UNIFICATION PROBLEM IN EQUATIONAL THEORIES

S. L. Kryvyi

The unification problem arose in connection with automated theorem proving in formal logic calculi, and in particular in first-order predicate logic. The first studies of the unification problem are associated with the names of Post (1920) and Herbrand (1930). In these studies, the unification problem arises as a particular issue of theorem proving in predicate calculus. It is only in 1965, however, that Robinson [1] restated the unification problem, proposed a unification algorithm in the absolute free algebra of terms, proved some properties of this algorithm, and developed a fairly powerful theorem proving method that essentially relies on the unification algorithm (it has since become known as the resolution method).

Robinson's work has given an initial impetus to an active study of theorem proving and in particular the unification problem. Soon after that unification methods began to appear for associative algebras (A-unification), commutative algebras (C-unification), associative-commutative algebras (AC-unification), associative-idempotent algebras (AI-unification), associative-commutative-idempotent algebras (ACI-unification), distributive algebras (D-unification), associative-distributive algebras (AD-unification), and so on (see surveys [62, 63]).

Studies of the unification problem in these algebras have revealed new properties of both classical and nonclassical algebras, because informally the unification problem involves solving equations in these algebras. Indeed, unifying two terms $s$ and $t$ in a given equational theory involves finding a substitution of the terms $t_i$ for the variables $x_i$, $\sigma = \{x_1 \rightarrow t_1, \ldots, x_k \rightarrow t_k\}$, such that its application to the terms $s$ and $t$ produces identical terms, i.e., $\sigma(s) = \sigma(t)$ in the sense of the identity laws of the given theory. Thus, the substitution $\sigma$ may be regarded as a solution of the equation $s = t$ in the given theory.

Recently, and especially in the last decade, the unification problem, and the matching problem as its particular case, are beginning to play a major role in logic and functional programming, automated theorem proving, program analysis and verification, deductive databases, and other areas.

This article considers the unification problem in classical universal algebras without attempting to cover all areas of unification and, in particular, unification problems in many-sorted algebras. The objective of this study is to familiarize the reader with the issues and methods of solving the unification problem in various equational theories and with some associated topics that arise in connection with the solution of the unification problem in these algebras.

1. STANDARD NOTATION

Let $\Omega$ be a signature of function symbols of fixed arity, $V$ a countable set of variables. The set of $\Omega$-terms over the alphabet $V$ is denoted $T(\Omega, V)$. Let $E$ be the set of identity relationships on the set $T(\Omega, V)$ that defines the equational theory $E$, i.e., specifies a congruence relation on the set of terms $T(\Omega, V)$.

The set $E$ is called a representation of the theory $E$. The factor-algebra $T(\Omega, V)/E$ is an $E$-free algebra with the generators $V$.

Let $t \in T(\Omega, V)$. Then $\text{Var}(t) = \{x \in V | x$ is a variable of the term $t\}$, and if $\text{Var}(t) = \emptyset$, the term $t$ is called a ground term.

Example 1. Let $\Omega$ be the signature consisting of a single binary function symbol $f$. The set of identities $A = \{f(x, f(y, z)) = f(f(x, y), z)\}$ defines the semigroup theory. Clearly, the $=A$-classes may be regarded as words on the alphabet $V$, and the $A$-free algebra $T(\Omega, V)/=A$ is isomorphic to the free semigroup $F(V)$.

End of example.


1060-0396/97/3306-0874$18.00 ©1998 Plenum Publishing Corporation
A substitution is a mapping \( \theta : V \rightarrow T(\Omega, V) \) such that \( \theta(x) \neq x \) only for finitely many elements \( x \) from \( V \). Since \( T(\Omega, V) \) is a free \( \Omega \)-algebra with the generators \( V \), the mapping \( \theta \) is uniquely continuatable to a homomorphism (endomorphism) \( \theta : T(\Omega, V) \rightarrow T(\Omega, V) \) so that \( \theta(\theta(x_1), \ldots, \theta(x_n)) = \theta(\theta(x_1), \ldots, \theta(x_n)) \).

