A1-Unification

Alwen Fernanto Tiu

February 1, 2001

1 Introduction

The unification problem over the associative equational theory

$$A = \{f(x, f(y, z)) = f(f(x, y), z)\}$$

had long been a difficult open problem until it was solved by Makanin [Makanin77]. In this paper, we will consider a slight extension of the associative theory by adding a unit element, i.e., the theory

$$A1 = \{f(x, f(y, z)) = f(f(x, y), z),\ f(x, e) = x,\ f(e, x) = x\}.$$

As we will see later, the algorithms (i.e., the decision procedure and the algorithm for generating a complete set of unifiers) for A-unification can be extended modularly to the algorithms for $A1$-unification.

The idea for this extension was first mentioned in [Makanin77], that is by reducing the $A1$-unfication problem to several subproblems in A-theory (see section 3). Since then, as far as the author knows, no publications were made concerning the decidability of $A1$-unification problem (see for example a recent survey paper by Baader [Baader99]). Based on the idea proposed originally by Makanin, we will prove that $A1$-unification is decidable, and furthermore, an algorithm for generating the complete set of unifiers will be given.

2 Basic Notions

2.1 Syntactical Unification

Let F be a finite set of function symbols, called *signature*, and V be a countably infinite set of variables. The set of terms built over F and V is denoted by $T(F, V)$. Elements of V will be denoted by x, y, z, and elements of $T(F, V)$ by l, r, s, t, u, v. The set of variables occuring in a term t will be denoted by $\mathrm{Vars}(t)$, and this will be extended to sets of variables, equations, and sets of equations.

A *substitution* is a mapping from variables to terms which is almost everywhere equal to identity, and will generally be represented by σ, θ, η, or ρ. The identity substitution is represented by Id. The application of a substitution σ to a term t, denoted $t\sigma$, is defined by induction on the structure of terms:

$$t\sigma = \begin{cases} x\sigma & \text{if } t = x, \\ f(t_1\sigma, ..., t_n\sigma) & \text{if } t = f(t_1, ..., t_n). \end{cases}$$

For a substitution σ, the *domain* is the set of variables

$$\mathrm{Dom}(\sigma) = \{x \mid x\sigma \neq x\},$$

and the *range* is the set of terms

$$\mathrm{Ran}(\sigma) = \bigcup \{x\sigma \mid x \in \mathrm{Dom}(\sigma)\},$$

and the set of variables occuring in the range is $\mathrm{VRan}(\sigma) = \mathrm{Vars}(\mathrm{Ran}(\sigma))$. A substitution will normally be represented by a set of bindings of variables in its domain, e.g. $\{x_1/s_1, ..., x_n/s_n\}$.

The *restriction* of a substitution θ to a set of variables X, denoted by $\theta_{|X}$, is the substitution which is equal to the identitiy everywhere except over $X \cap \mathrm{Dom}(\sigma)$, where it is equal to σ. *Composition* of two substitution is written $\sigma\theta$, and is defined by $t\sigma\theta = (t\sigma)\theta$. The composition $\sigma\theta$ can be constructed as follows:

- apply θ to every term in $\mathrm{Ran}(\sigma)$ to obtain σ_1 ;
- remove from θ any binding x/t, where $x \in Dom(\sigma)$, to obtain θ_1 ;
- remove from σ_1 any trivial binding x/x, to obtain σ_2;
- take the union of the two sets of bindings σ_2 and θ_1.

Two substitutions are equal, denoted $\sigma = \theta$, if $x\sigma = x\theta$ for every variable x. We say that σ is more general than θ, denoted $\sigma \preceq \theta$, if there exists an η such that $\theta = \sigma\eta$.

Definition 2.1 *A substitution σ is a* unifier *of two terms s and t if $s\sigma = t\sigma$; it is a* most general unifier *(*mgu*), if for every unifier θ of s and t, $\sigma \preceq \theta$. A* unification problem *for two terms s and t is represented by $s \doteq t$.*

2.2 Equational Unification

Equational unification is concerned with the problem of making terms equal modulo an equational theory E by applying a suitable substitution. An *equational theory* is defined by a set of identities E which is a subset of $T(F, V) \times T(F, V)$. We will write $s =_E t$ to denote that the term s is equal modulo E to the term t.

For a given set of identities E, we denote by $\mathrm{Sig}(E)$ the set of all function symbols occuring in E. We sometimes denote the equational theory with E_f where f is the function symbol being defined.

