Deutsches
Forschungszentrum
für Künstliche
Intelligenz GmbH

Research Report
RR-92-01

Unification in Monoidal Theories is Solving Linear Equations over Semirings

Werner Nutt

January 1992

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. The shareholder companies are Daimler Benz, Fraunhofer Gesellschaft, GMD, IBM, Insiders, Krupp-Atlas, Mannesmann-Kienzle, Philips, Sema Group Systems, Siemens and Siemens-Nixdorf. 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

Unification in Monoidal Theories is Solving Linear Equations over Semirings

Werner Nutt

DFKI-RR-92-01

This work has been supported by a grant from The Federal Ministry for Research and Technology (FKZ ITW-89030).

Unification in Monoidal Theories is Solving Linear Equations over Semirings

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

Abstract

Although unification algorithms have been developed for numerous equational theories there is still a lack of general methods. In this paper we apply algebraic techniques to the study of a whole class of theories, which we call *monoidal*. Our approach leads to general results on the structure of unification algorithms and the unification type of such theories.

An equational theory is monoidal if it contains a binary operation which is associative and commutative, an identity for the binary operation, and an arbitrary number of unary symbols which are homomorphisms for the binary operation and the identity. Monoidal theories axiomatize varieties of abelian monoids. Examples are the theories of abelian monoids (AC), idempotent abelian monoids (ACI), and abelian groups.

To every monoidal theory we associate a semiring. Intuitively, semirings are rings without subtraction. We show that every unification problem in a monoidal theory can be translated into a system of linear equations over the corresponding semiring. More specifically, problems without free constants are translated into homogeneous equations. For problems with free constants inhomogeneous equations have to be solved in addition.

Exploiting the correspondence between unification and linear algebra we give algebraic characterizations of the unification type of a theory. In particular, we show that with respect to unification without constants monoidal theories are either unitary or nullary. Applying Hilbert's Basis Theorem we prove that theories of groups with commuting homomorphisms are unitary with respect to unification with and without constants.

Contents

1 Introduction

Unification theory is concerned with problems of the following kind: Given two terms built from function symbols and variables, do there exist terms that can be substituted for the variables such that the two terms thus obtained are equal? This operation, called *unification* of terms, is the fundamental operation in automated deduction. In his seminal paper that presented the resolution calculus for first order predicate logic, Robinson [Rob65] gave an algorithm to compute a unifying substitution of two terms and proved that this *unifier* is most general in the sense that every other unifier can be obtained from it by further instantiation of variables.

Plotkin [Plo72] suggested to generalize Robinson's syntactic unification to unification modulo equationally defined first order theories as a more efficient means for equational deduction. Since then, equational unification has been built into resolution theorem provers, logic programming languages, and completion procedures for rewriting systems. In his survey, Siekmann [Sie89] gives an overview of the different applications of unification.

Unification algorithms have been designed for a number of equational theories. But in spite of the substantial body of results, the field still lacks abstraction and a reservoir of general methods. In this paper we apply algebraic techniques to investigate unification problems for a class of equational theories rather than for a single theory. Our approach leads to general results on the structure of unification algorithms and the unification type of the theories.

The class of *monoidal theories* contains several special theories that turned out useful in applications and for which special unification algorithms have been developed. An equational theory is monoidal if it contains a binary operation which is associative and commutative, an identity for the binary operation, and an arbitrary number of unary symbols which are homomorphisms for the binary operation and the identity. For instance, AC, i.e., the theory of abelian monoids, ACI, i.e., the theory of idempotent abelian monoids, and AG, i.e., the theory of abelian groups are monoidal. The varieties described by monoidal theories consist of abelian monoids. This fact motivated the name for the class.

It is well-known that AC-unification amounts to solving linear equations over the nonnegative integers [Büt86, For87, HS87, LS76, Sti75, Sti81], and unification in AG is done by solving linear equations over the integers [LBB84]. But up to now it was unclear whether the correlation between equational theories and linear equations was merely accidental or if there is some deeper structural connection. We will show that the latter is the case.

A monoidal theory $\mathcal{E}$ determines a semiring $\mathcal{S}_\mathcal{E}$, that is, an algebraic structure which can be thought of as a ring without substraction. For instance, the semirings corresponding to the theories AC, ACI, and AG are the natural numbers $\mathbf{N}$, the

boolean semiring $\mathbf{B} = \{0, 1\}$, and the ring of integers $\mathbf{Z}$, respectively. We will prove that solving unification problems without constants in $\mathcal{E}$ is equivalent to solving systems of homogeneous linear equations over $\mathcal{S}_\mathcal{E}$ and that problems with free constants give rise to inhomogeneous equation systems. Based on this result we can outline a schema for a universal unification algorithms for monoidal theories. In order to turn this schema into an effective unification algorithm for a given theory $\mathcal{E}$ one has to provide an algorithm that solves linear equations over $\mathcal{S}_\mathcal{E}$. There is a rich repertoire of algebraic techniques for solving linear equations in the mathematical literature and these can usefully be employed for unification algorithms.

Unlike the case of Robinson's syntactic unification, a single most general unifier representing all solutions need no longer exist when equalities are present. Equational theories have been classified according to the number of "most general solutions" that are needed to represent all solutions of a unification problem [Sie89]. A theory is of type *unitary* or *finitary* if one or finitely many most general solutions, respectively, are sufficient, otherwise the theory is *infinitary* or *nullary*. We will use the close correspondence between unification and linear algebra to characterize the unification type of monoidal theories algebraically: a theory $\mathcal{E}$ is unitary with respect to unification without constants if and only if the solution spaces of linear equation systems over $\mathcal{S}_\mathcal{E}$ are finitely generated; if this is not the case, the theory is nullary. Rings with similar properties have been studied extensively in algebra. A commutative ring $\mathcal{S}$ is *noetherian* if all ideals of $\mathcal{S}$ are finitely generated [Jac80]. As a consequence, the solution spaces of linear equation systems over $\mathcal{S}$ are finitely generated. A well-known result of this research is Hilbert's Basis Theorem, which we will apply to obtain a sufficient criterion for monoidal theories to be unitary—for unification with and without constants.

Baader [Baa89a] studied unification in so-called commutative theories which he defined by categorical properties. It has been shown that monoidal and commutative theories are identical modulo a signature transformation [BN91]. Therefore all results on monoidal theories apply to commutative theories as well. In his framework he proved some of the basic results on the unification type of commutative theories that are also contained in this paper. In contrast to his work, our approach clarifies the *algebraic* structure of unification problems, and thus allows us to use algebraic techniques directly for designing unification algorithms in these theories.

The paper is organized as follows. In Section 2 we briefly review basic definitions and fix our notation. In Section 3 we define monoidal theories and give examples. In Section 4 we give an abstract reformulation of unification as unification of morphisms rather than unification of terms. Section 5 presents semirings as basics of linear equations. In Section 6 we show how monoidal theories are related to semirings and develop a technique that allows us to represent morphisms by means of matrices over semirings. Section 7 treats unification problems without constants and Section 8 problems with constants. In both sections we give algebraic characterizations of

unification problems and derive schemata for algorithms. Section 8 summarizes our results.

2 Basic Notions and Notation

We briefly review the necessary notions and notation concerning preorders and unification theory, assuming that the reader is familiar with the basic concepts of universal algebra [Grä68]. A collection of papers representing the state of the art in unification theory can be found in [Kir90].

In this paper we will write composition of mappings 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 and not for the operations denoted by them). Moreover, if S, T are sets, $\phi\colon S \to T$ is a mapping, and S' is a subset of S, then $S'\phi$ denotes the set $\{a'\phi \mid a' \in S'\}$. This will simplify the notation later on.

2.1 Preorders

Some of the basic concepts of unification theory like the notion of a most general unifier and the notion of a complete or a minimal complete set of unifiers are defined in terms of a preorder on substitutions. Instead of studying this preorder directly we often will translate it into other preorders. For this purpose we provide a basic vocabulary for dealing with preorders in general.

A *preorder* is a reflexive and transitive relation. Let "$\leq$" be a preorder on a set S. We say that the elements a and a' of S are *independent* if neither $a \leq a'$ nor $a' \leq a$. The *strict part* of "$\leq$" is the relation "$<$" defined by $a < a'$ if $a \leq a'$ but not $a' \leq a$. An element $a \in S$ is *minimal* if there is no $a' \in S$ such that $a' < a$. A subset $S' \subseteq S$ is a *complete set* if for every $a \in S$ there exists some $a' \in S'$ such that $a' \leq a$. A *minimal complete set* is a complete set such that no proper subset is complete. A *least element* is an element $a \in S$ such that $a \leq a'$ for all $a' \in S$.

Obviously, complete subsets of S always exist, since S is a complete subset of itself. Minimal complete subsets, however, need not exist, but if they do exist, any two of them have equal cardinality [FH86]. If $S' \subseteq S$ is a minimal complete set, then every $a \in S'$ is minimal. A minimal complete subset of S exists if and only if the minimal elements of S form a complete subset. In other words, S has a minimal complete subset if and only if for every $a \in S$ there is a minimal element $a' \in S$ such that $a' \leq a$. If $S' \subseteq S$ is a complete set such that any two elements are independent, then S' is a minimal complete set. In particular, for any least element $a \in S$ the singleton $\{a\}$ is a minimal complete set.

2.2 Equational Theories

We assume that two disjoint infinite sets of symbols are given, namely, a set of function symbols (like f, h) and a set of variables (like x, y, z). A *signature* Σ is a finite set of function symbols each of which has a fixed arity. Every signature Σ determines a class of Σ-*algebras* and Σ-*homomorphisms*. The realization of a Σ-function symbol f in a Σ-algebra A is written as f^A. 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. Let X be a set of variables. The set of all Σ-terms with variables in X forms the term algebra $\mathcal{T}_\Sigma(X)$. If X is the set of all variables then substitutions are precisely the Σ-homomorphisms $\mathcal{T}_\Sigma(X) \to \mathcal{T}_\Sigma(X)$ that move only finitely many variables.

A Σ-*identity* is a pair $s \doteq t$ of Σ-terms. A *stable* Σ-*congruence* is a set of Σ-identities that is closed under the congruence operations and under the application of Σ-substitutions. An *equational theory* $\mathcal{E} = (\Sigma, E)$ is a pair consisting of a signature Σ and a stable congruence E on the set of all Σ-terms. We will write $s =_\mathcal{E} t$ if $s \doteq t \in E$. For every binary relation E' between Σ-terms there exists a least stable congruence E containing E'. We say that E is the stable congruence *generated by* E'. A Σ-algebra that satisfies every identity in E is called an $\mathcal{E}$-*algebra*. The set of all E-congruence classes $\overline{t}$ of Σ-terms $t \in \mathcal{T}_\Sigma(X)$ forms an $\mathcal{E}$-algebra $\mathcal{F}_\mathcal{E}(X)$ where every function symbol f is interpreted as the operation $\overline{t_1}, \ldots, \overline{t_n} \mapsto \overline{f(t_1, \ldots, t_n)}$. By abuse of notation we will often identify a term t with its congruence class $\overline{t}$ if it is clear from the context which is which.

The $\mathcal{E}$-algebra $\mathcal{F}_\mathcal{E}(X)$ is *free over* X in the following sense: for every $\mathcal{E}$-algebra A and every mapping $g\colon X \to A$ there exists a unique Σ-homomorphism $\sigma_g\colon \mathcal{F}_\mathcal{E}(X) \to A$ which extends g, that is $xg = x\sigma_g$ for all $x \in X$. For every set X, free $\mathcal{E}$-algebras are unique up to Σ-isomorphism. Therefore we call $\mathcal{F}_\mathcal{E}(X)$ *the free* $\mathcal{E}$-*algebra over the set of generators* X. If $X = \{x_1, \ldots, x_n\}$ is a finite set we sometimes write $\mathcal{F}_\mathcal{E}(x_1, \ldots, x_n)$ instead of $\mathcal{F}_\mathcal{E}(X)$.

If $X = \{x_1, \ldots, x_n\}$, then every Σ-homomorphism $\sigma\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ is uniquely determined by the images $x_i\sigma$ of the elements x_i, since $\mathcal{F}_\mathcal{E}(X)$ is free over X. Therefore we can represent σ by a substitution $\sigma' := [x_1/t_1, \ldots, x_n/t_n]$, where the terms $t_i \in \mathcal{T}_\Sigma(Y)$ are chosen such that $\overline{t_i} = x_i\sigma'$. Conversely, every substitution gives rise to a Σ-homomorphism $\sigma\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ if we put $x\sigma := \overline{x\sigma'}$. In the sequel we will identify a Σ-homomorphism between free $\mathcal{E}$-algebras with the substitution representing it, if there is no danger of confusion.

2.3 Unification

The following gives the traditional definitions of unification theory. However, later on, we will take an equivalent but more abstract approach, that will be presented

in Section 4.

A Σ-*equation* is a pair of Σ-terms written as $s \doteq t$. A Σ-*equation system* is a finite sequence of Σ-equations $\Gamma = \langle s_1 \doteq t_1, \ldots, s_n \doteq t_n \rangle$. The set of variables occurring in Σ is denoted as $\mathcal{V}(\Gamma)$.

A unification problem for an equational theory $\mathcal{E} = (\Sigma, E)$ is presented by a Σ-equation system Γ. An $\mathcal{E}$-*unifier* of Γ is a substitution δ such that $s_i\delta =_\mathcal{E} t_i\delta$ for $i = 1, \ldots, n$. We denote the set of all $\mathcal{E}$-unifiers of Γ as $U_\mathcal{E}(\Gamma)$.

Since we are only interested in equality of terms modulo the theory $\mathcal{E}$ we need not distinguish between substitutions that map variables to $\mathcal{E}$-equal terms. Given a unification problem Γ, we may also consider two unifiers as equal if they map the variables occurring in Γ to $\mathcal{E}$-equal terms. Usually we do not need the set of all $\mathcal{E}$-unifiers, but rather a subset from which all other unifiers can be generated by instantiation. To make this precise we introduce the following relations between substitutions. Let $\sigma, \tau: \mathcal{T}_\Sigma(X) \to \mathcal{T}_\Sigma(Y)$ and $\eta: \mathcal{T}_\Sigma(X) \to \mathcal{T}_\Sigma(Z)$. Then we write

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

Obviously, $\sigma =_{\mathcal{E},X} \tau$ if and only if σ and τ describe the same Σ-homomorphism $\mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ for any finite set of variables Y that contains the variables introduced by σ and τ. Moreover, it is easy to verify that "$\leq_{\mathcal{E},X}$" is a preorder.

In particular, "$\leq_{\mathcal{E},\mathcal{V}(\Gamma)}$" is a preorder on $U_\mathcal{E}(\Gamma)$. We say that a set $U \subseteq U_\mathcal{E}(\Gamma)$ is a *complete set of unifiers* or a *minimal complete set of unifiers* if U is a complete or minimal complete set with respect to the preorder "$\leq_{\mathcal{E},\mathcal{V}(\Gamma)}$". A unifier is *most general* if it is a least element of $U_\mathcal{E}(\Gamma)$. For applications one is not interested in arbitrary complete sets of unifiers but in minimal complete sets, because one wants to keep the set of unifiers under consideration as small as possible.

The *unification type* of a theory $\mathcal{E}$ is defined with reference to the existence and cardinality of minimal complete sets (see [Sie89]). A theory is $\mathcal{E}$ *infinitary* (*finitary*, or *unitary*) if for every unification problem minimal complete sets of $\mathcal{E}$-unifiers exist (and their cardinality is finite, or at most one, respectively). A theory $\mathcal{E}$ is *nullary* if there exists an $\mathcal{E}$-unification problem without a minimal complete set of $\mathcal{E}$-unifiers. These four classes form the *unification hierarchy*. Note that a theory is unitary if and only if every solvable unification problem has a most general unifier.

One may distinguish between three kinds of unification problems (cf. [Baa91]):

1. *problems without constants* or *elementary problems*, where the terms contain only symbols from the signature of the underlying theory;
2. *problems with constants*, where additional free constants may occur;

3. *problems with free function symbols*, where arbitrary function symbols not specified in the signature are allowed.

A proper formalization of the cases (2) and (3) would require to consider the problems in the theory that is obtained by adding the additional symbols to the signature.

All three variants may arise in applications. Free function symbols have to be taken into account in theorem proving, where they are introduced by skolemization, and in rewriting modulo equational theories. As shown in [Bür89], matching problems correspond to special unification problems with constants. In the present paper, we will only deal with elementary problems and problems containing free constants. Schmidt-Schauß [SS89] showed that an algorithm for arbitrary combinations of disjoint theories—and thus in particular for problems with free function symbols—can be derived from algorithms that solve problems with free constants in the individual theories.

If nothing else is specified, "unification"will always mean "unification without constants."

3 Monoidal Theories: Definitions and Examples

Monoidal theories generalize the equational theories AC, ACI, and AG. In this section we first define monoidal theories and then give examples.

An equational theory $\mathcal{E} = (\Sigma, E)$ is *monoidal* if

1. Σ contains a constant 0, a binary function symbol "+," and an arbitrary number of unary function symbols, but no other symbols
2. "+" is associative and commutative, that is, $(x + y) + z =_\mathcal{E} x + (y + z)$ and $x + y =_\mathcal{E} y + x$
3. 0 is the identity 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 $h(0) =_\mathcal{E} 0$.

A monoidal theory may contain arbitrary additional identities over Σ, the only requirement is, that *at least* the above laws hold. Monoidal theories describe varieties of abelian monoids with homomorphisms. This fact was the motivation for calling these theories "monoidal."

General Assumption. *In the rest of the paper we assume that $\mathcal{E} = (\Sigma, E)$ denotes a monoidal theory.*

Example 3.1 Suppose "+" is a binary function symbol and 0 is nullary. We consider the following signatures: $\Sigma := \{+, 0\}$; $\Sigma' := \Sigma \cup \{h\}$, where h is unary; $\Delta := \{+, 0, -\}$, where $-$ is unary; $\Delta' := \Delta \cup \{h\}$, where h is unary; and $\Omega := \{+, 0, i\}$, where i is unary.

AC $= (\Sigma, E_{\mathrm{AC}})$, where E_{AC} is generated by the associativity, commutativity, and identity laws for "+" and 0, axiomatizes the theory of *abelian monoids*. It is the least monoidal theory in that its signature contains no unary symbol and only the identities of the definition hold.

ACI $= (\Sigma, E_{\mathrm{ACI}})$ is the theory of *idempotent abelian monoids*. The congruence E_{ACI} is the least one that contains E_{AC} and the idempotence law $x + x \doteq x$.

AG $= (\Delta, E_{\mathrm{AG}})$ is the theory of *abelian groups*. E_{AG} is generated by the identities which state that "+" is the binary operation of an abelian group with neutral element 0 and inverse $-$.

ACH $= (\Sigma', E_{\mathrm{ACH}})$, the theory of *abelian monoids with homomorphism*, extends AC by the homomorphism laws for the symbol h.

AGH $= (\Delta, E_{\mathrm{AG}})$, the theory of *abelian groups with homomorphism*, extends AG by the homomorphism laws for the symbol h.

GAUSS $= (\Omega, E_{\mathrm{GAUSS}})$, where E_{GAUSS} is generated by the identities which state that "+" is associative and commutative with identity 0, that i is a homomorphism for "+", and by the identity $x + i(i(x)) \doteq 0$.

□

A monoidal theory $\mathcal{E}$ is a *theory with commuting homomorphisms* if for all unary function symbols h, $h' \in \Sigma$ we have $h(h'(x)) =_{\mathcal{E}} h'(h(x))$. A monoidal theory $\mathcal{E}$ is a *group theory* if for some term t we have $x + t =_{\mathcal{E}} 0$. Intuitively, in a group theory, there exist inverse elements for addition.

Example 3.2 With the exception of AGH, all theories in Example 3.1 have at most one unary function symbol. Thus, they are trivially theories with commuting homomorphisms. By some straightforward equational deduction one can show that $h(-x) =_{\mathrm{AGH}} -h(x)$. Hence, also in AGH homomorphisms commute.

The theories AG, AGH, and GAUSS are group theories. □

4 An Abstract View of Unification

Commonly, unification is understood as unification of terms by means of substitutions, taking account of an equational theory $\mathcal{E} = (\Sigma, E)$ (cf. Subsection 2.3). However, in this paper we will conceive it as unification of Σ-homomorphisms between free $\mathcal{E}$-algebras by means of Σ-homomorphisms. Similar reformulations of unification have been given by Rydeheard and Burstall [RB85], Goguen [Gog89], and Baader [Baa89a].

Let $\mathcal{E} = (\Sigma, E)$ be an equational theory, $\Gamma = \langle s_1 \doteq t_1, \ldots, s_n \doteq t_n \rangle$ be a Σ-equation system, and let $Y := \mathcal{V}(\Gamma)$. Suppose the substitution δ is an $\mathcal{E}$-unifier of Γ. Then $s_i\delta =_\mathcal{E} t_i\delta$ for $i = 1, \ldots, n$. Obviously, the $\mathcal{E}$-unification problem Γ is invariant under $\mathcal{E}$-equality in the following sense. If Γ' is obtained from Γ by replacing the terms s_i, t_i by terms s_i', t_i', respectively, such that $s_i =_\mathcal{E} s_i'$ and $t_i =_\mathcal{E} t_i'$, then δ is also a unifier of Γ'. Similarly, if δ' is a substitution with $\delta' =_{\mathcal{E},Y} \delta$, then δ' is also a unifier of Γ and Γ'.

