Symbolic Pattern Solving in Algebraic Structures

Dissertation

zur Erlangung des akademischen Grades
"Doktor der technischen Wissenschaften"

Eingereicht von

Dipl.-Ing. Olga Caprotti

March 1997

Erster Begutachter: Univ.-Doz. Dr. Hoon Hong
Zweiter Begutachter: Univ. Prof. Dr. Jochen Pfalzgraf

Angefertigt am Forschungsinstutut für Symbolisches Rechnen
Technisch-Naturwissenschaftliche Fakultät
Johannes Kepler Universität Linz

Eidesstattliche Erklärung

Ich versichere, daß ich die Dissertation selbständing verfaßt habe, andere als die angegebenen Quellen und Hilfsmittel nicht verwendet und mich auch sonst keiner unerlaubten Hilfe bedient habe.

Dipl.-Ing. Olga Caprotti

Linz, August 28, 1997

Supported by

ACCLAIM, (EP 7195): "Advanced Concurrent Constraint Languages"
CEI-PACT: "Programming Environments, Algorithms, Applications, Compilers and Tools for Parallel Computation", WP4 on *Parallel Computer Algebra*.

Abstract

This thesis introduces and develops a new method for finding symbolic solutions of equations in progressively richer algebraic structures. A symbolic solution, compared to corresponding 'numeric' answer, is advantageous because it is expressive, manipulatable, error-free and reusable. Intensive research in symbolic computation has already produced deep results, for instance in unification theory and computer algebra. But, it is not yet sufficient. As soon as the problems increase in complexity, whether for the number of equations, or their degree, or for the number of symbols involved, the symbolic methods fail to perform to the expectations of real-world applications. However, the problem instance often suggests a skeleton of the solution, a *solution pattern.* A promising approach, advocated here, uses these patterns to reduce the original complexity by requesting only solutions of a specific form. Pattern solving is successful if some substitution of the unknown coefficients, within the pattern, turns the pattern into a solution. The core of the method is the possibility of straightforward elimination of universally quantified variables from formulas related to the input problem and solution pattern. It is shown that fast elimination of universal quantifiers is complete in infinite integral domains, torsion-free modules over an infinite domain, finite dimensional division algebras over infinite fields, and in graded exterior algebras, if the underlying scalar field is infinite. These results promise that pattern solving can even be extended beyond the rich algebraic structures shown.

Zusammenfassung

Diese Arbeit stellt eine neue Methode für das Auffinden symbolischer Lösungen von Gleichungssystemen in fortschreitend reicheren algebraischen Strukturen vor. Eine symbolische Lösung hat (verglichen mit einer entsprechenden 'numerischen' Antwort) Vorteile in Bezug auf Ausdruckskraft, Manipulierbarkeit, Fehlerlosigkeit und Wiederverwendbarkeit. Intensive Forschung im Symbolischen Rechnen hat bereits zu tiefschürfenden Ergebnisen geführt, beispielsweise in der Unifikationstheorie und in der Computeralgebra. Dies ist allerdings noch nicht ausreichend. Sobald die Komplexität der Probleme ansteigt, sei es die Anzahl der Gleichungen, ihr Grad, oder die Anzahl der betroffenen Symbole, erfüllen die symbolischen Methoden nicht die Erwartungsanforderungen der realen Welt. Allerdings führt das Beispielsproblem oft zu einem Grundgerüst für eine Lösung d.h. zu einem *Lösungsmuster*. Ein vielversprechender Ansatz, der hier befürwortet wird, nutzt diese Muster um die ursprüngliche Komplexität zu reduzieren, indem nur Lösungen einer bestimmten Form angefordert werden. Dieses Lösen mit Hilfe von Mustern ist erfolgreich, wenn durch Ersetzung der unbekannten Koeffizienten (innerhalbs des Musters) das Muster in eine Lösung verwandelt wird. Der Kern der Methode besteht in der Möglichkeit einer geradlinigen Elimination universell quantifizierter Variablen aus bestimmten Formeln, die einen Bezug zum gegebenen Problem und zum Lösungsmuster haben. Es wird gezeigt, daß die schnelle Elimination universeller Quantoren vollständig ist in unendlichen Integritätsbereichen, in torsionsfreien Moduln über einem unendlichen Bereich, in endlichdimensionale Divisionsalgebren über unendlichen Körpern und in gradierten äußeren Algebren mit einem unendlichen Körper als Skalarbereich.

Acknowledgments

My sincere thanks go to my advisor, Dr. Hoon Hong who suggested the approach by patterns and strongly believed that I could work it out. His enthusiasm for science has always been a source of encouragement and a contagious disease. I want to thank him for the time he spent in discussions and explanations, for his lively lectures, that I will try to copy, and also for adding hectic to my life. I also want to thank him for devoting time to raise funds for the projects I worked in.
I am indebted to Prof. Bruno Buchberger for many reasons, first of all, for being one of the founders of symbolic computation. His views on computational mathematics will always accompany me and his teachings influence me. I admire his courage in turning a vision into reality; that vision turned a castle ruin into the Research Institute for Symbolic Computation. Being able to work in this atmosphere has been an incredible experience and an occasion to grow, both as a researcher and as a person.
These years would not have been as enjoyable if it wasn't for the colleagues. I thank all of them, but I want to mention Josef Schicho, who answered patiently my questions on parametrization, Ziming Li, who suggested the trick of substituting indeterminates used in one of the proofs, and Michael Joswig, with whom I talked about algebra. I thank all the STURM group for the wonderful team work in many occasions. I am grateful to Wolfgang Windsteiger, "Wind", for showing me how to fight LaTeX, and for introducing me to Austrian hospitality.
Last, I dedicate the thesis to my parents, to my brother and to Edward. Ai miei genitori, perché mi hanno educata a perseguire gli obiettivi e mi hanno lasciato la libertà di sceglierli. A mio fratello perché è sempre dalla mia parte. And to Edward, who understood me.

Alla mia famiglia.

...
Non domandarci la formula che mondi possa aprirti,
sí qualche storta sillaba e secca come un ramo.
Codesto solo oggi possiamo dirti,
ció che non siamo, ció che non vogliamo.

(E. Montale. Non chiederci la parola)

Contents

List of Figures

List of Tables

1

Introduction

This thesis introduces and develops a new approach, called "pattern solving", for finding symbolic solutions of (equational) constraints over arbitrary algebraic structures. Constraints occur in every branch of science, ranging from mechanical engineering to quantum physics. Constraints come in several forms, depending on the language used, but usually they are equations ($=$), inequations ($\neq$), and inequalities ($\leq, \geq, <, >$). Solving constraints in a specific algebraic structure means either deciding their truth, or finding values for the free variables that make the constraints true. In symbolic constraint solving, these values must be expressible as terms in the language of the algebraic structure. Symbolic solutions, compared to the corresponding 'numeric' answers, are advantageous for several reasons:

- they are expressive, they carry much more information than numeric solutions do, their form is often another description of the problem;
- they are easily manipulated further, used in further computations to derive new results, combined with other expressions and it is easy to reason with and about them;
- they are exact, no error is introduced during the computations since no approximations occur;
- they can be re-used over and over without need of a new computation, it is enough to substitute the proper values for the symbols.

Because of all these reasons, there has been intensive research in symbolic computation, around the topic of solving constraints, for instance in unification theory and in computer algebra. Both fields produced a wealth of deep results and there are now several computational methods available. However, all this is not yet sufficient. The state of the art symbolic methods usually cannot tackle real-world applications. As soon as the problems increase in complexity, whether for the number of constraints, or their degree or for the number of symbols involved, the symbolic methods fail to perform as efficiently as the numeric methods do.

A symbolic solution involves being very precise about the language in which the solution is given. Specifying the language might seem of no importance, but it is relevant. After the advent of computers, attention for the language, and the symbols of the language, has become more and more an issue. It is now clear that the language often determines the possibility of deciding a problem by computer. After Turing and Church defined precisely what is meant by algorithm and by computability, Gödel showed how some problems are inherently not computable, they are undecidable. Since then, many intractable problems have been found.

The constraints addressed in this thesis are equations. The complexity of symbolic solving of equational constraints ranges from polynomial-time decidable to undecidable, depending on the algebraic structure under consideration. Just consider Hilbert's Tenth Problem: given a polynomial equation with integer coefficients, find whether there are solutions over various algebraic structures. This famous equational constraint solving problem is unsolvable over the integers (Matijasevič, 1970), is decidable over the real numbers (Tarski, 1951), and is strongly believed to be undecidable over the rational numbers, where is still an open problem.

However, since undecidability is a property of a class of problems, one might focus on each instance of the class, very much like an engineer or a physicist does. In this fashion, an engineer or a physicist is able to compute in very "rich" algebraic structures. Moreover, the nature of the problem at hand often suggests a "skeleton" of the solution, a *solution pattern*. By using this pattern, "solving" becomes partly "verifying" whether this pattern is indeed a solution. The basic idea is one of reducing the complexity by guiding the solving process through this pattern, thereby requesting only solutions of a specific form. This thesis formalizes this methodology, henceforth referred to as *pattern solving*, explains it, derives an algorithm from it and investigates its applicability in various algebraic structures.

The "logical" core of the method and of the algorithm is the elimination of universally quantified variables from formulas related to the input problem and solution pattern. Pattern solving, in a specific algebraic structure, is effective only if the structure admits "straightforward" elimination of universal quantifiers for these specific formulas. The thesis addresses, for several structures, the necessary conditions for the easy elimination of universal quantifiers to be complete. Here, the emphasis is not showing that a structure admits elimination of quantifiers, because this has been answered extensively in the literature, but finding properties of the structure that allow efficient, fast elimination of universal quantifiers.

The "algebraic" core is to solve a system of equations for the unknown coefficients occurring in the solution pattern. This system of equations is related to the quantifier-free formula. The symbolic solution of this system, if it exists, yields an instance of the solution pattern that is a symbolic solution of the input problem. It is assumed that the resulting system of equations is simple enough to be effectively solvable by the available computational methods, specific to each algebraic structure. The justification is that, when using a "good" pattern, the original complexity of the input problem is reduced. Unsolvability at this step means that the proper pattern was not given. This also means that an engineer or a physicist does most of the work in 'guessing' the pattern.

Pattern solving is a clear example of how, in computational mathematics, the combination of the logical, axiomatic aspect with its algorithmic, algebraic aspect can be very fruitful.

1.1 Outline of the Thesis

The thesis is structured as a stepwise development of pattern solving in progressively richer algebraic structures, with respect to the signature of the languages.

Chapter 2 gives a brief overview of symbolic constraint solving in equational theories, where it is usually called unification. The algebraic structures studied in this context can be axiomatized by a finite set of universally quantified equations, or conditional equations. Although this covers important structures, it is not enough for capturing and modeling the richness of the computational domains of applicative problems in engineering and physics. In particular, fields and all structures built over fields are not equationally axiomatizable.

The goal of Chapter 2 is to introduce pattern solving. Two types of pattern solving problems will be introduced, one with no extra constants and one with a presentation of new constant symbols. For both problems, the general structure of the algorithm that solves the problem is described and its correctness is shown. The Chapter ends with a brief overview of the state of the art in problems related to pattern solving.

Starting from Chapter 4, pattern solving is developed, in the remaining chapters, for algebraic structures of increasing complexity with respect to the number of operations. The progression is as follows: the initial structure is commutative rings, developed Chapter 4. By adding another sort with operations, one obtains the structure of a module of a ring, this is studied in Chapter 5. A further generalization can be obtained by considering fields instead of rings, and algebras instead of modules, this yields the structure of associative commutative algebra over a field, studied in Chapter 6. An associative algebra in which commutativity does not necessarily hold is the exterior algebra over a vector space, the structure studied in Chapter 7.

Chapter 8 draws the conclusion that the work done in this thesis is just the beginning, and outlines some future directions.

2

Symbolic Constraint Solving

This chapter is an overview of the state of the art of constraint solving in equational theories. Axioms and constraints in these theories consist only of equations, as in semigroups, monoids, and groups. The most convenient model for equational theories is the term algebra. Constraint solving is solving term equations in the term algebra and is called *equational unification*. More precisely, unification studies the problem of algorithmically finding a term representation of the set of solutions.

Equational theories are indeed theoretically important. However, they are too weak to model real-world problems arising from areas such as mechanical engineering, nuclear physics, quantum chemistry and so on. Their major drawback is the expressiveness of the language. The attempts at overcoming this problem by studying combinations of several theories, each with its own language, have proven very cumbersome and are still at early stages. Moreover, several important computational domains are captured neither by equational theories nor by conditional equational theories.

This chapter is an introduction in unification theory motivated by an attempt at solving constraints in vector spaces over a field. It is by no means a complete description of the subject of unification. Section 2.1 recalls some basic notions and notations used to define unification problems. Equational unification is described in Section 2.2 with a brief sketch of unification procedures in Section 2.3. The state of the art in equational unification is summarized in Section 2.4. The decidability of a unification problem is a prerequisite to any attempt at designing an algorithm, especially in an area dealing with questions generally undecidable. Therefore, decidability of unification problems for classes of equational theories is addressed in Section 2.5. The final Section 2.6 discusses why it is not possible to utilize the techniques and results of unification theory to solve constraints in vector spaces.

2.1 Preliminary Notions

In this section the basic notions involved in the theory of unification are recalled. The reader who is trained in the subject may skip directly to the next section.

2.1.1 Signatures

One possible distinction among first-order languages considers whether the symbols are one-sorted or many-sorted. In the many-sorted case, one may distinguish between disjoint sorts or a hierarchy of sorts with a sub-sort/super-sort relation. This last case, called order-sorted language, is the most general one and comprises the other two.

In what follows, let S be a set of sort symbols, say s_1, $\mathsf{s}_2, \ldots$, and let X be a set of variables with sort, denoted like $x : \mathsf{s}$.

A set $A = \{A_\mathsf{s} \mid \mathsf{s} \in S\}$ is S-sorted if it is a family of sets A_s for each $\mathsf{s} \in S$. Given S-sorted sets A, B, an S-sorted function $f : A \to B$ is a family of functions $\{f_\mathsf{s} \mid f_\mathsf{s} : A_\mathsf{s} \to B_\mathsf{s}, \mathsf{s} \in S\}$.

DEFINITION 2.1
A many-sorted signature is a pair $\Sigma = (S, \mathcal{F})$ *where*

(a) S *is a set of sorts;*

(b) $\mathcal{F} = \{\mathcal{F}_{\mathsf{w},\mathsf{s}} \mid \mathsf{w} \in S^*, \mathsf{s} \in S\}$ *is an* $S^* \times S$*-sorted set of function symbols;*

For $f \in \mathcal{F}_{\mathsf{w},\mathsf{s}}$, we call w the arity and s the sort of f and write $f : \mathsf{w} \to \mathsf{s}$. A special case is the set $\mathcal{F}_{\lambda,\mathsf{s}}$ of constant symbols of sort s.

A sort $\mathsf{s} \in S$ is strict iff either the set $\mathcal{F}_{\lambda,\mathsf{s}}$ is not empty or the set $\mathcal{F}_{\mathsf{w},\mathsf{s}}$ is not empty and each sort s_i in $\mathsf{w} = \mathsf{s}_1 \ldots \mathsf{s}_n$, $1 \leq i \leq n$ is strict. A signature is strict iff each sort in S is strict.

In the order-sorted case, the set of sorts S is equipped by a partial order $\leq$ defined as the least partial order containing sub-sort declarations of the form $\mathsf{s}_1 \leq \mathsf{s}_2$. Not comparable sorts are denoted as $\mathsf{s}_1 \bowtie \mathsf{s}_2$. A pair $(S, \leq)$ is a partially ordered set (poset), if $\leq \subseteq S \times S$ is reflexive, transitive and antisymmetric.

DEFINITION 2.2
An order-sorted signature is a triple $\Sigma = (S, \leq, \mathcal{F})$ *such that* $(S, \mathcal{F})$ *is a signature and* $(S, \leq)$ *is a poset.*

A signature is finite if the set of sorts, of sub-sort declarations, and of functions are all finite.

2.1.2 Order-Sorted Structures

The main definitions and results from Jouannaud and Kirchner (1990); Meseguer *et al.* (1990) concerning order-sorted structures are recalled next.

Let $\Sigma = (S, \leq, \mathcal{F})$ be an order-sorted signature.

DEFINITION 2.3
A Σ*-structure* $\mathfrak{A} = \langle A, \mathcal{F}_A \rangle$ *consists of an* S*-indexed carrier set* $A = \{A_\mathsf{s} \mid \mathsf{s} \in S\}$ *and a family of functions* $\mathcal{F}_A = \{f_A \mid f_A : A_{\mathsf{s}_1} \times \ldots A_{\mathsf{s}_n} \to A_\mathsf{s}$ *for all* $(f : \mathsf{s}_1 \ldots \mathsf{s}_n \to \mathsf{s}) \in \mathcal{F}_{\mathsf{s}_1 \ldots \mathsf{s}_n, \mathsf{s}}\}$ *such that monotonicity conditions hold:*

(1) if $\mathsf{r} \leq \mathsf{s}$ *in* S*, then* $A_\mathsf{r} \subseteq A_\mathsf{s}$*;*

(2) if $f \in \mathcal{F}_{\mathsf{s}_1,\mathsf{s}} \cap \mathcal{F}_{\mathsf{s}_2,\mathsf{s}}$*, and* $\mathsf{s}_1 \leq \mathsf{s}_2$*, then* $f_A : A_{\mathsf{s}_2} \to A_\mathsf{s}$ *is identical to* $f_A : A_{\mathsf{s}_1} \to A_\mathsf{s}$ *on* A_{s_1}*.*

For a many-sorted signature $(S, \mathcal{F})$, the monotonicity conditions are not required and the resulting structure is called an $(S, \mathcal{F})$-structure.

The set of *ground* Σ*-terms* of sort $\mathsf{s} \in S$ is the smallest set $\mathcal{T}_\mathsf{s}(\Sigma)$ such that:

(a) $f \in \mathcal{T}_{\mathsf{s}}(\Sigma)$ and there is a declaration $(f :\rightarrow \mathsf{r})$ in $\mathcal{F}$ such that $\mathsf{r} \leq \mathsf{s}$;

(b) $f(t_1, \ldots, t_n) \in \mathcal{T}_{\mathsf{s}}(\Sigma)$ and there is a declaration $(f : \mathsf{r}_1 \ldots \mathsf{r}_n \rightarrow \mathsf{r})$ in $\mathcal{F}$ such that $\mathsf{r} \leq \mathsf{s}$, and $t_i \in \mathcal{T}_{\mathsf{r}_i}(\Sigma)$ for $1 \leq i \leq n$.

$\mathcal{T}(\Sigma) = \{\mathcal{T}_{\mathsf{s}}(\Sigma) \mid \mathsf{s} \in S\}$ is the set of all ground Σ-terms. Note that a term $t \in \mathcal{T}_{\mathsf{s}}(\Sigma)$, in short $t : \mathsf{r}$, can have multiple sorts, precisely $t : \mathsf{s}$ for all $\mathsf{r} \leq \mathsf{s}$. A signature Σ is regular if every Σ-term has a least sort $\mathcal{LS}(t)$, (non regular is e.g. $\{a :\rightarrow \mathsf{s}_1, a :\rightarrow \mathsf{s}_2\}$). Regularity of a finite signature is a decidable property (Smolka, 1989, see).

Definition 2.4
Let $(S, \mathcal{F})$ be a many-sorted signature and $\mathfrak{A}$, $\mathfrak{B}$ be $(S, \mathcal{F})$-structures. A $(S, \mathcal{F})$-homomorphism $h : \mathfrak{A} \rightarrow \mathfrak{B}$ is an S-sorted function $\{h_{\mathsf{s}} \mid h_{\mathsf{s}} : A_{\mathsf{s}} \rightarrow B_{\mathsf{s}}, \mathsf{s} \in S\}$ such that:

$$\begin{aligned} h_{\mathsf{s}}(f_A) &= f_B, & f &\in \mathcal{F}_{\lambda,\mathsf{s}} \\ h_{\mathsf{s}}(f_A(a)) &= f_B(h_{\mathsf{w}}(a)), & f &\in \mathcal{F}_{\mathsf{w},\mathsf{s}}, a \in A_{\mathsf{w}}, \end{aligned}$$

where $h_{\mathsf{w}}(a) = \langle h_{\mathsf{s}_1}(a_1), \ldots, \mathsf{s}_n(a_n)\rangle$, $\mathsf{w} = \mathsf{s}_1 \ldots \mathsf{s}_n, a = \langle a_1, \ldots, a_n\rangle$, $a_i \in A_{\mathsf{s}_i}(1 \leq i \leq n)$.

Definition 2.5
Let $\mathfrak{A}$,$\mathfrak{B}$ be Σ-structures. A Σ-homomorphism $h : \mathfrak{A} \rightarrow \mathfrak{B}$ is a $(S, \mathcal{F})$-homomorphism such that, if $\mathsf{s} \leq \mathsf{r}$, then $h_{\mathsf{s}}(a) = h_{\mathsf{r}}(a), a \in A_{\mathsf{s}}$.

$\mathcal{T}(\Sigma)$ is a Σ-structure called term structure and is obtained by taking as carrier set $A = \mathcal{T}(\Sigma)$, and as functions $f_A(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$. The term structure has the important property of being initial in the class of all Σ-structures. This means that given an arbitrary Σ-structure $\mathfrak{A}$, there is a unique homomorphism $h : \mathcal{T}(\Sigma) \rightarrow \mathfrak{A}$.

A set of Σ-variables $X = \{X_{\mathsf{s}} \mid \mathsf{s} \in S\}$ is an S-sorted set of variable symbols. Let X and $\mathcal{F}$ be disjoint sets. A new signature $(S, \leq, \mathcal{F} \cup X)$ can be built by considering the variables as new constant symbols, such that:

(a) $(\mathcal{F} \cup X)_{\lambda,\mathsf{s}} = \mathcal{F}_{\lambda,\mathsf{s}} \cup X$;

(b) $(\mathcal{F} \cup X)_{\mathsf{w},\mathsf{s}} = \mathcal{F}_{\mathsf{w},\mathsf{s}}$ for $\mathsf{w} \neq \lambda$.

Then the term structure $\mathcal{T}(\Sigma, X)$ is also a Σ-structure.

An assignment $\alpha : X \rightarrow \mathfrak{A}$ from a variable set X to a Σ-structure $\mathfrak{A}$ is a S-sorted function $\{\alpha_{\mathsf{s}} : X_{\mathsf{s}} \rightarrow \mathfrak{A}_{\mathsf{s}} \mid \mathsf{s} \in S\}$.

Theorem 2.1
The structure $\mathcal{T}(\Sigma, X)$ is the free Σ-structure generated by X if for every Σ-structure $\mathfrak{A}$ and every assignment $\alpha : X \rightarrow \mathfrak{A}$, there is a unique homomorphism $\alpha^* : \mathcal{T}(\Sigma, X) \rightarrow \mathfrak{A}$ extending α.

A *substitution* $\sigma : D(\sigma) \rightarrow \mathcal{T}(\Sigma, X)$ is an assignment from a set of variables $D(\sigma) \subseteq X$, the domain of σ, to the term structure $\mathcal{T}(\Sigma, X)$, that preserves sorts: for all $x \in D(\sigma)$ if $x : \mathsf{s}$ then $x\sigma : \mathsf{s}$. A substitution σ mapping variables $x_1, \ldots, x_n$ to terms $t_1, \ldots, t_n$ respectively, is usually denoted by $\sigma = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$.

2.1.3 Equations and Equational Presentations

A Σ-*equation* $(\forall X)\ t = t'$ is defined as a triple (X, t, t') where X is a set of variables and $t, t' \in \mathcal{T}(\Sigma, X)$ are terms. When X consists of the variables occurring in t and t', it is omitted.

Definition 2.6
Let $\mathfrak{A}$ be a Σ-structure. An equation $(\forall X)\ t = t'$ is valid in $\mathfrak{A}$,

$$\mathfrak{A} \models (\forall X)\ t = t'$$

iff for all the assignments $\alpha : X \to \mathfrak{A}$, $\alpha^*(t) = \alpha^*(t')$.

An equation $(\forall X)\ t = t'$ is satisfied in $\mathfrak{A}$ iff there exists an assignment $\alpha : X \to \mathfrak{A}$, such that $\alpha^*(t) = \alpha^*(t')$.

An Σ-structure $\mathfrak{A}$ is a *model* of a set of equations E iff every equation in E is valid in $\mathfrak{A}$. Let $\mathrm{Mod}(E)$ be the set of Σ-structures that are models of the Σ-equations E.

An *order-sorted equational presentation* $\mathcal{S} = (\Sigma, E)$ consists of a signature Σ and a set of Σ-equations E, called *axioms*.

Definition 2.7
Given an order-sorted equational presentation $\mathcal{S} = (\Sigma, E)$, the equational theory *of $\mathcal{S}$, or E-equality, is the smallest congruence $=_E \subseteq \mathcal{T}(\Sigma, X) \times \mathcal{T}(\Sigma, X)$ containing all equalities of the form $(l\sigma = r\sigma)$ for all $(l = r) \in E$ and all substitutions σ.*

A presentation is regular if its signature is. A regular presentation $\mathcal{S} = (\Sigma, E)$ is sort-preserving if $t =_E t'$ implies that $\mathcal{LS}(t) = \mathcal{LS}(t')$.

The Σ-structure $\mathcal{T}(\Sigma, X)_E = \mathcal{T}(\Sigma, X)/ =_E$ is free in $\mathrm{Mod}(E)$. Therefore, given any model $\mathfrak{A} \in \mathrm{Mod}(E)$ and any assignment $\alpha : X \to \mathfrak{A}$, there is a unique extension to a Σ-homomorphism, $\alpha^* : \mathcal{T}(\Sigma, X)_E \to \mathfrak{A}$. When the signature is strict, the Σ-structure $\mathcal{T}(\Sigma)_E = \mathcal{T}(\Sigma)/ =_E$ is initial in $\mathrm{Mod}(E)$. Hence, given any model $\mathfrak{A} \in \mathrm{Mod}(E)$ there is a unique homomorphism, $h : \mathcal{T}(\Sigma)_E \to \mathfrak{A}$.

By Birkhoff's theorem, it is true that for any $t, t' \in \mathcal{T}(\Sigma, X), t =_E t'$ iff $t = t'$ is valid in $\mathrm{Mod}(E)$, that is iff $\mathcal{T}(\Sigma, X)_E \models t = t'$.

2.2 Equational Unification

Let $\mathcal{S} = (\Sigma, E)$ be an order-sorted equational presentation.

Definition 2.8
A system of $(S, \leq, \mathcal{F})$-equations:

$$\langle t_1 = u_1, \ldots, t_n = u_n \rangle,\ n \geq 1,\ t_i, u_i \in \mathcal{T}(\Sigma, X)$$

is E-unifiable, *iff there exists a substitution $\sigma : X \to \mathcal{T}(\Sigma, X)$ such that*

$$t_i\sigma =_E u_i\sigma,\ 1 \leq i \leq n.$$

The set of E-unifiers of a system Γ is denoted by $\mathrm{U}_E(\Gamma)$. Let $W \subseteq X$ be a set of variables. Consider the quasi-ordering $\leq_E [W]$ on substitutions, defined by:

$$\sigma \leq_E \theta[W] \quad \text{iff there exists a substitution } \lambda \text{ such that } x\theta =_E x\sigma\lambda, \forall x \in W.$$

When $\sigma \leq_E \theta[W]$, θ is called and E-instance of σ on W and σ is called more general than θ on W.

Example 2.1
Let $\mathcal{F}_{\lambda,\mathsf{s}} = \{a, b\}$ and $\mathcal{F}_{\mathsf{ss},\mathsf{s}}$=$\{+\}$. Suppose that $+$ is commutative (C). Then the equation

$$x + y =_C a + b$$

has two C-unifiers

$$\{x \leftarrow a, y \leftarrow b\} \qquad \{x \leftarrow b, y \leftarrow a\}$$

that are not instance of one another.

In the following, let $W = \mathrm{Vars}(\Gamma)$. Rather than the whole set of unifiers $\mathrm{U}_E(\Gamma)$, one is interested in a *complete set* of unifiers. A complete set $\mathrm{cU}_E(\Gamma)$ of unifiers for a problem Γ is such that:

(1) $\mathrm{cU}_E(\Gamma) \subseteq \mathrm{U}_E(\Gamma)$
(2) for all $\theta \in \mathrm{U}_E(\Gamma)$, there exists $\sigma \in \mathrm{cU}_E(\Gamma)$ such that $\sigma \leq_E \theta[W]$.

It is also desirable that the set be as small as possible. A *minimal complete set* $\mu\mathrm{U}_E(\Gamma)$ is a complete set of E-unifiers for Γ that additionally satisfies:

(3) for all $\sigma, \theta \in \mu\mathrm{U}_E(\Gamma)$, $\sigma \leq_E \theta[W]$ implies that $\sigma = \theta$.

When a minimal complete set of unifiers exists, it is unique up to the equivalence $\equiv_E$ defined by:

$$\sigma \equiv_E \theta[W] \qquad \text{iff} \qquad \sigma \leq_E \theta[W], \quad \theta \leq_E \sigma[W]. \tag{2.1}$$

Therefore, equational theories E can be distinguished according to the existence and cardinality of the set of minimal complete unifiers. A theory E is of *unification type*:

1, or unitary, if for all Γ, $\mu\mathrm{U}_E(\Gamma)$ exists and its cardinality is at most 1;

ω, or finitary, if for all Γ, $\mu\mathrm{U}_E(\Gamma)$ exists and is finite;

∞, or infinitary, if for all Γ, $\mu\mathrm{U}_E(\Gamma)$ exists but it can be infinite;

0, or nullary, if for some Γ, $\mu\mathrm{U}_E(\Gamma)$ does not exist.

In the definitions above, the unification problem Γ can be either a single equation or a system of equations. This makes no difference for the case of unitary and finitary theories. In fact, from an algorithm for single equation, it is possible to derive an algorithm for a finite system of equations. However, there exists an equational theory which is infinitary when Γ contains a unique equation but is nullary when Γ is a system of equations. Moreover, there is a theory E for which E-unifiability of a single equation is decidable whereas it is undecidable for systems of equations.

2.3 Algorithms

A E-unification algorithm is an algorithm that decides whether a problem Γ is unifiable under a given equational theory E, and if it is, it computes a minimal complete set of E-unifiers for Γ. Computing a minimal set of E-unifiers, although desirable, it is often too expensive. A *E-unification procedure* is not required to decide E-unifiability but merely to enumerate a complete set of unifiers. In the optimal case a E-unification procedure enumerates a minimal complete set of unifiers.

The first E-unification algorithm was the algorithm for the empty theory, the transformation algorithm is given in Figure 2.1. Intuitively, a transformation algorithm works by transforming non-deterministically the initial problem according to rules. The rules are applied until a "solved form" is found from which a solution can be extracted very easily. It is assumed that the equations are unoriented, so that rules apply also in the reflexive case. For simplicity, there is only one sort but the order-sorted extension is straightforward in this case.

Remove Identities

$$\Gamma \cup \{s \doteq s\} \quad \Longrightarrow \quad \Gamma$$

Decompose

$$\Gamma \cup \{f(\vec{s}) \doteq f(\vec{t})\} \quad \Longrightarrow \quad \Gamma \cup \{s_1 \doteq t_1, \ldots, s_n \doteq t_n\}$$

Variable Elimination

$$\Gamma \cup \{x \doteq t\} \quad \Longrightarrow \quad \Gamma\{x \leftarrow t\} \cup \{x \doteq t\},$$

where x does not occur in t but occurs in Γ

Figure 2.1: Unification Rules for the Empty Theory

Unification algorithms for specific theories E differ very much and there is no general guideline for designing them. One way to approach the problem of designing a unification algorithm for a specific theory E is by optimizing the universal unification procedure. A unification procedure is called *universal* if it works for any arbitrary equational theory (or for a class of theories). Given as input a presentation of an equational theory E and a unification problem Γ, the output of a universal unification procedure is a "complete set" of E-unifiers for Γ. Observe that a trivial universal procedure can be obtained by recursively enumerating the substitutions and checking whether they are E-unifiers for Γ, hence the question is mainly one of efficiency.

In the literature, universal unification algorithms in terms of transformation rules have been proposed, among others, by Kirchner (1984); Gallier and Snyder (1987); Hsiang and Jouannaud (1988); Gallier and Snyder (1990). They are inspired by Herbrand (1930) and by Martelli and Montanari (1982) who worked out the algorithm for unification in the empty theory. Figure 2.1 recalls the transformation rules for unification in the empty theory. In order to obtain a universal E-unification procedure, the rule for "paramodulation" or the rule for "narrowing", see Figure 2.2, have to be added to those for syntactic unification in Figure 2.1.

2.4 Unification in Equational Theories

This section briefly recalls some well-known results in equational unification theory. For a detailed account, the reader may refer to the surveys (Jouannaud and Kirchner, 1991;

Lazy Paramodulation			
	$\Gamma \cup \{s \doteq t\}$	$\Longrightarrow$	$\Gamma \cup \{s_{\mid\beta} \doteq l, s[\beta \leftarrow r] \doteq t\}$, where $s_{\mid\beta}$ is a non-variable subterm, and $l = r$ is an equation in E
Narrowing			
	$\Gamma \cup \{s \doteq t\}$	$\Longrightarrow$	$\Gamma \cup \{s_{\mid\beta} \doteq l, s[\beta \leftarrow r] \doteq t\}$, where $s_{\mid\beta}$ is a non-variable subterm, and $l = r$ is an equation in E

Figure 2.2: Additional Unification Rules for an Equational Theory E

Siekmann, 1989; Baader and Siekmann, 1994), here are reported the summarizing tables.

Unification is very sensitive to the language over which the terms are built. Let the signature of an equational presentation, $sig(E)$, be the set of function and constant symbols occurring in the axioms of E and let Γ be a problem, then there are three types of E-unification:

elementary, when Γ contains only symbols in $sig(E)$;

with constants, when Γ contains also free constant symbols (constant symbols not in $sig(E)$);

general, when Γ contains also free function symbols (function symbols not in $sig(E)$);

Regarding the signature $sig(E)$ of a theory E, it must be recalled that Bockmayr (1989) showed how $sig(E)$ is relevant for the decidability of E-unification. For instance, unification is decidable for the theory of inverse semigroups in the signature $\Sigma = \langle *, ^{-1}, a\rangle$ but becomes undecidable in the augmented signature $\Sigma = \langle *, ^{-1}, a, b\rangle$.

Table 2.1 recalls some of the most studied equational axioms. Table 2.2 fixes the abbreviation and a presentation for some well-known equational theories.

Recall that the E-unification problem is decidable iff there exists an algorithm that, for any system of equations Γ, decides whether Γ is E-unifiable. For many equational theories unifiability is undecidable. For instance, undecidability of Hilbert's 10th problem is equivalent to undecidability of unification in the theory $CR1$ of commutative rings with unity. Solvability corresponds to solvability of polynomial equations over the integers which was shown to be undecidable by Matijasevič (1970). A stronger result holds: every theory in the signature of CRU whose axioms contain those of D_A and are contained in those of CRU has a undecidable elementary unification problem, (Arnborg and Tidén, 1985, see).

Nutt (1991) has also shown that the unification type of an equational theory is undecidable: given an arbitrary finite presentation of an equational theory E, there is no general algorithm that decides the unification type of E.

An idea of the state of the art on E-unification can be obtained by looking at the results reported in Table 2.3 for several equational theories. A distinction is made for general, with constant, or elementary unification. The unification type and the decidability type are reported. The empty slots corresponds to cases for which the author has found no literature. Available complexity result have been also listed. It is clear that decidability of general unification implies also decidability of the other unification problems. Likewise, undecidability of the elementary type implies undecidability of the other unification problems. Also,

Abbreviation	Name	Equational Axiom
$A(f)$	Associativity	$f(f(x,y),z) = f(x,f(y,z))$
$C(f)$	Commutativity	$f(x,y) = f(y,x)$
$D_R(f,g)$	Right Distributivity	$f(g(x,y),z) = g(f(x,z),f(y,z))$
$D_L(f,g)$	Left Distributivity	$f(z,g(x,y)) = g(f(z,x),f(z,y))$
$D(f,g)$	Distributivity	$D_R(f,g) \cup D_L(f,g)$
$I(f)$	Idempotency	$f(x,x) = x$
$E(h,*)$	Endomorphism	$h(x*y) = h(x)*h(y)$
$H(h,*,+)$	Homomorphism	$h(x*y) = h(x)+h(y)$
$Inv_R(*,i,e)$	Right Inverse	$x*i(x) = e$
$Inv_L(*,i,e)$	Left Inverse	$i(x)*x = e$
$U_R(*,e)$	Right Unit	$x*e = x$
$U_L(*,e)$	Left Unit	$e*x = x$
$S_R(f,g,h)$	Right Simplification	$f(g(x,y),h(y)) = x$
$S_L(f,g,h)$	Left Simplification	$f(h(y),g(y,x)) = x$
$C_R(f,g,h)$	Right Commutativity	$f(f(x,y),z) = f(f(x,z),y)$
$C_L(f,g,h)$	Left Commutativity	$f(x,f(y,z)) = f(y,f(x,z))$
$L(*)$	Lie Brackets	$(x*y)*z = z*(y*x)$
$T(f,g)$	Transitivity	$f(g(x,y),g(y,z)) = f(g(x,y),g(x,z))$
$Cur(f,g)$	Currying	$f(x,f(y,z)) = f(g(x,y),z)$

Table 2.1: Axioms Abbreviations

Abbreviation	Theory Name	Equational Axioms
AI	Band	$A(f), I(f)$
AC	Monoid	$A(f), C(f)$
$ACU(f,e)$	Monoid	$AC(f), U_R(f,e)$
AG	Abelian Group	$ACU(*,e), Inv_R(*,i,e)$
QG	Quasi Group	$S_L(., h), S_R(., /, h), h(x) = x$
BR	Boolean Ring	$ACU(+,0), ACU(*,1), I(*), D_R(*,+)$
CRU	Commutative Rings with Unit	$ACU(+,0), Inv_R(+,-,0), AC(*), D_R(*,+)$
D_A		$D(f,g), A(g)$
CC	Closed Categories	$ACU(\times,1), U_L(\Rightarrow,1), Cur(\times,\Rightarrow)$
CCC	Cartesian-Closed Categories	$CC, U_R(\Rightarrow,1), D_L(\times,\Rightarrow)$
DV	Discriminator Varieties	
L	Lattices	
DL	Distributive Lattices	

Table 2.2: Theories Abbreviations

finitary or unitary theories have clearly a decidable unification problem.

Abbreviation	General		with Constants		Elementary	
	decidability	type	decidability	type	decidability	type
$\emptyset$	yes	1				
$A(f)$	yes	∞	NP-h	∞		
$C(f)$		ω	NP-c	ω		
$I(f)$	yes	ω				
$AC(f)$	NP	ω	NP-h	ω		ω
$ACU(f,1)$	NP	ω		ω		1
$AC(f), U_R(f,1), I(f)$				ω		1
$AI(f)$	yes	0	NP-h	0		
$D_R(f,g)$	yes	1	P	1		
$D_L(f,g)$	yes	1	P	1		
$D_L(f,g), A(g), U_R(f,1)$	no	∞				
$D(f,g)$	?	∞				
$D(f,g), C(f), C(g)$	?	∞				
$D(f,g), AI(f), AI(g)$	yes	?				
$D(f,g), AC(g)$	no	∞				
$E(h,*)$	yes	1				
$E(h,*), AC(*)$	?	∞				
$H(h,*,+)$	yes	1				
$H(h,*,+), A(+)$	yes	∞				
$H(h,*,+), AC(+)$	yes	ω				
$C_R(f)$	yes	ω				
$Cur(f,g)$						
AG			P	1		1
QG	yes	ω				
BR			NP-c	1	yes	1
D_A	no	∞	no		no	
CRU					no	
CC			NP-c			
CCC			no			

Table 2.3: Equational Unification

The universal procedure for unification in an arbitrary equational theory is called narrowing. A summary of the completeness results of narrowing with respect to the presentation of the theory is given in Table 2.4 below and is taken from (Middeldorp and Hamoen, 1994), to which the reader is referred for further details.

2.4.1 Unification in Order-Sorted Signatures

Unification has been studied for the most in simple-sorted presentations. However, some work has also been done for the more complicated case of order-sorted equational presentations. In order-sorted signatures, sorts are ordered by a subsort relation and operator symbols may be overloaded. It is the feeling of the author that the order-sorted framework

TRS	Narrowing	Basic Narrowing
complete	Y	Y
semi-complete	Y	right linear
confluent	wrt n.s.	right linear wrt n.s.
orthogonal	wrt n.s.	wrt n.s. and g.
weakly normalizing orthogonal		Y

CTRS	Cond. Narrowing	Cond. Basic Narrowing
complete 1	Y	N
semi-complete 1	Y	
confluent 1	wrt n.s.	decreasing
complete 2	N	
level-confluent 2 wrt n.s.	N	
level-complete 2	Y	Y
level semi-complete 2		
level-complete 3	Y	

Table 2.4: Unification by Narrowing

has not yet found natural examples of applications beside the examples taken form the realm of algebraic specification.

