Lecture Notes

Algorithmic Quantifier Elimination

Thomas Sturm

CNRS, Inria, and the University of Lorraine, France
Max Planck Institute for Informatics and Saarland University, Germany

July 14, 2023

Contents

1 Introduction

1.1 Quantifier Elimination

Consider the real numbers $\mathbb{R}$ with the common arithmetic operations and order. The following formal statement φ asks whether or not one can find for all $x_1 \in \mathbb{R}$ some $x_2 \in \mathbb{R}$ such that a certain polynomial is greater than zero while another polynomial is less than or equal to zero:

$$\varphi = \forall x_1 \exists x_2 (x_1^2 + x_1 x_2 + y_2 > 0 \wedge x_1 + y_1 x_2^2 + y_2 \leq 0). \tag{1.1}$$

We have to expect that the answer is not "yes" or "no" but depends on the real values of the parameters y_1 and y_2. A quantifier elimination procedure computes $\varphi' = y_1 < 0 \wedge y_2 > 0$ as an answer, which formally satisfies the equivalence $\varphi \longleftrightarrow \varphi'$. The quantifier-free formula φ' has several advantages over the original formula φ. The set of all "true" choices for (y_1, y_2) for φ or, equivalently, φ' defines a binary relation on the real numbers. The quantifier-free definition φ' is much simpler and and allows easy efficient evaluation for given values of (y_1, y_2).

Consider more abstractly a formula ψ with parameters $y_1, \ldots, y_4$. The "true" choices for $(y_1, \ldots, y_4)$ geometrically describe a set of objects in real 4-space. The formula $\exists y_3 \exists y_4 (\psi)$ with parameters y_1, y_2 describes the projection of those objects onto the (y_1, y_2)-plane. Again, quantifier elimination provides intuitively and algorithmically simpler descriptions of both the original objects and the projected ones.

Quantifier elimination is possible in many interesting domains but not generally. Another positive example is the field of complex numbers, a negative example is the field of rational numbers. In some domains, quantifier elimination is possible only for a restricted class of formulas, e.g. for linear formulas over the ring of integers.

Direct applications of quantifier elimination in the literature include circuit design and error diagnosis, verification, hybrid control theory, geometric proving, computational geometry, motion planning, chemical reaction network theory, and systems biology. In applications in science and engineering, parameters typically correspond to quantities that are observable or measurable. In Automated Reasoning, quantifier elimination is used under the hood when algebraically theories are involved. Examples are superposition modulo theories and SMT solving. From a formal point of view, quantifier elimination provides a framework for a formally clean management of parametric settings.

1.2 History

1.2.1 Classical Algebra

In the field of algebra, elimination algorithms were historically concerned with the elimination of "variables" from "problems", which typically means elimination of existential quantifiers in

front of conjunctions of equations, sometimes admitting also inequalities or congruences. They date back to the 17th century with Descartes. Their heyday was in the 19th century and is associated with the names of Gauss, Budan, Fourier, Sturm, Bezout, Sylvester, Hermite, and Kronecker. At that time, algebra was surprisingly algorithmic, and generally mathematicians computed probably more than nowadays. It is handed down that Leibniz chaired so-called calculating committees and entered the room with the words "Lasset uns rechnen!" or using the Latin phrase "Calculemus!" At the end of the 19th century, algorithmic algebra had reached a level where proposed algorithmic techniques could hardly be applied to interesting problems sizes anymore, given that computer technology was not available yet. As a consequence, a new trend gradually prevailed in algebra that favored presumably more elegant non-constructive structural approaches over elaborate algorithmic methods. The title of van der Waerden's excellent textbook from 1931 coined the term Modern Algebra.

1.2.2 Mathematical Logic

Coinciding with the waning interest in algebra at the turn of the 20th century, elimination algorithms gained interest in the field of mathematical logic as a tool for solving decision problems. With the mathematically exact formulation of first-order logic, research aimed at decision procedures that algorithmically decided elementary statements in certain classes of mathematical structures, now featuring full quantification and a complete set of Boolean operations. From about 1915 on, a long series of positive results began, which contrasted strongly with the undecidability results for the ring of integers by Gödel in 1931.

Quantifier elimination procedures turned out to be the most important approach to decision procedures. They form a systematic methodological approach for elimination algorithms in the framework of elementary logic. Quantifier elimination procedures for specific classes of algebraic structures were found in the first half of the 20th century among others by Löwenheim, Langford, Szmielew, Presburger, Skolem, and Tarski. In the 2nd half of the 20th century many more such methods were found for increasingly complicated classes.

With the rapid progress in computer development, the question arose whether decision procedures could actually be applied practically. The probably earliest reference to a software implementation of a quantifier elimination procedure is a report by Davis to the US Army, which is dated August 1954. Davis had implemented Presburger's decision procedure for the linear theory of the integers from 1929, which we are going to discuss here as Theorem 8.6. Davis reported that he could automatically prove that $x + x$ is always an even number. His conclusions about the general potential of such implementations were quite pessimistic.

1.2.3 Symbolic Computation

With the development of complexity theory starting in the mid 1960s, research on the asymptotic complexity of quantifier elimination problems and methods gained interest. It turned out that most of the classical methods are in the worst case of such a high complexity that implementations would be of little use from a theoretical point of view. More precisely, existing procedures were typically not elementary recursive, meaning that their asymptotic worst-case complexity in terms of the input length n could not be bounded by functions in $O(2^n) \cup O(2^{2^n}) \cup \cdots$.