A possible way to account for this invariance would be to assume that a unification problem is given by a sequence $\overline{\Gamma} = \langle \overline{s}_1 \doteq \overline{t}_1, \ldots, \overline{s}_n \doteq \overline{t}_n \rangle$ of equations between elements of $\mathcal{F}_\mathcal{E}(Y)$ and to define a unifier of such a problem as a Σ-homomorphism $\delta\colon \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$ satisfying $\overline{s}_i\delta = \overline{t}_i\delta$ for $i = 1, \ldots, n$. An equivalent but more elegant way is the following: Let $X = \{x_1, \ldots, x_n\}$ be a set of cardinality n. Define $\sigma, \tau\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ as the Σ-homomorphisms satisfying $x_i\sigma = \overline{s}_i$ and $x_i\tau = \overline{t}_i$. Since $\mathcal{F}_\mathcal{E}(X)$ is free over X, σ and τ are uniquely determined by this condition. Conversely, $\overline{s}_i$ and $\overline{t}_i$ can be reconstructed from σ and τ as the values of the elements x_i.

Now, it is easy to see that a Σ-homomorphism $\delta\colon \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$ is a unifier of $\overline{\Gamma}$ if and only if $\sigma\delta = \tau\delta$. Actually, if $\sigma\delta = \tau\delta$, then $\overline{s}_i\delta = x_i\sigma\delta = x_i\tau\delta = \overline{t}_i\delta$ for $i = 1, \ldots, n$. Conversely, if for all i we have $\overline{s}_i\delta = \overline{t}_i\delta$, it follows that for all i we have $x_i\sigma\delta = x_i\tau\delta$. Thus, $\sigma\delta$ and $\tau\delta$ agree on the generators of $\mathcal{F}_\mathcal{E}(X)$ and therefore are equal.

The above discussion motivates the following definition. An *$\mathcal{E}$-unification problem* is a parallel pair $\sigma, \tau\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ of Σ-homomorphisms between finitely generated free $\mathcal{E}$-algebras. An *$\mathcal{E}$-unifier* of σ and τ is a Σ-homomorphism $\delta\colon \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$ such that $\sigma\delta = \tau\delta$.

We say that δ is *more general* than a Σ-homomorphism $\eta\colon \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z')$ if there exists some Σ-homomorphism $\lambda\colon \mathcal{F}_\mathcal{E}(Z) \to \mathcal{F}_\mathcal{E}(Z')$ such that $\eta = \delta\lambda$. In this case we write $\delta \leq \eta$. It is easy to verify that "$\leq$" is a preorder and that for two Σ-substitutions $\delta', \eta'\colon \mathcal{T}_\Sigma(X) \to \mathcal{T}_\Sigma(Y)$ we have $\delta' \leq_{\mathcal{E},X} \eta'$ if and only if the corresponding Σ-homomorphisms δ, η satisfy $\delta \leq \eta$. Therefore, one can equivalently define complete and minimal complete sets of unifiers as well as the unification type of a theory in terms of the preorder "$\leq$".

5 Basic Structures for Linear Equations: Semirings

Since unification in monoidal theories will be based on solving linear equations over semirings, we give a short introduction to these structures. In the literature, the theory of linear equations is usually developed as the theory of fields, vector spaces, and linear mappings. Few text books base the theory, more generally, on rings instead of fields (see e.g. [Jac74]). However, there exists no thorough presentation of linear algebra over semirings. Kuich and Salomaa [KS85] use semirings to study formal languages but are not concerned with linear equations of the kind we want to consider.

5.1 Semirings

A *semiring* is a set $\mathcal{S}$ with distinct elements 0 and 1 that is equipped with two binary operations "$+$" and "$\cdot$" such that $(\mathcal{S}, +, 0)$ is a commutative monoid, $(\mathcal{S}, \cdot, 1)$ is a monoid, and all α, β, $\gamma \in \mathcal{S}$ satisfy the identities

1. $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$ *(right distributivity)*
2. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ *(left distributivity)*
3. $0 \cdot \alpha = \alpha \cdot 0 = 0$ *(zero laws).*

We call the binary operations "$+$" and "$\cdot$" the *addition* and the *multiplication* of the semiring, respectively. The elements 0 and 1 are called *zero* and *unit*. In the sequel we will often omit the "$\cdot$" sign and write $\alpha\beta$ instead of $\alpha \cdot \beta$.

A semiring is *commutative* if its multiplication is commutative. Semirings are different from rings in that they need not be groups with respect to addition. In contrast to rings, we cannot deduce the zero laws from the rest of the axioms.

Example 5.1 The *natural numbers* (i.e., the nonnegative integers) form a semiring $\mathbf{N}$ if the operations are interpreted in the obvious way.

The *boolean semiring* $\mathbf{B}$ consists of the two elements 0 and 1. In addition to the semiring laws it satisfies $1 + 1 = 1$. The semirings $\mathbf{N}$ and $\mathbf{B}$ are *proper* in the sense that they are not rings.

Every *ring* is a semiring. In particular, the *ring of integers* $\mathbf{Z}$ is a semiring. The *ring of gaussian numbers* $\mathbf{Z} \oplus i\mathbf{Z}$, which consists of complex numbers $m + in$ where $m, n \in \mathbf{Z}$, is a semiring, too.

For every semiring $\mathcal{S}$ one can construct the semiring $\mathcal{S}[X]$ of *polynomials* in the indeterminate X with coefficients from $\mathcal{S}$. □

5.2 Modules

Modules over semirings are a generalization of vector spaces over fields. As in the case of non-commutative fields, where one has to distinguish between left and right vector spaces, we will define left and right modules.

A *left (right) module* over a semiring $\mathcal{S}$ is a commutative monoid $(M, +, 0)$ together with a scalar multiplication

$$\mathcal{S} \times M \to M \qquad (\alpha, a) \mapsto \alpha a \qquad\qquad (\ M \times \mathcal{S} \to M \qquad (a, \alpha) \mapsto a\alpha\ )$$

such that for all α, $\beta \in \mathcal{S}$ and a, $b \in M$ the identities (1) to (6) ((1′) to (6′)) hold:

1.	$(\alpha \cdot \beta)a = \alpha(\beta a)$	1′.	$a(\alpha \cdot \beta) = (a\alpha)\beta$
2.	$(\alpha + \beta)a = \alpha a + \beta a$	2′.	$a(\alpha + \beta) = a\alpha + a\beta$
3.	$\alpha(a + b) = \alpha a + \alpha b$	3′.	$(a + b)\alpha = a\alpha + b\alpha$
4.	$\alpha 0 = 0$	4′.	$0\alpha = 0$
5.	$1a = a$	5′.	$a1 = a$
6.	$0a = 0$	6′.	$a0 = 0.$

Example 5.2 The singleton $\{0\}$ is a left (right) module over $\mathcal{S}$ if the scalar multiplication is defined in the obvious way. We call it the *zero module* and denote it as 0.

For a finite set X we denote by $\mathcal{S}^X$ the set of tuples over $\mathcal{S}$ which are indexed by the elements of X. The set $\mathcal{S}^X$ is turned into a left (right) $\mathcal{S}$-module if we define the addition componentwise and the left scalar multiplication by $\alpha(\beta_x)_{x\in X} := (\alpha \cdot \beta_x)_{x\in X}$ (and the right one by $((\beta_x)_{x\in X})\alpha := (\beta_x \cdot \alpha)_{x\in X}$). The *y-th unit vector* $e_y \in \mathcal{S}^X$ is the tuple $(\alpha_x)_{x\in X}$ where $\alpha_y = 1$ and $\alpha_x = 0$ for $x \neq y$. Note that $\mathcal{S}^\emptyset$ is a singleton. We identify $\mathcal{S}^\emptyset$ with 0. □

Next we introduce structure preserving mappings between left (right) modules M, N. Recall that function application is written in suffix notation. A mapping $\sigma\colon M \to N$ is *left (right) linear* if all $\alpha \in \mathcal{S}$ and all a, $b \in M$ satisfy the identities (1), (2), and (3) ((1), (2′), and (3)):

1. $(a+b)\sigma = a\sigma + b\sigma$
2. $(\alpha a)\sigma = \alpha(a\sigma)$ 2′. $(a\alpha)\sigma = (a\sigma)\alpha$
3. $0\sigma = 0$.

In the above definitions, left and right modules are distinguished by the fact that semiring elements are applied in the first case to the left and in the second case to the right of module elements. An equivalent way of defining right modules is to introduce them in the same way as left modules with the only exception that identity (1) is replaced by the identity

1′. $(\alpha \cdot \beta)a = \beta(\alpha a)$.

For commutative semirings, identities (1) and (1′) are equivalent. In this case, there is only a notational difference between left and right modules and left and right linear mappings.

Many important properties of vector spaces over fields do not carry over to arbitrary modules over semirings. For instance, there is no one-to-one correspondence between matrices and linear mappings. Fortunately, we retain many nice properties if we restrict ourselves to free modules.

A left (right) module F is *free over a set of generators* $X \subseteq F$ if for every left (right) module M and every mapping $g: X \to M$ there is a unique left (right) linear mapping $\sigma_g: F \to M$ such that $x\sigma_g = xg$ for all $x \in X$. If F, F' are left (right) $\mathcal{S}$-modules such that F is free over X and F' is free over X', then F and F' are isomorphic if there exists a bijection between X and X'.

Since a free module is determined by its generators up to isomorphism, we will talk about *the* free left (right) $\mathcal{S}$-module over X for any given set X.

Proposition 5.3 *If X is finite then $\mathcal{S}^X$ with left (right) scalar multiplication is the free left (right) $\mathcal{S}$-module over $\{e_x \mid x \in X\}$.*

Proof. Let M be a left $\mathcal{S}$-module and $g: \{e_x \mid x \in X\} \to M$ be a mapping. Define $\sigma_g: \mathcal{S}^X \to M$ by $((\alpha_x)_{x\in X})\sigma_g := \sum_{x\in X} \alpha_x(e_x g)$. Then it is easy to see that σ_g is left linear. On the other hand, since for every $a = (\alpha_x)_{x\in X} \in \mathcal{S}^X$ we have $a = \sum_{x\in X} \alpha_x e_x$, it follows that for any left linear mapping $\tau: \mathcal{S}^X \to M$ satisfying $e_x\tau = e_x g$ the equation $a\tau = (\sum_{x\in X} \alpha_x e_x)\tau = \sum_{x\in X} \alpha_x(e_x\tau) = \sum_{x\in X} \alpha_x(e_x g) = a\sigma_g$ holds.

The case of right modules is treated analogously. □

5.3 Matrices

We compute with linear mappings by means of matrices. As long as we deal with linear mappings between finitely generated free modules the correspondence between linear mappings and matrices is the same as in linear algebra over fields.

A left linear mapping $\sigma: \mathcal{S}^X \to \mathcal{S}^Y$ can be described by an $X \times Y$-matrix C_σ with entries from $\mathcal{S}$ as follows: the x-th row of $C_\sigma = (\sigma_{xy})_{x \in X, y \in Y}$ contains the components of $e_x\sigma$, the image of the x-th unit vector e_x under σ. Following the usual rules of matrix and vector multiplication we have $a\sigma = aC_\sigma$ where $a \in \mathcal{S}^X$ is written as a row vector. Conversely, every $X \times Y$-matrix C defines a left linear mapping $\sigma_C: \mathcal{S}^X \to \mathcal{S}^Y$ by $a\sigma_C := aC$.

If σ is right linear we have to slightly modify the construction. We take C_σ as the $Y \times X$-matrix that has the components of $e_x\sigma$ in the x-th column. Then $a\sigma = C_\sigma a$, where $a \in \mathcal{S}^X$ is written as a column vector. For commutative semirings both constructions are equivalent, in linear algebra over commutative fields the second one is more common.

If $\sigma, \tau: \mathcal{S}^X \to \mathcal{S}^Y$ are left (right) linear, the pointwise sum of σ and τ is the mapping $\sigma + \tau: \mathcal{S}^X \to \mathcal{S}^Y$ defined by $a(\sigma + \tau) := a\sigma + a\tau$ for all $a \in \mathcal{S}^X$. The pointwise sum $\sigma + \tau$ is again left (right) linear and $C_{\sigma+\tau} = C_\sigma + C_\tau$. If in addition $\eta: \mathcal{S}^Y \to \mathcal{S}^Z$ is left (right) linear, then the composition $\sigma\tau$ is again left (right) linear and $C_{\sigma\eta} = C_\sigma C_\eta$. Conversely, for all matrices B, C, D over $\mathcal{S}$ we have $\sigma_{B+C} = \sigma_B + \sigma_C$ and $\sigma_{CD} = \sigma_C\sigma_D$.

For any left (right) linear mapping $\sigma: \mathcal{S}^X \to \mathcal{S}^Y$ the *dual mapping* of σ is the right (left) linear mapping $\sigma^*: \mathcal{S}^Y \to \mathcal{S}^X$ defined by $a\sigma^* := C_\sigma a$ $(:= aC_\sigma)$. It follows that $(\sigma + \tau)^* = \sigma^* + \tau^*$, $(\sigma\eta)^* = \eta^*\sigma^*$, and $\sigma^{**} = \sigma$. Moreover, we have $\sigma = \tau$ if and only if $\sigma^* = \tau^*$. Note that σ and σ^* are given by the same matrix and that C_{σ^*} is not the transpose of C_σ.

6 Monoidal Theories and Semirings

In this section we construct for every monoidal theory $\mathcal{E} = (\Sigma, E)$ a canonical semiring $\mathcal{S}_\mathcal{E}$ such that Σ-homomorphisms between free $\mathcal{E}$-algebras can be described by matrices over $\mathcal{S}_\mathcal{E}$. This fact will be used in the following sections to investigate unification problems using algebraic techniques.

6.1 Monoidal Theories Define Semirings

It has been shown that AC-unification amounts to solving linear equations over the semiring $\mathbf{N}$ [Büt86, For87, HS87, LS76, Sti75, Sti81] and that unification in

the theory of abelian groups amounts to solving linear equations over the ring $\mathbf{Z}$ [LBB84]. We will generalize these results by associating to every monoidal theory $\mathcal{E}$ a semiring $\mathcal{S}_\mathcal{E}$, that will be used to solve unification problems in $\mathcal{E}$ later on.

In order to define $\mathcal{S}_\mathcal{E}$ we need some preliminary definitions and results. Suppose A, B are Σ-algebras and $\sigma, \tau: A \to B$ are Σ-homomorphisms. The *pointwise sum* of σ and τ is the mapping $\sigma + \tau: A \to B$ defined by $a(\sigma + \tau) := a\sigma +^B a\tau$ for all $a \in A$. The mapping that maps every element of A to 0^B is denoted as 0_{AB}. If $A = B$ we write 0_A instead of 0_{AA}. The following propositions are straightforward gerneralization of well-known results for abelian monoids.

Proposition 6.1 *Suppose A, B are $\mathcal{E}$-algebras. Then:*

1. *$0_{AB}: A \to B$ is a Σ-homomorphism*
2. *For all Σ-homomorphisms $\sigma, \tau: A \to B$ the pointwise sum $\sigma + \tau$ is again a Σ-homomorphism.*

Proof. 1. It follows easily from the definition of monoidal theories that 0_{AB} is a Σ-homomorphism.

2. We show that $\sigma + \tau$ is compatible with the operations in Σ. For the nullary operation 0 we have

$$0^A(\sigma + \tau) = 0^A\sigma +^B 0^A\tau = 0^B +^B 0^B = 0^B,$$

using the fact that σ and τ are Σ-homomorphisms.

For the binary operation "+" we deduce for $a, b \in A$ that

$$\begin{aligned}
(a +^A b)(\sigma + \tau) &= (a +^A b)\sigma +^B (a +^A b)\tau \\
&= a\sigma +^B b\sigma +^B a\tau +^B b\tau \qquad (1) \\
&= a\sigma +^B a\tau +^B b\sigma +^B b\tau \qquad (2) \\
&= a(\sigma + \tau) +^B b(\sigma + \tau),
\end{aligned}$$

exploiting in (1) the fact that σ and τ are Σ-homomorphisms and in (2) the associativity and commutativity of $+^A$.

For any unary operation h and any $a \in A$ we deduce that

$$\begin{aligned}
(h^A(a))(\sigma + \tau) &= (h^A(a))\sigma +^B (h^A(a))\tau \\
&= h^B(a\sigma) +^B h^B(a\tau) \qquad (3) \\
&= h^B(a\sigma +^B a\tau) \qquad (4) \\
&= h^B(a(\sigma + \tau)),
\end{aligned}$$

exploiting in (3) that σ and τ are Σ-homomorphisms and in (4) that h^B is a homomorphism for $+^B$. □

Proposition 6.2 *Suppose A, B, C are Σ-algebras and $\sigma, \sigma' \colon A \to B$ and $\tau, \tau' \colon B \to C$ are Σ-homomorphisms. Then:*

1. $\sigma(\tau + \tau') = \sigma\tau + \sigma\tau'$
2. $(\sigma + \sigma')\tau = \sigma\tau + \sigma'\tau$
3. $\sigma 0_{BC} = 0_{AB}\tau = 0_{AC}$

Proof. 1. Applying the definition of pointwise addition we obtain for $a \in A$

$$a(\sigma(\tau + \tau')) = (a\sigma)(\tau + \tau') = a\sigma\tau +^C a\sigma\tau' = a(\sigma\tau + \sigma\tau').$$

2. For $a \in A$ we deduce that

$$\begin{aligned} a((\sigma + \sigma')\tau) = (a(\sigma + \sigma'))\tau &= (a\sigma +^B a\sigma')\tau && (1)\\ &= a\sigma\tau +^C a\sigma'\tau && (2)\\ &= a(\sigma\tau + \sigma'\tau), && (3) \end{aligned}$$

using in (1) and (3) the definition of pointwise addition and in (2) the fact that τ is a Σ-homomorphism.

3. Trivially, $\sigma 0_{BC} = 0_{AC}$. The equality $0_{AB}\tau = 0_{AC}$ holds, because τ is a Σ-homomorphism. □

For every $\mathcal{E}$-algebra A we denote the set of all Σ-homomorphisms from A to A by *end* A. An element of *end* A is an *endomorphism* on A. Endomorphisms inherit the monoid structure from A: with the pointwise addition of mappings "+", the endomorphisms on A form an abelian monoid, whose identity is the mapping 0_A. Moreover, with respect to the composition of mappings "$\circ$", *end* A is a monoid, whose identity is id_A.

Proposition 6.3 *Let A be an $\mathcal{E}$-algebra. Then $(\mathit{end}\, A, +, 0_A, \circ, id_A)$ is a semiring.*

Proof. As already shown, $(\mathit{end}\, A, +, 0_A)$ is an abelian monoid and $(\mathit{end}\, A, \circ, id_A)$ is a monoid. In addition, Proposition 6.2 implies that the distributitivity and the zero laws hold. □

We are now ready to introduce canonical semirings. Let u be a distinguished variable. By Proposition 6.3, the endomorphisms of $\mathcal{F}_\mathcal{E}(u)$ form a semiring. We call the semiring *end* $\mathcal{F}_\mathcal{E}(u)$ the *canonical semiring* of $\mathcal{E}$ and denote it as $\mathcal{S}_\mathcal{E}$. To ease our notation, we shall write 0 instead of $0_{\mathcal{F}_\mathcal{E}(u)}$ and 1 instead of $id_{\mathcal{F}_\mathcal{E}(u)}$ in the sequel.

Since $\mathcal{F}_\mathcal{E}(u)$ is free over $\{u\}$, every endomorphism α on $\mathcal{F}_\mathcal{E}(u)$ is uniquely determined by $u\alpha$. Conversely, every term $t \in \mathcal{T}_\Sigma(u)$ determines an element α_t of

$\mathcal{S}_\mathcal{E}$—that is an endomorphism on $\mathcal{F}_\mathcal{E}(u)$—which satisfies $u\alpha_t =_\mathcal{E} t$. Obviously, for any two terms t, t' we have $\alpha_t = \alpha_{t'}$ if and only if $t =_\mathcal{E} t'$. Observe that for the multiplication in $\mathcal{S}_\mathcal{E}$ we have $\alpha_s\alpha_t = \alpha_{s[u/t]}$.

Example 6.4 Let us look more closely at the canonical semirings that correspond to the monoidal theories as introduced in Example 3.1.

$\mathcal{S}_{\mathrm{AC}}$, the canonical semiring of the theory of abelian monoids, is isomorphic to the semiring of natural numbers $\mathbf{N}$. To show this we use the following notation. For $m \in \mathbf{N}$ let

$$um := \underbrace{u + \cdots + u}_{m \text{ times}},$$

where $u0$ is understood as 0. Consider now an arbitrary element $\alpha \in \mathcal{S}_{\mathrm{AC}}$, that is, a Σ-homomorphism $\alpha\colon \mathcal{F}_{\mathrm{AC}}(u) \to \mathcal{F}_{\mathrm{AC}}(u)$. Then α is uniquely determined by the value $u\alpha$. Since $u\alpha \in \mathcal{F}_{\mathrm{AC}}(u)$, there exists a number $m \in \mathbf{N}$ such that $u\alpha =_{\mathrm{AC}} um$. If $\beta \in \mathcal{S}_{\mathrm{AC}}$ is an endomorphism such that $u\beta =_{\mathrm{AC}} un$, then it is easy to see that $u(\alpha+\beta) =_{\mathrm{AC}} u(m+n)$ and that $u(\alpha\beta) =_{\mathrm{AC}} u(mn)$. Moreover, one easily checks that $m = n$ if $um =_{\mathrm{AC}} un$, and that for every $m \in \mathbf{N}$ there is an $\alpha in \mathcal{S}_{\mathrm{AC}}$ such that $um =_{\mathrm{AC}} u\alpha$. It follows that $\mathcal{S}_{\mathrm{AC}}$ and $\mathbf{N}$ are isomorphic semirings.

$\mathcal{S}_{\mathrm{ACI}}$, which corresponds to the theory of idempotent abelian monoids, is isomorphic to the boolean semiring $\mathbf{B}$. To see this observe that for every $\alpha \in \mathcal{S}_{\mathrm{ACI}}$ we either have $u\alpha =_{\mathrm{ACI}} 0$ or $u\alpha =_{\mathrm{ACI}} u$. Hence, $\mathcal{S}_{\mathrm{ACI}}$ has only the two elements 0 and 1. The idempotence law implies that $1 + 1 = 1$. Thus we have $\mathcal{S}_{\mathrm{ACI}} \simeq \mathbf{B}$.