When a specification is sort decreasing, then the results on completeness of equational deduction of the many sorted case apply. In particular, the theorem of McKinsey-Malcev on Quasivarieties and Birkhoff's Variety theorem has been stated for order-sorted algebras.

Theorem 2.2 (Goguen and Meseguer (1992))

1. *A class of $(S, \leq, \mathcal{F})$-algebras is definable by some set of conditional equations Γ iff it is closed under products, subalgebras, and filtered colimits.*
2. *A class of $(S, \leq, \mathcal{F})$-algebras is definable by some set of (unconditional) equations Γ iff it is closed under products, subalgebras, and homomorphic images.*

Condition 2.2-(1) means that the class is an implicational variety, and condition 2.2-(2) means that the class is a variety.

Unification is more complicated than in the case of simple sorted sorted signatures. Syntactic unification is not unitary in general and the size of a minimal complete set of unifiers may grow exponentially with the number of variables. For certain signatures, the unifiability problem is known to be NP-complete.

Meseguer *et al.* (1990) characterizes when an order-sorted signature has a minimal (or finite, or most general if solvable) family of order-sorted E-unifiers for a system of equations Γ, where E is a set of axioms sort preserving and not restricting the sorts of the variables. Waldmann (1989) gives a criterion for unitary unifiability in order-sorted signatures. Moreover, it is shown that when the axioms of E are sort preserving (equal terms have equal sorts - in particular constants), overloaded and non-overloaded E-equality are the same.

As far as the author knows, there is no published result on decidability of unification for specific classes of $(S, \leq, \mathcal{F})$-algebras. In the next section, decidability criteria for classes of simply-sorted theories are reviewed.

2.5 Decidability of Unification Problems

Decision problems in E-unifiability have been solved either for theories characterized by syntactical criteria, for instance for combination of theories, or for theories where decidability/undecidability is known for related problems in universal algebra and mathematical logic. Some of the relevant theorems and criteria are recalled below. All the theorems are true for simple-sorted languages with one sort or with many sorts.

2.5.1 Unification and Term Rewrite Systems

Let E be a simple-sorted presentation. The equational theory of E is decidable when there is an algorithm that tells whether a universally quantified equation is a theorem of Mod(E). It is well known, that theories with a Noetherian and Church-Rosser rewrite system have a decidable equational theory. Decidability of the equational theory of E is not enough for the decidability of the E-unification problem. Bockmayr (1987) gives examples of canonical theories with undecidable unification problem. However, there are also classes of confluent or canonical (terminating and confluent) theories that have decidable unification, as the following theorems show.

Definition 2.9
A rule $l \rightarrow r$ in a term rewriting system R is optimally reducing *iff for every substitution σ, if $\sigma(s)$ is irreducible for every proper subterm s of l, then $\sigma(r)$ is irreducible too. A term rewriting system R is* optimally reducing *iff every rule of R is.*

It is decidable whether a term rewriting system R is optimally reducing. For such systems, the normal form of a term $\sigma(s)$, where σ is an irreducible substitution, can be computed in at most $\mid s \mid$ steps. This observation leads to the theorem:

Theorem 2.3 (Narendran *et al.* (1993))
Every confluent, optimally reducing term rewriting system has a decidable unification problem (with constants).

The result can be generalized to the broader class of AC-rewriting systems. A term rewrite system in which, for all rules, no root symbol of the left hand side is not an AC operator, is called AC-rewriting system.

Theorem 2.4 (Narendran *et al.* (1993))
Every confluent, optimally AC-reducing term rewriting system has a decidable unification problem (with constants).

Along the same lines, restricted canonical rewrite systems have been studied by Mitra (1994) who defines other cases in which unification is decidable. It is very likely that Mitra (1994) was not aware of the work of Narendran *et al.* (1993) since some of the results can be generalized further by combining both works.

Given a term rewrite system R, a function symbol is a *defined function* if it appears at the root of some left hand side of a rule, otherwise it is a *constructor*.

THEOREM 2.5 (MITRA (1994))
Every canonical term rewriting system in which every right hand side is either a constructor, or a variable or is ground, has a decidable unification problem.

Another class of canonical term rewrite systems with decidable unification has rules that are subterm composing.

DEFINITION 2.10
A rule $l \to r$ in R is subterm composing *iff every subterm of r with a defined function symbol at its root is a proper subterm of l.*

THEOREM 2.6 (DERSHOWITZ AND MITRA (1995))
Every canonical term rewriting system in which every rule is subterm composing has a decidable unification problem.

Canonical term rewrite systems with flat terms have decidable unification problem.

DEFINITION 2.11
A term is flat *if it has a single defined function, and all variables below this function appear directly below it.*

THEOREM 2.7 (DERSHOWITZ AND MITRA (1993))
Every linear canonical term rewriting system in which, for every defined function, there is at most one rule whose right hand side is neither a constructor, nor a variable and is flat, has a decidable unification problem.

Relaxing the hypotheses of Theorem 2.7 might yield a undecidable unification problem (actually the theorem is stated in a misleading way and should be as below).

THEOREM 2.8 (DERSHOWITZ AND MITRA (1993))
The class of linear canonical term rewriting system in which every right hand side is either a constructor term, or a variable or is flat, has a undecidable unification problem.

The proof is based on translating any instance of Post's Correspondence Problem to a R-unification problem for some rewrite system R in the class described above. The theorem then follows from the undecidability of Post's Correspondence Problem. This undecidability result applies to a "class" of theories. It means that at least one theory in the class has undecidable unification problem.

Theorem 2.5 and Theorem 2.6 are a sub-case of Theorem 2.3 as it is shown below. However, Theorem 2.7 covers cases which cannot be dealt with by the criterion of optimal reducibility.

Since a subterm composing rule is optimally reducing, the following lemma is true.

LEMMA 2.1
A term rewriting system in which every rule is subterm composing is optimally reducing.

PROOF. It is enough to show that a subterm composing rule is optimally reducing. Assume that $l \rightarrow r$ is subterm composing, so that every subterm of r with a defined function as root is a proper subterm of l. The goal is to show that, if for all proper subterms s of l, $\sigma(s)$ is irreducible, then $\sigma(r)$ is irreducible. Assume by contradiction that $\sigma(s)$ is irreducible for all subterms s of l, but $\sigma(r)$ is not. Namely, there exists a position p in r such that $r\mid_p = r_p$ reduces. Now, observe that a term reduces only at redexes whose root symbol is a defined function, thus, the root symbol of r_p must be a defined function symbol. Moreover, in a subterm composing rule $l \rightarrow r$, if r reduces at position p, there exists a position p' at which also l reduces. Therefore there exists a a position p' in l such that $l\mid_{p'} = r_p$ and l reduces at p'. This contradicts the assumption. ■

The converse is not true, optimally reducing rules are not necessarily subterm composing. Consider the rewrite system consisting of the single rewrite rule:

$$f(x, f(y, z)) \rightarrow f(g(x, y), z). \tag{2.2}$$

The rule is optimally reducing but is not subterm composing since $g(x, y)$ is not a subterm of $f(x, f(y, z))$.

In view of Lemma 2.1, the hypothesis of Theorem 2.6 can be relaxed from canonical to confluent term rewriting system because termination is ensured by optimal reducibility.

THEOREM 2.9
Every confluent term rewriting system in which every rule is subterm composing has a decidable unification problem.

Moreover, the axiom of associativity is not subterm composing, the criterion as stated in Dershowitz and Mitra (1993) does not apply to the broad family of equational term rewriting systems modulo AC.

COROLLARY 2.1
Every confluent AC term rewriting system in which every rule is subterm composing and the left hand side does not have an AC operator as root has a decidable unification problem.

PROOF. By the Theorem 2.3 and Lemma 2.1. ■

The classes of confluent systems studied so far overlap but do not coincide. The class of rewriting systems described by the flatness criterion of Theorem 2.7 contains cases which cannot be solved by the criterion of optimal reducibility of Theorem 2.3. Vice-versa, the class of optimally reducing confluent rewrite system includes examples which cannot be solved by the flatness criterion.

THEOREM 2.10
There exists a linear and convergent term rewriting system in which, for every defined function symbol, there is at most one rule with a right hand side that is neither a constructor nor a variable and is flat, that is not optimally reducing.

PROOF. Consider the term rewriting system

$$R = \{f(x, y) \rightarrow g(x, y), g(s(z), w) \rightarrow a\}$$

in which f and g are defined function symbols while s and a are constructors. The rule $f(x, y) \to g(x, y)$ is not optimally reducing by the substitution $\theta = \{x \leftarrow s(z), y \leftarrow w\}$.

Vice-versa, there exists a linear optimally reducing term rewriting system that does not satisfy the requirements of Theorem 2.7: namely the system

$$R = \{f(g(x, y), z) \to f(x, f(y, z))\}$$

since the right hand side $f(x, f(y, z))$ is not a flat term.

2.5.2 Unification and Logic

This section is devoted to the connections between mathematical logic and unification. A lot of confusion is generated by not having a general agreement in the literature on the definition of problems. A typical example of this is the definition of *word problem* for a theory E.

Tarski (1966) stated the word problem as a decision problem for first-order theories in general and not restricted to equational ones. Given a theory Θ, enrich its language with a finite set Γ of individual constants. Construct a finite set Π of equations in the enriched language containing no variables and denote by $[\Theta, \Gamma, \Pi]$ the theory generated by $\Theta \cup \Pi$. The *word problem for* Θ is the problem of determining whether for all Γ and for all Π, there is an algorithm to decide if equations $w = w'$ containing no variables are theorems of the theory $[\Theta, \Gamma, \Pi]$.

The case in which Θ is an equational theory is a special case. In this case, Tarski observes that when the set of constants Γ is arbitrary and Π is empty, the existence of an algorithm to decide the word problem is equivalent to the decidability problem for the equational theory Θ. Hence, if Θ is undecidable also the word problem for the theory Θ is undecidable. Dershowitz and Jouannaud (1990) consider the case in which Γ and Π are empty. If it is undecidable which ground equations are theorems of $[\Theta, \emptyset, \emptyset]$, then also elementary unification in Θ is undecidable, as deciding a word equation is like unifying terms without variables.

Tarski (1966), Macintyre (1983) and Burris remark that the word problem for an arbitrary Θ is equivalent to the study of the universal Horn theory of Θ, $\mathrm{Th}_{\forall\mathrm{H}}(\Theta)$, since:

$$\mathrm{Th}(\Theta) \cup \Pi \vdash w = w' \qquad \text{iff} \qquad \mathrm{Th}(\Theta) \vdash \bigwedge_{e \in \Pi} e \to w = w'.$$

Notice that deciding equations without variables in $[\Theta, \Gamma, \emptyset]$ is a special case of unification with constants in the theory Θ and therefore the following connections between the word problem and unification holds. Let Θ be an equational theory in a language with at least one individual constant,

(a) If there is no algorithm to decide whether equations $w = w'$ containing no variables are theorems of the theory $[\Theta, \emptyset, \emptyset]$, then elementary unification is undecidable in Θ.

(b) If, for some finite set Γ, there is no algorithm to decide whether equations $w = w'$ containing no variables are theorems of the theory $[\Theta, \Gamma, \emptyset]$, then unification with constants is undecidable in Θ.

An alternative way for studying decidability of unification of E is to consider the *Diophantine theory* of E, namely the set of existentially quantified equations that are theorems of $\mathrm{Mod}(E)$. If the Diophantine theory of E is decidable, namely there exists an algorithm that decides whether an existentially closed equation is a theorem of $\mathrm{Mod}(E)$, then E-unification is decidable. Bockmayr (1989) proves that it is enough to consider the existential closure of the equations in the problem. In a finite signature moreover, if every finitely generated model of E is finite (E is locally finite), then the E-unification problem is decidable if the word problem is decidable. Since for finitely axiomatizable theories, the word problem is decidable, the next theorem holds.

Theorem 2.11 (Bockmayr (1989))
Let E be an equational theory over a finite signature. Then:

(1) elementary E-unification is decidable iff the Diophantine theory of $\mathrm{Mod}(E)$ *is decidable;*

(2) elementary E-unification is decidable if E is locally finite and finitely axiomatizable;

Theorem 2.11 holds also when E is a set of simple-sorted conditional equations.

While elementary E-unification is related to the Diophantine theory of E, unification with constants is related to the positive $\forall\exists$-theory of $\mathrm{Mod}(E)$.

Definition 2.12
Let C be a class of $(S, \mathcal{F})$-algebras. The positive $\forall\exists$-theory is the set of closed first-order formulas valid in C and of the form:

$$\forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_m ((t_{11} = u_{11} \wedge \ldots t_{1j_1} = u_{1j_1}) \vee \ldots \vee (t_{q1} = u_{q1} \wedge \ldots t_{qj_q} = u_{qj_q}))$$

Theorem 2.12 (Bockmayr (1990a))
Let E be a recursively enumerable set of conditional equations over a recursive signature. Then E-unification with constants is decidable if the positive $\forall\exists$-theory of $\mathrm{Mod}(E)$ *is decidable.*

Another central question in unification theory is deciding when a problem has no solution. This is important because the unification procedure might not terminate. The results of Bockmayr (1990b) shed some light in this direction investigating the properties of existential extensions of theories. His results are based on the following observation. If a unification problem has a solution in the term algebra, then it also has a solution in every extension of the term algebra. Assume that it is decidable whether there exists some extension of the term algebra that satisfies a problem. Knowing that a problem is not solvable in any extension implies that it is also not solvable in the term algebra. Clearly, unification remains semi-decidable: problems that are indeed solvable in some extension could be unsolvable in the term algebra. The theorems of Bockmayr (1990b) allows to find out when it is decidable that a problem has a solution in some extension of the term algebra of a set of conditional equations. Observe that the restriction to theories consisting of conditional equations does not allow to apply these results to the theory of fields and to all theories built over fields, like vector spaces and algebras.

2.5.3 Unification in a Combination of Theories

Another popular area of research is devoted to the study of the properties of combination of theories. Baader and Schulz (1992) give a method to decide unifiability in the union of arbitrary disjoint equational theories, provided that solvability of the unification problem with "linear" constant restrictions (a generalization of unification with constants) is decidable for the single theories. They additionally show that the union is finitary if the single theories are finitary with respect to general unification and that general unification under associativity is decidable.

Theorem 2.13
Let $E_1, \dots, E_n$ be equational theories over disjoint signatures and let E be the combined theory $E_1 \cup \dots \cup E_n$. Then:

(i) if solvability of general E_i-unification is decidable for $i = 1, \dots, n$, then elementary E-unification is decidable, see Schmidt-Schauß (1989).

(ii) if solvability of E_i-unification with linear constant restriction is decidable for $i = 1, \dots, n$, then elementary E-unification is decidable, see Baader and Schulz (1992).

One immediate consequence of Theorem 2.13 is the possibility of "lifting" decidability of elementary E-unification to decidability of general E-unification. The trick is to view general E-unification as unification in the combination of E with the empty theory of the free symbols appearing in the problem.

Corollary 2.2
If solvability of E-unification with linear constant restriction is decidable, then solvability of general E-unification is decidable.

Decidability of the problems of unification with linear constant restriction can be shown when decidability of the positive theory of E is known.

Theorem 2.14 (Baader and Schulz (1992))
The positive theory of E is decidable if and only if solvability of unification with linear constant restriction is decidable.

The results above can therefore be restated in logical terms as:

Theorem 2.15 (Baader and Schulz (1992))
Let $E_1, \dots, E_n$ be equational theories over disjoint signatures and let E be the combined theory $E_1 \cup \dots \cup E_n$. Then the positive theory of E is decidable if the positive theories of E_i are decidable for all $i = 1, \dots, n$.

2.6 Unification in Vector Spaces?

The main goal of this section is to study constraint solving in vector spaces over a field K. The elements of the field are called "scalars". A vector space over K is a nonempty set V, whose elements are called "vectors", together with the operations:

$\mathbf{0} :\rightarrow \mathsf{vector}$	(zero)
$- : \mathsf{vector} \rightarrow \mathsf{vector}$	(unary minus)
$+ : \mathsf{vector} \times \mathsf{vector} \rightarrow \mathsf{vector}$	(addition)
$\cdot : \mathsf{scalar} \times \mathsf{vector} \rightarrow \mathsf{vector}$	(multiplication by a scalar)

The axioms of vector spaces are recalled here below. Let $\mathbf{u}, \mathbf{v}, \mathbf{w}$ be variables of sort vector and x, y be variables of sort scalar.

$$\begin{aligned}
\forall \mathbf{u} \forall \mathbf{v} \forall \mathbf{w}\ (\mathbf{u} + \mathbf{v}) + \mathbf{w} &= \mathbf{u} + (\mathbf{v} + \mathbf{w}) \\
\forall \mathbf{u} \forall \mathbf{v}\ \mathbf{u} + \mathbf{v} &= \mathbf{v} + \mathbf{u} \\
\forall \mathbf{u}\ \mathbf{u} + (-\mathbf{u}) &= \mathbf{0} \\
\forall \mathbf{u}\ \mathbf{u} + \mathbf{0} &= \mathbf{u}
\end{aligned}$$

$$\begin{aligned}
\forall x \forall y \forall \mathbf{u}\ (x * y) \cdot \mathbf{u} &= x \cdot (y \cdot \mathbf{u}) \\
\forall x \forall y \forall \mathbf{u}\ (x + y) \cdot \mathbf{u} &= (x \cdot \mathbf{u}) + (y \cdot \mathbf{u}) \\
\forall x \forall \mathbf{u} \forall \mathbf{v}\ x \cdot (\mathbf{u} + \mathbf{v}) &= (x \cdot \mathbf{u}) + (x \cdot \mathbf{v}) \\
\forall \mathbf{u}\ 1 \cdot \mathbf{u} &= \mathbf{u}
\end{aligned}$$

In order to study constraint solving over vector spaces, it is clear that one has to know how to solve constraints over fields, since they can be stated in the language of vector spaces. Hence, unification for the theory of fields has to be solved first. The question arises as to whether fields are axiomatizable as an equational theory.

There are different presentations of the class of fields depending on the signature. The presentation of fields over the signature $\langle 0, 1, +, * \rangle$ contains $\forall\exists$ axioms:

$$\begin{aligned}
\forall x \forall y \forall z\ (x + y) + z &= x + (y + z) \\
\forall x \forall y\ x + y &= y + x \\
\forall x \exists y\ x + y &= 0 \\
\forall x\ x + 0 &= x
\end{aligned}$$

$$\begin{aligned}
\forall x \forall y \forall z\ (x * y) * z &= x * (y * z) \\
\forall x \forall y\ x * y &= y * x \\
\forall x \exists y\ x = 0 &\vee x * y = 1 \\
\forall x\ x * 1 &= x
\end{aligned}$$

$$\forall x \forall y \forall z\ x * (y + z) = x * y + x * z$$

The existential quantifier in the axiom $\forall x \exists y x + y = 0$ can be eliminated by introducing a new function symbol, $-$ (unary minus), and replacing the axiom with:

$$\forall x\ x + (-x) = 0.$$

Likewise, the other existential quantifier $\forall x \exists y x = 0 \vee x * y = 1$ can be eliminated by introducing a new function symbol, $^{-1}$, and replacing the axiom by:

$$\forall x\ x = 0 \vee x * (x)^{-1} = 1.$$

The signature becomes $\langle 0, 1, -, ^{-1}, +, *\rangle$ and the axiomatization of fields:

$$\begin{aligned}
\forall x \forall y \forall z\ (x+y)+z &= x+(y+z) \\
\forall x \forall y\ x+y &= y+x \\
\forall x\ x+(-x) &= 0 \\
\forall x\ x+0 &= x \\
\forall x \forall y \forall z\ (x*y)*z &= x*(y*z) \\
\forall x \forall y\ x*y &= y*x \\
\forall x\ x = 0 \vee x*x^{-1} &= 1 \\
\forall x\ x*1 &= x \\
\forall x \forall y \forall z\ x*(y+z) &= x*y+x*z
\end{aligned} \tag{2.3}$$

Observe that the implicational axiom is not positive conditional and as such it poses a problem. One may then think of using an order sorted framework to capture nonzero elements, thus avoiding the implicational axiom. All these attempts are doomed to fail.

Since the class of all fields is not closed under subalgebras, it is not a variety, and for the same reason, is not a quasi-variety. Thus, there is no equational theory E and no conditional positive theory E such that $\mathrm{Mod}(E)$ is the class of all fields. Theorem 2.2 allows to deduce that fields cannot be axiomatized by a set of universally quantified equations or positive conditional equations, the so-called Horn-clauses.

Therefore, there is no "canonical rewriting system" for fields, nor does there exist a "conditional term rewrite system", despite the framework of the language. This also implies that for solving constraints over fields is not possible to use the universal unification procedure which employs narrowing. The criteria established for the decidability of the unification problem of an equational theory, that are based on the syntactical properties of the associated canonical system, cannot be used. Likewise, the techniques based on combining theories do not work for fields.

Let the signature of the theory of fields be $\Sigma = \langle 0, 1, -, ^{-1}, +, *\rangle$ and let F be the presentation of commutative fields in signature Σ. A system of $(S, \mathcal{F})$-equations P:

$$s_1 = t_1, \ldots, s_n = t_n$$

for $s_i, t_i \in \mathcal{T}(S, \mathcal{F}, X)$, $(1 \leq i \leq n)$ is F*-unifiable*, iff there exists a substitution $\sigma : X \to \mathcal{T}(S, \mathcal{F}, X)$ such that

$$\mathrm{Mod}(F) \models s_1\sigma = t_1\sigma \wedge \ldots \wedge s_n\sigma = t_n\sigma.$$

The equations $s_i = t_i$ in P can be regarded as equations $s_i - t_i = 0$ and therefore of the form $h_i = 0$ for some rational term h_i consisting of a fraction of polynomials. Observe that, for the special case of constant denominators, the coefficients of the polynomial at the numerator can be reduced to integer numbers. Polynomial equations with integer coefficients are called Diophantine equations. Therefore, unification in fields subsumes the problem of solving Diophantine equations. This problem is known as "rational parametrization" when rational functions can be assigned to the variables. The algebraic geometry community studies this very hard problem (Cox *et al.*, 1992). Solutions are known only for *curves*, polynomials in two variables, and some work has been done in the case of *surfaces*, polynomials in three variables (Schicho, 1995). To the author's knowledge, there is nothing known about parametrization of polynomials in more than three variables, that is *hyper-surfaces*.

Hilbert's Tenth Problem is also related to unification in fields: given a Diophantine polynomial, find integer solutions for the variables. Observe that, depending on the signature Σ, the unification problem asks for solutions that are either Diophantine polynomials or rational functions. When the class of fields is axiomatized in the signature $\langle 0, 1, +, * \rangle$, the ground terms coincide with the integers and terms are Diophantine polynomials. Therefore, one can argue that, if elementary unification over fields was decidable, also Hilbert's Tenth Problem would be. Matijasevič (1970) has shown that Hilbert's Tenth Problem is undecidable in the integers, and therefore elementary unification in fields is undecidable. Although this reasoning has no apparent flaw, it is questionable because the integers $\mathbb{Z}$ are not a field. The author feels that the same reasoning wold be more acceptable taking the rational numbers $\mathbb{Q}$ instead of $\mathbb{Z}$. Unfortunately, Hilbert's Tenth Problem over $\mathbb{Q}$ is a major open problem.

These negative results seem to leave no hope of finding a way for solving constraints in domains that are built over fields, as vector spaces, and algebras. The rest of the thesis is devoted to presenting a novel approach for coping with the intractability of the constraint solving problem.

2.7 Summary

This chapter reviewed the state of the art of constraint solving in equational theory. The motivation was to assess the feasibility of using the techniques typical of unification theory for solving constraints in vector spaces over fields. There are two main results in this chapter.

Firstly, unification theory cannot be used to solve constraints over fields, and consequently also over vector spaces. The main reason lies in the fact that the class of field is not a quasi-variety, nor is it a variety. There is no positive conditional axiomatization of the theory of fields.

Secondly, it has been shown that the classes of rewrite systems described by the criteria of optimal reducibility and of flatness overlap but do not coincide. Future work in this direction includes searching for a criterion which encompasses both and ensures unifiability.

The next chapters investigate the novel approach of constraint solving by patterns. Patterns allow, at least in some cases, to "solve" equational constraints in riche algebraic structures, like those built over fields.

3

Symbolic Pattern Solving

In many structures, the problem of finding symbolic solutions for systems of equations is a very difficult problem, if not intractable. The goal of this chapter is to introduce an approach to deal with this inherent intractability. The method is called symbolic pattern solving and is a bridge between automatically solving equational constraints and verifying given solutions of constraints.

Let an arbitrary structure for some first-order, many-sorted language be given. Finding term solutions for system of equations in the structure is simplified by providing a *pattern of a solution*. Pattern solving means finding, if they exist, term expressions for the unknown coefficients in the pattern that turn it into a symbolic solution. Moreover, these expressions should be easy to compute, almost trivial.

The chapter is organized as follows. In Section 3.1, symbolic pattern solving is introduced after some basic notions are recalled. Section 3.2 describes the problem of pattern solving and the reader will see that many well known solving techniques deliver, when they succeed, parametric solutions of constraints, just like pattern solving. The general sketch of the algorithms for pattern solving are presented and their correctness is shown in Section 3.3. Finally, Section 3.4 overviews the state of the art in problems related to pattern solving.

3.1 Preliminary Notions

In this section, some of the basic notion introduced in Chapter 2 are generalized. In particular, the concept of equational theory is generalized to that of arbitrary first order theory. Some basic concepts of model theory are recalled below. The reader may refer to the exposition by Keisler (1977) or to any other textbook of logic.

Let the usual logical connectives of first-order logic be given:

$$\wedge(\text{ and}), \vee(\text{or}), \neg(\text{not}), \rightarrow (\text{implies}), \forall(\text{for all}), \exists(\text{there exists})$$

plus a set of variable symbols, and parentheses if needed to ensure unique readability of formulas. In first-order logic, the quantifiers always range on the elements of the domain. Given a many-sorted signature $\Sigma = (S, \leq, \mathcal{F})$, the set of $\Sigma - terms$ is defined as usual.

The set Φ_{s} of Σ-*atomic formulas* of sort $\mathsf{s} \in S$ is the set of all Σ-equations $t = t'$ where t, t' are Σ-terms of sort s. $\Phi = \{\Phi_{\mathsf{s}} \mid \mathsf{s} \in S\}$ is the set of all Σ-atomic formulas. The set $\mathcal{F}_\Sigma$ of Σ-*formulas* is the smallest set containing the set Φ of Σ-equations and closed under the formation rules:

(a) if ϕ and ψ are Σ-formulas, so are the formulas:

$$\neg\psi, \quad (\psi \wedge \phi), \quad (\psi \vee \phi), (\psi \to \phi);$$

(b) if ϕ is a Σ-formula and x is a variable, then:

$$(\forall x\ \phi), \qquad (\exists x\ \phi).$$

The notion of free variables is defined by induction on the length of the formulas. The set FVars(ψ) of a Σ-formula ψ is defined as follows:

(i) if ψ is an equation $t = t'$, then FVars(ψ)=Vars(t) $\cup$ Vars(t'),

(ii) FVars($\neg\psi$)=FVars(ψ)

(iii) FVars($\psi \wedge \phi$) = FVars($\psi \vee \phi$) = FVars($\psi \to \phi$) = FVars(ψ) $\cup$ FVars(ϕ)

(iv) FVars($\forall x\ \psi$) = FVars($\exists x\ \psi$) = FVars(ψ) $\setminus \{x\}$

A Σ-sentence is a Σ-formula without free variables.

Let $\mathfrak{A}$ be a Σ-structure and let $\alpha(\overset{a}{x})$ denote the assignment α' that agrees with α except for $\alpha(x) = a$. Then, all Σ-formulas ϕ and for all assignments $\alpha : X \to \mathfrak{A}$, the relation

$$\mathfrak{A} \models \phi[\alpha]$$

is defined in the usual way:

(i) $\mathfrak{A} \models (t = t')[\alpha]$ iff $\alpha(t) = \alpha(t')$

(ii) $\mathfrak{A} \models (\neg\psi)[\alpha]$ iff not $\mathfrak{A} \models \psi[\alpha]$

(iii) $\mathfrak{A} \models (\psi \wedge \phi)[\alpha]$ iff $\mathfrak{A} \models \psi[\alpha]$ and $\mathfrak{A} \models \phi[\alpha]$

(iv) $\mathfrak{A} \models (\psi \vee \phi)[\alpha]$ iff $\mathfrak{A} \models \psi[\alpha]$ or $\mathfrak{A} \models \phi[\alpha]$

(v) $\mathfrak{A} \models (\psi \to \phi)[\alpha]$ iff either not $\mathfrak{A} \models \psi[\alpha]$ or $\mathfrak{A} \models \phi[\alpha]$

(vi) $\mathfrak{A} \models (\exists x\psi)[\alpha]$ iff there is an $a \in A$ such that $\mathfrak{A} \models \psi[\alpha(\overset{a}{x})]$

(vii) $\mathfrak{A} \models (\exists x\psi)[\alpha]$ iff for all $a \in A$ such that $\mathfrak{A} \models \psi[\alpha(\overset{a}{x})]$

If for all assignments α, $\mathfrak{A} \models \phi[\alpha]$ then $\mathfrak{A}$ is a model of ϕ and is denoted by:

$$\mathfrak{A} \models \phi.$$

A theory T in the signature Σ is a set of Σ-sentences, and $\mathfrak{A}$ is a model of T if $\mathfrak{A} \models \phi$, for all $\phi \in T$. Naturally, two theories are equivalent if they have the same models. A theory T is consistent if it has at least one model. Theories also arise in another way. Let K be a class of Σ-structures, the theory of K is the set Th(K) of Σ-sentences that hold in every structure $\mathfrak{A} \in K$. A set of sentences which is equivalent to Th(K) is called a set of *axioms* for K. A theory T is called finitely axiomatizable if it is equivalent to a finite set of sentences, and recursively axiomatizable if it is equivalent to a recursively enumerable set of sentences in a recursive signature.

Example 3.1
The theories of:

- ▷ rings,
- ▷ integral domains,
- ▷ fields, and
- ▷ fields of characteristic p

are finitely axiomatizable. The theories of:

- ▷ fields of characteristic 0,
- ▷ algebraically closed fields, and
- ▷ real closed fields

are recursively axiomatizable but not finitely axiomatizable.

A sentence ψ is a *consequence* of T

$$T \models \psi,$$

if every model of T is a model of ψ. A theory T, in a recursive signature Σ, is *decidable* if there exists and algorithm to decide if an arbitrary sentence ψ is a consequence of T.

Equational theories studied in Chapter 2 are universal, namely they are equivalent to a set of universal sentences. A *universal formula* has the form:

$$\forall x_1 \dots \forall x_n \psi$$

where ψ contains no quantifiers. Universal theories enjoy the following important property.

THEOREM 3.1
If T is a universal theory, then every substructure of a model of T is again a model of T.

$\mathfrak{B}$ is a substructure of $\mathfrak{A}$, $\mathfrak{B} \subseteq \mathfrak{A}$, if $B \subseteq A$ and if the interpretation of each function symbol in $\mathfrak{B}$ is the restriction of the corresponding interpretation in $\mathfrak{A}$. $\mathfrak{B}$ is an elementary substructure of $\mathfrak{A}$, if it is a substructure, $\mathfrak{B} \subseteq \mathfrak{A}$, and if for every formula ψ and assignment α in $\mathfrak{B}$:

$$\mathfrak{B} \models \phi[\alpha] \qquad \text{iff} \qquad \mathfrak{A} \models \phi[\alpha].$$

A theory is *model-complete* if for any pair $\mathfrak{A}, \mathfrak{B}$ of models of T, $\mathfrak{B} \subseteq \mathfrak{A}$ implies that $\mathfrak{B}$ is an elementary substructure of $\mathfrak{A}$.

Recall the axioms for fields given in Section 2.6 and the signatures $\langle 0, 1, +, * \rangle$ and $\langle 0, 1, +, *, ^{-1} \rangle$. The theory of fields in the signature $\langle 0, 1, +, *, ^{-1} \rangle$ is a universal theory, whereas it is not the case for the theory of fields in the signature $\langle 0, 1, +, * \rangle$. In fact, in the latter case, the substructure $\mathbb{Z} \subseteq \mathbb{Q}$ is not a model of the theory. Fortunately, it is always possible to enlarge the signature so that the axiomatization of the theory becomes universal. A Σ'-theory T' is a *conservative extension* of a Σ-theory T, if the signature Σ' expands Σ, $\Sigma \subseteq \Sigma'$ in such a way that every model $\mathfrak{A}$ of T has an expansion into a model $\mathfrak{A}$' of T'.

THEOREM 3.2
Every theory T has a conservative extension T' which is universal and model-complete.

The extension T', constructed by introducing "Skolem functions", is called Skolem expansion of T.

A powerful tool used in model theory to assert decidability of a theory T is the method of elimination of quantifiers. Let the notation:

$$T \models \psi(x_1, \ldots, x_n)$$

mean that $\forall x_1 \ldots \forall x_n \psi(x_1, \ldots, x_n)$ is a consequence of T.

DEFINITION 3.1
A theory T admits elimination of quantifiers *if every Σ-formula $\psi(x_1, \ldots, x_n)$ is T-equivalent to a quantifier-free Σ-formula $\phi(x_1, \ldots, x_n)$:*

$$T \models \psi(x_1, \ldots, x_n) \leftrightarrow \phi(x_1, \ldots, x_n)$$

Every theory T which admits elimination of quantifiers is model-complete. The reader interested in elimination of quantifiers in algebraic structures might begin with (Macintyre *et al.*, 1983).

EXAMPLE 3.2
Among theories that admit quantifier elimination are the following:

- ▷ fields,
- ▷ differential fields,
- ▷ commutative rings,
- ▷ Abelian groups and modules.

Quantifier elimination has also been emplyed by Tarski (1951) to show that the theory of real closed fields is decidable. The reader should not be fooled into thinking that the proof of decidability directly corresponds to an efficient algorithm. For the theory of real closed field, it took a lot of research to improve quantifier elimination to the point of being actually executable. Initiated by (Collins, 1975), it culminated in the partial cylindrical algebraic decomposition (Collins and Hong, 1991) implemented in the SACLIB computer algebra system (Collins *et al.*, 1992). This powerful decision algorithm has been employed as a solver for constraints over the real numbers and incorporated in the constraint logic programming language RISC-CLP, (Hong, 1993; Caprotti, 1993). Recently, it was used for problems in stability theory by Hong *et al.* (1996).

Having given all the ingredients, the concept of parametric solution and of solution pattern are introduced next.

In theories, where the term structure is not an initial model, there exists elements which cannot be expressed explicitly by a term of the language. Thus one has to be careful in defining what is intended by symbolic solution of a system of equations since not every solution is a term solution. To exemplify, consider the real numbers $\mathbb{R}$ as structure for the language $\langle 0, 1, +, -, *, / \rangle$. Then, the equation

$$x * x = 2 \tag{3.1}$$

has no symbolic solution over $\mathbb{R}$ in this language since there is no function symbol to express the square root of 2. Nevertheless, the existential closure of the formula is true in $\mathbb{R}$:

$$\mathbb{R} \models \exists x \; x * x = 2.$$

Observe that, on the contrary, the same equation has no solution in the field of rational numbers $\mathbb{Q}$, nor does $\mathbb{Q}$ model the existential closure of the equation. Thus, while in equational theories, all solutions can be represented as term solutions, the same cannot be said for universal theories in general. Parametric solutions are solutions which can be expressed as terms of the language and take value in the intended domain.

In what follows, let $\Sigma = (S, \mathcal{F})$ be a many-sorted signature, $\mathfrak{A}$ a Σ-structure, and X, Y, Z disjoint sets of variables.

Definition 3.2
Let Γ be a system of term equations:

$$\{t_1 = u_1, \ldots, t_n = u_n\}$$

where $t_i, u_i \in \mathcal{T}(\Sigma, X)$, $(1 \leq i \leq n)$ are terms with free variables $X = \{x_1, \ldots, x_k\}$. A substitution $\sigma : X \to \mathcal{T}(\Sigma, Y)$ of the form:

$$\sigma = \{x_1 \leftarrow \tau_1(Y), \ldots, x_k \leftarrow \tau_k(Y)\}$$

where $\tau_i(Y) \in \mathcal{T}(\Sigma, Y)$, $(1 \leq i \leq k)$, is a parametric solution for P in the structure $\mathfrak{A}$, if and only if

$$\mathfrak{A} \models t_1\sigma = u_1\sigma \wedge \ldots \wedge t_n\sigma = u_n\sigma.$$

The variables Y are called parameters and range over the elements of the intended domain. A parametric solution in which the set of parameters is empty is called *ground term solution*.

Example 3.3
The most general unifiers are parametric solutions for problems in equational theories, as the reader can easily verify by recalling chapter 2.

Example 3.4
The rational parametrizations of algebraic curves are parametric solutions for problems in fields of characteristic zero for the language $\langle 0, 1, +, -, *, / \rangle$. Let C be a plane algebraic curve over a field K of characteristic zero defined by an irreducible polynomial $f(x, y) \in K[x, y]$. Then the pair (ϕ, ψ) of rational functions $\phi(t), \psi(t) \in K[t]$ is a rational parametrization of C, when it exists, iff the following conditions are satisfied:

(1) for almost all (but a finite number of exceptions) $t_0 \in K$, $f(\phi(t_0), \psi(t_0)) = 0$, namely, $(\phi(t_0), \psi(t_0))$ is a point on the curve C; and

(2) for almost every point (x_0, y_0) on the curve C there is a $t_0 \in K$ such that:

$$(x_0, y_0) = (\phi(t_0), \psi(t_0)).$$

For instance, the curve defined by:

$$f(x, y) = x^2 + y^2 - 1 \tag{3.2}$$

has a parametrization:

$$\phi(t) = \frac{2t}{t^2 + 1} \qquad \psi(t) = \frac{t^2 - 1}{t^2 + 1} \tag{3.3}$$

There is no parametrization for the curve:

$$f(x, y) = x^3 + y^3 - 1. \tag{3.4}$$

The problem of deciding whether a curve has a parametrization is decidable.

EXAMPLE 3.5
If the language in which the symbolic solution is expressed can be enlarged by extra function symbols, then the situation changes again. Take, for instance Galois theory, the theory of solvability of equations over a field by radicals. It provides another example of parametric solutions. In this case, they contain with no parameters, since the number of solutions is finite, and some additional function symbols (radicals).

A solution pattern is simply a parametric solution with some unspecified coefficients.

DEFINITION 3.3
Let Γ *be as above. A* solution pattern $\pi : X \to \mathcal{T}(\Sigma, Y \cup Z)$ *for* P *in the structure* $\mathfrak{A}$ *is a substitution*

$$\pi = \{X_1 \leftarrow \tau_1(Y,Z), \ldots, X_k \leftarrow \tau_k(Y,Z)\}$$

where $\tau_i(Y,Z) \in \mathcal{T}(\Sigma, Y \cup Z)$ *for* $1 \leq i \leq k$ *are terms with free variables* Y, Z*.* π *is such that there exists a ground term substitution* $\gamma : Z \to \mathcal{T}(\Sigma)$ *with the property that* $\pi \cdot \gamma$ *is a parametric solution for* Γ *in the structure* $\mathfrak{A}$*.*

Most theories have undecidable parametric solution problem, naturally one may ask the similar question concerning the pattern solution problem.

DEFINITION 3.4
A structure $\mathfrak{A}$ *has a decidable solution pattern problem iff there exists an algorithm that, for all inputs* $\langle \Gamma, \pi \rangle$*, decides whether* π *is a solution pattern for* Γ *in* $\mathfrak{A}$*.*

In the following chapters, this decidability question is addressed for some many-sorted structures of computational interest. In the case in which the pattern solution problem is undecidable, it is always possible to limit the attention to special classes of input problems:

DEFINITION 3.5
Given a structure $\mathfrak{A}$*, a class* C *of problems* $\langle \Gamma, \pi \rangle$*, has a decidable pattern solution problem iff there exists an algorithm such that: for all inputs* $\langle \Gamma, \pi \rangle \in C$*, it decides whether* π *is a solution pattern for* Γ *in* $\mathfrak{A}$*.*

In the next section, the problem of constraint solving by patterns is described.

3.2 Problem Description

The approach by solution patterns that is presented here and investigated in the rest of the thesis has a strong motivational basis. In the last chapter, it has been shown that solving symbolic constraints, for instance over vector spaces, is a very hard, often intractable problem. However, engineers and physicists seem to be able to find solutions for the same problems. The key is that "in practice" one is interested in solutions of a special form rather than in all solutions. More often than not, a skeleton of the expected solution, the solution pattern, is available. Therefore, engineers and physicists do not try to solve a problem by finding all solutions, rather, they verify whether the expected solution is truly a solution. This remark allowed to redefine the constraint solving problem by shifting the emphasis on using solution patterns.

The pattern solving problem is defined in Figure 3.1.