Definition 2.2 *Let E be an equational theory and F a signature containing* $\mathrm{Sig}(E)$*. An $E-$*unification problem *over F is a finite set of equations*

$$\Gamma = \{s_1 \doteq_E t_1, ..., s_n \doteq_E t_n\}.$$

An E-unifier is a substitution σ such that $s_1\sigma =_E t_1\sigma, ..., s_n\sigma =_E t_n\sigma$. The set of all E-unifiers of Γ is denoted by $\mathrm{U}_E(\Gamma)$, and Γ is E-unifiable iff $\mathrm{U}_E(\Gamma) \neq \emptyset$.

Definition 2.3 *Let E be an equational theory and X a set of variables. The substitution σ is* more general modulo E on X *than the substitution θ iff there exists a substitution λ such that $x\theta =_E x\sigma\lambda$ for all $x \in X$. In this case we write $\sigma \preceq_E^X \theta$ and say that θ is an E-instance of σ on X.*

When comparing E-unifiers of a problem Γ, the set X is the set of all variables occuring in Γ. Unlike the case of syntactic unification, unifiable E-unification problems need not have a most general E-unifier. For example, the unification problem $\Gamma = \{f(x,y) \doteq_C f(a,b)\}$ of the theory $C = \{f(x,y) \approx f(y,x)\}$ has two C-unifiers $\sigma_1 = \{x/a, y/b\}$ and $\sigma_2 = \{x/b, y/a\}$. On $\mathrm{Var}(\Gamma) = \{x,y\}$, any unifier of Γ is equal to either σ_1 or σ_2, and σ_1 and σ_2 are not comparable with respect to $\preceq_C^{\{x,y\}}$.

Definition 2.4 *Let Γ be an E-unification problem over F and let $X = \mathrm{Vars}(\Gamma)$ be the set of all variables occuring in Γ. A* complete set of E-unifiers *of Γ is a set CSU_E of substitutions such that*

- $\mathrm{CSU}_E \subseteq \mathrm{U}_E(\Gamma)$*, i.e., each element of CSU_E is an E-unifier of Γ,*
- *for each $\theta \in \mathrm{U}_E(\Gamma)$ there exists $\sigma \in \mathrm{CSU_E}$ such that $\sigma \preceq_E^X \theta$.*

The set CSU_E is a minimal complete set of E-unifiers *of Γ iff it is a complete set that satisfies*

- *two distinct elements of CSU_E are incomparable w.r.t. $\preceq_E^X$, i.e., for all $\sigma, \sigma' \in \mathrm{CSU}_E$, $\sigma \preceq_E^X \sigma'$ implies $\sigma = \sigma'$.*

The substitution σ is a most general E-unifier of Γ iff $\{\sigma\}$ is a (minimal) complete set of E-unifiers of Γ.

Definition 2.5 *Let E be an equational theory, and let Γ be an E-unification problem over F. The problem Γ has type unitary (finitary, infinitary) iff it has a minimal complete set of E-unifiers of cardinality 1 (finite cardinality, infinite cardinality). If Γ does not have a minimal complete set of E-unifiers, then it is of type zero. We abbreviate type unitary by 1, type finitary by ω, type infinitary by ∞, and type zero by 0, and order these types as follows: $1 < \omega < \infty < 0$. The unification type of E w.r.t. the signature F is the maximal type of an E-equational problem over F.*

The unification properties of an equational theory (like decidability, unification type, etc.) may depend on the set of function symbols involved in the unification problem. We therefore need to distinguish the following types of unification problem.

Definition 2.6 *Let E be an equational theory and Γ an E-unification problem over F.*

- Γ *is an* elementary *E-unification problem iff* $F = \mathrm{Sig}(E)$.
- Γ *is an E-unification problem* with constants *iff* $F \setminus \mathrm{Sig}(E)$ *is a set of constant symbols.*
- *In a* general *E-unification problem,* $F \setminus \mathrm{Sig}(E)$ *may contain arbitratry function symbols.*

In addition to the three types of unification problem above, we may want to impose certain constraints to the problem. The constraints are particularly necessary in solving the combination problem in unification theory [Baader91].

Definition 2.7 *An E-unification problem with* linear constant restrictions (lcr) *consists of an E-unification problem with constants, Γ, and a linear ordering $<$ on the variables and free constants occuring in Γ. A substitution σ is an E-unifier of $(\Gamma, <)$ iff it is an E-unifier of Γ that satisfies: $x < c$ implies c does not occur in $x\sigma$ for all variables x and free constants c in Γ.*

3 Decidability of A1-Unification Problem

In this section, we are going to see how we can extend the existing decision procedure for the A-unification problems to that of the $A1$-unification problems. The A-unification problem with constants has been known to be decidable, as it was first shown in [Makanin77]. Later on, using the combination technique for disjoint equational theories, Baader and Schulz generalised Makanin's decision procedure to solve the general A-unification problem [Baader91].