$\mathcal{S}_{\mathrm{AG}}$, the semiring corresponding to the theory of abelian groups, is isomorphic to $\mathbf{Z}$, the semiring of integers. This can be seen using similar arguments as in the proof showing that $\mathcal{S}_{\mathrm{AC}} \simeq \mathbf{N}$. One has to observe that for every $\alpha \in \mathcal{S}_{\mathrm{AG}}$ there exists an integer m such that $u\alpha =_{\mathrm{AG}} um$, where um is defined in the obvious way.

$\mathcal{S}_{\mathrm{ACH}}$, the canonical semiring of the theory of abelian monoids with a homomorphism, is isomorphic to $\mathbf{N}[X]$, the semiring of polynomials in one indeterminate X with nonnegative integer coefficients. To see this, consider an arbitrary element $\alpha \in \mathcal{S}_{\mathrm{ACH}}$, that is a Σ-homomorphism $\alpha\colon \mathcal{F}_{\mathrm{ACH}}(u) \to \mathcal{F}_{\mathrm{ACH}}(u)$. Then, there exist $m_1, \ldots, m_k \in \mathbf{N}$ such that $u\alpha =_{\mathrm{ACH}} um_0 + h(u)m_1 + \cdots + h^k(u)m_k$. We associate with α the polynomial $p_\alpha = m_0 + m_1X^1 + \cdots + m_kX^k$, which is an element of $\mathbf{N}[X]$. It is straightforward to prove that mapping every $\alpha \in \mathcal{S}_{\mathrm{ACH}}$ to the polynomial $p_\alpha \in \mathbf{N}[X]$ yields a semiring isomorphism between $\mathcal{S}_{\mathrm{ACH}}$ and $\mathbf{N}[X]$.

$\mathcal{S}_{\text{AGH}}$, the canonical semiring of the theory of abelian groups with a homomorphism, is isomorphic to $\mathbf{Z}[X]$, the semiring of polynomials in one indeterminate X with nonnegative integer coefficients. This can be seen as in the previous example.

$\mathcal{S}_{\text{GAUSS}}$, which corresponds to the theory GAUSS, is isomorphic to the ring of gaussian numbers $\mathbf{Z} \oplus i\mathbf{Z}$ consisting of the complex numbers $m+in$, where $m, n \in \mathbf{Z}$. To see this, note that the canonical semiring of GAUSS is isomorphic to the quotient semiring of $\mathbf{N}[X]$ that results from identifying the polynomials $1+X^2$ and 0. This quotient is isomorphic to the ring $\mathbf{Z} \oplus i\mathbf{Z}$. An isomorphism is obtained by mapping the class of X to the imaginary number i. It follows that the polynomial X^2 is mapped to the number -1.

□

As in the above examples, the canonical semiring $\mathcal{S}_\mathcal{E}$ mirrors properties of $\mathcal{E}$.

Proposition 6.5 *$\mathcal{S}_\mathcal{E}$ is a ring if and only if $\mathcal{E}$ is a group theory.*

Proof. "$\Rightarrow$" If $\mathcal{S}_\mathcal{E}$ is a ring, then there exists some $\alpha \in \mathcal{S}_\mathcal{E}$ such that $1 + \alpha = 0$. Let t be a term such that $t =_\mathcal{E} u\alpha$. Then $u + t = u1 + u\alpha = u(1 + \alpha) =_\mathcal{E} u0 = 0$. That is, there exists a term t such that $u + t =_\mathcal{E} 0$. Hence, $\mathcal{E}$ is a group theory.

"$\Leftarrow$" If $\mathcal{E}$ is a group theory, there is a term s such that $u + s =_\mathcal{E} 0$. Let $x_1, \ldots, x_n$ be the variables occurring in s and let $t := s[x_1/u, \ldots, x_n/u]$. Then we have $t \in \mathcal{T}_\Sigma(u)$ and $u + t =_\mathcal{E} 0$. Hence, $u(1 + \alpha_t) = 0$. From this it follows that for any $\beta \in \mathcal{S}_\mathcal{E}$ the endomorphism $\beta\alpha_t$ is an inverse with respect to addition, since $\beta + \beta\alpha_t = \beta(1 + \alpha_t) = \beta 0 = 0$. □

Proposition 6.6 *$\mathcal{S}_\mathcal{E}$ is commutative if and only if $\mathcal{E}$ is a theory with commuting homomorphisms.*

Proof. "$\Rightarrow$" Let $\mathcal{S}_\mathcal{E}$ be commutative and let h, h' be unary symbols from Σ. Then we have $\alpha_{h(u)}\alpha_{h'(u)} = \alpha_{h'(u)}\alpha_{h(u)}$. This implies $h(h'(u)) = u\alpha_{h(u)}\alpha_{h'(u)} =_\mathcal{E} u\alpha_{h'(u)}\alpha_{h(u)} = h'(h(u))$. Hence, $\mathcal{E}$ is a theory with commuting homomorphisms.

"$\Leftarrow$" The semiring $\mathcal{S}_\mathcal{E}$ is generated by the elements that are of the form $\alpha_{h(u)}$ for some unary function symbol $h \in \Sigma$. Since homomorphisms commute, we have $\alpha_{h(u)}\alpha_{h'(u)} = \alpha_{h(h'(u))} = \alpha_{h'(h(u))} = \alpha_{h'(u)}\alpha_{h(u)}$ for all unary symbols h, $h' \in \Sigma$. Hence, $\mathcal{S}_\mathcal{E}$ has a set of commuting generators. This implies that $\mathcal{S}_\mathcal{E}$ is commutative. □

Finally we show that the concept of a monoidal theory and the concept of a semiring are equally general.

Proposition 6.7 *For every semiring $\mathcal{S}$ there exists a monoidal theory $\mathcal{E}$ such that $\mathcal{S}$ and $\mathcal{S}_\mathcal{E}$ are isomorphic.*

Proof. If $\mathcal{S}$ is a semiring, let Σ be the signature containing the symbols 0 and "+"and for every $\beta \in \mathcal{S}$ a unary symbol h_β. Let E be the set of identities that hold over $\mathcal{S}$ if 0 and "+"are interpreted as zero and addition and every unary symbol h_β is interpreted such that $h_\beta^\mathcal{S}(\gamma) = \beta \cdot \gamma$ for all $\gamma \in \mathcal{S}$. Then $\mathcal{E} = (\Sigma, E)$ is a monoidal theory.

We are going to show that $\mathcal{S}$ and $\mathcal{S}_\mathcal{E}$ are isomorphic. First, observe that by definition of $\mathcal{E}$ the following identities hold for all $\beta, \gamma \in \mathcal{S}$:

$$0 =_\mathcal{E} h_0(u) \tag{1}$$
$$u =_\mathcal{E} h_1(u) \tag{2}$$
$$h_\beta(u) + h_\gamma(u) =_\mathcal{E} h_{\beta+\gamma}(u) \tag{3}$$
$$h_\beta(h_\gamma(u)) =_\mathcal{E} h_{\beta\gamma}(u). \tag{4}$$

Next we define a mapping $\chi: \mathcal{S} \to end\, \mathcal{F}_\mathcal{E}(u)$ by $\beta\chi := \alpha_{h_\beta(u)}$. We will show that χ is a semiring isomorphism.

Using identities (1) to (4) one can prove by induction that for every term $t \in \mathcal{T}_\Sigma(u)$ there is an element $\beta \in \mathcal{S}$ such that $t =_\mathcal{E} h_\beta(u)$. Since every endomorphism on $\mathcal{F}_\mathcal{E}(u)$ has the form α_t for some $t \in \mathcal{T}_\Sigma(u)$ this proves that χ is surjective.

To prove injectivity it suffices to show that $\beta = \gamma$ if $h_\beta(u) =_\mathcal{E} h_\gamma(u)$. If $h_\beta(u) =_\mathcal{E} h_\gamma(u)$, then the definition of $\mathcal{E}$ implies that $h_\beta^\mathcal{S}$ and $h_\gamma^\mathcal{S}$ are the same functions on $\mathcal{S}$. Hence, $\beta = \beta \cdot 1 = h_\beta^\mathcal{S}(1) = h_\gamma^\mathcal{S}(1) = \gamma \cdot 1 = \gamma$, which yields the claim.

Finally, from the identities (1) to (4) it follows that χ is a semiring homomorphism. As examples, we give the proofs that χ respects 0 and multiplication. From $h_0(u) =_\mathcal{E} 0$ we conclude that $0\chi = \alpha_{h_0(u)} = \alpha_0 = 0$. From $h_{\beta\gamma}(u) =_\mathcal{E} h_\beta(h_\gamma(u))$ we conclude that $(\beta\gamma)\chi = \alpha_{h_{\beta\gamma}(u)} = \alpha_{h_\beta(h_\gamma(u))} = \alpha_{h_\beta(u)}\alpha_{h_\gamma(u)} = (\beta\chi)(\gamma\chi)$. □

The above theorem can be interpreted in such a way that the concept of monoidal theory is general enough to cover all equational theores where unification consists in solving linear equations over semirings.

6.2 Σ-Homomorphisms and Left Linear Mappings

The aim of this subsection is to relate Σ-homomorphisms between free $\mathcal{E}$-algebras to left linear mappings between free left $\mathcal{S}_\mathcal{E}$-modules. Since unification problems, as we reformulated them in Section 4, are about Σ-homomorphisms between free $\mathcal{E}$-algebras, this allows us to translate unification problems into algebraic problems.

More precisely, we will associate to every Σ-homomorphism $\sigma\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ a unique left linear mapping $\sigma^{\mathrm{lin}}\colon \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$. Moreover, $\cdot^{\mathrm{lin}}$ will be such that

- $(id_{\mathcal{F}_\mathcal{E}(X)})^{\mathrm{lin}} = id_{\mathcal{S}_\mathcal{E}^X}$
- $(\sigma\tau)^{\mathrm{lin}} = \sigma^{\mathrm{lin}}\tau^{\mathrm{lin}}$.

Conversely, we will associate to every left linear mapping $\sigma\colon \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ a unique Σ-homomorphism $\sigma^{\mathrm{hom}}\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$. Moreover, $\cdot^{\mathrm{hom}}$ will be such that

- $(id_{\mathcal{S}_\mathcal{E}^X})^{\mathrm{hom}} = id_{\mathcal{F}_\mathcal{E}(X)}$
- $(\sigma\tau)^{\mathrm{hom}} = \sigma^{\mathrm{hom}}\tau^{\mathrm{hom}}$.

Both operations will be shown to be mutually inverse, that is, $\sigma^{\mathrm{lin}\,\mathrm{hom}} = \sigma$ and $\tau^{\mathrm{hom}\,\mathrm{lin}} = \tau$ for any Σ-homomorphism σ and any left linear mapping τ.

Using the terminology of category theory, we are going to show that the category of finitely generated $\mathcal{E}$-algebras and the category of finitely generated left $\mathcal{S}_\mathcal{E}$-modules are isomorphic and that $\cdot^{\mathrm{lin}}$ and $\cdot^{\mathrm{hom}}$ are mutually inverse functors between these categories.

The basic idea in establishing this relationship is to present a Σ-homomorphism between arbitrary finitely generated $\mathcal{E}$-algebras by an $X \times Y$-matrix of endomorphisms on $\mathcal{F}_\mathcal{E}(u)$. In order to do so we need the following notation.

Let X be a finite set of variables. For $x, x' \in X$ let $\delta_{xx'}\colon \mathcal{F}_\mathcal{E}(u) \to \mathcal{F}_\mathcal{E}(u)$ be 1 if $x = x'$ and 0 if $x \neq x'$. To simplify our notation, we write id_X instead of $id_{\mathcal{F}_\mathcal{E}(X)}$. If $(\sigma_x)_{x\in X}$ is a family of Σ-homomorphisms with the same domain and the same range then $\sum_{x\in X}\sigma_x$ denotes the pointwise sum of the σ_x. If the set X is clear from the context we simply write $\sum_x \sigma_x$.

For $x \in X$ we define $\iota_x\colon \mathcal{F}_\mathcal{E}(u) \to \mathcal{F}_\mathcal{E}(X)$ as the unique Σ-homomorphism satisfying $u\iota_x = x$, and we define $\pi_x\colon \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(u)$ as the unique Σ-homomorphism satisfying $x\pi_x = u$ and $x'\pi_x = 0$ for $x' \neq x$. Intuitively, ι_x is a substitution that replaces the variable u by the variable x, thus transforming a term from $\mathcal{T}_\Sigma(u)$ into a term in $\mathcal{T}_\Sigma(X)$. Conversely, π_x is a substitution that takes a term from $\mathcal{T}_\Sigma(X)$ and replaces all variables with 0, except the variable x, which is replaced by u. For instance, if $t = x+x'+x'$, then $t\pi_x =_\mathcal{E} u$ and $t\pi_{x'} =_\mathcal{E} u+u$. The term t can be reconstructed from $t\pi_x$ and $t\pi_{x'}$ by means of ι_x and $\iota_{x'}$, since $x+x'+x' =_\mathcal{E} u\iota_x+(u+u)\iota_{x'}$. The following lemma says that the π_x and ι_x always interact in this way.

Lemma 6.8 *Let X be finite. Then*

1. $\sum_{x\in X}\pi_x\iota_x = id_X$.

2. $\iota_x \pi_{x'} = \delta_{xx'}$

Proof. 1. From the above definitions we deduce that $\pi_x \iota_x$ is the endomorphism on $\mathcal{F}_\mathcal{E}(X)$ that maps x to x and x' to 0 for $x' \neq x$. Hence, $\sum_x \pi_x \iota_x$, the pointwise sum of all $\pi_x \iota_x$, is an endomorphism that maps each element of X to itself. Thus $\sum_{x \in X} \pi_x \iota_x$ and id_X agree on the generators of $\mathcal{F}_\mathcal{E}(X)$. Since X generates $\mathcal{F}_\mathcal{E}(X)$ this yields the claim.

2. By definition, $u \iota_x \pi_x = x \pi_x = u$. Hence, $\iota_x \pi_x = 1$. Now, suppose $x \neq x'$. Then, by definition, we have $u \iota_x \pi_{x'} = x \pi_{x'} = 0$. Hence, $\iota_x \pi_{x'} = 0$. □

We are now ready to define $\cdot^{\text{lin}}$. Let X, Y be finite and $\sigma: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ be a Σ-homomorphism. For $x \in X$ and $y \in Y$ let

$$\sigma_{xy} := \iota_x \sigma \pi_y.$$

Note that each σ_{xy} is an endomorphism on $\mathcal{F}_\mathcal{E}(u)$ and thus an element of $\mathcal{S}_\mathcal{E}$. We define $\sigma^{\text{lin}}: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ as the left linear mapping that corresponds to the matrix $(\sigma_{xy})_{x \in X, y \in Y}$.

Proposition 6.9 *Let X, Y, Z be finite and $\sigma: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ and $\tau: \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$ be Σ-homomorphisms. Then*

1. $(id_X)^{\text{lin}} = id_{\mathcal{S}_\mathcal{E}^X}$
2. $(\sigma\tau)^{\text{lin}} = \sigma^{\text{lin}} \tau^{\text{lin}}$.

Proof. 1. The matrix of $(id_X)^{\text{lin}}$ contains the entries $\iota_x id_X \pi_{x'} = \iota_x \pi_{x'} = \delta_{xx'}$. The left linear mapping corresponding to the matrix $(\delta_{xx'})_{x,x' \in X}$ is the identity on $\mathcal{S}_\mathcal{E}^X$.

2. It suffices to show that the matrix derived from $\sigma\tau$ is the product of the matrices derived from σ and τ. We compute the entry in the x-th row and the z-th column of the matrix derived from $\sigma\tau$ as

$$\begin{aligned}
(\sigma\tau)_{xz} &= \iota_x \sigma\tau \pi_z \\
&= \iota_x \sigma id_Y \tau \pi_z \\
&= \iota_x \sigma (\textstyle\sum_y \pi_y \iota_y) \tau \pi_z \qquad (1) \\
&= \textstyle\sum_y (\iota_x \sigma \pi_y)(\iota_y \tau \pi_z) \qquad (2) \\
&= \textstyle\sum_y \sigma_{xy} \tau_{yz},
\end{aligned}$$

using in (1) Lemma 6.8 and in (2) the distributivity of composition over pointwise sum of Σ-homomorphisms (Proposition 6.2). By the rules of matrix multiplication

we know that the entry in the x-th row and the z-th column of the product of $(\sigma_{xy})_{x\in X,y\in Y}$ and $(\tau_{yz})_{y\in Y,z\in Z}$ is $\sum_y \sigma_{xy}\tau_{yz}$. Thus the two matrices are equal. □

Next we define $\cdot^{\mathrm{hom}}$. Let $\sigma\colon \mathcal{S}_{\mathcal{E}}^X \to \mathcal{S}_{\mathcal{E}}^Y$ be a left linear mapping which has the matrix $(\sigma_{xy})_{x\in X,y\in Y}$. Note that each σ_{xy} is an element of $\mathcal{S}_{\mathcal{E}}$ and thus an endomorphism on $\mathcal{F}_{\mathcal{E}}(u)$. Then $\sigma^{\mathrm{hom}}\colon \mathcal{F}_{\mathcal{E}}(X) \to \mathcal{F}_{\mathcal{E}}(Y)$ is the Σ-homomorphism defined by

$$\sigma^{\mathrm{hom}} := \sum_{x\in X,y\in Y} \pi_x \sigma_{xy} \iota_y.$$

Proposition 6.10 *Let X, Y, Z be finite and $\sigma\colon \mathcal{S}_{\mathcal{E}}^X \to \mathcal{S}_{\mathcal{E}}^Y$ and $\tau\colon \mathcal{S}_{\mathcal{E}}^Y \to \mathcal{S}_{\mathcal{E}}^Z$ be left linear. Then*

1. $(id_{\mathcal{S}_{\mathcal{E}}^X})^{\mathrm{hom}} = id_X$
2. $(\sigma\tau)^{\mathrm{hom}} = \sigma^{\mathrm{hom}}\tau^{\mathrm{hom}}$.

Proof. 1. Since $(\delta_{xx'})_{x,x'\in X}$ is the matrix describing the identity on $\mathcal{S}_{\mathcal{E}}^X$, we conclude by Lemma 6.8 that

$$(id_{\mathcal{S}_{\mathcal{E}}^X})^{\mathrm{hom}} = \textstyle\sum_{x,x'} \pi_x \delta_{xx'} \iota_{x'} = \sum_x \pi_x \iota_x = id_X.$$

2. Let $(\sigma_{xy})_{x\in X,y\in Y}$ be the matrix of σ and $(\tau_{xy})_{x\in X,y\in Y}$ be the matrix of τ. Then the matrix of $\sigma\tau$ has in the x-th row and z-th column the entry $\sum_y \sigma_{xy}\tau_{yz}$. Hence, by definition of $\cdot^{\mathrm{hom}}$,

$$(\sigma\tau)^{\mathrm{hom}} = \sum_{x,z} \pi_x (\sum_y \sigma_{xy}\tau_{yz}) \iota_z.$$

Applying the definition of σ^{hom} and τ^{hom} we obtain

$$\begin{aligned}
\sigma^{\mathrm{hom}}\tau^{\mathrm{hom}} &= (\sum_{x,y} \pi_x \sigma_{xy} \iota_y)(\sum_{y',z} \pi_{y'} \tau_{y'z} \iota_z) \\
&= \sum_{x,y,y',z} \pi_x \sigma_{xy} \iota_y \pi_{y'} \tau_{y'z} \iota_z \qquad (1) \\
&= \sum_{x,y,y',z} \pi_x \sigma_{xy} \delta_{yy'} \tau_{y'z} \iota_z \qquad (2) \\
&= \sum_{x,y,z} \pi_x \sigma_{xy} \tau_{yz} \iota_z \\
&= \sum_{x,z} \pi_x (\sum_y \sigma_{xy}\tau_{yz}) \iota_z, \qquad (3)
\end{aligned}$$

where we used in (1) and (3) the distributivity of composition over pointwise addition (Proposition 6.2) and in (2) Lemma 6.8. Thus, $(\sigma\tau)^{\mathrm{hom}}$ and $\sigma^{\mathrm{hom}}\tau^{\mathrm{hom}}$ are equal. □

Proposition 6.11 *Let X, Y be finite. Suppose $\sigma: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ is a Σ-homomorphism and $\tau: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ be left linear. Then*

1. $\sigma^{\text{lin}^{\text{hom}}} = \sigma$
2. $\tau^{\text{hom}^{\text{lin}}} = \tau$

Proof. 1. The entry in the x-th row and y-th column of the matrix of σ^{lin} is $\sigma_{xy} = \iota_x \sigma \pi_y$. Applying the definition of $\sigma^{\text{lin}^{\text{hom}}}$, Proposition 6.2, and Lemma 6.8, we obtain

$$\begin{aligned} \sigma^{\text{lin}^{\text{hom}}} &= \textstyle\sum_{x,y} \pi_x \sigma_{xy} \iota_y = \sum_{x,y} \pi_x \iota_x \sigma \pi_y \iota_y \\ &= (\textstyle\sum_x \pi_x \iota_x) \sigma (\sum_y \pi_y \iota_y) = id_X \sigma id_Y = \sigma. \end{aligned}$$

2. Let $(\tau_{xy})_{x \in X, y \in Y}$ be the matrix of τ. By definition, $\tau^{\text{hom}} = \sum_{x',y'} \pi_{x'} \tau_{x'y'} \iota_{y'}$. Using once more Proposition 6.2 and Lemma 6.8 we deduce that the entry in the x-th row and y-th column of the matrix of $\tau^{\text{hom}^{\text{lin}}}$ is

$$\begin{aligned} \iota_x \tau^{\text{hom}} \pi_y &= \iota_x (\textstyle\sum_{x',y'} \pi_{x'} \tau_{x'y'} \iota_{y'}) \pi_y = \sum_{x',y'} \iota_x \pi_{x'} \tau_{x'y'} \iota_{y'} \pi_y \\ &= \textstyle\sum_{x',y'} \delta_{xx'} \tau_{x'y'} \delta_{y'y} = \tau_{xy}. \end{aligned}$$

Thus, the matrices of $\tau^{\text{hom}^{\text{lin}}}$ and τ are equal, which yields the claim. □

The results of this subsection could have been obtained as corollaries from more general results in category theory (cf. [HS73]). Actually, from Propositions 6.1 and 6.2 it follows that the finitely generated $\mathcal{E}$-algebras as objects together with the Σ-homomorphisms as morphisms form a semiadditive category. Together with Lemma 6.8 this fact implies that a free $\mathcal{E}$-algebra $\mathcal{F}_\mathcal{E}(x_1, \ldots, x_n)$ is a biproduct whose factors are the elementary algebras $\mathcal{F}_\mathcal{E}(x_1), \ldots, \mathcal{F}_\mathcal{E}(x_n)$. For morphisms between biproducts it is known that they can be represented by matrices whose entries are morphisms between the factors. Since the factors $\mathcal{F}_\mathcal{E}(x_i)$ and the algebra $\mathcal{F}_\mathcal{E}(u)$ are isomorphic, morphisms between the factors can be identified with morphisms $\mathcal{F}_\mathcal{E}(u) \to \mathcal{F}_\mathcal{E}(u)$, that is, elements of the semiring $\mathcal{S}_\mathcal{E}$. We have preferred to prove the above results in a noncategorical framework in order to make the paper self-contained and also more accessible for readers not familiar with category theory.