GIVEN:	$\mathfrak{A}$ a structure for an arbitrary signature Σ.
	$\Gamma = \{t_1 = u_1, \ldots, t_n = u_n\}$ a system of equations among Σ-terms in variables X.
	$\pi = \{x_1 \leftarrow \tau_1(Y, Z), \ldots, x_k \leftarrow \tau_k(Y, Z)\}$ a solution pattern in parameters Y and unknowns Z.
FIND:	γ an *easily computable* ground term substitution for the unknowns Z such that $\pi \cdot \gamma$ is a parametric solution for Γ in the structure $\mathfrak{A}$: $$\mathfrak{A} \models t_1\pi\gamma = u_1\pi\gamma \wedge \ldots \wedge t_n\pi\gamma = u_n\pi\gamma.$$

Figure 3.1: Pattern Solving Problem

The pattern solving problem is different in presence of new constants defined by a set of equations. New constant symbols are introduced when the set of terms of the language is the trivial set, either empty or consisting of the zero only. Figure 3.2 described pattern solving in the presence of extra constants.

GIVEN:	$\mathfrak{A}$ a structure for an arbitrary Σ.
	$\Psi = \{s_1 = v_1, \ldots, s_n = v_n\}$ a finite set of ground equations in the expanded signature $\Sigma' = \Sigma \cup \Phi$ obtained by adding a set of individual constants Φ.
	$\Gamma = \{t_1 = u_1, \ldots, t_m = u_m\}$ a system of equations among Σ'-terms with variables X.
	$\pi = \{x_1 \leftarrow \tau_1(Y, Z), \ldots, x_k \leftarrow \tau_k(Y, Z)\}$ a solution pattern of Σ'-terms with parameters Y and unknowns Z.
FIND:	γ an *easily computable* ground Σ'-term substitution for Z such that: $$\mathfrak{A} \models (s_1 = v_1 \wedge \ldots \wedge s_n = v_n) \rightarrow (t_1\pi\gamma = u_1\pi\gamma \wedge \ldots \wedge t_1\pi\gamma = u_1\pi\gamma).$$

Figure 3.2: Pattern Solving Problem with Extra Constants

Remark that the problems coincide when the set of new individual constants is empty, $\Phi = \emptyset$, and therefore also the set of ground equations in the expanded signature is empty, $\Psi = \emptyset$.

It must be stressed that the problem is to find whether there is an "easily computable" ground term substitution. A substitution is easily computable if it is effectively solvable by using some appropriate constraint solving method. A typical example might be, for instance, the computation of solutions of a system of polynomial equations by using the method of Gröbner basis. Such a method is very effective for special classes of problems, namely in the case of zero-dimensional varieties.

If a ground term substitution exists and can be effectively computed, then the solution pattern can be instantiated and solution pattern is successful. Otherwise, failure is reported to the user. In this fashion, completeness is given up for effectiveness. The justification is that, using the "right" solution pattern, the original complexity of the input problem is reduced. Unsolvability at this step means that the proper pattern was not given. This also means that an engineer or a physicist does actually most of the work in 'guessing' the pattern and this is why he is able, potentially, to solve symbolic constraint problems in cases where the completely automatic approach fails.

It has not yet been explained how the ground term substitution γ is computed. In the next section, the algorithm for pattern solving is introduced and will provide an answer.

3.3 Algorithms

The algorithm that allows to solve symbolic constraints by solution patterns is based on the definition of parametric solution and on the availability of a fast algorithm for the elimination of universal quantifiers in the structure under consideration. Two algorithms are sketched, one for the pattern solving problem with no extra constant symbols, the other for pattern solving when extra constants are given.

Figure 3.3 sketches the basic steps of the algorithm *SolPat* to solve constraints by solution patterns in the case with no new constant symbols. Initially, from the input equations:

$$\Gamma = \{t_1 = u_1, \ldots, t_n = u_n\} \tag{3.5}$$

the problem formula $\psi(Y, Z)$:

$$t'_1(Y, Z) = u'_1(Y, Z) \wedge \ldots \wedge t'_n(Y, Z) = u'_n(Y, Z) \tag{3.6}$$

is constructed. It is obtained by applying the substitution related to the solution pattern:

$$\pi = \{x_1 \leftarrow \tau_1(Y, Z), \ldots, x_k \leftarrow \tau_k(Y, Z)\} \tag{3.7}$$

to all terms $t_1, u_1, \ldots, t_n, u_n$ in the system of equations. The problem formula is the universal closure of the conjunction of the equations. If in the structure $\mathfrak{A}$ there is a "straightforward" quantifier elimination algorithm for formulas like the problem formula, then it is used to find an equivalent quantifier-free formula, $\phi(Z)$, in terms of the unknown coefficients only:

$$\mathfrak{A} \models \forall Y\ \psi(Y, Z) \leftrightarrow \phi(Z). \tag{3.8}$$

If the quantifier-free formula $\phi(Z)$ is a conjunction of equations in the unknown coefficients, then the final step consists in finding a ground term solution for this system of equations. When a solution exists and can be easily computed by known techniques, the algorithm returns it and yields one instance of the solution pattern. If no solution exists, then the user is warned that there is no instance of the solution pattern turning it into a parametric solution. If a solution cannot be easily computed, the user is asked for further information on the solution pattern.

In Figure 3.3, the algorithm for computing a ground term substitution γ, as specified in the pattern solving problem in Figure 3.3, is presented in its most generic form, namely for an arbitrary algebraic structure $\mathfrak{A}$.

SolPat $(\mathfrak{A}, P, \pi; \gamma)$

Input: $\mathfrak{A}$ a structure for a signature Σ
$\Gamma = \{t_1 = u_1, \ldots, t_n = u_n\}$ a system of equations among terms in variables X
$\pi = \{x_1 \leftarrow \tau_1(Y, Z), \ldots, x_k \leftarrow \tau_k(Y, Z)\}$ a candidate solution pattern in parameters Y and unknown coefficients Z

Output: γ a substitution such that $\pi \cdot \gamma$ is a parametric solution of Γ in the structure $\mathfrak{A}$ when it is easy to compute. Otherwise report.

(1) [Initialize.]
Construct the problem formula :

$$\begin{aligned}\psi(Y, Z) &:= t_1\pi = u_1\pi \wedge \ldots \wedge t_n\pi = u_n\pi \\ &:= t_1'(Z, Y) = u_1'(Z, Y) \wedge \ldots \wedge t_n'(Z, Y) = u_n(Z, Y)\end{aligned}$$

(2) [Eliminate Universal Quantifiers.]
Find an equivalent quantifier-free formula $\phi(Z)$ such that:

$$\mathfrak{A} \models \forall Y\ \psi(Y, Z) \leftrightarrow \phi(Z).$$

(3) [Find Ground Unifier.]
Find an "easily computable" ground unifier γ for the system of equations in $\phi(Z)$, considering the unknown coefficients Z as variables. If solutions are not easy to compute, then ask to the user whether to continue.

(4) [Return.]
If no solution exists, then return "No instance of this form". Otherwise return γ.

Figure 3.3: The algorithm *SolPat* for instantiation of a solution pattern

Correctness of the algorithm is not difficult to show.

THEOREM 3.3
The algorithm SolPat is correct.

PROOF. Let $\mathfrak{A}$ be a Σ-structure, and let $\Gamma = \{t_1 = u_1, \ldots, t_n = u_n\}$ be a system of equations among Σ-terms in variables X and $\pi = \{\, x_1 \leftarrow \tau_1(Y, Z), \ldots, x_k \leftarrow \tau_k(Y, Z)\}$ a solution pattern in parameters Y and unknown coefficients Z.

Suppose that *PatSol* returns a ground term substitution γ for variables Z that is a solution for the system of equations in the quantifier-free formula $\psi(Z)$. The goal is to show that $\pi \cdot \gamma$ is a parametric solution for the input problem Γ in the structure $\mathfrak{A}$. By assumption, the term ground substitution γ satisfies:

$$\mathfrak{A} \models \psi(Z)\gamma. \tag{3.9}$$

Since $\psi(Z)$ is the quantifier-free equivalent formula to $\phi(Z, Y)$, by construction it holds:

$$\mathfrak{A} \models \psi(Z) \leftrightarrow \forall Y\ \phi(Z, Y). \tag{3.10}$$

This implies that:

$$\mathfrak{A} \models \psi(Z)\gamma \leftrightarrow \forall Y\ \phi(Z, Y)\gamma, \tag{3.11}$$

namely:

$$\mathfrak{A} \models \forall Y\ \phi(Z, Y)\gamma. \tag{3.12}$$

But this is equivalent to:

$$\mathfrak{A} \models \forall Y\ t'_1(Z, Y)\gamma = u'_1(Z, Y)\gamma \wedge \ldots \wedge t'_n(Z, Y)\gamma = u_n(Z, Y)\gamma, \tag{3.13}$$

$$\mathfrak{A} \models \forall Y\ t_1\pi\gamma = t_1\pi\gamma\ \wedge \ldots \wedge\ t_n\pi\gamma = t_n\pi\gamma \tag{3.14}$$

hence $\pi\gamma$ is a parametric solution for Γ in $\mathfrak{A}$. ■

In Figure 3.4, the algorithm *SolPatC* for pattern solving takes into account the presence of constants defined by a set of equations. It computes the ground term substitution γ as specified in the pattern solving problem of Figure 3.2. There is only one major computational difference compared to the generic algorithm *SolPat* of Figure 3.3. It lies in the step of finding ground term solutions for a system of equations derived from the quantifier-free formula. The rest of the algorithm is still the same.

Therefore, initially, from the input equations:

$$\Gamma = \{t_1 = u_1, \ldots, t_m = u_m\} \tag{3.15}$$

the problem formula $\psi(Y, Z)$:

$$t'_1(Y, Z) = u'_1(Y, Z) \wedge \ldots \wedge t'_m(Y, Z) = u'_m(Y, Z) \tag{3.16}$$

is constructed by applying the solution pattern to all terms $t_1, u_1, \ldots, t_n, u_n$ in Γ. The problem formula is the universal closure of the conjunction of the equations. If in the

$SolPatC\ (\mathfrak{A}, \Psi, \Gamma, \pi; \gamma)$

Input: $\mathfrak{A}$ a structure for a signature Σ.
$\Psi = \{s_1 = v_1, \ldots, s_n = v_n\}$ be a finite set of ground Σ'- equations, with $\Sigma' = \Sigma \cup \Phi$ for a set of individual constants Φ.
$\Gamma = \{t_1 = u_1, \ldots, t_m = u_m\}$ a system of equations among Σ'-terms in variables X
$\pi = \{x_1 \leftarrow \tau_1(Y, Z, a), \ldots, x_k \leftarrow \tau_k(Y, Z, a)\}$ a solution pattern of Σ'-terms with parameters Y and unknowns Z.

Output: γ a substitution such that $\pi\gamma$ is a parametric solution of Γ in the structure $\mathfrak{A}$ when it is easy to compute. Otherwise report.

(1) [Initialize.]
Construct the problem formula:

$$\begin{aligned} \psi(Y, Z) &:= t_1\pi = u_1\pi \wedge \ldots \wedge t_m\pi = u_m\pi \\ &:= t_1'(Z, Y) = u_1'(Z, Y) \wedge \ldots \wedge t_m'(Z, Y) = u_m(Z, Y) \end{aligned}$$

(2) [Eliminate Universal Quantifiers.]
Find an equivalent quantifier-free formula $\phi(Z)$ such that:

$$\mathfrak{A} \models \forall Y\ \psi(Y, Z) \leftrightarrow \phi(Z).$$

(3) [Find Ground Unifier.]
Find an "easily computable" ground solution γ for the system of equations in $\phi(Z)$ such that:

$$\mathfrak{A} \models (s_1 = v_1 \wedge \ldots \wedge s_n = v_n) \rightarrow \phi(Z)\gamma.$$

If solutions are not easy to compute, then ask to the user whether to continue.

(4) [Return.]
If no solution exists, then return "No instance of this form". Otherwise return γ.

Figure 3.4: The algorithm *SolPatC* for instantiation of a solution pattern in the presence of new constants

structure $\mathfrak{A}$ admits "straightforward" quantifier elimination for $\forall Y\ \psi(Y,Z)$, then it is used to find an equivalent quantifier-free formula, $\phi(Z)$, in terms of the unknown coefficients only:

$$\mathfrak{A}\ \models \forall Y\ \psi(Y,Z) \leftrightarrow \phi(Z). \tag{3.17}$$

Suppose that the quantifier-free formula $\phi(Z)$ is a conjunction of equations in the unknown coefficients. The final step of the algorithm *SolPat* consists in finding a ground term solution γ for this system of equations such that:

$$\mathfrak{A}\ \models (s_1 = v_1 \wedge \ldots \wedge s_n = v_n) \rightarrow \phi(Z)\gamma. \tag{3.18}$$

When a solution γ exists that is easily computable, the algorithm returns it. If a solution cannot be easily computed, the user is asked for further information on the solution pattern. If no solution exists, the user is warned that there is no instance of the solution pattern turning it into a parametric solution.

Correctness is shown in a similar way as for Theorem 3.3.

THEOREM 3.4
The algorithm SolPatC is correct.

PROOF. Let $\mathfrak{A}$ be a Σ-structure, and let $\Sigma' = \Sigma \cup \Phi$ be an expansion of the signature Σ by a set of individual constants Φ presented by a set of ground Σ'-equations $\Psi = \{s_1 = v_1, \ldots, s_n = v_n\}$. Additionally, let $\Gamma = \{t_1 = u_1, \ldots, t_m = u_m\}$ be a system of equations among Σ'-terms in variables X and $\pi = \{\ x_1 \leftarrow \tau_1(Y,Z), \ldots, x_k \leftarrow \tau_k(Y,Z)\}$ a solution pattern in parameters Y and unknown coefficients Z.

Suppose that *PatSolC* returns a ground term substitution γ for variables Z that is a solution for the system of equations in the quantifier-free formula $\phi(Z)$ such that:

$$\mathfrak{A} \models (s_1 = v_1 \wedge \ldots \wedge s_n = v_n) \rightarrow \phi(Z)\gamma. \tag{3.19}$$

The goal is to show that $\pi \cdot \gamma$ is a parametric solution for the input problem Γ in the structure $\mathfrak{A}$, namely:

$$\mathfrak{A}\ \models (s_1 = v_1 \wedge \ldots \wedge s_n = v_n) \rightarrow (t_1\pi\gamma = u_1\pi\gamma \wedge \ldots \wedge t_1\pi\gamma = u_1\pi\gamma). \tag{3.20}$$

Hence, assume that:

$$\mathfrak{A}\ \models (s_1 = v_1 \wedge \ldots \wedge s_n = v_n) \tag{3.21}$$

Then, by (3.19):

$$\mathfrak{A} \models \phi(Z)\gamma. \tag{3.22}$$

Since $\phi(Z)$ is the quantifier-free equivalent formula to $\forall X\ \psi(Z,Y)$, by construction it holds:

$$\mathfrak{A} \models \phi(Z) \leftrightarrow \forall Y\ \psi(Z,Y).$$

This implies that:

$$\mathfrak{A} \models \phi(Z)\gamma \leftrightarrow \forall Y\ \psi(Z,Y)\gamma,$$

namely:

$$\mathfrak{A} \models \forall Y\ \psi(Z,Y)\gamma.$$

But this, again, is equivalent to:

$$\mathfrak{A} \models \forall Y\ t'_1(Z,Y)\gamma = u'_1(Z,Y)\gamma \wedge \ldots \wedge t'_n(Z,Y)\gamma = u_n(Z,Y)\gamma,$$

$$\mathfrak{A} \models \forall Y\ t_1\pi\gamma = t_1\pi\gamma\ \wedge \ldots \wedge\ t_m\pi\gamma = t_m\pi\gamma$$

hence $\pi\gamma$ is a parametric solution for Γ in $\mathfrak{A}$ because (3.20) is shown. ■

Two considerations concerning the algorithms are in order. Firstly, the step of quantifier elimination must be done straightforwardly and without losing completeness for the procedure to be effective. There is confidence that this is possible because it is only an elimination of universal quantifiers from a conjunction of equations. Even if the structure might not admit elimination of quantifiers in the general case, it can still admit a fast elimination of universal quantifiers for this type of formulas. These cases are the ones which yield a practical overall algorithm and which will be object of research in the rest of the thesis.

Secondly, a consideration about the last step of the algorithms. The system of equations obtained from the quantifier-free problem formula might well be a constraint solving problem of the same type as the input problem. Therefore, it is crucial to request that it is "easier" to solve than the original one. If no easy solution can be obtained for it, then the algorithm fails. As it has been said before, a solution is considered easy to find if the known algorithms are effective for solving the problem.

It is clear now that in order to perform pattern solving in a Σ-structure $\mathfrak{A}$, two ingredients must be available:

1. a fast method to eliminate universal quantifiers from conjunctions of equational constraints, and
2. some effective method to solve equational constraints in the ground term structure of the signature Σ.

The following chapters are devoted to providing these ingredients for several algebraic structures, from commutative rings to graded exterior algebras.

3.4 State of the Art

The basic motivation for introducing solution patterns is the general intractability of the problem of symbolic constraint solving. This approach is, to the author's knowledge, a very new approach. The novelty is definitely one of attitude. In fact, while mathematics tries always to find complete solutions for problems, the approach advocated here takes another attitude in solving. Pattern solving is a procedure in the sense that it might not yield an answer, but if it does, then it is very efficient.

Pattern solving employs elimination of universal quantifiers in combination with solving systems of equations in order to find parametric solutions. This combination of techniques from distinct areas of expertise is also new. Moreover, even if elimination of quantifiers has been widely studied in the logic community as a technique to show the decidability of a theory, it is rarely studied in a many-sorted framework. For these reasons, it is hard to discuss the state of the art in pattern solving.

Concerning decidability of the problem of pattern solving for a theory T, one can remark that it is equivalent to the decidability of the $\forall\exists$ fragment of the theory. A $\forall\exists$ *formula* has the form:

$$\forall x_1 \ldots \forall x_n \exists y_1 \ldots \exists y_m \psi$$

where ψ contains no quantifiers and $m, n \geq 1$. Thus, undecidability of the existential fragment of T implies also undecidability of the pattern solving problem. For special theories, decidability of classes of constraint solving problems are known. For instance, a lot is known already about commutative rings.

The problem of symbolic constraint solving in commutative rings, mentioned also in Section 2.4, is a famous problem dating back to 1900, namely it is Hilbert's Tenth Problem:

> ...to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers...

The negative answer to the question of Hilbert came in 1970 by the work of Matijasevič (1970) who showed the undecidability of the symbolic constraint solving problem over commutative rings. There is no algorithm that will find for any equation with integer coefficients, whether there exists an integer solution. Many results pertaining to variations of Hilbert's Tenth Problem (hereafter abbreviated as HTP) are summarized by Pheidas (1994). A short list of results, without references, is reported here below, the classifications is done according to the degree of the equation, and to the number of variables:

(1d) HTP for systems of linear Diophantine equations is solvable.

(2d) HTP for a single quadratic Diophantine equation is solvable.

(3d) HTP for cubic Diophantine equations was open in 1994 (at the time the paper was written).

(4d) HTP for Diophantine equations of degree 4 is unsolvable.

(1v) HTP for Diophantine equations in one variable is solvable.

(2v) HTP for Diophantine equations in 2 to 8 variables was open in 1994.

(3v) HTP for Diophantine equations in more than 9 variables is unsolvable.

Other variations take into account different rings beside the integers. It is clear that rings with a decidable theory also have a decidable HTP, among them are on the positive bright side:

(1t) the theory of an algebraically closed field in the language $\langle +, *, 0, 1 \rangle$,

(2t) the theory of $\mathbb{R}$,

(3t) the theory of a field $\mathbb{Q}_p$ of p-adic numbers,

(4t) the existential theory $\langle +, |, 0, 1 \rangle$ of addition and divisibility of $\mathbb{Z}$, although the full theory of $\mathbb{Z}$ is not,

(5t) the theory of addition and exponentiation $\langle +, exp_2, 0, 1 \rangle$ of $\mathbb{Z}$ (where $exp_2(x) = 2^x$).

The theory of the field of rationals has been shown undecidable by Robinson (1949) so that the major open problem is nowadays HTP for $\mathbb{Q}$. This is also strictly related to results obtained in the area of rational parameterization of algebraic varieties, the topic of algebraic geometry.

Kim and Roush (1993) showed that, for any field $\mathfrak{F}$ of characteristic zero that satisfies an hypothesis related to not being algebraically closed, the problem of finding non-constant parametric solutions in $F[t]$ to a system of polynomials with coefficients in $\mathcal{F}$ is undecidable. This settles the question of decidability of the constraint solving problem negatively for the case of commutative fields of characteristic zero. In fact, it is enough to consider the case in which the field $\mathcal{F}$ is $\mathbb{Q}$. Moreover, the result extends to all structures that are built over fields, like algebras and vector spaces. But this was to be expected.

3.5 Symbolic Pattern Solving in Algebraic Structures

Although the approach of symbolic constraint solving by patterns is a general method for solving systems of equations, its range of applicability depends very much on the possibility of performing easy elimination of universal quantifiers from the input formulas. This possibility in turn depends on the special theory and on the type of formulas. Even when an algorithm to eliminate quantifiers is known to exist for some particular theory, it is not certain that such algorithm is effective. In particular, there might exists a faster algorithm for eliminating the universal quantifiers from formulas like the ones produced by pattern solving. The same can be said for structures that do not admit quantifier elimination. Most of the work in the rest of the thesis concentrates in finding algebraic properties that allow an efficient, and straighforward quantifier elimination algorithm for several theories and for particular problem formulas.

Once that fast quantifier elimination is established and a quantifier free formula is obtained, still there need to be a fast way of finding ground term solutions for this last system of equations. This is a very hard problem. As it has been seen in the previous chapter, this problem is already very hard for equational theories. Neverthless, for many interesting structures, algorithms are available that are effective for special cases. Comparatively, less investigation has been devoted to inventing algorithms for finding ground term solutions of the quantifier free problems. This is due to the reason that the last step of the pattern solving algorithm should be easy, meaning that it should be computable in a reasonable time by the known methods. Therefore, the parts on solving constraints will in most cases just outline the main idea of the solving algorithm.

In the next chapters, equational constraint solving via patterns is studied for stepwise richer algebraic structures: commutative rings, modules over a commutative ring, commutative algebras and exterior graded algebras. The framework is always first-order logic with many sorts. Many sorted domains are taken into consideration instead of the simpler one sorted structures because, in real-world aoplication, “types” are natural. Admittedly, having to deal with a typed language, and typed formulas adds a level of complication to the proofs and this explains why most of the literature in quantifier elimination hardly deals with sorts. Neverthless, the author feels that showing the results already for formulas of a sorted language allows to implement them directly and it is worth the effort.

The exposition starts with one-sorted domains containing less function symbols and stepwise tackles domains containing more function symbols and more sorts by building upon the previous results.

3.6 Summary

In this chapter the approach to constraint solving using solution patterns has been introduced. The method is called pattern solving since it shifts the emphasis of solving from the constraints to the unknown coefficients in the solution pattern. Precisely, the problem is to find term expressions that, substituted for these coefficients, turn the pattern into a solution for the system of equational constraints.

Two types of pattern solving problems have been introduced, one with no extra constants and one with a presentation of new constant symbols. For both problems, the general structure of the algorithm that solves the problem is described and its correctness is shown.

Pattern solving can now be developed for specific algebraic structures, starting with commutative rings.

4

Pattern Solving in Commutative Rings

After having introduced pattern solving in a generic algebraic structure, this chapter develops the method to commutative rings. This case is very illustrative of the general way to approach the development of a pattern solving algorithm for a specific algebraic structure. Commutative rings are structures with two binary operations, like the integer numbers $\mathbb{Z}$ with addition and multiplication. Symbolic constraint solving in commutative rings with unit amounts to finding integer solution for Diophantine polynomials. This problem is the well known Hilbert's Tenth Problem and was proven undecidable by Matijasevič (1970). Because of this, it makes sense to try to attack constraint solving by using patterns.

It will be shown that for rings that are integral domains, it is possible to perform very fast quantifier elimination on problem formulas obtained by equational problems. Moreover, the ground terms solutions for the resulting system of equations can, in some lucky cases, be found by computational techniques of elimination theory in computer algebra, like the Gröbner basis. Therefore, having the basic ingredients, pattern solving can be easily applied to problems in commutative rings with unit.

The Chapter is organized in a first Section recalling some algebraic properties of commutative rings. The pattern solving problem is described in Section 4.2. The central part of the Chapter is Section 4.3 that deals with elimination of quantifiers from problem formulas that arise in this context. Section 4.4 outlines a semi-decision algorithm for finding a ground term solution to the final system of equations associated to the problem formula. Finally, an example is presented in Section 4.5.

4.1 Algebraic Preliminaries

This chapter is devoted to the study of pattern solving in rings that are both associative and commutative. From now on, let "ring" mean "associative commutative ring". A ring is a structure for the signature $\langle 0, -, +, * \rangle$ with three operations: addition, subtraction and multiplication. Addition has a zero element 0 and is associative and commutative. Multiplication is associative and commutative. Furthermore, every element has and additive inverse (which makes the structure an additive group) and multiplication distributes over addition. Commutative rings in the signature $\langle 0, -, +, * \rangle$ can be axiomatized by a set of universal equations, hence their theory is equational:

$$\begin{aligned} \forall x \forall y \forall z\ (x+y)+z &= x+(y+z) \\ \forall x \forall y\ x+y &= y+x \\ \forall x \forall y\ x+(-x) &= 0 \\ \forall x\ x+0 &= x \end{aligned} \tag{4.1}$$

$$\begin{aligned} \forall x \forall y (\forall z)\ (x*y)*z &= x*(y*z) \\ \forall x \forall y\ x*y &= y*x \\ \forall x \forall y (\forall z)\ x*(y+z) &= x*y+x*z \end{aligned} \tag{4.2}$$

A ring with identity is a structure for the signature $\langle 0, 1, +, -, * \rangle$ which satisfies the axioms of rings (4.1)-(4.2) together with the following:

$$\begin{aligned} \forall x\ x*1 &= x \\ 1 &\neq 0 \end{aligned} \tag{4.3}$$

The integer numbers $\mathbb{Z}$ are the usual model of a ring, but also the rationals $\mathbb{Q}$, the real $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are rings. Another example of a ring is the ring of polynomials with rational coefficients. Let $\mathfrak{R}$ be a ring.

Rings with no nonzero zero divisors are called integral domains or also domains. The theory of integral domains is a universal theory, namely it is obtained by adding the axiom:

$$\forall x \forall y\ x*y=0 \rightarrow x=0 \vee y=0 \tag{4.4}$$

to the axioms (4.1)-(4.2)-(4.3) of rings with unit. Note that it is not an equational theory. All fields are integral domains and, vice-versa, all finite domains are fields.

Many properties of rings are related to the characteristic of the ring. The smallest prime number c for which $c*1=0$ is called the characteristic of $\mathfrak{R}$. If no such number exists, then the ring $\mathfrak{R}$ is said to have characteristic 0.

If the ring is a domain, then the characteristic c has to be a prime number otherwise the divisors of c would be nonzero zero divisors. Domains of characteristic zero are not finitely axiomatizable because there is no first-order axiom stating that the characteristic is zero. The natural axiom is an infinite conjunction:

$$1 \neq 0 \wedge 3*1 \neq 0 \wedge 5*1 \neq 0 \wedge 7*1 \neq 0 \wedge \ldots \tag{4.5}$$

Thus, domains of characteristic zero are recursively axiomatizable.

Let t be a term in the language of rings, for instance:

$$x*x+(1+1)*x+1$$

with free variables x, then $t^{\mathfrak{R}}: R \rightarrow R$ is the corresponding polynomial function from R into R. Hence, terms in free variables X are indeed polynomials in $R[X]$ and are interpretable as polynomial functions.

This last observation is very useful for establishing a unique way of writing terms in the language of rings. In fact, adopting a common technique of computational algebra, it is enough to fix an ordering on the free variables appearing in the term. This variable ordering induces a term ordering among the monomials, the subterms of the polynomial, by which there is a unique way of writing a polynomial. The reader may learn more by consulting some standard textbooks for the theory of commutative rings.

Before studying the problem of instantiation of solution pattern for systems of equations over commutative rings, some well known facts about polynomials are recalled, for the details see for instance van der Waerden (1948). These results are necessary for showing how it is possible to perform straightforward quantifier elimination on problem formulas produced by the pattern solving algorithm.

Most of the theorems recalled deal with the number of roots of polynomials. Let $p(x)$ be a univariate polynomial in variable x, then an element $\alpha \in \mathfrak{R}$ is a root of p if $p^{\mathfrak{R}}(\alpha) = 0$. In particular in a domain $\mathfrak{D}$, the degree of a polynomial is a bound on its number of roots.

Theorem 4.1
Let $p(x) \in D[x]$ be a univariate polynomial of degree $n > 0$ and $\mathfrak{D}$ be an integral domain. Then $p(x)$ has at most n roots in $\mathfrak{D}$.

Theorem 4.1 holds in integral domains, it does not hold neither in rings with nonzero zero divisors, nor in non-commutative rings. For instance, in $\mathbb{Z}_{16}$, the residue class modulo 16, the polynomial x^2 has more than 2 roots: all

$$\alpha_1 = 2, \qquad \alpha_2 = 4, \qquad \alpha_3 = 8, \qquad \alpha_4 = 12 \tag{4.6}$$

are roots.

The next theorem states that, for a nonzero multivariate polynomial, there is at least a set of values which is not a root.

Theorem 4.2
Let $\mathfrak{D}$ be an infinite integral domain or an extension of one and let $p(x_1, \ldots, x_r)$ be a nonzero multivariate polynomial in $D[x_1, \ldots, x_r]$. Then there exists $\alpha_1, \ldots, \alpha_r \in D$ for which $p^{\mathfrak{D}}(\alpha_1, \ldots, \alpha_r) \neq 0$.

Proof. The proof is by induction of the number of variables. The case $n = 1$ is taken care of by the Theorem 4.1. Assume that the result holds for polynomials with up to $r - 1$ variables. Then, it must be shown for polynomials with r variables. Let $p(x_1, \ldots, x_r)$ be one such polynomial. Writing it as a polynomial in x_r:

$$p(x_1, \ldots, x_r) = q_0 + q_1 x_r + \ldots + q_n x_r^n$$

with nonzero coefficients $q_0, \ldots, q_n \in D[x_1, \ldots, x_{r-1}]$. By the induction hypothesis, there exist $\alpha_1, \ldots, \alpha_{n-1} \in D$ such that $q_n^{\mathfrak{D}}(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. But then:

$$p(\alpha_1, \ldots, \alpha_{n-1}, x_r) = q_0(\alpha_1, \ldots, \alpha_{n-1}) + q_1(\alpha_1, \ldots, \alpha_{n-1})x_r + \ldots + q_n(\alpha_1, \ldots, \alpha_{n-1})x_r^n \neq 0$$

is a polynomial in $D[x_n]$. By Theorem 4.1, there exists $\alpha_n \in D$:

$$p^{\mathfrak{D}}(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \neq 0.$$

∎

The corollary of Theorem 4.2 states that the only polynomial which has an infinite number of roots is the constant zero polynomial. This result is used in Section 4.3 for showing fast elimination of quantifiers.

Corollary 4.1
Let $\mathfrak{D}$ be an infinite integral domain or an extension of one and let $p(x_1, \ldots, x_r)$ be a polynomial in $D[x_1, \ldots, x_r]$ such that for all $\alpha_1, \ldots, \alpha_n \in D$,

$$p(\alpha_1, \ldots, \alpha_r) = 0.$$

Then $p(x_1, \ldots, x_r)$ vanishes identically (all coefficients are zero).

Corollary 4.1 can be extended in a straightforward way to a finite set of polynomials. In the next section, pattern solving is described for the structure of rings.

4.2 Problem Description

This section will study pattern solving when the structure $\mathfrak{A}$ is a ring $\mathfrak{R}$ for the signature $\Sigma = \langle 0, 1, +, -, * \rangle$.

Let $\mathfrak{R}$ be a Σ-ring. A problem Γ can be reduced to a system of polynomial term equations of the form:

$$\begin{array}{rcl} a_{1,1}X_1 + a_{1,2}X_2 + \ldots + a_{1,n}X_n + a_{1,n+1} & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m,1}X_1 + a_{m,2}X_2 + \ldots + a_{m,n}X_n + a_{m,n+1} & = & 0 \end{array} \tag{4.7}$$

where $X_1, \ldots, X_n \in [x_1, \ldots, x_k]$ are monomials in variables $x_1, \ldots, x_k$ over R, while $a_{1,1}, \ldots, a_{m,n+1}$ are ground ring terms, namely they have the form $1 + \ldots + 1$ or 0. It is notational convention to abbreviate a sum of 1's by the corresponding numeral, so that the polynomial terms have integer coefficients. Recall that polynomials with integer coefficients are also called Diophantine polynomials.

A solution pattern π is an assignment of ring terms to each variable in the problem:

$$\begin{array}{rcl} x_1 & = & p_1(Z, Y) \\ \vdots & \vdots & \vdots \\ x_k & = & p_k(Z, Y). \end{array} \tag{4.8}$$

containing unknown coefficients Z and parameters Y.

Recall the algorithm described in Section 3.3. Once the substitution π is applied to the problem Γ, the resulting problem formula $\psi(Y, Z)$ is a conjunction of equations among terms with universally quantified variables Y. The terms in the formula $\psi(Y, Z)$ can be read as polynomials in Y with as coefficients polynomials in Z. Hence the problem formula $\psi(Y, Z)$ is a conjunction of the form:

$$\forall Y \bigwedge_{1 \le i \le n} t_{i,1}(Z)Y_1 + \ldots + t_{i,h}(Z)Y_h + t_{i,h+1}(Z) = 0. \tag{4.9}$$

The next step in the algorithm for pattern solving is the elimination of the universal quantifiers over the parameters from formula (4.9). The reader will recognize that this can be efficiently achieved by the high-school trick of comparison of coefficients as the next section shows.

4.3 Elimination of Universal Quantifiers

Effective quantifier elimination can be shown for commutative rings that are infinite integral domains. The model theoretic properties of associative rings that admit elimination of quantifiers have been studied by Rose (1978) and by Berline (1981). What is presented in this section is a well known elimination method that follows from Corollary 4.1 and applies only to problem formulas.

Since there is only one sort in the language, there is also only one type of problem formula to be considered for quantifier elimination, formula (4.9). In order to use the pattern solving algorithm, it is necessary to find an equivalent quantifier-free formula, $\phi(Z)$, in terms of the unknown coefficients only, such that:

$$\mathfrak{R} \models \forall Y \bigwedge_{1 \leq i \leq n} t_{i,1}(Z)Y_1 + \ldots + t_{i,h}(Z)Y_h + t_{i,h+1}(Z) = 0 \leftrightarrow \phi(Z). \tag{4.10}$$

One direction is trivial, if all the coefficients are zero, then the polynomials in the problem formula evaluate to zero for all values of the parameters Y. For showing the reverse direction, the results on roots of polynomials recalled in section 4.1 are used. Fast quantifier elimination can be achieved when the ring $\mathfrak{R}$ is an infinite integral domain.

THEOREM 4.3
Let $\mathfrak{D}$ be an infinite integral domain for the signature Σ, $t_0, \ldots, t_n$ be Σ-terms not containing Y and $Y_1, \ldots, Y_h \in [Y]$ be monomials. Then

$$\mathfrak{D} \models \forall Y\ t_0 + t_1Y_1 + \ldots + t_hY_h + t_{h+1} = 0 \leftrightarrow t_0 = 0 \wedge \ldots \wedge t_h = 0 \wedge t_{h+1} = 0.$$

PROOF. One direction is trivial.

The remaining direction follows from Corollary 4.1 since, when $\mathfrak{D}$ is an integral domain, then $t_0 + t_1Y_1 + \ldots + t_nY_h + t_{h+1}$ is interpreted as a polynomial in $D[Y]$. ■

When the ring is a domain but it is not infinite, this effective way of eliminating the universal quantifiers does not apply. As a counterexample consider for instance the case of $\mathbb{Z}_2$, a finite domain, and consider the formula

$$\forall y\ y^2 + y = 0. \tag{4.11}$$

This formula is verified for all elements of the domain $\mathbb{Z}_2 : \alpha_1 = 0, \alpha_2 = 1$ despite the fact that the polynomial is not the zero polynomial. Hence:

$$\mathbb{Z}_2 \models \forall y\ y^2 + y = 0 \quad \text{but} \quad \mathbb{Z}_2 \not\models 1 = 0. \tag{4.12}$$

Examples of infinite integral domains, where this type of quantifier elimination is applicable, are the ring of integers and the ring of polynomials with coefficients in an integral domain.

Theorem 4.3 applied to the quantifier elimination problem (4.10) allows to derive the quantifier-free formula $\psi(Z)$:

$$\bigwedge_{1 \leq i \leq n} t_{i,1}(Z) = 0 \wedge \ldots \wedge t_{i,h+1}(Z) = 0. \tag{4.13}$$

Since $\psi(Z)$ is a conjunction of equations, the last step of the pattern solving algorithm consists in solving the associated system of equations for finding ground term solutions for Z.

4.4 *Symbolic Constraint Solving in Commutative Rings*

The last step of the algorithm described in Section 3.3 is solving the system of equations associated to the quantifier free formula $\psi(Z)$ derived from the problem formula. For commutative rings, this system of polynomial equations is:

$$\{t_{i,j}(Z) = 0 \mid 1 \leq i \leq n, 1 \leq j \leq h, t_j^{(i)}(Z) \in D[Z]\}. \tag{4.14}$$

At this point, the undecidable problem of Diophantine equations shows up again. The pattern solving approach necessarily gives only a partial solution to the problem. Here follows a sketch of one possible solution. Consider the equations in the algebraic closure of the field of quotients of the integral domain. Clearly, if there is no solution in the algebraic closure, there cannot be any solution in the integral domain. If, on the other hand, there are solutions in the algebraic closure, then one has to check where these solution lie.

For instance, if the integral domain $\mathfrak{D}$ is the integers $\mathbb{Z}$, then the equations are solved in the complex numbers $\mathbb{C}$. In fact $\mathbb{C}$ is the algebraic closure of the field of rational numbers $\mathbb{Q}$, that is the field of quotients of the integers. Several methods are available for solving polynomial equations over $\mathbb{C}$. The introductory survey (Kapur and Lakshman, 1992) on elimination methods applicable to systems of polynomial equations covers the method of resultants, of Gröbner bases, and the characteristic set method. Computing the lexicographic Gröbner basis according to some variable ordering is one of the most effective computational methods available for polynomial system solving. It is not in the scope of this thesis to introduce the theory of Gröbner basis, the reader can consult a wealth of books on the subject, for instance Buchberger (1965); Becker and Weispfenning (1993); Buchberger and Loos (1982). If the basis is triangular and there is a univariate polynomial, then the set of solutions is finite and they can be enumerated. In this case it is easy to check if among the solutions, there is one solution which is integer. If the basis is not triangular, then not much can be said since the set of solutions is infinite. In order to lower the dimension of the solution space, the user may be asked to specify one or more values for the unknown coefficients and ask for recomputation of the basis, until the basis is triangular. The method of pattern solving has no pretense of completeness, and this is exactly a point in which at times it gives up.

The author has not yet investigated any criteria, based on the number of unknown coefficients in relation to the input problem, which would ensure that the system of polynomial equations has a ground term solution. This problem is related to the problem of *Diophantine equations with parameters* in number theory, in Figure 4.1. Denote by $\forall^n\exists$, the class of formulas of type:

$$\forall x_1 \ldots \forall x_n \forall y \; f(x_1, \ldots, x_n, y) = 0. \tag{4.15}$$

GIVEN:	a Diophantine polynomial $f(x_1, \ldots, x_n, y) = 0$,
FIND:	if for any numbers $x'_1, \ldots, x'_n$, the equation $f(x'_1, \ldots, x'_n, y) = 0$ is solvable over $\mathbb{N}$, or $\mathbb{Z}$ or $\mathbb{Q}$.

Figure 4.1: The Problem of Diophantine Equations with Parameters.

Assume that the parameters in a pattern solving problem are $Y = \{y_1, \ldots, y_n\}$ and the unknown coefficients are $Z = \{z_1, \ldots, z_m\}$. Then, the existence of a criteria ensuring a ground term solution for the system (4.14) of polynomial equations implies the decidability of the Diophantine parameter problem for the class $\forall^n \exists^m$ over $\mathbb{Z}$. Interestingly, for special classes one is able to decide if a ground term solution exists. Tung (1988, 1990) has shown that the class $\forall^n \exists$ is indeed decidable over the integers. The class $\forall\exists$ is decidable both in $\mathbb{Z}$ and $\mathbb{Q}$, with computational complexities of the decision algorithms co-NP and P respectively. Tung (1995) has also shown that the $\forall\exists$ theory of integral domains of characteristic zero is decidable.