The idea of extending the decision procedure of A-unification to the decision procedure for $A1$-unification was first mentioned in [Makanin77]. The basic idea is to reduce a given $A1$-unification problem Γ to several subproblems in A-unification by guessing in advance the variables to be instantiated with the unit element. The unit elements produced can then be removed (with one exception for the case where the term is equal modulo $A1$ to e), and thus we obtain a set of A-unification problems. We will give a formal treatment of this reduction, and show that it preserves solvability, and hence the decidability of $A1$-unification.

We restrict ourselves to the $A1$-unification problem with constants and the $A1$-unification with linear constant restriction. The general case can be reduced to the problem with linear constant restriction by using the combination technique for disjoint equational theories [Baader91].

Since we are dealing with associativity, it is convenient to represent each term $t \in T(\{f, e\} \cup C, V)$ in the form $f(s_1, f(...f(s_{n-1}, s_n)...))$.

Definition 3.1 *A term* $t \in T(\{f, e\} \cup C, V)$ *is said to be in* normal form *iff* $t = e$ *or* $t = f(s_1, f(\ldots, f(s_{n-1}, s_n)\ldots))$ *and* $s_i \in V \cup C$. *A substitution is in normal form iff every* $t \in \mathrm{Ran}(\sigma)$ *is in normal form. Similarly, a unification problem* Γ *is in the normal form iff for every equation* $s \doteq t \in \Gamma$, s *and* t *are in normal forms. We denote by* norm(t) *the normal form of* t, $\mathrm{norm}(\sigma)$ *the normal form of* σ *and* $\mathrm{norm}(\Gamma)$ *the normal form of* Γ.

It is obvious that any term $t \in T(\{f, e\} \cup C, V)$ can be rewritten to a normal form, and this normal form is unique, i.e., if $s =_{A1} t$ then $\mathrm{norm}(s) = \mathrm{norm}(t)$. In the normal form, an $A1$-term that is not the unit can also be seen as an A-term. This fact is stated in the following proposition.

Proposition 3.1 $s =_{A1} t$ *iff* $s =_A t$ *for all* $s, t \in T(\{f\} \cup C, V)$, *where* C *is the set of free constants and* V *is the set of variables.*

We now define the reduction of a given $A1$-unification problem Γ to the unification problems in A as follows:

$$r(\Gamma) = \{\mathrm{norm}(\Gamma\sigma) \mid \mathrm{Dom}(\sigma) \subseteq \mathrm{Vars}(\Gamma) \text{ and } \mathrm{Ran}(\sigma) = \{\mathrm{e}\}\}.$$

We call an element of $r(\Gamma)$ a *reduct* of Γ and the substitution σ where $\mathrm{Ran}(\sigma) = \{\mathrm{e}\}$ an *erasing substitution*. Note that the only equations in $\mathrm{norm}(\Gamma\sigma)$ that contain the unit element e are the equations of the forms $s \doteq e$ or $e \doteq t$. The unification problem $\mathrm{norm}(\Gamma\sigma)$ can then be seen as an A-unification problem with constants where the unit element e is treated as a free constant.

Lemma 3.1 *A given* $A1$*-unification problem with constants* Γ *is solvable iff there exists a reduct* $\Gamma' \in r(\Gamma)$ *that is solvable in* A*-theory.*

Proof:

Let $\Gamma = \{s \doteq_{A1} t\}$ be our $A1$-unification problem. We consider here only the unification problem with single equation since multipe equations can be dealed with the trick of adding new constant symbols as delimiter, e.g., $\{f(s_1, f(a, s_2)) \doteq_{A1} f(t_1, f(a, t_2))\}$ to represent $\{s_1 \doteq_{A1} t_1,\ s_2 \doteq_{A1} t_2\}$. Without loss of generality, we also assume that Γ is in normal form, and that $s \neq_{A1} t$. By definition, the set of reducts of Γ may contain the unit element e. We will treat this unit element as a free constant when we are working in A-theory.