We conclude this section with examples that show how to compute the matrix of σ^{lin} for a Σ-homomorphism σ and how to change a left linear mapping τ into τ^{hom}.

Example 6.12 Let $X = \{x_1, x_2\}$, $Y = \{y_1, y_2, y_3\}$, and $\sigma: \mathcal{F}_{\text{GAUSS}}(X) \to \mathcal{F}_{\text{GAUSS}}(Y)$ be given by

$$x_1\sigma = i(y_1) + y_3 \qquad x_2\sigma = y_1 + y_3 + y_3.$$

For the sake of simplicity we will write in this and the following example ι_i, π_j, and σ_{ij} instead of ι_{x_i}, π_{y_j}, and $\sigma_{x_i y_j}$, respectively. With this notation we have

$$(\sigma_{ij})_{ij} = \begin{pmatrix} \iota_1\sigma\pi_1 & \iota_1\sigma\pi_2 & \iota_1\sigma\pi_3 \\ \iota_2\sigma\pi_1 & \iota_2\sigma\pi_2 & \iota_2\sigma\pi_3 \end{pmatrix} = \begin{pmatrix} [u/i(u)] & [u/0] & [u/u] \\ [u/u] & [u/0] & [u/u+u] \end{pmatrix}.$$

The isomorphism between $\mathcal{S}_{\text{GAUSS}}$ and $\mathbf{Z} \oplus i\mathbf{Z}$ described in Example 6.4 identifies the matrix $(\sigma_{ij})_{ij}$ with the matrix

$$\begin{pmatrix} i & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix}$$

over $\mathbf{Z} \oplus i\mathbf{Z}$. □

Example 6.13 Let X, Y be as in the preceding example and let $\tau\colon (\mathbf{Z} \oplus i\mathbf{Z})^X \to (\mathbf{Z} \oplus i\mathbf{Z})^Y$ be given by the matrix

$$(\tau_{ij})_{ij} = \begin{pmatrix} 0 & 1+i & 0 \\ 1 & i & 0 \end{pmatrix}.$$

The isomorphism between $\mathbf{Z} \oplus i\mathbf{Z}$ and $\mathcal{S}_{\text{GAUSS}}$ gives us τ as the mapping $\mathcal{S}_{\text{GAUSS}}^X \to \mathcal{S}_{\text{GAUSS}}^Y$ with the matrix

$$(\tau_{ij})_{ij} = \begin{pmatrix} [u/0] & [u/u+i(u)] & [u/0] \\ [u/u] & [u/i(u)] & [u/0] \end{pmatrix}.$$

Since $\tau^{\text{hom}} = \sum_{i,j} \pi_i \tau_{ij} \iota_j$, it follows for $k = 1, 2$ that

$$\begin{aligned} x_k\tau^{\text{hom}} = x_k \textstyle\sum_{i,j} \pi_i\tau_{ij}\iota_j &= \textstyle\sum_{i,j} x_k\pi_i\tau_{ij}\iota_j && (1) \\ &= \textstyle\sum_j x_k\pi_k\tau_{kj}\iota_j, && (2) \end{aligned}$$

where (1) holds by the definition of pointwise addition and (2) holds because $x_k\pi_i = 0$ for $i \neq k$. Hence

$$\begin{aligned} x_1\tau^{\text{hom}} &=_{\text{GAUSS}} 0 + y_2 + i(y_2) + 0 &=_{\text{GAUSS}}\ & y_2 + i(y_2) \\ x_2\tau^{\text{hom}} &=_{\text{GAUSS}} y_1 + i(y_2) + 0 &=_{\text{GAUSS}}\ & y_1 + i(y_2). \end{aligned}$$

□

7 Unification without Constants

In this section we investigate unification problems in a monoidal theory $\mathcal{E}$ that do not contain free constants. We show that such problems correspond to systems of homogeneous linear equations over $\mathcal{S}_\mathcal{E}$. This leads to a schema for a universal unification algorithm for monoidal theories that requires as parameter an algorithm for solving such linear equations. Finally, using results from algebra we derive sufficient conditions for a monoidal theory to be of unification type unitary.

7.1 Unification of Linear Mappings

Unification problems for an equational theory $\mathcal{E} = (\Sigma, E)$ can be understood as the task of describing for a pair of Σ-homomorphisms $\sigma, \tau: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ all Σ-homomorphism $\delta: \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$ such that $\sigma\delta = \tau\delta$ (see Section 4). The description is to be given by a complete or even better a minimal complete set of unifiers.

If the theory $\mathcal{E}$ is monoidal, we can translate unification problems into problems for left linear mappings between free left $\mathcal{S}_\mathcal{E}$-modules, using the results in Section 6. When given σ, τ as above, $\sigma^{\text{lin}}, \tau^{\text{lin}}: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ are left linear. Now, instead of some Σ-homomorphism δ, we look for some left linear $\eta: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$ such that $\sigma^{\text{lin}}\eta = \tau^{\text{lin}}\eta$. This suffices to solve the original problem, because $\delta := \eta^{\text{hom}}$ is a unifier of σ and τ. This can be seen as follows:

$$\sigma\delta = \sigma^{\text{lin}^{\text{hom}}}\eta^{\text{hom}} = (\sigma^{\text{lin}}\eta)^{\text{hom}} = (\tau^{\text{lin}}\eta)^{\text{hom}} = \tau^{\text{lin}^{\text{hom}}}\eta^{\text{hom}} = \tau\delta.$$

Conversely, if δ is a unifier of σ and τ, then $\eta := \delta^{\text{lin}}$ solves $\sigma^{\text{lin}}\eta = \tau^{\text{lin}}\eta$.

In the rest of this section we assume that $\mathcal{E}$-unification problems are already translated into the framework of linear algebra. If $\sigma, \tau: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ is a pair of linear mappings then a *unifier of σ and τ* is a left linear mapping $\delta: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$ such that $\sigma\delta = \tau\delta$. We define the relations of being more general and strictly more general for left linear mappings exactly as in the case of $\mathcal{E}$-unification. Most general unifiers, complete and minimal complete sets of unifiers are defined in the obvious way. Using the translation technique as developed in Subsection 6.2, results can be transferred back and forth from one framework into the other.

7.2 Characterization of Unifiers

The notions of the kernel and the image of a linear mapping are fundamental to linear algebra, but in order to generalize to semirings we have to slightly modify them.

Let $\sigma, \tau: \mathcal{S}^X \to \mathcal{S}^Y$ be left (right) linear. The *kernel of σ and τ* is the set

$$ker(\sigma, \tau) := \{a \in \mathcal{S}^X \mid a\sigma = a\tau\}.$$

The kernel of σ and τ is a left (right) submodule of $\mathcal{S}^X$. It is the set of solutions to the linear equation system

$$a\sigma = a\tau.$$

Since there is no subtraction in arbitrary semirings, homogeneous linear equations over $\mathcal{S}$ cannot be supposed to be in general of the form $a\sigma = 0$.

The *image of* σ is the set

$$im\,\sigma := \mathcal{S}^X\sigma = \{b \in \mathcal{S}^Y \mid \exists a \in \mathcal{S}^X.\, a\sigma = b\}.$$

The image of σ is a left (right) submodule of $\mathcal{S}^Y$.

We use the above definitions to characterize the instance relation between left linear mappings in terms of kernels and images of their dual mappings.

Theorem 7.1 *Let $\delta: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ and $\eta: \mathcal{S}_\mathcal{E}^X m \to \mathcal{S}_\mathcal{E}^Z$ be left linear. Then the following equivalences hold:*

1. $\delta \leq \eta \iff im\,\eta^* \subseteq im\,\delta^*$
2. $\delta < \eta \iff im\,\eta^*$ *is a proper subset of* $im\,\delta^*$.

Proof. 1. "$\Rightarrow$" If $\delta \leq \eta$, then $\eta = \delta\lambda$ for some $\lambda: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$. Hence $\eta^* = \lambda^*\delta^*$, which implies $im\,\eta^* = (im\,\lambda^*)\delta^* \subseteq (\mathcal{S}_\mathcal{E}^Y)\delta^* = im\,\delta^*$.

"$\Leftarrow$" It suffices to show that there is a right linear mapping $\mu: \mathcal{S}_\mathcal{E}^Z \to \mathcal{S}_\mathcal{E}^Y$ such that $\mu\delta^* = \eta^*$, since then $\delta\mu^* = \eta$. Let e_z, $z \in Z$, be the unit vectors of $\mathcal{S}_\mathcal{E}^Z$. Since $im\,\eta^* \subseteq im\,\delta^*$, it follows that $e_z\eta^* \in im\,\delta^*$ for all $z \in Z$. Hence, there exist vectors $a_z \in \mathcal{S}_\mathcal{E}^Y$ such that $a_z\delta^* = e_z\eta^*$. Define μ by $e_z\mu := a_z$. Since $\mathcal{S}_\mathcal{E}^Z$ is a free module, μ is completely defined by the values it takes on the unit vectors. Then $e_z\mu\delta^* = e_z\eta^*$. Since $\mu\delta^*$ and η^* agree on the generators of $\mathcal{S}_\mathcal{E}^Z$, they are equal.

2. The claim is a trivial consequence of statement (1). □

The next theorem characterizes unifiers.

Theorem 7.2 *Let $\sigma, \tau: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ and $\delta: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$ be left linear. Then the following equivalences hold:*

1. *δ is a unifier of σ and τ* $\iff$ $im\,\delta^* \subseteq ker(\sigma^*, \tau^*)$

2. δ is a most general unifier of σ and τ $\iff$ $im\,\delta^* = ker(\sigma^*, \tau^*)$.

Proof. 1. δ is a unifier of σ and $\tau \iff \sigma\delta = \tau\delta \iff \delta^*\sigma^* = \delta^*\tau^* \iff \forall a \in \mathcal{S}_\mathcal{E}^Z.\, a\delta^*\sigma^* = a\delta^*\tau^* \iff \forall b \in im\,\delta^*.\, b\sigma^* = b\tau^* \iff im\,\delta^* \subseteq ker(\sigma^*, \tau^*)$.

2. "$\Rightarrow$" Suppose δ is a unifier of σ and τ and there exists some $a \in ker(\sigma^*, \tau^*)$ such that $a \notin im\,\delta^*$. Define $\eta: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^{\{z\}}$ by $e_z\eta^* = a$. Then $im\,\eta^* \subseteq ker(\sigma^*, \tau^*)$, and therefore η is a unifier of σ and τ by part (1). Since $a \in im\,\eta^*$ and $a \notin im\,\delta^*$, it follows from Theorem 7.1 that δ is not more general than η.

"$\Leftarrow$" Suppose $im\,\delta^* = ker(\sigma^*, \tau^*)$. We know by part (1) that for every unifier η we have $im\,\eta^* \subseteq ker(\sigma^*, \tau^*) = im\,\delta^*$. By Theorem 7.1, δ is more general than η. □

As an immediate consequence we note that every $\mathcal{E}$-unification problem is solvable.

Corollary 7.3 *For every pair $\sigma, \tau: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ the constant mapping $0: \mathcal{S}_\mathcal{E}^Y \to 0$ is a unifier.*

Proof. The transpose of 0 is the constant mapping $0^*: 0 \to \mathcal{S}_\mathcal{E}^Y$. Hence, $im\,0^* = \{0\} \subseteq ker(\sigma^*, \tau^*)$, since $ker(\sigma^*, \tau^*)$ is a right submodule of $\mathcal{S}_\mathcal{E}^Y$ and therefore contains the element 0. □

Intuitively, δ is a most general unifier of σ and τ if δ^* parameterizes the right submodule $ker(\sigma^*, \tau^*)$ of $\mathcal{S}_\mathcal{E}^Y$. Whether or not such a δ can exist depends on the size of a generating set of $ker(\sigma^*, \tau^*)$. To formalize this idea we need some definitions.

We consider $\mathcal{S}_\mathcal{E}^X$ as a right $\mathcal{S}_\mathcal{E}$-module. Let $S \subseteq \mathcal{S}_\mathcal{E}^X$. The *right submodule generated by* S is the least right submodule of $\mathcal{S}_\mathcal{E}^X$ that contains S. It is denoted as $[S]$. It consists of all right linear combinations of elements of S, that is $[S] = \{\sum_{i=1}^n a_i\alpha_i \mid n \in \mathbf{N},\ \alpha_i \in \mathcal{S}_\mathcal{E},\ a_i \in S\}$. A right submodule M of $\mathcal{S}_\mathcal{E}^X$ is *finitely generated* if $M = [S]$ for some finite set $S \subseteq M$.

Theorem 7.4 (Type Unitary) *Let $\sigma, \tau: \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ be left linear. Then there exists a most general unifier of σ and τ if and only if $ker(\sigma^*, \tau^*)$ is finitely generated.*

Proof. "$\Rightarrow$" If $\delta: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$ is a most general unifier of σ and τ, then $ker(\sigma^*, \tau^*) = im\,\delta^* = (\mathcal{S}_\mathcal{E}^Z)\delta^*$. Since $\mathcal{S}_\mathcal{E}^Z$ is generated by the finite set of unit vectors $\{e_z \mid z \in Z\}$, it follows that $ker(\sigma^*, \tau^*) = (\mathcal{S}_\mathcal{E}^Z)\delta^*$ is generated by the finite set $\{e_z\delta^* \mid z \in Z\}$.

"$\Leftarrow$" If $ker(\sigma^*, \tau^*)$ is generated by the finite set $\{a_z \mid z \in Z\}$, then define $\delta: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$ by $e_z\delta^* := a_z$. Since $\mathcal{S}_\mathcal{E}^Z$ is generated by the unit vectors e_z, it follows that $im\,\delta^* = (\mathcal{S}_\mathcal{E}^Z)\delta^*$ is generated by the vectors $e_z\delta^* = a_z$. Hence, we know that $im\,\delta^* = ker(\sigma^*, \tau^*)$. By Theorem 7.2, δ is a most general unifier of σ and τ. □

Theorem 7.5 (Type Nullary) *Let $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^X \to \mathcal{S}_{\mathcal{E}}^Y$ be left linear. Then there do not exist minimal elements in the set of unifiers of σ and τ if and only if $ker(\sigma^*, \tau^*)$ is not finitely generated.*

Proof. "$\Rightarrow$" If $ker(\sigma^*, \tau^*)$ is finitely generated, then by Theorem 7.4 a most general unifier δ of σ and τ exists. The unifier δ is a minimal element in the set of all unifiers of σ and τ.

"$\Leftarrow$" Let $\eta: \mathcal{S}_{\mathcal{E}}^Y \to \mathcal{S}_{\mathcal{E}}^Z$ be a unifier of σ and τ and suppose that $ker(\sigma^*, \tau^*)$ is not finitely generated. We show that there exists a unifier δ that is strictly more general.

Since $im\eta^*$ is generated by the finite set $\{e_z\eta^* \mid z \in Z\}$, it follows that $im\eta^*$ is a proper subset of $ker(\sigma^*, \tau^*)$. Hence, there exists some $a \in ker(\sigma^*, \tau^*) \setminus im\eta^*$. Suppose $z' \notin Z$ and let $\delta: \mathcal{S}_{\mathcal{E}}^Y \to \mathcal{S}_{\mathcal{E}}^{Z \cup \{z'\}}$ such that $e_z\delta^* := e_z\eta^*$ for $z \in Z$ and $e_{z'}\delta^* := a$. Then $im\delta^* \subseteq ker(\sigma^*, \tau^*)$, which implies that δ is a unifier of σ and τ. Furthermore, $im\eta^*$ is a proper subset of $im\delta^*$, which implies that δ is strictly more general than η. □

The preceding theorems allow us to describe the possible locations of monoidal theories in the unification hierarchy and to give an algebraic characterization of the unification type.

Theorem 7.6 (Unitary-Or-Nullary) *Every monoidal theory $\mathcal{E}$ is either unitary or nullary. In particular,*

1. *$\mathcal{E}$ is unitary if and only if for every pair $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^X \to \mathcal{S}_{\mathcal{E}}^Y$ of right linear mappings, $ker(\sigma, \tau)$ is finitely generated*
2. *$\mathcal{E}$ is nullary if and only if there is a pair; $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^X \to \mathcal{S}_{\mathcal{E}}^Y$ of right linear mappings such that $ker(\sigma, \tau)$ is not finitely generated.*

Proof. 1. By Corollary 7.3 every unification problem has a solution. Thus, if $\mathcal{E}$ is unitary, for every unification problem there exists a most general unifier. Hence, for every pair of right linear mappings σ, τ the unification problem given by σ^* and τ^* has a most general unifier. By Theorem 7.4, $ker(\sigma^{**}, \tau^{**}) = ker(\sigma, \tau)$ is finitely generated.

Conversely, if for every pair σ, τ of right linear mappings, $ker(\sigma, \tau)$ is finitely generated, then Theorem 7.4 implies that a most general unifier exists for every $\mathcal{E}$-unification problem. Hence, $\mathcal{E}$ is unitary.

2. If $\mathcal{E}$ is nullary, then $\mathcal{E}$ is not unitary. Hence, part (1) implies that there is a pair σ, τ of right linear mappings such that $ker(\sigma, \tau)$ is not finitely generated.

- input: left linear mappings σ and τ
- let C_σ, C_τ be the matrices describing $\sigma, \tau: \mathcal{S}^X \to \mathcal{S}^Y$
- find a generating set $\{a_z \mid z \in Z\}$ of solutions for $C_\sigma a = C_\tau a$
- for every finite set $V \subseteq Z$ let D_V be the matrix whose vth column is a_v, $v \in V$
- let $\delta_V: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^V$ be given by D_V
- if Z is finite
  then δ_Z is a most general unifier
  else $\{\delta_V \mid V \subseteq Z, V \text{ finite}\}$ is a complete set of unifiers

Figure 1: Schema of a unification algorithm for a monoidal theory $\mathcal{E}$

Conversely, if for σ, τ the module $ker(\sigma, \tau)$ is not finitely generated, then Theorem 7.5 implies that the set of unifiers of σ^* and τ^* does not contain a minimal element. Hence, there exists no minimal complete set of unifiers for σ and τ. □

Example 7.7 It has been proved that the theories AC [Sti75, LS76], ACI [BB88], and AG [LBB84] are unitary for unification without constants, and that ACH is nullary [Baa89a]. □

The proof of Theorem 7.4 contains the construction for a most general unifier of σ and τ for the case that $ker(\sigma^*, \tau^*)$ is finitely generated. The proof of Theorem 7.5 shows how to construct arbitrarily general unifiers of σ and τ if $ker(\sigma^*, \tau^*)$ is not finitely generated. We can summarize these constructions in the schema of a universal unification algorithm for monoidal theories. The schema is given in Figure 1. In order to obtain a full-fledged unification algorithm for a theory $\mathcal{E}$, one has to provide a procedure that computes generating sets of the solution spaces of linear equations systems over $\mathcal{S}_\mathcal{E}$. In order to understand the schema, note that the matrix representation of the equation $a\sigma^* = a\tau^*$ is $C_\sigma a = C_\tau a$.

If we fill into the schema procedures that solve homogeneous equations over $\mathcal{S}_{\mathrm{AC}} = \mathbf{N}$, $\mathcal{S}_{\mathrm{ACI}} = \mathbf{B}$, and $\mathcal{S}_{\mathrm{AG}} = \mathbf{Z}$, we obtain essentially the algorithms that have been described in the literature for the theories AC [LS76, Sti81], ACI [BB88], and AG [LBB84]. We illustrate the algorithm with an example from the theory GAUSS.

