Deutsches
Forschungszentrum
für Künstliche
Intelligenz GmbH

Research
Report
RR-90-16

Adding Homomorphisms to Commutative/Monoidal Theories

or:

How Algebra Can Help in Equational Unification

Franz Baader Werner Nutt

December 1990

Deutsches Forschungszentrum für Künstliche Intelligenz
GmbH

Postfach 20 80
D-6750 Kaiserslautern, FRG
Tel.: (+49 631) 205-3211/13
Fax: (+49 631) 205-3210

Stuhlsatzenhausweg 3
D-6600 Saarbrücken 11, FRG
Tel.: (+49 681) 302-5252
Fax: (+49 681) 302-5341

Deutsches Forschungszentrum
für
Künstliche Intelligenz

The German Research Center for Artificial Intelligence (Deutsches Forschungszentrum für Künstliche Intelligenz, DFKI) with sites in Kaiserslautern und Saarbrücken is a non-profit organization which was founded in 1988 by the shareholder companies ADV/Orga, AEG, IBM, Insiders, Fraunhofer Gesellschaft, GMD, Krupp-Atlas, Mannesmann-Kienzle, Nixdorf, Philips and Siemens. Research projects conducted at the DFKI are funded by the German Ministry for Research and Technology, by the shareholder companies, or by other industrial contracts.

The DFKI conducts application-oriented basic research in the field of artificial intelligence and other related subfields of computer science. The overall goal is to construct *systems with technical knowledge and common sense* which - by using AI methods - implement a problem solution for a selected application area. Currently, there are the following research areas at the DFKI:

- ❑ Intelligent Engineering Systems
- ❑ Intelligent User Interfaces
- ❑ Intelligent Communication Networks
- ❑ Intelligent Cooperative Systems.

The DFKI strives at making its research results available to the scientific community. There exist many contacts to domestic and foreign research institutions, both in academy and industry. The DFKI hosts technology transfer workshops for shareholders and other interested groups in order to inform about the current state of research.

From its beginning, the DFKI has provided an attractive working environment for AI researchers from Germany and from all over the world. The goal is to have a staff of about 100 researchers at the end of the building-up phase.

Prof. Dr. Gerhard Barth
Director

Adding Homomorphisms to Commutative/Monoidal Theories, or: How Algebra Can Help in Equational Unification

Franz Baader, Werner Nutt

DFKI-RR-90-16

A short version of this paper will appear in the Proceedings of the 4th International Conference on Rewriting Techniques and Applications, Springer Verlag, 1991.

Adding Homomorphisms to Commutative/Monoidal Theories
or
How Algebra Can Help in Equational Unification

Franz Baader Werner Nutt
German Research Center for Artificial Intelligence (DFKI)
Postfach 2080, D-6750 Kaiserslautern, Germany
e-mail: {baader, nutt}@dfki.uni-kl.de

Abstract

Two approaches to equational unification can be distinguished. The syntactic approach relies heavily on the syntactic structure of the identities that define the equational theory. The semantic approach exploits the structure of the algebras that satisfy the theory. If little is known of the algebras involved, the first approach is useful, whereas the second is applicable to theories that describe algebraic structures which have already been investigated in mathematics.

With this paper we pursue the semantic approach to unification. We consider the class of theories for which solving unification problems is equivalent to solving systems of linear equations over a semiring. This class has been introduced by the authors independently of each other as commutative theories (Baader) and monoidal theories (Nutt). The class encompasses important examples like the theories of abelian monoids, idempotent abelian monoids, and abelian groups.

We identify a large subclass of commutative/monoidal theories that are of unification type zero by studying equations over the corresponding semiring. As a second result, we show with methods from linear algebra that unitary and finitary commutative/monoidal theories do not change their unification type when they are augmented by a finite monoid of homomorphisms, and how algorithms for the extended theory can be obtained from algorithms for the basic theory. The two results illustrate how using algebraic machinery can lead to general results and elegant proofs in unification theory.

Contents

1 Introduction

Equational unification is concerned with solving term equations modulo an equational theory. The theory is called *unitary* (*finitary*) if the solutions of an equation can always be represented by one (finitely many) "most general" solutions. Otherwise the theory is of type *infinitary* or *zero*. Equational theories which are of unification type unitary or finitary play an important rôle in automated theorem provers with built in theories [PL72, Ne74, Sl74, St85], in generalizations of the Knuth-Bendix algorithm [Hu80, PS81, JK86, Bm87], and in logic programming with equality [JL84, GR86].

For that reason, determining unification types of equational theories is not only interesting for unification theory but has also consequences for automated reasoning. Of course, for practical applications it is not enough to know that a given theory $\mathcal{E}$ is of type finitary.

One also needs a finite $\mathcal{E}$-unification algorithm which computes the finitely many most general solutions. Unfortunately, but not at all surprisingly, there cannot be a general method which determines the unification type of an equational theory [Nu89]; and even if a theory is finitary it is still not clear whether a unification algorithm exists.

Consequently, general methods which try to derive such an algorithm from a given set of axioms for the theory are doomed to fail. One solution proposed for this problem is to restrict the attention to certain classes of theories which are defined by syntactic properties of the set of axioms (see e.g., [KK90]). These efforts mostly depend on transformations of terms; they usually do not take the properties of the algebras defined by the theory into account. On the other hand, special purpose algorithms designed for theories of practical importance—such as the theory of abelian monoids (AM), idempotent abelian monoids (AIM), and abelian groups (AG)—often depend on algebraic properties of these theories.

The theories AM, AIM, and AG belong to the class of commutative theories—roughly speaking, theories where the finitely generated free algebras are direct products of the free algebras in one generator [Ba89a, Ba89b, Ba90]. It turns out (see Section 3 below) that the class of commutative theories is—modulo a translation of the signature—the same as the class of monoidal theories [Nu88, Nu90].

Unification in these theories can always be reduced to solving linear equations in certain semirings [Nu88]. On the one hand, this fact can be used to derive general results on unification in commutative/monoidal theories. For example, it can be shown that constant free unification problems are either unitary or of type zero, and the unification type of a theory can be characterized by algebraic properties of the corresponding semiring. These characterizations were used in [Nu88, Ba89b, Nu90] to determine the unification types of several commutative/monoidal theories. On the other hand, unification algorithms for certain commutative/monoidal theories—for example, the theory of abelian groups with n commuting homomorphisms—can be derived with the help of well-known algebraic methods for the corresponding semiring—for instance, Buchberger's algorithm for the ring $\mathbf{Z}[X_1, \ldots, X_n]$ of integer polynomials in n indeterminates [Ba90].

Let us now reconsider two of the examples in [Ba89b, Ba90]. Using algebraic properties of the semiring of polynomials with nonnegative integer coefficients, $\mathbf{N}[X]$, it was shown in [Ba90] that the corresponding theory, i.e., the theory of abelian monoids with a homomorphism, is of unification type zero. In contrast, the theory of abelian monoids with an involution[1] is unitary (finitary w.r.t. unification with constants). In both cases, the corresponding semiring has a specific structure: it is a monoid semiring $\mathcal{S}\langle H\rangle$, i.e., a semiring $\mathcal{S}$ with an adjoint monoid H. In the first example, the monoid H is the free monoid in one generator, which is an infinite monoid, while in the second example, we have the cyclic group of order two, which is finite. In both examples, the semiring $\mathcal{S}$ is the semiring $\mathbf{N}$ of all nonnegative integers. This semiring corresponds to the theory AM of all commutative monoids, which is a finitary commutative/monoidal theory.

In the present paper we shall consider commutative/monoidal theories where the corresponding semiring is a monoid semiring $\mathcal{S}\langle H\rangle$ more closely. The result for the theory of abelian monoids with a homomorphism can now be generalized to a whole class of theories as follows. If $\mathcal{S}$ is a *strict semiring*—i.e., a semiring which is not a ring—and H is a *free monoid* then the corresponding commutative/monoidal theory is of unification type zero. On the other hand, assume that $\mathcal{S}$ is a semiring such that unification in the corresponding commutative/monoidal theory is unitary (finitary w.r.t. unification with constants), and let H be a *finite monoid.* In that case, the theory corresponding to the semiring $\mathcal{S}\langle H\rangle$ is also of unification type unitary (finitary w.r.t. unification with constants). This generalizes the result for the theory of abelian monoids with an involution. Moreover, a finite unification algorithm for the theory corresponding to $\mathcal{S}$ can be used to derive a finite unification algorithm for the theory corresponding to $\mathcal{S}\langle H\rangle$. These two general results demonstrate the usefulness of the algebraic approach to unification. With this approach one can determine the unification types of whole classes of theories. It is not at all clear how this could be achieved with a purely syntactical approach.

The paper is organized as follows. After recalling some basic definitions concerning equational theories, unification theory, and semirings in Section 2, we shall introduce commutative theories and monoidal theories in Section 3. This section will also contain a proof of the equivalence between commutative and monoidal theories. In Section 4 we shall recall the algebraic characterizations of the unification types for these theories, and give some examples for the results which can be obtained using these characterizations. The next two sections con-

[1]An involution is a homomorphism h satisfying $h^2(x) = x$.

tain the exact formulations and the proofs of the two general results mentioned above. In the conclusion we shall state some interesting open problems in this area.

2 Basic Definitions

In the following we assume that the reader is familiar with the basic notions of universal algebra [Co65, Gr68]. For more information on unification theory see [Si89]. The notions from category theory used below are for instance defined in [Ba89a], or in any introductory textbook on categories. The composition of mappings is written from left to right, that is, $\phi \circ \psi$ or simply $\phi\psi$ means first ϕ and then ψ. Consequently, we use suffix notation for mappings (but not for function symbols in terms).

2.1 Equational Theories

We assume that two disjoint infinite sets of symbols are given, a set of function symbols and a set of variables. A *signature* Σ is a finite set of function symbols each of which is associated with its arity. Every signature Σ determines a class of Σ-*algebras* and Σ-*homomorphisms*. We define Σ-terms and Σ-substitutions as usual. By $[x_1/t_1, \ldots, x_n/t_n]$ we denote the substitution which replaces the variables x_i by the terms t_i.

