}'} * y_2{}^{p_2{}'} * \ldots * y_m{}^{p_m{}'} * a^{p''}$ with $y_1{}^{p_1{}''} * y_2{}^{p_2{}''} * \ldots * y_m{}^{p_m{}''} * a^{p'}$, where

(a) a is a constant, and the y_i's are variables,

(b) the indeterminates $x_1, \ldots, x_n$ of the polynomial ring are treated as constants, and

(c) the primes and double-primes stand for the positive and negative parts as mentioned before.

Example: Consider the polynomials $p_1 = y^2 - x$ and $p = y^4 - x^2$ from the ring $\mathsf{Z}[x, y]$. The corresponding unification problem is

$$\begin{array}{c} ((y \times y) \Rightarrow y_1) \times ((x \times x) \Rightarrow a) \quad = \\ (x \Rightarrow y_1) \times ((y \times y \times y \times y) \Rightarrow a) \end{array}$$

The solution $\theta = \{((x \Rightarrow a) \times ((y \times y) \Rightarrow a))/y_1\}$ corresponds to the solution $q_1 = x + y^2$ for the polynomial problem. □

5.3 Multiset constraints

Solving *set constraints* has been found to be very useful in program analysis and type inference [9]. Let F be a signature containing at least one constant and let $T(F)$ be the set of all ground terms formed using symbols from F. A set constraint over $T(F)$ is any expression relating two sets, built using F, a set of variables X ranging over subsets of $T(F)$, set operations $\cup$ (union) $\cap$ (intersection) and $\setminus$ (set difference), and standard boolean operations. If $x_1, \ldots, x_n$ are sets and f is an n-ary function symbol, then $f(x_1, \ldots, x_n)$ is defined as

$$f(x_1, \ldots, x_n) = \{f(t_1, \ldots, t_n) \mid t_i \in x_i \ (1 \leq i \leq n)\}$$

$f(x_1, \ldots, x_n)$ is empty if any of the x_i's is empty. The empty set is denoted by 0 and the set of all ground terms $T(F)$ is denoted by 1.

Solvability of set constraints as defined above has been shown to be decidable in several papers [1, 5].

Here we show that the similar problem of *multiset constraints,* where all the set operations are understood as operations over multisets, is undecidable, even if we only have *one* unary function symbol. The reduction is from elementary AC1h-unification (Section 5.1).

Corresponding to each elementary term over the theory AC1h we define a multiset as follows: treat 0 as the empty set, each constant a as a singleton set $\{a\}$, the AC1 operator $+$ as multiset union, and each variable x as standing for a multiset. Thus any elementary unification problem P can be mapped to a multiset constraint problem $\psi(P)$. Conversely, any finite multiset S over the given signature can be viewed as an elementary term, by mapping the empty set to 0, singleton sets $\{t\}$ to the terms t, and $\{t_1, t_2, \ldots, t_m\}$ to the term $t_1 + \cdots + t_m$.

Lemma 5.3 *Let Q be any instance of elementary AC1h-unification. Then S has a solution if and only if the corresponding multiset constraint $\psi(Q)$ has a finite solution.*

Proof: Straightforward. □

Strictly speaking, this only shows that the problem of checking whether a system of multiset constraints has a *finite* solution is undecidable. But extending this to the case of general (i.e., possibly infinite) solutions is not very difficult. (This is very easy if we use negative constraints of the form $X \neq \emptyset$.)

Theorem 5.4 *Solvability of multiset constraints is undecidable, even when there is only one unary function symbol.*

Sketch of proof: See Appendix. □

5.4 ACh-unification

The difference between the theories AC1h and ACh is that in the latter[3], the associative-commutative operator + does not have an identity. In other words, ACh consists of

$$\begin{aligned} x + (y + z) &= (x + y) + z \\ x + y &= y + x \\ h(x + y) &= h(x) + h(y) \end{aligned}$$

Unification modulo ACh is also related to solving linear equations over $\mathsf{N}[x]$, but with the additional stipulation that none of the variables can take the values 0. For instance, consider the equation

$$(x - 1)Y = Z - 1$$

used in Lemma 3.1. This is related to the unification problem

$$h(y) + a =_{ACh} y + z$$

but note that $z \leftarrow a$ will not lead to a unifier since we have no 0. On the other hand, $z \leftarrow h(a)$ is indeed possible, with $y \leftarrow a$. Generalizing this, $z \leftarrow h^i(a)$, $i \geq 1$, is a possible unifier, with $y \leftarrow h^{i-1}(a) + \ldots + a$. Going back to the linear equation above, we can see that the solution that is ruled out is precisely $< Z = 1, Y = 0 >$.