$\Rightarrow$: *If* Γ *is solvable then there exists* $\Gamma' \in r(\Gamma)$ *that is solvable in* A*-theory.*

Suppose that σ is a solution for Γ. There are two cases to consider:

- $x\sigma \neq_{A1} e$, for all $x \in \mathrm{Dom}(\sigma)$.
  Since the normal form of σ is also a solution for Γ, we have

  $$s\,\mathrm{norm}(\sigma) =_{A1} t\,\mathrm{norm}(\sigma).$$

  Take the reduct $\Gamma' = \{s \doteq_A t\}$. If $s = e$ then by the uniqueness of normal form $t = e$. In this case, we take the identity substitution Id as a solution. If $s \neq e \neq t$, then by Proposition 3.1, we have

  $$s\,\mathrm{norm}(\sigma) =_A t\,\mathrm{norm}(\sigma)$$

which means that $\mathrm{norm}(\sigma)$ is a solution for Γ'.

- $x_1\sigma =_{A1} e, \ldots, x_n\sigma =_{A1} e$ where $\{x_1, \ldots, x_n\} \subseteq \mathrm{Dom}(\sigma)$, and $x\sigma \neq_{A1} e$, for all $x \in \mathrm{Dom}(\sigma) \setminus \{x_1, \ldots, x_n\}$.
  Take the normal form of σ, i.e., $\sigma' = n(\sigma)$, and decompose it into $\sigma' = \sigma_1\sigma_2$ where $\sigma_1 = \{x_1/e, \ldots, x_n/e\}$. By the definition of composition of substitution, $s(\sigma_1\sigma_2) = (s\sigma_1)\sigma_2$ and $t(\sigma_1\sigma_2) = (t\sigma_1)\sigma_2$, hence

  $$(s\sigma_1)\sigma_2 =_{A1} \mathrm{norm}(s\sigma_1)\sigma_2 =_{A1} \mathrm{norm}(t\sigma_1)\sigma_2 =_{A1} (t\sigma_1)\sigma_2.$$

  Take
  $$\Gamma' = \{\mathrm{norm}(s\sigma_1) \doteq_A \mathrm{norm}(t\sigma_1)\} = \{e \doteq_A e\}.$$

  If $\mathrm{norm}(s\sigma_1) = \mathrm{norm}(t\sigma_1) = e$, then the identitiy substitution Id is a possible solution. If $\mathrm{norm}(s\sigma_1) \neq e \neq \mathrm{norm}(t\sigma_1)$, since $\mathrm{norm}(s\sigma_1)$, $\mathrm{norm}(t\sigma_1)$ and σ_2 contains no unit element e, we can apply Proposition 3.1 and get

  $$\mathrm{norm}(s\sigma_1)\sigma_2 =_A \mathrm{norm}(t\sigma_1)\sigma_2$$

  which means that σ_2 is an A-unifier of Γ'.

$\Leftarrow$: *If there exists $\Gamma' \in r(\Gamma)$ that is solvable in A-theory, then Γ is solvable.*
Suppose that $\Gamma' = \{\mathrm{norm}(s\sigma) \doteq_A \mathrm{norm}(t\sigma)\}$ and suppose θ is a solution for Γ'.

- $\mathrm{norm}(s\sigma) = e$ and $\mathrm{norm}(t\sigma) = e$, then θ must be an instance of Id, and $\sigma\theta$ is a solution for Γ.

- $\mathrm{norm}(s\sigma) \neq e$ and $\mathrm{norm}(t\sigma) = e$, or $\mathrm{norm}(s\sigma) = e$ and $\mathrm{norm}(t\sigma) \neq e$, this case is possible only if $\mathrm{norm}(s\sigma) = x$ (or $\mathrm{norm}(t\sigma) = x$ for the other case), for some variable $x \in \mathrm{Vars}(\Gamma)$. Then θ must be an A- instance of $\{x/e\}$, and any $A1$-instance of $\sigma\{x/e\}$ is a solution, including $\sigma\theta$.

- $\mathrm{norm}(s\sigma) \neq e$ and $\mathrm{norm}(t\sigma) \neq e$.
  By Proposition 3.1 θ is also a solution for $\{\mathrm{norm}(s\sigma) \doteq_{A1} \mathrm{norm}(t\sigma)\}$. Since $\mathrm{norm}(s\sigma) =_{A1} s\sigma$ and $\mathrm{norm}(t\sigma) =_{A1} t\sigma$, we have $(s\sigma)\theta =_{A1} (t\sigma)\theta$, and by definition of composition of substitution: $s(\sigma\theta) =_{A1} t(\sigma\theta)$. Then, it is obvious that $\sigma\theta$ is a solution for Γ. □

Lemma 3.1, together with the decidability of A-unification problem with constants, trivially entails the decidability of $A1$-unification with constants.

Theorem 3.1 *The $A1$-unification problem with constants is decidable.*

The $A1$-unification problem with linear constant restriction was shown to be decidable in [Baader91] by a slight modification of Makanin's decision procedure.