4.5 Example

EXAMPLE 4.1
Consider the following problem over the ring of integers $\mathbb{Z}$:

$$-2y^3 - 1 + 2z + 2y^3 z - z^2 - y^6 + x^3 = 0$$

Let the solution pattern π be:

$$\begin{aligned} x &= t^2 + as^2, \\ y &= bt + s, \\ z &= ct^3 + ds^3 + 1 \end{aligned}$$

The parameters are t and s. The unknown coefficients are a, b, c, and d. After substitution, the formula from which the quantifiers have to be eliminated is the following:

$$\begin{aligned} (\forall s)(\forall t) \quad & 2s^6 d - c^2 t^6 - d^2 s^6 - b^6 t^6 - s^6 + t^6 + 2b^3 t^6 c + 2s^3 ct^3 - 6b^5 t^5 s - \\ & 15b^4 t^4 s^2 - 20b^3 t^3 s^3 - 15b^2 t^2 s^4 - 6bts^5 + 3t^4 as^2 + 3t^2 a^2 s^4 + \\ & 2b^3 t^3 ds^3 + 6b^2 t^5 sc + 6b^2 t^2 s^4 d + 6bt^4 s^2 c + 6bts^5 d - 2ct^3 ds^3 + a^3 s^6 = 0 \end{aligned}$$

By considering the coefficients of the monomials in s and t to be zero, the equivalent quantifier-free formula is obtained:

$$
\begin{aligned}
2d - 1 - d^2 + a^3 &= 0\wedge \\
-c^2 + 2b^3c - b^6 + 1 &= 0\wedge \\
2c + 2b^3d - 2cd - 20b^3 &= 0\wedge \\
-6b^5 + 6b^2c &= 0\wedge \\
6bc + 3a - 15b^4 &= 0\wedge \\
-15b^2 + 6b^2d + 3a^2 &= 0\wedge \\
6bd - 6b &= 0.
\end{aligned}
$$

There are two solutions for this set of equations:

$$\{a = b = 0, c = d = 1\} \qquad \{a = b = 0, c = -1, d = 1\}$$

Respectively, they yield the instances of the solution pattern:

$$
\begin{array}{ll}
x = t^2 & x = t^2 \\
y = s & y = s \\
z = t^3 + s^3 + 1 & z = -t^3 + s^3 + 1
\end{array}
$$

4.6 Summary

In this chapter, the method of symbolic pattern solving has been developed and studied for the one-sorted structure of commutative rings. It has been shown that infinite integral domains admit fast elimination of universal quantifiers for problem formulas arising from pattern solving. Infinite integral domains are rings without nonzero zero divisors, as the ring of integers and the ring of polynomials with coefficients in a domain.

The main contribution of this chapter is the illustration of the technique for devising fast elimination of quantifiers. The same reasoning used here for commutative rings will be used again in the following chapters.

Future work is the investigation of criteria to ensure that the final system of equations to be solved has a finite number of solutions. Such a criterion exists for special cases. When the pattern problem contains one parameter and one unknown coefficient then the decidability of the $\forall\exists$ class of Diophantine equations provides the criterion. The question is open for other classes.

5

Pattern Solving in Modules over a Ring

This chapter develops the pattern solving method for the algebraic structures of modules over commutative rings. While the former chapter studied pattern solving for the one-sorted structure of commutative rings, the novelty here consists in dealing with a structure for a signature with two sorts. The sorts are the scalar sort, ranging over a commutative ring, and the vector sort, ranging over an additive group. As operations, there are the ring operations for the scalars, the group operations for the vectors, and additionally a group valued scalar multiplication between a scalar and a vector.

Modules over commutative rings, or R-modules, are generalizations of vector spaces. In fact, when the ring is a field, the module is indeed a vector space. This relation with vector spaces makes the structure of R-modules interesting from the applicative point of view. The many-sorted formulation of the problem is also motivated by the applicative contexts in which constraint solving arises. In fact, types often enforce correctness.

In order to use the pattern solving approach, the theory of modules over rings must admit efficient quantifier elimination for the problem formulas that arise. Two quantifier elimination theorems are shown in this chapter: one for universally quantified vector variables and one for universally quantified scalar variables. Combining the two, it is possible to show the general result that torsion-free modules over infinite integral domains allow efficient elimination of universal quantifiers over scalar and vector variables.

The chapter is organized as follows. Section 5.1 presents the algebraic preliminary notions that are needed subsequently. The problem of pattern solving in R-modules is described in detail in Section 5.2. The core of the chapter is Section 5.3 on the fast elimination of universal quantifiers in problem formulas. Section 5.4 briefly outlines a possible procedure for finding ground term solutions to the systems of equations associated to the quantifier free formulas. The final Section 5.5 applies pattern solving to some simple examples.

5.1 Algebraic Preliminaries

Let $\mathfrak{R}$ be ring structure for the signature $\langle 0, 1, -, +, *\rangle$. There are two ways of looking at modules over $\mathfrak{R}$: as one-sorted structures or as two-sorted structures. In the first case, R-modules are additive groups over the sort vector with additionally one unary operation $\cdot_r$, for each scalar $r \in R$, verifying certain properties. In a two-sorted setting, R-modules contain the sort scalar ranging over the ring $\mathfrak{R}$ and the sort vector ranging over the additive group $\mathfrak{M}$. The group $\mathfrak{M}$ is a structure for the signature $\langle \mathbf{0}, \mathbf{+}, \mathbf{-} \rangle$ and for a binary operation $\cdot$.

The group operations are specified in the following way:

$$\begin{array}{rlll} \mathbf{0}: & \to \mathsf{vector} & \text{(zero)} & \\ \mathbf{-}: \mathsf{vector} & \to \mathsf{vector} & \text{(unary minus)} & \\ \mathbf{+}: \mathsf{vector} \times \mathsf{vector} & \to \mathsf{vector} & \text{(addition)} & (5.1) \\ \cdot: \mathsf{scalar} \times \mathsf{vector} & \to \mathsf{vector} & \text{(multiplication by scalar)} & \end{array}$$

The axioms of R-modules include the axioms of rings (4.1)-(4.2)-(4.3) for the signature $\langle 0, 1, -, +, *\rangle$, and the following group axioms. Let the variables $\mathbf{u}, \mathbf{v}, \mathbf{w}$ be of sort vector and x, y be of sort scalar,

$$\begin{array}{r} \forall\mathbf{u}\forall\mathbf{v}\forall\mathbf{w}\ (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w}) \\ \forall\mathbf{u}\forall\mathbf{v}\ \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} \\ \forall\mathbf{u}\ \mathbf{u} + (\mathbf{-}\,\mathbf{u}) = \mathbf{0} \\ \forall\mathbf{u}\ \mathbf{u} + \mathbf{0} = \mathbf{u} \\ \forall x\forall y\forall\mathbf{u}\ (x * y) \cdot \mathbf{u} = x \cdot (y \cdot \mathbf{u}) \\ \forall x\forall y\forall\mathbf{u}\ (x + y) \cdot \mathbf{u} = (x \cdot \mathbf{u}) \mathbf{+} (y \cdot \mathbf{u}) \\ \forall x\forall\mathbf{u}\forall\mathbf{v}\ x \cdot (\mathbf{u} + \mathbf{v}) = (x \cdot \mathbf{u}) \mathbf{+} (x \cdot \mathbf{v}) \\ \forall\mathbf{u}\ 1 \cdot \mathbf{u} = \mathbf{u} \end{array} \tag{5.2}$$

More precisely, depending on the side on which the multiplication by a scalar is defined, the module is either a left or a right R-module. Axioms (5.2) are of a left R-module. Every Abelian group is an example of $\mathbb{Z}$-module.

Observe that the theory of R-modules is, not only a universal theory, but is also an equational theory if the ring is associative and commutative. This is true anymore when the ring is a field or when the module is torsion-free.

Definition 5.1
A module $\mathfrak{M}$ is torsion free if for all $r \in R$, $rM = \mathbf{0}$ implies that either $M = \mathbf{0}$ or $r = 0$.

The theory of torsion-free modules is obtained by adding the axiom:

$$\forall r\forall\mathbf{u}\ r \cdot \mathbf{u} = \mathbf{0} \to r = 0 \vee \mathbf{u} = \mathbf{0}. \tag{5.3}$$

to the axioms (5.2). This theory is universal but it is neither equational nor positive conditional. As it will be shown, efficient elimination of quantifiers is complete in the class of torsion free modules over an infinite integral domain.

In the two-sorted signature for R-modules $\Sigma = \langle 0, \mathbf{0}, 1, -, \mathbf{-}, +, \mathbf{+}, *, \cdot\rangle$, terms can be brought to the form of linear polynomials with coefficients in the scalar domain:

$$t_1 \cdot \mathbf{u_1} \mathbf{+} t_2 \cdot \mathbf{u_2} \mathbf{+} \ \ldots\ \mathbf{+} t_n \cdot \mathbf{u_n} \tag{5.4}$$

where $t_1, \ldots, t_n$ are scalar terms (polynomials over R). An equation is a formula:

$$t_1 \cdot \mathbf{u_1} \mathbf{+} t_2 \cdot \mathbf{u_2} \mathbf{+} \ \ldots\ \mathbf{+} t_n \cdot \mathbf{u_n} = \mathbf{0}. \tag{5.5}$$

Observe that it is possible to write an equation in this form because the signature Σ contains the unary minus.

Before describing the pattern solving problem in R-modules, a remark is in order. When the signature Σ does not contain any vector constant beside $\mathbf{0}$, the pattern solving problem is trivial. In fact, the only possible term assignment for vector variables is the one assigning the zero vector $\mathbf{0}$ to all variables. Therefore, there must be some extra user-defined constant symbols of type vector. There are two possibilities for defining extra constants, either these new constants are linearly independent, or they are related by some equations.

DEFINITION 5.2
Let $\mathfrak{M}$ be a left R-module. A family of elements $\mathbf{a_1}, \ldots, \mathbf{a_n} \in \mathbf{M}$ is linearly independent if for any $\alpha_i \in R$:

$$\alpha_1 \cdot \mathbf{a_1} + \ldots + \alpha_n \cdot \mathbf{a_1} = \mathbf{0} \Rightarrow \alpha_1 = 0 \wedge \ldots \wedge \alpha_n = 0.$$

Definition 5.2 is extended naturally to an infinite family of elements by considering the linear independence of all finite sub-families. A linearly independent set is called a *basis* if it generates the module. A module is called *free* if it has a basis. Note that every module can be expressed as a homomorphic image of a free module. It will be shown that pattern solving in two-sorted free R-modules reduces to pattern solving over $\mathfrak{R}$.

When the constant are related by some equation, the pattern solving method is the more general one described in Section 3.2. Namely, additionally there is a set Ψ of ground equations in an extended signature $\Sigma' = \Sigma \cup \{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$.

$$\Psi = \{\epsilon_{i,1} \cdot \mathbf{a}_1 + \epsilon_{i,2} \cdot \mathbf{a}_2 + \ldots + \epsilon_{i,n} \cdot \mathbf{a}_n = \mathbf{0} \mid \epsilon_{i,j} \in R, 1 \leq i \leq h, 1 \leq j \leq n\} \tag{5.6}$$

The next section, several types of pattern solving problems arising in the context of R-modules are described.

5.2 Problem Description

A constraint solving problem in a many sorted setting is again a set of equations in which some variables are free. Unlike the one-sorted framework in which there is only one sort of variables, hence one type of problems; in the two-sorted case, there are several types of problems, depending on the sort of the free variables. Moreover, in the solution pattern approach, the types of solution patterns can also be distinguished according to the sorts of the unknown coefficients and of the parameters that occur. It is possible that the pattern solving method is effective and elimination of quantifiers complete only for a particular combination of problem type and solution pattern type.

Since the theory of R-modules is equational, symbolic constraint solving is unification in a combination of theories that share a function symbol, multiplication by a scalar. The two theories are the theory of rings and the theory of additive Abelian groups. Since unification in rings is subsumed by unification in R-modules, any undecidability theorem holding for rings carries over to the theory of R-modules too. Thus, from the undecidability of unification in rings, it follows that unification in R-modules is also undecidable. This again motivates the pattern solving approach.

For the structure of R-modules in two sorts, there are three types of constraint solving problem: one where the free variables occurring are of sort scalar only, one where they are of sort vector and one where they are of both sorts. Each type of problem is studied separately in the following subsections. The exposition is willfully done by distinguishing the sub-cases because afterwards the general result follows easily.

5.2.1 Pattern Solving of Scalar Variables

A constraint solving problem Γ in R-modules is of type scalar when no vector variable appear. For what has been said about equations in R-modules, the input system Γ can be written as:

$$\begin{array}{rcl} t_{1,1}(X)\cdot \mathbf{a_1} + t_{1,2}(X)\cdot \mathbf{a_2} + \ldots + t_{1,n}(X)\cdot \mathbf{a_n} & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ t_{m,1}(X)\cdot \mathbf{a_1} + t_{m,2}(X)\cdot \mathbf{a_2} + \ldots + t_{m,n}(X)\cdot \mathbf{a_n} & = & \mathbf{0} \end{array} \tag{5.7}$$

where $t_{1,1}(X), \ldots, t_{m,n}(X)$ are scalar terms in variables $X = \{x_1, \ldots, x_l\}$ over the ring R, and $\mathbf{a} = \{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$ is a finite set of vector constants available in the extended signature Σ'.

With the additional assumption that the vector constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$ are linearly independent, problem (5.7) reduces to a pattern solving problem over the ring $\mathfrak{R}$. In fact, it is equivalent to the system of scalar equations:

$$\begin{array}{rcl} t_{1,1}(X) = 0 \wedge t_{1,2}(X) = 0 & \wedge \ldots \wedge & t_{1,n}(X) = 0 \\ \vdots & \vdots & \vdots \\ t_{m,1}(X) = 0 \wedge t_{m,2}(X) = 0 & \wedge \ldots \wedge & t_{m,n}(X) = 0. \end{array} \tag{5.8}$$

The reader can consult Chapter 4 for pattern solving in commutative rings.

Things are more involved when the constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$ are defined by a set Ψ of generating equations, say the set of equations (5.6).

The solution pattern π for the scalar variables $X = \{x_1, \ldots, x_l\}$ appearing in the problem (5.7) is an assignment of scalar terms $p_1, \ldots, p_l$ in scalar parameters Y and scalar unknown coefficients Z:

$$\begin{array}{rcl} x_1 & = & p_1(Z, Y) \\ \vdots & \vdots & \vdots \\ x_l & = & p_l(Z, Y). \end{array} \tag{5.9}$$

These scalar terms are polynomials in indeterminates Y with coefficients in $R[Z]$, thus elements of the polynomial ring $(R[Z])[Y]$. Note that there appear no variable of type vector in the solution.

The pattern solving algorithm described in Section 3.3 initially builds the problem formula form the input problem Γ and the pattern solution π. After substitution, the problem formula $\psi(Y, Z)$ is the conjunction:

$$\forall Y \bigwedge_{1\le i\le m} t'_{i,1}(Z, Y)\cdot \mathbf{a_1} + \ldots + t'_{i,n}(Z, Y)\cdot \mathbf{a_n} = \mathbf{0} \tag{5.10}$$

for some scalar terms $t'_{1,1}(Z, Y), \ldots, t'_{m,n}(Z, Y)$. Using the axioms of distributivity, $\psi(Y, Z)$ can be reordered by collecting all the monomials $Y_{i,1}, \ldots, Y_{i,k} \in [y_1, \ldots, y_l]$ in the scalar parameters Y:

$$\forall Y \bigwedge_{1\le i\le m} Y_{i,1}\cdot \mathbf{q_{i,1}}(Z) + \ldots + Y_{i,k}\cdot \mathbf{q_{i,k}}(Z) + \mathbf{q_{i,k+1}}(Z) = \mathbf{0}. \tag{5.11}$$

Each $\mathbf{q_{i,1}}(Z), \ldots, \mathbf{q_{i,k+1}}(Z)$ is a vector term in free scalar variables Z and extra constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$. If the vector subterms are linear combinations of the constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$, then formula (5.11) can be written in a unique way, provided that the monomials $Y_{i,1}, \ldots, Y_{i,k}$ are pairwise disjoint and ordered according to some fixed term ordering. Moreover, there can be only one vector term $\mathbf{q_{i,k+1}}(Z)$ multiplied by no monomial.

The next step requires elimination of quantifiers. In order to simplify the notation, observe that the universal quantifier distributes over the conjunction:

$$\bigwedge_{1 \le i \le m} \forall Y \; Y_{i,1} \cdot \mathbf{q}_{i,1}(Z) + \ldots + Y_{i,k} \cdot \mathbf{q}_{i,k}(Z) + \mathbf{q_{i,k+1}}(Z) = \mathbf{0}.$$

Therefore, it is enough to study efficient quantifier elimination for one equation only:

$$\forall Y \; Y_1 \cdot \mathbf{q}_1(Z) + \ldots + Y_k \cdot \mathbf{q}_k(Z) + \mathbf{q_{k+1}}(Z) = \mathbf{0}. \tag{5.12}$$

The reader may skip to Section 5.3.1 to read about elimination of quantifiers in formulas like (5.12). The next Section describes a second type of pattern solving problem in modules over rings.

5.2.2 Pattern Solving of Vector Variables

A second type of pattern solving problem in the two sorted theory of R-modules is one in which only free variables of sort vector occur. In general, such a problem Γ can be brought to the form:

$$\begin{array}{rcl} t_{1,1} \cdot \mathbf{x_1} + t_{1,2} \cdot \mathbf{x_2} + \ldots + t_{1,n} \cdot \mathbf{x_n} + \mathbf{t_{1,n+1}} & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ t_{m,1} \cdot \mathbf{x_1} + t_{m,2} \cdot \mathbf{x_2} + \ldots + t_{m,n} \cdot \mathbf{x_n} + \mathbf{t_{m,n+1}} & = & \mathbf{0} \end{array} \tag{5.13}$$

where $\mathbf{x_1}, \ldots, \mathbf{x_n} \in \mathbf{X}$ are vector variables over M, $t_{i,1}, \ldots, t_{i,n}, (1 \le i \le m)$ are pure scalar terms while $\mathbf{t_{i,n+1}}, \mathbf{1 \le i \le m}$ are vector terms, eventually containing the constants $\mathbf{a} = \{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$.

The solution pattern π studied in this section is an assignment of vector terms $\mathbf{q_1}, \ldots, \mathbf{q_n}$:

$$\begin{array}{rcl} \mathbf{x_1} & = & \mathbf{q_1}(Z, \mathbf{Z}, \mathbf{Y}) \\ \vdots & \vdots & \vdots \\ \mathbf{x_n} & = & \mathbf{q_n}(Z, \mathbf{Z}, \mathbf{Y}). \end{array} \tag{5.14}$$

where Z, $\mathbf{Z}$ are unknown scalar and vector coefficients respectively, while $\mathbf{Y}$ are parameters of sort vector. This is not the more general form for a solution pattern, since it would be possible to allow for scalar parameters also. Nevertheless, this form is general enough to obtain results that can be used for solving the fully general problem described in next Section.

As usual, the problem formula $\psi(Z, \mathbf{Z}, \mathbf{Y})$ is constructed from the input problem Γ applying the substitution π. The result is a conjunction of equations universally quantified:

$$\forall \mathbf{Y} \bigwedge_{1 \le i \le m} t_{i,1} \cdot \mathbf{q_1}(Z, \mathbf{Z}, \mathbf{Y}) + \cdots + \mathbf{t_{i,n+1}} = \mathbf{0}. \tag{5.15}$$

Instead of studying elimination of quantifiers for the formula (5.15) in this form, distributivity is applied to collect the vector parameters, say $\mathbf{y_1}, \ldots, \mathbf{y_r} \in \mathbf{Y}$:

$$\forall \mathbf{Y} \bigwedge_{1 \le i \le m} p_{i,1}(Z) \cdot \mathbf{y}_1 + \ldots + p_{i,r}(Z) \cdot \mathbf{y}_r + \mathbf{p_{i,r+1}}(Z, \mathbf{Z}) = \mathbf{0}. \tag{5.16}$$

Observe that the equations in the problem formula (5.16) have the same form of the input equations (5.13): the vector parameters $\mathbf{y_1}, \ldots, \mathbf{y_r}$ occur linearly, multiplied by scalarterms $p_{i,1}(Z), \ldots, p_{i,r}(Z)$, and there is a vector subterm $\mathbf{p_{i,r+1}}(Z, \mathbf{Z})$ eventually containing the constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$.

Like was done for the pattern solving problem of type scalar, described in Section 5.2.1, quantifier elimination is studied on a single equation:

$$\forall \mathbf{Y}\ p_1(Z) \cdot \mathbf{y_1} + \ldots + p_r(Z) \cdot \mathbf{y_r} + \mathbf{p_{r+1}}(Z, \mathbf{Z}) = \mathbf{0}. \tag{5.17}$$

After reordering, since each unknown vector coefficient appears only linearly, the only subterm that can contain the unknown vector coefficients $\mathbf{Z}$ is the subterm $\mathbf{p}_{r+1}(Z, \mathbf{Z})$. All other terms $p_1(Z), \ldots, p_r(Z)$ are pure scalar terms.

The reader interested in elimination of quantifiers in formulas like (5.17) can go to Section 5.3.2. The next Section describes the most general type of pattern solving problem in modules over rings.

5.2.3 Pattern Solving of Scalar and Vector Variables

The most general type of pattern solving problem in R-modules contains free variables of both sorts, scalar and vector. An input problem Γ can be brought to the general form:

$$\begin{array}{rcl} t_{1,1}(X) \cdot \mathbf{x_1} + t_{1,2}(X) \cdot \mathbf{x_2} + \ldots + t_{1,n}(X) \cdot \mathbf{x_n} + \mathbf{t_{1,n+1}}(X) & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ t_{m,1}(X) \cdot \mathbf{x_1} + t_{m,2}(X) \cdot \mathbf{x_2} + \ldots + t_{m,n}(X) \cdot \mathbf{x_n} + \mathbf{t_{m,n+1}}(X) & = & \mathbf{0} \end{array} \tag{5.18}$$

where $t_{i,1}(X), \ldots, t_{i,1}(X)$, $(1 \le i \le m)$ are scalar terms in variables $X = \{x_1, \ldots, x_l\}$, $\mathbf{x_1}, \ldots, \mathbf{x_n}$ are vector variables ranging over M, and $\mathbf{t_{i,n+1}}(X)$, $(1 \le i \le m)$ are vector terms in the extended signature Σ'.

The pattern solution π is an assignment of vector terms $\mathbf{q_1}, \ldots, \mathbf{q_n}$ in M for the vector variables and of scalar terms $p_1, \ldots, p_l$ for the scalar variables:

$$\begin{array}{rcl} \mathbf{x_1} & = & \mathbf{q}_1(Z, \mathbf{Z}, Y, \mathbf{Y}) \\ \vdots & \vdots & \vdots \\ \mathbf{x_n} & = & \mathbf{q}_n(Z, \mathbf{Z}, Y, \mathbf{Y}) \\ x_1 & = & p_1(Z, Y) \\ \vdots & \vdots & \vdots \\ x_l & = & p_l(Z, Y). \end{array} \tag{5.19}$$

As before, $\mathbf{Z}, \mathbf{Y}$ denote vector unknown coefficients and parameters respectively, while Z, Y scalar unknown coefficients and parameters respectively.

After substituting the pattern solution π for the variables in the initial problem Γ, the problem formula $\psi(Z, \mathbf{Z}, Y, \mathbf{Y})$ contains universally quantified scalar and vector parameters:

$$\forall \mathbf{Y}\ \forall Y \bigwedge_{1 \leq i \leq m} t'_{i,1}(Z, Y) \cdot \mathbf{q_1}(Z, \mathbf{Z}, \mathbf{Y}) + \cdots + \mathbf{t'_{i,n+1}}(Y, Z) = \mathbf{0}. \tag{5.20}$$

for some scalar terms $t'_{i,1}(Z, Y), (1 \leq i \leq m)$ and vector terms $\mathbf{t'_{i,n+1}}(Y, Z), (1 \leq i \leq m)$. The elimination can be done on either type first. As usual, quantifier elimination will be studied on one equation only:

$$\forall \mathbf{Y}\ \forall Y\ t'_1(Z, Y) \cdot \mathbf{q_1}(Z, \mathbf{Z}, \mathbf{Y}) + \cdots + \mathbf{t_{n+1}}'(Z, \mathbf{Z}, Y) = \mathbf{0}, \tag{5.21}$$

Efficient quantifier elimination is possible for faithful modules over infinite integral domains as the next section will show.

5.3 Quantifier Elimination

Quantifier elimination for R-modules has been widely studied in the literature when the language is one sorted. The classic result is the Bauer-Monk theorem by Baur (1976), but also many others have worked on R-modules. As far as the author knows, there is no result in the literature on R-modules concerning elimination of quantifiers for two-sorted formulas that contain existentially quantified scalar variables. Van den Dries and Holly (1992) have shown that two-sorted R-module admits elimination of quantifiers for formulas without existentially quantified scalar variables. Their result is based on the original Baur-Monk theorem for quantifier elimination in one-sorted modules. Since, in one-sorted modules, variables only range over the module elements, it is not possible to adapt the quantifier elimination proof of Baur-Monk to two-sorted formulas over modules that contain quantified scalar variables. This partly explains the restrictions imposed by van Den Dries and Holly.

In this section, three types of universal two-sorted R-module formulas, arising from the pattern solving problems described in the previous section, will be studied. As always, in all three cases, the straightforward solution of the quantifier elimination is incomplete when no conditions are imposed on the R-module.

One type of universally quantified formula has the form:

$$\forall Y\ Y_1 \cdot \mathbf{q_1} + \ \ldots\ + Y_k \cdot \mathbf{q_k} + \mathbf{q_{k+1}} = \mathbf{0} \tag{5.22}$$

where $Y_1, \ldots, Y_k \in [y_1, \ldots, y_l]$ are scalar monomials. The algorithm for pattern solving requires the elimination of the universally quantified scalar variables in formulas like (5.22).

The other type of universally quantified formula has the form:

$$\forall \mathbf{Y}\ p_1 \cdot \mathbf{y_1} + \ \ldots\ + p_r \cdot \mathbf{y_r} + \mathbf{p_{r+1}} = \mathbf{0} \tag{5.23}$$

where $p_1, \ldots, p_r$ are scalar terms, $\mathbf{y_1}, \ldots, \mathbf{y_r}$ are quantified vector variables and $\mathbf{p_{r+1}}$ is a vector term. In formulas like (5.23), the universally quantified vector variables must be eliminated in order for the pattern solving algorithm to continue.

The last type of problem formulas arising in the case of pattern solving in R-modules is a combination of the previous ones, recall formula (5.21):

$$\forall \mathbf{Y}\ \forall Y\ t'_1(Z, Y) \cdot \mathbf{q_1}(Z, \mathbf{Z}, \mathbf{Y}) + \cdots + \mathbf{t_{n+1}}'(Z, \mathbf{Z}, Y) = \mathbf{0}.$$

The results on quantifier elimination of scalar and vector parameters will be used for this general form of problem formula.

5.3.1 Quantifier Elimination of Scalar Variables

The goal of this section is to show how to perform fast elimination of the universal quantifiers from the two-sorted R-module formula (5.22). First of all, the formula can be further simplified. Since it holds for all assignments of the scalar parameters Y, it must hold also for the assignment:

$$y_1 = \ldots = y_n = 0.$$

This implies that the formula:

$$\mathbf{q_{k+1}} = \mathbf{0} \tag{5.24}$$

must hold. Therefore, combining formula (5.24) with the original problem formula (5.22) yields the new problem formula:

$$\forall Y \; Y_1 \cdot \mathbf{q_1} + \ \ldots \ + Y_k \cdot \mathbf{q_k} = \mathbf{0} \tag{5.25}$$

in which the monomials $Y_1, \ldots, Y_k \in [y_1, \ldots, y_n]$ are all pairwise distinct and not constant in R.

With no restriction of the R-module $\mathfrak{M}$, the direction:

$$\mathfrak{M} \ \models \mathbf{q_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{q_k} = \mathbf{0} \rightarrow \forall Y \; Y_1 \cdot \mathbf{q_1} + \ \ldots \ + Y_k \cdot \mathbf{q_k} = \mathbf{0}$$

holds by applying the axioms. This "easy" quantifier elimination becomes complete, so that also the reverse direction of the implication is satisfied, when the ring of scalars $\mathfrak{R}$ is an infinite integral domain or an extension of one.

In order to show the theorem on efficient quantifier elimination, the next Lemma is necessary.

LEMMA 5.1
Let $m_1, \ldots, m_k \in D[y_1, \ldots, y_n]$ be pairwise disjoint and non-constant monomials. Let $\mathfrak{D}$ be an infinite integral domain. Then there exists at least k tuples of D^n, say $\alpha_1, \ldots, \alpha_k$, such that the matrix:

$$\begin{bmatrix} m_1^{\mathfrak{D}}(\alpha_1) & m_2^{\mathfrak{D}}(\alpha_1) & \ldots & m_k^{\mathfrak{D}}(\alpha_1) \\ m_1^{\mathfrak{D}}(\alpha_2) & m_2^{\mathfrak{D}}(\alpha_2) & \ldots & m_k^{\mathfrak{D}}(\alpha_2) \\ \vdots & & \ddots & \vdots \\ m_1^{\mathfrak{D}}(\alpha_k) & m_2^{\mathfrak{D}}(\alpha_k) & \ldots & m_k^{\mathfrak{D}}(\alpha_k) \end{bmatrix} \tag{5.26}$$

has nonzero determinant.

PROOF. The proof shows that there exist $\alpha_1, \ldots, \alpha_k \in D^n$ such that the determinant of the matrix is not zero. Consider k tuples $X_1, \ldots, X_k$ of new variables:

$$\begin{array}{rcl} X_1 & = & (x_{11}, \ldots, x_{1n}) \\ X_2 & = & (x_{21}, \ldots, x_{2n}) \\ \vdots & \vdots & \vdots \\ X_k & = & (x_{k1}, \ldots, x_{kn}) \end{array} \tag{5.27}$$

$$\tag{5.28}$$

and construct the matrix with monomial entries in $D[X_1, \ldots, X_k]$:

$$\begin{bmatrix} m_1(X_1) & m_2(X_1) & \ldots & m_k(X_1) \\ m_1(X_2) & m_2(X_2) & \ldots & m_k(X_2) \\ \vdots & & \ddots & \vdots \\ m_1(X_k) & m_2(X_k) & \ldots & m_k(X_k) \end{bmatrix}$$

First of all, observe that the determinant $\mathrm{Det}(X_1, \ldots, X_k)$ of this matrix cannot be identically zero. In order to show this, is enough to show that each column is independent from any other column. By contradiction, suppose that column m_1 is not independent from columns $m_2, \ldots, m_k$. That is:

$$\begin{bmatrix} m_1(X_1) \\ m_1(X_2) \\ \vdots \\ m_1(X_K) \end{bmatrix} = \mu_2 \cdot \begin{bmatrix} m_2(X_1) \\ m_2(X_2) \\ \vdots \\ m_2(X_K) \end{bmatrix} + \mu_3 \cdot \begin{bmatrix} m_3(X_1) \\ m_3(X_2) \\ \vdots \\ m_3(X_K) \end{bmatrix} + \ldots + \mu_k \cdot \begin{bmatrix} m_k(X_1) \\ m_k(X_2) \\ \vdots \\ m_k(X_K) \end{bmatrix}$$

where $\mu_1, \ldots, \mu_k \in D[X_1, \ldots, X_k]$ are monomials and not all of them are zero. Now consider the first row:

$$m_1(X_1) = \sum_{j=2}^{k} \mu_j \cdot m_j(X_1).$$

From this, one can derive the following formula for the coefficients:

$$\mu_j = \frac{m_1(X_1)}{\delta_j m_j(X_1)} \qquad (1 \leq j \leq k, \delta_j \in D) \tag{5.29}$$

because of the rules for summing monomials. Moreover, since the monomials are pairwise disjoint, all coefficients $\mu_j \in D[X_1]$ are not constants in D. Substituting the expressions for the coefficients in (5.29) into the second row:

$$m_1(X_2) = \sum_{j=2}^{k} \frac{m_1(X_1)}{\delta_j m_j(X_1)} \cdot m_2(X_2).$$

yields a clearly false statement. Therefore, the columns are linearly independent. This implies that $\mathrm{Det}(X_1, \ldots, X_k)$ is a nonzero polynomial. Recall now that $\mathfrak{D}$ is an infinite integral domain and $\mathrm{Det}(X_1, \ldots, X_k)$ is a polynomial $p(X_1, \ldots, X_k) \in D[X_1, \ldots, X_k]$, hence $p(X_1, \ldots, X_k)$ has only a finite number of roots. By Theorem 4.2 there must exist at least one point

$$\alpha = (\alpha_{11}, \ldots, \alpha_{1n}, \alpha_{21}, \ldots, \alpha_{2n}, \ldots, \alpha_{k1}, \ldots, \alpha_{kn})$$

in $D^{n \times k}$ such that $p^{\mathfrak{D}}(\alpha_1, \ldots, \alpha_k) \neq 0$ where

$$\begin{aligned} \alpha_1 &= (\alpha_{11}, \ldots, \alpha_{1n}) \\ \alpha_2 &= (\alpha_{21}, \ldots, \alpha_{2n}) \\ \vdots & \quad \vdots \quad \vdots \\ \alpha_k &= (\alpha_{k1}, \ldots, \alpha_{kn}). \end{aligned}$$

■

Now all ingredients are available to show how to eliminate universally quantified scalar variables from problem formulas of scalar type.

THEOREM 5.1
Let $\mathfrak{D}$ be an infinite integral domain and let $\mathfrak{M}$ be the a torsion-free D-module. Let $m_1, \ldots, m_k \in D[Y]$ be monomials and let $\mathbf{q_1}, \ldots, \mathbf{q_k}$ be terms of sort vector *not containing any scalar variable Y. Then*

$$\mathfrak{M} \models \forall Y\ m_1 \cdot \mathbf{q}_1 + \ldots + m_k \cdot \mathbf{q}_k = \mathbf{0} \leftrightarrow \mathbf{q}_1 = \mathbf{0} \wedge \ldots \wedge \mathbf{q}_k = \mathbf{0}.$$

PROOF. Let $\mathfrak{D}$ be an infinite integral domain, M be a D-module, and $Y = \{y_1, \ldots, y_n\}$ denote the scalar variables.

The direction

$$\mathfrak{M} \models \forall Y\ m_1 \cdot \mathbf{q}_1 + \ldots + m_k \cdot \mathbf{q}_k = \mathbf{0} \leftarrow \mathbf{q}_1 = \mathbf{0} \wedge \ldots \wedge \mathbf{q}_k = \mathbf{0}.$$

is obvious.

The other direction of the implication has to be shown. Assume:

$$\forall Y\ m_1 \cdot \mathbf{q}_1 + \ldots + m_k \cdot \mathbf{q}_k = \mathbf{0}. \tag{5.30}$$

The goal is to show the consequence:

$$\mathbf{q}_1 = \mathbf{0} \wedge \ldots \wedge \mathbf{q}_k = \mathbf{0}.$$

Assume also that $m_1, \ldots, m_k$ are pairwise disjoint and non-constant monomials in the domain $D[y_1, \ldots, y_n]$. By Lemma 5.1, there exist at least k tuples of D^n, say $\alpha_1, \ldots, \alpha_k$, such that the matrix M:

$$\begin{bmatrix} m_1^{\mathfrak{D}}(\alpha_1) & m_2^{\mathfrak{D}}(\alpha_1) & \ldots & m_k^{\mathfrak{D}}(\alpha_1) \\ m_1^{\mathfrak{D}}(\alpha_2) & m_2^{\mathfrak{D}}(\alpha_2) & \ldots & m_k^{\mathfrak{D}}(\alpha_2) \\ \vdots & & \ddots & \vdots \\ m_1^{\mathfrak{D}}(\alpha_k) & m_2^{\mathfrak{D}}(\alpha_k) & \ldots & m_k^{\mathfrak{D}}(\alpha_k) \end{bmatrix}$$

is has nonzero determinant. Since (5.30) holds for all assignments of the parameters Y, it must be true for all the k assignments $y_1 = \alpha_{j1}, \ldots, y_n = \alpha_{jn}$ $(1 \leq j \leq k)$. It follows that the system of equations:

$$\begin{array}{rcl} m_1^{\mathfrak{D}}(\alpha_1) \cdot \mathbf{q_1} + m_2^{\mathfrak{D}}(\alpha_1) \cdot \mathbf{q_2} + \ldots + m_k^{\mathfrak{D}}(\alpha_1) \cdot \mathbf{q_k} & = & \mathbf{0} \\ m_1^{\mathfrak{D}}(\alpha_2) \cdot \mathbf{q_1} + m_2^{\mathfrak{D}}(\alpha_2) \cdot \mathbf{q_2} + \ldots + m_k^{\mathfrak{D}}(\alpha_2) \cdot \mathbf{q_k} & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ m_1^{\mathfrak{D}}(\alpha_k) \cdot \mathbf{q_1} + m_2^{\mathfrak{D}}(\alpha_k) \cdot \mathbf{q_2} + \ldots + m_k^{\mathfrak{D}}(\alpha_k) \cdot \mathbf{q_k} & = & \mathbf{0} \end{array}$$

is true. In matrix form:

$$M\mathbf{q} = \mathbf{0},$$

where $\mathbf{q}$, $\mathbf{0}$ are vectors containing respectively $\mathbf{q_1}, \ldots, \mathbf{q_k}$ and $\mathbf{0}, \ldots, \mathbf{0}$. The determinant of M is nonzero. Two cases must be distinguished. If $\mathrm{Det}(M)$ is a unit in $\mathfrak{D}$, then M is invertible in D:

$$\begin{aligned} M^{-1}M\mathbf{q} &= M^{-1}\mathbf{0} \\ I\mathbf{q} &= \mathbf{0}, \end{aligned}$$

where I is the identity matrix. Therefore:

$$\mathbf{q}_1 = \mathbf{0} \wedge \mathbf{q}_2 = \mathbf{0} \wedge \ldots \wedge \mathbf{q}_k = 0$$

as wanted.

If, instead, $\mathrm{Det}(M)$ is not a unit in D, the matrix M is similar to a upper triangular matrix M' (because D is a domain, hence triangularization of the matrix is well defined). Moreover, M' has no zero entries in the diagonal, since it has the same rank of M and M has rank k. Therefore:

$$M'\mathbf{q} = \mathbf{0}.$$

This implies, by expanding the rows, that:

$$\begin{array}{cccccc} m'_{1,1}\cdot\mathbf{q}_1 + & \ldots & \ldots & + m'_{1,k}\cdot\mathbf{q}_k & = \mathbf{0} \\ & \ddots & \vdots & \vdots & \vdots \\ & & m'_{k-1,k-1}\cdot\mathbf{q}_{k-1} & + m'_{k-1,k}\cdot\mathbf{q}_k & = \mathbf{0} \\ & & & m'_{k,k}\cdot\mathbf{q}_k & = \mathbf{0} \end{array} \tag{5.31}$$

for some $m'_{i,j} \in D$, entries of the matrix M'. By torsion freeness, since $m'_{k,k} \neq 0$, it follows that $\mathbf{q}_k = \mathbf{0}$. Now, back substitution into the system of equations and torsion freeness allows to derive the conclusion. ■

Summarizing, easy quantifier elimination can be applied to the R-module problem formula (5.11) yielding the equivalent quantifier free conjunction of vector equations in the scalar unknown coefficients:

$$\mathbf{q_1}(Z) = \mathbf{0} \wedge \ldots \wedge \mathbf{q_k}(Z) = \mathbf{0} \wedge \mathbf{q_{k+1}}(Z) = \mathbf{0},$$

if the module is torsion-free and the ring $\mathfrak{R}$ is an infinite integral domain.

5.3.2 Quantifier Elimination of Vector Variables

This section deals with efficient quantifier elimination of universally quantified vector variables from the two-sorted R-module formula (5.23). Again, straightforward simplification of this problem formula is possible. Since the formula is true for all assignments of the vector parameters $\mathbf{Y}$, it is in particular true for the trivial assignment:

$$\mathbf{y_1} = \ldots = \mathbf{y_r} = \mathbf{0}.$$

This implies that the formula:

$$\mathbf{p_{r+1}} = \mathbf{0} \tag{5.32}$$

must hold. Therefore, combining formula (5.32) with the original problem formula (5.23) yields a simpler problem formula:

$$\forall \mathbf{Y}\ p_1 \cdot \mathbf{y_1} + \ \ldots\ + p_r \cdot \mathbf{y_r} = \mathbf{0} \tag{5.33}$$

where $p_1, \ldots, p_r$ are scalar terms, $\mathbf{y_1}, \ldots, \mathbf{y_r}$ are quantified vector variables.

As usual, without any restriction on the R-module $\mathfrak{M}$, only one direction is true:

$$\mathfrak{M}\ \models p_1 = 0, \ldots, p_r = 0 \rightarrow \forall \mathbf{Y}\ p_1 \cdot \mathbf{y}_1 + \ \ldots\ + p_r \cdot \mathbf{y}_r = \mathbf{0}.$$

In order for the opposite direction to hold, the $\mathfrak{M}$ has to be torsion-free and there must exist at least one nonzero vector.

THEOREM 5.2
Let $\mathfrak{R}$ be a ring and let $\mathfrak{M}$ be a non trivial torsion-free R-module. Let $p_1, \ldots, p_r$ be scalar terms and let $\mathbf{y_1}, \ldots, \mathbf{y_r}$ be universally quantified vector variables. Then

$$\mathfrak{M}\ \models \forall \mathbf{Y}\ p_1 \cdot \mathbf{y_1} + \ \ldots\ + p_r \cdot \mathbf{y_r} = \mathbf{0} \leftrightarrow p_1 = 0 \wedge \ldots \wedge p_r = 0.$$

PROOF. The implication:

$$\mathfrak{M}\ \models p_1 = 0 \wedge \ldots \wedge p_r = 0 \rightarrow (\forall \mathbf{Y})\ p_1 \cdot \mathbf{y_1} + \ \ldots\ + p_r \cdot \mathbf{y_r} = \mathbf{0}$$

in this direction is clear.