An *equational theory* $\mathcal{E} = (\Sigma, E)$ is a pair consisting of a signature Σ and a set of identities E. The equality of Σ-terms induced by $\mathcal{E}$ will be denoted by $=_\mathcal{E}$. Every equational theory $\mathcal{E}$ determines a variety $\mathcal{V}(\mathcal{E})$, the class of all Σ-algebras satisfying each identity of E. For any set of generators X, the variety $\mathcal{V}(\mathcal{E})$ contains a free algebra over $\mathcal{V}(\mathcal{E})$ with generators X, which will be denoted by $\mathcal{F}_\mathcal{E}(X)$. Thus any mapping of X into a Σ-algebra A can be uniquely extended to a Σ-homomorphism of $\mathcal{F}_\mathcal{E}(X)$ into A.

The following category $\mathcal{C}(\mathcal{E})$ is associated with each equational theory $\mathcal{E} = (\Sigma, E)$: the objects of $\mathcal{C}(\mathcal{E})$ are the free algebras $\mathcal{F}_\mathcal{E}(X)$ for finite sets of variables X; the morphisms of $\mathcal{C}(\mathcal{E})$ are the Σ-homomorphisms between free algebras, and the composition of morphisms is the usual composition of mappings. The set of all objects of $\mathcal{C}(\mathcal{E})$ will be denoted by $\mathcal{F}(\mathcal{E})$, and the set of all morphisms from an object $\mathcal{F}_\mathcal{E}(X)$ to an object $\mathcal{F}_\mathcal{E}(Y)$ by $hom(\mathcal{F}_\mathcal{E}(X), \mathcal{F}_\mathcal{E}(Y))$. The coproduct of $\mathcal{F}_\mathcal{E}(X)$ and $\mathcal{F}_\mathcal{E}(Y)$ in $\mathcal{C}(\mathcal{E})$ is given by the free algebra $\mathcal{F}_\mathcal{E}(X \uplus Y)$, where $\uplus$ denotes disjoint union. If $|X| = |Y|$, then $\mathcal{F}_\mathcal{E}(X)$ and $\mathcal{F}_\mathcal{E}(Y)$ are isomorphic. Thus $\mathcal{F}_\mathcal{E}(X)$ is the coproduct of the isomorphic objects $\mathcal{F}_\mathcal{E}(x)$ for $x \in X$, where x is used as abbreviation for the singleton $\{x\}$.

2.2 Unification

Let $\mathcal{E} = (\Sigma, E)$ be an equational theory. An *$\mathcal{E}$-unification problem* is a finite sequence of equations $\Gamma = \langle s_i \doteq t_i \mid 1 \leq i \leq n \rangle$, where s_i and t_i are Σ-terms. A substitution θ is called an *$\mathcal{E}$-unifier* of Γ if $s_i\theta =_{\mathcal{E}} t_i\theta$ for each i. The set of all $\mathcal{E}$-unifiers of Γ is denoted by $U_{\mathcal{E}}(\Gamma)$. In general one does not need the set of all $\mathcal{E}$-unifiers. A complete set of $\mathcal{E}$-unifiers, i.e., a set of $\mathcal{E}$-unifiers from which all unifiers may be generated by $\mathcal{E}$-instantiation, is usually sufficient. More precisely, for every set of variables V we extend $=_{\mathcal{E}}$ to a relation $=_{\mathcal{E},V}$ between substitutions, and introduce the *$\mathcal{E}$-instantiation quasi-ordering* $\leq_{\mathcal{E},V}$ as follows:

- $\sigma =_{\mathcal{E},V} \theta$ iff $x\sigma =_{\mathcal{E}} x\theta$ for all $x \in V$
- $\sigma \leq_{\mathcal{E},V} \theta$ iff there exists a substitution λ such that $\theta =_{\mathcal{E},V} \sigma \circ \lambda$.

A set $C \subseteq U_{\mathcal{E}}(\Gamma)$ is a *complete set of $\mathcal{E}$-unifiers* of Γ if for every unifier θ of Γ there exists $\sigma \in C$ such that $\sigma \leq_{\mathcal{E},V} \theta$, where V is the set of variables occurring in Γ. For reasons of efficiency, this set should be as small as possible. Thus one is interested in *minimal* complete sets of $\mathcal{E}$-unifiers. In minimal complete sets two different elements are not comparable w.r.t. $\mathcal{E}$-instantiation.

The *unification type* of a theory $\mathcal{E}$ is defined with reference to the existence and cardinality of minimal complete sets. The theory $\mathcal{E}$ is *unitary* (*finitary*, *infinitary*, respectively) if minimal complete sets of $\mathcal{E}$-unifiers always exist, and their cardinality is at most one (always finite, at least once infinite, respectively). The theory $\mathcal{E}$ is of *unification type zero* if there exists an $\mathcal{E}$-unification problem without a minimal complete set of $\mathcal{E}$-unifiers.

If the terms in the unification problems may contain free constants, we talk about *unification with constants*, otherwise we talk about unification without constants. If nothing else is specified, "unification" will mean "unification without constants."

An $\mathcal{E}$-unification problem $\Gamma = \langle s_1 \doteq t_1, \ldots, s_n \doteq t_n \rangle$ can be reformulated as a problem for morphisms in the category $\mathcal{C}(\mathcal{E})$. Let Y be the finite set of variables occurring in some s_i or t_i. Evidently, we can consider s_i and t_i as elements of $\mathcal{F}_{\mathcal{E}}(Y)$. Since we do not distinguish between $=_{\mathcal{E}}$-equivalent unifiers, any $\mathcal{E}$-unifier can be regarded as a Σ-homomorphism from $\mathcal{F}_{\mathcal{E}}(Y)$ into $\mathcal{F}_{\mathcal{E}}(Z)$ for some finite set of variables Z. Let $X = \{x_1, \ldots, x_n\}$ be a set of cardinality n. We define Σ-homomorphisms $\sigma, \tau: \mathcal{F}_{\mathcal{E}}(X) \to \mathcal{F}_{\mathcal{E}}(Y)$ by $x_i\sigma := s_i$ and $x_i\tau := t_i$. Now, $\delta: \mathcal{F}_{\mathcal{E}}(Y) \to \mathcal{F}_{\mathcal{E}}(Z)$ is an $\mathcal{E}$-unifier of Γ if and only if $x_i\sigma\delta = s_i\delta = t_i\delta = x_i\tau\delta$ for all i, that is, if and only if $\sigma\delta = \tau\delta$. This observation justifies to conceive $\mathcal{E}$-unification as a problem involving only morphisms of the category $\mathcal{C}(\mathcal{E})$: given $\sigma, \tau: \mathcal{F}_{\mathcal{E}}(X) \to \mathcal{F}_{\mathcal{E}}(Y)$, find a $\delta: \mathcal{F}_{\mathcal{E}}(Y) \to \mathcal{F}_{\mathcal{E}}(Z)$ such that $\sigma\delta = \tau\delta$.

2.3 Semirings

A *semiring* $\mathcal{S}$ is a tuple $(\mathcal{S}, +, 0, \cdot, 1)$ such that $(\mathcal{S}, +, 0)$ is an abelian monoid, $(\mathcal{S}, \cdot, 1)$ is a monoid, and all q, r, $s \in \mathcal{S}$ satisfy the equalities

1. $(q + r) \cdot s = q \cdot s + r \cdot s$
2. $q \cdot (r + s) = q \cdot r + q \cdot s$
3. $0 \cdot s = s \cdot 0 = 0.$

The elements 0 and 1 are called *zero* and *unit*. Semirings are different from rings in that they need not be groups w.r.t. addition. Obviously, any ring is a semiring. A prominent example for a semiring which is not a ring is the semiring $\mathbf{N}$ of nonnegative integers.

Similar to the construction of polynomial rings over a given ring, one can use a semiring $\mathcal{S}$ and a monoid H to construct a new semiring, namely the *monoid semiring* $\mathcal{S}\langle H\rangle$. As for polynomials, the elements of the monoid semiring may be represented as sums of the form $\sum_{h\in H} s_h \cdot h$ where only finitely many of the coefficients $s_h \in \mathcal{S}$ are nonzero. The zero element of $\mathcal{S}\langle H\rangle$ is the sum where all the coefficients are zero, and the unit element is the sum where only the unit of H has a coefficient different from zero and this coefficient is the unit element of $\mathcal{S}$. Addition and multiplication in $\mathcal{S}\langle H\rangle$ are defined as follows:

$$\begin{aligned}
\sum_{h\in H} s_h \cdot h + \sum_{h\in H} t_h \cdot h &= \sum_{h\in H} (s_h + t_h) \cdot h \\
\sum_{f\in H} s_f \cdot f \cdot \sum_{g\in H} t_g \cdot g &= \sum_{h\in H} \Big(\sum_{h=fg} s_f \cdot t_g \Big) \cdot h
\end{aligned}$$

Polynomial semirings are special cases of monoid semirings. For example, the ring $\mathbf{Z}[X_1, \ldots, X_n]$ of integer polynomials in n indeterminates is the monoid semiring $\mathbf{Z}\langle FAM_n\rangle$ where FAM_n denotes the free abelian monoid in n generators.

As mentioned in the introduction, unification in commutative/monoidal theories can be reduced to solving systems of linear equations in certain semirings. Similar to unification in abelian monoids [LS75], problems without constants will correspond to systems of homogeneous equations. For problems with constants one has to solve in addition systems of inhomogeneous equations.

Modules over semirings are a generalization of vector spaces over fields. Since $(\mathcal{S}, \cdot, 1)$ need not be commutative, we have to distinguish between left and right $\mathcal{S}$-modules. Solutions of homogeneous systems form right $\mathcal{S}$-modules. The unification type of a theory will depend on whether these modules are finitely generated or not. A subset M of the n-fold cartesian product $\mathcal{S}^n$ is a *finitely generated* right $\mathcal{S}$-module if there exist finitely many $x_1, \ldots, x_k \in \mathcal{S}^n$ such that $M = \{x_1 s_1 + \cdots + x_k s_k \mid s_1, \ldots, s_k \in \mathcal{S}\}$.

Solutions of inhomogeneous systems do not form right modules, but unions cosets of right modules. For the unification type it will be crucial how many cosets are needed to represent all solutions. If $M \subseteq \mathcal{S}^n$ is a right $\mathcal{S}$-module, and

N is a subset of $\mathcal{S}^n$, then N is a *coset* of M if there exists some $y \in \mathcal{S}^n$ such that $N = \{y + x \mid x \in M\}$. Consequently, the set N is a *finite union of cosets* of M if there exist finitely many $y_1, \ldots, y_k \in \mathcal{S}^n$ such that $N = \bigcup_{i=1}^{k} \{y_i + x \mid x \in M\}$.