Let $\mathsf{N}^+[x_1, \ldots, x_n] = \mathsf{N}[x_1, \ldots, x_n] \setminus \{0\}$. We can easily show that for any set of linear equations of the form

$$p_1 X_1 + \ldots + p_m X_m + p_{m+1} = q_1 X_1 + \ldots + q_m X_m + q_{m+1}$$

where the X_i's are variables and $p_i, q_i \in \mathsf{N}^+[x]$ for $1 \leq i \leq m + 1$, we can construct an elementary ACh-unification problem such that the set of equations is solvable over $\mathsf{N}^+[x]$ if and only if the unification problem has a solution modulo ACh.

Going back to the lemmas of Section 3, we can see that they all hold with very minor modifications for $\mathsf{N}^+[x]$:

Lemma 5.5 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate. Then the solution set of*

$$(x - 1)Y = Z - 1$$

over $\mathsf{N}^+[x_1, \ldots, x_n]$ is $\{< Y = x^{k-1} + x^{k-2} + \ldots + 1,\ Z = x^k > \mid k \geq 1\}$.

Lemma 5.6 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate and d be a nonzero natural number. Then the solution set of*

$$(x^d - 1)Y = Z - 1$$

over $\mathsf{N}^+[x_1, \ldots, x_n]$ is $\{< Y = x^{d(k-1)} + x^{d(k-2)} + \ldots + 1,\ Z = x^{dk} > \mid k \geq 1\}$.

[3] The theory ACh is referred to as $\{E(h, *), A(*), C(*)\}$ in [10].

Lemma 5.7 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate and $v \in \mathsf{N}^+[x_1, \ldots, x_n]$. The equations*

$$\begin{aligned} (x - 1)U_1 &= W_1 - 1 \\ (x^2 - 1)U_2 &= W_2 - 1 \\ (x - 1)U_3 &= U_2 - U_1 \\ (x - 2)Y_1 &= U_1 - v \\ (x^2 - 2)Y_2 &= U_2 - v \end{aligned}$$

are solvable over $\mathsf{N}^+[x_1, \ldots, x_n]$ if and only if $v = 2^k - 1$ for some $k \geq 2$.

Lemma 5.8 *Let $x \in \{x_1, \ldots, x_n\}$ be an indeterminate and v_1, v_2 be non-negative integers. The equations*

$$\begin{aligned} (x - 1)Y_1 &= Z - 1 \\ (x - 1)Y_2 &= Y_1 - v_1 \\ (x - 1)Y_3 &= Y_2 - v_2 \end{aligned}$$

are solvable over $\mathsf{N}^+[x_1, \ldots, x_n]$ if and only if $v_1 \geq 3$, and $v_2 = v_1(v_1 - 1)/2$. (Thus $v_2 \geq 3$ and $2v_2 + v_1 = {v_1}^2$.)

The proofs are straightforward and are left to the reader.

The undecidability proof is by reduction from a slight modification of Hilbert's 10^{th} problem where the solutions all have to be greater than 2.

Theorem 5.9 *ACh-unification is undecidable.*

This settles, negatively, an open problem mentioned in [10]. We also get the result that unification modulo ACD_l, where there is an associative-commutative function $+$ and a function * that distributes over it from the left, i.e.,

$$\begin{aligned} x + (y + z) &= (x + y) + z \\ x + y &= y + x \\ x * (y + z) &= (x * y) + (x * z) \end{aligned}$$

is undecidable.

