Unification for Infinite Sets of Equations Between Finite Terms*

Wan Fokkink
University of Wales Swansea
Department of Computer Science
Singleton Park, Swansea SA2 8PP, Wales
e-mail: w.j.fokkink@swan.ac.uk

Abstract

A standard result from unification theory says that if a finite set E of equations between finite terms is unifiable, then there exists a most general unifier for E. In this paper, the theorem is generalized to the case where E may be infinite. In order to obtain this result, substitutions are allowed to have an infinite domain.

Keywords: Programming languages, logic programming, most general unifier, infinite sets.

1 Introduction

The unification problem is to determine, given an equation $s = t$ in some logic, whether there exists a substitution σ such that $(s)\sigma \equiv (t)\sigma$. The substitution σ is a 'unifier', and $s = t$ is called 'unifiable'. For an introduction into the field of unification theory, see [2, 1].

A first algorithm, which solves the unification problem for finite terms in first-order logic, stems from Herbrand's thesis [8] (see [7]). This algorithm was rediscovered by Prawitz [16], and its full significance was recognized only after Robinson [17] had employed it in his resolution principle for automatic theorem-proving. Robinson was the first to define the basic concepts for unification. His algorithm decides whether an equation between finite terms is unifiable or not, and if so, then it produces a unifier which is 'most general', meaning that all other unifiers for the equation can be derived from it. Linear unification algorithms were proposed by Martelli and Montanari [12] and by Paterson and Wegman [15]. The well-known unification algorithm by Martelli and Montanari [13] has a worst-case time complexity of $O(n+G(n))$, where G is the inverse of the Ackermann function.

*This research was carried out at CWI, Department of Computer Science, Amsterdam, The Netherlands.

The unification algorithms work only for finite sets of equations. For example, the infinite collection $\{x_i = x_{i+1} \mid i = 0, 1, 2, ...\}$ has most general unifiers σ_n for $n = 0, 1, 2, ...$ with $(x_i)\sigma_n \equiv x_n$ for $i = 0, 1, 2, ...$ The unification algorithms would not terminate in the process of computing one of these unifiers.

This paper considers, in first-order logic, the unification problem for collections of infinitely many equations between finite terms. Substitutions are allowed to have an infinite domain, that is, for a substitution σ there may be infinitely many variables x such that $(x)\sigma \not\equiv x$. It is proved that each (possibly infinite) unifiable collection of equations allows a most general unifier. Basically, the construction of this most general unifier mimics the algorithm of Martelli-Montanari, extended with limit procedures.

The unification result in this paper is incomparable with unification results for infinite sets of equations based on lattices by Huet [9] and Eder [5], where substitutions always have a finite domain. In [5] an artificial top element ∞ is added to the collection of idempotent substitutions, and each set of equations between terms that cannot be unified by a substitution with finite support is awarded the same most general unifier, ∞.

An example of the use of unification of infinite sets of equations between finite terms can be found in [6], where a general format for structured operational semantics is studied. Such a semantics may contain operational rules with infinitely many variables; in order to give meaning to these rules one needs substitutions with infinite domains. In [6] it is needed that a substitution τ which can be unified by a substitution σ (meaning that $\tau\sigma \equiv \sigma$), allows a most general unifier, being a substitution, and not just some artificial top element. Only existence of such a most general unifier is needed, not its actual computation; existence follows immediately from the result in this paper.

Acknowledgements. This research was initiated by discussions with Catuscia Palamidessi, Rob van Glabbeek, and Fer-Jan de Vries. Catuscia is thanked for many valuable discussions, and Gérard Huet for lucid explanations on lattices.

2 Preliminaries

Assume an alphabet, which consists of the disjoint union of an infinite, possibly uncountable, set of variables, and a possibly uncountable set of function symbols. Each function symbol f is provided with an arity $ar(f)$, being a natural number ≥ 0. The collection of *terms* over the alphabet is defined inductively as follows:

- each variable is a term,
- for f is a function symbol, and $t_1, ..., t_{ar(f)}$ terms, $f(t_1, ..., t_{ar(f)})$ is a term.