3 Commutative and Monoidal Theories

In this section we shall give the definitions of commutative and monoidal theories, and show in what sense these two notions are equivalent.

3.1 Definitions and Examples

Motivated by the categorical reformulation of $\mathcal{E}$-unification (see Subsection 2.2), the class of commutative theories is defined by properties of the category $\mathcal{C}(\mathcal{E})$ of finitely generated $\mathcal{E}$-free algebras as follows: an equational theory $\mathcal{E}$ is commutative if the corresponding category $\mathcal{C}(\mathcal{E})$ is semiadditive (see [HS73, Ba89a] for the definition and for properties of semiadditive categories). In order to give a more algebraic definition we need some additional notation from universal algebra.

Let $\mathcal{E} = (\Sigma, E)$ be an equational theory. A constant symbol e of the signature Σ is called *idempotent in* $\mathcal{E}$ if for all symbols $f \in \Sigma$ we have $f(e, \ldots, e) =_{\mathcal{E}} e$. Note that for nullary f this means $f =_{\mathcal{E}} e$.

Let $\mathcal{K}$ be a class of Σ-algebras. An *n-ary implicit operation* in $\mathcal{K}$ is a family $o = \{o_A \mid A \in \mathcal{K}\}$ of mappings $o_A\colon A^n \to A$ which is compatible with all homomorphisms, i.e., for all homomorphisms $\omega\colon A \to B$ with A, $B \in \mathcal{K}$ and all $a_1, \ldots, a_n \in A$, we have $(o_A(a_1, \ldots, a_n))\omega = o_B(a_1\omega, \ldots, a_n\omega)$. In the sequel we shall omit the index and just write o in place of o_A. Σ-terms induce implicit operations on any class of Σ-algebras in the following way: let t be a Σ-term and let $x_1, \ldots, x_n$ be a sequence of variables such that all the variables occurring in t are contained in this sequence. The n-ary implicit operation $(t; x_1, \ldots, x_n)$ is defined by

$$(a_1, \ldots, a_n) \longmapsto t[x_1/a_1, \ldots, x_n/a_n].$$

For example, assume that the signature consists of a binary symbol "$\cdot$" and a unary symbol "$^{-1}$", and let $\mathcal{K}$ be the class of all groups. Then the binary implicit operation $(x \cdot y^{-1}; x, y)$ expresses division in a group. If we apply this operation to a pair of group elements a, b, we obtain the quotient $a \cdot b^{-1}$. For the classes $\mathcal{V}(\mathcal{E})$ and $\mathcal{F}(\mathcal{E})$ all implicit operations can be defined by Σ-terms [La63].

We are now ready to give an algebraic definition of commutative theories. An equational theory $\mathcal{E} = (\Sigma, E)$ is called *commutative* if the following holds:

1. the signature Σ contains a constant symbol e which is idempotent in $\mathcal{E}$
2. there is a binary implicit operation "$*$" in $\mathcal{F}(\mathcal{E})$ such that

(a) the constant e is a neutral element for "$*$" in any algebra $\mathcal{F}_\mathcal{E}(X) \in \mathcal{F}(\mathcal{E})$

(b) for any n-ary function symbol $f \in \Sigma$, any algebra $\mathcal{F}_\mathcal{E}(X) \in \mathcal{F}(\mathcal{E})$, and any $s_1, \dots, s_n, t_1, \dots, t_n \in \mathcal{F}(\mathcal{E})$ we have $f(s_1 * t_1, \dots, s_n * t_n) = f(s_1, \dots, s_n) * f(t_1, \dots, t_n)$.

Though it is not explicitly required by the definition, the implicit operation "$*$" turns out to be associative and commutative (see [Ba89a], Corollary 5.4). This justifies the name "commutative theory."

Well-known examples of commutative theories are the theory AM of abelian monoids, the theory AIM of idempotent abelian monoids (sometimes called AC1 in the literature), and the theory AG of abelian groups (see [Ba89a]). In these theories, the implicit operation "$*$" is given by the explicit binary operation in the signature. An example for a commutative theory where "$*$" is really implicit can also be found in [Ba89a] (Example 5.1). We shall now consider examples of commutative theories where the signature contains some additional function symbols (see [Ba90, Nu90] for more examples).

Examples 3.1 We consider the following signatures: $\Sigma := \{+, 0, h\}$, where "$+$" is binary, 0 is nullary, and h is unary; $\Delta := \{+, 0, f\}$, where "$+$" is binary, 0 is nullary, and f is binary; and $\Omega := \{+, 0, -, i\}$, where "$+$" is binary, 0 is nullary, and $-$ and i are unary.

AMH $= (\Sigma, E_{\mathrm{AMH}})$, the theory of *abelian monoids with a homomorphism.* E_{AMH} consists of the identities which state that "$+$" is associative, commutative with neutral element "0", and the identities which state that h is a homomorphism, i.e., the identities $h(x + y) \doteq h(x) + h(y)$, $h(0) \doteq 0$.

AMIn $= (\Sigma, E_{\mathrm{AMIn}})$, the theory of *abelian monoids with an involution.* E_{AMIn} consists of the identities of E_{AMH}, and the additional identity $h(h(x)) \doteq x$, which states that h is an involution.

COM $= (\Delta, E_{\mathrm{COM}})$. E_{COM} consists of the identities which state that "$+$" is associative, commutative with neutral element 0, and the identities $f(x + x', y + y') \doteq f(x, y) + f(x', y')$ and $f(0, 0) \doteq 0$ which ensure that COM is really commutative.

GAUSS $= (\Omega, E_{\mathrm{GAUSS}})$. E_{GAUSS} consists of the identities which state that "$+$" is the binary operation of an abelian group with neutral element 0 and inverse $-$, and the additional identity $x + i(i(x)) \doteq 0$.

With the exception of the third example, the additional function symbols—i.e., the function symbols apart from the binary symbol yielding the implicit operation, and the idempotent constant symbol—are all unary symbols. This motivates the definition of monoidal theories. An equational theory $\mathcal{E} = (\Sigma, E)$ is *monoidal* if

1. Σ contains a constant symbol 0, a binary function symbol "+", and all the other symbols in Σ are unary

2. "+" is associative and commutative

3. 0 is the neutral element for "+", that is, $0 + x =_{\mathcal{E}} x + 0 =_{\mathcal{E}} x$

4. every unary symbol h is a homomorphism for "+" and 0, that is, $h(x+y) =_{\mathcal{E}} h(x) + h(y)$ and $h(0) =_{\mathcal{E}} 0$.

It is easy to see that monoidal theories are always commutative theories. Obviously, the theories AM, AIM, AG, AMH, AMIn, and GAUSS are monoidal. The theory COM is not monoidal, since its signature contains an additional *binary* function symbol. However, we shall see in the next subsection that COM may also be regarded as monoidal theory if the signature is translated appropriately.

3.2 Adding Monoids of Homomorphisms

There is an interesting difference between the theory GAUSS on the one hand, and the theories AMH and AMIn on the other hand. The additional identity $x + i(i(x)) \doteq 0$ in the theory GAUSS establishes a closer connection between the unary symbol i and the binary symbol "+" than just the fact that i is a homomorphism for "+". This is not the case for the additional identity $h(h(x)) \doteq h(x)$ in AMIn which says something about h alone. This observation will now be put into a more general setting.

Let $\mathcal{E} = (\Sigma, E)$ be a monoidal theory, and let H be a monoid generated by the finitely many elements $h_1, \ldots, h_n$. We define the augmented theory $\mathcal{E}\langle H\rangle = (\Sigma', E')$ as follows: the signature Σ' extends Σ by the unary function symbols $h_1, \ldots, h_n$; the set of identities E' extends E with the identities which state that $h_1, \ldots, h_n$ are homomorphisms, and the identities $\{h_{i_1}(\ldots h_{i_k}(x)\ldots) \doteq h_{j_1}(\ldots h_{j_l}(x)\ldots) \mid h_{i_1}\ldots h_{i_k} = h_{j_1}\ldots h_{j_l}$ holds in $H\}$. In Sections 5 and 6 we shall study unification in theories of the form $\mathcal{E}\langle H\rangle$.

The theory AMH is $\mathrm{AM}\langle h^*\rangle$ where h^* stands for the free monoid in one generator, and AMIn is $\mathrm{AM}\langle Z_2\rangle$ where Z_2 stands for the cyclic group of order 2, i.e., Z_2 consists of two elements e and h, and the multiplication in Z_2 is defined as $e\cdot e = e$, $h\cdot e = e\cdot h = h$, and $h\cdot h = e$. On the other hand, one can prove that GAUSS cannot be represented in the form $\mathrm{AG}\langle H\rangle$ because of the interaction between i and "+" stated by $x + i(i(x)) \doteq 0$.

3.3 Commutative and Monoidal Theories are Equivalent

Next we show that by means of a signature transformation every commutative theory can be turned into a monoidal theory that, from the viewpoint of unification, is equivalent.

Let Σ and Σ' be signatures. A *signature transformation from Σ' to Σ* is a mapping θ that associates to every Σ'-term a Σ-term such that

1. $x\theta = x$ for every variable x
2. $f(t_1, \ldots, t_n)\theta = (f(x_1, \ldots, x_n)\theta)[x_1/t_1\theta, \ldots, x_n/t_n\theta]$ if f is an n-ary symbol and $x_1, \ldots, x_n$ are n distinct variables.

It follows from the definition that θ is completely defined by the images of the flat terms $f(x_1, \ldots, x_n)$ where f ranges over Σ'. Intuitively, θ interprets every Σ'-symbol by a Σ-term, and then extends this interpretation consistently to arbitrary Σ'-terms.