Corollary 5.10 *ACD_l-unification is undecidable.*

Acknowledgements: The author wishes to thank Franz Baader, Deepak Kapur, Klaus Madlener, Bob McNaughton, Friedrich Otto, Mahadevan Subramaniam, and Volker Weispfenning for their comments and suggestions.

References

[1] A. Aiken, D. Kozen, M. Vardi and E. Wimmers. The complexity of set constraints. Presented at the 7th workshop on Computer Science Logic (CSL 93), Swansea, U.K., September 1993.

[2] F. Baader. Unification in Commutative Theories, Hilbert's Basis Theorem, and Gröbner bases. *Journal of the ACM* 40 (3) (1993) 477–503.

[3] F. Baader and W. Nutt. Adding Homomorphisms to Commutative/Monoidal Theories, or: How Algebra Can Help in Equational Unification. In: Proceedings of the 4th International Conference on Rewriting Techniques and Applications, RTA 91, Lecture Notes in Computer Science 488, 124–135, 1991. (To appear in *Applicable Algebra in Engineering, Communication and Computing.*)

[4] F. Baader and J.S. Siekmann. Unification theory. In: *Handbook of Logic in Artificial Intelligence and Logic Programming* (D.M. Gabbay, C.J. Hogger, J.A. Robinson, eds.), Oxford University Press, 1994.

[5] L. Bachmair, H. Ganzinger, and U. Waldmann. Set constraints are the monadic class. Presented at LICS '93, Montreal, Canada.

[6] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In *Multidimensional systems theory* (N.K. Bose, ed.), Reichel, Dordrecht, 1985, 184–229.

[7] M. Davis. *Computability and Unsolvability.* Dover Publications, 1982.

[8] N. Dershowitz and J.-P. Jouannaud. Rewrite Systems. *Handbook of Theoretical Computer Science*, Elsevier Science Publishers, 1990, 245–320.

[9] N. Heintze and J. Jaffar. A decision procedure for a class of set constraints. In *Proc. of the 5th Symposium on Logic in Computer Science* (LICS), pages 42–51, IEEE, June 1990.

[10] J.-P. Jouannaud and C. Kirchner. Solving Equations in Abstract Algebras: A Rule-Based Survey of Unification. In: *Computational Logic: Essays in Honor of Alan Robinson,* (Lassez and Plotkin, eds.), MIT Press, 1991, 360-394.

[11] A. Kandri-Rody and D. Kapur. Computing the Gröbner Basis of a Polynomial Ideal over Integers. Proceedings of the *Third MACSYMA Users' Conference,* Schenectady, NY, July 1984, pp. 436-451.

[12] D. Kapur and P. Narendran. Complexity of Unification Problems with Associative-Commutative Operators. *Journal of Automated Reasoning* 9 (2) (1992) 261-288.

[13] P. Narendran, F. Pfenning and R. Statman. On the Unification Problem for Cartesian Closed Categories. Presented at the Workshop on Higher Order Logic, Banff, Alberta, September 24-27, 1989.

[14] P. Narendran, F. Pfenning and R. Statman. On the Unification Problem for Cartesian Closed Categories. Presented at LICS '93, Montreal, Canada. (To appear in the *Journal of Symbolic Logic.*)

[15] W. Nutt. Unification in monoidal theories. Proceedings of the *10th International Conference on Automated Deduction (CADE-10),* Kaiserslautern, West Germany, July 1990 (Springer LNCS 449).

[16] W. Nutt. Unification in monoidal theories is solving linear equations over semirings. Research Report RR-92-01, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), Saarbrücken, Germany, January 1992.

[17] M. Schmidt-Schauss. An algorithm for distributive unification. Interner Bericht 13/94, Fachbereich Informatik, Universität Frankfurt, Frankfurt, Germany, 1995. (To be presented at RTA'96.)

Appendix

Throughout this section, let Σ be a signature consisting of a monadic function symbol h and a constant c and let $T_\Sigma = T(\Sigma)$ be the set of all ground terms over Σ.