Syntactic equivalence between terms is denoted by $\_ \equiv \_$. The number of function symbols in a term is called the *size* of the term. (Note that variables do not add any weight.)

A *substitution* is a mapping from variables to terms. The notation $\sigma \equiv \tau$ means that $(x)\sigma \equiv (x)\tau$ for all variables x. Each substitution is extended to a mapping from terms to terms in the standard way. The *domain* of a substitution σ is the collection of variables x for which $(x)\sigma \not\equiv x$. Unlike the standard approach in logic programming, here substitutions are allowed to have an infinite, possibly uncountable, domain. On the other hand, we deal with finite terms.

In the sequel, E denotes a set of equations $s = t$ between terms. A substitution σ applies to a set E as expected; each equation $s = t$ in E is mapped to $(s)\sigma = (t)\sigma$. An equation $s = t$ is said to be a *proper sub-equation* of equations $C[s] = C[t]$ for non-trivial contexts $C[]$.

Definition 1 *A substitution σ is a* unifier *for E if for all $s = t \in E$ we have $(s)\sigma \equiv (t)\sigma$. The set E is called* unifiable *if it allows a unifier.*

A substitution σ is a unifier *for a substitution τ if $\tau\sigma \equiv \sigma$.*

The fact that substitutions are allowed to have an infinite domain is essential for the unification of infinite sets of equations. For example, if $x_0, x_1, x_2, ...$ are distinct variables, then the set $\{x_i = x_{i+1} \mid i = 0, 1, 2, ...\}$ is unified by the substitution σ with $(x_i)\sigma \equiv x_0$ for $i = 0, 1, 2, ...$

Definition 2 *A unifier Θ for E is called* most general *if $\Theta\sigma \equiv \sigma$ for each unifier σ for E.*

3 The Main Theorem

A standard result from unification theory says that if a *finite* set E of equations between terms is unifiable, then there exists a most general unifier for E. In this paper, the theorem is generalized to the case where E may be infinite.

Theorem 3 *If E is unifiable, then it has a most general unifier.*

Proof. We are to find a most general unifier Θ for E. Let τ_0 denote the identity substitution, and define $E_0^e = \{e\}$ for each $e \in E$. The following construction produces from a substitution τ_{n-1} and unifiable sets of equations E_{n-1}^e, a substitution τ_n and unifiable sets of equations E_n^e. It is based on the transformation rules "decomposition" and "variable elimination" from the algorithm of Martelli-Montanari.

- If E_{n-1}^e contains an equality $f(s_1, ..., s_{ar(f)}) = g(t_1, ..., t_{ar(g)})$, then $f \equiv g$, because E_{n-1}^e is unifiable. Replace each such equation in E_{n-1}^e by its proper sub-equations $s_i = t_i$ for $i = 1, ..., ar(f)$. Denote the resulting set by F_n^e. Note that a substitution unifies E_{n-1}^e if and only if it unifies F_n^e.

- Consider the variables x outside the domain of τ_{n-1} for which $\cup_{e \in E} F_n^e$ contains (one or more) equations of the form $x = t$ or $t = x$, where t is not a single variable. For each such a variable x, choose one of these equations $x = t$ or $t = x$, and put $(x)\tau_n \equiv t$. Put $(y)\tau_n \equiv (y)\tau_{n-1}$ for all other variables y. In particular, τ_n equals τ_{n-1} on the domain of τ_{n-1}.

- Put $E_n^e = (F_n^e)\tau_n$.

From the following Property 1, and from the fact that τ_0 and E are unifiable, it follows immediately that all E_n^e are unifiable.

1. Each unifier σ for τ_{n-1} and $\cup_{e\in E}E_{n-1}^e$, is also a unifier for τ_n and $\cup_{e\in E}E_n^e$.

Proof. Since σ unifies E_{n-1}^e, it also unifies F_n^e, for each $e \in E$.

If $(x)\tau_n \equiv (x)\tau_{n-1}$ for a variable x, then $(x)\tau_n\sigma \equiv (x)\tau_{n-1}\sigma \equiv (x)\sigma$, because σ unifies τ_{n-1}. Otherwise, if $(x)\tau_n \not\equiv (x)\tau_{n-1}$, then it follows from the construction of τ_n that $(x)\tau_n = x$ (or its reverse) is in $\cup_{e\in E}F_n^e$. Since σ unifies all F_n^e, it follows that $(x)\tau_n\sigma \equiv (x)\sigma$. Hence, σ unifies τ_n.