To every commutative theory $\mathcal{E} = (\Sigma, E)$ we associate a theory $\widehat{\mathcal{E}} = (\widehat{\Sigma}, \widehat{E})$ and a signature transformation θ from $\widehat{\Sigma}$ to Σ as follows. The signature $\widehat{\Sigma}$ consists of a constant 0, a binary symbol "+", and unary symbols $f_1, \ldots, f_n$ for every n-ary symbol $f \in \Sigma$, where $n \geq 1$. To define the set of identities $\widehat{E}$ we need the transformation θ. Let e be the idempotent constant in $\mathcal{E}$ and let $(t_*; x, y)$ be the pair corresponding to the implicit operation "$*$" in $\mathcal{E}$. We define θ by $0\theta := e$, $(x + y)\theta := t_*$, and $f_i(x)\theta := f(e, \ldots, x, \ldots, e)$, where $f(e, \ldots, x, \ldots, e)$ has the variable x in the i-th argument position and the constant e in the other positions. Now, with the help of this signature transformation we define $\widehat{E}$ as $\widehat{E} := \{\hat{s} \doteq \hat{t} \mid \hat{s}\theta =_{\mathcal{E}} \hat{t}\theta\}$. That is, $\widehat{E}$ is the preimage of $=_{\mathcal{E}}$ under θ.

Proposition 3.2 *Let $\mathcal{E} = (\Sigma, E)$ be a commutative theory with associated theory $\widehat{\mathcal{E}} = (\widehat{\Sigma}, \widehat{E})$ and signature transformation θ. Then:*

1. *$\widehat{\mathcal{E}}$ is a monoidal theory*
2. *$\hat{s} =_{\widehat{\mathcal{E}}} \hat{t}$ implies $\hat{s}\theta =_{\mathcal{E}} \hat{t}\theta$ for all $\widehat{\Sigma}$-terms $\hat{s}$, $\hat{t}$.*

Proof. 1. Since the implicit operation "$*$" is associative and commutative, the same is true for "+". From part (2.b) of the definition of commutative theories we conclude that every f_i is a homomorphism for "+". Finally, since e is neutral for "$*$", we have that 0 is a zero for "+", and since e is idempotent, we conclude that 0 is a zero for the homomorphisms f_i.

2. The claim follows from the definition of $\widehat{E}$ and the fact that $\widehat{E}$ is a stable congruence. □

Let $\mathcal{E} = (\Sigma, E)$ and $\mathcal{E}' = (\Sigma', E')$ be equational theories. We say that $\mathcal{E}$ and $\mathcal{E}'$ are *equivalent* if there exist signature transformations θ' from Σ to Σ' and θ from Σ' to Σ such that

1. $s =_{\mathcal{E}} t$ implies $s\theta' =_{\mathcal{E}'} t\theta'$ for all Σ-terms s and t and $s' =_{\mathcal{E}'} t'$ implies $s'\theta =_{\mathcal{E}} t'\theta$ for all Σ'-terms s' and t'

2. $s\theta'\theta =_{\mathcal{E}} s$ for all Σ-terms s, and $s'\theta\theta' =_{\mathcal{E}'} s'$ for all Σ'-terms s'.

The first condition means that θ and θ' can be seen as mappings on equivalence classes of terms. The second says that θ and θ' are inverses of each other modulo the equational theories.

One of the most prominent examples of equivalent theories are boolean rings and boolean algebras. If two theories are equivalent they describe essentially the same structures. More precisely, if $\mathcal{E}$ and $\mathcal{E}'$ are equivalent, then the categories $\mathcal{C}(\mathcal{E})$ and $\mathcal{C}(\mathcal{E}')$ are isomorphic, and so are the varieties of $\mathcal{E}$ and $\mathcal{E}'$ [Ta79]. Since unification properties of a theory $\mathcal{E}$ depend on the category $\mathcal{C}(\mathcal{E})$, it follows that equivalent theories share the same unification properties.

Theorem 3.3 *Let $\mathcal{E} = (\Sigma, E)$ be a commutative theory with associated theory $\widehat{\mathcal{E}} = (\widehat{\Sigma}, \widehat{E})$. Then $\mathcal{E}$ and $\widehat{\mathcal{E}}$ are equivalent.*

Proof. Let θ be the signature transformation from $\widehat{\Sigma}$ to Σ. To show the equivalence of $\mathcal{E}$ and $\widehat{\mathcal{E}}$ we exhibit a signature transformation $\hat{\theta}$ from Σ to $\widehat{\Sigma}$ and show that θ and $\hat{\theta}$ have the required properties. We define $\hat{\theta}$ by $e\hat{\theta} = 0$, and $f(x_1, \ldots, x_n)\hat{\theta} = f_1(x_1) + \cdots + f_n(x_n)$ for every n-ary symbol f in Σ.

By Proposition 3.2 we already know that $\hat{s} =_{\widehat{\mathcal{E}}} \hat{t}$ implies $\hat{s}\theta =_{\mathcal{E}} \hat{t}\theta$ for all $\widehat{\Sigma}$-terms $\hat{s}$, $\hat{t}$.

Next we prove that $s\hat{\theta}\theta =_{\mathcal{E}} s$ for every Σ-term s. For this purpose it suffices to show the claim for flat terms of the form $f(x_1, \ldots, x_n)$. For such terms we have

$$\begin{aligned} f(x_1, \ldots, x_n)\hat{\theta}\theta &= (f_1(x_1) + \cdots + f_n(x_n))\theta \\ &= f(x_1, e, \ldots) * \cdots * f(\ldots, e, x_n) \\ &=_{\mathcal{E}} f(x_1 * e * \cdots * e, \ldots, e * \cdots * e * x_n) \\ &=_{\mathcal{E}} f(x_1, \ldots, x_n), \end{aligned}$$

where the first two equalities follow from the definition of $\hat{\theta}$ and θ, and the last two equalities follow from parts (2.b) and (2.a) of the definition of commutative theories.

To show that $\hat{s}\theta\hat{\theta} =_{\widehat{\mathcal{E}}} \hat{s}$ for every $\widehat{\Sigma}$-term $\hat{s}$, it suffices by the definition of $\widehat{E}$ to show that $\hat{s}\theta\hat{\theta}\theta =_{\mathcal{E}} \hat{s}\theta$, which is a consequence of the fact that $s\hat{\theta}\theta =_{\mathcal{E}} s$ for every Σ-term s.

Finally, we show that for all Σ-terms s, t we have that $s =_{\mathcal{E}} t$ implies $s\hat{\theta} =_{\widehat{\mathcal{E}}} t\hat{\theta}$. But this follows again from the definition of $\widehat{E}$, since $s\hat{\theta}\theta =_{\mathcal{E}} s =_{\mathcal{E}} t =_{\mathcal{E}} t\hat{\theta}\theta$ then yields $s\hat{\theta} =_{\widehat{\mathcal{E}}} t\hat{\theta}$. □

From this result it follows that from the viewpoint of unification there is no difference between commutative and monoidal theories.

4 Unification in Commutative/Monoidal Theories

First we shall show the connection between unification modulo commutative/monoidal theories and solving linear equations in semirings. In [Ba89a] the following properties for a commutative theory $\mathcal{E}$ are shown within the categorical framework, using well-known results for semiadditive theories.

1. The implicit operation "$*$" required in the definition of commutative theories induces a binary operation "$+$" on any morphism set $hom(\mathcal{F}_\mathcal{E}(X), \mathcal{F}_\mathcal{E}(Y))$ as follows: for $\sigma, \tau: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ we define $\sigma + \tau$ by $t(\sigma + \tau) := (t\sigma) * (t\tau)$ for all $t \in \mathcal{F}_\mathcal{E}(X)$. This operation is associative and commutative, and it distributes with the composition of morphisms. The morphism $0: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ defined by $x \mapsto e$ for all $x \in X$, where e is the idempotent constant required in the definition of commutative theories, is a neutral element for "$+$" on $hom(\mathcal{F}_\mathcal{E}(X), \mathcal{F}_\mathcal{E}(Y))$.

2. The cartesian product of $\mathcal{F}_\mathcal{E}(X)$ and $\mathcal{F}_\mathcal{E}(Y)$ is also a product in the categorical sense. Furthermore, the product is isomorphic to the coproduct, that is $\mathcal{F}_\mathcal{E}(X \uplus Y) \simeq \mathcal{F}_\mathcal{E}(X) \times \mathcal{F}_\mathcal{E}(Y)$.

3. Consider $\sigma: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$. Let u_x for $x \in X$ be the injections of the coproduct $\mathcal{F}_\mathcal{E}(X) = \bigoplus_{x \in X} \mathcal{F}_\mathcal{E}(x)$ and p_y for $y \in Y$ be the projections of the product $\mathcal{F}_\mathcal{E}(Y) = \bigotimes_{y \in Y} \mathcal{F}_\mathcal{E}(y)$. Then σ is uniquely determined by the matrix $M_\sigma := (u_x \sigma p_y)_{x \in X, y \in Y}$. For σ, $\tau: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ and $\delta: \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$, we have $M_{\sigma+\tau} = M_\sigma + M_\tau$, and $M_{\sigma\delta} = M_\sigma M_\delta$.

As an example, consider the morphism $\sigma = [x_1/h(y_1), x_2/y_1 + h^2(y_2)]$ from $\mathcal{F}_{\mathrm{AMH}}(x_1, x_2)$ to $\mathcal{F}_{\mathrm{AMH}}(y_1, y_2)$. Then σ is determined by the matrix

$$M_\sigma = \begin{pmatrix} \sigma_{11} & \sigma_{12} \\ \sigma_{21} & \sigma_{22} \end{pmatrix} = \begin{pmatrix} [x_1/h(y_1)] & [x_1/0] \\ [x_2/y_1] & [x_2/h^2(y_2)] \end{pmatrix}.$$

Let $\mathbf{1}$ be an arbitrary set of cardinality one. Property 1 from above yields that the set $hom(\mathcal{F}_\mathcal{E}(\mathbf{1}), \mathcal{F}_\mathcal{E}(\mathbf{1}))$ with addition "$+$" and composition as multiplication is a semiring, which will be denoted by $\mathcal{S}_\mathcal{E}$. Any $\mathcal{F}_\mathcal{E}(x)$ is isomorphic to $\mathcal{F}_\mathcal{E}(\mathbf{1})$, and thus, for $|X| = n$, $\mathcal{F}_\mathcal{E}(X)$ is the n-th power and copower of $\mathcal{F}_\mathcal{E}(\mathbf{1})$. Consequently, for $\sigma: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$, the entries $u_x \sigma p_y$ of the $|X| \times |Y|$-matrix M_σ may all be considered as elements of $\mathcal{S}_\mathcal{E}$. That means that all morphisms in $\mathcal{C}(\mathcal{E})$ can be written as matrices over the semiring $\mathcal{S}_\mathcal{E}$. Addition and multiplication of matrices correspond to addition and composition of morphisms, as stated in Property 3 above.