Lemma A1 *Let α and v be multisets over T_Σ. Then the multiset constraints*

$$\begin{aligned} \alpha + U &= h(U) + \{c\} \\ \alpha + U' + U' &= h(U') + v \\ U \cap v &= \{c\} \\ U &\subseteq U' \end{aligned}$$

are solvable if and only if $\alpha = \{h^n(c)\}$ and $v = \{\underbrace{c, \ldots, c}_{2^n}\}$ for some $n \geq 0$.

Sketch of proof: We represent each multiset S by its characteristic function $\mu_S : T_\Sigma \longrightarrow \mathbb{N}$. Clearly, for all X,

$\mu_{h(X)}(c) = 0$ and

$\mu_{h(X)}(h(w)) = \mu_X(w)$.

Suppose $\alpha = \emptyset$. Then the (only) solution to the first equation is $U = \{c, h(c), \ldots, h^k(c), \ldots\}$, or, in other words, $\mu_U(x) = 1$ for all $x \in T_\Sigma$. Hence (by the third equation) the multiset v can only contain c's. Let $\mu_v(c) = k$ for some $k > 0$. Since α is empty, $\mu_{U'}(c) = k/2$. In general,

$$\begin{aligned} \mu_{U'}(h^{j+1}(c)) &= \mu_{h(U')}(h^{j+1}(c))/2 \\ &= \mu_{U'}(h^j(c))/2. \end{aligned}$$

Thus $\mu_{U'}(c) = k/2$, $\mu_{U'}(h(c)) = k/4$, $\mu_{U'}(h^2(c)) = k/8$, and so on. In general,

$$\mu_{U'}(h^i(c)) = k/2^{i+1}$$

for all i. If $l = \lfloor \log_2(k) \rfloor$, then $\mu_{U'}(h^l(c))$ will have to be 0. This contradicts the last inequality $U \subseteq U'$.

If $\alpha \neq \emptyset$, then it is not hard to see that every solution to the first equation has to be of the form

$$\alpha = \{h^n(c)\},\ U = \{c, h(c), \ldots, h^{n-1}(c)\}$$

Hence v must consist of 2^n c's, i.e.,

$$\mu_v(x) = \begin{cases} 2^n & \text{if } x = c \\ 0 & \text{otherwise} \end{cases}$$

and,

$$\mu_{U'}(h^i(c)) = \begin{cases} 2^{n-i-1} & \text{if } 0 \leq i \leq n-1 \\ 0 & \text{otherwise} \end{cases}$$

□

From the above proof, it is easy to see that the following lemma holds.

Lemma A2 *Let β be a multiset over T_Σ. Then the multiset constraints*

$$\begin{aligned} Z + U &= h(U) + \{c\} \\ Z + U' + U' &= h(U') + V \\ U \cap V &= \{c\} \\ U &\subseteq U' \\ \beta &\subseteq U' \end{aligned}$$

are solvable if and only if β is a finite multiset.

Sketch of Proof: It is clear from the above proof that β has to be finite, since U' is finite. On the other hand, if β is a finite multiset over T_Σ, then it can be 'accommodated' by choosing a large enough n for $Z = \{h^n(c)\}$. □

Suppose the natural numbers are represented by multisets consisting of c alone, (i.e., m is represented by $\{\underbrace{c, \ldots, c}_{m}\}$). Then Lemma A1 enables us to restrict the multiset variables to such multisets. Also, Lemma A2 allows us to constrain multisets to be finite. Now the following lemma, which can be called the "multiset version" of Lemma 3.5, can be proved:

Lemma A3 *Let v_1 and v_2 be multisets that represent natural numbers. The constraints*

$$\begin{aligned} h(Y_1) + \{c\} &= Z + Y_1 \\ h(Y_2) + v_1 &= Y_1 + Y_2 \\ h(Y_3) + v_2 &= Y_2 + Y_3 \end{aligned}$$

have a solution over finite multisets over T_Σ if and only if $|v_2| = |v_1|(|v_1| - 1)/2$.

($|v|$ stands for the cardinality of multiset v.)

The undecidability result of Theorem 5.4 follows easily.