Example 7.8 Consider the term unification problem

$$
\begin{aligned}
i(y_1) + y_3 &\doteq y_2 + i(y_2) \\
y_1 + y_3 + y_3 &\doteq y_1 + i(y_2)
\end{aligned}
$$

for the theory GAUSS. Let $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2, y_3\}$. The problem is equivalent to the task of unifying the Σ_{GAUSS}-homomorphisms

$$\sigma', \tau' : \mathcal{F}_{\text{GAUSS}}(X) \to \mathcal{F}_{\text{GAUSS}}(Y)$$

given by the equations

$$
\begin{aligned}
x_1\sigma' &= i(y_1) + y_3 & \qquad x_1\tau' &= y_2 + i(y_2) \\
x_2\sigma' &= y_1 + y_3 + y_3 & \qquad x_2\tau' &= y_1 + i(y_2).
\end{aligned}
$$

Instead of looking for unifiers of σ' and τ' directly we look for unifiers of $\sigma := \sigma'^{\text{lin}}$ and $\tau := \tau'^{\text{lin}}$. By Examples 6.12 and 6.13 we know that σ and τ have the matrices

$$C_\sigma = \begin{pmatrix} i & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix} \quad \text{and} \quad C_\tau = \begin{pmatrix} 0 & 1+i & 0 \\ 1 & i & 0 \end{pmatrix}.$$

Since $\mathbf{Z} \oplus i\mathbf{Z}$ is a ring, we can subtract matrices. Thus $ker(\sigma^*, \tau^*) = \{a \in \mathbf{Z} \oplus i\mathbf{Z} \mid (C_\sigma - C_\tau)a = 0\}$. The solutions of the corresponding equation system[1]

$$\begin{pmatrix} i & -1-i & 1 \\ 0 & -i & 2 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

are generated by the vector $a = (2+i, 2i, -1)$. The mapping $\delta : (\mathbf{Z} \oplus i\mathbf{Z})^X \to (\mathbf{Z} \oplus i\mathbf{Z})^{\{z\}}$ given by the matrix

$$\begin{pmatrix} 2+i \\ 2i \\ -1 \end{pmatrix}$$

is a most general unifier of σ and τ. Hence $\delta' := \delta^{\text{hom}}$ is a most general unifier of σ' and τ'. It is represented by the substitution

$$[y_1/z + z + i(z),\ y_2/i(z+z),\ y_3/i(i(z))].$$

□

[1] Since $\mathbf{Z} \oplus i\mathbf{Z}$ is a euclidean ring, the algorithm for solving linear equation systems over euclidean rings described in [Sim84] is applicable.

7.3 Noetherian Theories

We will now look for sufficient conditions for a monoidal theory to be unitary. Bürckert et al. [BHSS89] called an equational theory $\mathcal{E} = (\Sigma, E)$ *noetherian*[2] if there exists no infinite strictly decreasing sequence $\sigma_1 > \sigma_2 > \ldots$ of Σ-homomorphisms $\sigma_n: \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y_n)$, $n \geq 1$. By Zorn's Lemma, this implies that, given a unification problem, for every unifier δ there is a minimal unifier μ such that $\mu \leq \delta$. Hence, the set of minimal unifiers is a complete set. Therefore, a noetherian theory is not nullary. Since monoidal theories are either unitary or nullary we have thus identified a class of unitary monoidal theories.

Proposition 7.9 *A noetherian monoidal theory is unitary.*

Noetherian rings are algebraic structures that have been extensively studied (see for example [Jac80]). A commutative ring is *noetherian* if all its ideals are finitely generated. Interestingly, this concept is intimately related to the concept of a noetherian monoidal theory. In the following we give a generalized definition that coincides with the original one if the semiring in question is a commutative ring.

A semiring $\mathcal{S}$ is *noetherian* if for finite sets X every right submodule of the right module $\mathcal{S}^X$ is finitely generated. As an example, the ring $\mathbf{Z}$ of integers is noetherian [Jac80]. The following theorem shows how noetherian monoidal theories and noetherian semirings are connected.

Theorem 7.10 *A monoidal theory $\mathcal{E}$ is noetherian if and only if $\mathcal{S}_\mathcal{E}$ is a noetherian semiring.*

Proof. We identify Σ-homomorphisms between free algebras and left linear mappings between free left modules.

"$\Rightarrow$" Suppose $\mathcal{S}_\mathcal{E}$ is not a noetherian semiring. Then for some finite set X there exists a right submodule M of $\mathcal{S}_\mathcal{E}^X$ that is not finitely generated. We will inductively define a sequence $(Y_n)_{n=1}^\infty$ of finite sets and a sequence $(\sigma_n)_{n=1}^\infty$ of right linear mappings $\sigma_n: \mathcal{S}_\mathcal{E}^{Y_n} \to \mathcal{S}_\mathcal{E}^X$ such that

- $im\,\sigma_n \subseteq M$
- $im\,\sigma_n$ is a proper subset of $im\,\sigma_{n+1}$.

Then $\sigma_1^* > \sigma_2^* > \ldots$ is an infinite strictly decreasing sequence of left linear mappings.

Since $M \neq \emptyset$, there exists some $a_1 \in M$. Let $Y_1 := \{y_1\}$ be a singleton. Define $\sigma_1: \mathcal{S}_\mathcal{E}^{Y_1} \to \mathcal{S}_\mathcal{E}^X$ by $e_{y_1}\sigma_1 := a_1$. Obviously, $im\,\sigma_1 \subseteq M$. Now, suppose Y_n and σ_n are

[2]Note that this definition has nothing to do with noetherian term rewriting systems.

already defined. Then $im\,\sigma_n$ is generated by the finite set $\{e_y\sigma_n \mid y \in Y_n\}$. Hence, $im\,\sigma_n$ is a proper subset of M, and there exists some $a_{n+1} \in M \setminus im\,\sigma_n$. Suppose $y_{n+1} \notin Y_n$ and let $Y_{n+1} := Y_n \uplus \{y_{n+1}\}$. Define $\sigma_{n+1}: \mathcal{S}_{\mathcal{E}}^{Y_n} \to \mathcal{S}_{\mathcal{E}}^{X}$ by $e_y\sigma_{n+1} := e_y\sigma_n$ for $y \in Y$ and $e_{y_{n+1}}\sigma_{n+1} := a_{n+1}$. Then $im\,\sigma_{n+1} \subseteq M$ and $im\,\sigma_n$ is a proper subset of $im\,\sigma_{n+1}$.

"$\Leftarrow$" Suppose $\mathcal{E}$ is not noetherian. Then there exists an infinite descending sequence of left linear mappings $\sigma_1 > \sigma_2 > \ldots$. By Theorem 7.1, this implies that $im\,\sigma_n^*$ is a proper subset of $im\,\sigma_{n+1}^*$. Define a submodule $M \subseteq \mathcal{S}_{\mathcal{E}}^{X}$ by $M := \bigcup_{n=1}^{\infty} im\,\sigma_n^*$. We will show that M is not finitely generated.

To do so, we first observe that $im\,\sigma_n^*$ is a proper subset of M, since $im\,\sigma_n^*$ is a proper subset of $im\,\sigma_{n+1}^* \subseteq M$. Now, suppose that M is generated by some finite set S. Since S is finite, there must be an index m such that $S \subseteq im\,\sigma_m^*$. This implies $M = [S] \subseteq im\,\sigma_m^*$, which contradicts the fact that $im\,\sigma_m^*$ is a proper subset of M. □

This characterization gives us a first hint how to identify noetherian theories.

Corollary 7.11 *A monoidal theory $\mathcal{E}$ is noetherian if $\mathcal{S}_{\mathcal{E}}$ is finite.*

Proof. If $\mathcal{S}_{\mathcal{E}}$ is finite, then for all finite sets X all right submodules of $\mathcal{S}_{\mathcal{E}}^{X}$ are finite and therefore finitely generated. □

Example 7.12 Since $\mathcal{S}_{\mathrm{ACI}} \simeq \mathbf{B}$ has only two elements, the above corollary proves that ACI is unitary without referring to an algorithm. □

Noetherian semirings and rings have important inheritance properties. It is folklore in algebra that quotients of noetherian rings are again noetherian [Jac80]. We show that the result holds as well for noetherian semirings.

Theorem 7.13 *Every quotient semiring of a noetherian semiring is noetherian.*

Proof. Let $\mathcal{S}$ be a noetherian semiring and let $\hat{\mathcal{S}}$ be a quotient of $\mathcal{S}$. To prove the theorem, it suffices to show that for all finite sets X every right submodule of the right $\hat{\mathcal{S}}$-module $\hat{\mathcal{S}}^X$ is finitely generated.

Let $\kappa: \mathcal{S} \to \hat{\mathcal{S}}$ be the quotient mapping and let X be a finite set. By $\hat{a}\alpha := \hat{a}(\alpha\kappa)$ we define a right scalar multiplication $\hat{\mathcal{S}}^X \times \mathcal{S} \to \hat{\mathcal{S}}^X$ that turns $\hat{\mathcal{S}}^X$ into a right $\mathcal{S}$-module. By $((\alpha_x)_{x\in X})\kappa_X := (\alpha_x\kappa)_{x\in X}$ we define a surjective $\mathcal{S}$-linear mapping $\kappa_X: \mathcal{S}^X \to \hat{\mathcal{S}}^X$. Now, let $\widehat{M}$ be a submodule of the right $\hat{\mathcal{S}}$-module $\hat{\mathcal{S}}^X$. We have defined the above scalar multiplication in such a way that $\widehat{M}$ is also a submodule of $\hat{\mathcal{S}}^X$ if considered as a right $\mathcal{S}$-module. Since κ_X is $\mathcal{S}$-linear, $M := \widehat{M}\kappa_X^{-1}$, the

preimage of $\widehat{M}$ under κ_X, is a $\mathcal{S}$-submodule of $\mathcal{S}^X$. Since $\mathcal{S}$ is noetherian, M is generated by some finite set $S \subseteq M$.

It suffices to show that $\widehat{M}$ is generated by $S\kappa_X$. To do so, let $\hat{a} \in \widehat{M}$. There is some $a \in M$ such that $\hat{a} = a\kappa_X$. Since M is generated by S, there are finitely many elements $\alpha_1, \ldots, \alpha_k \in \mathcal{S}$ and $a_1, \ldots, a_k \in S$ such that $a = \sum_{i=1}^{k} a_i\alpha_i$. Since κ_X is $\mathcal{S}$-linear, it follows that $\hat{a} = a\kappa_X = \sum_{i=1}^{k}(a_i\alpha_i)\kappa_X = \sum_{i=1}^{k}(a_i\kappa_X)(\alpha_i\kappa)$. Since $\alpha_i\kappa \in \widehat{\mathcal{S}}$ and $a_i\kappa_X \in S\kappa_X$, this yields the claim. □

The preceding theorem immediately implies a result for equational theories.

Theorem 7.14 *Let $\mathcal{E} = (\Sigma, E)$ be a noetherian monoidal theory. If E' is a stable congruence on Σ-terms such that $E' \supseteq E$, then $\mathcal{E}' := (\Sigma, E')$ is again a noetherian monoidal theory.*

Proof. Since E' contains every identity that E contains, it follows that $\mathcal{E}' = (\Sigma, E')$ is monoidal and that $\mathcal{F}_{\mathcal{E}'}(u)$ is a quotient Σ-algebra of $\mathcal{F}_{\mathcal{E}}(u)$. It remains to be shown that the canonical semiring $\mathcal{S}_{\mathcal{E}'}$ of $\mathcal{E}'$ is a quotient semiring of $\mathcal{S}_{\mathcal{E}}$, because then Theorem 7.13 yields the claim.

Let $\kappa\colon \mathcal{S}_{\mathcal{E}} \to \mathcal{S}_{\mathcal{E}'}$ be the mapping that associates to α_t, i.e., the endomorphism on $\mathcal{F}_{\mathcal{E}}(u)$ given by $[u/t]$, the element $\alpha'_t \in \mathcal{S}_{\mathcal{E}'}$, i.e., the endomorphism on $\mathcal{F}_{\mathcal{E}'}(u)$ given by the same substitution. If $\alpha_s = \alpha_t$, then $s =_{\mathcal{E}} t$, which implies $s =_{\mathcal{E}'} t$ and $\alpha'_s = \alpha'_t$. Thus, κ is well defined. Obviously, κ is surjective. Now, it is straightforward to prove that κ is a semiring homomorphism. We have $0\kappa = \alpha_0\kappa = \alpha'_0 = 0$ and $1\kappa = \alpha_u\kappa = \alpha'_u = 1$. Thus κ respects zero and unit. Moreover, for $s, t \in \mathcal{T}_\Sigma(u)$ we have $(\alpha_s + \alpha_t)\kappa = \alpha_{s+t}\kappa = \alpha'_{s+t} = \alpha'_s + \alpha'_t$ and $(\alpha_s\alpha_t)\kappa = \alpha_{s[u/t]}\kappa = \alpha'_{s[u/t]} = \alpha'_s\alpha'_t$. Thus κ respects addition and multiplication. □

Intuitively the above theorem says that given a noetherian monoidal theory, we may add arbitrary identities and still have a noetherian theory provided we did not change the signature. This result is in sharp contrast to the general situation. Adding identities to an arbitrary noetherian theory can produce a theory that is no longer noetherian. For instance, the theory of associativity is noetherian [BHSS89], but adding idempotence yields a nullary theory [Baa86, SS86].

Under which circumstances can we add unary symbols to the signature of a noetherian monoidal theory such that the resulting theory is still noetherian? For an answer, Hilbert's Basis Theorem about noetherian rings will be helpful. For a proof see [Jac80].

Theorem 7.15 (Hilbert's Basis Theorem) *If $\mathcal{S}$ is a noetherian commutative ring, then $\mathcal{S}[X_1, \ldots, X_n]$, the ring of polynomials in n indeterminates with coefficients from $\mathcal{S}$, is again a noetherian commutative ring.*

The following theorem is an easy consequence of Hilbert's Basis Theorem. It says that given a noetherian group theory with commuting homomorphisms, one can safely add finitely many homomorphism symbols and arbitrary identities provided the new symbols commute with each other and with the homomorphism symbols of the original theory.

Theorem 7.16 *Let $\mathcal{E} = (\Sigma, E)$ be a noetherian group theory with commuting homomorphisms. Suppose $\mathcal{E}' = (\Sigma', E')$ is such that*

1. $\Sigma' = \Sigma \uplus \{h_1, \ldots, h_n\}$ *for finitely many unary symbols* $h_1, \ldots, h_n$
2. $E' \supseteq E$
3. $\mathcal{E}'$ *is a theory with commuting homomorphisms.*

Then $\mathcal{E}'$ is again a noetherian group theory.

Proof. It follows from the assumptions that $\mathcal{S}_\mathcal{E}$ is a noetherian commutative ring. We will show that $\mathcal{S}_{\mathcal{E}'}$, the canonical semiring of $\mathcal{E}'$, is isomorphic to a quotient ring of $\mathcal{S}_\mathcal{E}[X_1, \ldots, X_n]$. Since by Hilbert's Basis Theorem the latter is a noetherian ring, Theorem 7.14 will imply that $\mathcal{S}_{\mathcal{E}'}$ is a noetherian ring and thus $\mathcal{E}'$ is a noetherian group theory.

There is a Σ-term t such that $x + t =_\mathcal{E} 0$. Since E' is an extension of E, every identity that holds in $\mathcal{E}$ also holds in $\mathcal{E}'$. Hence, $x + t =_{E'} 0$. Thus, $\mathcal{E}'$ is a group theory and $\mathcal{S}_{\mathcal{E}'}$ is a ring. Moreover, $\mathcal{S}_{\mathcal{E}'}$ is commutative because homomorphisms commute in $\mathcal{E}'$.

As already mentioned, for all term s, $t \in \mathcal{T}_\Sigma(u)$ we have $s =_{\mathcal{E}'} t$ if $s =_\mathcal{E} t$. Thus we can define a ring homomorphism $\kappa_0 \colon \mathcal{S}_\mathcal{E} \to \mathcal{S}_{\mathcal{E}'}$ by mapping $\alpha_t \in \mathcal{S}_\mathcal{E}$, i.e., the endomorphism on $\mathcal{F}_\mathcal{E}(u)$ given by $[u/t]$, to $\alpha'_t \in \mathcal{S}_{\mathcal{E}'}$, i.e., the endomorphism on $\mathcal{F}_{\mathcal{E}'}(u)$ given by the same substitution. By the universal property of polynomial rings (see [Jac74]) there exists a unique ring homomorphism $\kappa \colon \mathcal{S}_\mathcal{E}[X_1, \ldots, X_n] \to \mathcal{S}_{\mathcal{E}'}$ such that $\alpha\kappa = \alpha\kappa_0$ for $\alpha \in \mathcal{S}_\mathcal{E}$ and $X_i\kappa = \alpha'_{h_i(u)}$ for $i = 1, \ldots, n$.

Every element $\alpha' \in \mathcal{S}_{\mathcal{E}'}$ can be represented as $\alpha'_{t'}$ for some term $t' \in \mathcal{T}_{\Sigma'}(u)$. Therefore α' can be obtained by the ring operations from the elements of $\mathcal{S}_\mathcal{E}\kappa_0$ and $\alpha_{h_1(u)}, \ldots, \alpha_{h_n(u)}$. This implies that κ is surjective. Hence, $\mathcal{S}_{\mathcal{E}'}$ is isomorphic to the quotient of $\mathcal{S}_\mathcal{E}[X_1, \ldots, X_n]$ by the ring ideal $\{p \mid p\kappa = 0\}$. □

In the preceding theorem the condition that $\mathcal{E}$ is a group theory cannot be dismissed. As a counterexample consider the theory ACI, which is noetherian. Adding one homomorphism symbol to ACI leads to a theory, which is nullary and thus not noetherian [Baa89b]. This is a special case of a general result saying that adding a single homomorphism symbol to a monoidal theory that is not a group theory leads to a nullary theory [BN91].

Corollary 7.17 *A group theory with finitely many commuting homomorphisms is noetherian.*

Proof. Let $\mathcal{E} = (\Sigma, E)$ be a group theory with finitely many commuting homomorphisms. Since $\mathcal{E}$ is a group theory, there exists a Σ-term t such that $x + t =_\mathcal{E} 0$. Without loss of generality we can assume that t contains no other variable than x. We assume as well that the unary symbol "$-$" does not occur in the signature Σ. Let $\Sigma' := \Sigma \cup \{-\}$, and let E' be the stable Σ'-congruence generated by $E \cup \{-x \doteq t\}$. We denote the theory (Σ', E') as $\mathcal{E}'$. Since the new symbol "$-$" can be expressed in terms of the signature Σ, we have $\mathcal{S}_\mathcal{E} \simeq \mathcal{S}_{\mathcal{E}'}$. Hence, $\mathcal{E}'$ is a group theory with commuting homomorphisms. Moreover, $\mathcal{E}'$ is an extension of AG that satisfies the conditions of Theorem 7.16. Since AG is noetherian, this yields the claim. □

Example 7.18 The above corollary implies that AGH and GAUSS are noetherian. □

Unfortunately, Hilbert's proof is not constructive. No general method is known to find a generating set for submodules of $\mathcal{S}[X_1, \ldots, X_n]^X$ if one has generating sets for the submodules of $\mathcal{S}^X$. Therefore, devising unification algorithms for arbitrary group theories with commuting homomorphisms is still an open problem. Baader [Baa90] describes a method for solving linear equations over the ring $\mathbf{Z}[X_1, \ldots, X_n]$ thus furnishing the cornerstone of a unification algorithm for the theory of abelian groups with commuting homomorphisms.

8 Unification with Constants

In applications it is rarely sufficient to solve elementary unification problems (cf. Subsection 2.3). Problems containing free constants arise naturally through skolemization and in problems for combinations of theories. In the previous section we investigated unification problems without constants in a monoidal theory $\mathcal{E}$, which turned out to be equivalent to systems of homogeneous linear equations over the semiring $\mathcal{S}_\mathcal{E}$. In this section we will show that unification problems with free constants translate to systems of inhomogeneous linear equations over $\mathcal{S}_\mathcal{E}$.

8.1 The Problem

First, we adapt our framework to unification with constants.

General Assumption. *As before, we assume that $\mathcal{E} = (\Sigma, E)$ is a monoidal theory. Moreover, we assume that C is a finite set of free constants that is disjoint from the set of variables.*

We want to solve $\mathcal{E}$-unification problems that contain free constants from the set C. We may assume that C contains the constants occurring in the unification problem at hand. Free constants can be viewed as special variables which are not allowed to be instantiated. In the previous section, where we considered unification without constants, we modeled unification problems and unifiers as arbitrary Σ-homomorphisms between finitely generated free $\mathcal{E}$-algebras. To deal with problems containing free constants we consider Σ-homomorphisms that do not move the elements of C.[3]

We say that a Σ-homomorphism $\sigma\colon \mathcal{F}_{\mathcal{E}}(X \cup C) \to \mathcal{F}_{\mathcal{E}}(Y \cup C)$ *respects constants* if $c\sigma = c$ for all $c \in C$. A *unification problem with constants* is presented by a parallel pair $\sigma, \tau\colon \mathcal{F}_{\mathcal{E}}(X \cup C) \to \mathcal{F}_{\mathcal{E}}(Y \cup C)$ where σ and τ respect constants. We say that $\delta\colon \mathcal{F}_{\mathcal{E}}(Y \cup C) \to \mathcal{F}_{\mathcal{E}}(Z \cup C)$ is a *unifier with constants* of σ and τ if $\sigma\delta = \tau\delta$ and δ respects constants.

Next we modify the instantiation preorder so as to cope with constants. If δ, η respect constants, then we write $\delta \leq_C \eta$ if $\eta = \delta\lambda$ for some λ that respects constants. Obviously, the relation "$\leq_C$" is a preorder. The strict part of "$\leq_C$" is denoted as "$<_C$". Complete sets and minimal complete sets of unifiers with constants are defined in terms of the preorder "$\leq_C$."

As in the preceding section we translate unification problems for Σ-homomorphisms into unification problems for left linear mappings. We say that a left linear mapping $\sigma\colon \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ *respects constants* if $\sigma^{\hom}\colon \mathcal{F}_{\mathcal{E}}(X \cup C) \to \mathcal{F}_{\mathcal{E}}(Y \cup C)$ respects constants. Obviously, this is the case if and only if σ does not move the unit vectors e_c, that is $e_c\sigma = e_c$, for all $c \in C$. Similarly as above, we define for left linear mappings the notion of a unifier with constants and the instantiation preorder "$\leq_C$." It follows from this definition that for all left linear mappings σ, τ, δ, and η we have that δ is a unifier with constants of σ and τ if and only if $\delta^{\hom}$ is a unifier with constants of $\sigma^{\hom}$ and $\tau^{\hom}$ and that $\delta \leq_C \eta$ if and only if $\delta^{\hom} \leq_C \eta^{\hom}$.