As an example, consider an arbitrary morphism $\gamma: \mathcal{F}_{\mathrm{AMH}}(y) \to \mathcal{F}_{\mathrm{AMH}}(y)$. Then there exist $a_0, \ldots, a_k \in \mathbf{N}$ such that $y\gamma =_{\mathrm{AMH}} a_0 y + a_1 h(y) + \ldots + a_k h^k(y)$. We associate with the morphism γ the polynomial $a_0 + a_1 X + \ldots + a_k X^k$, which is an element of the semiring $\mathbf{N}[X]$ of polynomials in one indeterminate X with nonnegative integer coefficients.

The morphism $\sigma = [x_1/h(y_1),\ x_2/y_1 + h^2(y_2)]$ from above and the morphism $\delta = [y_1/h(z), y_2/2z]$ can be expressed by the matrices

$$M_\sigma = \begin{pmatrix} X & 0 \\ 1 & X^2 \end{pmatrix} \quad \text{and} \quad M_\delta = \begin{pmatrix} X \\ 2 \end{pmatrix}$$

over $\mathbf{N}[X]$. An easy calculation shows that the morphism $\sigma\delta = [x_1/h^2(z), x_2/h(z) + 2h^2(z)]$ corresponds to the matrix $M_\sigma M_\delta$.

Examples 4.1 The theories of Example 3.1 yield the following semirings (see [Nu90, Ba90]).

$\mathcal{S}_{\mathrm{AMH}}$, the semiring corresponding to the theory AMH of abelian monoids with a homomorphism, is isomorphic to $\mathbf{N}[X]$, the semiring of polynomials in one indeterminate X with nonnegative integer coefficients.

$\mathcal{S}_{\mathrm{AMIn}}$, which corresponds to the theory of abelian monoids with an involution, is the monoid semiring $\mathbf{N}\langle Z_2\rangle$, where Z_2 denotes the cyclic group of order 2.

$\mathcal{S}_{\mathrm{COM}}$, the semiring corresponding to the theory COM, is isomorphic to $\mathbf{N}\langle X, Y\rangle$, the semiring of polynomials in two *noncommuting* indeterminates X, Y with nonnegative integer coefficients. Note that $\mathbf{N}\langle X, Y\rangle$ is the monoid semiring $\mathbf{N}\langle \{X, Y\}^*\rangle$, where $\{X, Y\}^*$ denotes the free monoid in two generators X, Y.

$\mathcal{S}_{\mathrm{GAUSS}}$ is isomorphic to the ring of Gaussian numbers $\mathbf{Z} \oplus i\mathbf{Z}$, consisting of the complex numbers $m + in$, where $m, n \in \mathbf{Z}$.

The first two examples suggest that there is a close connection between augmenting a commutative/monoidal theory by a monoid (as defined at the end of Subsection 3.1) and adjoining a monoid to the corresponding semiring (as defined in Subsection 2.3). For $\mathrm{AMIn} = \mathrm{AM}\langle Z_2\rangle$, for instance, one verifies that the semirings $\mathcal{S}_{\mathrm{AM}\langle Z_2\rangle}$ and $\mathcal{S}_{\mathrm{AM}}\langle Z_2\rangle$ are isomorphic. It is easy to see that this kind of connection holds in general.

Theorem 4.2 *Let $\mathcal{E}$ be a commutative/monoidal theory, and let H be a finitely generated monoid. Then $\mathcal{S}_{\mathcal{E}\langle H\rangle}$, the semiring corresponding to $\mathcal{E}$ augmented by H, and the monoid semiring $\mathcal{S}_{\mathcal{E}}\langle H\rangle$ are isomorphic.*

Proof. Let $\mathcal{E} = (\Sigma, E)$ be a commutative/monoidal theory and H be a monoid generated by the finitely many elements $h_1, \ldots, h_n$. Then $\mathcal{E}\langle H\rangle$ has the signature $\Sigma' = \Sigma \cup \{h_1, \ldots, h_n\}$.

We shall construct a semiring isomorphism that maps every element $\gamma \in \mathcal{S}_{\mathcal{E}\langle H\rangle}$ to an element $\hat{\gamma} \in \mathcal{S}_{\mathcal{E}}\langle H\rangle$. Recall that the elements of $\mathcal{S}_{\mathcal{E}\langle H\rangle}$ are the Σ'-homomorphisms from $\mathcal{F}_{\mathcal{E}\langle H\rangle}(\mathbf{1})$ to $\mathcal{F}_{\mathcal{E}\langle H\rangle}(\mathbf{1})$ where $\mathbf{1} = \{x\}$ is a singleton. Let γ be such a Σ'-homomorphism. Then γ is uniquely determined by the element $x\gamma$. Without loss of generality we can assume that $x\gamma =_{\mathcal{E}\langle H\rangle} \sum_{i=1}^{m} h_{i1}(\ldots(h_{in_i}(t_i))\ldots)$ where the t_i's are Σ-terms. For every $i = 1, \ldots, m$ let γ_i be the Σ-homomorphism from $\mathcal{F}_{\mathcal{E}}(\mathbf{1})$ to $\mathcal{F}_{\mathcal{E}}(\mathbf{1})$ defined by $x\gamma_i := t_i$. Then we have $\gamma_i \in \mathcal{S}_{\mathcal{E}}$. We define $\hat{\gamma}$ as $\hat{\gamma} := \sum_{i=1}^{m} \gamma_i \cdot h_{i1} \cdots h_{in_i} \in \mathcal{S}_{\mathcal{E}}\langle H\rangle$.

One can verify that the definition of $\hat{\gamma}$ does not depend on the particular presentation of γ and that the mapping "$\hat{\ }$" is bijective. Exploiting the fact that $h_1, \ldots, h_n$ are homomorphisms in $\mathcal{E}\langle H\rangle$ one shows that "$\hat{\ }$" is compatible with the semiring operations and hence is a semiring isomorphism. □

The isomorphism of $\mathcal{S}_{\mathcal{E}\langle H\rangle}$ and $\mathcal{S}_{\mathcal{E}}\langle H\rangle$ will be used in the next two sections to study the unification problem for $\mathcal{E}\langle H\rangle$ in an algebraic setting.

In Subsection 2.2 we have seen that $\mathcal{E}$-unification can be reformulated as unification in the category $\mathcal{C}(\mathcal{E})$. A unification problem in $\mathcal{C}(\mathcal{E})$ is given by a pair of morphisms σ, τ, and unifier is morphism δ such that $\sigma\delta = \tau\delta$. If we translate the morphisms into matrices over $\mathcal{S}_{\mathcal{E}}$, this means that an $\mathcal{E}$-unifier corresponds to a matrix M over $\mathcal{S}_{\mathcal{E}}$ such that $M_\sigma M = M_\tau M$. This correspondence is used in [Nu88, Nu90, Ba90] to characterize the unification types of commutative/monoidal theories by algebraic properties of the corresponding semirings.

Theorem 4.3 *A commutative/monoidal theory $\mathcal{E}$ is unitary w.r.t. unification without constants if and only if $\mathcal{S}_{\mathcal{E}}$ satisfies the following condition: for any pair M_σ, M_τ of $m\times n$-matrices over $\mathcal{S}_{\mathcal{E}}$ the set*

$$\mathcal{U}(M_\sigma, M_\tau) := \{x \in \mathcal{S}_{\mathcal{E}}{}^n \mid M_\sigma x = M_\tau x\}$$

is a finitely generated right $\mathcal{S}_{\mathcal{E}}$-module.

If $\mathcal{U}(M_\sigma, M_\tau)$ is generated by $x_1, \ldots, x_k \in \mathcal{S}_{\mathcal{E}}{}^n$, then the matrix which has $x_1, \ldots, x_k$ as columns corresponds to a most general $\mathcal{E}$-unifier of σ and τ.

Since constant-free unification problems in commutative/monoidal theories are either unitary or of type zero [Nu88, Ba89a, Nu90], the theorem yields that the theory $\mathcal{E}$ is of type zero iff there exist matrices M_σ, M_τ over $\mathcal{S}_{\mathcal{E}}$ such that the right $\mathcal{S}_{\mathcal{E}}$-module $\mathcal{U}(M_\sigma, M_\tau)$ is not finitely generated. Using this characterization, it can be shown that the theories AMH and COM are of type zero (see [Ba89a, Ba90]). The theories AMIn and GAUSS are unitary w.r.t. unification without constants (see [Ba89a] for the first, and [Nu90] for the second result).

For unification with constants, we have to solve—in addition to homogeneous systems $M_\sigma x = M_\tau x$ of linear equations over $\mathcal{S}_{\mathcal{E}}$—inhomogeneous systems of the form $M_\sigma x + a = M_\tau x + b$, where $a, b \in \mathcal{S}_{\mathcal{E}}{}^m$. The solutions of the inhomogeneous equations together with the generators of $\mathcal{U}(M_\sigma, M_\tau)$ can then be translated into unifiers in a way that is similar to the unification method for AM described in [LS75].

Theorem 4.4 *Let $\mathcal{E}$ be a commutative/monoidal theory which is unitary w.r.t. unification without constants. Then $\mathcal{E}$ is unitary (finitary) w.r.t. unification with constants if and only if $\mathcal{S}_\mathcal{E}$ satisfies the following condition: for any pair M_σ, M_τ of $m{\times}n$-matrices over $\mathcal{S}_\mathcal{E}$, and any pair a, $b \in {\mathcal{S}_\mathcal{E}}^m$ the set*

$$\{x \in {\mathcal{S}_\mathcal{E}}^n \mid M_\sigma x + a = M_\tau x + b\}$$

is a coset (finite union of cosets) of the right $\mathcal{S}_\mathcal{E}$-module $\mathcal{U}(M_\sigma, M_\tau)$.

This characterization can be used to show that AMIn is finitary w.r.t. unification with constants. The theory GAUSS is even unitary w.r.t. unification with constants. This is due to the fact that $\mathcal{S}_{\mathrm{GAUSS}} \simeq \mathbf{Z} \oplus i\mathbf{Z}$ is a ring, and not only a semiring. In fact, let $\mathcal{S}_\mathcal{E}$ be a ring, and let x_0 be an arbitrary solution of the equation $M_\sigma x + a = M_\tau x + b$. Then any solution y of this inhomogeneous equation is of the form $y = x_0 + z$, where $z := y - x_0$ is a solution of the homogeneous equation $M_\sigma x = M_\tau x$. This shows that any solution y of the inhomogeneous equation is an element of the coset $\{x_0 + z \mid z \in \mathcal{U}(M_\sigma, M_\tau)\}$. Conversely, any element of this coset is a solution of the inhomogeneous equation.