$(E_n^e)\sigma = (F_n^e)\tau_n\sigma = (F_n^e)\sigma$, because σ unifies τ_n. Since σ unifies F_n^e, it follows that σ unifies E_n^e, for each $e \in E$. □

2. Each unifier σ for τ_n and E_n^e, is also a unifier for τ_{n-1} and E_{n-1}^e.

Proof. τ_{n-1} equals τ_n on its domain, and σ unifies τ_n, so σ also unifies τ_{n-1}.

$(F_n^e)\sigma = (F_n^e)\tau_n\sigma = (E_n^e)\sigma$, and σ unifies E_n^e, so σ unifies F_n^e. Then σ unifies E_{n-1}^e. □

Since τ_n equals τ_{n-1} on the domain of τ_{n-1}, we can define the 'union' τ of the substitutions τ_n:

$$(x)\tau \equiv \begin{cases} (x)\tau_n & \text{if } (x)\tau_n \not\equiv x \text{ for some } n, \\ x & \text{otherwise.} \end{cases}$$

3. For each variable x, either $(x)\tau \equiv x$, or $(x)\tau$ is not a variable.

Proof. If $(x)\tau \not\equiv x$, then $(x)\tau \equiv (x)\tau_n$ for some $n > 0$. Let n be the smallest number for which this equality holds, so that $(x)\tau_n \not\equiv (x)\tau_{n-1}$. Then it follows from the construction of τ_n that there is an equation $x = t$ or $t = x$ in $\cup_{e\in E}F_n^e$, where t is not a variable, and $(x)\tau_n \equiv t$. Hence, $(x)\tau \equiv t$ is not a variable. □

4. For each variable x, there is a natural number $M(x)$ such that $(x)\tau^{M(x)+1} \equiv (x)\tau^{M(x)}$.

Proof. Fix a unifier σ for E. Since σ also unifies the identity τ_0, Property 1 implies that σ is a unifier for all τ_n. So σ is a unifier for their union τ, which means that $(x)\tau^m\sigma \equiv (x)\sigma$ for all m. Thus, the size of the terms $(x)\tau^m$ cannot grow beyond the size of $(x)\sigma$. The term $(x)\tau^{m+1}$ is obtained from $(x)\tau^m$ by application of τ, so the size of $(x)\tau^{m+1}$ is at least the size of $(x)\tau^m$. Hence, there is a natural number $M(x)$ such that for $m \geq M(x)$, all terms $(x)\tau^m$ have the same size. Then Property 3 of τ implies $(x)\tau^{m+1} \equiv (x)\tau^m$ for $m \geq M(x)$. □

The 'limit' $\bar{\tau}$ of τ is defined by

$$(x)\bar{\tau} \equiv (x)\tau^{M(x)}.$$

Property 4 implies that $\tau\bar{\tau} \equiv \bar{\tau}$. So, since τ is the union of all τ_n, $\tau_n\bar{\tau} \equiv \bar{\tau}$ for all n.

5. For each $e \in E$, there is a natural number $N(e)$ such that $E^e_{N(e)}$ contains only equations of the form $x = y$, where x and y are not in the domain of $\bar{\tau}$.

Proof. Fix an $e \in E$, and consider the sequence $\{(E^e_n)\bar{\tau}\}_{n=0}^{\infty}$.

Each equation in E^e_{n-1} is either maintained, or replaced by proper sub-equations in F^e_n. Hence, each equation in $(E^e_{n-1})\bar{\tau}$ is either maintained, or replaced by proper sub-equations in $(F^e_n)\bar{\tau} = (F^e_n)\tau_n\bar{\tau} = (E^e_n)\bar{\tau}$. Since the total size of these proper sub-equations is smaller than the size of the original equation, if follows that there is some $N(e)$ such that all equations in $(E^e_{n-1})\bar{\tau}$ are maintained in $(E^e_n)\bar{\tau}$ for each $n > N(e)$.