Given this definition, a substitution is representable in the form \( \theta : \{x_1 \rightarrow t_1, \ldots, x_k \rightarrow t_k\} \). With each substitution \( \theta = \{x_1 \rightarrow t_1, \ldots, x_k \rightarrow t_k\} \) are associated the following sets:

- **\( \text{DOM}(\theta) = \{x \in V \mid \theta(x) \neq x\} = \{x_1, \ldots, x_k\} \)**
- **\( \text{COD} = \{\theta(x) \mid x \in \text{DOM}(\theta)\} = \{t_1, \ldots, t_k\} \)**
- **\( \text{VCOD} = V(\text{COD}(\theta)) = \{x_i | x_i \text{ are variables entering } t_i, i = 1, 2, \ldots, k\} \)**
- **\( \text{CCOD}(\theta) = C(\text{COD}(\theta)) = \{c_{ij} | c_{ij} \text{ are constants entering } t_i, i = 1, 2, \ldots, k\} \)**

If \( \text{VCOD}(\theta) = \emptyset \), then \( \theta \) is called a ground substitution.

The product \( \sigma \tau \) of two substitutions \( \sigma \) and \( \tau \) is the composition (superposition) of two mappings, i.e., \( (\sigma \tau)(t) = \tau(\sigma(t)) \).

The unification problem (equality problem) for a pair of terms \( s \) and \( t \) in a given \( E \)-theory involves finding a substitution \( \theta \) such that \( \theta(s) = \theta(t) \).

If such a substitution \( \theta \) exists, then it is called a \( E \)-unifier of the terms \( s \) and \( t \). The set of all \( E \)-unifiers of the terms \( s \) and \( t \) is denoted \( UE(s, t) \).

The matching problem is a particular case of the unification problem that often arises in applications. The matching problem is stated as follows: given the terms \( s, t \in T(\Omega, V) \), find a substitution \( \sigma \) such that \( \sigma(s) = t \). Here, the term \( s \) is the pattern, and the substitution \( \sigma \) is a matching. The matching problem is central to rule rewriting systems.

Note that both the unification problem and the matching problem imply the existence of yet another problem, a so-called identity problem in the equational theory. This is so because terms are compared apart from identities from the set \( E \).

**Example 2.** Let \( \Omega = \{f, a\} \), where \( f \) is a binary function symbol, \( a \) a constant (a 0-ary function symbol), and \( s = f(x, a), t = f(a, y) \) two terms from \( T(\Omega, V) \), where \( V = \{x, y\} \). Then:

- a) \( E = \emptyset \). In this case \( \theta = \{x \rightarrow a, y \rightarrow a\} \) is the unique \( \emptyset \)-unifier of \( s \) and \( t \);
- b) \( E = C = \{f(x, y) = f(y, x)\} \). Clearly, \( \theta \) is also a \( C \)-unifier for \( s \) and \( t \). But \( f \) is a commutative function symbol, and therefore another \( C \)-unifier exists: \( \sigma = \{x \rightarrow y\} \). Indeed, by commutativity, we have \( s = f(x, a) \) and \( t = f(a, y) = f(y, a) \).

Thus, \( \sigma = \{x \rightarrow y\} \) gives the identity \( \sigma(s) = f(y, a) = f(a, y) = \sigma(t) \). Note that these unifiers are dependent, because \( \theta = \sigma \{y \rightarrow a\} \), i.e., \( \theta \) is a particular case of \( \sigma \).

End of example.

Recall that for two given substitutions \( \sigma = \{x_1 \rightarrow t_1, \ldots, x_k \rightarrow x_k\} \) and \( \theta = \{y_1 \rightarrow q_1, \ldots, y_m \rightarrow t_m\} \), their product \( \sigma \theta((\sigma \theta(t)) = \theta(\sigma(t)) \) is obtained by the following rules:

- a) construct the set \( \{x_1 \rightarrow \theta(t_1), \ldots, x_k \rightarrow \theta(t_k); y_1 \rightarrow q_1, \ldots, y_m \rightarrow q_m\} \);
- b) from this set remove elements of the form \( y_j \rightarrow q_j \) if \( y_j \in \{x_1, \ldots, x_k\} \).

For instance, if \( \theta \) and \( \sigma \) are substitutions from the previous example, then \( \{x \rightarrow \theta(y), y \rightarrow a\} = \{x \rightarrow a, y \rightarrow a\} = \sigma \{y \rightarrow a\} \).

In most applications we do not need all \( E \)-unifiers; it suffices to have a complete set of \( E \)-unifiers. A complete set of \( E \)-unifiers is defined by the quasi-order \( \leq_E [W] \), where \( W \subseteq V \). This quasi-order is defined as follows: \( \forall x \in W \) and the substitutions \( \sigma \) and \( \theta \),