5 A Sufficient Condition for Unification Type Zero

In this section we shall generalize the "type zero" result for the theory AMH to a whole class of commutative/monoidal theories. This class will be defined by properties of the corresponding semiring. Before we can do that, we need one more notation.

Let $\mathcal{S}$ be a semiring which is not a ring. That means that the abelian monoid $(\mathcal{S}, +, 0)$ is not a group, i.e., there exists an element $p \in \mathcal{S}$ such that, for all $q \in \mathcal{S}$, we have $p+q \neq 0$. We shall call such an element p of $\mathcal{S}$ *non-invertible.* An element $s \in \mathcal{S}$ which has an inverse w.r.t. "+" is called *invertible.* For the semiring $\mathbf{N}$, all elements different from 0 are non-invertible. For the direct product $\mathbf{N} \times \mathbf{Z}$, an element (n, z) is invertible iff $n = 0$. Here are some trivial facts about invertible and non-invertible elements.

1. The elements $s_1, \ldots, s_k$ of $\mathcal{S}$ are invertible if and only if their sum $s_1 + \cdots + s_k$ is invertible.
2. The element $\sum_{h \in H} s_h \cdot h$ of the monoid semiring $\mathcal{S}\langle H\rangle$ is non-invertible if and only if there exists $h \in H$ such that s_h is non-invertible in $\mathcal{S}$. Thus, if $\mathcal{S}$ is not a ring, then $\mathcal{S}\langle H\rangle$ is not a ring for any monoid H.

Recall that the theory AMH corresponds to the semiring $\mathbf{N}[X]$ of polynomials in one indeterminate X with nonnegative integer coefficients. That means that we have a monoid semiring $\mathcal{S}\langle H\rangle$ where *all the nonzero elements* of $\mathcal{S}$ are non-invertible, and where the monoid H is the free monoid X^* in one generator. The "type zero" result for AMH can now be generalized to the case where $\mathcal{S}$ contains *at least one* non-invertible element.

Theorem 5.1 *Let $\mathcal{E}$ be a commutative/monoidal theory such that the corresponding semiring $\mathcal{S}_\mathcal{E}$ is isomorphic to a monoid semiring $\mathcal{S}\langle X^*\rangle$. If $\mathcal{S}$ is not a ring, i.e., if $\mathcal{S}$ contains at least one non-invertible element, then $\mathcal{E}$ is of unification type zero.*

As mentioned before the monoid semiring $\mathcal{S}\langle X^*\rangle$ is just the polynomial semiring $\mathcal{S}[X]$. The theorem is proved if we can find matrices M_σ, M_τ over $\mathcal{S}[X]$ such that the right $\mathcal{S}[X]$-module $\mathcal{U}(M_\sigma, M_\tau)$ is not finitely generated.

In the following we shall show that the 1×3-matrices $M_\sigma := (X, X, 0)$ and $M_\tau := (0, 1, X^2)$ have the required property. Thus we consider the homogeneous linear equation

$$X \cdot x_1 + X \cdot x_2 \;=\; x_2 + X^2 \cdot x_3 \qquad (1)$$

which has to be solved by a vector $L \in \mathcal{S}[X]^3$. If L is such a vector, we denote its components by $L^{(1)}$, $L^{(2)}$, $L^{(3)}$.

Let p be a non-invertible element in $\mathcal{S}$. Obviously, for any $n \geq 1$, the vector L_n which consists of the components $L_n^{(1)} := p$, $L_n^{(2)} := pX + \cdots + pX^{n+1}$, $L_n^{(3)} := pX^n$ is a solution of (1).

Now assume that $\mathcal{U}(M_\sigma, M_\tau)$ is finitely generated, i.e., there exist finitely many solutions $G_1, \cdots, G_m$ of (1) which generate all the solutions of (1). Let $n \geq 1$ be arbitrary but fixed. Since L_n is a solution of (1) there exist $l_1, \cdots, l_m \in \mathcal{S}[X]$ such that

$$L_n = \sum_{i=1}^{m} G_i l_i. \qquad (2)$$

If we consider (2) in the first component, we get $p = \sum_{i=1}^{m} G_i^{(1)} l_i$. For $i = 1, \ldots, m$, let $p_i \in \mathcal{S}$ be the constant coefficient of the polynomial $G_i^{(1)}$, and $h_i \in \mathcal{S}$ be the constant coefficient of l_i. The last equation implies that $p = \sum_{i=1}^{m} p_i h_i$. Since p is non-invertible, there exists some j with $1 \leq j \leq m$ such that $p_j h_j$ is non-invertible.

Lemma 5.2 *The polynomial $G_j^{(3)}$ is of degree at least n.*

Proof. Assume that the degree of $G_j^{(3)}$ is less than n. Since G_j is a solution of (1), we know that $G_j h_j$ is also a solution, that is,

$$X \cdot G_j^{(1)} h_j + X \cdot G_j^{(2)} h_j = G_j^{(2)} h_j + X^2 \cdot G_j^{(3)} h_j. \tag{3}$$

The components of the solution $G_j h_j$ satisfy the following properties:

- The constant coefficient of the polynomial $G_j^{(1)} h_j$ is $e_1 := p_j h_j$. Thus we know by the choice of j that e_1 is non-invertible.

- The polynomial $G_j^{(2)} h_j$ has constant coefficient 0. This is an immediate consequence of the equation (3).

- All the coefficients of $G_j^{(3)} h_j$ are invertible. This can be seen by considering equation (2) in the third component, which yields $pX^n = \sum_{i=1}^{m} G_i^{(3)} l_i$. Since $G_j^{(3)} h_j$ contains only monomials of degree less than n, all these monomials vanish during the summation. Consequently, all the coefficients of these monomials have to be invertible.

From the fact that the coefficient of X in $X \cdot G_j^{(1)} h_j$ is e_1 and in $X \cdot G_j^{(2)} h_j$ is 0 we get by (3) that the coefficient of X in $G_j^{(2)} h_j + X^2 \cdot G_j^{(3)} h_j$ is also e_1. Hence, the coefficient of X in $G_j^{(2)} h_j$ is e_1.

Starting with the fact the coefficient e_1 of X in $G_j^{(2)} h_j$ is non-invertible, we shall now deduce that the coefficient of X^2 in $G_j^{(2)} h_j$ is also non-invertible. Since the coefficient of X in $G_j^{(2)} h_j$ is e_1, the coefficient of X^2 in $X \cdot G_j^{(2)} h_j$ is also e_1. Thus the coefficient of X^2 on the left hand side of (3) is $e' := e_1 + e$ for some e. The coefficient e' is non-invertible because otherwise e_1 could not be non-invertible. By (3), the coefficient of X^2 in $G_j^{(2)} h_j + X^2 \cdot G_j^{(3)} h_j$ is also e'. Since all the coefficients of $X^2 \cdot G_j^{(3)} h_j$ are invertible, this finally shows that the coefficient e_2 of X^2 in $G_j^{(2)} h_j$ is non-invertible.

This argument can be iterated to show that, for all $k \geq 1$, the coefficient e_k of X^k in $G_j^{(2)} h_j$ is non-invertible. This is a contradiction to the fact that the polynomial $G_j^{(2)} h_j$ has only finitely many nonzero coefficients. □

We have just shown that, for any $n \geq 1$, there exists a j such that $G_j^{(3)}$ is of degree at least n. This is a contradiction to our assumption that there are finitely many generators G_j of all solutions of (1). This completes the proof of the theorem.

6 Adding Finite Monoids of Homomorphisms

In this section we investigate commutative/monoidal theories that are augmented with finite monoids of homomorphisms. In contrast to the case of free monoids, that was treated in the previous section, we can derive the positive result that adding finite monoids doesn't change the unification type and that algorithms for the original theory can be used to solve problems in the augmented theory.

An example for such a theory is AMIn, the theory of abelian monoids with an involution. Recall that AMIn can be written as $\mathrm{AM}\langle Z_2\rangle$, and that the corresponding semiring is $\mathbf{N}\langle Z_2\rangle$.

General Assumption. *In this section $\mathcal{E}$ is a commutative/monoidal theory and H is a finite monoid.*

Since unification problems in $\mathcal{E}\langle H\rangle$ are equivalent to systems of linear equations over $\mathcal{S}_\mathcal{E}\langle H\rangle$, our basic technique will be to reduce such systems to systems of linear equations over $\mathcal{S}_\mathcal{E}$. As a first step we shall establish a one-to-one correspondence between vectors.

Every vector $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$ has a unique representation as $x = \sum_{h\in H} x_h{\cdot}h$ where $a_h \in {\mathcal{S}_\mathcal{E}}^n$. As an example the vector

$$x = \begin{pmatrix} 1+2h \\ h \end{pmatrix} \in \mathbf{N}\langle Z_2\rangle$$

can be written as

$$x = \begin{pmatrix} 1{\cdot}e + 2{\cdot}h \\ 0{\cdot}e + 1{\cdot}h \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}{\cdot}e + \begin{pmatrix} 2 \\ 1 \end{pmatrix}{\cdot}h.$$

We can formally justify this notation if we consider $\mathcal{S}_\mathcal{E}$ and H as subsets of $\mathcal{S}_\mathcal{E}\langle H\rangle$. This can be done by identifying every element $s \in \mathcal{S}_\mathcal{E}$ with $s{\cdot}e \in \mathcal{S}_\mathcal{E}\langle H\rangle$, where e is the unit in H, and every element $h \in H$ with $1{\cdot}h \in \mathcal{S}_\mathcal{E}\langle H\rangle$.