Consider an equation $s = t$ in E^e_{n-1} for some $n > N(e)$. Since $(s = t)\bar{\tau} \in (E^e_{n-1})\bar{\tau}$ is maintained in $(E^e_n)\bar{\tau}$, $s = t \in E^e_{n-1}$ is maintained in F^e_n. So $s = t$ cannot have any proper sub-equations, or in other words, s or t must be a variable, say, $s \equiv x$.

Now suppose, towards a contradiction, that t is *not* a variable. First, we show that then $(x)\tau_n$ is not a variable. Distinguish two cases.

- $(x)\tau_{n-1} \not\equiv x$. Since τ_n and τ_{n-1} coincide on the domain of τ_{n-1}, we have $(x)\tau_n \equiv (x)\tau_{n-1} \not\equiv x$. Then Property 3 yields that $(x)\tau_n$ is not a variable.

- $(x)\tau_{n-1} \equiv x$. Then x is not in the domain of τ_{n-1}. Furthermore, $x = t \in F^e_n$ where t is not a variable. So from the construction of τ_n we see that $(x)\tau_n$ is not a variable.

The equation $x = t \in F^e_n$ takes the form $(x = t)\tau_n$ in E^e_n. Since $(x)\tau_n$ and $(t)\tau_n$ are not variables, this equation is replaced by proper sub-equations in F^e_{n+1}. But this contradicts the fact that equations in $(E^e_n)\bar{\tau}$ are maintained in $(E^e_{n+1})\bar{\tau}$. So apparently, t must be a variable.

Thus, each equation in E^e_{n-1} for $n > N(e)$ is of the form $x = y$. In E^e_n, such an equation takes the form $(x = y)\tau_n$, so $(x)\tau_n$ and $(y)\tau_n$ are variables too. Then Property 3 yields $(x)\tau_n \equiv x$ and $(y)\tau_n \equiv y$. Hence, x and y are not in the domain of τ_n for any $n > N(e)$, so they are not in the domain of their union τ. Then x and y are not in the domain of $\bar{\tau}$. □

The 'limit' $\bar{E}$ of E is defined by

$$\bar{E} \;=\; \bigcup_{e \in E} E^e_{N(e)}.$$

Construct a unifier ρ for $\bar{E}$ as follows. Two variables are said to be 'equivalent' if they can be equated by equations in $\bar{E}$. We define ρ to contract the elements of each equivalence class C to one variable in this class. That is, just pick some $x_0 \in C$, and put $(x)\rho \equiv x_0$ for $x \in C$.

Finally, we define the desired most general unifier Θ for E:

$$\Theta \equiv \bar{\tau}\rho.$$

6. Θ is a unifier for E.

Proof. Since $\tau_n\bar{\tau} \equiv \bar{\tau}$, also $\tau_n\Theta \equiv \tau_n\bar{\tau}\rho \equiv \bar{\tau}\rho \equiv \Theta$. So Θ unifies τ_n for all n.

Consider an equation $x = y \in \bar{E}$. Since x and y can be equated in $\bar{E}$, by definition ρ maps x and y to the same variable. Property 5 ensures that x and y are not in the domain of $\bar{\tau}$, so

$$(x)\Theta \;\equiv\; (x)\bar{\tau}\rho \;\equiv\; (x)\rho \;\equiv\; (y)\rho \;\equiv\; (y)\bar{\tau}\rho \;\equiv\; (y)\Theta.$$

Hence, Θ unifies $\bar{E}$.

Since Θ unifies all τ_n and $\bar{E}$, in particular it unifies $\tau_{N(e)}$ and $E^e_{N(e)}$ for each $e \in E$. Then Property 2 yields that Θ unifies $E^e_0 = \{e\}$, for each $e \in E$. □

7. Θ is most general.

Proof. Let σ unify E. Then according to Property 1, σ unifies τ_n and E^e_n for all natural numbers n and $e \in E$.

σ unifies all τ_n, so it unifies their union τ. Since $(x)\bar{\tau} \equiv (x)\tau^{M(x)}$ for each x, σ unifies $\bar{\tau}$.