In the following, we will investigate the structure of left linear mappings that respect constants and characterize the preorder "$\leq_C$." Suppose $\sigma\colon \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ respects constants. Then the fact that $e_c\sigma = e_c$ for all $c \in C$ implies that the matrix C_σ has the form

$$C_\sigma = \begin{pmatrix} C_\sigma^h & C_\sigma^i \\ 0 & I \end{pmatrix},$$

where C_σ^h is a $X \times Y$-matrix, C_σ^i is an $X \times C$-matrix, and I is the $C \times C$-unit matrix.

[3] This idea first appeared in [Baa89a].

The superscripts $\cdot^h$ and $\cdot^i$ are chosen so as to indicate that in unification problems C^h_σ and C^i_σ will give rise to homogeneous and inhomogeneous linear equations, respectively. The matrices C^h_σ and C^i_σ describe left linear mappings $\sigma_h: \mathcal{S}^X_\mathcal{E} \to \mathcal{S}^Y_\mathcal{E}$ and $\sigma_i: \mathcal{S}^X_\mathcal{E} \to \mathcal{S}^C_\mathcal{E}$. Obviously, σ is uniquely determined by σ_h and σ_i.

Conversely, if $\eta: \mathcal{S}^X_\mathcal{E} \to \mathcal{S}^Y_\mathcal{E}$ and $\mu: \mathcal{S}^X_\mathcal{E} \to \mathcal{S}^C_\mathcal{E}$ are arbitrary left linear mappings, then there exists a unique left linear mapping $\langle \eta, \mu \rangle: \mathcal{S}^{X \cup C}_\mathcal{E} \to \mathcal{S}^{Y \cup C}_\mathcal{E}$ that respects constants such that $\langle \eta, \mu \rangle_h = \eta$ and $\langle \eta, \mu \rangle_i = \mu$. The mapping $\langle \eta, \mu \rangle$ is given by the matrix

$$C_{\langle \eta, \mu \rangle} = \begin{pmatrix} C_\eta & C_\mu \\ 0 & I \end{pmatrix}.$$

The next proposition shows how the components of the product of mappings that respect constants are related to the components of the factors.

Proposition 8.1 *Suppose $\sigma: \mathcal{S}^{X \cup C}_\mathcal{E} \to \mathcal{S}^{Y \cup C}_\mathcal{E}$ and $\tau: \mathcal{S}^{Y \cup C}_\mathcal{E} \to \mathcal{S}^{Z \cup C}_\mathcal{E}$ respect constants. Then $\sigma\tau$ respects constants and $\sigma\tau = \langle \sigma_h \tau_h, \sigma_h \tau_i + \sigma_i \rangle$.*

Proof. The proof is by a straightforward matrix calculation:

$$\begin{aligned} C_{\sigma\tau} = C_\sigma C_\tau &= \begin{pmatrix} C^h_\sigma & C^i_\sigma \\ 0 & I \end{pmatrix} \begin{pmatrix} C^h_\tau & C^i_\tau \\ 0 & I \end{pmatrix} \\ &= \begin{pmatrix} C^h_\sigma C^h_\tau & C^h_\sigma C^i_\tau + C^i_\sigma \\ 0 & I \end{pmatrix} = \begin{pmatrix} C_{\sigma_h \tau_h} & C_{\sigma_h \tau_i + \sigma_i} \\ 0 & I \end{pmatrix}. \end{aligned}$$

□

The following definitions will be used to characterize the preorder "$\leq_C$." Let M be a right submodule of $\mathcal{S}^X_\mathcal{E}$. If $a \in \mathcal{S}^X_\mathcal{E}$, then the *coset of M for a* is the set $a + M := \{a + m \mid m \in M\}$. We define a binary relation "$\leq_M$" on $\mathcal{S}^X_\mathcal{E}$ by $a \leq_M a'$ iff $a + M \supseteq a' + M$. Note that $a \leq_M a'$ if and only if $a' \in a + M$. Obviously, "$\leq_M$" is a preorder, since "$\supseteq$" is a preorder. We extend this preorder to left linear mappings $\lambda, \mu: \mathcal{S}^X_\mathcal{E} \to \mathcal{S}^C_\mathcal{E}$ by defining $\lambda \preceq_M \mu$ iff $e_c \lambda^* \leq_M e_c \mu^*$ for all $c \in C$. Evidently, "$\preceq_M$" is again a preorder. The strict parts of "$\leq_M$" and "$\preceq_M$" are denoted as "$<_M$" and "$\prec_M$."

The preorder "$\leq_C$" can be characterized in terms of the usual instantiation preorder "$\leq$" and the preorder "$\preceq_M$".

Theorem 8.2 *Suppose $\delta: \mathcal{S}^{X \cup C}_\mathcal{E} \to \mathcal{S}^{Y \cup C}_\mathcal{E}$ and $\eta: \mathcal{S}^{X \cup C}_\mathcal{E} \to \mathcal{S}^{Z \cup C}_\mathcal{E}$ respect constants. Then the following are equivalent:*

- $\delta \leq_C \eta$

- $\delta_h \leq \eta_h$ *and* $\delta_i \preceq_M \eta_i$ *where* $M = im\,\delta_h^*$.

Proof. Suppose that $\delta \leq_C \eta$. Then there is some $\lambda: \mathcal{S}_{\mathcal{E}}^{Y \cup C} \to \mathcal{S}_{\mathcal{E}}^{Z \cup C}$ that respects constants such that $\eta = \delta\lambda$. By Proposition 8.1 we have $\eta_h = \delta_h\lambda_h$. Thus $\delta_h \leq \eta_h$. Furthermore, by 8.1 we have $\eta_i = \delta_h\lambda_i + \delta_i$. If $c \in C$, then $e_c\eta_i^* = e_c(\lambda_i^*\delta_h^* + \delta_i^*) = e_c\delta_i^* + e_c\lambda_i^*\delta_h^* \in e_c\delta_i^* + im\,\delta_h^*$. Hence, $e_c\delta_i^* \leq_M e_c\eta_i^*$ where $M = im\,\delta_h^*$.

Suppose that $\delta_h \leq \eta_h$ and $\delta_i \preceq_M \eta_i$ where $M = im\,\delta_h^*$. It suffices to show that there exist linear mappings $\lambda_h: \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{Z}$ and $\lambda_i: \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{C}$ such that $\eta_h = \delta_h\lambda_h$ and $\eta_i = \delta_h\lambda_i + \delta_i$. Since $\delta_h \leq \eta_h$, the existence of λ_h is guaranteed. To prove the existence of λ_i, observe that for all $c \in C$, we have $e_c\eta_i^* \in e_c\delta_i^* + im\,\delta_h^*$. Hence there exist $a_c \in \mathcal{S}_{\mathcal{E}}^{Y}$ such that $e_c\eta_i^* = a_c\delta_h^* + e_c\delta_i^*$. There exists a unique λ_i such that for all $c \in C$ we have $e_c\lambda_i^* = a_c$. This implies that η_i^* and $\lambda_i^*\delta_h^* + \delta_i^*$ agree on the unit vectors of $\mathcal{S}_{\mathcal{E}}^{C}$, hence they are equal. By dualization, we obtain $\eta_i = \delta_h\lambda_i + \delta_i$. □

8.2 Complete Sets of Unifiers with Constants

If a monoidal theory is nullary for unification without constants, then it is also nullary for unification with constants. Therefore we restrict our attention to theories that are not nullary for unification without constants and thus are unitary.

General Assumption. *In the rest of this section, if nothing else is said, we assume that* $\mathcal{E}$ *is a monoidal theory which is unitary with respect to unification without constants.*

We first investigate the structure of unifiers with constants. Suppose that σ, $\tau: \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ respect constants and δ is a unifier with constants of σ and τ. Then $\sigma\delta = \tau\delta$. By Proposition 8.1 this is equivalent to

$$\langle \sigma_h\delta_h, \sigma_h\delta_i + \sigma_i \rangle = \langle \tau_h\delta_h, \tau_h\delta_i + \tau_i \rangle.$$

Both sides of this equation are equal if and only if the first and second components are equal, that is

$$\begin{aligned} \sigma_h\delta_h &= \tau_h\delta_h \\ \sigma_h\delta_i + \sigma_i &= \tau_h\delta_i + \tau_i. \end{aligned}$$

The first equation means that δ_h is a unifier of σ_h and τ_h. By the results of Section 7 we know that the component δ_h of δ can be computed by solving a system of homogeneous equations. The condition imposed on δ_i by the second equation will be captured by the following definition.

Let σ, τ be as above. A left linear mapping $\eta: \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{C}$ is an *inhomogeneous solution for* σ *and* τ if

$$\sigma_h\eta + \sigma_i = \tau_h\eta + \tau_i.$$

We denote the set of all inhomogeneous solution for σ and τ as $\mathcal{I}(\sigma, \tau)$.

We can now give a first characterization of unifiers with constants.

Proposition 8.3 *Suppose σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ and $\delta: \mathcal{S}_\mathcal{E}^{Y \cup C} \to \mathcal{S}_\mathcal{E}^{Z \cup C}$ respect constants. Then δ is a unifier with constants of σ and τ if and only if δ_h is a unifier of σ_h and τ_h, and δ_i is an inhomogeneous solution for σ and τ.*

In Theorem 8.2, we have characterized the preorder "$\leq_C$" by showing that $\delta \leq_C \eta$ if and only if $\delta_h \leq \eta_h$ and $\delta_i \preceq_M \eta_i$ where $M = im\,\delta_h^*$. This characterization has the disadvantage that the preorder "$\preceq_M$" depends on one of the mappings, namely δ. If we restrict "$\leq_C$" to unifiers with constants δ such that δ_h is most general, then "$\preceq_M$" no longer depends on the mappings involved.

Proposition 8.4 *Let σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ be mappings that respect constants, and let $K := ker(\sigma_h^*, \tau_h^*)$. Suppose δ, η are unifiers with constants of σ and τ such that both δ_h and η_h are most general unifiers of σ_h and τ_h. Then $\delta \leq_C \eta$ if and only if $\delta_i \preceq_K \eta_i$.*

Proof. Since δ_h and η_h are both most general unifiers of σ_h and τ_h, we have $\delta_h \leq \eta_h$. Furthermore, we know by 7.2 that $im\,\delta_h^* = ker(\sigma_h^*, \tau_h^*) = K$. Hence, $\delta \leq_C \eta$ if and only if $\delta_h \leq \eta_h$ and $\delta_i \preceq_K \eta_i$, which yields the claim. □

Consider the unification problem with constants that is given by two mappings σ and τ. Let $K := ker(\sigma_h^*, \tau_h^*)$. Then "$\preceq_K$" is a preorder on $\mathcal{I}(\sigma, \tau)$, the set of inhomogeneous solutions for σ and τ. A subset of $\mathcal{I}(\sigma, \tau)$ is a *complete* or *minimal complete* set of inhomogeneous solutions if it is a complete or minimal complete subset with respect to the preorder "$\preceq_K$".

If U is a set of unifiers with constants of σ and τ, then we define

$$I_U := \{\delta_i \mid \delta \in U \text{ and } \delta_h \text{ is a most general unifier of } \sigma_h \text{ and } \tau_h\}.$$

Obviously, I_U is a set of inhomogeneous solutions.

Theorem 8.5 *Suppose σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ respect constants and U is a set of unifiers with constants of σ and τ. Then*

1. *I_U is a complete set of inhomogeneous solutions if and only if U is a complete set of unifiers with constants*

2. *I_U is a minimal complete set of inhomogeneous solutions if U is a minimal complete set of unifiers with constants.*

Proof. Let $K := ker(\sigma_h^*, \tau_h^*)$.

1. "$\Rightarrow$" Suppose I_U is a complete set of inhomogeneous solutions. Let η be a unifier with constants of σ and τ. We will show that there is some $\delta \in U$ such that $\delta \leq_C \eta$.

By 8.3 we know that η_i is an inhomogeneous solution for σ and τ. Since I_U is complete, there exists some $\delta \in U$ such that $\delta_i \preceq_K \eta_i$. Moreover $\delta_h \leq \eta_h$, since η_h is a unifier of σ_h and τ_h, and δ_h is most general. By 8.2 and the fact that $im\,\delta_h^* = K$ this implies $\delta \leq_C \eta$.

"$\Leftarrow$" Suppose U is a complete set of unifiers with constants. Let η'' be an inhomogeneous solution for σ and τ. We will show that there is a $\delta \in U$ such that δ_h is a most general unifier of σ_h and τ_h, and $\delta_i \preceq_K \eta''$.

Let η' be a most general unifier of σ_h and τ_h and let $\eta := \langle \eta', \eta'' \rangle$. Then η is a unifier with constants of σ and τ. Hence, there exists some $\delta \in U$ such that $\delta \leq_C \eta$. By 8.2 this implies $\delta_h \leq \eta_h = \eta'$. Since η' is most general, δ_h is most general, which means that $\delta_i \in I_U$. Thus $\delta \leq_C \eta$ implies $\delta_i \preceq_K \eta_i = \eta''$ by Proposition 8.4. This shows that δ is the required element of U.

2. Suppose that U is a minimal complete set of unifiers with constants. By part (1) we know that I_U is a complete set of inhomogeneous solutions. Thus it suffices to show that any two elements of I_U are independent with respect to "$\preceq_K$". The minimality of U implies that δ_h is a most general unifier of σ_h and τ_h for every $\delta \in U$. Hence $\delta_h \leq \eta_h$ for all $\delta, \eta \in U$. If there are $\delta, \eta \in U$ such that $\delta_i \preceq_K \eta_i$, then Proposition 8.4 implies that $\delta \leq_C \eta$. Hence $\delta = \eta$ and therefore $\delta_i = \eta_i$. □

Note that the converse of part (2) of the preceding theorem does not hold. It is only true if δ_h is a most general unifier for all $\delta \in U$.

We have seen that from a complete set of unifiers one can construct a complete set of inhomogeneous solutions. We will show that, conversely, from a complete set of inhomogeneous solutions one can construct a complete set of unifiers.

If I is a set of inhomogeneous solutions for σ and τ, and δ is a most general unifier of σ_h and τ_h, then we define

$$U_I^\delta := \{\langle \delta, \eta \rangle \mid \eta \in I\}.$$

The set U_I^δ consists of all combinations of δ and the elements of I. Obviously, U_I^δ is a set of unifiers with constants of σ and τ.

Theorem 8.6 *Suppose σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ respect constants. Let δ be a most general unifier of σ_h and τ_h, and I a set of inhomogeneous solutions for σ and τ. Then U_I^δ is a (minimal) complete set of unifiers with constants if and only if I is a (minimal) complete set of inhomogeneous solutions.*

Proof. Observe that by construction of U_I^δ we have $I_{U_I^\delta} = I$. Thus, we know by Theorem 8.5 that U_I^δ is complete if and only if I is complete, and that I is a minimal complete set if U_I^δ is a minimal complete set.

It remains to be shown that U_I^δ is a minimal complete set if I is a minimal complete set. Let $K := ker(\sigma_h^*, \tau_h^*)$. Assume by contradiction that U_I^δ is not a minimal complete set. Then there exist η, $\eta' \in I$ such that $\langle \delta, \eta \rangle \leq_C \langle \delta, \eta' \rangle$ and $\langle \delta, \eta \rangle \neq \langle \delta, \eta' \rangle$, i.e., $\eta \neq eta'$. Since δ is a most general unifier of σ_h and τ_h, this implies $\eta \preceq_K \eta'$, which contradicts the minimality of I. □

8.3 Complete Sets of Inhomogeneous Solutions

In the previous subsection we have reduced the problem of finding complete sets of unifiers with constants to the one of finding complete sets of inhomogeneous solutions. In this section we show that a unification problem with constants gives rise to a family of systems of inhomogeneous linear equations, and that an inhomogeneous solution has to solve this family simultaneously.

Suppose σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ respect constants and η is an inhomogeneous solution for σ and τ. Then

$$\sigma_h \eta + \sigma_i = \tau_h \eta + \tau_i$$

holds. By dualization, this is equivalent to

$$\eta^* \sigma_h^* + \sigma_i^* = \eta^* \tau_h^* + \tau_i^*.$$

Since the mappings on both sides of the equations are determined by their values on the unit vectors $e_c \in \mathcal{S}_\mathcal{E}^C$, this is equivalent to the condition

$$e_c \eta^* \sigma_h^* + e_c \sigma_i^* = e_c \eta^* \tau_h^* + e_c \tau_i^* \quad \text{for all } c \in C. \tag{1}$$

Equations (1) state that for every $c \in C$ the vector $e_c \eta^*$ must satisfy a certain inhomogeneous linear equation.

We extend our formalism so that we can handle also inhomogeneous equations. We say that a mapping $\phi: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^X$ is *affine* if there exist a right linear mapping $\lambda: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^X$ and a vector $b \in \mathcal{S}_\mathcal{E}^X$ such that

$$a\phi = a\lambda + b \quad \text{for all } a \in \mathcal{S}_{\mathcal{E}}^{Y}.$$

We will write such a mapping as $\phi = \lambda + b$. The idea behind this definition is that linear mappings correspond to homogeneous linear equations while affine mappings are related to inhomogeneous equations.

As for linear mappings, the *kernel* of affine mapppings $\phi, \psi: \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{X}$ is defined as

$$ker(\phi, \psi) := \{a \in \mathcal{S}_{\mathcal{E}}^{Y} \mid a\phi = a\psi\}.$$

In general, kernels of affine mappings are not submodules of $\mathcal{S}_{\mathcal{E}}^{Y}$. If $\phi = \lambda + b$ and $\psi = \mu + d$, then $ker(\phi, \psi)$ is the set of solutions a to the inhomogeneous equation

$$a\lambda + b = a\mu + d. \tag{2}$$

If $\mathcal{S}_{\mathcal{E}}$ is a ring, then this equation is equivalent to $a(\lambda - \mu) = d - b$. However, since subtraction need not exist in arbitrary semirings, inhomogeneous linear equations over $\mathcal{S}_{\mathcal{E}}$ are in general of the form (2).

Condition (1) can now be reformulated by saying that every vector $e_c\eta^*$ has to be an element of the kernel of two particular affine mappings that are obtained from σ and τ. For a mapping $\sigma: \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ that respects constants and $c \in C$ we define the affine mapping $\sigma^c: \mathcal{S}_{\mathcal{E}}^{C} \to \mathcal{S}_{\mathcal{E}}^{X}$ as

$$\sigma^c := \sigma_h^* + e_c\sigma_i^*.$$

With this definition we can characterize inhomogeneous solutions in terms of kernels of affine mappings.

Proposition 8.7 *Suppose $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ respect constants. Let $\eta: \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{C}$ be left linear. Then η is an inhomogeneous solution for σ and τ if and only if $e_c\eta^* \in ker(\sigma^c, \tau^c)$ for all $c \in C$.*

Our next goal is to characterize complete sets of inhomogeneous solutions.

Proposition 8.8 *Suppose $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ respect constants, and I is a set of inhomogeneous solutions for σ and τ. Let $K := ker(\sigma_h^*, \tau_h^*)$. Then I is complete if and only if for every family of vectors $(a_c)_{c \in C}$ with $a_c \in ker(\sigma^c, \tau^c)$ there exists some $\eta \in I$ such that $e_c\eta^* \leq_K a_c$ for all $c \in C$.*

Proof. "$\Rightarrow$" Suppose I is complete. Let $(a_c)_{c \in C}$ be a family with $a_c \in ker(\sigma^c, \tau^c)$. There exists a unique left linear mapping $\mu: \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{C}$ such that $e_c\mu^* = a_c$. By

Proposition 8.7, the mapping μ is an inhomogeneous solution. Since I is complete, there exists some $\eta \in I$ such that $\eta \preceq_K \mu$. Hence $e_c\eta^* \leq_K e_c\mu^* = a_c$ for all $c \in C$.

"$\Leftarrow$" Suppose that for every family $(a_c)_{c\in C}$ with $a_c \in ker(\sigma^c, \tau^c)$ there exists some $\eta \in I$ such that $e_c\eta^* \leq_K a_c$ for all $c \in C$. We show that I is complete. Let μ be an inhomogeneous solution for σ and τ. Then $(e_c\mu^*)_{c\in C}$ is a family of vectors with $e_c\mu^* \in ker(\sigma^c, \tau^c)$. There exists some $\eta \in I$ such that $e_c\eta^* \leq_C e_c\mu^*$ for all $c \in C$. This yields $\eta \preceq_K \mu$ by definition of "$\preceq_K$". □

The preceding proposition suggests to look for subsets of $ker(\sigma^c, \tau^c)$ that are complete for the preorder "$\leq_K$". Since such sets will play an important role in our theory, we provide a name for them. Let M be a right submodule of $\mathcal{S}_\mathcal{E}^X$ and T be a subset of $\mathcal{S}_\mathcal{E}^X$. A set $S \subseteq T$ that is is a complete subset of T for "$\leq_M$" will be called an *M-cover of T*.

In the context of inhomogeneous equations, a cover can be understood as a set of solutions that represents all solutions. More precisely, if $\lambda + b$ and $\mu + d$ are affine mappings, and S is a $ker(\lambda, \mu)$-cover of $ker(\lambda + b, \mu + d)$, then every solution a of the inhomogeneous equation $a\lambda + b = a\mu + d$ can be expressed as the sum of an element of S and a solution a' to the homogeneous equation $a'\lambda = a'\mu$.