These complexity results stimulated the development of more efficient quantifier elimination methods. Cooper proposed an "only" triple exponential algorithm for linear integer arithmetic in 1972. Implementations of efficient quantifier elimination methods for the real numbers by Collins and his students started in around 1972 and continue to this day. Their method of Cylindrical Algebraic Decomposition is "only" double exponential in the input word length, which later turned out to be optimal for the problem. Their implementations played an important role in the comeback of algorithmic algebra as Computer Algebra, also called Symbolic Computation. Remarkably, after 50 years the software of Collins's school is still considered a reference implementation. It is freely available as Qepcad B.

During the 1980s research in algorithmic quantifier elimination diverged. One research line is concerned with the development of asymptotically fast algorithms, also taking into consideration more specific complexity parameters than the input word length, like coefficient sizes or degrees of polynomials. On the one hand, these works are very impressive with regard to their high mathematical level, which establishes a significant contribution to mathematics. On the other hand, most of the results have never been implemented because implementations would be correspondingly complex. In addition, there are arguments that the constants hidden in the big O notation of those complexity results are so large that implementation would not be interesting from a practical point of view.

Another research line more pragmatically focused on the implementation and application of quantifier elimination. This has led to specialized quantifier elimination procedures for certain classes of input. A prominent example are quantifier elimination procedures based on Virtual Substitution, developed by Weispfenning and his students for various domains, including the real numbers, p-adic numbers, and the linear theory of the integers. Virtual substitution methods are typically limited to formulas where the degree of the occurring terms does not exceed a certain bound. One principal advantage is that parameters, in contrast to quantified variables, do not significantly contribute to complexity. The work of Weispfenning's school resulted in the software package Redlog, which is freely distributed with the computer algebra system Reduce.

The commercial computer algebra system Mathematica features real quantifier elimination, and real quantifier elimination in Maple has been announced.

1.3 Scope and Plan of the Course

The course focuses on classical quantifier elimination results developed throughout the 20th century. It leaves out efficient procedures that have been developed after 1970, especially for Presburger Arithmetic and Real Closed Fields. Nevertheless, both these model classes are covered here. Since the mathematical arguments and techniques developed with the classical results and discussed here play a crucial role also in more modern approaches, the course material lays a solid foundation for further study.

Chapter 2 sketches various familiar mathematical situations where variables are eliminated. One goal is to approach QE by emphasizing finding conditions for solvability, as opposed to actually solving in the positive case. Formal representations with a separation of syntax and semantics are deliberately avoided in the hope that this lack of rigor will give the reader a sense of the usefulness of the principles developed in the following chapter.

Subsequently Chapter 3 then provides a systematic formal introduction to interpreted first-order logic with equality, with an emphasis on the strict separation of syntax and semantics.

Chapter 4 introduces the key concepts of quantifier elimination, completeness, and decidability and discusses the interrelationships.

After these preparations, we are ready in Chapter 5 to treat systematically a first set of QE procedures, namely for sets and ordered sets.

Chapter 6 adds further important notions such as elementary equivalence, substructures, substructure completeness as a semantic characterization of quantifier eliminability, and model completeness as a characterization of quantifier elimination down to to existential quantifiers.

Chapter 7 deals with quantifier elimination for different types of Abelian groups and ordered Abelian groups. For the unordered case we discuss torsion-free divisible Abelian groups and infinite divisible Abelian groups with p-torsion. Examples are the additive groups of the reals and of polynomials over the integers modulo a prime p, respectively. The ordered case includes, on the one hand, divisible ordered Abelian groups, for which the ordered additive group of the reals is a natural example. Here we present Fourier–Motzkin elimination as a quantifier elimination procedure and discuss its application to linear programming. On the other hand, we have discretely ordered Abelian groups in suitable extension languages. Here we present Presburger's original result as a quantifier elimination procedure and discuss linear integer programming as a use case. We also study quantifier eliminability and decidability of various extensions of Presburger Arithmetic.

Chapter 9 turns to quantifier elimination in fields. We focus on Tarski's procedure for algebraically closed fields, and conclude with negative results for the rational numbers.

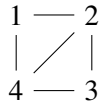
2 Examples for Elimination of Variables

In this introductory section, we address some familiar mathematical situations from the point of view of *elimination theory*. Each of our examples chooses a particular mathematical structure and makes a statement about that structure depending on parameters, which may take arbitrary values in the structure. We are looking for a "simple" condition on these parameters "in closed form" that is necessary and sufficient for the correctness of the statement made. In that course, all variables of the statement that are not parameters are "eliminated".

The obtained conditions are "simple" in the following sense. For any concrete choice of values of the parameters in the given structure, the validity or invalidity of the original statement shall be easy to decide automatically via evaluation of the obtained condition. By "closed form" we mean that the obtained condition is a finite object, which covers, in general, infinitely many possible values of the parameters.

2.1 Graphs and Sets

Example 2.1 (Constraints on a certain undirected graph)**.** Let G be the following undirected graph:



(2.1)

Let $a, b \in \{1, 2, 3, 4\}$. Consider the statement that the following is solvable for a node x in G:

$$x \text{ — } a \quad \text{and} \quad x \text{ — } b \quad \text{and} \quad \text{not} \quad a \text{ — } b. \tag{2.2}$$

This holds if and only if

$$a = b \quad \text{or} \quad \{a, b\} = \{1, 3\}. \tag{2.3}$$

Proof. Assume that (2.3) does not hold, i.e., $a \neq b$ and $\{a, b\} \neq \{1, 3\}$. Then it is easy to see by inspection of G that a — b. It follows that (2.2) cannot hold for any choice of x.