In order to show the opposite direction, assume:

$$\forall \mathbf{Y}\ p_1 \cdot \mathbf{y_1} + \ \ldots\ + p_r \cdot \mathbf{y_r} = \mathbf{0}.$$

Since it holds for all values of $\mathbf{Y}$, it also holds for $\mathbf{y_1} = \mathbf{a}$, where $\mathbf{a} \neq \mathbf{0}$ exists by assumption, and $\mathbf{y_2} = \ldots = \mathbf{y_r} = \mathbf{0}$. This yields

$$p_1 \cdot \mathbf{a} = \mathbf{0}$$

and by torsion-freeness:

$$p_1 = 0.$$

By similar reasoning, it is possible to find r proper assignments such that for all $1 \leq i \leq r$, $p_i = 0$. ■

Summarizing, eliminating the quantifiers from the problem formula (5.17) yields a conjunction of scalar equations together with one vector equation:

$$p_1(Z) = 0 \wedge \ldots \wedge p_r(Z) = 0 \wedge \mathbf{p}_{r+1}(Z, \mathbf{Z}) = \mathbf{0} \tag{5.34}$$

provided that the R-module is a non trivial torsion-free module.

5.3.3 Quantifier Elimination of Scalar and Vector Variables

A combination of the results of the previous Section 5.3.1 and Section 5.3.2 allows to apply efficient quantifier elimination to formulas containing both scalar and vector quantified parameters. Consider the most general problem formula (5.21):

$$\forall \mathbf{Y}\ \forall Y\ t'_1(Z,Y)\cdot \mathbf{q_1}(Z,\mathbf{Z},\mathbf{Y}) + \cdots + \mathbf{t'_{n+1}}(Z,\mathbf{Z},Y) = \mathbf{0}.$$

Elimination of quantifiers can be done on either sort first. It is understood that, in order to have a complete and easy quantifier elimination, all the conditions of the theorems developed for the former cases must be verified. This means that efficient quantifier elimination is possible for non trivial torsion-free modules over infinite integral domains.

Using distributivity, reorder formula (5.21) by collecting the vector variables $\mathbf{y_1},\ldots,\mathbf{y_r} \in \mathbf{Y}$:

$$\forall Y\ \forall \mathbf{Y}\ p_1(Z,Y)\cdot \mathbf{y}_1 + \ldots + p_r(Z,Y)\cdot \mathbf{y}_r + \mathbf{p_{r+1}}(Z,\mathbf{Z},Y) = \mathbf{0}. \tag{5.35}$$

Then, if the module is non trivial and torsion-free, by Theorem 5.2, the formula (5.35) is equivalent to the conjunction of equations:

$$(\forall Y)\ p_1(Z,Y) = 0 \wedge \ldots \wedge p_r(Z,Y) = 0 \wedge \mathbf{p}_{r+1}(Z,\mathbf{Z},Y) = \mathbf{0}. \tag{5.36}$$

Distribution of the universal quantifier over the conjunction yields:

$$\forall Y\ p_1(Z,Y) = 0 \wedge \ldots \wedge \forall Y\ p_r(Z,Y) = 0 \wedge (\forall Y)\ \mathbf{p_{r+1}}(Z,\mathbf{Z},Y) = \mathbf{0}. \tag{5.37}$$

Then, in order to eliminate the universal quantifiers on the scalar variables Y, observe that the terms $p_1(Z,Y),\ldots,p_r(Z,Y)$ are polynomials in $(D[Z])[Y]$:

$$\bigwedge_{1\le i\le r} (\forall Y) \sum_{j=1}^{k_i} \alpha_{i,j}(Z) Y_{i,j} = 0. \tag{5.38}$$

where $\alpha_{i,j}(Z) \in D[Z]$ are scalar terms. Instead, the term $\mathbf{p}_{r+1}(Z,\mathbf{Z},Y)$ is a vector term, and can be rewritten by collecting the scalar monomials:

$$\forall Y\ Y_{s,1}\cdot \mathbf{q'_{s,1}}(Z,\mathbf{Z}) + \ldots + \mathbf{q'_{s,k_s+1}}(Z,\mathbf{Z}) = \mathbf{0} \tag{5.39}$$

where $s = r+1$ and $\mathbf{q'_{s,1}}(Z),\ldots,\mathbf{q'_{s,k_s+1}}$ are vector terms. By Theorem 5.1, if the ring $\mathfrak{D}$ is an infinite integral domain, elimination of the quantifiers gives the equivalent formula:

$$\bigwedge_{1\le i\le r}\ \bigwedge_{1\le j\le k_i} \alpha_{i,j}(Z) = 0\ \wedge \bigwedge_{1\le j\le k_s+1} \mathbf{q'}_{s,j}(Z,\mathbf{Z}) = \mathbf{0}. \tag{5.40}$$

Once the elimination of quantifier is done, the algorithm for pattern solving has to find a ground term solution for the associated system of equations. This is the topic of next Section, solving systems of equations in non trivial torsion-free modules over an infinite integral domain.

5.4 Symbolic Constraint Solving in Modules over a Ring

This section deals with the final step of the pattern solving algorithm *SolPatC*, in Figure 3.4 on page 43, that takes into account the presence of constants defined by a set of equations. Recall the system Ψ of equations (5.6):

$$\{\epsilon_{i,1}\cdot \mathbf{a}_1 + \epsilon_{i,2}\cdot \mathbf{a}_2 + \ldots + \epsilon_{i,n}\cdot \mathbf{a}_n = \mathbf{0} \mid \epsilon_{i,j} \in R, 1 \le i \le h, 1 \le j \le n\}$$

The problem is finding a ground term solution of a system of equations associated to the quantifier-free formula obtained from the elimination of the universal quantifiers. In torsion-free modules of an infinite integral domain, there are two types of systems of equations. Problems of scalar type yield a system of vector equations to be solved. The system associated to formula (5.32) is:

$$\{\mathbf{q_i}(Z) = \mathbf{0} \mid \mathbf{1} \leq \mathbf{i} \leq \mathbf{k}+\mathbf{1}\}, \tag{5.41}$$

in free scalar variables $Z = \{z_1, \ldots, z_r\}$. Problems of vector and of mixed type yield a mixed system of scalar and vector equations to be solved. The system associated to formula (5.34) is:

$$\{p_i(Z) = 0 \mid 1 \leq i \leq r\} \cup \{\mathbf{p_{r+1}}(Z, \mathbf{Z}) = \mathbf{0}\}. \tag{5.42}$$

The system associated to formula (5.40) is:

$$\{\alpha_{i,j}(Z) = 0 \mid 1 \leq i \leq r, 1 \leq j \leq k_i\} \cup \{\mathbf{q'_{s,j}}(Z, \mathbf{Z}) = \mathbf{0} \mid 1 \leq j \leq k_s + 1\}. \tag{5.43}$$

The free variables are scalar and vector variables, $Z, \mathbf{Z}$. All equations in these systems are among terms in the signature Σ' obtained from Σ by adding the vector constants $\mathbf{a} = \{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$.

Before entering the details of the solving procedure, consider the expansion of the generating equations Ψ:

$$\begin{array}{ll}
\epsilon_{1,1} \cdot \mathbf{a}_1 + \epsilon_{1,2} \cdot \mathbf{a}_2 + \ldots + \epsilon_{1,n} \cdot \mathbf{a}_n & = \mathbf{0} \\
\epsilon_{2,1} \cdot \mathbf{a}_1 + \epsilon_{2,2} \cdot \mathbf{a}_2 + \ldots + \epsilon_{2,n} \cdot \mathbf{a}_n & = \mathbf{0} \\
\vdots & \vdots \\
\epsilon_{h,1} \cdot \mathbf{a}_1 + \epsilon_{h,2} \cdot \mathbf{a}_2 + \ldots + \epsilon_{h,n} \cdot \mathbf{a}_n & = \mathbf{0}
\end{array}$$

or equivalently in matrix notation:

$$E\mathbf{a} = \mathbf{0}.$$

where E is an $h \times n$ matrix with entries $\epsilon_{i,j} \in R$. Without loss of generality, it may be assumed that the rows of matrix E, say $E_1, \ldots, E_h$, are linearly independent. If they are not, it is enough to transform the matrix in an equivalent "almost row-reduced matrix" by doing row operations:

1. multiply one row by a nonzero scalar of R,
2. replace the i^{th} row by the sum of row i and row j multiplied by a nonzero scalar,
3. interchange row i and row j.

Recall that the entries of matrix E range over an infinite integral domain, hence all row operations are well defined.

DEFINITION 5.3
An $m \times n$ matrix A over a field is called row-reduced iff:

(a) *the first nonzero entry in each nonzero row of A is equal to* 1

(b) *each column of R which contains the leading nonzero entry of some row has all its other entries equal to* 0.

The concept of "row-reduced" matrix is defined for matrices with entries in a field, it does not apply to matrices with entries in a commutative ring. An "almost row-reduced matrix" is a matrix in which condition $5.3-(b)$ can be ensured, while nothing can be said about condition $5.3-(a)$.

Observe also that E can be assumed to have less rows than columns, namely $h < n$. If not, either the system of equations is never true or, if the E is square and non-singular, then the constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$ would all be equal to $\mathbf{0}$.

In the following it is shown how to tackle the problem of finding a solution γ for a system (5.41) such that:

$$\mathfrak{M} \models \bigwedge_{1\leq i\leq h, 1\leq j\leq n} \epsilon_{i,1}\cdot \mathbf{a}_1 + \epsilon_{i,2}\cdot \mathbf{a}_2 + \ldots + \epsilon_{i,n}\cdot \mathbf{a}_n = \mathbf{0} \rightarrow \bigwedge_{1\leq i\leq k+1} \mathbf{q_i}(Z)\gamma = \mathbf{0}. \tag{5.44}$$

when $\mathfrak{M}$ is a torsion-free module over $\mathbb{Z}$. Consider the expansion of the system of vector equations:

$$\begin{array}{ll}
q_{1,1}(Z)\cdot \mathbf{a}_1 + q_{1,2}(Z)\cdot \mathbf{a}_2 + \ldots + q_{1,n}(Z)\cdot \mathbf{a}_n & = \mathbf{0} \\
q_{2,1}(Z)\cdot \mathbf{a}_1 + q_{2,2}(Z)\cdot \mathbf{a}_2 + \ldots + q_{2,n}(Z)\cdot \mathbf{a}_n & = \mathbf{0} \\
\vdots & \vdots \\
q_{k,1}(Z)\cdot \mathbf{a}_1 + q_{k,2}(Z)\cdot \mathbf{a}_2 + \ldots + q_{k,n}(Z)\cdot \mathbf{a}_n & = \mathbf{0}
\end{array}$$

and more compactly, for the $k \times n$ matrix Q with entries $q_{i,j} \in R[Z]$:

$$Q\mathbf{a} = \mathbf{0}.$$

The integer solutions for the unknown scalar coefficients Z must be such that $Q\mathbf{a} = \mathbf{0}$ is a consequence of $E\mathbf{a} = \mathbf{0}$. This is equivalent to saying that each row $Q_1, \ldots, Q_k$ of Q must be a linear combination of the rows $E_1, \ldots, E_h$ of E. In other words, $Q_1, \ldots, Q_k$ are in the span of $E_1, \ldots, E_h$. Hence, for some $w_{ij} \in R$:

$$Q_i = w_{i,1}E_1 + \ldots + w_{i,h}E_h, \qquad 1 \leq i \leq k \tag{5.45}$$

Inspection reveals that $Q_i \in (R[Z])^n$ and $E_1, \ldots, E_h \in (R)^n \subseteq (R[Z])^n$, where:

$$R[Z])^n = \underbrace{R[z_1, \ldots, z_r] \times \ldots \times R[z_1, \ldots, z_r]}_{\text{n times}}. \tag{5.46}$$

Observe that $(R[Z])^n$ is a module with the operations defined naturally. Thus, the system of equations can be solved in $R[Z]$. The goal is to find $w_{i,j} \in \mathbb{Z}$ such that the resulting system of scalar equations (5.45) has an integer solution for the variables Z. This is possible by considering a new system of scalar equations obtained by equating the components in in equation (5.45), $(1 \leq i \leq k)$:

$$\begin{array}{ll}
q_{i,1}(Z) & = w_{i,1}\epsilon_{1,1} + \ldots + w_{i,h}\epsilon_{h,1}, \\
\vdots & \vdots \\
q_{i,n}(Z) & = w_{i,1}\epsilon_{1,n} + \ldots + w_{i,h}\epsilon_{h,n}.
\end{array} \tag{5.47}$$

Equivalently:

$$\{q_{i,j}(Z) - \epsilon_{1,j}w_{i,1} - \ldots - \epsilon_{h,j}w_{i,h} = 0 \mid 1 \leq i \leq k,\ 1 \leq j \leq n\} \tag{5.48}$$

This is, in general, a nonlinear system of polynomial equations in $\mathbb{Z}[Z, w_{1,1}, \ldots, w_{k,h}]$, where $w_{i,j}$ are treated as new variables. Nonlinearity is due to the scalar polynomial terms $q_{i,j}(Z)$.

The method of Gröbner basis can be employed in the same fashion as done previously in Section 4.4 for incrementally finding integer solutions. Begin by solving the system (5.47) for $i = 1$. Since $h < n$, it is possible that for each fixed i, the system of equations (5.47) is zero dimensional. In such a case, it is easy to check if there are integer solutions for the variables Z and for the coefficients of the linear combination $w_{i,1}, \ldots, w_{i,h}$. If such a solution exists, then the values for the variables Z can be substituted in the systems (5.47) obtained for the remaining values of i. Notice that the total degree of all these systems is lower and eventually will become linear. Each system must be solved in the same fashion as the first one. As soon as one system is not solvable, the process begins again by choosing another integer solution, if it exists, from the first system ($i = 1$) and so on.

The other type of constraint solving problem generated by the elimination of quantifiers contains a system of vector equations like:

$$p_1(Z) \cdot \mathbf{a_1} + \ldots + p_n(Z) \cdot \mathbf{a_n} = q_1(Z) \cdot \mathbf{z_1} + \ldots + q_m(Z) \cdot \mathbf{z_m} \tag{5.49}$$

where $\mathbf{z_1}, \ldots, \mathbf{z_m} \in \mathbf{Z}$ are vector variables, Z are scalar variables and $p_1(Z), \ldots, p_n(Z)$, $q_1(Z), \ldots, q_m(Z)$ are polynomials with integer coefficients. A solution γ for the vector variables is an assignment of a $\mathbb{Z}$-linear combination of constants $\mathbf{a_1}, \ldots, \mathbf{a_n}$ and for the scalar variables Z is an assignment of integers. Again, the solution must verify a condition similar to (5.44). There seems to be no general method for solving this problem. Observe that if no vector coefficients are specified, then the problem reduces to the same problem described above.

5.5 *Examples*

EXAMPLE 5.1
Consider a simple example of pattern solving problem in the presence of new constants, $\mathbf{a_1}, \mathbf{a_2}$ satisfying the equation:

$$\Psi = \{\mathbf{a_1} + \mathbf{a_2} = \mathbf{0}\}.$$

Let the input equation be:

$$\Gamma = \{(x_1 + x_2) \cdot \mathbf{a_1} + (x_1^2 + x_2 + x_1) \cdot \mathbf{a_2} = \mathbf{0}.\}$$

Moreover, let the solution pattern be of the form:

$$\begin{aligned} x_1 &= z_1 y \\ x_2 &= y + z_2 \end{aligned}$$

This is a problem of scalar type in which y is the only parameter and z_1, z_2 are the unknown coefficients.

After substitution, the universally quantified problem formula is:

$$\forall y\ (z_1 y + y + c_2) \cdot \mathbf{a_1} + (z_1^2 y^2 + y + z_2 + z_1 y) \cdot \mathbf{a_2} = \mathbf{0}$$

which is rewritten as:

$$\forall y\ y^2 \cdot (z_1^2 \cdot \mathbf{a_2}) + y \cdot (z_1 \cdot \mathbf{a_1} + z_1 \cdot \mathbf{a_2} + \mathbf{a_1} + \mathbf{a_2}) + (z_2 \cdot \mathbf{a_1} + z_2 \cdot \mathbf{a_2}) = \mathbf{0}.$$

Elimination of the quantifier according to Theorem 5.1 yields the conjunction:

$$z_1^2 \cdot \mathbf{a_2} = \mathbf{0} \wedge (z_1 + 1) \cdot \mathbf{a_1} + (z_1 + 1) \cdot \mathbf{a_2} = \mathbf{0} \wedge z_2 \cdot \mathbf{a_1} + z_2 \cdot \mathbf{a_2} = \mathbf{0}.$$

Thus, the associated system of vector equations to be solved is:

$$\{z_1^2 \cdot \mathbf{a_2} = \mathbf{0}, z_1 + 1) \cdot \mathbf{a_1} + (z_1 + 1) \cdot \mathbf{a_2} = \mathbf{0}, z_2 \cdot \mathbf{a_1} + z_2 \cdot \mathbf{a_2} = \mathbf{0}\}.$$

Now this is a lucky case since one equation, namely $z_1^2 \cdot \mathbf{a_2} = \mathbf{0}$, can be easily solved by torsion freeness. Since $\mathbf{a_2} \neq \mathbf{0}$, it must be

$$z_1 = 0.$$

Propagating this result in the system of equations yields the identity $\mathbf{a_1} + \mathbf{a_2} = \mathbf{0}$ and the equation:

$$z_2 \cdot \mathbf{a_1} + z_2 \cdot \mathbf{a_2} = \mathbf{0}$$

to be solved for z_2. This equation must be a scalar multiple of the equation in Ψ, hence there must exist a $w \in \mathbb{Z}$ such that:

$$z_2 = w$$

This is clearly true for an any arbitrary value of w. Hence, in this simple example there is an infinite number of instances of the pattern that turn it into a solution for the problem Γ.

5.6 Summary

This chapter developed symbolic pattern solving in modules over rings in a two-sorted signature. It has been shown that non trivial torsion-free modules over an infinite integral domain admit fast elimination of the universal quantifiers in problem formulas. This takes care of the first step of the algorithm for pattern solving in modules over a ring. The second step is one of solving a system of equations associated to the quantifier free formulas. It has been shown that for the case of equations containing only scalar variables, this can be done by using known computational methods. The more general case of equations containing also vector variables needs more investigation.

The next chapter deals with associative algebras. Nonlinearity will appear for vectors, while until now far they have behaved linearly. A new multiplication operation is available among vectors and the ring is a field, hence also division is available among scalars.

6

Pattern Solving in Commutative Algebras

Associative algebras are one natural generalization of R-modules obtained when the ring $\mathfrak{R}$ is a field and another vector operation is defined. The new operation is multiplication of vectors and the algebra is both a vector space and a ring. It is not a surprise that, as a consequence of the results shown in the former chapters, the pattern solving algorithm applies to algebras.

For the first time in this thesis, a modification of the problem formula is considered. More precisely, an algebra problem formula is, in general, a conjunction of equations and negated equations, also called "inequations". The inequations are obtained from the simplification of the scalar denominators. Since for some fields it is not possible to check the validity of inequations, think of the field of rationals, the presence of inequations is a serious limitation. One way to avoid this difficulty is to allow only input problems not containing any free variable or any parameter in a denominator.

It will be shown that algebras that are infinite integral domains over an infinite field admit fast elimination of universal quantifiers in problem formulas. For finite dimensional algebras, this is the class of division algebras over an infinite field.

The chapter is organized as the former chapters. The algebraic preliminary notions are briefly presented in Section 6.1. The detailed description of pattern solving in algebras over a field is given in Section 6.2. Section 6.3 deals with the fast elimination of universal quantifiers in problem formulas. Finding ground term solutions to the systems of equations associated to the quantifier free formulas is addressed in the last section, Section 6.4.

6.1 Algebraic Preliminaries

Let $\mathfrak{F}$ be a field for the signature $\Sigma_F = \langle 0, 1, -, ^{-1}, +, * \rangle$ axiomatized by axioms (6.2) on page 76. In most books, by "associative algebra" is intended a vector space $\mathfrak{A}$ over $\mathfrak{F}$ in the signature $\langle \mathbf{0}, \boldsymbol{+}, \boldsymbol{-}, \cdot \rangle$, which is also a commutative ring for the signature $\langle \mathbf{0}, \mathbf{1}, \boldsymbol{+}, \boldsymbol{-}, \boldsymbol{*} \rangle$. As for modules, the elements of the field are called "scalars" and the elements of the vector space called "vectors". In a two-sorted signature there are the respective sorts: scalar and vector. The operations $\langle \mathbf{0}, \boldsymbol{+}, \boldsymbol{-}, \cdot \rangle$ are specified as in modules, recall (5.1) on page 58. Additionally, multiplication of vectors is available and multiplicative unit:

$$\begin{array}{llll} \mathbf{1} : & \to \mathsf{vector} & \text{(one)} & \\ \boldsymbol{*} : \mathsf{vector} \times \mathsf{vector} & \to \mathsf{vector} & \text{(multiplication)} & (6.1) \end{array}$$

To obtain the axiomatization of algebras, the following axioms for multiplication of vectors must be added to the axioms (5.2) of modules. Using the same notational conventions, let

$\mathbf{u}, \mathbf{v}, \mathbf{w}$ be variables of sort vector and x, y be variables of sort scalar.

$$\begin{aligned} &\forall\mathbf{u}\forall\mathbf{v}\forall x\ x \cdot (\mathbf{u} * \mathbf{v}) = (x \cdot \mathbf{u}) * \mathbf{v} \\ &\forall\mathbf{u}\forall\mathbf{v}\forall\mathbf{w}\ (\mathbf{u} * \mathbf{v}) * \mathbf{w} = \mathbf{u} * (\mathbf{v} * \mathbf{w}) \\ &\forall\mathbf{u}\forall\mathbf{v}\ \mathbf{u} * \mathbf{v} = \mathbf{v} * \mathbf{u} \\ &\forall\mathbf{u}\ \mathbf{u} * \mathbf{1} = \mathbf{u} \\ &\forall\mathbf{u}\forall\mathbf{v}\forall\mathbf{w}\ (\mathbf{u} + \mathbf{v}) * \mathbf{w} = (\mathbf{u} * \mathbf{v}) + (\mathbf{u} * \mathbf{w}) \end{aligned} \tag{6.2}$$

Depending on the dimension of the vector space $\mathfrak{A}$, the algebra is finite or infinite dimensional. The ring $F[X]$ of formal polynomials in variables X with coefficients in F is an example of infinite dimensional associative commutative algebra over the field F. All rings are examples of $\mathbb{Z}$-algebras, therefore the theory of rings is a special case of that of algebras. In rest of the chapter, by "algebra" will be intended an associative and commutative algebra.

Because of the multiplicative unit, it is possible to define a homomorphism $h : \mathfrak{F} \to \mathfrak{R}$, by $h(x) = x \cdot \mathbf{1}$. It is easy to see that h is a homomorphism of rings. In fact, the addition $\boldsymbol{+}$ extends the scalar addition $+$:

$$\begin{aligned} h(x+y) &= (x+y) \cdot \mathbf{1} \\ &= (x \cdot \mathbf{1}) \boldsymbol{+} (y \cdot \mathbf{1}) \\ &= h(x) \boldsymbol{+} h(y) \end{aligned}$$

likewise the multiplication $\boldsymbol{*}$ extends the scalar multiplication $*$:

$$\begin{aligned} h(x * y) &= (x * y) \cdot \mathbf{1} \\ &= x \cdot (y \cdot \mathbf{1}) \\ &= x \cdot (y \cdot (\mathbf{1} \boldsymbol{*} \mathbf{1})) \\ &= x \cdot (\mathbf{1} \boldsymbol{*} (y \cdot \mathbf{1})) \\ &= (x \cdot \mathbf{1}) \boldsymbol{*} (y \cdot \mathbf{1}) \\ &= h(x) \boldsymbol{*} h(y). \end{aligned}$$

The additive identity and the multiplicative units are mapped to the respective identity and unit of the vector ring. By the properties of ring homomorphisms, the following are well-known facts:

$$h(-x) = \boldsymbol{-}\, h(x) \qquad h(0) = \mathbf{0}$$

$$h(x) = h(x * 1) = h(x) \boldsymbol{*} h(1) \qquad \text{implies} \qquad h(1) = \mathbf{1}$$

Hence, since the homomorphic image of a ring is a ring, it follows that h is an embedding of $\mathfrak{F}$ in $\mathfrak{A}$ and $\mathfrak{F}$ can be considered a sub-ring of $\mathfrak{A}$. Observe that the ring multiplication $\boldsymbol{*}$ extends also the scalar product $\cdot$:

$$\begin{aligned} x \cdot \mathbf{u} &= x \cdot (\mathbf{1} \boldsymbol{*} \mathbf{u}) \\ &= (x \cdot \mathbf{1}) \boldsymbol{*} \mathbf{u} \\ &= h(x) \boldsymbol{*} \mathbf{u} \end{aligned}$$

Hence, all scalar and vector terms can be interpreted as elements of the ring $\mathfrak{A}$ by the embedding h.

It will be shown that the pattern solving algorithm can be applied to problems in algebras that are infinite integral domains. Recall that integral domain are rings with no nonzero zero divisors:

$$\forall \mathbf{u} \forall \mathbf{v}\ \mathbf{u} * \mathbf{v} = \mathbf{0} \rightarrow \mathbf{u} = \mathbf{0} \vee \mathbf{v} = \mathbf{0}.$$

The theory of algebras is universal. It is not equational because the field fragment is not.

One may think that since algebras are special rings, namely they have a field as a sub-ring, they are always domains. This is not true. There are indeed examples of algebras that are rings with zero-divisors. For instance, in the non-commutative algebra $M_n(F)$ of square $n \times n$ matrices with entries in a field F, all non invertible matrices are zero divisors. One other example, suggested by Dardano (1996), is the F-algebra $A = F^S$ of all functions from a set S, containing at least 2 elements, into a field F. Then A is a finitely dimensional (its dimension being equal to the cardinality of the set S) F-algebra when the operations of addition and multiplication are defined pointwise and F is identified with the constant functions. This algebra is not an integral domain, because it is possible to find a pair of non null functions whose products is the zero constant: it is enough to choose them such that one function is zero where the other is not.

F-algebras are often studied as rings having a field as a sub-ring of their center. Recall that the center of a ring is the set of elements that commute with the whole ring. A *division ring* is a ring $\mathfrak{R}$ in which each nonzero element has an inverse (is a unit). A commutative division ring is a field. A finite-dimensional F-algebra which is a division ring is called a *division algebra*. Any finite integral domain is a division ring. Any division ring is an integral domain.

Theorem 6.1 (Wedderburn)
Any finite division ring is commutative.

In other word, every finite integral domain is a field, namely a commutative division ring.

Every finite dimensional F-algebra without zero divisors is a division algebra (Cohn (1989), page 188). Hence, any finitely dimensional F-algebra which is an integral domain is a division algebra. In view of this result, the algorithm of pattern solving applies to finite dimensional division algebras. The following theorems recall some results on division algebras from the books of Jacobson (1974, 1980).

Finite dimensional algebras over a finite field $\mathfrak{F}$ are fields since they are finite division rings. A field $\mathfrak{F}$ is *algebraically closed* if every monic polynomial equation $x^n + a_1x^{n-1} + \ldots + a_n = 0$, $a_i \in F$ has a root in $\mathfrak{F}$. The most common example of algebraically closed field is the field of complex numbers $\mathbb{C}$.

Theorem 6.2
If $\mathfrak{F}$ is algebraically closed, then the only finite dimensional division algebra over $\mathfrak{F}$ is $\mathfrak{F}$ itself.

Therefore, the only finite dimensional division algebra over $\mathbb{C}$ is $\mathbb{C}$. The next theorem gives a useful characterization of real division algebras.

Theorem 6.3 (Froebenius)
The only finite dimensional division algebras over $\mathbb{R}$ are

$$(1)\ \mathbb{R}, \qquad (2)\ \mathbb{C}, \qquad (3)\ \mathbb{H}.$$

Thus, any $\mathbb{R}$-algebra that is a finite dimensional integral domain must be either the real numbers $\mathbb{R}$, or the complex numbers $\mathbb{C}$ or the hyper-complex numbers $\mathbb{H}$, since it must be a finite dimensional division algebra. The author has found no result concerning finite dimensional division algebras over $\mathbb{Q}$.

Things are more complicated for infinite dimensional algebras that are integral domains. In order to relax the dimensionality condition, is necessary to talk about *algebraic algebras* over a field $\mathfrak{F}$, algebras in which every element is algebraic over $\mathfrak{F}$. An element $a \in \mathfrak{A}$ is algebraic over $\mathfrak{F}$ if it satisfies a non trivial polynomial equation with coefficients in $\mathfrak{F}$. Then Froebenius theorem can be restated:

THEOREM 6.4 (FROEBENIUS)
The only algebraic division algebras over $\mathbb{R}$ are

$$(1)\quad \mathbb{R}, \qquad (2)\quad \mathbb{C}, \qquad (3)\quad \mathbb{H}.$$

THEOREM 6.5 (JACOBSON)
Any algebraic division algebra over a finite field F is commutative (and thus is a an algebraic field extension of F).

The interested reader may read the proofs and more about the structure theory of rings on Lam (1991); Jacobson (1974); Cohn (1989). When the ground field $\mathfrak{F}$ is $\mathbb{Q}$ instead of a finite field or a real closed field like $\mathbb{R}$, then there are many algebraic division algebras over it. Finitely dimensional algebraic division algebras over $\mathbb{Q}$ are classified by Albert, Hasse, Brauer, and Noether. but infinitely dimensional algebraic division algebras over $\mathbb{Q}$ are not yet completely classified.

Terms in the two-sorted signature $\Sigma = \langle 0, \mathbf{0}, 1, \mathbf{1}, -, ^{-1}, \boldsymbol{-}, +, \boldsymbol{+}, *, \boldsymbol{*} \rangle$ of an algebra $\mathfrak{A}$, are polynomials with coefficients in the scalar domain, interpretable as rational functions, and monomials consisting of vectors multiplied together, vector monomials. That is, an algebra Σ-term can be written as:

$$t_1 \cdot \mathbf{m_1} \boldsymbol{+} t_2 \cdot \mathbf{m_2} \boldsymbol{+} \ \ldots \ \boldsymbol{+} t_n \cdot \mathbf{m_n}$$

where $t_1, \ldots, t_n$ are scalar terms and $\mathbf{m_1}, \ldots, \mathbf{m_n}$ are vector monomials. An algebra Σ-equation is a formula:

$$t_1 \cdot \mathbf{m_1} \boldsymbol{+} t_2 \cdot \mathbf{m_2} \boldsymbol{+} \ \ldots \ \boldsymbol{+} t_n \cdot \mathbf{m_n} = \mathbf{0}. \tag{6.3}$$

In order to use the theorems on the elimination of quantifiers shown in the former chapter, it is necessary to be able to interpret a Σ-equations as a formula in the signature: $\Sigma = \langle 0, \mathbf{0}, 1, \mathbf{1}, -, \boldsymbol{-}, +, \boldsymbol{+}, *, \boldsymbol{*} \rangle$. This can be done by eliminating the denominators appearing in the scalar terms $t_1, \ldots, t_n$ and imposing the side condition stating that none of these denominator is zero. Therefore, equation (6.3) is equivalent to a conjunction:

$$t'_1 \cdot \mathbf{m_1} \boldsymbol{+} t'_2 \cdot \mathbf{m_2} \boldsymbol{+} \ \ldots \ \boldsymbol{+} t'_n \cdot \mathbf{m_n} = \mathbf{0} \ \wedge \ \Delta \neq 0, \tag{6.4}$$

where $t'_1, \ldots, t'_n$ are now scalar terms in the signature of rings $\Sigma_R = \langle 0, 1, -, +, * \rangle$ and Δ is a scalar term obtained as product of all the denominators appearing in equation (6.3), also in signature Σ_R.

6.2 Problem Description

Pattern solving in algebras is similar to pattern solving in R-modules that was described in the previous chapter. The major difference lies in the general form of the problem formula. In an algebra problem, it is a conjunction of equations and inequations. The inequations are a condition stating that the simplified scalar denominators are nonzero. This negative part of the problem formula can be postponed for verification until the last step of the algorithm. But for some fields, it is never possible to check the validity of this condition. Therefore, the way to avoid this difficulty, is to prevent it from arising by restricting the form of the input problem.

Pattern solving in an algebra can be reduced to pattern solving over the underlying field by considering the vector space representation of the problem and working on the coordinates. Although this is feasible for finite dimensional algebras, it often means to solve a larger system of equations, with all the drawbacks that it involves. The approach taken here avoids using the transformation to coordinate representation if the problem is given at a higher level of specification.

The next subsections will analyze each type of pattern solving problem according to the sort of the free variables in the input set of equations.

6.2.1 Pattern Solving of Scalar Variables

A pattern solving problem in an algebra is of type scalar if all variables appearing in the input system of equations are scalar variables. Given a system of equations:

$$\begin{aligned} h_{1,1}(X)\cdot\mathbf{m_{1,1}} + \ldots + h_{1,n}(X)\cdot\mathbf{m_{1,n}} &= \mathbf{0} \\ &\vdots \\ h_{m,1}(X)\cdot\mathbf{m_{m,1}} + \ldots + h_{m,n}(X)\cdot\mathbf{m_{m,n}} &= \mathbf{0} \end{aligned}$$

where $X = \{x_1, \ldots, x_l\}$ are scalar variables and $\mathbf{m_{1,1}}, \ldots, \mathbf{m_{m,n}}$ are ground vector terms (monomials of constants). The coefficients $h_{1,1}(X), \ldots, h_{m,n}(X)$ are scalar terms in signature Σ_F, hence they might contain denominators. Transform each equation to an equivalent Σ_R-formula in which all denominators are explicitly non vanishing:

$$\begin{aligned} t_{1,1}(X)\cdot\mathbf{m_{1,1}} + \ldots + t_{1,n}(X)\cdot\mathbf{m_{1,n}} = \mathbf{0},\ &\Delta_1(X)\neq 0 \\ \vdots\quad &\vdots \\ t_{m,1}(X)\cdot\mathbf{m_{m,1}} + \ldots + t_{m,n}(X)\cdot\mathbf{m_{m,n}} = \mathbf{0},\ &\Delta_n(X)\neq 0 \end{aligned}$$

and let Γ be the system of equations:

$$\begin{aligned} t_{1,1}(X)\cdot\mathbf{m_{1,1}} + \ldots + t_{1,n}(X)\cdot\mathbf{m_{1,n}} &= \mathbf{0}, \\ &\vdots \\ t_{m,1}(X)\cdot\mathbf{m_{m,1}} + \ldots + t_{m,n}(X)\cdot\mathbf{m_{m,n}} &= \mathbf{0}, \end{aligned} \tag{6.5}$$

where $t_{1,1}(X), \ldots, t_{m,n}(X)$ are Σ_R-terms. The side condition: $\Delta_1(X)\neq 0, \ldots, \Delta_n(X)\neq 0$ is equivalent to a single inequation:

$$\Delta(X)\neq 0 \tag{6.6}$$

where $\Delta_1(X) * \ldots * \Delta_n(X) = \Delta(X)$. A solution pattern for a scalar problem is an assignment of scalar terms:

$$\begin{array}{rcl} x_1 & = & p_1(Z,Y) \\ \vdots & \vdots & \vdots \\ x_l & = & p_l(Z,Y) \end{array} \tag{6.7}$$

where $p_1(Z,Y), \ldots, p_l(Z,Y)$ are scalar terms in unknown coefficients Z and parameters Y. There appear no vector variable in the solution. Observe that $p_1(Z,Y), \ldots, p_l(Z,Y)$ can be assumed to be Σ_R-terms if, again, a side condition states that the denominators are nonzero:

$$\Lambda(Z,Y) \neq 0$$

The problem formula $\psi(Z,Y)$ is a conjunction of equations and inequations:

$$\begin{array}{l} \forall Y \bigwedge_{1 \leq i \leq m} t'_{i,1}(Z,Y) \cdot \mathbf{m_{i,1}} + \ldots + t'_{i,n}(Z,Y) \cdot \mathbf{m_{i,n}} = \mathbf{0} \wedge \\ \qquad \Delta'(Z,Y) \neq 0 \wedge \Lambda(Z,Y) \neq 0, \end{array} \tag{6.8}$$

for the appropriate $t'_{i,1}(Z,Y), \ldots, t'_{i,n}(Z,Y)$ scalar Σ_R-terms. The condition $\Delta'(Z,Y)$ is obtained by substituting the variables X according to the solution pattern π. Since the problem formula is a conjunction, it is possible to deal with each conjunct separately. Therefore, consider the positive conjunction:

$$\forall Y \bigwedge_{1 \leq i \leq m} t'_{i,1}(Z,Y) \cdot \mathbf{m_{i,1}} + \ldots + t'_{i,n}(Z,Y) \cdot \mathbf{m_{i,n}} = \mathbf{0} \tag{6.9}$$

and the conditions:

$$\forall Y \; \Delta'(Z,Y) \neq 0 \wedge \Lambda(Z,Y) \neq 0. \tag{6.10}$$

It is easy to see that when Z are instantiated in formula (6.10), the result is a conjunction of inequations that can be interpreted as polynomials in variables Y with coefficients in F. This conjunction is false if the resulting polynomials have at least a root in $\mathfrak{F}$. For instance, if the field $\mathfrak{F}$ is algebraically closed then all equations have a solution in $\mathfrak{F}$, thus the inequations are always false. If the field $\mathfrak{F}$ is the field of rational numbers, then the condition cannot be checked in general. If $\mathfrak{F}$ is a real closed field, then Sturm's Theorem gives a criteria to check the existence of solutions (see Jacobson, 1974, pag. 298). Condition (6.10) becomes easy to check if no parameter Y occurs in it and the algorithm returns a ground term solution for the unknown coefficients Z. This last case amounts to when the input problem (6.5) and the solution pattern (6.7) do not contain any variable X and any parameter Y in a denominator.

Back to formula (6.9), using the axioms of distributivity, it can be reordered by collecting the monomials $Y_{1,i}, \ldots, Y_{i,h}$ containing the parameters Y:

$$\forall Y \bigwedge_{1 \leq i \leq m} Y_{i,1} \cdot \mathbf{u_{i,1}}(Z) + \cdots + Y_{i,h} \cdot \mathbf{u_{i,h}}(Z) + \mathbf{u_{i,h+1}}(Z) = \mathbf{0} \tag{6.11}$$

where each $\mathbf{u_{i,j}}(Z)$, $(1 \leq i \leq m, 1 \leq j \leq h+1)$ is a vector term in free scalar variables Z. The formula (6.11) can be written in a unique way provided that, for $(1 \leq i \leq m)$, the monomials $Y_{i,1}, \ldots, Y_{i,h}$ are pairwise disjoint and ordered according to some fixed ordering.

To simplify notation, quantifier elimination will be studied on a single equation:

$$\forall Y\; Y_1 \cdot \mathbf{u_1}(Z) + \cdots + Y_h \cdot \mathbf{u_h}(Z) + \mathbf{u_{h+1}}(Z) = \mathbf{0} \tag{6.12}$$

The results can then be applied to a finite conjunction in a straightforward fashion. The reader wishing to directly read about elimination of quantifiers from formula (6.12) may skip to Section 6.3.1. In the next Section the pattern solving problem of type vector in algebras is described.

6.2.2 Pattern Solving of Vector Variables

A pattern solving problem in a two-sorted algebra is of type vector if the free variables in the input equations are of sort vector only. Then, the input problem Γ can be written as a system of equations of the form:

$$\begin{aligned} \mathbf{t_{1,1}} * \mathbf{X_{1,1}} + \ldots + \mathbf{t_{1,k}} * \mathbf{X_{1,k_1}} + \mathbf{t_{1,k_1+1}} &= \mathbf{0} \\ &\vdots \quad \vdots \\ \mathbf{t_{r,1}} * \mathbf{X_{r,1}} + \ldots + \mathbf{t_{r,k_r}} * \mathbf{X_{r,k_r}} + \mathbf{t_{r,k_r+1}} &= \mathbf{0} \end{aligned} \tag{6.13}$$

where $\mathbf{X_{i,j}} \in [\mathbf{x_1}, \ldots, \mathbf{x_n}]$ are monomials of vector variables $\mathbf{X}$ and the $\mathbf{t_{i,j}}$'s are ground vector terms that, without loss of generality, may be assumed to have no denominators. Note that there is no need of side conditions since the only denominators that can appear are ground scalar terms that are easy to multiply out.

It is enough to study solution patterns in which may appear unknown scalar coefficients, Z, unknown vector coefficients, $\mathbf{Z}$ and vector parameters $\mathbf{Y}$. There appear no scalar parameters. Hence, the solution pattern π is an assignment of vector terms in a two sorted language of the form:

$$\begin{aligned} \mathbf{x_1} &= \mathbf{h_1}(Z, \mathbf{Z}, \mathbf{Y}) \\ \vdots \;&\;\vdots\; \;\vdots \\ \mathbf{x_n} &= \mathbf{h_n}(Z, \mathbf{Z}, \mathbf{Y}) \end{aligned} \tag{6.14}$$

where the vector terms $\mathbf{h_i}(Z, \mathbf{Z}, \mathbf{Y})$ might possibly contain scalar denominators in unknown coefficients Z. In order to assume without loss of generality that no denominators are present, it is necessary to introduce a side condition about the denominators, just as was done in the pattern solving problem of type scalar. Hence, assume that the scalar subterms in (6.14) are Σ_R-terms and let:

$$\Lambda(Z) \neq 0 \tag{6.15}$$

be the condition on the denominators.