Proposition 8.9 *Let $\lambda + b,\ \mu + d: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^X$ be affine mappings and let $S \subseteq ker(\lambda + b, \mu + d)$. Then S is a $ker(\lambda, \mu)$-cover of $ker(\lambda + b, \mu + d)$ if and only if*

$$ker(\lambda + b, \mu + d) = \bigcup_{a\in S} a + ker(\lambda, \mu).$$

Proof. To shorten our notation, we use the abbreviations $K := ker(\lambda, \mu)$ and $K_{b,d} := ker(\lambda + b, \mu + d)$.

"$\Rightarrow$" Suppose S is a K-cover of $K_{b,d}$. We show that $K_{b,d} = \bigcup_{a\in S} a + K$. Let $a' \in K_{b,d}$. There exists some $a \in S$ such that $a \leq_K a'$, that is $a' \in a + K$. This proves the inclusion "$\subseteq$". Let $a \in S \subseteq K_{b,d}$ and $a' \in K$. Then $a\lambda + b = a\mu + d$ and $a'\lambda = a'\mu$. From this it follows that $(a + a')\lambda + b = (a + a')\mu + d$. Thus $a + a' \in K_{b,d}$, which yields the inclusion "$\supseteq$".

"$\Leftarrow$" Suppose $K_{b,d} = \bigcup_{a\in S} a + K$. We show that S is a K-cover of $K_{b,d}$. Let $a' \in K_{b,d}$. Then there is some $a \in S$ such that $a' \in a + K$. Hence $a \leq_K a'$. □

The statement of the above proposition can intuitively be rephrased as follows: a set S is a $ker(\lambda, \mu)$-cover of $ker(\lambda + b, \mu + d)$ if and only if the cosets of $ker(\lambda, \mu)$ for the elements of S cover $ker(\lambda + b, \mu + d)$. This property motivated the name "cover".

It is known that one solution suffices to represent all solutions of an inhomogeneous equation over a ring.

Proposition 8.10 *Suppose $\mathcal{S}_\mathcal{E}$ is a ring. Let $\lambda + b,\ \mu + d\colon \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^X$ be affine mappings. Then for every $a \in ker(\lambda+b, \mu+d)$ the singleton $\{a\}$ is a $ker(\lambda,\mu)$-cover of $ker(\lambda + b, \mu + d)$, that is,*

$$ker(\lambda + b, \mu + d) = a + ker(\lambda, \mu).$$

Proof. Let $K := ker(\lambda, \mu)$ and $K_{b,d} := ker(\lambda + b, \mu + d)$.

Suppose $a \in K_{b,d}$. We show that $K_{b,d} = a + K$. The inclusion "$\supseteq$" is valid for arbitrary semirings. A proof for this fact is contained in the proof of Proposition 8.9. To prove the inclusion "$\subseteq$", let $a' \in K_{b,d}$. Since $a,\ a' \in K_{b,d}$, we have $a\lambda + b = a\mu + d$ and $a'\lambda + b = a'\mu + d$. From this we conclude that $(a' - a)\lambda = a'\lambda + b - (a\lambda + b) = a'\mu + b - (a\mu + b) = (a' - a)\mu$, hence $a' - a \in K$. Thus $a' = a + (a' - a) \in a + K$. □

Our next step is to relate covers to complete sets of inhomogeneous solutions.

If $\mathbf{a} = (a_c)_{c\in C}$ is a familiy of vectors in $\mathcal{S}_\mathcal{E}^Y$, then we denote with $\eta_\mathbf{a}\colon \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^C$ the unique left linear mapping that satisfies $e_c\eta_\mathbf{a}^* = a_c$ for all $c \in C$.

Let $\mathbf{S} = (S_c)_{c\in C}$ be a family of subsets of $\mathcal{S}_\mathcal{E}^Y$. Then we define the set of linear mappings $I_\mathbf{S}$ by

$$I_\mathbf{S} := \left\{\eta_\mathbf{a} \;\middle|\; \mathbf{a} \in \textstyle\prod_{c\in C} S_c\right\},$$

where $\prod_{c\in C} S_c$ is the cartesian product of the S_c, that is, the set of all families $\mathbf{a} = (a_c)_{c\in C}$ such that $a_c \in S_c$.

Theorem 8.11 *Let $\sigma,\ \tau\colon \mathcal{S}_\mathcal{E}^{X\cup C} \to \mathcal{S}_\mathcal{E}^{Y\cup C}$ respect constants, and let $K := ker(\sigma_h^*, \tau_h^*)$. Suppose $\mathbf{S} = (S_c)_{c\in C}$ is a family of sets such that S_c is a K-cover of $ker(\sigma^c, \tau^c)$ for every $c \in C$. Then:*

1. *$I_\mathbf{S}$ is a complete set of inhomogeneous solutions for σ and τ*
2. *$I_\mathbf{S}$ is a minimal complete set of inhomogeneous solutions for σ and τ if each S_c is a minimal K-cover of $ker(\sigma^c, \tau^c)$.*

Proof. 1. We prove the claim using Proposition 8.8. Let $(a_c)_{c\in C}$ be a family of vectors such that $a_c \in ker(\sigma^c, \tau^c)$ for all $c \in C$. Since each set S_c is a K-cover of $ker(\sigma^c, \tau^c)$, there exists for every $c \in C$ an element $b_c \in S_c$ such that $b_c \leq_K a_c$. Let $\mathbf{b} := (b_c)_{c\in C}$. Then $\eta_\mathbf{b} \in I_\mathbf{S}$ and $e_c\eta_\mathbf{b}^* = b_c \leq_K a_c$.

2. Assume that $I_\mathbf{S}$ is not minimal. Then there exist $\eta_\mathbf{a},\ \eta_\mathbf{b} \in I_\mathbf{S}$ such that $\mathbf{a} \neq \mathbf{b}$ and $\eta_\mathbf{a} \preceq_K \eta_\mathbf{b}$. Let $\mathbf{a} = (a_c)_{c\in C}$ and $\mathbf{b} = (b_c)_{c\in C}$. Since $\mathbf{a} \neq \mathbf{b}$, there is some $c \in C$ such that $a_c \neq b_c$. From $\eta_\mathbf{a} \preceq_K \eta_\mathbf{b}$ we obtain $a_c = e_c\eta_\mathbf{a}^* \leq_K e_c\eta_\mathbf{b}^* = b_c$, which contradicts the minimality of S_c. □

- input: mappings $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ that respect constants
- let $\begin{pmatrix} C_\sigma^h & C_\sigma^i \\ 0 & I \end{pmatrix}, \begin{pmatrix} C_\tau^h & C_\tau^i \\ 0 & I \end{pmatrix}$ be the matrices describing σ, τ
- let D^h be a matrix representing a most general unifier of σ^h and τ^h
- for $c \in C$ let b_c and d_c be the c-th column of C_σ^i and C_τ^i, respectively
- let $K := \{a \in \mathcal{S}_{\mathcal{E}}^Y \mid C_\sigma^h a = C_\tau^h a\}$
- for $c \in C$ find a (minimal) K-cover S_c of $\{a \in \mathcal{S}_{\mathcal{E}}^Y \mid C_\sigma^h a + b_c = C_\tau^h a + d_c\}$
- the set of matrices

$$\left\{ \begin{pmatrix} D^h & D^i \\ 0 & I \end{pmatrix} \;\middle|\; \text{the } c\text{-th column of } D^i \text{ is in } S_c \right\}$$

represents a (minimal) complete set of unifiers with constants of σ and τ

Figure 2: Schema of an algorithm for unification with constants

Since an algorithm for computing covers, that is for solving inhomogeneous linear equations, will depend on the structure of the semiring $\mathcal{S}_{\mathcal{E}}$ a general theory cannot be developed beyond the preceding theorem.

8.4 Computing Complete Sets of Unifiers with Constants

By Theorem 8.11 we know how to obtain complete sets of inhomogeneous solutions for σ and τ. By Theorem 8.6 we can combine such a set with a most general unifier of σ_h and τ_h to construct a complete set of unifiers with constants.

Theorem 8.12 (Unification with Constants) *Suppose $\sigma, \tau: \mathcal{S}_{\mathcal{E}}^{X \cup C} \to \mathcal{S}_{\mathcal{E}}^{Y \cup C}$ respect constants. Let δ be a most general unifier of σ_h and τ_h, and let $\mathbf{S} = (S_c)_{c \in C}$ be a family of sets such that S_c is a (minimal) $ker(\sigma_h^*, \tau_h^*)$-cover of $ker(\sigma^c, \tau^c)$ for every $c \in C$. Then*

$$U_{I_{\mathbf{S}}}^{\delta} = \left\{ \langle \delta, \eta_{\mathbf{a}} \rangle \;\middle|\; \mathbf{a} \in \textstyle\prod_{c \in C} S_c \right\}$$

is a (minimal) complete set of unifiers with constants of σ and τ.

From Theorem 8.12 we derive the schema of an algorithm that computes complete sets of unifiers with constants. We present it in Figure 2. To make it work for a theory $\mathcal{E}$, two procedures have to be provided: when given $X \times Y$-matrices C_1, C_2 over $\mathcal{S}_\mathcal{E}$, the first one computes a generating set of vectors for $K := \{a \in \mathcal{S}_\mathcal{E}^Y \mid C_1 a = C_2 a\}$, and the second one computes for arbitrary vectors $b_1, b_2 \in \mathcal{S}_\mathcal{E}^Y$ a K-cover of $\{a \in \mathcal{S}_\mathcal{E}^Y \mid C_1 a + b_1 = C_2 a + b_2\}$. Loosely speaking, the first procedure solves homogeneous linear equations over $\mathcal{S}_\mathcal{E}$, and the second one solves inhomogeneous equations.

When computing unifiers with constants, every constant gives rise to its own inhomogeneous equation that is independent from other constants. In order to construct a complete set of unifiers with constants the solutions to each of these equations have to be combined in all possible ways with the solutions corresponding to other constants.

Most of the algorithms which have been given in the literature for unification with constants in the theories AC [LS76, HS87], ACI [BB88], and AG can be obtained as instances of the schema. As to AG, the optimized algorithm in [LBB84] is the one that corresponds to our approach. Remarkably, Stickel's algorithm for AC-unification with free constants [Sti81] uses a different technique.

As an illustration, we apply the schema in Figure 2 to a problem in the theory GAUSS.

Example 8.13 Consider the term unification problem

$$\begin{aligned} i(y_1) + y_3 + i(c_1) + c_2 &\doteq y_2 + i(y_2) + c_1 + i(c_1) + i(i(i(c_2))) \\ y_1 + y_3 + y_3 + c_1 + i(c_2) &\doteq y_1 + i(y_2) + c_1 + c_1 \end{aligned}$$

in the theory GAUSS. Let $X := \{x_1, x_2\}$, $Y := \{y_1, y_2, y_3\}$, and $C := \{c_1, c_2\}$. The above term unification problem is equivalent to the unification problem for the two constant respecting mappings

$$\sigma', \tau' : \mathcal{F}_{\mathrm{GAUSS}}(X \cup C) \to \mathcal{F}_{\mathrm{GAUSS}}(Y \cup C)$$

which are given by the equations

$$\begin{aligned} x_1\sigma' &= i(y_1) + y_3 + i(c_1) + c_2 \\ x_2\sigma' &= y_1 + y_3 + y_3 + c_1 + i(c_2) \\ x_1\tau' &= y_2 + i(y_2) + c_1 + i(c_1) + i(i(i(c_2))) \\ x_2\tau' &= y_1 + i(y_2) + c_1 + c_1 \end{aligned}$$

and $c_1\sigma' = c_1\tau' = c_1$, and $c_2\sigma' = c_2\tau' = c_2$.

In order to solve the unification problem for σ' and τ' we consider the analogue problem for $\sigma := \sigma'^{\mathrm{lin}}$ and $\tau := \tau'^{\mathrm{lin}}$. The mappings σ_h and τ_h are described by the matrices

$$C_\sigma^h = \begin{pmatrix} i & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix} \quad \text{and} \quad C_\tau^h = \begin{pmatrix} 0 & 1+i & 0 \\ 1 & i & 0 \end{pmatrix},$$

while σ_i and τ_i have the matrices

$$C_\sigma^i = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \quad \text{and} \quad C_\tau^i = \begin{pmatrix} 1+i & -i \\ 2 & 0 \end{pmatrix}.$$

We already know from Example 7.8 that the matrix

$$D^h = \begin{pmatrix} 2+i \\ 2i \\ -1 \end{pmatrix}$$

represents a most general unifier of σ_h and τ_h.

It remains to solve the inhomogeneous equations corresponding to the constants c_1 and c_2. The c_1-th columns of C_σ^i and C_τ^i are

$$b_{c_1} = \begin{pmatrix} i \\ 1 \end{pmatrix} \quad \text{and} \quad d_{c_1} = \begin{pmatrix} 1+i \\ 2 \end{pmatrix}.$$

Since $\mathbf{Z} \oplus i\mathbf{Z}$, the canonical semiring of the theory GAUSS, is a ring, the inhomogeneous equation $C_\sigma^h a + b_{c_1} = C_\tau^h a + d_{c_1}$ is equivalent to $(C_\sigma^h - C_\tau^h)a = d_{c_1} - b_{c_1}$, and any solution for this equation provides a $ker(\sigma_h^*, \tau_h^*)$-cover of $ker(\sigma^{c_1}, \tau^{c_1})$. Therefore it suffices to find one solution to the equation

$$\begin{pmatrix} i & -1-i & 1 \\ 0 & -i & 2 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

The vector $a = (1, i, 0)$ is such a solution. Hence, the set $\{(1, i, 0)\}$ is a $ker(\sigma_h^*, \tau_h^*)$-cover of $ker(\sigma^{c_1}, \tau^{c_1})$.

For the constant c_2 we have to solve $(C_\sigma^h - C_\tau^h)a = d_{c_2} - b_{c_2}$, that is

$$\begin{pmatrix} i & -1-i & 1 \\ 0 & -i & 2 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} -1-i \\ -i \end{pmatrix}.$$

The vector $a = (0, 1, 0)$ is a solution to this equation. Hence, the set $\{(0, 1, 0)\}$ is a $ker(\sigma_h^*, \tau_h^*)$-cover of $ker(\sigma^{c_2}, \tau^{c_2})$.

Combining the covers computed for the two constants we obtain the matrix

$$D^i = \begin{pmatrix} 1 & 0 \\ i & 1 \\ 0 & 0 \end{pmatrix}.$$

Now, the singleton set containing

$$D = \begin{pmatrix} D^h & D^i \\ 0 & I \end{pmatrix}$$

represents a complete set of unifiers with constants of σ and τ. From D we can compute a unifier δ' of σ' and τ', which is represented by the substitution

$$[y_1/z + z + i(z) + c_1,\ y_2/i(z + z) + i(c_1) + c_2,\ y_3/i(i(z))]$$

□

8.5 Characterization of the Unification Type

We now characterize the unification type of a monoidal theory with respect to unification with constants by algebraic means.

A semiring is of *cover type infinitary* if for all right linear mappings λ, μ and vectors b, d there exists a minimal $ker(\lambda, \mu)$-cover of $ker(\lambda + b, \mu + d)$. A semiring is of cover type *finitary* or *unitary* if there always exists such a minimal $ker(\lambda, \mu)$-cover that is finite or a singleton, respectively. A semiring is of cover type *nullary* if it is not of type infinitary.

Example 8.14 By Proposition 8.10, every ring is of cover type unitary. Obviously, a finite semiring is of cover type finitary. Thus the boolean semiring **B** is of cover type finitary. The semiring of natural numbers **N** is of cover type finitary. □

As the main result of this subsection we show that for a monoidal theory $\mathcal{E}$ the unification type for unification with constants and the cover type of $\mathcal{S}_\mathcal{E}$ are the same.

Theorem 8.15 *Let $\mathcal{E}$ be a monoidal theory that is unitary for elementary unification. Then $\mathcal{E}$ is unitary, finitary, infinitary, or nullary for unification with constants if and only if $\mathcal{S}_\mathcal{E}$ is of cover type unitary, finitary, infinitary, or nullary, respectively.*

Proof. The claim on type nullary is equivalent to the claim on type infinitary, since a theory is nullary if and only if it is not infinitary, and a semiring is of cover

type nullary if and only if it is not of cover type infinitary. It remains to show the claim on the types infinitary, finitary, and unitary.

"$\Rightarrow$" Suppose that $\mathcal{E}$ is infinitary (finitary, unitary) with respect to unification with constants. We show that $\mathcal{S}_\mathcal{E}$ is of cover type infinitary (finitary, unitary).

Let λ, $\mu: \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^X$ be right linear and b, $d \in \mathcal{S}_\mathcal{E}^X$. Without loss of generality suppose that $C = \{c\}$ contains a single constant. Let σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ be the constant respecting mappings that satisfy $\sigma_h^* = \lambda$, $e_c\sigma_i^* = b$, and $\tau_h^* = \mu$, $e_c\tau_i^* = d$. Observe that $\sigma^c = \lambda + b$ and $\tau^c = \mu + d$.

Since $\mathcal{E}$ is infinitary with respect to unification with constants, there exists a minimal complete set U of unifiers with constants of σ and τ. By Theorem 8.5, the set

$$I_U = \{\delta_i \mid \delta \in U \text{ and } \delta_h \text{ is a most general unifier of } \sigma_h \text{ and } \tau_h\}$$

is a minimal complete set of inhomogeneous solutions for σ and τ that has the same cardinality as U. By Proposition 8.8, for every vector $a \in ker(\sigma^c, \tau^c)$ there is some $\eta \in I_U$ such that $e_c\eta^* \leq_K a$, where $K := ker(\sigma_h^*, \tau_h^*)$. Hence, $S := \{e_c\eta^* \mid \eta \in I_U\}$ is a K-cover of $ker(\sigma^c, \tau^c)$. Every $\eta \in I_U$ is uniquely determined by the value $e_c\eta^*$. Thus I_U and S have the same cardinality. Since for any δ, $\eta \in I_U$ we have $\delta \preceq_K \eta$ if and only if $e_c\delta^* \leq_K e_c\eta^*$, the minimality of I_U entails the minimality of S.

Now observe that $K = ker(\sigma_h^*, \tau_h^*) = ker(\lambda, \mu)$ and that $ker(\sigma^c, \tau^c) = ker(\lambda + b, \mu + d)$. Hence, S is a minimal $ker(\lambda, \mu)$-cover of $ker(\lambda + b, \mu + d)$ that has the same cardinality as U.

"$\Leftarrow$" Suppose that $\mathcal{S}_\mathcal{E}$ is of cover type infinitary. We show that for every unification problem with constants there exists a minimal complete set of unifiers with constants.

Let σ, $\tau: \mathcal{S}_\mathcal{E}^{X \cup C} \to \mathcal{S}_\mathcal{E}^{Y \cup C}$ respect constants. Since $\mathcal{E}$ is unitary, there exists a most general unifier δ of σ_h and τ_h. Since $\mathcal{S}_\mathcal{E}$ is of cover type infinitary, there exists for every constant $c \in C$ a minimal $ker(\sigma_h^*, \tau_h^*)$-cover S_c of $ker(\sigma^c, \tau^c)$. By Theorem 8.12, $U := \{\langle \delta, \eta_\mathbf{a} \rangle \mid \mathbf{a} \in \prod_{c \in C} S_c\}$ is a minimal complete set of unifiers with constants of σ and τ. This proves that $\mathcal{E}$ is infinitary for unification with constants if $\mathcal{S}_\mathcal{E}$ is of cover type infinitary.

Obviously, the cardinality of U is the product of the cardinalities of the covers S_c. Therefore, U is finite if each S_c is finite, and U is a singleton if each S_c is a singleton. This proves that $\mathcal{E}$ is finitary or unitary for unification with constants if $\mathcal{S}_\mathcal{E}$ is of cover type finitary or unitary, respectively. □

The above theorem allows us to draw a series of immediate conclusions, which are given in the following corollaries.

Corollary 8.16 *Let $\mathcal{E}$ be a monoidal theory such that $\mathcal{S}_\mathcal{E}$ is finite. Then $\mathcal{E}$ is finitary with respect to unification with constants.*

Proof. If $\mathcal{S}_\mathcal{E}$ is finite, then $\mathcal{E}$ is unitary by 7.11, and $\mathcal{S}_\mathcal{E}$ is of cover type finitary. Thus $\mathcal{E}$ is finitary with respect to unification with constants. □

Corollary 8.17 *Let $\mathcal{E}$ be a group theory. Then $\mathcal{E}$ has the same type with respect to unification with constants as with respect to unification without constants.*

Proof. By Theorem 7.6 we know that $\mathcal{E}$ is either unitary or nullary. If $\mathcal{E}$ is unitary then $\mathcal{E}$ is also unitary with respect to unification with constants, since $\mathcal{S}_\mathcal{E}$ is a ring and rings are of cover type unitary. If $\mathcal{E}$ is nullary then $\mathcal{E}$ is also nullary with respect to unification with constants. □

Corollary 8.18 (Unitary-Or-Nullary) *Let $\mathcal{E}$ be a group theory. Then $\mathcal{E}$ is either unitary or nullary with respect to unification with constants.*

Corollary 8.19 *A unitary group theory is also unitary with respect to unification with constants.*

Corollary 8.20 *A group theory with finitely many commuting homomorphisms is unitary with respect to unification with constants.*

Proof. By Corollary 7.17 a group theory with finitely many commuting homomorphisms is noetherian and thus unitary. □

Example 8.21 It follows from 8.20 that AG, AGH, and GAUSS are unitary with respect to unification with constants.

Corollary 8.16 implies that ACI is finitary with respect to unification with constants. It has been shown that ACI is not unitary [BB88].

It is well-known that AC is finitary with respect to unification with constants, but not unitary [LS76]. □

Until now we only know examples of unitary monoidal theories that are unitary or finitary with respect to unification with constants. In particular, we do not know whether unitary monoidal theories exist which are infinitary or nullary with respect to unification with constants. Since semirings and monoidal theories are closely related, the question whether such theories exist can be reformulated algebraically: Is there 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? By Corollary 8.17 we already know that such a semiring would be a proper semiring.