Conversely, assume that (2.3) holds. If $a = b$, then there is x in G such that $(a = b)$ — x, because G has no isolated vertices. Furthermore, we have not a — b, because G has no loops. If $\{a, b\} = \{1, 3\}$, then it is easy to see by inspection of G that not 1 — 3, and we can choose, e.g., $x = 2$. In both cases, (2.2) holds. ⌟

Example 2.2 (Set theory)**.** Let s be a non-empty set, and consider its *power set* $P = \mathscr{P}(s) = \{\, t \mid t \subseteq s \,\}$. Let $a, b \in P$. Consider the statement that the following is solvable for $x \in P$:

$$x \not\subseteq a \quad \text{and} \quad x \cap b = \varnothing. \tag{2.4}$$

This holds if and only if

$$a \cup b \neq s. \tag{2.5}$$

Proof. Assume that $x \in P$ such that (2.4) holds. From $x \not\subseteq a$ it follows that there is $y \in s$ with $y \in x$ but $y \notin a$. Using $x \cap b = \varnothing$ it follows that also $y \notin b$. Hence $y \notin a \cup b$.

Conversely Assume that (2.5) holds. Then $a \cup b \subsetneq s$. Thus there is $y \in s$ with $y \notin a \cup b$, i.e. $y \notin a$ and $y \notin b$. Choose $x = \{y\}$. ⌟

Generally, it is important to understand that our goal is not the computation of a suitable x but the computation of conditions for the existence of such an x in exclusively the parameters a and b using common set operations on P, including the constants $\varnothing$ and s.

2.2 Single Equations

Example 2.3 (One linear equation over $\mathbb{R}$)**.** Let $a, b \in \mathbb{R}$. Consider the following statement about x:

$$ax + b = 0. \tag{2.6}$$

It is easy to see that this is solvable for $x \in \mathbb{R}$ if and only if

$$a \neq 0 \quad \text{or} \quad b = 0. \tag{2.7}$$

The same holds in $\mathbb{Q}$ and $\mathbb{C}$ instead of $\mathbb{R}$.

Proof. Assume that (2.7) does *not* hold, i.e., $a = 0$ and $b \neq 0$. Then $ax + b = 0$ is equivalent to $b = 0$, which has no solution for x. Hence (2.6) does not hold either.

Conversely, assume that (2.7) holds. If $a \neq 0$ set $x = -b/a$. If $b = 0$ set $x = 0$. In either case x satisfies (2.6). ⌟

Example 2.4 (One quadratic equation over $\mathbb{R}$)**.** Let $a, b, c \in \mathbb{R}$. Consider the following statement about x:

$$ax^2 + bx + c = 0. \tag{2.8}$$

Carefully taking into account the possible vanishing of a, which reduces our problem to Example 2.3, and using the well-known solution formula for quadratic equations otherwise, this is solvable for $x \in \mathbb{R}$ if and only if

$$\big(a = 0 \quad \text{and} \quad (b \neq 0 \quad \text{or} \quad c = 0)\big) \quad \text{or} \quad \big(a \neq 0 \quad \text{and} \quad b^2 - 4ac \geq 0\big). \tag{2.9}$$

Condition (2.9) does not work over $\mathbb{C}$, where the order inequality makes no sense. It also does not work over $\mathbb{Q}$, where the square root does not always exist. As an exercise, find a concrete counterexample over $\mathbb{Q}$. ⌟

Recall that Tschirnhaus transformations can be used to get rid of quadratic summands in cubic equations. From that perspective the following example is more general than it might seem at first glance.

Example 2.5 (One cubic equation over $\mathbb{R}$)**.** Let $a, b, c \in \mathbb{R}$. Consider the following statement about x:

$$ax^3 + bx + c = 0. \tag{2.10}$$

This is solvable for $x \in \mathbb{R}$ if and only if

$$a \neq 0 \quad \text{or} \quad b \neq 0 \quad \text{or} \quad c = 0. \tag{2.11}$$

The same holds over $\mathbb{C}$ instead of $\mathbb{R}$, but not over $\mathbb{Z}$ or $\mathbb{Q}$.

The proof for $\mathbb{C}$ is a direct application of the fundamental theorem of algebra, which states that every non-zero univariate polynomial of degree n has, counted with multiplicity, exactly n roots. We leave the presentation of a counterexample for $\mathbb{Q}$ and the proof for $\mathbb{R}$ as an exercise. Due to the negative result for $\mathbb{Q}$, it is inevitable that the proof for $\mathbb{R}$ relies on certain properties of $\mathbb{R}$ that do not hold in $\mathbb{Q}$. ⌟

2.3 Systems of Linear Equations

Example 2.6 (Systems of univariate linear equations over $\mathbb{R}$)**.** Fix numbers $a_1, \ldots, a_m \in \mathbb{R}$ with $a_1 \neq 0$. Let $b_1, \ldots, b_m \in \mathbb{R}$. Consider the statement about x:

$$a_1 x + b_1 = 0 \quad \text{and} \quad \ldots \quad \text{and} \quad a_m x + b_m = 0. \tag{2.12}$$

This is solvable for $x \in \mathbb{R}$ if and only if

$$a_2 b_1 = a_1 b_2 \quad \text{and} \quad \ldots \quad \text{and} \quad a_m b_1 = a_1 b_m. \tag{2.13}$$

The same holds in any field K instead of $\mathbb{R}$.

Proof. Assume that (2.13) does not hold. Let $i \in \{2, \ldots, m\}$ such that $a_i b_1 \neq a_1 b_i$. If $a_i = 0$, then $b_i \neq 0$, and it follows that $a_i x + b_i = 0$ in (2.12) has no solution. If $a_i \neq 0$, then $x = -b_i/a_i$ is the only solution of $a_i x + b_i = 0$ in (2.12). Similarly $x = -b_1/a_1$ is the only solution of $a_1 x + b_1 = 0$ in (2.12). But our assumption $a_i b_1 \neq a_1 b_i$ is equivalent to $-b_1/a_1 \neq -b_i/a_i$. Hence (2.12) is not solvable $x \in \mathbb{R}$.