After substitution of the solution pattern π in the input equations Γ and in condition (6.15), the problem formula $\psi(Z, \mathbf{Z}, \mathbf{Y})$ can be rewritten by collecting the monomials $\mathbf{Y_{i,1}}, \ldots, \mathbf{Y_{i,h_i}}$, for $1 \leq i \leq r$, consisting of vector parameters $\mathbf{Y}$:

$$\forall \mathbf{Y} \bigwedge_{1 \leq i \leq r} \mathbf{p_{i,1}}(Z, \mathbf{Z}) * \mathbf{Y_{i,1}} + \ldots + \mathbf{p_{i,h_i}}(Z, \mathbf{Z}) * \mathbf{Y_{i,h_i}} + \mathbf{p_{i,h_i+1}}(Z, \mathbf{Z}) = \mathbf{0} \wedge \Lambda(Z) \neq 0. \tag{6.16}$$

for appropriate vector terms $\mathbf{p_{i,j}}(Z, \mathbf{Z})$. The condition on the denominators can be checked easily if some ground term substitution is found for the variables Z in the last step of the algorithm. Hence this part of the conjunction can be disregarded until the last step.

In order to study an efficient way to eliminate the quantifiers, it is enough to consider one equation only, hence:

$$\forall \mathbf{Y}\ \mathbf{p_1}(Z, \mathbf{Z}) * \mathbf{Y_1} + \ldots + \mathbf{p_h}(Z, \mathbf{Z}) * \mathbf{Y_h} + \mathbf{p_{h+1}}(Z, \mathbf{Z}) = \mathbf{0} \tag{6.17}$$

Elimination of quantifiers from formula (6.17) is discussed in Section 6.3.1. In the next Section, the more general type of pattern solving problem in algebras is described.

6.2.3 Pattern Solving of Scalar and Vector Variables

When the free variables in the input system of an algebra problem are both vector and scalar, the general form is a combination of the previous problems. Let Γ be:

$$\begin{aligned} \mathbf{t_{1,1}}(X) * \mathbf{X_{1,1}} + \ldots + \mathbf{t_{1,k_1}}(X) * \mathbf{X_{1,k_1}} + \mathbf{t_{1,k_1+1}}(X) &= \mathbf{0} \\ \vdots \quad & \vdots \\ \mathbf{t_{r,1}}(X) * \mathbf{X_{r,1}} + \ldots + \mathbf{t_{r,k_r}}(X) * \mathbf{X_{r,k_r}} + \mathbf{t_{r,k_r+1}}(X) &= \mathbf{0} \end{aligned} \tag{6.18}$$

where $\mathbf{X_{i,j}} \in [\mathbf{x_1}, \ldots, \mathbf{x_n}]$ are again monomials of vector variables $\mathbf{X}$, the $\mathbf{t_{i,j}}(X)$ are scalar terms with free scalar variables X for $1 \leq i \leq r, 1 \leq j \leq k_i + 1$. The scalar subterms eventually occurring in the equations (6.18) can be assumed to be Σ_R-terms if a side condition:

$$\Delta(X) \neq 0 \tag{6.19}$$

states that the simplified denominators are nonzero.

There are several types of solution patterns, depending on the occurrence of unknown coefficients of parameters of either sort. The most general type is the one in which there occur unknown scalar and vector coefficients, Z and $\mathbf{Z}$ rrespectively, and unknown vector coefficients, $\mathbf{Z}$ and both scalar and vector parameters, respectively Y and $\mathbf{Y}$. Hence, the solution pattern π is an assignment of vector terms for the variables $\mathbf{x_1}, \ldots, \mathbf{x_n} \in \mathbf{X}$ and of scalar terms for the variables $x_1, \ldots, x_l \in X$:

$$\begin{aligned} \mathbf{x_1} &= \mathbf{h_1}(Z, Y, \mathbf{Z}, \mathbf{Y}) \\ \vdots \quad & \vdots \quad \vdots \\ \mathbf{x_n} &= \mathbf{h_n}(Z, Y, \mathbf{Z}, \mathbf{Y}) \\ x_1 &= h_1(Z, Y) \\ \vdots \quad & \vdots \quad \vdots \\ x_l &= h_l(Z, Y) \end{aligned} \tag{6.20}$$

The vector terms $\mathbf{h_1}(Z, Y, \mathbf{Z}, \mathbf{Y})$, $\ldots$, $\mathbf{h_n}(Z, Y, \mathbf{Z}, \mathbf{Y})$, and the scalar terms $h_1(Z, Y)$, $\ldots$, $h_l(Z, Y)$ can be assumed to contain only scalar Σ_R-subterms if a condition is provided, say:

$$\Lambda(Z, Y) \neq 0. \tag{6.21}$$

Condition (6.21) ensures that the denominators are nonzero.

The reader is by now accustomed to the process of substituting the solution pattern into the input problem and then reordering the resulting problem formula according to some criteria, mostly by collecting the parameters for which the universal quantifier has to be eliminated. The same thing is done on the problem formula obtained for this type of problem in associative algebras over a field. The result is a problem formula $\psi(Z, Y, \mathbf{Z}, \mathbf{Y})$:

$$\begin{aligned}\forall Y\ (\forall \mathbf{Y})\ & \bigwedge_{1\leq i\leq r} \mathbf{p_{i,1}}(Z,\mathbf{Z},Y) * \mathbf{Y_{i,1}} + \ \ldots\ + \mathbf{p_{i,s_i}}(Z,\mathbf{Z},Y) * \mathbf{Y_{i,s}} + \mathbf{p_{i,s_i+1}}(Z,\mathbf{Z},Y) = \mathbf{0}\\ & \wedge \Delta(Z,Y) \neq 0 \wedge \Lambda(Z,Y) \neq 0.\end{aligned}$$

For this formula, the same considerations done for problem formula (6.8) in the scalar case hold. Since the problem formula is a conjunction, it is possible to consider separately:

$$\forall Y\ \forall \mathbf{Y}\ \bigwedge_{1\leq i\leq r} \mathbf{p_{i,1}}(Z,\mathbf{Z},Y) * \mathbf{Y_{i,1}} + \ \ldots\ + \mathbf{p_{i,s_i}}(Z,\mathbf{Z},Y) * \mathbf{Y_{i,s}} + \mathbf{p_{i,s_i+1}}(Z,\mathbf{Z},Y) = \mathbf{0}, \tag{6.22}$$

and the condition consisting of inequations:

$$\forall Y\ \forall \mathbf{Y}\ \wedge \Delta(Z,Y) \neq 0 \wedge \Lambda(Z,Y) \neq 0. \tag{6.23}$$

The next section will deal with elimination of quantifiers for algebras.

6.3 Quantifier Elimination

Elimination of universal quantifiers for pattern solving in algebras can be shown by using the results of rings and of modules over rings. The more general type of pattern solving problem requires, for fast elimination of quantifiers, that the algebra is an infinite integral domain over an infinite field.

Results on the elimination of quantifiers for rings, and in particular for division rings can be found in the papers by Rose (1978) and by Berline (1981). Recall that a prime ring is a ring in which the following axiom is true:

$$\forall x \forall y \exists z x = 0 \vee y = 0 \vee xzy \neq 0.$$

The prime ring is also the sub-ring generated by the unit. Since division rings are prime rings, the following theorem applies to division algebras.

Theorem 6.6 (Rose)
If $\mathfrak{R}$ is a prime ring with an infinite center and $\mathfrak{R}$ admits elimination of quantifiers, then $\mathfrak{R}$ is an algebraically closed field.

Let $\mathfrak{D}$ be a division ring. Then $\mathfrak{D}$ admits elimination of quantifiers if and only if $\mathfrak{D}$ is a finite or algebraically closed field.

In this section, again three types of elimination will be studied. In all three cases, the straightforward solution of the quantifier elimination is incomplete when no conditions are imposed on the algebra. From pattern solving problems of type scalar, the problem formula $\psi(Z, Y)$ is of the form of (6.12):

$$\forall Y\ Y_1 \cdot \mathbf{u_1} + \ \cdots\ + Y_h \cdot \mathbf{u_h} + \mathbf{u_{h+1}} = \mathbf{0} \tag{6.24}$$

where $Y_1, \ldots, Y_h \in [y_1, \ldots, y_l]$ are scalar monomials. The reader might compare this formula with the problem formula (5.22) of scalar problem in R-modules on page 63 and notice the similarity.

From pattern solving problems of type vector, the problem formula $\psi(Z, \mathbf{Z}, \mathbf{Y})$ is of the form of (6.17):

$$\forall \mathbf{Y}\ \mathbf{p_1} * \mathbf{Y_1} + \ldots + \mathbf{p_h} * \mathbf{Y_h} + \mathbf{p_{h+1}} = \mathbf{0} \tag{6.25}$$

where $\mathbf{Y_1}, \ldots, \mathbf{Y_h} \in [\mathbf{y_1}, \ldots, \mathbf{y_n}]$ are vector monomials.

The more general type of problem formulas generated by pattern solving in algebras is formula (6.22):

$$\forall Y\ \forall \mathbf{Y} \bigwedge_{1 \le i \le r} \mathbf{p_{i,1}}(Z, \mathbf{Z}, Y) * \mathbf{Y_{i,1}} + \ldots + \mathbf{p_{i,h_i}}(Z, \mathbf{Z}, Y) * \mathbf{Y_{i,h}} + \mathbf{p_{i,h_i+1}}(Z, \mathbf{Z}, Y) = \mathbf{0}.$$

The quantifiers can be eliminated from this formula by using the elimination techniques developed for the former cases of formulas (6.24)-(6.25).

6.3.1 Quantifier Elimination of Scalar Variables

The goal of this section is to eliminate the universal quantifier from the scalar parameters in problem formula (6.24). First, it is easy to reduce the formula by considering the assignment $\mathbf{y_1} = \ldots = \mathbf{y_l} = \mathbf{0}$. This implies that:

$$\mathbf{u_{h+1}} = \mathbf{0} \tag{6.26}$$

which substituted back in (6.24) yields

$$\forall Y\ Y_1 \cdot \mathbf{u_1} + \cdots + Y_n \cdot \mathbf{u_n} = \mathbf{0}. \tag{6.27}$$

The scalar monomials $Y_1, \ldots, Y_n \in F[X]$ are pairwise distinct and not constant.

A straightforward but usually incomplete solution is the usual:

$$\mathbf{u_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{u_1} = \mathbf{0} \rightarrow (\forall Y)\ Y_1 \cdot \mathbf{u_1} + \ldots + Y_n \cdot \mathbf{u_n} = \mathbf{0}.$$

Trivial quantifier elimination becomes complete when the underlying field is infinite.

THEOREM 6.7
Let $\mathfrak{F}$ be an infinite field and let $\mathfrak{A}$ be an associative commutative algebra over $\mathfrak{F}$. Let $Y_1, \ldots, Y_n \in F[Y]$ be pairwise disjoint and not constant monomials in scalar variables Y and let $\mathbf{u_1}, \ldots, \mathbf{u_n}$ be vector *terms non containing any variable Y. Then*

$$\mathfrak{A} \models \forall Y\ Y_1 \cdot \mathbf{u_1} + \ldots + Y_n \cdot \mathbf{u_n} = \mathbf{0} \leftrightarrow \mathbf{u_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{u_n} = \mathbf{0}.$$

PROOF. The proof is very similar to the proof of Theorem 5.1 for the elimination of quantifiers in R-modules. Hence, assume that $\mathfrak{F}$ is an infinite field, $\mathfrak{A}$ an algebra over $\mathfrak{F}$. One direction of the implication is trivially verified. The goal is to show the direction:

$$\mathfrak{A} \models \forall Y\ Y_1 \cdot \mathbf{u_1} + \ldots + Y_n \cdot \mathbf{u_n} = \mathbf{0} \rightarrow \mathbf{u_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{u_n} = \mathbf{0}.$$

Assume therefore that:

$$\mathfrak{A} \models (\forall Y)\, Y_1 \cdot \mathbf{u_1} + \ldots + Y_n \cdot \mathbf{u_n} = \mathbf{0}. \tag{6.28}$$

Since $\mathfrak{F}$ is an infinite integral domain, by Lemma 5.29, there exist at least n tuples of F^l, say $\alpha_1, \ldots, \alpha_n$, such that the matrix M:

$$\begin{bmatrix} Y_1^{\mathfrak{F}}(\alpha_1) & Y_2^{\mathfrak{F}}(\alpha_1) & \ldots & Y_n^{\mathfrak{F}}(\alpha_1) \\ Y_1^{\mathfrak{F}}(\alpha_2) & Y_2^{\mathfrak{F}}(\alpha_2) & \ldots & Y_n^{\mathfrak{F}}(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ Y_1^{\mathfrak{F}}(\alpha_n) & Y_2^{\mathfrak{F}}(\alpha_n) & \ldots & Y_n^{\mathfrak{F}}(\alpha_n) \end{bmatrix}$$

is has nonzero determinant $\mathrm{Det}(M) \neq 0$.

Since (6.28) holds for all assignments of the parameters Y, it must be true for all the n assignments $y_1 = \alpha_{j1}, \ldots, y_l = \alpha_{jl}$ $(1 \leq j \leq n)$. It follows that the system of equations:

$$\begin{array}{rcl} Y_1^{\mathfrak{F}}(\alpha_1) \cdot \mathbf{u_1} + Y_2^{\mathfrak{F}}(\alpha_1) \cdot \mathbf{u_2} + \ldots + Y_n^{\mathfrak{F}}(\alpha_1) \cdot \mathbf{u_n} & = & \mathbf{0} \\ Y_1^{\mathfrak{F}}(\alpha_2) \cdot \mathbf{u_1} + Y_2^{\mathfrak{F}}(\alpha_2) \cdot \mathbf{u_2} + \ldots + Y_n^{\mathfrak{F}}(\alpha_2) \cdot \mathbf{u_n} & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ Y_1^{\mathfrak{F}}(\alpha_n) \cdot \mathbf{u_1} + Y_2^{\mathfrak{F}}(\alpha_n) \cdot \mathbf{u_2} + \ldots + Y_n^{\mathfrak{F}}(\alpha_n) \cdot \mathbf{u_n} & = & \mathbf{0} \end{array}$$

is true in the algebra $\mathfrak{A}$. Using a matrix notation:

$$M\mathbf{u} = \mathbf{0},$$

where $\mathbf{u}$, $\mathbf{0}$ are vectors containing respectively $\mathbf{u_1}, \ldots, \mathbf{u_n}$ and $\mathbf{0}, \ldots, \mathbf{0}$. Then also the sum of any two equations is true and any scalar multiple of any equation is true. Therefore, it is possible to carry out all the row operations on matrix M until it becomes a diagonal matrix M' of rank n (since the determinant of M is nonzero):

$$M'\mathbf{u} \;=\; \mathbf{0}$$

This implies that also:

$$I\mathbf{u} \;=\; \mathbf{0},$$

where I is the identity matrix. Therefore:

$$\mathbf{u_1} = \mathbf{0} \wedge \mathbf{u_2} = \mathbf{0} \wedge \ldots \wedge \mathbf{u_n} = \mathbf{0}$$

as wanted. ∎

Recall the problem formula of type scalar (6.12):

$$\forall Y\; Y_1 \cdot \mathbf{u_1}(Z) + \cdots + Y_h \cdot \mathbf{u_h}(Z) + \mathbf{u_{h+1}}(Z) = \mathbf{0}. \tag{6.29}$$

When the underlying field $\mathfrak{F}$ is infinite, it is equivalent to the quantifier-free conjunction:

$$\mathbf{u_1}(Z) = \mathbf{0} \ \wedge \cdots \wedge \ \mathbf{u_h}(Z) = \mathbf{0} \ \wedge \ \mathbf{u_{h+1}}(Z) = \mathbf{0}. \tag{6.30}$$

Since this formula is a conjunction of equations in free scalar variables Z, the last step of the pattern solving algorithm is required to solve the corresponding system:

$$\{\mathbf{u_i}(Z) = \mathbf{0} \mid \mathbf{1} \leq \mathbf{i} \leq \mathbf{h} + \mathbf{1}\}. \tag{6.31}$$

Solving equations in algebras is the topic of Section 6.4.

6.3.2 Quantifier Elimination of Vector Variables

The second type of problem formula, formula (6.25) contains universally quantified vector parameters to be eliminated. Also this formula can be simplified by assigning the zero vector to all parameters $\mathbf{y_1} = \ldots = \mathbf{y_n} = \mathbf{0}$ and obtaining:

$$\mathbf{p_{h+1}} = \mathbf{0}. \tag{6.32}$$

Hence, by substituting it in the problem formula, it yields the new problem formula:

$$\forall \mathbf{Y} \ \mathbf{p_1} * \mathbf{Y_1} + \ \ldots \ + \mathbf{p_h} * \mathbf{Y_h} = \mathbf{0}, \tag{6.33}$$

where the vector monomials $\mathbf{Y_1}, \ldots, \mathbf{Y_h}$ are pairwise disjoint and not constant.

Theorem 6.8
Let $\mathfrak{A}$ be an associative commutative algebra that is an infinite integral domain. Let $\mathbf{p_1}, \ldots, \mathbf{p_h}$ be vector terms in the two-sorted language with signature Σ_A and let $\mathbf{Y_1}, \ldots, \mathbf{Y_h}$ be monomials in vector variables $\mathbf{Y}$. Then:

$$\forall \mathbf{Y} \ \mathbf{p_1} * \mathbf{Y_1} + \ \ldots \ + \mathbf{p_h} * \mathbf{Y_h} = \mathbf{0} \leftrightarrow \mathbf{p_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{p_h} = \mathbf{0}.$$

Proof. Let $\mathfrak{A}$ be an associative commutative algebra that is an infinite integral domain and let $\mathfrak{R} \subseteq \mathfrak{A}$ be the ring substructure for the signature $\langle \mathbf{0}, \mathbf{1}, \ +\ , \ -\ , \ *\ \rangle$. By assumption, the ring $\mathfrak{R}$ is an infinite integral domain. One direction of the implication is clear, namely:

$$\mathfrak{A} \ \models \forall \mathbf{Y} \ \mathbf{p_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{p_h} = \mathbf{0} \rightarrow \mathbf{p_1} * \mathbf{Y_1} + \ \ldots \ + \mathbf{p_h} * \mathbf{Y_h} = \mathbf{0}.$$

In order to show the other direction, assume:

$$\mathfrak{A} \models \forall \mathbf{Y} \ \mathbf{p_1} * \mathbf{Y_1} + \ \ldots \ + \mathbf{p_h} * \mathbf{Y_h} = \mathbf{0}. \tag{6.34}$$

The goal is to show that:

$$\mathfrak{A} \ \models \mathbf{p_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{p_n} = \mathbf{0}.$$

In order to apply Theorem 4.3 on page 53, the formula (6.34) must be a formula interpretable as a ring formula in the one-sorted signature $\langle \mathbf{0}, \mathbf{1}, \ +\ , \ -\ , \ *\ \rangle$. Recall that all scalar denominators appearing in the formula have been multiplied out, thus the scalar subterms appearing are terms in the signature Σ_R. Because of the embedding $h : \mathfrak{F} \hookrightarrow \mathfrak{R}$, each scalar term can be interpreted as a ring term in signature $\langle \mathbf{0}, \mathbf{1}, \ +\ , \ -\ , \ *\ \rangle$. When this is done, then also multiplication by a scalar coincides with the ring multiplication. Therefore:

$$\mathfrak{R} \models \forall \mathbf{Y} \ \mathbf{p_1} * \mathbf{Y_1} + \ \ldots \ + \mathbf{p_h} * \mathbf{Y_h} = \mathbf{0}. \tag{6.35}$$

Since $\mathfrak{R}$ is an infinite integral domain, by Theorem 4.3 it follows that:

$$\mathfrak{R} \models \mathbf{p_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{p_h} = \mathbf{0}. \tag{6.36}$$

Hence:

$$\mathfrak{A} \models \mathbf{p_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{p_n} = \mathbf{0}.$$

∎

Summarizing, it is possible to eliminate the universal quantifiers in the problem formula (6.17) of vector type:

$$\forall \mathbf{Y}\ \mathbf{p_1}(Z, \mathbf{Z}) * \mathbf{Y_1} + \ \ldots\ + \mathbf{p_h}(Z, \mathbf{Z}) * \mathbf{Y_h} + \mathbf{p_{h+1}}(Z, \mathbf{Z}) = \mathbf{0}$$

if the algebra $\mathfrak{A}$ is a infinite integral domain. Elimination of the quantifiers yields the conjunction:

$$\mathbf{p_1}(Z, \mathbf{Z}) = \mathbf{0} \wedge \ldots \wedge \mathbf{p_h}(Z, \mathbf{Z}) = \mathbf{0} \wedge \mathbf{p_{h+1}}(Z, \mathbf{Z}) = \mathbf{0} \tag{6.37}$$

that corresponds to the system of vector equations in scalar and vector variables $Z, \mathbf{Z}$:

$$\{\mathbf{p_i}(Z, \mathbf{Z}) = \mathbf{0} \mid \mathbf{1} \le \mathbf{i} \le \mathbf{h} + \mathbf{1}\}. \tag{6.38}$$

Solving this and other systems of equations in an algebra $\mathfrak{A}$ is the topic of Section 6.4. The last part of this section deals with elimination of universally quantified vector and scalar parameters from a problem formula of general type.

6.3.3 Quantifier Elimination of Scalar and Vector Variables

The more general formula in algebras is formula (6.22):

$$\forall Y\ \forall \mathbf{Y} \bigwedge_{1 \le i \le r} \mathbf{p_{i,1}}(Z, \mathbf{Z}, Y) * \mathbf{Y_{i,1}} + \ \ldots\ + \mathbf{p_{i,s_i}}(Z, \mathbf{Z}, Y) * \mathbf{Y_{i,s}} + \mathbf{p_{i,s_i+1}}(Z, \mathbf{Z}, Y) = \mathbf{0}.$$

The goal of this section is to show how to eliminate the universal quantifiers on both the scalar and the vector parameters by using the results shown in Theorem 6.7 and in Theorem 6.8. Hence, assume that the algebra $\mathfrak{A}$ is an infinite integral domain and the underlying field $\mathfrak{F}$ is also an infinite domain. By Theorem 6.8, formula (6.22) is equivalent to the conjunction:

$$\forall Y \bigwedge_{1 \le i \le r} \mathbf{p_{i,1}}(Z, \mathbf{Z}, Y) = \mathbf{0} \wedge \ldots \wedge \mathbf{p_{i,s_i}}(Z, \mathbf{Z}, Y) = \mathbf{0} \wedge \mathbf{p_{i,s_i+1}}(Z, \mathbf{Z}, Y) = \mathbf{0}.$$

In short:

$$\forall Y \bigwedge_{1 \le i \le r} \bigwedge_{1 \le j \le s_i + 1} \mathbf{p_{i,j}}(Z, \mathbf{Z}, Y) = \mathbf{0}, \tag{6.39}$$

for vector terms $\mathbf{p_{i,j}}(Z, \mathbf{Z}, Y)$. Each vector term $\mathbf{p_{i,j}}(Z, \mathbf{Z}, Y)$ can be written by collecting the scalar monomials:

$$\forall Y \bigwedge_{1 \le i \le r} \bigwedge_{1 \le j \le s_i + 1} Y_{1,i,j} \cdot \mathbf{u_{1,i,j}}(Z, \mathbf{Z}) + \ \cdots\ + \mathbf{u_{k_{i,j},i,j}}(Z, \mathbf{Z}) = \mathbf{0}, \tag{6.40}$$

and by Theorem 6.7:

$$\bigwedge_{1 \le i \le r} \bigwedge_{1 \le j \le h_i + 1} \mathbf{u_{1,i,j}}(Z, \mathbf{Z}) = \mathbf{0} \wedge \ldots \wedge \mathbf{u_{k_{i,j},i,j}}(Z, \mathbf{Z}) = \mathbf{0}. \tag{6.41}$$

To this last conjunction corresponds a system of vector equations containing both scalar and vector variables:

$$\{\mathbf{u_{i,j,h}}(Z, \mathbf{Z}) = \mathbf{0} \mid \mathbf{1} \le \mathbf{i} \le \mathbf{r}, \mathbf{1} \le \mathbf{j} \le \mathbf{s_i} + \mathbf{1}, \mathbf{1} \le \mathbf{h} \le \mathbf{k_{i,j}} + \mathbf{1}\}. \tag{6.42}$$

This system of equations is of the same form as the one obtained in the previous section, system (6.38). It must be solved for vector and scalar variables.

6.4 *Symbolic Constraint Solving in Algebras over a Field*

The last step in the algorithm *SolPat* on page 43 requires a ground term solution for the unknown coefficients. This amounts to solving a system of polynomial equations obtained from the problem formula. It has been seen in the previous section that, in algebras, the systems of equations are of the following forms. From problems of scalar type, the systems are like (6.31):

$$\{\mathbf{u_i}(Z) = \mathbf{0} \mid \mathbf{1} \le \mathbf{i} \le \mathbf{h} + \mathbf{1}\}.$$

From problems of vector or of general type, the systems are of the form of (6.38):

$$\{\mathbf{p_i}(Z, \mathbf{Z}) = \mathbf{0} \mid \mathbf{1} \le \mathbf{i} \le \mathbf{h} + \mathbf{1}\}.$$

By considering the embedding of the scalar field $\mathfrak{F}$ in the algebra $\mathfrak{A}$, and knowing that the algebra is an integral domain, it is possible to solve both the systems of equations in the algebraic closure of $\mathfrak{A}$. Then if the set of solution is finite, each solution can be verified to ensure that it is of the proper type. Variables of type scalar are assigned ground terms over the field $\mathfrak{F}$, whereas variables of type vector are assigned ground terms over the ring $\mathfrak{A}$. The reader may refer to Section 4.4 on solving constraints in commutative rings for a sketch of the approach.

If a ground term solution γ is found for the scalar variables Z, then there is a further step in the algorithm for algebras. Recall the condition (6.23) on the denominators in the general problem:

$$\forall Y \ \forall \mathbf{Y} \ \Delta(Z, Y) \neq 0 \wedge \Lambda(Z, Y) \neq 0,$$

for some scalar terms $\Delta'(Z, Y), \Lambda(Z, Y)$. Substituting the solution γ in the condition yields a conjunction of inequations of the form:

$$\forall Y \ \forall \mathbf{Y} \ \Delta'(Y) \neq 0 \wedge \Lambda'(Y) \neq 0.$$

This conjunction is verified for all assignments of the parameters Y only if the polynomials $\Delta'(Y), \Lambda'(Y)$ have no root in the field $\mathfrak{F}$. Depending on the field $\mathfrak{F}$, this can be either trivial or impossible to verify, as already mentioned in Section 6.2.1.

6.5 Examples

EXAMPLE 6.1
This example is a problem from a physics textbook. Knowing that the force acting on an electrical charge q in an electrical field $\mathbf{E}$ is described by the equation $\mathbf{F} = q\mathbf{E}$ and that the force acting on a particle of mass M moving with acceleration $\mathbf{a}$ is described by $\mathbf{F} = M\mathbf{a}$, express the acceleration of the charge in terms of the energy field. This formulation can be turned into the following pattern solving problem:

$$\Gamma := \{\mathbf{F} = M\mathbf{a}\}$$

is the input equation in vector variables $\mathbf{F}, \mathbf{a}$, and

$$\{\mathbf{a} \leftarrow x\mathbf{E}, \mathbf{F} \leftarrow q\mathbf{E}\}$$

is the solution pattern π where $\mathbf{E}$ is the parameter, and x is an unknown scalar coefficient.

After substitution, elimination of the quantifier from:

$$(\forall \mathbf{E}) q\mathbf{E} = Mx\mathbf{E}$$

$$(\forall \mathbf{E})(q - Mx)\mathbf{E} = \mathbf{0}$$

yields the formula to be solved for x:

$$q - Mx = 0$$

$$x = \frac{q}{M}$$

Hence the solution,

$$\mathbf{a} = \frac{q}{M}\mathbf{E}$$

Observe that this solution is not a term solution in the language of modules over a ring since the unknown coefficient x is instantiated to a fraction and there is no fraction symbol in the language of rings. It is a term solution in a field. The structure is that of modules over a field, that is of vector spaces, hence algebras.

6.6 Summary

This chapter studied symbolic pattern solving in algebras over fields. Because algebras are a generalization of rings, efficient quantifier elimination is possible when the algebra is an infinite integral domain over an infinite field. A complication, due to vanishing scalar denominators, arises in this context. The side conditions that must be verified in order to ensure the existence of the scalar inverses are representable as inequations. For some fields, these side conditions can never be satisfied and therefore the input to the pattern solving algorithm has to obey certain restrictions.

The next chapter will deal with a further generalization of algebras, namely a skew-commutative algebra, the graded exterior algebra over a finite dimensional vector space. It is a generalization in the sense that the commutativity axiom is relaxed to skew-commutativity.

7

Pattern Solving in Exterior Algebras

This chapter develops the pattern solving method for the structures of exterior graded algebras over a field. These algebras are skew commutative, associative algebras arising in physics applications, for instance in fluid dynamics. In the investigation of pattern solving in algebraic structures, this is the first example in the thesis of a structure that is not commutative. Again, it is a ring, but not a commutative one. Lacking the usual axiom of commutativity, replaced by skew commutativity, complicates things because the intuition is lost. The first to introduce skew commutativity was Graßmann (1862), who observed it in geometry.

Given a finite dimensional vector space over a field, there is a canonical way to construct the exterior algebra over the vector space. This algebra is finite dimensional and is generated by the vector space. Having a basis is crucial for the proof of some of the quantifier elimination results. Most of the work for this chapter has concentrated on the quantifier elimination results. Although solving equational constraints in graded exterior algebras is also very interesting, it has not been studied in enough detail due to lack of time. Graded exterior algebras admit fast elimination of quantifiers, for a particular kind of problem formula, when the underlying field is infinite and the grade of the equation is not bigger than the dimension of the vector space.

This chapter introduces the algebraic notions concerning graded exterior algebras in Section 7.1. The detailed description of pattern solving in exterior algebras is presented in Section 7.2. Several types of problems, of increasing complexity, are introduced with the deliberate intention of building intuition. Section 7.3 deals with the fast elimination of universal quantifiers in several types of problem formulas. Finding ground term solutions to the systems of equations associated to the quantifier free formulas is addressed in the Section 6.4. The last Section presents an application to a problem in Quantum Chemistry.

7.1 Algebraic Preliminaries

From a finite dimensional vector space $\mathfrak{V}$, it is possible to construct the exterior algebra of $\mathfrak{V}$, denoted by $\mathfrak{E}(\mathfrak{V})$. This algebra is generated by $\mathfrak{V}$, is finite dimensional, is associative but is not commutative. Assume that the scalar field $\mathfrak{F}$ signature is $\Sigma_F = \langle 0, 1, +, -, *, / \rangle$ and the vector space $\mathfrak{V}$ signature is $\Sigma_V = \langle \mathbf{0}, \mathbf{+}, \mathbf{-}, \cdot \rangle$. Recall the axioms of fields (2.3) on page 30, and those of modules (5.1) on page 58. In this chapter, the framework is again many-sorted so that one can distinguish three sorts, the sort scalar ranging over F, the sort vector ranging over V and the sort $\mathsf{multivector}$ ranging over $E(V)$. Observe that there is a subsort-supersort relation between the sorts vector and $\mathsf{multivector}$: $\mathsf{vector} \leq \mathsf{multivector}$.

Multiplication in the exterior algebra $\mathfrak{E}(\mathfrak{V})$, called exterior multiplication, is specified in a a natural fashion:

$$\wedge\ : \mathsf{multivector} \times \mathsf{multivector} \to \mathsf{multivector} \qquad \text{(exterior product)}$$

The exterior algebra of $\mathfrak{V}$ is generated by $\mathfrak{V}$ under the additional assumption that multiplication among vectors satisfies the axiom:

$$\forall \mathbf{v}\ \ \mathbf{v} \wedge \mathbf{v} = \mathbf{0}. \tag{7.1}$$

Axiom (7.1) implies anti-commutativity for all vectors $\mathbf{u}, \mathbf{v} \in \mathfrak{V}$:

$$\forall \mathbf{u} \forall \mathbf{v}\ \ \mathbf{u} \wedge \mathbf{v} = -(\mathbf{v} \wedge \mathbf{u}). \tag{7.2}$$

As already said, the exterior algebra of $\mathfrak{V}$ is generated by $\mathfrak{V}$. This amounts to saying that each element in $\mathfrak{E}(\mathfrak{V})$ is an F-linear combination of vectors in $\mathfrak{V}$. If $\mathbf{e}_1, \ldots, \mathbf{e}_n$ is a basis of the vector space $\mathfrak{V}$, then the exterior monomials:

$$\mathbf{e}_{i_1} \wedge \mathbf{e}_{i_2} \wedge \cdots \wedge \mathbf{e}_{i_r} \tag{7.3}$$

where $i_1 < i_2 < \ldots < i_r$, $\{i_1, i_2, \ldots, i_r\} \subseteq \{1, 2, \ldots, n\}$, are called *standard monomials* and are denoted as $\mathbf{e}_{i_1, \ldots, i_r}$ for all $1 \leq r \leq n$. Then, every element of $\mathfrak{E}(\mathfrak{V})$ is an F-linear combination of 1 and of the standard monomials. Moreover, $\mathfrak{E}(\mathfrak{V})$ can be decomposed into the sum of the subspaces:

$$\mathfrak{E}(\mathfrak{V}) = \mathfrak{F} \oplus \mathfrak{V} \oplus \mathfrak{V}^2 \oplus \cdots \oplus \mathfrak{V}^n \tag{7.4}$$

where $\mathfrak{V}^r$ is the space spanned by the products $\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_r}$ for $\mathbf{v}_i \in \mathfrak{V}$ for $1 \leq r \leq n$. Multivectors in $\mathfrak{V}^r$ are said to have grade r. Scalars in $\mathfrak{F}$ have grade zero. Each subspace $\mathfrak{V}^r$ of grade r is generated by the set of standard monomials of grade r and has dimension $\frac{n!}{r!(n-r)!}$. In the rest of the chapter, denote by S_n the set $\{1, 2, \ldots, n\}$ and by E_r^n the set of standard monomials of $\mathfrak{E}(\mathfrak{V})$ of grade r when $\mathfrak{V}$ has dimension n.

Reasoning on the representation of multivectors in terms of standard monomials, it is possible to show that the following axioms hold in the exterior algebra. Let $\mathbf{u}, \mathbf{v}, \mathbf{w}$ denote variables of sort $\mathsf{multivector}$ and x, y variables of sort scalar:

$$\begin{array}{l} \forall \mathbf{u} \forall \mathbf{v} \forall x\ \ x \cdot (\mathbf{u} \wedge \mathbf{v}) = (x \cdot \mathbf{u}) \wedge \mathbf{v} \\ \forall \mathbf{u} \forall \mathbf{v} \forall \mathbf{w}\ (\mathbf{u} \wedge \mathbf{v}) \wedge \mathbf{w} = \mathbf{u} \wedge (\mathbf{v} \wedge \mathbf{w}) \\ \forall \mathbf{u} \forall \mathbf{v} \forall \mathbf{w}\ (\mathbf{u} + \mathbf{v}) \wedge \mathbf{w} = (\mathbf{u} \wedge \mathbf{v}) + (\mathbf{u} \wedge \mathbf{w}) \end{array} \tag{7.5}$$

The product $\wedge$ creates an element of the exterior algebra whose grade is the sum of grades of the factors: if $\mathbf{u} \in \mathfrak{V}$ and $\mathbf{v} \in \mathfrak{V}^r$, then $\mathbf{u} \wedge \mathbf{v} \in \mathfrak{V}^{r+1}$, provided that $1 \leq r < n$. If $\mathbf{u} \in \mathfrak{V}$ and $\mathbf{v} \in \mathfrak{V}^n$ then $\mathbf{u} \wedge \mathbf{v} = \mathbf{0}$. From this it follows that, for all $\mathbf{v} \in \mathfrak{V}^r$, if $\dim(\mathfrak{V}) = n$ and $rd > n$ then $\mathbf{v}^d = 0$.

In order to find a normal form for exterior terms, commutativity and anti-commutativity properties need to be established. It is easy to see that commutativity holds when one multivector is of even grade, otherwise, between multivectors of odd grade, anti-commutativity holds: this kind of commutativity is called *skew commutativity*.

LEMMA 7.1
Let $\mathbf{u}, \mathbf{v}$ be multivectors and let μ, ν be their grades respectively. Then:

$$\mathbf{u} \wedge \mathbf{v} = (-1)^{\mu\nu} \cdot \mathbf{v} \wedge \mathbf{u} \tag{7.6}$$

PROOF. Trivial, after reducing each vector to a linear combination of multivectors in the appropriate subspaces or to the representation in terms of standard monomials. ∎

As a corollary, axiom (7.1) can be generalized to multivectors of odd grade in general.

COROLLARY 7.1
Let $\mathbf{v}$ *be a multivector of odd grade. Then:*

$$\mathbf{v} \wedge \mathbf{v} = \mathbf{0}. \tag{7.7}$$

PROOF. By Lemma 7.1, $\mathbf{v} \wedge \mathbf{v} = -(\mathbf{v} \wedge \mathbf{v}) = \mathbf{0}$. ∎

The kind of equations considered here will obey the following limitation:

addition is restricted to terms of same grade.

Hence, they will be algebra equations:

$$t_1 \cdot \mathbf{m_1} + t_2 \cdot \mathbf{m_2} + \ \dots \ + t_k \cdot \mathbf{m_k} = \mathbf{0}. \tag{7.8}$$

where $t_1, \dots, t_k$ are scalar terms and $\mathbf{m_1}, \dots, \mathbf{m_k}$ are exterior monomials all of same grade. If $\mathbf{m_i}$ is the exterior monomial $\mathbf{v_1}^{d_1} \wedge \dots \wedge \mathbf{v_h}^{d_h}$, then the *grade* of $\mathbf{m_i}$ is the number:

$$\eta_i = d_1\gamma_1 + \ldots + d_h\gamma_h$$

where γ_j is the grade of the multivector $\mathbf{v_j}$, $1 \leq j \leq h$. Since addition is well defined only among terms of same grade, equation (7.8) satisfies the grade constraint:

$$\eta_1 = \eta_2 = \ldots = \eta_k. \tag{7.9}$$

Moreover, the only degree for multivectors of odd grade is 1 because of Corollary 7.7. This restriction is not so unusual, Whitehead (1898), in the treatise on universal algebra, also excludes forms of mixed degree, such as $\mathbf{e}_1 + \mathbf{e}_{1,\dots,3}$, on the ground that they are "meaningless". Graßmann (1862) never introduced such forms but he also never explicitly excluded them. Structures like the one presented by Whitehead are nowadays also called *graded algebras* and terms in these structures are called *exterior forms*, for instance by Arnold (1989).

Observe that, in equation (7.8), each scalar subterm can be considered as coefficient of an exterior monomial only if the scalars commute with multivectors. This is true since:

$$\begin{aligned} \mathbf{u} \wedge (x \cdot \mathbf{v}) &= (-1)^{\mu\nu}(x \cdot \mathbf{v}) \wedge \mathbf{u} \\ &= (-1)^{\mu\nu} x \cdot (\mathbf{v} \wedge \mathbf{u}) \\ &= (-1)^{\mu\nu}(-1)^{\mu\nu} x \cdot (\mathbf{u} \wedge \mathbf{v}) \\ &= x \cdot (\mathbf{u} \wedge \mathbf{v}) \end{aligned} \tag{7.10}$$

Property (7.10), together with distributivity, allows to write an exterior term as a sum of subterms, each being a scalar subterm multiplied by an exterior monomial, just as in the equation (7.8).

Moreover, rule (7.6) on skew commutativity ensures that, given a ordering on the multivector variables, an exterior monomial has a normal form. Each monomial consists of a product of a scalar subterm followed by a subterm containing only variables of grade 1, then a subterm containing only variables of grade 2 and so on. All variables of odd grade appear linearly. Hence, terms are sums of exterior monomials which are all distinct.

Recall, from the previous chapter on algebras, that scalar denominators should be nonzero and, in such case, they can be multiplied out. When this is done, the equation (7.8) is equivalent to a conjunction:

$$t'_1 \cdot \mathbf{m_1} + t'_2 \cdot \mathbf{m_2} + \ \ldots \ + t'_n \cdot \mathbf{m_n} = \mathbf{0} \ \wedge \ \Delta \neq 0, \tag{7.11}$$

where $t'_1, \ldots, t'_n$ are now scalar terms in the signature of rings $\Sigma_R = \langle 0, 1, -, +, * \rangle$ and Δ is a scalar term obtained as product of all the denominators appearing in equation (7.8), also in signature Σ_R.