Suppose the elements of H are numbered as $h_1, \ldots, h_{|H|}$. If $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$ has a representation as $x = x_{h_1}{\cdot}h_1 + \cdots + x_{h_{|H|}}{\cdot}h_{|H|}$, we define

$$\widehat{x} = \begin{pmatrix} x_{h_1} \\ \vdots \\ x_{h_{|H|}} \end{pmatrix} \in {\mathcal{S}_\mathcal{E}}^{n|H|}$$

as the vector obtained from x by writing the vectors x_h one below another. Continuing our example from above we have

$$\widehat{x} = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 1 \end{pmatrix}.$$

We thus obtain a bijection between $\mathcal{S}_\mathcal{E}\langle H\rangle^n$ and ${\mathcal{S}_\mathcal{E}}^{n|H|}$. In particular, every vector in ${\mathcal{S}_\mathcal{E}}^{n|H|}$ has a representation as $\widehat{x}$ for some $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$. Obviously, for all x, $y \in {\mathcal{S}_\mathcal{E}}^{n|H|}$ and all $s \in \mathcal{S}_\mathcal{E}$ we have

$$\widehat{x+y} = \widehat{x} + \widehat{y} \qquad \text{and} \qquad \widehat{x}{\cdot}s = \widehat{x{\cdot}s}. \tag{4}$$

In algebraic terms we can rephrase these equalities by saying that the mapping "$\widehat{\cdot}$" is a right $\mathcal{S}_\mathcal{E}$-module isomorphism.

Next we will associate to every $m{\times}n$-matrix M with entries in $\mathcal{S}_\mathcal{E}\langle H\rangle$ an $m|H|{\times}n|H|$-matrix $\widehat{M}$ with entries in $\mathcal{S}_\mathcal{E}$, such that $\widehat{Mx} = \widehat{M}\widehat{x}$ holds for every $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$. To derive an appropriate definition of $\widehat{M}$, observe that, similar to a vector, the matrix M has a unique representation $M = \sum_{h\in H} M_h\cdot h$, where the M_h are matrices with entries in $\mathcal{S}_\mathcal{E}$. Applying M to a vector x yields

$$\begin{aligned} Mx &= (\sum_{f\in H} M_f\cdot f)(\sum_{g\in H} x_g\cdot g) = \sum_{f,g\in H} M_f x_g\cdot f\cdot g \\ &= \sum_{h\in H}(\sum_{h=fg} M_f x_g)\cdot h = \sum_{h\in H}(\sum_{g\in H}(\sum_{h=f\cdot g} M_f)x_g)\cdot h. \end{aligned}$$

This series of equalities says that the component of the vector $\widehat{Mx}$ corresponding to the element h is obtained by summing over all g the products $(\sum_{h=f\cdot g} M_f)x_g$. This shows that we have to define $\widehat{M}$ as the $m|H|{\times}n|H|$-matrix consisting of the submatrices

$$\widehat{M}_{i,j} = \sum_{\substack{h\in H \\ h_i = h\cdot h_j}} M_h,$$

where a sum over an empty set of indices is to be understood as the zero matrix. With this definition we obtain

$$\widehat{Ma} = \widehat{M}\widehat{a}. \tag{5}$$

Returning to our example theory AMIn, consider a matrix M over $\mathbf{N}\langle Z_2\rangle$. If $M = M_e\cdot e + M_h\cdot h$, then the associated matrix is

$$\widehat{M} = \begin{pmatrix} M_e & M_h \\ M_h & M_e \end{pmatrix}.$$

Thus, our general approach gives us the same representation of unification problems in AMIn as the one derived in [Ba89a].

Next we apply our transformation technique to unification problems without constants.

Proposition 6.1 *Let M_σ, M_τ be $m{\times}n$-matrices over $\mathcal{S}_\mathcal{E}\langle H\rangle$, and $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$. Then:*

1. *$x \in \mathcal{U}(M_\sigma, M_\tau)$ if and only if $\widehat{x} \in \mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$*
2. *$\mathcal{U}(M_\sigma, M_\tau)$ is generated by $x_1, \ldots, x_k$ if $\mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$ is generated by $\widehat{x}_1, \ldots, \widehat{x}_k$.*

Proof. 1. Let $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$. Then we have $x \in \mathcal{U}(M_\sigma, M_\tau)$ if and only if $M_\sigma x = M_\tau x$ if and only if $\widehat{M_\sigma x} = \widehat{M_\tau x}$ if and only if $\widehat{M}_\sigma \widehat{x} = \widehat{M}_\tau \widehat{x}$ if and only if $\widehat{x} \in \mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$.

2. It suffices to show that every $x \in \mathcal{U}(M_\sigma, M_\tau)$ is a linear combination of $x_1, \ldots, x_k$. If $x \in \mathcal{U}(M_\sigma, M_\tau)$, then $\widehat{x} \in \mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$ by part (1). Hence, $\widehat{x} = \widehat{x}_1 \cdot s_1 + \cdots + \widehat{x}_k \cdot s_k$. Using equalities (4), we conclude that $x = x_1 \cdot s_1 + \cdots + x_k \cdot s_k$. Thus, x is a linear combination of $x_1, \ldots, x_k$. $\square$

If $\mathcal{E}$ is unitary w.r.t. unification without constants, then for all matrices M_σ, M_τ with entries from $\mathcal{S}_\mathcal{E}\langle H\rangle$ the right $\mathcal{S}_\mathcal{E}$-module $\mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$ is finitely generated, and by the preceding proposition, $\mathcal{U}(M_\sigma, M_\tau)$ is finitely generated. Together with Theorem 4.3 this proves our next theorem.

Theorem 6.2 *If $\mathcal{E}$ is unitary w.r.t. unification without constants, then $\mathcal{E}\langle H\rangle$ is unitary w.r.t. unification without constants.*

The approach to unification problems with constants again consists in reducing a problem for $\mathcal{E}\langle H\rangle$ to a problem for $\mathcal{E}$. Speaking in terms of semirings, we shall reduce inhomogeneous linear equations over $\mathcal{S}_\mathcal{E}\langle H\rangle$ to inhomogeneous linear equations over $\mathcal{S}_\mathcal{E}$.

For a set $S \subseteq \mathcal{S}_\mathcal{E}\langle H\rangle^n$ let $\widehat{S} := \{\widehat{x} \mid x \in S\}$.

Proposition 6.3 *Let M_σ, M_τ be $m \times n$-matrices with entries in $\mathcal{S}_\mathcal{E}\langle H\rangle$ and a, $b \in \mathcal{S}_\mathcal{E}\langle H\rangle^m$. Let $N := \{x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n \mid M_\sigma x + a = M_\tau x + b\}$. Then:*

1. $\widehat{N} = \{y \in {\mathcal{S}_\mathcal{E}}^{n|H|} \mid \widehat{M}_\sigma y + \widehat{a} = \widehat{M}_\tau y + \widehat{b}\}$
2. *N is a coset (finite union of cosets) of $\mathcal{U}(M_\sigma, M_\tau)$, if $\widehat{N}$ is a coset (finite union of cosets) of $\mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$.*

Proof. 1. By equalities (4) and (5) it follows that for all $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$ we have $M_\sigma x + a = M_\tau x + b$ if and only if $\widehat{M}_\sigma \widehat{x} + \widehat{a} = \widehat{M}_\tau \widehat{x} + \widehat{b}$. Since for every $y \in {\mathcal{S}_\mathcal{E}}^{n|H|}$ there is a unique $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$ such that $y = \widehat{x}$, this yields the claim.

2. If $\widehat{N}$ is a coset of $\mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)$, then there exists a vector $x \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$ such that $\widehat{N} = \{\widehat{x} + y \mid y \in \mathcal{U}(\widehat{M}_\sigma, \widehat{M}_\tau)\}$. Using equality (4) and Proposition 6.1 we conclude that $N = \{x + z \mid z \in \mathcal{U}(M_\sigma, M_\tau)\}$.

For the case that $\widehat{N}$ is a finite union of cosets, the argument has to be slightly generalized. $\square$

By Theorem 4.4, the preceding result gives us a condition for $\mathcal{E}\langle H\rangle$ to be unitary or finitary.

Theorem 6.4 *Suppose $\mathcal{E}$ is unitary w.r.t. unification without constants. If $\mathcal{E}$ is unitary (finitary) w.r.t. unification with constants, then $\mathcal{E}\langle H\rangle$ is unitary (finitary) w.r.t. unification with constants, if $\mathcal{E}$ is unitary (finitary) w.r.t. unification with constants.*

Propositions 6.1 and 6.3 tell us how we can use an algorithm for $\mathcal{E}$ to solve problems in $\mathcal{E}\langle H\rangle$. An $\mathcal{E}\langle H\rangle$-unification problem without constants is given by $m\times n$-matrices M_σ, M_τ with entries in $\mathcal{S}_{\mathcal{E}\langle H\rangle} \simeq \mathcal{S}_\mathcal{E}\langle H\rangle$. We compute the transforms $\widehat{M}_\sigma$ and $\widehat{M}_\tau$ and solve the equation $\widehat{M}_\sigma y = \widehat{M}_\tau y$ over $\mathcal{S}_\mathcal{E}$, which we can do with the algorithm for $\mathcal{E}$. If the set of solutions of the matrix equation over $\mathcal{S}_\mathcal{E}$ is generated by vectors $y_1, \ldots, y_k \in {\mathcal{S}_\mathcal{E}}^{n|H|}$, we compute $x_1, \ldots, x_k \in \mathcal{S}_\mathcal{E}\langle H\rangle^n$ such that $\widehat{x}_i = y_i$. Then the set of solutions of the original equation is generated by $x_1, \ldots, x_k$ and the matrix M_δ that has $x_1, \ldots, x_k$ as colums represents a most general unifier of the given problem.

Since inhomogeneous linear equations over $\mathcal{S}_{\mathcal{E}\langle H\rangle} \simeq \mathcal{S}_\mathcal{E}\langle H\rangle$ can be transformed into inhomogeneous equations over $\mathcal{S}_\mathcal{E}$, an algorithm for $\mathcal{E}$ can be used in a similar way as in the constant free case to solve unification problems with constants in $\mathcal{E}\langle H\rangle$.

7 Conclusion

Two approaches to solving unification problems can be distinguished. The first, which might be called the "syntactic approach," relies heavily on the syntactic structure of the identities that define the equational theory (see for instance [GS89, NR89, KK90]). The second, which we may characterize as the "semantic approach," exploits the structure of the algebras that satisfy the theory. If little or nothing is known of the algebras involved, the first approach is useful, whereas the second is applicable to theories that describe algebraic structures which have been investigated in mathematics.

With this paper we pursue the semantic approach to unification. We have combined techniques for commutative and monoidal theories that had been developed independently. We have shown that both classes of theories are essentially the same in that every monoidal theory is commutative, and every commutative theory can be turned into a monoidal theory by a signature transformation.