Conversely, assume that (2.13) holds. Set $x = -b_1/a_1$, which obviously solves the first equation $a_1 x + b_1 = 0$ in (2.12). Consider now any other equation in (2.12), i.e., $a_i x + b_i = 0$ for $i \in \{2, \ldots, m\}$. We know that $a_i b_1 = a_1 b_i$. If $a_i = 0$ then also $b_i = 0$, and our considered equation $a_i x + b_i = 0$ becomes trivial. Otherwise, we equivalently transform $a_i b_1 = a_1 b_i$ into $-b_i/a_i = -b_1/a_1 = x$, and we see that x solves our considered equation. Hence our x solves (2.12) ⌟

When interested in solvability with respect to several variables, like x_1, x_2, one can start with considering x_2 as a parameter, obtain an equivalent condition that still contains x_2 but not x_1 anymore, and from this subsequently derive another equivalent condition for the solvability with respect to x_2.

Example 2.7 (Systems of bivariate linear equations over $\mathbb{R}$)**.** Fix numbers $a_{11}, \dots, a_{m1}, a_{12}, \dots, a_{m2} \in \mathbb{R}$ with $a_{11} \neq 0$ and $a_{21}a_{12} - a_{11}a_{22} \neq 0$. Let $b_1, \dots, b_m \in \mathbb{R}$. Consider the following statement about x_1 and x_2:

$$a_{11}x_1 + a_{12}x_2 + b_1 = 0 \quad \text{and} \quad \dots \quad \text{and} \quad a_{m1}x_1 + a_{m2}x_2 + b_m = 0. \tag{2.14}$$

This is solvable for $x_1, x_2 \in \mathbb{R}$ if and only if

$$\begin{aligned} (a_{31}a_{12} - a_{11}a_{32})(a_{21}b_1 - a_{11}b_2) &= (a_{21}a_{12} - a_{11}a_{22})(a_{31}b_1 - a_{11}b_3) \quad \text{and} \\ &\vdots \\ \text{and} \quad (a_{m1}a_{11} - a_{11}a_{m2})(a_{21}b_1 - a_{11}b_2) &= (a_{21}a_{12} - a_{11}a_{22})(a_{m1}b_1 - a_{11}b_m). \end{aligned} \tag{2.15}$$

The same holds in any field K instead of $\mathbb{R}$.

Proof. Considering $x_2 \in \mathbb{R}$ as another parameter, system (2.14) can be rewritten as

$$a_{11}x_1 + (a_{12}x_2 + b_1) = 0 \quad \text{and} \quad \dots \quad \text{and} \quad a_{m1}x_1 + (a_{m2}x_2 + b_m) = 0. \tag{2.16}$$

This matches (2.12), and Example 2.6 states that this is solvable for $x_1 \in \mathbb{R}$ if and only if

$$\begin{aligned} a_{21}(a_{12}x_2 + b_1) &= a_{11}(a_{22}x_2 + b_2) \quad \text{and} \\ &\vdots \\ \text{and} \quad a_{m1}(a_{12}x_2 + b_1) &= a_{11}(a_{m2}x_2 + b_m). \end{aligned} \tag{2.17}$$

This can be equivalently rewritten as

$$\begin{aligned} (a_{21}a_{12} - a_{11}a_{22})x_2 + (a_{21}b_1 - a_{11}b_2) &= 0 \quad \text{and} \\ &\vdots \\ \text{and} \quad (a_{m1}a_{12} - a_{11}a_{m2})x_2 + (a_{m1}b_1 - a_{11}b_m) &= 0, \end{aligned} \tag{2.18}$$

which once more matches (2.12), and Example 2.6 states that this is solvable for $x_2 \in \mathbb{R}$ if and only if (2.15) holds. ⌟

Example 2.7 can be generalized to systems with an arbitrary number n of variables:

$$a_{11}x_1 + \cdots + a_{1n}x_n + b_1 = 0 \quad \text{and} \quad \dots \quad \text{and} \quad a_{m1}x_1 + \cdots + a_{mn}x_n + b_n = 0. \tag{2.19}$$

The coefficients a_{ij} form a real $m \times n$-Matrix $\mathbf{A}$, and the x_i and b_i form column vectors $\mathbf{x}$ and $\mathbf{b}$, respectively. In these terms, (2.19) can be more concisely rewritten as

$$\mathbf{A} \cdot \mathbf{x} = -\mathbf{b}. \tag{2.20}$$

In fact, one arrives at essentially Gaussian elimination generalized to parametric right hand sides $-\mathbf{b}$ of the equations.

2.4 Systems of Linear Inequalities

Example 2.8 (One linear inequality over $\mathbb{R}$)**.** Let $a, b \in \mathbb{R}$. Consider the following statement about x:

$$ax + b \leq 0. \tag{2.21}$$

It is easy to see that this is solvable for $x \in \mathbb{R}$ if and only if

$$a \neq 0 \quad \text{or} \quad b \leq 0. \tag{2.22}$$

The same holds in $\mathbb{Q}$ instead of $\mathbb{R}$. ⌟

Example 2.9 (Systems of univariate linear inequalities over $\mathbb{R}$)**.** Fix numbers $a_1, \ldots, a_m \in \mathbb{R}$ with $a_1, \ldots, a_k < 0 < a_{k+1}, \ldots, a_m$. Let $b_1, \ldots, b_m \in \mathbb{R}$. Consider the following statement about x:

$$a_1 x + b_1 \leq 0 \quad \text{and} \quad \ldots \quad \text{and} \quad a_m x + b_m \leq 0. \tag{2.23}$$

This is solvable for $x \in \mathbb{R}$ if and only if

$$a_j b_i - a_i b_j \leq 0 \qquad (1 \leq i \leq k, \quad k+1 \leq j \leq m). \tag{2.24}$$

The same holds in any ordered field K instead of $\mathbb{R}$.