By definition of ρ, $(x)\rho$ and x can be equated in $\bar{E}$ for each x, that is, there exists a deduction $(x)\rho = y_1 = \cdots = y_k = x$ in $\bar{E}$. Since σ unifies all $E^e_{N(e)}$, it unifies their union $\bar{E}$. Hence, $(x)\rho\sigma \equiv (y_1)\sigma \equiv \cdots \equiv (y_k)\sigma \equiv (x)\sigma$. So σ unifies ρ.

Hence, $\Theta\sigma \equiv \bar{\tau}\rho\sigma \equiv \bar{\tau}\sigma \equiv \sigma$. □

This finishes the proof of Theorem 3. ■

4 Examples

Example 4 Assume distinct function symbols $f_0, f_1, f_2, ...$ of arity one and distinct variables $x_0, x_1, x_2, ...$ The technique employed in the proof of Theorem 3 produces a most general unifier for the infinite unifiable set of equations $\{x_i = f_{i-1}(x_{i-1}) \mid i = 1, 2, ...\}$ as follows.

First, we obtain $(x_0)\tau_1 \equiv x_0$ and $(x_i)\tau_1 \equiv f_{i-1}(x_{i-1})$ for $i = 1, 2, ...$ The union τ of all the τ_n is already determined at this point; it equals τ_1. Hence, the limit $\bar{\tau}$ of τ is defined by $(x_i)\bar{\tau} \equiv f_{i-1} \cdots f_0(x_0)$ for $i = 0, 1, 2, ...$

It is not difficult to find that the sequences $\{E_n^{x_i = f_{i-1}(x_{i-1})}\}_{n=0}^{\infty}$ for $i = 1, 2, ...$ all converge to $x_0 = x_0$. Hence, the union $\bar{E}$ of the limit sets of these sequences is $\{x_0 = x_0\}$. So the substitution ρ which contracts variables that can be equated in $\bar{E}$ is simply the identity. Thus, the most general unifier $\Theta \equiv \bar{\tau}\rho$ equals $\bar{\tau}$.

Example 5 Assume a function symbol f of arity one. We study how the procedure employed in the proof of Theorem 3 acts on the non-unifiable equation $x = f(x)$.

Starting from the identity substitution τ_0 and $E_0 = \{x = f(x)\}$, and performing the consecutive steps of the procedure, we obtain

$$\begin{array}{ll} F_n = \{x = f(x)\} & n = 0, 1, 2, ... \\ (x)\tau_n \equiv f(x) & n = 1, 2, ... \\ E_n = \{f(x) = f(f(x))\} & n = 1, 2, ... \end{array}$$

For the union τ of all the τ_n we have $(x)\tau \equiv f(x)$.

The construction of a most general unifier for $x = f(x)$ from τ and the E_n breaks down at Property 4, for which apparently it is essential that the original set of equations is unifiable. That is, for the τ in this example there does not exist a natural number M such that $(x)\tau^{M+1} \equiv (x)\tau^M$, so we cannot construct its limit $\bar{\tau}$.

5 Related and Future Work

The unification result in this paper is incomparable with unification results for infinite sets of equations based on lattices [9, 5] where substitutions have a finite domain. In [5] an artificial top element ∞ is added to the collection of idempotent substitutions, in order to obtain a complete lattice, and each set of equations between finite terms which cannot be unified by a substitution (with finite support) is awarded the same most general unifier, ∞. For example, the infinite set $\{x_i = x_{i+1} \mid i = 0, 1, 2, ...\}$ is in that setting unified by ∞, while in this paper it is unified by any substitution σ_n for $n = 0, 1, 2, ...$, with $(x_i)\sigma_n \equiv x_n$ for $i = 0, 1, 2, ...$

Berarducci and Venturini Zilli [3] compare several variants of unification for finite sets of equations, between finite terms as well as between infinite terms (see e.g. [4]). Also, they study unification on the basis of substitutions with finite as well as with infinite domains. In [3] the notion of a stable substitution is introduced; a substitution σ is stable if, for each variable x, the sequence $\{(x)\sigma^i \mid i = 0, 1, 2, ...\}$ either contains a non-variable, or converges to a unique variable. In this paper, enforcing stableness made a key step in building the desired most general unifier; stableness was obtained by the introduction of substitution ρ.