As for the other sorted structures, it is possible to identify several types of problems depending on the sort of the free variables. In the rest of the chapter, when confusion does not arise, the exterior multiplication $\wedge$ will be dropped.

7.2 Problem Description

The reader is by now familiar with the distinction that can be made, in a many-sorted setting, among constraint solving problems. In the previous chapters, there were two sorts and basically three types of problems, one where the only free variables are scalar, one where they are vector and one in which they are mixed. For graded exterior algebras over a finitely dimensional vector space of dimension n, the number of sorts is basically still two and the types of problems is still the same: three. The reader will see that the types of solution patterns influence whether efficient quantifier elimination is available for the derived problem formula. The presentation of the various problems is deliberately done in steps, first introducing a simpler type of problem and then stepwise increasing the problem complexity. This has the pleasant side effect of building the intuition about the way things behave in exterior algebras.

7.2.1 Pattern Solving of Scalar Variables

If the only free variables appearing are scalar, the input problem is a system Γ of equations that can be brought to the form:

$$\begin{array}{cccc} t_{1,1}(X) \cdot \mathbf{u}_{1,1} + & \ldots & + t_{1,k}(X) \cdot \mathbf{u}_{1,k} = \mathbf{0} \\ \vdots & \vdots & \vdots \\ t_{m,1}(X) \cdot \mathbf{u}_{m,1} + & \ldots & + t_{m,k}(X) \cdot \mathbf{u}_{m,k} = \mathbf{0} \end{array} \tag{7.12}$$

where $t_{i,j}(X)$ are scalar terms containing the variables X and the $\mathbf{u}_{i,j}$'s are ground exterior terms. Taking into consideration what has been said about algebra problems of scalar type in Section 6.2.1, one may assume that the scalar terms are in the signature Σ_R and a further condition on the simplified denominators is given:

$$\Delta(X) \neq 0. \tag{7.13}$$

Recall that $\Delta(X)$ is again a scalar Σ_R-term.

When the exterior ground monomials $\mathbf{u}_{i,j}$'s are standard monomials, since they are independent, the input problem (7.12) can be reduced to a problem over the underlying scalar field:

$$\begin{array}{ccc} t_{1,1}(X) = 0, & \ldots, & t_{1,k}(X) = 0 \\ \vdots & \vdots & \vdots \\ t_{m,1}(X) = 0, & \ldots, & t_{m,k}(X) = 0 \end{array} \tag{7.14}$$

The method of pattern solving can be applied to this problem provided that the side condition (7.13) is taken into consideration. The theorem on fast quantifier elimination in infinite integral domains applies to problem formulas arising in pattern solving over infinite fields.

When the exterior ground monomials $\mathbf{u_{i,j}}$'s are exterior monomials of constants (maybe defined by a set of equations), the input problem Γ can be brought to the form:

$$\begin{array}{ccc} t_{1,1}(X) \cdot \mathbf{g_{1,1}} + & \ldots & + t_{1,k}(X) \cdot \mathbf{g_{1,k}} = \mathbf{0} \\ \vdots & \vdots & \vdots \\ t_{m,1}(X) \cdot \mathbf{g_{m,1}} + & \ldots & + t_{m,k}(X) \cdot \mathbf{g_{m,k}} = \mathbf{0} \end{array}$$

where $t_{i,j}(X)$ are scalar terms containing the variables X and the $\mathbf{g_{i,j}}$'s are ground exterior terms. The scalar terms are in the signature Σ_R and a further condition on the simplified denominators is given:

$$\Delta(X) \neq 0, \tag{7.15}$$

where $\Delta(X)$ is again a scalar Σ_R-term.

A solution pattern π is a scalar assignment for the variables X:

$$\begin{array}{ccc} x_1 & = & h_1(Z,Y) \\ \vdots & \vdots & \vdots \\ x_l & = & h_l(Z,Y). \end{array}$$

A pattern solving problem of scalar type in exterior algebras is very similar to a pattern solving problem of scalar type in algebras. The problem formula $\psi(Z,Y)$ is a conjunction of equations and inequations obtained from the input problem and the solution pattern:

$$\begin{aligned} \forall Y \bigwedge_{1 \leq i \leq m} & t'_{i,1}(Z,Y) \cdot \mathbf{g_{i,1}} + \ldots + t'_{i,k}(Z,Y) \cdot \mathbf{g_{i,k}} = \mathbf{0} \wedge \\ & \Delta(Z,Y) \neq 0 \wedge \Lambda(Z,Y) \neq 0, \end{aligned} \tag{7.16}$$

for the appropriate scalar Σ_R-terms $t'_{i,1}(Z,Y), \ldots, t'_{i,k}(Z,Y)$. Observe the additional side condition on the denominators eventually introduced by the solution pattern:

$$\Lambda(Z,Y) \neq 0. \tag{7.17}$$

$\Lambda(Z,Y)$ is a scalar term in the signature Σ_R. The negative part of conjunction (7.16), arising from the side conditions, is postponed for verification until the last step of the algorithm. The considerations on the verifiability of such inequations, done in Section 6.2.1 for algebra problems, are also valid for this case. The positive part of the conjunction in formula (7.16) can be reordered by collecting the monomials $Y_{i,1}, \ldots, Y_{i,h}$ containing the parameters Y:

$$\forall Y \bigwedge_{1 \leq i \leq m} Y_{i,1} \cdot \mathbf{g_{i,1}}(Z) + \cdots + Y_{i,h} \cdot \mathbf{g_{i,h}}(Z) + \mathbf{g_{i,h+1}}(Z) = \mathbf{0} \tag{7.18}$$

where each $\mathbf{1} \leq \mathbf{i} \leq \mathbf{m}, \mathbf{g_{i,j}}(Z)$, $(1 \leq j \leq h+1)$ is an exterior term in free scalar and exterior variables Z. The formula (6.11) can be written in a unique way provided that, for $(1 \leq i \leq m)$, the monomials $Y_{i,1}, \ldots, Y_{i,h}$ are pairwise disjoint, ordered according to some fixed ordering and an ordering is imposed also on the exterior constants.

Elimination of quantifiers will be studied on a single equation:

$$\forall Y \; Y_1 \cdot \mathbf{g_1}(Z) + \cdots + Y_k \cdot \mathbf{g_h}(Z) + \mathbf{g_{h+1}}(Z) = \mathbf{0} \tag{7.19}$$

The results apply to a finite conjunction in a straightforward fashion. The reader wishing to directly read about elimination of quantifiers from formula (7.19) may skip to Section 7.3.1. In the next Section the pattern solving problem of type vector in algebras is described.

7.2.2 Pattern Solving of Vector Variables

A second type of pattern solving problem does not contain any free variable of sort scalar. Two forms of pattern solving problem are described in this section, the first one is easier to deal with, and the second one generalizes it.

Consider the first kind of input equations of a pattern solving problem in a graded exterior algebra. The system Γ can be brought to the form:

$$\begin{array}{rcl} t_{1,1} \cdot \mathbf{X_{1,1}} + \ldots + t_{1,k} \cdot \mathbf{X_{1,k}} & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ t_{m,1} \cdot \mathbf{X_{m,1}} + \ldots + t_{m,k} \cdot \mathbf{X_{m,k}} & = & \mathbf{0} \end{array} \tag{7.20}$$

where $\mathbf{X_{i,j}} \in [\mathbf{x_1}, \ldots, \mathbf{x_n}]$ are monomials of multivector variables $\mathbf{X}$ and the $t_{i,j}$'s are scalar terms. Without loss of generality, the scalar terms may be assumed to have no denominators. Notice that this is not the most general form of the problem since it does not allow multivector coefficients and no constant term appears. Nevertheless, in order to gain confidence with the structure of graded algebras, this is a very useful case to be studied. Moreover, it turns out that the more general problem can be solved along the same lines as this one.

For input problem (7.20), consider a solution pattern π in which there may appear unknown scalar coefficients, Z, and exterior parameters $\mathbf{Y}$. There appear no scalar parameters and no vector coefficients. Thus, the solution pattern π is an assignment of terms of the exterior algebra of the form:

$$\begin{array}{rcl} \mathbf{x_1} & = & f_{1,1}(Z) \cdot \mathbf{Y_{1,1}} + \ldots + f_{1,r_1}(Z) \cdot \mathbf{Y_{1,r_1}} \\ \vdots & \vdots & \vdots \\ \mathbf{x_n} & = & f_{n,1}(Z) \cdot \mathbf{Y_{n,1}} + \ldots + f_{n,r_n}(Z) \cdot \mathbf{Y_{n,r_n}} \end{array} \tag{7.21}$$

where the $f_{i,j}(Z) \neq 0, (1 \leq i \leq n, 1 \leq j \leq r_i)$ are scalar terms. In order to assume that the denominators are non-zero, a condition must be taken into account:

$$\Lambda(Z) \neq 0. \tag{7.22}$$

Recall that the same was done for the pattern solving problem of type vector in algebras, described in Section 6.2.2. In the solution pattern (7.21), the exterior monomials of multivector parameters, $\mathbf{Y_{i,j}} \in [\mathbf{y_1}, \ldots, \mathbf{y_l}]$, satisfy the grade constraints:

$$\nu_{i,1} = \ldots = \nu_{i,r_i} = \gamma_i, \tag{7.23}$$

where $\nu_{i,j}$ is the grade of $\mathbf{Y_{i,j}}$, $1 \leq i \leq n, 1 \leq j \leq r_i$, and γ_i is the grade of $\mathbf{x_i}$.

After substitution, by distributivity and by the rules of skew commutativity, the problem formula $\psi(Z, \mathbf{Y})$ can be written by collecting the exterior monomials $\mathbf{Y_1}, \ldots, \mathbf{Y_r} \in [\mathbf{y_1}, \ldots, \mathbf{y_l}]$. Hence, it will be of the form:

$$\forall \mathbf{Y} \bigwedge_{1 \leq i \leq m} p_{i,1}(Z) \cdot \mathbf{Y_1} + \ldots + p_{i,r}(Z) \cdot \mathbf{Y_r} = \mathbf{0} \wedge \Lambda(Z) \neq 0. \tag{7.24}$$

where $p_{i,j}(Z)$ are scalar terms again in the signature Σ_R. All exterior monomials $\mathbf{Y_1}, \ldots, \mathbf{Y_r}$ are pairwise distinct, provided that an ordering on the variables in $\mathbf{Y}$ is fixed and monomials are ordered accordingly using skew commutativity. As before, the condition on the denominators can be checked easily if some ground term substitution is found for the variables Z in the last step of the algorithm. Hence this part of the conjunction can be disregarded until the last step.

Again, as in the previous chapters, quantifier elimination can be studied on a single universally quantified equation. In this case, it is enough to consider a formula like:

$$\forall \mathbf{Y}\ p_1(Z) \cdot \mathbf{Y_1} + \ldots + p_r(Z) \cdot \mathbf{Y_r} = \mathbf{0}. \tag{7.25}$$

In Section 7.3.2, Theorem 7.1 will show that fast elimination of universal quantifiers holds for this kind of problem formula.

A more general input problem, compared to (7.20), is obtained by allowing ground exterior coefficients of the multivector variables. Hence, the input problem Γ is a system of equations of the form:

$$\begin{array}{rcl} \mathbf{t_{1,1}} \wedge \mathbf{X_{1,1}} + \ldots + \mathbf{t_{1,\ell_1}} \wedge \mathbf{X_{1,\ell_1}} + \mathbf{t_{1,\ell_1+1}} & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ \mathbf{t_{m,1}} \wedge \mathbf{X_{m,1}} + \ldots + \mathbf{t_{m,\ell_m}} \wedge \mathbf{X_{m,\ell_m}} + \mathbf{t_{m,\ell_m+1}} & = & \mathbf{0} \end{array} \tag{7.26}$$

where $\mathbf{X_{i,1}}, \ldots, \mathbf{X_{i,\ell_i}} \in [\mathbf{x_1}, \ldots, \mathbf{x_n}]$ are exterior monomials of multivector variables $\mathbf{X}$, and $\mathbf{t_{i,1}}, \ldots, \mathbf{t_{i,\ell_i+1}}$ are ground exterior terms, ($\mathbb{Q}$-linear combination of standard monomials) for $(1 \leq i \leq m)$. Let $\nu_{i,j}$ be the grade of monomial $\mathbf{X_{i,j}}$, and let $\tau_{i,j}$ be the grade of the ground exterior term $\mathbf{t_{i,k}}$, then for $(1 \leq i \leq m, 1 \leq j \leq \ell_i, 1 \leq k \leq \ell_1 + 1)$, the grade constraint holds:

$$\gamma_i = \nu_{i,1} + \tau_{i,1} = \ldots = \nu_{i,\ell_i} + \tau_{i,\ell_i} = \tau_{i,\ell_i+1}, \tag{7.27}$$

since addition is well defined only among terms of same grade.

For solution patterns containing only scalar unknown coefficients, beside the vector parameters, it is possible to show efficient quantifier elimination. Hence, let a solution pattern π be of the form (where the exterior multiplication symbol is dropped):

$$\begin{array}{rcl} \mathbf{x_1} & = & \mathbf{f_{1,1}}(Z)\mathbf{Y_{1,1}} + \ldots + \mathbf{f_{1,r_1}}(Z)\mathbf{Y_{1,r_1}} + \mathbf{f_{1,r_1+1}}(Z) \\ \vdots & \vdots & \vdots \\ \mathbf{x_n} & = & \mathbf{f_{n,1}}(Z)\mathbf{Y_{n,1}} + \ldots + \mathbf{f_{n,r_n}}(Z)\mathbf{Y_{n,r_n}} + \mathbf{f_{n,r_n+1}}(Z) \end{array} \tag{7.28}$$

where the $\mathbf{f_{i,k}}(Z), (1 \leq i \leq n, 1 \leq k \leq r_i + 1)$ are nonzero vector terms. The exterior monomials of multivector parameters $\mathbf{Y_{i,j}} \in [\mathbf{y_1}, \ldots, \mathbf{y_l}]$, $(1 \leq i \leq n, 1 \leq j \leq r_i)$ satisfy the grade constraints:

$$\phi_{i,1} + \eta_{i,1} = \ldots = \phi_{i,r_i} + \eta_{i,r_i} = \phi_{i,r_i+1} = \gamma_i, \tag{7.29}$$

where $\phi_{i,k}$ is the grade of the multivector coefficient $\mathbf{f_{i,k}}$ and $\eta_{i,j}$ is the grade of $\mathbf{Y_{i,j}}$ for $(1 \leq i \leq n, 1 \leq j \leq r_i, 1 \leq k \leq r_i + 1)$. In order to assume that the scalar subterms occurring in the multivector coefficients $\mathbf{f_{i,k}}$ do not contain vanishing denominators, an additional condition must be present:

$$\Lambda'(Z) \neq 0. \tag{7.30}$$

As in the former pattern solving problem, $\Lambda'(Z)$ is a scalar term in the signature Σ_R.

The problem formula $\psi(Z, \mathbf{Y})$ is a conjunction of equations and inequations obtained from the input problem Γ, from the condition (7.30), and from the solution pattern π. Having fixed an ordering on the exterior parameters and on the unknown scalar coefficients, the problem formula can be rewritten in a unique way by collecting the exterior monomials:

$$\forall \mathbf{Y} \bigwedge_{1 \leq i \leq m} \mathbf{g_{i,1}}(Z)\mathbf{Y_1} + \ldots + \mathbf{g_{i,h_i}}(Z)\mathbf{Y_{h_i}} + \mathbf{g_{i,h_i+1}}(Z) = \mathbf{0} \wedge \Lambda'(Z) \neq 0. \tag{7.31}$$

where $\mathbf{g_{i,j}}(Z)$, for $(1 \leq i \leq m, 1 \leq j \leq h_i + 1)$, are exterior terms not containing any parameter $\mathbf{Y}$. The scalar subterms occurring in the problem formula (7.31) are terms in the signature Σ_R since denominators introduced by the solution pattern can be simplified. Observe that all exterior monomials $\mathbf{Y_j}$, $(1 \leq i \leq m, 1 \leq j \leq h_i)$ are distinct because of the skew commutativity property and of the ordering on the exterior parameters. The condition on the denominators is easily checked if some ground term substitution is found for the variables Z in the last step of the algorithm. In fact, it becomes a ground equation. For this reason, the negative part of the conjunction can be disregarded until the last step.

Fast elimination of quantifiers will be studied on formulas consisting of one equation only:

$$\forall \mathbf{Y}\, \mathbf{g_1}(Z)\mathbf{Y_1} + \ldots + \mathbf{g_h}(Z)\mathbf{Y_h} + \mathbf{g_{h+1}}(Z) = \mathbf{0}. \tag{7.32}$$

The results then generalize to a conjunction like formula (7.31). The reader can go to Section 7.3.2 to directly read Theorem (7.3) about fast elimination of quantifiers for this type of formula.

One last further generalization in the solution pattern π for input problem (7.26) allows also unknown multivector coefficients $\mathbf{Z}$. Let $\Lambda''(Z)$ be a scalar term in the signature Σ_R to ensure that the scalar denominators in the solution pattern are non-zero. Then the pattern solving problem is basically the same as the one described in detail above. The main distinction is the form of the problem formula (7.31). In this case, the problem formula $\psi(Z, \mathbf{Z}, \mathbf{Y})$ contains unknown multivector coefficients:

$$\forall \mathbf{Y} \bigwedge_{1 \leq i \leq m} \mathbf{g_{i,1}}(Z, \mathbf{Z})\mathbf{Y_1} + \ldots + \mathbf{g_{i,h_i}}(Z, \mathbf{Z})\mathbf{Y_{h_i}} + \mathbf{g_{i,h_i+1}}(Z, \mathbf{Z}) = \mathbf{0} \wedge \Lambda''(Z) \neq 0. \tag{7.33}$$

where $\mathbf{g_{i,j}}(Z, \mathbf{Z})$, for $(1 \leq i \leq r, 1 \leq j \leq h_i + 1)$, are exterior terms not containing any parameter $\mathbf{Y}$.

In order to eliminate the universal quantifiers appearing in formula (7.33), a theorem will be shown for formulas consisting of one conjunct only:

$$\forall \mathbf{Y}\, \mathbf{g_1}(Z, \mathbf{Z})\mathbf{Y_1} + \ldots + \mathbf{g_h}(Z, \mathbf{Z})\mathbf{Y_h} + \mathbf{g_{h+1}}(Z, \mathbf{Z}) = \mathbf{0}. \tag{7.34}$$

A further restriction on the exterior monomials $\mathbf{Y_1}, \ldots, \mathbf{Y_h}$ is necessary for fast elimination to be complete. Theorem (7.2) in Section 7.3.2 takes care of this case. Next, the general type of pattern solving problem is described which will be a combination of the types of problem encountered until now.

7.2.3 Pattern Solving of Scalar and Vector Variables

The most general type for constraint solving problems in many-sorted graded exterior algebras is a combination of the former two since there appear free variables of all sorts, scalar and multivector.

When scalar variables occur in input problem (7.20), a general pattern solving problem arises. The input system of equations Γ has the form:

$$\begin{array}{rcl} \mathbf{t_{1,1}}(X) \wedge \mathbf{X_{1,1}} + \ldots + \mathbf{t_{1,\ell}}(X) \wedge \mathbf{X_{1,\ell}} + \mathbf{t_{1,\ell+1}}(X) & = & \mathbf{0} \\ \vdots & \vdots & \vdots \\ \mathbf{t_{m,1}}(X) \wedge \mathbf{X_{m,1}} + \ldots + \mathbf{t_{m,\ell}}(X) \wedge \mathbf{X_{m,\ell}} + \mathbf{t_{m,\ell+1}}(X) & = & \mathbf{0} \end{array} \tag{7.35}$$

where $\mathbf{X_{i,j}} \in [\mathbf{x_1}, \ldots, \mathbf{x_n}]$, are exterior monomials of multivector variables X and the $\mathbf{t_{i,k}}(X)$ are exterior terms containing free scalar variables $X = \{x_1, \ldots, x_l\}$, for $(1 \leq i \leq m, 1 \leq j \leq \ell, 1 \leq k \leq \ell+1)$. Without loss of generality, assume that the scalar subterms are in the signature Σ_R and a further condition on the simplified denominators is given:

$$\Delta(X) \neq 0. \tag{7.36}$$

The scalar term $\Delta(X$ is obtained as a product of scalar denominators eventually simplified.

The solution pattern that allows efficient quantifier elimination is an assignment of exterior terms for the multivector variables and of scalar terms for the scalar variables:

$$\begin{array}{rcl} \mathbf{x_1} & = & \mathbf{h_1}(Z, \mathbf{Z}, Y, \mathbf{Y}) \\ \vdots & \vdots & \vdots \\ \mathbf{x_n} & = & \mathbf{h_n}(Z, \mathbf{Z}, Y, \mathbf{Y}) \\ x_1 & = & h_1(Z, Y) \\ \vdots & \vdots & \vdots \\ x_l & = & h_l(Z, Y). \end{array} \tag{7.37}$$

The vector terms $\mathbf{h_i}(Z, \mathbf{Z}, Y, \mathbf{Y}), (1 \leq i \leq n)$ have the form:

$$\mathbf{f_{i,1}}(Z, \mathbf{Z}, Y) \cdot \mathbf{Y_{i,1}} + \ldots + \mathbf{f_{i,r_i}}(Z, \mathbf{Z}, Y) \cdot \mathbf{Y_{i,r_i}} + \mathbf{f_{i,r_i+1}}(Z, \mathbf{Z}, Y). \tag{7.38}$$

The exterior parameters occur in exterior monomials $\mathbf{Y_{i,j}} \in [\mathbf{y_1}, \ldots, \mathbf{y_l}]$ that satisfy the grade constraints:

$$\phi_{i,1} + \eta_{i,1} = \ldots = \phi_{i,r_i} + \eta_{i,r_i} = \phi_{i,r_i+1} = \gamma_i \tag{7.39}$$

where $\phi_{i,k}$ is the grade of the multivector coefficient $\mathbf{f_{i,k}}$ and $\eta_{i,j}$ is the grade of $\mathbf{Y_{i,j}}$, for $(1 \leq i \leq n, 1 \leq j \leq r_i, 1 \leq k \leq r_i + 1)$. In order to assume that the scalar subterms occurring in the multivector coefficients $\mathbf{f_{i,k}}$ and the scalar terms $h_1(Z,Y),\ldots,h_l(Z,Y)$ do not contain vanishing denominators, an additional condition must be present:

$$\Lambda(Z,Y) \neq 0. \tag{7.40}$$

As in the former pattern solving problems, $\Lambda(Z,Y)$ is a scalar term in the signature Σ_R.

Hence, by substituting the solution pattern (7.37) in the input problem (7.35), the problem formula $\psi(Z,\mathbf{Z},Y,\mathbf{Y})$ has universally quantified scalar and exterior parameters:

$$\begin{aligned} \forall Y\ \forall \mathbf{Y} \bigwedge_{1\le i\le m} & \mathbf{g_{i,1}}(Z,\mathbf{Z},Y)\mathbf{Y_{i,1}} + \ldots + \mathbf{g_{i,h_i}}(Z,\mathbf{Z},Y)\mathbf{Y_{i,h_i}} + \mathbf{g_{i,h_i+1}}(Z,\mathbf{Z},Y) = \mathbf{0} \\ & \wedge \Delta(Z,Y) \neq 0 \ \wedge\ \Lambda(Z,Y) \neq 0 \end{aligned} \tag{7.41}$$

where $\mathbf{g_{i,j}}(Z,\mathbf{Z},Y)$ are exterior terms, for $(1 \le i \le m, 1 \le j \le h_i+1)$. As in the previous section, it is possible to distinguish two cases: $\mathbf{g_{i,j}}(Z,\mathbf{Z},Y)$ are F-linear combinations of standard exterior monomials or they are general exterior terms not containing any parameter $\mathbf{Y}$. Without loss of generality, one may assume that the scalar subterms occurring in (7.41) are terms in the signature Σ_R. Moreover, all exterior monomials $\mathbf{Y_{i,1}},\ldots,\mathbf{Y_{i,h_i}}$, for every $(1 \le i \le m)$ are pairwise distinct because of the ordering on the variables and of the skew commutativity.

In Section 7.3 on quantifier elimination, an efficient procedure will be obtained for formulas consisting of one equation only:

$$\forall Y\ \forall \mathbf{Y}\ \mathbf{g_1}(Z,\mathbf{Z},Y)\mathbf{Y_1} + \ldots + \mathbf{g_h}(Z,\mathbf{Z},Y)\mathbf{Y_h} + \mathbf{g_{h+1}}(Z,\mathbf{Z},Y) = \mathbf{0}. \tag{7.42}$$

7.3 Quantifier Elimination

In this section, efficient quantifier elimination is shown for universally quantified formulas of a many-sorted language for graded exterior algebras. In most cases, the straightforward solution of the quantifier elimination is incomplete when no conditions are imposed on the exterior algebra or on the form of the quantified formula.

From pattern solving problems of type scalar, the problem formula $\psi(Z,Y)$ is of the form of (7.19):

$$\forall Y\ Y_1 \cdot \mathbf{g_1} + \cdots + Y_h \cdot \mathbf{g_h} + \mathbf{g_{h+1}} = \mathbf{0} \tag{7.43}$$

where $Y_1,\ldots,Y_h \in [y_1,\ldots,y_l]$ are pairwise distinct scalar monomials. The reader can compare this formula with the problem formula of scalar problem in algebras (6.24) on page 83. They are very similar and the elimination of quantifiers for formula (7.43) follows from the results on the algebra.

Pattern solving problems of type vector give rise to several types of formulas. The simper one is of the form of (7.25):

$$\forall \mathbf{Y}\ p_1 \cdot \mathbf{Y_1} + \ldots + p_r \cdot \mathbf{Y_r} = \mathbf{0}. \tag{7.44}$$

where $p_1,\ldots,p_r$ are scalar terms in the signature Σ_R, and $\mathbf{Y_1},\ldots,\mathbf{Y_r}$ are pairwise distinct exterior monomials. The next more complicated type allows exterior coefficients to the monomials. It is of the form of formula (7.32):

$$\forall \mathbf{Y}\ \mathbf{g_1}\mathbf{Y_1} + \ldots + \mathbf{g_h}\mathbf{Y_h} + \mathbf{g_{h+1}} = \mathbf{0}. \tag{7.45}$$

where $\mathbf{Y_1}, \ldots, \mathbf{Y_h}$ are exterior monomials of vector parameters and $\mathbf{g_1}, \ldots, \mathbf{g_{h+1}}$ are F-linear combinations of standard monomials. The third type of formulas is of the form of formula (7.34) and resembles formula (7.45). The difference is that $\mathbf{g_1}, \ldots, \mathbf{g_{h+1}}$ are, more generally, exterior terms not containing any parameter $\mathbf{Y}$.

The general type of problem formulas contains universally quantifier scalar and multivector parameters. Recall formula (7.42):

$$\forall Y\ \forall \mathbf{Y}\ \mathbf{g_1}(Z, \mathbf{Z}, Y)\mathbf{Y_1} + \ \ldots\ + \mathbf{g_h}(Z, \mathbf{Z}, Y)\mathbf{Y_h} + \mathbf{g_{h+1}}(Z, \mathbf{Z}, Y) = \mathbf{0} \tag{7.46}$$

where $\mathbf{g_1}(Z, \mathbf{Z}, Y)$,..., $\mathbf{g_{h+1}}(Z, Y)$ are exterior terms.

7.3.1 Quantifier Elimination of Scalar Variables

The goal of this section is to show how to eliminate efficiently the universal quantifiers in problem formula (7.43). The main observation is that the results shown for the algebra case in Section 6.3.1 can be used also here.

It is easy to simplify the formula by considering the zero assignment $\mathbf{y_1} = \ldots = \mathbf{y_l} = \mathbf{0}$. This yields:

$$\mathbf{g_{h+1}} = \mathbf{0} \tag{7.47}$$

which substituted back in (7.43) yields

$$(\forall Y)\ Y_1 \cdot \mathbf{g_1} + \ \cdots\ + Y_h \cdot \mathbf{g_h} = \mathbf{0}. \tag{7.48}$$

The scalar monomials $Y_1, \ldots, Y_h \in F[Y]$ are pairwise distinct and not constant. The exterior monomials are terms in the exterior algebra, which is associative and skew-commutative. Inspection of the proof of Theorem 6.7, shows that commutativity of the algebra has not been used. Therefore, the following Corollary is true.

COROLLARY 7.2
Let $\mathfrak{V}$ be a vector space of dimension n over an infinite field $\mathfrak{F}$, $\mathbf{g_1}, \ldots, \mathbf{g_h}$ be exterior terms and $Y_1, \ldots, \ldots Y_h \in F[y_1, \ldots, y_k]$ be pairwise distinct scalar monomials. Then:

$$\mathfrak{E}(\mathfrak{V}) \models \forall Y\ Y_1 \cdot \mathbf{g_1} + \ \cdots\ + Y_h \cdot \mathbf{g_h} = \mathbf{0}\ \leftrightarrow\ \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0},$$

if $\gamma \leq n$, where γ is the grade of any exterior term $\mathbf{g_1}, \ldots, \mathbf{g_h}$.

PROOF. The same proof of Theorem 6.7, when the algebra is $\mathfrak{E}(\mathfrak{V})$. ■

Recall the problem formula of type scalar (7.19):

$$\forall Y\ Y_1 \cdot \mathbf{g_1}(Z) + \ \cdots\ + Y_h \cdot \mathbf{g_h}(Z) + \mathbf{g_{h+1}}(Z) = \mathbf{0}.$$

When the underlying field $\mathfrak{F}$ is infinite, it is equivalent to the quantifier-free conjunction:

$$\mathbf{g_1}(Z) = \mathbf{0}\ \wedge \cdots \wedge\ \mathbf{g_h}(Z) = \mathbf{0}\ \wedge\ \mathbf{g_{h+1}}(Z) = \mathbf{0}.$$

Since this formula is a conjunction of equations in free scalar variables Z, the last step of the pattern solving algorithm is required to solve the corresponding system:

$$\{\mathbf{g_i}(Z) = \mathbf{0} \mid 1 \leq i \leq h+1\}. \tag{7.49}$$

Solving equations in exterior algebras is the topic of Section 7.4.

7.3.2 Quantifier Elimination of Vector Variables

Before proving the more general quantifier elimination for formulas with universally quantified vector variables, a simpler type of formula will be considered. Quantifier elimination is shown for formula (7.44), with scalar coefficients first. Then, it is generalized to the formulas (7.45) with exterior coefficients.

Theorem 7.1
Let $\mathfrak{V}$ be a vector space of dimension n over an infinite field $\mathfrak{F}$, $p_1, \dots, p_h$ be scalar terms and $\mathbf{Y_1}, \dots, \mathbf{Y_h} \in [\mathbf{y_1}, \dots, \mathbf{y_k}]$ be pairwise distinct exterior monomials of grade γ. If $\gamma \leq n$, then:

$$\mathfrak{E}(\mathfrak{V}) \models \forall \mathbf{Y}\ p_1 \cdot \mathbf{Y_1} + \dots + p_h \cdot \mathbf{Y_h} = \mathbf{0} \ \leftrightarrow\ p_1 = 0 \wedge \dots \wedge p_h = 0.$$

Proof. The direction

$$\mathfrak{E}(\mathfrak{V}) \models \forall \mathbf{Y}\ p_1 \cdot \mathbf{Y_1} + \dots + p_h \cdot \mathbf{Y_h} = \mathbf{0} \ \leftarrow\ p_1 = 0 \wedge \dots \wedge p_h = 0$$

is trivially true. More interesting is the direction

$$\mathfrak{E}(\mathfrak{V}) \models \forall \mathbf{Y}\ p_1 \cdot \mathbf{Y_1} + \dots + p_h \cdot \mathbf{Y_h} = \mathbf{0} \ \rightarrow\ p_1 = 0 \wedge \dots \wedge p_h = 0.$$

The proof is by induction on the size s of the formula:

$$\forall \mathbf{Y}\ p_1 \cdot \mathbf{Y_1} + \dots + p_h \cdot \mathbf{Y_h} = \mathbf{0} \tag{7.50}$$

measured as $s = k + h$, where k is the number of quantified variables in $\mathbf{Y}$ and h is the number of terms in the equation (7.50).

Base case: $s = 1 + 1$, corresponding to one variable, $\mathbf{y_1}$ and one term in the equation (7.50). Two cases are distinguished, depending on the grade of the variable $\mathbf{y_1}$.

When $\mathbf{y_1}$ is a variable $\mathbf{y}$ of odd grade, then it can appear only linearly. Therefore, equation (7.50) is of the form:

$$\forall \mathbf{y}\ p \cdot \mathbf{y} = \mathbf{0}. \tag{7.51}$$

Assume that $\mathfrak{E}(\mathfrak{V})$ satisfies equation (7.51) and that the dimension n of $\mathfrak{V}$ is greater or equal to the grade γ of the equation, which is also the grade of $\mathbf{y}$. Therefore $\mathfrak{V}$ contains at least $\{\mathbf{e}_1, \dots, \mathbf{e}_\gamma\}$ base vectors and $\mathfrak{E}(\mathfrak{V})$ contains at least the multivectors $\{\mathbf{e}_1, \dots, \mathbf{e}_\gamma, \dots, \mathbf{e}_{1,\dots,\gamma}\}$. Since equation (7.51) holds for all multivectors of grade γ in $\mathfrak{E}(\mathfrak{V})$, it must hold also for $\mathbf{y} = \mathbf{e}_{1,\dots,\gamma} \neq \mathbf{0}$, and therefore $p = 0$.

When $\mathbf{y_1}$ is a variable $\mathbf{y}$ of even grade, then it can appear nonlinearly. Therefore, equation (7.50) is of the form:

$$\forall \mathbf{y}\ p \cdot \mathbf{y}^d = \mathbf{0}. \tag{7.52}$$

Assume that $\mathfrak{E}(\mathfrak{V})$ satisfies equation (7.52) and that the dimension n of $\mathfrak{V}$ is greater or equal to the grade $\gamma = d\lambda$ of the equation, where λ is the grade of $\mathbf{y}$. Therefore $\mathfrak{V}$ contains at least $\{\mathbf{e}_1, \dots, \mathbf{e}_{d\lambda}\}$ base vectors and $\mathfrak{E}(\mathfrak{V})$ contains at least the multivectors $\{\mathbf{e}_1, \dots, \mathbf{e}_\gamma, \dots, \mathbf{e}_{1,\dots,d\lambda}\}$. Since the equation (7.52) holds for all multivectors of grade λ in $\mathfrak{E}(\mathfrak{V})$, it must hold also for $\mathbf{y} = \mathbf{e}_{1,\dots,\lambda} + \dots + \mathbf{e}_{d\lambda-\lambda,\dots,d\lambda}$. Then, $\mathbf{y}^d = \mathbf{e}_{1,\dots,d\lambda}$ and $p\mathbf{e}_{1,\dots,d\lambda} \neq 0$ implies $p = 0$.

Induction Step. Assume that the theorem holds for all formulas of length $s < n$. The goal is to show it for equations of size n. Distinguish two cases: there is a quantified variable that does not appear in some monomial, and all variables appear in all monomials.

Consider the case in which at least one variable , say $\mathbf{y_k}$, does not appear in every monomial. Without loss of generality, assume that $\mathbf{y_k}$ does not appear in the last i monomial terms, $\mathbf{Y_{h-i}}, \ldots, \mathbf{Y}_i$ and it appears in the first $h-i-1$, $\mathbf{Y_1}, \ldots, \mathbf{Y_{h-i-1}}$. Then, since the equation (7.50) holds for all values of $\mathbf{y_k}$, it holds also for $\mathbf{y_k} = \mathbf{0}$, which yields:

$$\forall \mathbf{Y}\; p_{h-i} \cdot \mathbf{Y_{h-i}} + \ldots + p_h \cdot \mathbf{Y_h} = \mathbf{0} \tag{7.53}$$

where $\mathbf{Y_j} \in [\mathbf{y_1}, \ldots, \mathbf{y_{k-1}}]$, for $h-i \le j \le h$, are monomials in the first $k-1$ exterior parameters. Since the equation (7.53) has certainly size smaller than n, because it contains one less variable and less monomials than the original equation (7.50), it follows by induction hypothesis that:

$$p_{h-i} = 0 \wedge \ldots \wedge p_h = 0.$$

But then, by substituting back into equation (7.50), it also holds that:

$$\forall \mathbf{Y}\; p_1 \cdot \mathbf{Y_1} + \ldots + p_{h-i-1} \cdot \mathbf{Y_{h-i-1}} = \mathbf{0}.$$

Induction hypothesis applies again since the number of monomials is certainly less than h, thus:

$$p_1 = 0 \wedge \ldots \wedge p_{h-i-1} = 0$$

which concludes this case of the proof.

At last, it remains to consider the case in which all variables appear in all monomials. The proof for this case is rather technical and is based on the representation of each element of the exterior algebra $\mathfrak{E}(\mathfrak{V})$ as an F-linear combination of standard monomials. Let $\mathbf{y_1}, \ldots, \mathbf{y_k}$ be the quantified variables and let $\gamma_1, \ldots, \gamma_k$ be their grades respectively. Consider a quantified variable $\mathbf{y_j}$ of grade γ_j and let $\mathbf{v_j}$ be an arbitrary multivector in V^{γ_j} that can be assigned to $\mathbf{y_j}$. Let Γ_j be the set of indices of standard monomials in $E^n_{\gamma_j}$. Then, the vector $\mathbf{v_j}$ can be represented in terms of standard monomials of grade γ_j:

$$\mathbf{v_j} = \sum_{i \in \Gamma_j} a_{i,j} \mathbf{u_i}.$$

When the coefficients $a_j = \{a_{i,j} \mid i \in \Gamma_j\}$ vary on the scalar field, the vector $\mathbf{v_j}$ varies over V^{γ_j}. This implies that, in order to consider all possible assignments for $\mathbf{y_j}$, it is enough to consider all possible coefficients. Thus, a formula with universally quantified multivector variables:

$$\forall \mathbf{y_1} \ldots \forall \mathbf{y_k}\; \Psi(\mathbf{y_1}, \ldots, \mathbf{y_k})$$

is equivalent to a formula with universally quantified scalar variables:

$$\forall a_1 \ldots \forall a_k\; \Psi(\sum_{i \in \Gamma_1} a_{i,1} \mathbf{u_i}, \ldots, \sum_{i \in \Gamma_k} a_{i,k} \mathbf{u_i}).$$

A short notation is used above and in what follows: $a_j = \{a_{i,j} \mid i \in \Gamma_j\}, 1 \le j \le k$. This equivalence can be used to show the last case left in the proof. Let $\mathbf{y_1}^{e_1} \ldots \mathbf{y_k}^{e_k}$ be an exterior monomial of total grade $\mu = e_1\gamma_1 + \ldots + e_k\gamma_k$ in the original formula. As linear combination of standard monomials of grade μ, it eventually reduces to:

$$\sum_{i \in \Gamma_\mu} q_i(a_1, \ldots, a_k) \cdot \mathbf{u_i}$$

where each $q_i(a_1, \ldots, a_k)$ is a scalar Σ_R-term in free variables $a_1, \ldots, a_k$. Recall that in every exterior monomial the odd variables occur linearly while the even ones may appear nonlinearly. Since by hypothesis all monomials are distinct, they must differ pairwise in at least one degree of some even variable (because all variables occur in every monomial). Therefore, because of the different degree of some variable, every monomial is equivalent to a combination of standard monomials of grade μ such that the scalar coefficients $q_i(a_1, \ldots, a_k)$ arising from distinct monomials are distinct. Considering this standard representation, the initial formula (7.50) is equivalent to:

$$\forall a_1 \ldots \forall a_k \ \sum_{j=1}^{h} p_j \sum_{i \in \Gamma_\mu} q_{i,j}(a_1, \ldots, a_k) \cdot \mathbf{u_i} = \mathbf{0}. \tag{7.54}$$

Reordering formula (7.54), yields the coordinate representation in terms of the standard monomials of grade μ:

$$\forall a_1 \ldots \forall a_k \ \sum_{i \in \Gamma_\mu} \sum_{j=1}^{h} p_j q_{i,j}(a_1, \ldots, a_k) \cdot \mathbf{u_i} = \mathbf{0}. \tag{7.55}$$

Since the scalar terms are all distinct, the coefficients: $\sum_{j=1}^{h} p_j q_{i,j}(a_1, \ldots, a_k)$ do not vanish. Moreover, since the standard monomials are linearly independent, formula (7.55) is equivalent to the scalar formula:

$$\forall a_1 \ldots \forall a_k \ \bigwedge_{i \in \Gamma_\mu} \sum_{j=1}^{h} p_j q_{i,j}(a_1, \ldots, a_k) = 0$$

Since the scalar terms are related to the exterior monomials, that were pairwise disjoint, the following is true: for any pair $n, m \in \{1, \ldots, h\}$, there exists a least one $i \in \Gamma_\mu$ such that $q_{i,n}(a_1, \ldots, a_k) \neq q_{i,m}(a_1, \ldots, a_k)$. From this, it follows that also a formula:

$$\forall a_1 \ldots \forall a_k \ \ldots + p_n q_{i,n}(a_1, \ldots, a_k) + p_m q_{i,m}(a_1, \ldots, a_k) + \ldots = 0$$

must be true. This shows that p_n and p_m appear as coefficients of some universally quantified variable. Then, since the scalar field is an infinite integral domain, it follows that

$$p_n = 0 \wedge p_m = 0.$$

Repeating the same reasoning for all pairs m, n, the conclusion follows:

$$p_1 = 0 \wedge \ldots \wedge p_h = 0.$$

■

Recall the vector problem formula (7.25):

$$\forall \mathbf{Y} \ p_1(Z) \cdot \mathbf{Y_1} + \ \ldots \ + p_r(Z) \cdot \mathbf{Y_r} = \mathbf{0}.$$

Then, if the scalar field is infinite, by Theorem (7.1), an equivalent quantifier-free formula is the conjunction of scalar equations:

$$p_1(Z) = 0 \wedge \ldots \wedge p_r(Z) = 0.$$

The corresponding system of equations to be solved in the last step of the SolPat algorithm is:

$$\{p_i(Z) = 0 \mid 1 \leq i \leq r\}. \tag{7.56}$$

Having shown the special case of scalar subterms, the next theorem allows to eliminate quantifiers from the problem formula which contains as coefficients some standard monomials. It is a generalization of the previous one.