Proof. Condition (2.23) can be equivalently rewritten as

$$-\frac{b_1}{a_1} \leq x \ \text{ and } \ \ldots \ \text{ and } \ -\frac{b_k}{a_k} \leq x \ \text{ and } \ x \leq -\frac{b_{k+1}}{a_{k+1}} \ \text{ and } \ \ldots \ \text{ and } \ x \leq -\frac{b_m}{a_m}. \tag{2.25}$$

It is not hard to see that this is equivalent to

$$-\frac{b_i}{a_i} \leq -\frac{b_j}{a_j} \qquad \big(i \in \{1, \ldots, k\}, \quad j \in \{k+1, \ldots, m\}\big). \tag{2.26}$$

Multiplication of the inequality in (2.26) by $a_i a_j < 0$ followed by addition of $a_j b_i$ yields $0 \geq a_j b_i - a_i b_j$. Hence (2.26) can be equivalently rewritten as (2.24). ⌟

Condition (2.24) should be read as a an informal logical conjunction, similarly to (2.23). There are two border cases in Example 2.9:

1. all $a_1, \ldots, a_m$ are positive, i.e., $k = m$;
2. all $a_1, \ldots, a_m$ are negative, i.e., $k = 0$.

In both these cases the list of conditions in (2.24) becomes empty. It is a common convention that such an empty condition is defined as "true", which is the neutral element of the logical conjunction.[1]

Inspection of the proof shows that the result can be generalized as follows. In (2.23) one can mix the *weak inequalities* "$\leq$" with *strict inequalities* "$<$". Accordingly, one puts the strict inequality in (2.24) whenever at least one of the involved i, j has the strict inequality in (2.23).

[1] Similarly, empty disjunctions are typically considered "false", empty sums are 0, empty products are 1, etc.

Similarly to our result for equations in Example 2.6 via Example 2.7, the result of Example 2.9 can be iterated for several variables $x_1, \ldots, x_n$ instead of x. This leads to a simple feasibility criterion for systems

$$\mathbf{A} \cdot \mathbf{x} \leq -\mathbf{b}. \tag{2.27}$$

With fixed values in $\mathbf{A}$ and parametric right hand sides $-\mathbf{b}$. The corresponding algorithm is known as Fourier–Motzkin Elimination.

We conclude our discussion of linear systems of equations and inequalities with an example over the integers $\mathbb{Z}$, which form an integral domain but not a field. For $x, y \in \mathbb{Z}$ we write $x \mid y$ if x *divides* y, i.e., if there is $z \in \mathbb{Z}$ such that $xz = y$.

Example 2.10 (Constraints in Presburger Arithmetic)**.** Let $a, b, c \in \mathbb{Z}$. Consider the following statement about x:

$$2x = a \quad \text{and} \quad b < x \quad \text{and} \quad x < c. \tag{2.28}$$

This is solvable for $x \in \mathbb{Z}$ if and only if

$$2 \mid a \quad \text{and} \quad 2b < a \quad \text{and} \quad a < 2c. \tag{2.29}$$

Proof. Assume that $x \in \mathbb{Z}$ such that (2.28) holds. This implies $2x = a$ and $2b < 2x < 2c$, which in turn implies

$$2x = a \quad \text{and} \quad 2b < a < 2c. \tag{2.30}$$

The constraint $2x = a$ admits only the formal solution $x = a/2$, which exists in $\mathbb{Z}$ if and only if $2 \mid a$. This yields (2.29).

Conversely, assume that (2.29) holds. We must show that there exists $x \in \mathbb{Z}$ such that (2.28) holds. Since $2 \mid a$, we can set $x = a/2 \in \mathbb{Z}$. Plugging into (2.28) yields

$$2(a/2) = a \quad \text{and} \quad b < a/2 < c, \tag{2.31}$$

where $2(a/2) = a$ obviously holds and $b < a/2 < c$ follows immediately from (2.29). ⌟

2.5 Universal Statements

All our examples so far were concerned with the *existence* of one or several elements x or x_i subject to parametric constraints. We conclude with an example where a given condition is required to hold *for all* x.

Example 2.11 (A universal condition on real inequalities)**.** Let $a, b \in \mathbb{R}$. Consider the statement that the following holds for all $x \in \mathbb{R}$:

$$2x - a \geq 0 \quad \text{or} \quad 3x + 2b + 1 < 0. \tag{2.32}$$

This holds if and only if

$$3a + 4b + 2 \leq 0. \tag{2.33}$$

Proof. We prove the, logically equivalent, contrapositive of our equivalence, which can be phrased as follows: The condition

$$-3x - 2b - 1 \leq 0 \quad \text{and} \quad 2x - a < 0 \tag{2.34}$$

is solvable for $x \in \mathbb{R}$ if and only if

$$3a + 4b + 2 < 0. \tag{2.35}$$

According to Example 2.9, a solution $x \in \mathbb{R}$ for (2.34) exists if and only if $0 > 2 \cdot (-2b - 1) - (-3) \cdot (-a) = 3a + 4b + 2$. ⌟

3 Interpreted First-order Logic

3.1 Languages and $\mathcal{L}$-Structures

An elementary *language* is a triplet $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$, where $\mathcal{F} \cap \mathcal{R} = \varnothing$ and $\sigma : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$. It fixes *function symbols* $f \in \mathcal{F}$ and *relation symbols* $R \in \mathcal{R}$ along with their *arities* σf and σR, respectively. One can shortly write $f^{(\sigma f)}$ and $R^{(\sigma R)}$ to annotate function and relation symbols with their arities. A function symbol $f^{(0)} \in \mathcal{F}$ is called a *constant symbol*. A language is *algebraic* if $\mathcal{R} = \varnothing$, and it is *relational* if $\mathcal{F} = \varnothing$.