Theorem 3.2 *The $A1$-unification problem with linear constant restriction is decidable.*

Proof:

We apply the same reduction as in Lemma 3.1. Since the linear restriction in a given unification problem involves only free constants, this reduction does not alter the restriction. And since any solution for the problem with linear restriction is also a solution for the problem without the restriction, the reduction still preserves the solvability of the original $A1$-unification problem. $\square$

We now consider the problem of computing the complete set of unifiers of the $A1$-unification problem. In [Plotkin72], a simple algorithm was given to compute the minimal complete set of unifiers of the A-unification problem. By using the reduction in the proof of Lemma, we can obtain the complete set of unifiers for a given $A1$-unification problem, if it exists, by composing the solutions for its reducts with their corresponding erasing substitutions.

Theorem 3.3 *Let Γ be an $A1$-unification problem with constants (with or without linear constant restriction), and let*

$$r(\Gamma) = \{norm(\Gamma\sigma_i) \mid norm(\Gamma\sigma_i) \neq e,\, \sigma_i \in S\}$$

be the set of reducts of Γ, where $S = \{\sigma \mid Dom(\sigma) \subseteq Vars(\Gamma),\, Ran(\sigma) = \{e\}\}$ is the set of all erasing substitution correspond to Γ. Let M_i be the minimal complete set of A-unifiers for $norm(\Gamma\sigma_i)$, then

$$R = \{\sigma_i\theta \mid \sigma_i \in S,\, \theta \in M_i\}$$

is a complete set of $A1$-unifiers of Γ.

Proof:

We only have to show that no solution is lost in the reduction. Suppose that there exists an $A1$-unifier γ that is not an instance of any unifier in R. From Lemma 3.1, we know that γ corresponds to at least one unifier γ' of some reduct $\Gamma\sigma_i$. The unifier γ' must be an instance of a more general unifier $\theta \in M_i$, i.e., $\gamma' =_A \theta\eta$. Thus, we have $\gamma =_{A1} \sigma_i\gamma' =_{A1} \sigma_i\theta\eta$. But this would mean that γ is an instance of some unifier in R, a contradiction. $\square$

The set of unifiers obtained this way is complete, but not necessarily minimal. For example, consider the equation

$$\Gamma = \{f(x,a) \doteq_{A1} f(y, f(z,a))\}$$

and two of its reducts $\Gamma_0 = \{f(x,a) \doteq_A f(y, f(z,a))\}$, $\Gamma_1 = \{f(x,a) \doteq_A f(y,a)\}$ with $\sigma_0 = Id$ and $\sigma_1 = \{z/e\}$. Two of the minimal solutions for Γ_0 and Γ_1 are $\theta_0 = \{x/f(y,z)\}$ and $\theta_1 = \{x/y\}$ respectively. Composing them with σ_0 and σ_1, we obtain two solutions for Γ: $\theta_0' = \{x/f(y,z)\}$ and $\theta_1' = \{x/y,\, z/e\}$. We can see that θ_1' is an instance of θ_0' , i.e., $x'\theta_1' =_{A1} x'\theta_0'\{z/e\}$, for all $x' \in \mathrm{Vars}(\Gamma)$.

4 Conclusion

We have proved that $A1$-unification problem with constant, and its variant with the linear constant restriction are decidable. The decision procedure extends those of the A-unification in a modular way, i.e., the extension is independent of how the A-unification problem is solved. The general $A1$-unification can be reduced to the $A1$-unification problem with linear constant restriction by using the combination technique described in [Baader91].

The complete set of $A1$-unifiers for a given $A1$-unification problem can be generated from the set of unifiers of the reducts. This set is complete, but not necessarily minimal as shown in our example in the end of Section 3.

References

[Baader99] F. Baader, W. Snyder (1999), "Unification Theory", Chapter 1, Handbook of Automated Reasoning, ed. Alan Robinson and Andrei Voronkov, Elsevier Science Publishers, B.V. 1999.

[Baader91] F. Baader, K.U.Schulz (1991), "General A- and AX-Unification via Optimized Combination Procedures," Proceedings of the Second International Workshop on Word Equations and Related Topics, Rouen 1991.

[Makanin77] G.S. Makanin (1977), "The Problem of Solvability of Equations in A Free Semigroup", Math. Sbornik 103, 147-236. English Translation of Math. USSR Sbornik 32, 1977.

[Plotkin72] G. Plotkin (1972), "Building in Equational Theories," Machine Intelligence, 7, 73-90.

[Schulz93] K.U. Schulz (1993), "Word Unification and Transformation of Generalized Equations", Journal of Automated Reasoning 11, 149-184.