Jonkers [11] studies a many-sorted algebra, called Description Algebra, where terms are built from variables, constants, and n-tuples $\langle t_1, ..., t_n \rangle$. Jonker proves [11, Theorem 2.4.7] that each countable unifiable set of equations between terms over this signature allows a most general unifier. The proof depends in a crucial way on the countability of the set of equations: there exist most general unifiers for each finite subset of a set of equations, and the 'limit' of these substitutions constitutes a most general unifier for the full set of equations. Although the setting in this paper is single-sorted, the proof technique employed here can be generalized to many-sortedness without any complication, to capture the unification result in [11].

A unification problem of a countably infinite set of equations between finite terms can be rephrased into a unification problem of an equation between infinite terms. The aim of the first problem would be to find a unifier which maps variables to finite terms, while the aim of the second problem would be to find a unifier which maps variables to infinite terms. For future research, it would be interesting to try and transfer the result in this paper to the case of infinite terms, that is, to obtain that each set of equations between infinite terms which has a unifier (mapping variables to infinite terms), allows a most general unifier; see also [10, 14].

References

[1] K.R. Apt, *From Logic Programming to Prolog*, Prentice Hall, 1996.

[2] F. Baader and J.H. Siekmann, Unification theory, in: D.M. Gabbay, C.J. Hogger, and J.A. Robinson, eds., *Handbook of Logic in Artificial Intelligence and Logic Programming, Volume 2: Deduction Methodologies*, pp. 41–125, Oxford University Press, 1994.

[3] A. Berarducci and M. Venturini Zilli, Generalizations of unification, *Journal of Symbolic Computation*, **16**(5):479–492, 1993.

[4] B. Courcelle, Fundamental properties of infinite terms, *Theoretical Computer Science*, **25**:95–169, 1983.

[5] E. Eder, Properties of substitutions and unifications, *Journal of Symbolic Computation*, **1**(1):31–46, 1985.

[6] W.J. Fokkink and R.J. van Glabbeek, Ntyft/ntyxt rules reduce to ntree rules, *Information and Computation*, **126**(1):1–10, 1996.

[7] J. van Heijenoort, ed., *Jacques Herbrand: Écrits Logiques*, Presses Universitaires de France, 1968. English translation: W.D. Goldfarb, ed., *Jacques Herbrand: Logical Writings*, Reidel, 1971.

[8] J. Herbrand, *Recherches sur la Théorie de la Démonstration*, PhD thesis, University of Paris, 1930.

[9] G. Huet, *Résolution d'Équations dans des Langages d'Ordre 1,2,...,ω*, PhD thesis, University of Paris VII, 1976.

[10] J. Jaffar, Efficient unification over infinite terms, *New Generation Computing*, **2**(3):207–219, 1984.

[11] H.B.M. Jonkers, Description algebra, in *Proceedings METEOR Workshop on Algebraic Methods: Theory, Tools and Applications*, Passau, M. Wirsing and J.A. Bergstra, eds., LNCS 394, pages 283–305, Springer-Verlag, 1987.

[12] A. Martelli and U. Montanari, Unification in linear time and space: a structured presentation, Internal Report B76-16, Instituto di Elaborazione delle Informazione, Consiglio Nazionale delle Ricerche, Pisa, Italy, July 1976.

[13] A. Martelli and U. Montanari, An efficient unification algorithm, *ACM Transactions on Programming Languages and Systems*, **4**(2):258–282, 1982.

[14] A. Martelli and G. Rossi, Efficient unification with infinite terms in logic programming, *Proceedings Conference on Fifth Generation Computer Systems (FGCS'84)*, Tokyo, pages 202–209, North-Holland, 1984.

[15] M. Paterson and M. Wegman, Linear unification, *Journal of Computer and System Sciences*, **16**(2):158–167, 1978.

[16] D. Prawitz, An improved proof procedure, *Theoria*, **26**:102–139, 1960.

[17] J.A. Robinson, A machine-oriented logic based on the resolution principle, *Journal of the ACM*, **12**(1):23–41, 1965.