A language is *finite* if $\mathcal{F} \cup \mathcal{R}$ is finite. There is a convenient notation for finite languages $\mathcal{L} = (\{f_1, \ldots, f_n\}, \{R_1, \ldots, R_m\}, \sigma)$ as follows:

$$\mathcal{L} = \left(f_1^{(\sigma f_1)}, \ldots, f_n^{(\sigma f_n)};\ R_1^{(\sigma R_1)}, \ldots, R_m^{(\sigma R_m)}\right). \tag{3.1}$$

Similarly, a language is *countable* if $\mathcal{F} \cup \mathcal{R}$ is countable. For families $(f_i)_{i\in\mathbb{N}}$ and $(R_j)_{j\in\mathbb{N}}$ we can write $\mathcal{L} = (f_0^{(\sigma f_0)}, f_1^{(\sigma f_1)}, \ldots;\ R_0^{(\sigma R_0)}, R_1^{(\sigma R_1)}, \ldots)$. The annotations of the arities can be omitted when they are obvious from the choice of the function and relation symbols.

Example 3.1 (Finite language)**.** The *language of ordered rings* is given by

$$\mathcal{L}_{Rings_<} = (\{0, 1, +, -, \cdot\}, \{<\}, \sigma) \tag{3.2}$$

with $\sigma(0) = 0$, $\sigma(1) = 0$, $\sigma(+) = 2$, $\sigma(-) = 1$, $\sigma(\cdot) = 2$, $\sigma(<) = 2$. There are constant symbols 0 and 1. The language is neither algebraic nor relational. Since the language is finite, it can be written as

$$\mathcal{L}_{Rings_<} = (0^{(0)}, 1^{(0)}, +^{(2)}, -^{(1)}, \cdot^{(2)};\ <^{(2)}) \tag{3.3}$$

or even shorter as $\mathcal{L}_{Rings_<} = (0, 1, +, -, \cdot;\ <)$. ⌟

Consider languages $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ and $\mathcal{L}' = (\mathcal{F}', \mathcal{R}', \sigma')$. We write $\mathcal{L} \subseteq \mathcal{L}'$ if $\mathcal{F} \subseteq \mathcal{F}'$, $\mathcal{R} \subseteq \mathcal{R}'$, and $\sigma = \sigma'|_{\mathcal{F}\cup\mathcal{R}}$. We then call $\mathcal{L}$ is a *sublanguage* of $\mathcal{L}'$, and we call $\mathcal{L}'$ an *extension language* of $\mathcal{L}$.

Example 3.2 (Sublanguage and extension language)**.** The *language of rings* is a sublanguage of the language of ordered rings, and thus the language of ordered rings is an extension language of the language of rings:

$$\mathcal{L}_{Rings} = (0, 1, +, -, \cdot) \subseteq (0, 1, +, -, \cdot\ ; <) = \mathcal{L}_{Rings_<}. \tag{3.4}$$

The language of rings is algebraic. ⌟

We are now going to define semantics, which gives a meaning to the function and relation symbols of our languages. Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$. An *$\mathcal{L}$-structure* is a triplet $\mathbf{A} = (A, \imath_{\mathcal{F}}, \imath_{\mathcal{R}})$, where $A \neq \varnothing$ is called the *universe* of $\mathbf{A}$. The *interpretation* $\imath_{\mathcal{F}}$ assigns to each $f^{(n)} \in \mathcal{F}$ a function $f^{\mathbf{A}} : A^n \to A$. The functions $f^{\mathbf{A}}$ are called the *functions of* $\mathbf{A}$. For constant symbols $f^{(0)} \in \mathcal{F}$ we identify the constant function $f^{\mathbf{A}}$ with its value and call $f^{\mathbf{A}} \in A$ a *constant* of $\mathbf{A}$. The *interpretation* $\imath_{\mathcal{R}}$ assigns to each $R^{(n)} \in \mathcal{R}$ a function $R^{\mathbf{A}} : A^n \to \{\top, \bot\}$. The symbols $\top$ and $\bot$ stand for "true" and "false", respectively. We agree that there is an ordering $\top > \bot$. The functions $R^{\mathbf{A}}$ are called the *relations of* $\mathbf{A}$.

If $\mathcal{L}$ is algebraic, then $\mathbf{A}$ is called an *$\mathcal{L}$-algebra*. If $\mathcal{L}$ is relational, then $\mathbf{A}$ is called a *relational $\mathcal{L}$-structure*. An $\mathcal{L}$-structure $\mathbf{A}$ is called *finite* if its universe A is finite.

Example 3.3 ($\mathbb{R}$ as an ordered ring)**.** There is a natural $\mathcal{L}_{Rings_<}$-structure $\mathbf{R} = (\mathbb{R}, \imath_{\mathcal{F}}, \imath_{\mathcal{R}})$ with the real numbers as its universe. We define

$$\imath_{\mathcal{F}}(0) = 0^{\mathbf{R}} \in \mathbb{R}, \quad \imath_{\mathcal{F}}(1) = 1^{\mathbf{R}} \in \mathbb{R}, \tag{3.5}$$

where $0^{\mathbf{R}}$ and $1^{\mathbf{R}}$ are the real numbers 0 and 1, respectively,

$$\imath_{\mathcal{F}}(+) = +^{\mathbf{R}} : \mathbb{R}^2 \to \mathbb{R}, \quad \imath_{\mathcal{F}}(-) = -^{\mathbf{R}} : \mathbb{R} \to \mathbb{R}, \quad \imath_{\mathcal{F}}(\cdot) = \cdot^{\mathbf{R}} : \mathbb{R}^2 \to \mathbb{R}, \tag{3.6}$$

where $+^{\mathbf{R}}$, $-^{\mathbf{R}}$, and $\cdot^{\mathbf{R}}$ are the usual real addition, additive inverse, and multiplication, respectively, and

$$\imath_{\mathcal{R}}(<) = <^{\mathbf{R}} : \mathbb{R}^2 \to \{\top, \bot\} \quad \text{with} \quad <^{\mathbf{R}}(x, y) = \begin{cases} \top & \text{if } x < y \text{ in } \mathbb{R} \\ \bot & \text{else.} \end{cases} \tag{3.7}$$