9 Conclusion

Many special monoidal theories, like AC, ACI, and the theory of abelian groups, turned out to be important in automated deduction. They have been built into the unification algorithms of theorem provers and into Knuth-Bendix-like completion procedures for term rewriting systems.

All of these theories have the common characteristic that unification problems can be reduced to linear equation systems over a semiring. For problems without constants the systems are homogeneous. If constants are present, inhomogeneous systems have to be solved in addition. In the case of elementary unification, problems either have a most general unifier, or arbitrarily general unifiers exist. In the case of unification with constants we have a similar result for group theories: a group theory has the same unification type with constants as it has without constants. In particular, group theories with finitely many commuting homomorphisms are unitary without and with constants.

Since the reduction of a given unification problem to linear equations is the same for all monoidal theories, we have been able to set up a general schema for unification algorithms. This has to be filled with a solution procedure for linear equations in order to yield a complete unification algorithm.

Since such an algorithm depends on the structure of the semiring, the general theory cannot go further. But algebra can still provide useful techniques. For instance, if the semiring is a field, Gauss's algorithm can be employed. A variant of Gauss's algorithm exists for solving linear equations over euclidean rings [Sim84]. Examples of such rings are the integers or the gaussian numbers. This yields, for instance, algorithms for the theories AG (cf. [LBB84]) and GAUSS.

In other cases special methods have to be developed. The widespread use of AC-unification motivated research on efficient algorithms for solving linear equations over the natural numbers [BCD90, CF89, Dom91, Hue78]. The paper by Baader and Büttner [BB88] on unification in ACI implicitly contains an algorithm for solving systems of linear equations over the boolean semiring $\mathbf{B}$, although it seems that the authors were not aware of this fact. Applying Gröbner Base techniques, Baader devised algorithms for the rings $\mathbf{Z}[X_1, \ldots, X_n]$ and $\mathbf{Z}\langle X_1, \ldots, X_n \rangle$ of polynomials over the integers with commuting and noncommuting variables. These rings correspond to the theories of abelian groups with n commuting and noncommuting homomorphisms, respectively [Baa90].

In [BN91] it has been shown how a unification algorithm for a monoidal theory $\mathcal{E} = (\Sigma, E)$ can be used for certain conservative extensions of $\mathcal{E}$. If H is a monoid, then the theory $\mathcal{E}\langle H \rangle$ is obtained from $\mathcal{E}$ by adding a set of generators of H to Σ, where they are considered as unary function symbols, and by adding to E identities which express that the new function symbols are composed in the same way as

the corresponding elements of the monoid H. For example, the theory ACH can be obtained from AC by adjoining a free monoid with one generator. The theory $\mathcal{E}\langle H\rangle$ is a conservative extension of $\mathcal{E}$. The semiring $\mathcal{S}_{\mathcal{E}\langle H\rangle}$ of $\mathcal{E}\langle H\rangle$ is isomorphic to the monoid semiring $\mathcal{S}_{\mathcal{E}}\langle H\rangle$, which is obtained from $\mathcal{S}_{\mathcal{E}}$ by adjoining the monoid H. Exploiting this algebraic structure, it has been shown in [BN91] how for finite monoids H an algorithm for $\mathcal{E}$ can be extended to an algorithm for $\mathcal{E}\langle H\rangle$.

Acknowledgements

Thanks go to Franz Baader, Hans-Jürgen Bürckert, and Jörg H. Siekmann for many discussions on the subject of this paper and their comments on draft versions. In particular, Franz provided me with a rich supply of pointers to the literature.

References

[Baa86] F. Baader. The theory of idempotent semigroups is of unification type zero. *J. Automated Reasoning*, 2(3):283–286, 1986.

[Baa89a] F. Baader. Unification in commutative theories. *J. Symbolic Computation*, 8(5):479–497, 1989.

[Baa89b] F. Baader. Unification properties of commutative theories: A categorical treatment. In D. H. Pitt, D. E. Rydeheard, P. Dybjer, A. M. Pitts, and A. Poigné, editors, *Proc. of the Summer Conference on Category Theory and Computer Science, Manchester (England)*, September 1989.

[Baa90] F. Baader. Unification in commutative theories, Hilbert's Basis Theorem, and Gröbner bases. SEKI-Report SR-90-01, Universität Kaiserslautern, Germany, 1990. Also: to appear in *J. ACM*.

[Baa91] F. Baader. Unification theory. In *Proc. of the Workshop on Word Equations and Related Topics, Tübingen (Germany)*, volume 572 of *Lecture Notes in Computer Science*. Springer-Verlag, 1991.

[BB88] F. Baader and W. Büttner. Unification in commutative idempotent monoids. *Theoretical Computer Science*, 56:345–352, 1988.

[BCD90] A. Boudet, E. Contejean, and H. Devie. A new AC-unification algorithm with a new algorithm for solving diophantine equations. In *Proc. 5th IEEE Symposium on Logic in Computer Science, Philadelphia (Pennsylvania, USA)*, pages 141–150. IEEE Computer Society Press, June 1990.

[BHSS89] H.-J. Bürckert, A. Herold, and M. Schmidt-Schauß. On equational theories, unification, and decidability. *J. Symbolic Computation*, 8(3,4):3–49, 1989.

[BN91] F. Baader and W. Nutt. Adding homomorphisms to commutative/monoidal theories or How algebra can help in equational unification. In R. V. Book, editor, *Proc. 4th International Conference on Rewriting Techniques and Applications, Como (Italy)*, volume 488 of *Lecture Notes in Computer Science*, pages 124–135. Springer-Verlag, April 1991.

[Bür89] H.-J. Bürckert. Matching—a special case of unification? *J. Symbolic Computation*, 8(5):523–536, 1989.

[Büt86] W. Büttner. Unification in the data structure multiset. *J. Automated Reasoning*, 2(1):75–88, 1986.

[CF89] M. Clausen and A. Fortenbacher. Efficient solution of linear diophantine equations. *J. Symbolic Computation*, 8, 1989.

[Dom91] E. Domenjoud. Solving systems of linear diophantine equations: An algebraic approach. In A. Tarlecki, editor, *Proc. 16th International Symposium on Mathematical Fondation of Computer Science, Kazimierz Dolny (Poland)*, volume 520 of *Lecture Notes in Computer Science*, pages 141–150. Springer-Verlag, September 1991.

[FH86] F. Fages and G. Huet. Complete sets of unifiers and matchers in equational theories. *Theoretical Computer Science*, 43(2,3):189–200, 1986.

[For87] A. Fortenbacher. An algebraic approach to unification under associativity and commutativity. *J. Symbolic Computation*, 3:217–229, 1987.

[Gog89] J. A. Goguen. What is unification? In H. Aït Kaci and M. Nivat, editors, *Resolution of Equations in Algebraic Structures, Volume 1, Algebraic Techniques*, pages 217–261. Academic Press, 1989.

[Grä68] G. Grätzer. *Universal Algebra.* Van Nostrand, Princeton, 1968.

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

[HS87] A. Herold and J. H. Siekmann. Unification in abelian semigroups. *J. Automated Reasoning*, 3:247–283, 1987.

[Hue78] G. Huet. An algorithm to generate the basis of solutions to homogeneous linear diophantine equations. *Information Processing Letters*, 7(3):144–147, 1978.

[Jac74] N. Jacobson. *Basic Algebra I.* Freeman and Company, San Francisco, 1974.

[Jac80] N. Jacobson. *Basic Algebra II.* Freeman and Company, New York, 1980.

[Kir90] C. Kirchner, editor. *Unification.* Academic Press, 1990.

[KS85] W. Kuich and A. Salomaa. *Semirings, Automata, Languages*, volume 5 of *EATCS Monographs on Theoretical Computer Science.* Springer-Verlag, 1985.

[LBB84] D. Lankford, G. Butler, and B. Brady. Abelian group unification algorithms for elementary terms. *Contemporary Mathematics*, 29, 1984.

[LS76] M. Livesey and J. H. Siekmann. Unification of sets and multisets. MEMOSEKI 76-II, Universität Karlsruhe, 1976.

[Plo72] G. Plotkin. Building in equational theories. In *Machine Intelligence*, volume 7, pages 73–90. Edinburgh University Press, 1972.

[RB85] D. E. Rydeheard and R. M. Burstall. A categorical unification algorithm. In *Proc. of the Workshop on Category Theory and Computer Programming*, volume 240 of *Lecture Notes in Computer Science*. Springer-Verlag, 1985.

[Rob65] J. A. Robinson. A machine-oriented logic based on the resolution principle. *J. ACM*, 12(1):23–41, 1965.

[Sie89] J. H. Siekmann. Unification theory: A survey. *J. Symbolic Computation*, 7(3,4):207–274, 1989.

[Sim84] C. C. Simms. *Abstract Algebra: A Computational Approach*. John Wiley & Sons, New York, 1984.

[SS86] M. Schmidt-Schauß. Unification under associativity and idempotence is of type nullary. *J. Automated Reasoning*, 2(3):277–281, 1986.

[SS89] M. Schmidt-Schauß. Unification in a combination of arbitrary disjoint equational theories. *J. Symbolic Computation*, 8(1,2):51–99, 1989.

[Sti75] M. E. Stickel. A complete unification algorithm for associative-commutative functions. In *Proc. of the 4th International Joint Conference on Artificial Intelligence, Tblisi (USSR)*, pages 71–82, 1975.

[Sti81] M. E. Stickel. A unification algorithm for associative-commutative functions. *J. ACM*, 28(3):423–434, 1981.

Deutsches
Forschungszentrum
für Künstliche
Intelligenz GmbH

DFKI
-Bibliothek-
PF 2080
D-6750 Kaiserslautern
FRG

DFKI Publikationen

Die folgenden DFKI Veröffentlichungen sowie die aktuelle Liste von allen bisher erschienenen Publikationen können von der oben angegebenen Adresse bezogen werden.
Die Berichte werden, wenn nicht anders gekennzeichnet, kostenlos abgegeben.

DFKI Publications

The following DFKI publications or the list of all publisched papers so far can be ordered from the above address.
The reports are distributed free of charge except if otherwise indicated.

DFKI Research Reports

RR-91-08
Wolfgang Wahlster, Elisabeth André, Som Bandyopadhyay, Winfried Graf, Thomas Rist: WIP: The Coordinated Generation of Multimodal Presentations from a Common Representation
23 pages

RR-91-09
Hans-Jürgen Bürckert, Jürgen Müller, Achim Schupeta: RATMAN and its Relation to Other Multi-Agent Testbeds
31 pages

RR-91-10
Franz Baader, Philipp Hanschke: A Scheme for Integrating Concrete Domains into Concept Languages
31 pages

RR-91-11
Bernhard Nebel: Belief Revision and Default Reasoning: Syntax-Based Approaches
37 pages

RR-91-12
J.Mark Gawron, John Nerbonne, Stanley Peters: The Absorption Principle and E-Type Anaphora
33 pages

RR-91-13
Gert Smolka: Residuation and Guarded Rules for Constraint Logic Programming
17 pages

RR-91-14
Peter Breuer, Jürgen Müller: A Two Level Representation for Spatial Relations, Part I
27 pages

RR-91-15
Bernhard Nebel, Gert Smolka: Attributive Description Formalisms ... and the Rest of the World
20 pages

RR-91-16
Stephan Busemann: Using Pattern-Action Rules for the Generation of GPSG Structures from Separate Semantic Representations
18 pages

RR-91-17
Andreas Dengel, Nelson M. Mattos: The Use of Abstraction Concepts for Representing and Structuring Documents
17 pages

RR-91-18
John Nerbonne, Klaus Netter, Abdel Kader Diagne, Ludwig Dickmann, Judith Klein: A Diagnostic Tool for German Syntax
20 pages

RR-91-19
Munindar P. Singh: On the Commitments and Precommitments of Limited Agents
15 pages

RR-91-20
Christoph Klauck, Ansgar Bernardi, Ralf Legleitner FEAT-Rep: Representing Features in CAD/CAM
48 pages

RR-91-21
Klaus Netter: Clause Union and Verb Raising Phenomena in German
38 pages

RR-91-22
Andreas Dengel: Self-Adapting Structuring and Representation of Space
27 pages

RR-91-23
Michael Richter, Ansgar Bernardi, Christoph Klauck, Ralf Legleitner: Akquisition und Repräsentation von technischem Wissen für Planungsaufgaben im Bereich der Fertigungstechnik
24 Seiten

RR-91-24
Jochen Heinsohn: A Hybrid Approach for Modeling Uncertainty in Terminological Logics
22 pages

RR-91-25
Karin Harbusch, Wolfgang Finkler, Anne Schauder: Incremental Syntax Generation with Tree Adjoining Grammars
16 pages

RR-91-26
M. Bauer, S. Biundo, D. Dengler, M. Hecking, J. Koehler, G. Merziger:
Integrated Plan Generation and Recognition
- A Logic-Based Approach -
17 pages

RR-91-27
A. Bernardi, H. Boley, Ph. Hanschke, K. Hinkelmann, Ch. Klauck, O. Kühn, R. Legleitner, M. Meyer, M. M. Richter, F. Schmalhofer, G. Schmidt, W. Sommer:
ARC-TEC: Acquisition, Representation and Compilation of Technical Knowledge
18 pages

RR-91-28
Rolf Backofen, Harald Trost, Hans Uszkoreit:
Linking Typed Feature Formalisms and Terminological Knowledge Representation Languages in Natural Language Front-Ends
11 pages

RR-91-29
Hans Uszkoreit: Strategies for Adding Control Information to Declarative Grammars
17 pages

RR-91-30
Dan Flickinger, John Nerbonne:
Inheritance and Complementation: A Case Study of *Easy* Adjectives and Related Nouns
39 pages

RR-91-31
H.-U. Krieger, J. Nerbonne:
Feature-Based Inheritance Networks for Computational Lexicons
11 pages

RR-91-32
Rolf Backofen, Lutz Euler, Günther Görz:
Towards the Integration of Functions, Relations and Types in an AI Programming Language
14 pages

RR-91-33
Franz Baader, Klaus Schulz:
Unification in the Union of Disjoint Equational Theories: Combining Decision Procedures
33 pages

RR-91-34
Bernhard Nebel, Christer Bäckström:
On the Computational Complexity of Temporal Projection and some related Problems
35 pages

RR-91-35
Winfried Graf, Wolfgang Maaß: Constraint-basierte Verarbeitung graphischen Wissens
14 Seiten

RR-92-01
Werner Nutt: Unification in Monoidal Theories is Solving Linear Equations over Semirings
57 pages

RR-92-02
Andreas Dengel, Rainer Bleisinger, Rainer Hoch, Frank Hönes, Frank Fein, Michael Malburg:
Π_{ODA}: The Paper Interface to ODA
53 pages

RR-92-03
Harold Boley:
Extended Logic-plus-Functional Programming
28 pages

RR-92-04
John Nerbonne: Feature-Based Lexicons: An Example and a Comparison to DATR
15 pages

RR-92-05
Ansgar Bernardi, Christoph Klauck, Ralf Legleitner, Michael Schulte, Rainer Stark:
Feature based Integration of CAD and CAPP
19 pages

RR-92-07
Michael Beetz:
Decision-theoretic Transformational Planning
22 pages

RR-92-08
Gabriele Merziger: Approaches to Abductive Reasoning - An Overview -
46 pages

RR-92-09
Winfried Graf, Markus A. Thies:
Perspektiven zur Kombination von automatischem Animationsdesign und planbasierter Hilfe
15 Seiten

RR-92-11
Susane Biundo, Dietmar Dengler, Jana Koehler:
Deductive Planning and Plan Reuse in a Command Language Environment
13 pages

RR-92-13
Markus A. Thies, Frank Berger:
Planbasierte graphische Hilfe in objektorientierten Benutzungsoberflächen
13 Seiten

RR-92-14
Intelligent User Support in Graphical User Interfaces:

1. InCome: A System to Navigate through Interactions and Plans
   Thomas Fehrle, Markus A. Thies
2. Plan-Based Graphical Help in Object-Oriented User Interfaces
   Markus A. Thies, Frank Berger

22 pages

RR-92-15
Winfried Graf: Constraint-Based Graphical Layout of Multimodal Presentations
23 pages

RR-92-17
Hassan Aït-Kaci, Andreas Podelski, Gert Smolka:
A Feature-based Constraint System for Logic Programming with Entailment
23 pages

RR-92-18
John Nerbonne: Constraint-Based Semantics
21 pages

DFKI Technical Memos

TM-91-01
Jana Köhler: Approaches to the Reuse of Plan Schemata in Planning Formalisms
52 pages

TM-91-02
Knut Hinkelmann: Bidirectional Reasoning of Horn Clause Programs: Transformation and Compilation
20 pages

TM-91-03
Otto Kühn, Marc Linster, Gabriele Schmidt:
Clamping, COKAM, KADS, and OMOS:
The Construction and Operationalization of a KADS Conceptual Model
20 pages

TM-91-04
Harold Boley (Ed.):
A sampler of Relational/Functional Definitions
12 pages

TM-91-05
Jay C. Weber, Andreas Dengel , Rainer Bleisinger:
Theoretical Consideration of Goal Recognition Aspects for Understanding Information in Business Letters
10 pages

TM-91-06
Johannes Stein: Aspects of Cooperating Agents
22 pages

TM-91-08
Munindar P. Singh: Social and Psychological Commitments in Multiagent Systems
11 pages

TM-91-09
Munindar P. Singh: On the Semantics of Protocols Among Distributed Intelligent Agents
18 pages

TM-91-10
Béla Buschauer, Peter Poller, Anne Schauder, Karin Harbusch: Tree Adjoining Grammars mit Unifikation
149 pages

TM-91-11
Peter Wazinski: Generating Spatial Descriptions for Cross-modal References
21 pages

TM-91-12
Klaus Becker, Christoph Klauck, Johannes Schwagereit: FEAT-PATR: Eine Erweiterung des D-PATR zur Feature-Erkennung in CAD/CAM
33 Seiten

TM-91-13
Knut Hinkelmann:
Forward Logic Evaluation: Developing a Compiler from a Partially Evaluated Meta Interpreter
16 pages

TM-91-14
Rainer Bleisinger, Rainer Hoch, Andreas Dengel:
ODA-based modeling for document analysis
14 pages

TM-91-15
Stefan Bussmann: Prototypical Concept Formation
An Alternative Approach to Knowledge Representation
28 pages

TM-92-01
Lijuan Zhang:
Entwurf und Implementierung eines Compilers zur Transformation von Werkstückrepräsentationen
34 Seiten

DFKI Documents

D-91-01
Werner Stein , Michael Sintek: Relfun/X - An Experimental Prolog Implementation of Relfun
48 pages

D-91-02
Jörg P. Müller: Design and Implementation of a Finite Domain Constraint Logic Programming System based on PROLOG with Coroutining
127 pages

D-91-03
Harold Boley, Klaus Elsbernd, Hans-Günther Hein, Thomas Krause: RFM Manual: Compiling RELFUN into the Relational/Functional Machine
43 pages

D-91-04
DFKI Wissenschaftlich-Technischer Jahresbericht 1990
93 Seiten

D-91-06
Gerd Kamp: Entwurf, vergleichende Beschreibung und Integration eines Arbeitsplanerstellungssystems für Drehteile
130 Seiten

D-91-07
Ansgar Bernardi, Christoph Klauck, Ralf Legleitner
TEC-REP: Repräsentation von Geometrie- und Technologieinformationen
70 Seiten

D-91-08
Thomas Krause: Globale Datenflußanalyse und horizontale Compilation der relational-funktionalen Sprache RELFUN
137 Seiten

D-91-09
David Powers, Lary Reeker (Eds.):
Proceedings MLNLO´91 - Machine Learning of Natural Language and Ontology
211 pages
Note: This document is available only for a nominal charge of 25 DM (or 15 US-$).

D-91-10
Donald R. Steiner, Jürgen Müller (Eds.):
MAAMAW´91: Pre-Proceedings of the 3rd European Workshop on „Modeling Autonomous Agents and Multi-Agent Worlds"
246 pages
Note: This document is available only for a nominal charge of 25 DM (or 15 US-$).

D-91-11
*Thilo C. Horstmann:*Distributed Truth Maintenance
61 pages

D-91-12
Bernd Bachmann:
$H^{iera}C_{on}$ - a Knowledge Representation System with Typed Hierarchies and Constraints
75 pages

D-91-13
International Workshop on Terminological Logics
Organizers: Bernhard Nebel, Christof Peltason, Kai von Luck
131 pages

D-91-14
Erich Achilles, Bernhard Hollunder, Armin Laux, Jörg-Peter Mohren: KRIS : Knowledge Representation and Inference System
- Benutzerhandbuch -
28 Seiten

D-91-15
Harold Boley, Philipp Hanschke, Martin Harm, Knut Hinkelmann, Thomas Labisch, Manfred Meyer, Jörg Müller, Thomas Oltzen, Michael Sintek, Werner Stein, Frank Steinle:
µCAD2NC: A Declarative Lathe-Worplanning Model Transforming CAD-like Geometries into Abstract NC Programs
100 pages

D-91-16
Jörg Thoben, Franz Schmalhofer, Thomas Reinartz:
Wiederholungs-, Varianten- und Neuplanung bei der Fertigung rotationssymmetrischer Drehteile
134 Seiten

D-91-17
Andreas Becker:
Analyse der Planungsverfahren der KI im Hinblick auf ihre Eignung für die Abeitsplanung
86 Seiten

D-91-18
Thomas Reinartz: Definition von Problemklassen im Maschinenbau als eine Begriffsbildungsaufgabe
107 Seiten

D-91-19
Peter Wazinski: Objektlokalisation in graphischen Darstellungen
110 Seiten

Unification in Monoidal Theories is Solving Linear Equations over Semirings

Werner Nutt

RR-92-01
Research Report