One of the major topics of research in unification in recent years was to construct algorithms for the combination of equational theories. This problem has been solved—at least in principle—for theories with disjoint signatures [SS89]. Of course, the case where signatures are not disjoint is too difficult to be treated in full generality. We concentrated on a special case, namely the combination of a commutative/monoidal theory with a monoid of homomorphisms. By exploiting the algebraic structure of the canonical semiring associated to such a theory, we have found combinations that are of unification type zero, and others that are of type unitary or finitary. For the latter case we have pointed out how a unification algorithm can be derived.

There still remain open questions for this kind of combination. We have augmented a given theory either by free monoids or by finite monoids, but we do not know what happens with infinite monoids that are not free.

The only commutative/monoidal theories of unification type zero that we know are those described in this paper. They all have canonical semirings that are not rings. It would be interesting to know whether there exist theories of unification type zero for which the canonical semiring is a ring. Since every semiring can be obtained from a commutative/monoidal theory this question can be posed in purely algebraic terms: is there a ring such that the set of solutions for some system of homogeneous linear equations is not finitely generated?

It is not known whether there exists a unitary or finitary equational theory that is infinitary or of type zero for unification w.r.t. constants. This question has been raised in the context of combining theories with disjoint signatures. A combination algorithm requires that problems with free constants can be solved in the single theories. We can reformulate the corresponding question for commutative/monoidal theories as an algebraic problem: does there exist a semiring such that for every system of homogeneous equations the set of solutions is a finitely generated right module, but there is a system of inhomogeneous equations such that the corresponding set of solutions is not a finite union of cosets? Given the substantial body of results in linear algebra, it is conceivable to find a semiring satisfying this condition. Such a semiring would then give us an example of an equational theory with the above property.

References

[Ba89a] F. Baader, "Unification in Commutative Theories", *J. Symbolic Computation* **8**, 1989.

[Ba89b] F. Baader, "Unification Properties of Commutative Theories: A Categorical Treatment", *Proceedings of the Summer Conference on Category Theory and Computer Science, Manchester (England)*, 1989.

[Ba90] F. Baader, *Unification in Commutative Theories, Hilbert's Basis Theorem, and Gröbner Bases*, SEKI-Report SR-90-01, Universität Kaiserslautern, West Germany, 1990.

[Bm87] L. Bachmair, *Proof Methods for Equational Theories*, Ph.D. Thesis, Dep. of Comp. Sci., University of Illinois at Urbana-Champaign, 1987.

[Co65] P.M. Cohn, *Universal Algebra*, Harper and Row, New York, 1965.

[GR86] J. Gallier, S. Raatz, "SLD-Resolution Methods for Horn Clauses with Equality Based on E-Unification", *Proceedings of Symposium on Logic Programing* 1986.

[GS89] J. Gallier, S. Snyder, "Complete Sets of Transformations for General E-Unification", *Theoretical Computer Science* **27**, 1989.

[Gr68] G. Grätzer, *Universal Algebra*, Van Nostrand, Princeton, 1968.

[HS73] H. Herrlich, G.E. Strecker, *Category Theory*, Allyn and Bacon, Boston, 1973.

[Hu80] G. Huet, "Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems", *J. ACM* **27**, 1980.

[JL84] J. Jaffar, J.L. Lassez, M. Maher, "A Theory of Complete Logic Programs with Equality", *J. Logic Programming* **1**, 1984.

[JK86] J.P. Jouannaud, H. Kirchner, "Completion of a Set of Rules Modulo a Set of Equations", *SIAM J. Comp.* **15**, 1986.

[KK90] C. Kirchner, F. Klay, "Syntact Theories and Unification", *Proceedings of LICS 90*, 1990.

[La63] F.W. Lawvere, *Functional Semantics of Algebraic Theories*, Ph.D. Thesis, Columbia University, 1963.

[LS75] M. Livesey, J. Siekmann, *Unification of Bags and Sets*, Technical Report, Institut für Informatik I, Universität Karlsruhe, 1976.

[Ne74] A.J. Nevins, "A Human Oriented Logic for Automated Theorem Proving", *J. ACM* **21**, 1974.

[Nu88] W. Nutt, "Unification in Monoidal Theories", Presentation at the Second Workshop on Unification, Val d'Ajol, France, 1988.

[NR89] W. Nutt, P. Réty, G. Smolka, "Basic Narrowing Revisited", *J. Symbolic Computation* **7**, 1989.

[Nu89] W. Nutt, "The Unification Hierarchy is Undecidable", to appear in *J. Automated Reasoning*. Also SEKI-Report SR-89-06, Universität Kaiserslautern, West Germany, 1989.

[Nu90] W. Nutt, "Unification in Monoidal Theories", *Proceedings 10th International Conference on Automated Deduction*, Springer LNCS 449, 1990.

[PS81] G. Peterson, M. Stickel, "Complete Sets of Reductions for Some Equational Theories", *J. ACM* **28**, 1981.

[PL72] G. Plotkin, "Building in Equational Theories", *Machine Intelligence* **7**, 1972.

[SS89] M. Schmidt-Schauß, "Combination of Unification Algorithms", *J. Symbolic Computation* **8**, 1989.

[Si89] J. H. Siekmann, "Unification Theory: A Survey", *J. Symbolic Computation* **7**, 1989.

[Sl74] J.R. Slagle, "Automated Theorem Proving for Theories with Simplifiers, Commutativity and Associativity", *J. ACM* **21**, 1974.

[St85] M. Stickel, "Automated Deduction by Theory Resolution", *J. Automated Reasoning* **1**, 1985.

[Ta79] W. Taylor, *Equational Logic*, Houston J. of Mathematics **5**, 1979.

Deutsches
Forschungszentrum
für Künstliche
Intelligenz GmbH

DFKI
-Bibliothek-
Stuhlsatzenhausweg 3
6600 Saarbrücken 11
FRG

DFKI Publikationen

Die folgenden DFKI Veröffentlichungen oder die aktuelle Liste von erhältlichen Publikationen können bezogen werden von der oben angegebenen Adresse.

DFKI Publications

The following DFKI publications or the list of currently available publications can be ordered from the above address.

DFKI Research Reports

RR-90-01
Franz Baader
Terminological Cycles in KL-ONE-based Knowledge Representation Languages
33 pages

RR-90-02
Hans-Jürgen Bürckert
A Resolution Principle for Clauses with Constraints
25 pages

RR-90-03
Andreas Dengel & Nelson M. Mattos
Integration of Document Representation, Processing and Management
18 pages

RR-90-04
Bernhard Hollunder & Werner Nutt
Subsumption Algorithms for Concept Languages
34 pages

RR-90-05
Franz Baader
A Formal Definition for the Expressive Power of Knowledge Representation Languages
22 pages

RR-90-06
Bernhard Hollunder
Hybrid Inferences in KL-ONE-based Knowledge Representation Systems
21 pages

RR-90-07
Elisabeth André, Thomas Rist
Wissensbasierte Informationspräsentation: Zwei Beiträge zum Fachgespräch Graphik und KI:

1. Ein planbasierter Ansatz zur Synthese illustrierter Dokumente
2. Wissensbasierte Perspektivenwahl für die automatische Erzeugung von 3D-Objektdarstellungen

24 pages

RR-90-08
Andreas Dengel
A Step Towards Understanding Paper Documents
25 pages

RR-90-09
Susanne Biundo
Plan Generation Using a Method of Deductive Program Synthesis
17 pages

RR-90-10
Franz Baader, Hans-Jürgen Bürckert, Bernhard Hollunder, Werner Nutt, Jörg H. Siekmann
Concept Logics
26 pages

RR-90-11
Elisabeth André, Thomas Rist
Towards a Plan-Based Synthesis of Illustrated Documents
14 pages

RR-90-12
Harold Boley
Declarative Operations on Nets
43 pages

RR-90-13
Franz Baader
Augmenting Concept Languages by Transitive Closure of Roles: An Alternative to Terminological Cycles
40 pages

RR-90-14
Franz Schmalhofer, Otto Kühn, Gabriele Schmidt
Integrated Knowledge Acquisition from Text, Previously Solved Cases, and Expert Memories
20 pages

RR-90-15
Harald Trost
The Application of Two-level Morphology to Non-concatenative German Morphology
13 pages

RR-90-16
Franz Baader, Werner Nutt
Adding Homomorphisms to Commutative/Monoidal Theories, or: How Algebra Can Help in Equational Unification
25 pages

DFKI Technical Memos

TM-89-01
Susan Holbach-Weber
Connectionist Models and Figurative Speech
27 pages

TM-90-01
Som Bandyopadhyay
Towards an Understanding of Coherence in Multimodal Discourse
18 pages

TM-90-02
Jay C. Weber
The Myth of Domain-Independent Persistence
18 pages

TM-90-03
Franz Baader, Bernhard Hollunder
KRIS: Knowledge Representation and Inference System
-System Description-
15 pages

TM-90-04
Franz Baader, Hans-Jürgen Bürckert, Jochen Heinsohn, Bernhard Hollunder, Jürgen Müller, Bernhard Nebel, Werner Nutt, Hans-Jürgen Profitlich
Terminological Knowledge Representation: A Proposal for a Terminological Logic
7 pages

DFKI Documents

D-89-01
Michael H. Malburg & Rainer Bleisinger
HYPERBIS: ein betriebliches Hypermedia-Informationssystem
43 Seiten

D-90-01
DFKI Wissenschaftlich-Technischer Jahresbericht 1989
45 pages

D-90-02
Georg Seul
Logisches Programmieren mit Feature -Typen
107 Seiten

D-90-03
Ansgar Bernardi, Christoph Klauck, Ralf Legleitner
Abschlußbericht des Arbeitspaketes PROD
36 Seiten

D-90-04
Ansgar Bernardi, Christoph Klauck, Ralf Legleitner
STEP: Überblick über eine zukünftige Schnittstelle zum Produktdatenaustausch
69 Seiten

D-90-05
Ansgar Bernardi, Christoph Klauck, Ralf Legleitner
Formalismus zur Repräsentation von Geometrie- und Technologieinformationen als Teil eines Wissensbasierten Produktmodells
66 Seiten

Adding Homomorphisms to Commutative/Monoidal Theories, or:
How Algebra Can Help in Equational Unification

Franz Baader, Werner Nutt

RR-90-16
Research Report