$\mathcal{L}_{Rings_<}$ is a finite language but $\mathbf{R}$ is an infinite $\mathcal{L}_{Rings_<}$-structure. ⌟

For finite languages $\mathcal{L}$ as in (3.1), $\mathcal{L}$-structures can be more conveniently written in the form

$$\mathbf{A} = (A;\ \omega_1, \ldots, \omega_n;\ \varrho_1, \ldots, \varrho_m), \tag{3.8}$$

where $(\omega_i : A^{\sigma f_i} \to A) = \imath_{\mathcal{F}}(f_i)$ and $(\varrho_j : A^{\sigma R_j} \to \{\bot, \top\}) = \imath_{\mathcal{R}}(R_j)$. The definition of the functions ω_i and ϱ_j can typically be derived from their names in combination with the specified universe A.

Example 3.4. (i) The following is the $\mathcal{L}_{Rings_<}$-structure defined in Example 3.3:

$$(\mathbb{R};\ 0, 1, +, -, \cdot;\ <). \tag{3.9}$$

(ii) The *language of monoids* is defined as $\mathcal{L}_{Monoids} = (*^{(2)}, e^{(0)})$. The following are examples for $\mathcal{L}_{Monoids}$-structures:

$$(\mathbb{Z};\ +, 0), \quad (\mathbb{Q};\ \cdot, 1), \quad (\{\texttt{'a'}, \ldots, \texttt{'z'}\}^*;\ \circ, \varepsilon), \quad (\mathscr{P}(\mathbb{C});\ \cap, \mathbb{C}). \tag{3.10}$$

The following is an $\mathcal{L}_{Monoids}$-structure as well, where the function $/ : (\mathbb{Q}\setminus\{0\})^2 \to \mathbb{Q}\setminus\{0\}$ denotes division:

$$(\mathbb{Q} \setminus \{0\};\ /, 1). \tag{3.11}$$

The $\mathcal{L}_{Monoids}$-structures in (3.10) are indeed monoids. The one in (3.11), in contrast, is not a monoid, because division is not associative. All $\mathcal{L}_{Monoids}$-structures are algebras. ⌟

The examples in 3.4(ii) illustrate that the short notation (3.8) for $\mathcal{L}$-structures is not suitable and should not be used for implicitly specifying the language $\mathcal{L}$ along with an $\mathcal{L}$-structure.

Consider languages $\mathcal{L}' = (\mathcal{F}', \mathcal{R}', \sigma') \subseteq (\mathcal{F}, \mathcal{R}, \sigma) = \mathcal{L}$, and let $\mathbf{A} = (A, \iota_{\mathcal{F}}, \iota_{\mathcal{R}})$ be an $\mathcal{L}$-structure. Restricting the interpretations $\iota_{\mathcal{F}}$ and $\iota_{\mathcal{R}}$ of $\mathbf{A}$ to $\mathcal{F}'$ and $\mathcal{R}'$, respectively, yields an $\mathcal{L}'$-structure

$$\mathbf{A}|_{\mathcal{L}'} = (A, \iota_{\mathcal{F}}|_{\mathcal{F}'}, \iota_{\mathcal{R}}|_{\mathcal{R}'}). \tag{3.12}$$

We call $\mathbf{A}|_{\mathcal{L}'}$ the *$\mathcal{L}'$-restriction* of $\mathbf{A}$, and we call $\mathbf{A}$ an *$\mathcal{L}$-expansion* of $\mathbf{A}|_{\mathcal{L}'}$. Note that $\mathbf{A}$ and $\mathbf{A}|_{\mathcal{L}'}$ have the same universe A.

Example 3.5. Recall from (3.4) that $\mathcal{L}_{Rings} \subseteq \mathcal{L}_{Rings_<}$, and recall from Example 3.3 and (3.9) that the ordered ring of real numbers $\mathbf{R} = (\mathbb{R};\ 0, 1, +, -, \cdot;\ <)$ is an $\mathcal{L}_{Rings_<}$-structure. The $\mathcal{L}_{Rings}$-restriction of $\mathbf{R}$ yields the ring of real numbers $\mathbf{R}|_{\mathcal{L}_R} = (\mathbb{R};\ 0, 1, +, -, \cdot)$. The $\mathcal{L}_{Rings_<}$-structure $(\mathbb{R};\ 0, 1, +, -, \cdot;\ >)$ is another $\mathcal{L}_{Rings_<}$-expansion of $(\mathbb{R};\ 0, 1, +, -, \cdot)$. Notice that $(\mathbb{R};\ 0, 1, +, -, \cdot;\ >)$ is an $\mathcal{L}_{Rings_<}$-structure but not an ordered ring, such as (3.11) was not a monoid. ⌟

3.2 Terms and Term Functions

We fix a set $\mathcal{X} = \{\boxed{(}, \boxed{)}, \boxed{,}\}$ of *special symbols*, and we fix an infinite set $\mathcal{V}$ of *variables*. Let $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ be a language. The *alphabet* of $\mathcal{L}$ is given by $\mathcal{Z} = \mathcal{X} \cup \mathcal{V} \cup \mathcal{F} \cup \mathcal{R}$. As usual, $\mathcal{Z}^*$ is the set of all finite words over $\mathcal{Z}$, and $\varepsilon \in \mathcal{Z}^*$ is the empty word, and $|w|$ is the word length of w. We assume that $\mathcal{X}$, $\mathcal{V}$, $\mathcal{F}$, $\mathcal{R}$, are pairwise disjoint. Furthermore, no composite word in $\mathcal{Z}^*$ equals any alphabet character.[1]

The set $\mathcal{T} \subseteq \mathcal{Z}^*$ of $\mathcal{L}$-terms is recursively defined as follows:

(i) If $x \in \mathcal{V}$, then $x \in \mathcal{T}$.