Using the same reasoning as for problems in R-modules, it is easy to deduce, from formula (7.45), and equivalent conjunction:

$$\forall \mathbf{Y}\ \mathbf{g_1 Y_1} + \ldots + \mathbf{g_h Y_h} = \mathbf{0}\ \wedge\ \mathbf{g_{h+1}} = \mathbf{0}. \tag{7.57}$$

In fact, by assigning zero in (7.32) to all parameters, that is $\mathbf{y_1} = \ldots = \mathbf{y_l} = \mathbf{0}$, it is clear that:

$$\mathbf{g_{h+1}} = \mathbf{0}, \tag{7.58}$$

which combined again with the formula (7.45), yields the first conjunct in (7.57):

$$\forall \mathbf{Y}\ \mathbf{g_1 Y_1} + \ldots + \mathbf{g_h Y_h} = \mathbf{0}. \tag{7.59}$$

Now, it is necessary to show efficient elimination of quantifiers for formula (7.59). The next Corollary does the job and is an easy consequence of Theorem 7.1.

Corollary 7.3
Let $\mathfrak{V}$ be a vector space of dimension n over an infinite field $\mathfrak{F}$, $\mathbf{g_1}, \ldots, \mathbf{g_h}$ be F-linear combinations of standard monomials, and $\mathbf{Y_1}, \ldots, \mathbf{Y_h} \in \{\mathbf{y_1}, \ldots, \mathbf{y_k}\}$ be pairwise disjoint exterior monomials. Then:

$$\mathfrak{E}(\mathfrak{V}) \models (\forall \mathbf{Y})\ \mathbf{g_1 Y_1} + \ldots + \mathbf{g_h Y_h} = \mathbf{0} \leftrightarrow \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0}$$

when the grade γ of the equation satisfies $n \geq \gamma$.

Proof. The direction:

$$\mathfrak{E}(\mathfrak{V}) \models \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0} \rightarrow \forall \mathbf{Y}\ \mathbf{g_1 Y_1} + \ldots + \mathbf{g_h Y_h} = \mathbf{0}$$

is trivially true. The opposite direction:

$$\mathfrak{E}(\mathfrak{V}) \models \forall \mathbf{Y}\ \mathbf{g_1 Y_1} + \ldots + \mathbf{g_h Y_h} = \mathbf{0} \rightarrow \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0}$$

has to be shown. Assume that:

$$\mathfrak{E}(\mathfrak{V}) \models \forall \mathbf{Y}\ \mathbf{g_1 Y_1} + \ldots + \mathbf{g_h Y_h} = \mathbf{0}.$$

Recall that each exterior term $\mathbf{g_i}$ among $\mathbf{g_1}, \ldots, \mathbf{g_h}$ in (7.60) is an F-linear combinations of standard monomials $\mathbf{u_{i,1}}, \ldots, \mathbf{u_{i,s_i}}$:

$$\mathbf{g_i} := p_{i,1} \cdot \mathbf{u_{i,1}} + \ldots + p_{i,s_i} \cdot \mathbf{u_{i,s_i}} \tag{7.60}$$

for some scalar subterms $p_{i,1}, \ldots, p_{i,s_i}$. Thus, if all the exterior coefficients $\mathbf{g_1}, \ldots, \mathbf{g_h}$ are expanded in formula (7.60), the assumption becomes:

$$\forall \mathbf{Y}\ p_{1,1} \cdot \mathbf{u_{1,1}Y_1} + \ \ldots \ + p_{h,s_h} \cdot \mathbf{u_{h,s_h}Y_h} = \mathbf{0}. \tag{7.61}$$

By viewing each standard monomial as a new exterior variable, that is also universally quantified, formula (7.61) satisfies all hypotheses of Theorem 7.1. Therefore, it is equivalent to the quantifier-free conjunction:

$$p_{1,1} = 0 \wedge \ldots \wedge p_{h,s_h} = 0.$$

But this implies, since the standard monomials are F-linear independent that:

$$p_{i,1} \cdot \mathbf{u_{i,1}} + \ \ldots \ + p_{i,s_i} \cdot \mathbf{u_{i,s_i}} = \mathbf{0}$$

for all $1 \leq i \leq h$. Therefore the assertion is shown:

$$\mathbf{g_1} = \mathbf{0} \ \wedge \ldots \wedge \ \mathbf{g_h} = \mathbf{0}.$$

■

Summarizing, by Corollary 7.3 shown above and by formula (7.57), it is possible to eliminate the quantified parameters from problem formula (7.32), provided that the scalar field is infinite. The quantifier-free equivalent formula is a conjunction of equations:

$$\mathbf{g_1}(Z) = 0 \wedge \ldots \wedge \mathbf{g_{h+1}}(Z) = 0$$

in which each exterior term is a combination of standard monomials. The associated system of equations:

$$\{\mathbf{g_i}(Z) = \mathbf{0} \mid 1 \leq i \leq h+1\} \tag{7.62}$$

has to be solved for the unknown scalar coefficients Z over the field $\mathfrak{F}$.

One may try to show even a more general theorem. In this case, the exterior coefficients $\mathbf{g_1}, \ldots, \mathbf{g_h}$ are arbitrary and not an F-linear combination of standard monomials as in Corollary 7.3. Once again, by the same reasoning as above, problem formula (7.34) implies the conjunction of formulas:

$$\forall \mathbf{Y}\ \mathbf{g_1}(Z, \mathbf{Z})\mathbf{Y_1} + \ \ldots \ + \mathbf{g_{h_i}}(Z, \mathbf{Z})\mathbf{Y_h} = \mathbf{0} \ \wedge \ \mathbf{g_{h+1}}(Z, \mathbf{Z}) = \mathbf{0}.$$

Since the universally quantified variables occur only in the first conjunct, one may consider the elimination on formulas:

$$\forall \mathbf{Y}\ \mathbf{g_1}(Z, \mathbf{Z})\mathbf{Y_1} + \ \ldots \ + \mathbf{g_h}(Z, \mathbf{Z})\mathbf{Y_h} = \mathbf{0} \tag{7.63}$$

where $\mathbf{Y_1}, \ldots, \mathbf{Y_h} \in [\mathbf{Y}]$ are pairwise disjoint exterior monomials and $\mathbf{g_1}(Z, \mathbf{Z}), \ldots, \mathbf{g_h}(Z, \mathbf{Z})$ are exterior terms. The next Theorem does not show fast quantifier elimination in the full general form, but a special case. An additional hypothesis on the exterior monomials is needed.

THEOREM 7.2
Let $\mathfrak{V}$ be a vector space of dimension n over a field $\mathfrak{F}$, $\mathbf{g_1}, \ldots, \mathbf{g_h}$ be exterior terms, and $\mathbf{Y} = \{\mathbf{y_1}, \ldots, \mathbf{y_k}\}$ be variables ranging over the graded exterior algebra. Additionally,

assume that there is at least one parameter, among $\mathbf{y_1}, \ldots, \mathbf{y_k}$*, that does not occur in some monomial among* $\mathbf{Y_1}, \ldots, \mathbf{Y_h}$*. Then*

$$\mathfrak{C}(\mathfrak{V}) \models \forall \mathbf{Y}\ \mathbf{g_1}\mathbf{Y_1} + \ldots + \mathbf{g_h}\mathbf{Y_h} = \mathbf{0} \leftrightarrow \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0}$$

when the grade γ *of the equation satisfies* $n \geq \gamma$*.*

PROOF. The proof follows the lines of Theorem 7.1. Again, the direction:

$$\mathfrak{C}(\mathfrak{V}) \models \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0} \rightarrow \forall \mathbf{Y}\ \mathbf{g_1}\mathbf{Y_1} + \ldots + \mathbf{g_h}\mathbf{Y_h} = \mathbf{0}$$

is trivially true. Hence, the goal is to show:

$$\mathfrak{C}(\mathfrak{V}) \models \forall \mathbf{Y}\ \mathbf{g_1}\mathbf{Y_1} + \ldots + \mathbf{g_h}\mathbf{Y_h} = \mathbf{0} \rightarrow \mathbf{g_1} = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h} = \mathbf{0}.$$

Assume:

$$\mathfrak{C}(\mathfrak{V}) \models \forall \mathbf{Y}\ \mathbf{g_1}\mathbf{Y_1} + \ldots + \mathbf{g_h}\mathbf{Y_h} = \mathbf{0}.$$

The proof is by induction on the size s of the formula:

$$\forall \mathbf{Y}\ \mathbf{g_1}\mathbf{Y_1} + \ldots + \mathbf{g_h}\mathbf{Y_h} = \mathbf{0} \tag{7.64}$$

measured as $s = k + h$, where k is the number of quantified variables in $\mathbf{Y}$ and h is the number of terms in the equation.

Base case: $s = 1 + 1$, corresponding to one variable, $\mathbf{y_1}$ and one term in the equation. Two cases can be distinguished, depending on the parity of the variable $\mathbf{y_1}$.

When $\mathbf{y_1}$ is a variable $\mathbf{y}$ of odd grade then it can appear only linearly. Therefore equation (7.64) is of the form:

$$\forall \mathbf{y}\ \mathbf{g}\mathbf{y} = \mathbf{0}. \tag{7.65}$$

Assume that $\mathfrak{C}(\mathfrak{V})$ satisfies the equation and that the dimension n of $\mathfrak{V}$ is greater or equal to the grade of the equation $\mu = \gamma_g + \gamma$, where γ_g is the grade of the exterior term $\mathbf{g}$ and γ is the grade of $\mathbf{y}$. By contradiction, assume that $\mathbf{g} \neq \mathbf{0}$. Then, it is generated as an F-linear combination of standard monomials in $E^n_{\gamma_g}$. Let Γ_g be the set of indices of standard monomials in $E^n_{\gamma_g}$. Then $\mathbf{g}$ can be represented in terms of standard monomials:

$$\mathbf{g} = \sum_{i \in \Gamma_g} \alpha_i \mathbf{u_i}.$$

Since $\mathbf{g} \neq \mathbf{0}$, at least one coefficient must be nonzero in the combination, without loss of generality let $\alpha_1 \neq 0$. Recall that $\mathfrak{V}$ contains at least $\{\mathbf{e}_1, \ldots, \mathbf{e}_\mu\}$ base vectors and $\mathfrak{C}(\mathfrak{V})$ contains at least $\{\mathbf{e}_1, \ldots, \mathbf{e}_{1,\ldots,\mu}\}$. Assign to $\mathbf{y}$ the standard monomial $\mathbf{u}$ in E^n_γ such that: $\mathbf{u_1} \wedge \mathbf{u} = \mathbf{e}_{1,\ldots,\mu}$. This yields, when substituted in the formula (7.65):

$$\begin{aligned}(\sum_{i \in \Gamma_g} \alpha_i \mathbf{u_i}) \wedge \mathbf{u} &= \ldots + \alpha_1 \cdot (\mathbf{u_1} \wedge \mathbf{u}) + \ldots \\ &= \ldots + \alpha_1 \cdot \mathbf{e}_{1,\ldots,\mu} + \ldots \\ &\neq \mathbf{0}.\end{aligned}$$

Therefore $\mathbf{g} = \mathbf{0}$.

When $\mathbf{y_1}$ is a variable $\mathbf{y}$ of even grade then it can appear nonlinearly and therefore equation (7.64) is of the form:

$$\forall \mathbf{y}\ \mathbf{g}\mathbf{y}^d = \mathbf{0}. \tag{7.66}$$

The proof is the same as the previous case. Assume that $\mathfrak{E}(\mathfrak{V})$ satisfies the equation and that the dimension n of $\mathfrak{V}$ is greater or equal to the grade of the equation $\mu = \gamma_g + d\gamma$, where γ_g is the grade of $\mathbf{g}$ and γ is the grade of $\mathbf{y}$. Therefore, $\mathfrak{V}$ contains at least $\{\mathbf{e_1}, \dots, \mathbf{e}_\mu\}$ base vectors and $\mathfrak{E}(\mathfrak{V})$ contains at least $\{\mathrm{e}_1, \dots, \mathrm{e}_{1,\dots,\mu}\}$. Like above, by contradiction, assume that $\mathbf{g} \neq \mathbf{0}$. Then, it is generated as an F-linear combination of standard monomials in $E^n_{\gamma_g}$. Let Γ_g be the set of indices of standard monomials in $E^n_{\gamma_g}$, then $\mathbf{g}$ can be represented in terms of standard monomials:

$$\mathbf{g} = \sum_{i \in \Gamma_g} \alpha_i \mathbf{u_i}.$$

Since $\mathbf{g} \neq \mathbf{0}$, at least one coefficient must be nonzero in the combination, without loss of generality let $\alpha_1 \neq 0$. Assign to $\mathbf{y}$ a multivector $\mathbf{v}$, consisting in a sum of standard monomials in E^n_γ, such that: $\mathbf{u_1} \wedge \mathbf{v}^d = \sigma \mathrm{e}_{1,\dots,\mu}$ where σ is eventually a negative sign. (It is not difficult to construct such a multivector $\mathbf{v}$). This yields, when substituted in the formula (7.66):

$$\begin{aligned}(\sum_{i \in \Gamma_g} \alpha_i \mathbf{u_i}) \wedge \mathbf{u^d} &= \dots + \alpha_1 \cdot (\mathbf{u_1} \wedge \mathbf{u}^d) + \dots \\ &= \dots + \alpha_1 \cdot \mathrm{e}_{1,\dots,\mu} + \dots \\ &\neq \mathbf{0}.\end{aligned}$$

Therefore $\mathbf{g} = \mathbf{0}$.

Induction Step. Assume that the theorem holds for all equations of length $s < n$. The goal is to show it for equations of size n.

By hypothesis, at least one variable , say $\mathbf{y_k}$, does not appear in every monomial. Without loss of generality, assume that $\mathbf{y_k}$ does not appear in the last i monomial terms, $\mathbf{Y_{h-i}}, \dots, \mathbf{Y_i}$ and it appears in the first $h-i-1$, $\mathbf{Y_1}, \dots, \mathbf{Y_{h-i-1}}$. Then, since the equation holds for all values of $\mathbf{y_k}$, it holds also for $\mathbf{y_k} = \mathbf{0}$, which yields:

$$\forall \mathbf{Y}\ \mathbf{g_{h-i}Y_{h-i}} + \dots + \mathbf{g_h Y_h} = 0$$

where $\mathbf{Y_j} \in [\mathbf{y_1}, \dots, \mathbf{y_{k-1}}]$, for $h - i \leq j \leq h$, are monomials in the first $k-1$ exterior parameters. Since this equation has certainly size smaller than n (it contains one less variable than the original equation and less monomials), it follows by induction hypothesis that:

$$\mathfrak{E}(\mathfrak{V}) \models \forall \mathbf{Y}\ \mathbf{g_{h-i}Y_{h-i}} + \dots + \mathbf{g_h Y_h} = \mathbf{0} \to \mathbf{g_{h-i}} = \mathbf{0} \wedge \dots \wedge \mathbf{g_h} = \mathbf{0}.$$

But then, by substituting $\mathbf{g_{h-i}} = \mathbf{0}, \dots, \mathbf{g_h} = \mathbf{0}$ back into the initial equation, it also holds that

$$\mathfrak{E}(\mathfrak{V}) \models (\forall \mathbf{Y})\ \mathbf{g_1} \cdot \mathbf{Y_1} + \dots + \mathbf{g_{h-i-1}Y_{h-i-1}} = \mathbf{0}.$$

Again induction hypothesis applies, since the number of monomials is certainly less than h, thus:

$$\mathfrak{E}(\mathfrak{V}) \models \mathbf{g_1} = \mathbf{0} \wedge \dots \wedge \mathbf{g_{h-i-1}} = \mathbf{0}$$

which concludes the proof. ∎

Now recall formula (7.63). If, beside the condition on the grade of the equation, the exterior monomials are pairwise disjoint and there exists at least one parameter in $\mathbf{Y}$ that does not occur in every monomial, then the quantifier-free formula is the conjunction:

$$\mathbf{g_1}(Z, \mathbf{Z}) = \mathbf{0} \wedge \ldots \wedge \mathbf{g_h}(Z, \mathbf{Z}) = \mathbf{0}.$$

Hence, the associated system of equations is:

$$\{\mathbf{g_i}(Z, \mathbf{Z}) = \mathbf{0} \mid 1 \leq i \leq h+1\}. \tag{7.67}$$

Solving this and the other systems of equations is the topic of Section 7.4. The next Section deals with elimination of quantifiers over scalar and multivector parameters in problem formulas of general form.

7.3.3 Quantifier Elimination of Scalar and Vector Variables

In the section on quantifier elimination, an efficient procedure will be obtained for problem formulas with quantified scalar and multivector parameters. In the rest of the section, let $\mathfrak{V}$ be a finite dimensional vector space of dimension n over a field $\mathfrak{F}$, and let $\mathfrak{E}(\mathfrak{V})$ be the graded exterior algebra over $\mathfrak{V}$.

Recall problem formula (7.42):

$$\forall Y\ \forall \mathbf{Y}\ \mathbf{g_1}(Z, \mathbf{Z}, Y)\mathbf{Y_1} + \ \ldots\ + \mathbf{g_h}(Z, \mathbf{Z}, Y)\mathbf{Y_h} + \mathbf{g_{h+1}}(Z, \mathbf{Z}, Y) = \mathbf{0}$$

With the same reasoning as done in the previous sections, by considering the null assignment for parameters $\mathbf{Y}$, it is immediate to deduce the conjunction:

$$\forall Y\ \forall \mathbf{Y}\ \mathbf{g_1}(Z, \mathbf{Z}, Y)\mathbf{Y_1} + \ \ldots\ + \mathbf{g_h}(Z, \mathbf{Z}, Y)\mathbf{Y_h} = \mathbf{0}\ \wedge (\forall Y)\ \mathbf{g_{h+1}}(Z, \mathbf{Z}, Y) = \mathbf{0}. \tag{7.68}$$

Efficient quantifier elimination can be approached for each conjunct separately. Consider the sub-formula:

$$\forall Y\ \forall \mathbf{Y}\ \mathbf{g_1}(Z, \mathbf{Z}, Y)\mathbf{Y_1} + \ \ldots\ + \mathbf{g_h}(Z, \mathbf{Z}, Y)\mathbf{Y_h} = \mathbf{0}. \tag{7.69}$$

first. The exterior terms $\mathbf{g_1}(Z, Y), \ldots, \mathbf{g_h}(Z, Y)$ are not in general F-linear combination of standard monomials. The conjunction:

$$\bigwedge_{1 \leq i \leq h} \forall Y\ \mathbf{g_i}(Z, \mathbf{Z}, Y) = \mathbf{0}. \tag{7.70}$$

is the equivalent quantifier-free formula only if the grade γ of equation (7.69) is less or equal n, and at least one multivector parameter does not occur in every monomial in formula (7.69). No further hypothesis is needed on the field $\mathfrak{F}$ according to Theorem 7.2. Nevertheless, the field $\mathfrak{F}$ must be infinite in order to eliminate the quantifiers on the scalar parameters in formulas (7.70) and in the sub-formula:

$$\forall Y\ \mathbf{g_{h+1}}(Z, \mathbf{Z}, Y) = \mathbf{0}$$

of formula (7.68). By Corollary 7.2, the equivalent quantifier-free formula is a conjunction of exterior terms in free scalar and multivector variables Z of the same form as (7.67):

$$\bigwedge_{1 \le i \le h+1} \bigwedge_{1 \le j \le k_i} \mathbf{g}'_{\mathbf{i},\mathbf{j}}(Z, \mathbf{Z}) = \mathbf{0}. \tag{7.71}$$

The next Section outlines very briefly computational methods available for solving polynomial equations in graded exterior algebras.

7.4 Symbolic Constraint Solving in Graded Exterior Algebras

The last step in the pattern solving algorithm SolPat deals with solving a system of equations related to the quantifier free problem formula. According to what has been said in the former Sections about pattern solving problems in graded exterior algebras, there are several types of systems of equations that may arise.

Recall from Section 7.3.1, the form of the final system of equations (7.49) for a pattern solving problem of type scalar:

$$\{\mathbf{g}_\mathbf{i}(Z) = \mathbf{0} \mid \mathbf{1} \le \mathbf{i} \le \mathbf{h} + \mathbf{1}\}.$$

This is also similar to the form of the final system of equations obtained from pattern solving problems of vector and mixed type, as in system (7.67),

$$\{\mathbf{g}_\mathbf{i}(Z, \mathbf{Z}) = \mathbf{0} \mid 1 \le i \le h + 1\}.$$

where the exterior terms are combinations of multivector constants. The constants are defined by a system of equations Ψ as in the pattern solving problem for modules over a ring discussed in Chapter 5. The solving method briefly sketched here is along the same lines as the one discussed in Section 5.4. The difference is that, in this setting, the linear span must be replaced by the ideal generated by the system of equations Ψ. Since the exterior algebra is a non-commutative ring, one must distinguish between the left and the right ideal. Accordingly, there is a right and a left Gröbner basis of the ideal generated by the polynomials in Ψ. There is a lot of work done in studying non commutative Gröbner basis, from the results of Mora (1986) to those of Kandri-Rody and Weispfenning (1990), of Hartley and Tuckey (1995), and of Stokes (1990), to name only a few. The reader may refer also to the classical textbook in non-commutative ring theory by Lam (1991).

One may observe the following, concerning system (7.49) of exterior equations with only scalar variables. Each polynomial $\mathbf{g}_\mathbf{i}(Z)$ must be in the ideal generated by a left of a right Gröbner basis of Ψ. Let G be the reduced left Gröbner basis of Ψ. Then, by the properties of Gröbner bases, each polynomial in the left ideal of Ψ (left) reduces to zero by G. This implies that also each polynomial $\mathbf{g}_\mathbf{i}(Z)$ must reduce to zero by G. Since the coefficients of the exterior monomials in $\mathbf{g}_\mathbf{i}(Z)$ must be scalar, a polynomial $\mathbf{g}_\mathbf{i}(Z)$ reduces to zero by G only if, for each exterior monomial $\mathbf{m}$ in $\mathbf{g}_\mathbf{i}(Z)$, there is a polynomial $\mathbf{p}$ in G whose leading monomial is $\mathbf{m}$. It is easy to show that, if $\mathbf{g}_\mathbf{i}(Z)$ reduces to zero, then the trailing terms introduced by the reduction must cancel out. If this is true, then it is possible to setup a system of scalar polynomial equations by equating the scalar coefficient of the monomial $\mathbf{m}$ in $\mathbf{g}_\mathbf{i}(Z)$ with the leading coefficient of the polynomial $\mathbf{p}$ in G. Hence, it remains to solve a system of scalar polynomial equations. Any computational method discussed previously can be applied to find ground term solutions for Z.

System of equations (7.67), in which also exterior variables are present, is more involved. The author has not yet investigated, due to lack of time, a computational method for finding ground term solutions in this case. Future work will concentrate on the aspect of solving such systems of exterior equations in graded exterior algebras.

7.5 Examples

One possible application of the results of this chapter is pattern solving in vector spaces where a vector product $\times$ is defined. Although these structures do not behave exactly like graded exterior algebras, it is not difficult to adapt the theorems to fit them. The major difficulty lies in the fact that vector multiplication, as it is known in vector analysis, is not associative. This problem can be side stepped when all exterior terms at most contain two subterms, so that the total grade is at most two. This is often the case in many examples since the equivalence:

$$\mathbf{u} \times (\mathbf{v} \times \mathbf{w}) = \mathbf{v} \cdot (\mathbf{u} \bullet \mathbf{w}) - \mathbf{w} \cdot (\mathbf{u} \bullet \mathbf{v})$$

where $\bullet$ is the scalar product while $\cdot$ is the usual multiplication by a scalar.

Example 7.1
This example is taken from a problem in Quantum Chemistry. The magnetic field produced by the apparent nuclear motion is

$$\mathbf{B} = \frac{Ze}{cr^3} \cdot \mathbf{v_N} \times \mathbf{r}$$

when viewed from the electron, where $\mathbf{v_N}$ is the apparent velocity of the nucleus. From the laboratory view, the magnetic field of the nucleus of the electron is

$$\mathbf{B} = \frac{\mathbf{E} \times \mathbf{v}}{\mathbf{c}} = \frac{(Ze \cdot \mathbf{r}/r^3) \times \mathbf{v}}{c}$$

where $\mathbf{v}$ is the actual velocity of the electron. What is the relation between $\mathbf{v}$ and $\mathbf{v_N}$?

The problem can be formalized as a pattern solving in the following way. Let the input system Γ be:

$$\{\mathbf{B} - \frac{Ze}{cr^3} \cdot \mathbf{v_N} \times \mathbf{r} = \mathbf{0}\}.$$

Since there appear a denominator, a side condition must be verified:

$$cr^3 \neq 0$$

before simplifying the denominator:

$$\{cr^3 \cdot \mathbf{B} - Ze \cdot \mathbf{v_N} \times \mathbf{r} = \mathbf{0}\}.$$

Let the solution pattern π:

$$\begin{aligned} \mathbf{v_N} &= x \cdot \mathbf{v}, \\ \mathbf{B} &= \tfrac{(Ze \cdot \mathbf{r}/r^3) \times \mathbf{v}}{c} \end{aligned}$$

The vector parameter is $\mathbf{v}$, while r is a constant defined elsewhere. After substitution of π in the problem Γ, the problem formula is:

$$\forall \mathbf{v}\ cr^3 \cdot \frac{(Ze \cdot \frac{\mathbf{r}}{r^3}) \times \mathbf{v}}{c} - Ze \cdot (x \cdot \mathbf{v}) \times \mathbf{r} = \mathbf{0} \wedge cr^3 \neq 0.$$

Observe that the denominators appearing in the solution pattern do not introduce any side condition beside the initial one. By simplifying the denominators:

$$\forall \mathbf{v}\ cr^3 \cdot (Ze \cdot \frac{\mathbf{r}}{\mathbf{r^3}}) \times \mathbf{v} - cZe \cdot (x \cdot \mathbf{v}) \times \mathbf{r} = \mathbf{0}.$$

$$\forall \mathbf{v}\ Ze \cdot \mathbf{r} \times \mathbf{v} - Ze \cdot (x \cdot \mathbf{v}) \times \mathbf{r} = \mathbf{0}.$$

Assuming the ordering on the exterior symbols: $\mathbf{v} < \mathbf{r}$, the formula can be reordered:

$$\forall \mathbf{v}\ Ze \cdot \mathbf{r} \times \mathbf{v} + Zex \cdot \mathbf{r} \times \mathbf{v} = \mathbf{0}.$$

and rewritten as:

$$\forall \mathbf{v}\ (Ze + Zex) \cdot \mathbf{r} \times \mathbf{v} = \mathbf{0}.$$

Elimination of the quantifier yields:

$$(Ze + Zex) \cdot \mathbf{r} = \mathbf{0}.$$

If the constant $\mathbf{r}$ is not zero, then it is equivalent to:

$$Ze + Zex = 0$$

can be easily solved for x:

$$x = -1.$$

The solution pattern can be instantiated to a solution, when $cr^3 \neq 0$ and assuming that $\mathbf{r} \neq \mathbf{0}$:

$$\mathbf{v_N} = (-1) \cdot \mathbf{v} = -\mathbf{v}.$$

■

7.6 Summary

This chapter has introduced pattern solving in the structures of graded exterior algebras. Thus, it establishes the possibility of using pattern solving in structures that are not commutative. This is very promising since many structures that model physical systems are not commutative.

The major effort done in this chapter is showing the fast elimination of quantifiers for a formula in a ring with zero divisors, as is the exterior algebra. This is possible for two reasons: the exterior algebra over a finite dimensional vector space is finite dimensional, and the scalar field is an infinite domain. A minor contribution is represented by the outline of an algorithm to solve the final system of exterior polynomial equations in the case where only scalar variables have to be solved.

Many problems are left for future work and could not possibly be tackled in this thesis. The aspect of solving systems of polynomial equations in the exterior algebra needs further investigation. Another line for future work is studying structures very close to exterior algebras, like differential algebras.

8

Conclusion

This thesis introduced a new approach, called pattern solving, for finding symbolic solutions of equational constraints. Pattern solving applies effectively to algebraic structures in which a fast, 'straightforward' elimination of universal quantifiers is possible. Starting from commutative rings, to modules over a ring, associative algebras over a field, and finally to graded exterior algebras over a vector space, the thesis addressed the necessary algebraic properties for easy elimination of universal quantifiers to be complete. Stepwise, it was shown that this is true in infinite integral domains, torsion-free modules over an infinite domain, finite dimensional division algebras over an infinite field and graded exterior algebras on an infinite scalar field.

These results are, by no means, the end of the story, rather they show a promising beginning. From the results obtained here, it is very likely that the method of pattern solving can be employed in very rich algebraic structures, typically arising from engineering and physics, where the computational performance of conventional symbolic constraint solving methods does not meet the expectations. Another very interesting topic will be to characterize the class of algebraic structures in which 'straightforward' elimination of universal quantifiers is complete.

Much in the same way as was done in the thesis, the more immediate future work is showing that pattern solving applies in more structures: starting from non-associative algebras as Lie algebras, and Jordan algebras, and continuing on to differential algebras. These algebraic structures often model real-world applications, where the initial motivation for developing pattern solving lies.

Some further work is also planned for solving the systems of equations produced by pattern solving in R-modules, see Section 5.4, and in graded exterior algebras, see Section 7.4. Related to solving the final system of equations, one may also think of investigating heuristic criteria to guide a "good" choice of the solution pattern, when nothing is known. This has been briefly mentioned in Section 4.4 and seems to be a very hard problem, at least theoretically.

Finally, one may also think of using the approach of pattern solving for dealing with general constraints, not only equations but also inequalities. This direction is again a totally new area which needs deep investigation.

Bibliography

Arnborg, A. and Tidén, E. (1985). Unification Problems with One-Sided Distributivity. In J.-P. Jouannaud, editor, *Proc. of the 1st International Conference on Rewriting Techniques and Applications*, volume 202 of *lncs*, pages 398–406, Dijon, France. sv.

Arnold, V. I. (1989). *Mathematical methods of classical mechanics*, volume 60 of *GTM*. Springer Verlag, second edition.

Baader, F. and Schulz, K. (1992). Unification in the union of disjoint equational theories: Combining decision procedures. In D. Kapur, editor, *Proceedings of the Eleventh International Conference on Automated Deduction (Saratoga Springs, NY)*, Berlin. Springer Verlag.

Baader, F. and Siekmann, J. H. (1994). *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 2, chapter Unification Theory. Oxford University Press.

Baur, W. (1976). Elimination of Quantifiers for Modules. *Israel Jornal of Mathemathics*, **25**, 64–70.

Becker, T. and Weispfenning, V. (1993). *Gröbner Bases: a Computational Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer–Verlag.

Berline, C. (1981). Rings which Admit Elimination of Quantifiers. *Journal of Symbolic Logic*, **46**(1), 56–58.

Bockmayr, A. (1987). A note on a canonical theory with undecidable unification and matching problem. *Journal of Automated Reasoning*, **3**, 379–381.

Bockmayr, A. (1989). On the decidability of the unification problem. In *Proceedings of the Third International Workshop on Unification*, pages 79–82.

Bockmayr, A. (1990a). Algebraic and logic aspects of unification. In *1st International Workshop on Word Equations and Related Topics*.

Bockmayr, A. (1990b). Model-theoretic aspects of unification. In *1st International Workshop on Word Equations and Related Topics*.

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal*. Ph.D. thesis, Universitat Innsbruck, Institut fur Mathematik. German.

Buchberger, B. and Loos, R. (1982). Algebraic simplification. In B. Buchberger, G. E. Collins, and R. Loos, editors, *Computer Algebra*, pages 11–43. Springer, Wien-New York.

Caprotti, O. (1993). Extending RISC-CLP(Real) to Handle Symbolic Functions. In A. Miola, editor, *DISCO '93: International Symposium on Design and Implementation of Symbolic Computation Systems*, Lecture Notes in Computer Science, Gmunden, Austria. Springer Verlag.

Cohn, P. M. (1989). *Algebra*. John Wiley & Sons, second edition.

Collins, G. E. (1975). Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In *Lecture Notes In Computer Science*, pages 134–183. Springer-Verlag, Berlin. Vol. 33.

Collins, G. E. and Hong, H. (1991). Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation*, **12**(3), 299–328.

Collins, G. E., Hong, H., and Buchberger, B. (1992). *SACLIB User's Guide*. Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria A-4040.

Cox, D., Little, J., and O'Shea, D. (1992). *Ideals, Varieties, and Algorithms*. Springer Verlag.

Dardano, U. (1996). Personal Communication.

den Dries, L. V. and Holly, J. (1992). Quantifier elimination for modules with scalar variables. *Annals of Pure and Applied Logic*, **57**, 161–179.

Dershowitz, N. and Jouannaud, J.-P. (1990). *Handbook of Theoretical Computer Science*, chapter Rewrite Systems. Elsevier Science Publishers.

Dershowitz, N. and Mitra, S. (1993). Higher-order and semantic unification. In *Proc. of the Thirteenth International Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 761 of *Lecture Notes in Computer Science*, pages 139–150, Bombay, India. Springer Verlag.

Dershowitz, N. and Mitra, S. (1995). Matching and Unification in Restricted Convergent Systems. Submitted for publication.

Gallier, J. and Snyder, W. (1990). Complete set of transformations for general E-unification. *Theoretical Computer Science*, **67**, 203–260.

Gallier, J. H. and Snyder, W. (1987). A general complete E-unification procedure. In P. Lescanne, editor, *Proceedings of the Second International Conference on Rewriting Techniques and Applications (Bordeaux, France)*, pages 192–203, Berlin. Springer Verlag.

Goguen, J. A. and Meseguer, J. (1992). Order-sorted algebra I: Equational deduction for multiple inheritance, overloading, exceptions and partial operations. *Theoretical Computer Science*, **105**(2), 217–273.

Graßmann, H. (1862). *Die Ausdehnungslehre*. Verlag von Th. Chr. Fr. Enslin.

Hartley, D. and Tuckey, P. (1995). Gröbner Bases in Clifford and Grassmann algebras. *Journal of Symbolic Computation*, **20**, 197–205.

Herbrand, J. (1930). Recherches sur la théorie de la démonstration. *Travaux de la Soc. des Sciences et des Letters de Varsovie*, **33**(128).

Hong, H. (1993). Risc-clp(real): Constraint logic programming over real numbers. In F. Benhamou and A. Colmerauer, editors, *Constraint Logic Programming: Selected Research*. MIT Press.

Hong, H., Liska, R., and Steinberg, S. (1996). Testing stability by quantifier elimination. *Journal of Symbolic Computation*. To appear.

Hsiang, J. and Jouannaud, J.-P. (1988). Complete sets of inference rules for E-unification. In C. Kirchner, editor, *Proceedings of the Second Unification Workshop*, Val d'Ajol, France. CRIN Report, Universite de Nancy, France.

Jacobson, N. (1974). *Basic Algebra I.* W. H. Freeman and Company, San Francisco.

Jacobson, N. (1980). *Basic Algebra II.* W. H. Freeman and Company, San Francisco.

Jouannaud, J.-P. and Kirchner, C. (1990). Solving equations in abstract algebras: A rule-based survey of unification. Technical Report 561, Université de Paris Sud, Orsay, France.

Jouannaud, J.-P. and Kirchner, C. (1991). Solving Equations in Abstract Algebras: A Rule-Based Survey of Unification. In J.-L. Lassez and G. Plotkin, editors, *Computational Logic. Essays in honour of Alan Robinson*, chapter 8, pages 257–321. MIT Press, Cambridge, (MA) USA.

Kandri-Rody, A. and Weispfenning, V. (1990). Non-commutative Gröbner Bases in Algebras of Solvable Type. *Journal of Symbolic Computation*, **9**, 1–26.

Kapur, D. and Lakshman, Y. N. (1992). *Symbolic and Numerical Computation for Artificial Intelligence*, chapter Elimination Methods: an Introduction, pages 45–87. Academic Press.

Keisler, H. J. (1977). *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*, chapter Fundamentals of Model Theory, pages 47–103. North Holland Publishing Company.

Kim, K. H. and Roush, F. W. (1993). Undecidability of Parametric Solutions of Polynomial Equations. *Proceedings of the American Mathematical Society*, **118**(2), 345–348.

Kirchner, C. (1984). A New Equational Unification Method: A generalization of Martelli–Montanari's Algorithm. In R. E. Shostak, editor, *7th International Conference on Automated Deduction*. Springer LNCS 170.

Lam, T. Y. (1991). *A First Course in Noncommutative Rings*, volume 131 of *Graduate Texts in Mathematics*. Springer Verlag.

Macintyre, A. (1983). The Word Problem for Division Rings. *Journal of Symbolic Logic*, **38**(3), 428–436.

Macintyre, A., McKenna, K., and van Den Dries, L. (1983). Elimination of Quantifiers in Algebraic Structures. *Advances in Mathematics*, **47**, 74–87.

Martelli, A. and Montanari, U. (1982). An Efficient Unification Algorithm. In *ACM Transactions on Programming Languages and Systems*, volume 4, pages 258–282.

Matijasevič, Y. (1970). Diophantine representation of recursively enumerable predicates. In *Actes du Congrès International des Mathématiciens*, volume 1, pages 235–238, Nice, France.

Meseguer, J., Goguen, J. A., and Smolka, G. (1990). Order-sorted unification. In C. Kirchner, editor, *Unification*. Academic Press.

Middeldorp, A. and Hamoen, E. (1994). Completeness Results for Basic Narrowing. *Applicable Algebra in Engineering, Communication and Computing*, **5**, 213–253.

Mitra, S. (1994). *Semantic Unification for Convergent Systems*. Ph.D. thesis, University of Illinois at Urbana-Champaign, Urbana, Illinois.

Mora, F. (1986). Gröbner bases for non-commutative polynomial rings. volume 229 of *LNCS*, pages 353–362. SV.

Narendran, P., Pfenning, F., and Statman, R. (1993). On the unification problem for cartesian closed categories. In M. Vardi, editor, *Eighth Annual IEEE Symposium on Logic in Computer Science*, pages 57–63, Montreal, Canada.

Nutt, W. (1991). The unification hierarchy is undecidable. *Journal of Automated Reasoning*, **7**(3), 369–382.

Pheidas, T. (1994). Extensions of Hilbert's Tenth Problem. *Journal of Symbolic Logic*, **59**(2), 372–397.

Robinson, J. (1949). Definability and Decision Problems in Arithmetic. *Journal of Symbolic Logic*, **14**, 98–114.

Rose, B. I. (1978). Rings which Admit Elimination of Quantifiers. *Journal of Symbolic Logic*, **43**(1), 92–112.

Schicho, J. (1995). *Rational Parametrization of Algebraic Surfaces*. Ph.D. thesis, RISC-Linz, Research Institute for Symbolic Computation.

Schmidt-Schauß, M. (1989). Combination of unification algorithms. *Journal of Symbolic Computation*, **8**.

Siekmann, J. (1989). Unification Theory. *Journal of Symbolic Computation*, **7**(3-4), 207–274. Special Issue on Unification, part one.

Smolka, G. (1989). *Logic Programming over Polymorphically Order-Sorted Types*. Ph.D. thesis, Universität Kaiserlautern.

Stokes, T. (1990). Gröbner bases in exterior algebra. *Journal of Automated Reasoning*, **6**, 233–250.

Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry*. Univ. of California Press, Berkeley, second edition.

Tarski, A. (1966). Equational Logic and Equational Theories of Algebras. Hannover.

Tung, S.-P. (1988). Decidable Sentences over Polynomial Rings. *Proceedings of the American Mathematical Society*, **102**(2), 382–388.

Tung, S.-P. (1990). Algorithms for Sentences over Integral Domains. *Annals of Pure and Applied Logic*, **47**(2), 189–197.

Tung, S.-P. (1995). Computational Complexity of Arithmetical Sentences. *Inform. Comput.*, **120**(2), 315–325.

van der Waerden, B. L. (1948). *Modern Algebra*, volume I. Ungar Publishing Company, New York.

Waldmann, U. (1989). Unification in Order-Sorted Signatures. Forschungsbericht 298, Universität Dortmund, Dortmund, Germany.

Whitehead, A. N. (1898). *A Treatise on Universal Algebras with Applications*. Cambridge University Press, Cambridge.