(ii) If $f^{(0)} \in \mathcal{F}$, then $f \in \mathcal{T}$.

(iii) If $f^{(n)} \in \mathcal{F}$ with $n > 0$ and $t_1, \ldots, t_n \in \mathcal{T}$, then $f\boxed{(}t_1\boxed{,}\ldots\boxed{,}t_n\boxed{)} \in \mathcal{T}$.

The definition of terms uses exclusively prefix notation. We admit infix notation as a shorthand with common function symbols such as $+$, $\cdot$ in $\mathcal{L}_{Rings}$. One may also save parentheses following common rules like the precedence of multiplication over addition in situations where this is adequate.

Recall that $\mathcal{L}$-structures $\mathbf{A}$ interpret function symbols of $\mathcal{L}$ as functions in their universe A. We want to use terms to define further such functions.

Example 3.6 (Motivation of extended terms)**.** Consider the following definition of a polynomial function:

$$f(x, y, z) = x^2 + 2xy - 5y. \tag{3.13}$$

On the right hand side of the defining equation we have $x^2 + 2xy - 5y$, which is a convenient notation for an $\mathcal{L}_{Rings}$-term. On the left hand side of that equation, the extension (x, y, z) defines a mapping between argument positions and variables of the defining term. The variable z does not occur in the defining term, but it is relevant for obtaining a function with arity 3. ⌟

[1] One way to state this formally is that $z \notin (\mathcal{Z} \setminus \{z\})^*$ for all $z \in \mathcal{Z}$.

Let $t \in \mathcal{T}$. We denote by $\mathcal{V}(t)$ the finite set of variables occurring in t. Let $x_1, \ldots, x_n \in \mathcal{V}$ be such that $\mathcal{V}(t) \subseteq \{x_1, \ldots, x_n\}$. Then $(t, (x_1, \ldots, x_n)) \in \mathcal{T} \times \mathcal{V}^n$ is an *extended term*, which we shortly write as $t(x_1, \ldots, x_n)$. Let $\mathbf{A}$ be an $\mathcal{L}$-structure. Then $t(x_1, \ldots, x_n)$ specifies a *term function* $t^{\mathbf{A}} : A^n \to A$, which is recursively defined at $(a_1, \ldots, a_n) \in A^n$ as follows:

(i) If $t = x_i$, then $t^{\mathbf{A}}(a_1, \ldots, a_n) = a_i$.

(ii) If $t = f^{(0)} \in \mathcal{F}$, then $t^{\mathbf{A}}(a_1, \ldots, a_n) = f^{\mathbf{A}}$.

(iii) If $t = f(t_1, \ldots, t_m)$ with $f^{(m)} \in \mathcal{F}$ and $t_1, \ldots, t_m \in \mathcal{T}$, then

$$t^{\mathbf{A}}(a_1, \ldots, a_n) = f^{\mathbf{A}}\big(t_1^{\mathbf{A}}(a_1, \ldots, a_n), \ldots, t_m^{\mathbf{A}}(a_1, \ldots, a_n)\big) \tag{3.14}$$

using extended terms $t_1(x_1, \ldots, x_n), \ldots, t_m(x_1, \ldots, x_n)$.

Lemma 3.7 (Term functions under restriction and expansion)**.** Let $\mathcal{L}' \subseteq \mathcal{L}$, let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $t(x_1, \ldots, x_n)$ be an extended $\mathcal{L}'$-term. Then $t^{\mathbf{A}|_{\mathcal{L}'}} = t^{\mathbf{A}}$.

Proof. Let $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$. We show by induction on $|t|$ that $t^{\mathbf{A}|_{\mathcal{L}'}}(\mathbf{a}) = t^{\mathbf{A}}(\mathbf{a})$. Let $|t| = 1$. Then $t = x_i \in \mathcal{V}$ or t is a constant symbol. If $t \in \mathcal{V}$, then $t \in \{x_1, \ldots, x_n\}$, say $t = x_i$, and it follows that $t^{\mathbf{A}|_{\mathcal{L}'}}(\mathbf{a}) = a_i = t^{\mathbf{A}}(\mathbf{a})$. If t is a constant symbol from $\mathcal{L}'$, then $t^{\mathbf{A}|_{\mathcal{L}'}}(\mathbf{a}) = t^{\mathbf{A}} = t^{\mathbf{A}}(\mathbf{a})$. Let now $|t| > 1$. Then there are $f^{(m)} \in \mathcal{F}'$ and extended $\mathcal{L}'$-terms $t_1(x_1, \ldots, x_n)$, $\ldots, t_m(x_1, \ldots, x_n)$ such that $t = f(t_1, \ldots, t_m)$. We know that $t_j^{\mathbf{A}|_{\mathcal{L}'}} = t_j^{\mathbf{A}}$ by induction hypothesis. It follows that $t^{\mathbf{A}|_{\mathcal{L}'}}(\mathbf{a}) = f^{\mathbf{A}|_{\mathcal{L}'}}(t_1^{\mathbf{A}|_{\mathcal{L}'}}(\mathbf{a}), \ldots, t_m^{\mathbf{A}|_{\mathcal{L}'}}(\mathbf{a})) = f^{\mathbf{A}}(t_1^{\mathbf{A}}(\mathbf{a}), \ldots, t_m^{\mathbf{A}}(\mathbf{a})) = t^{\mathbf{A}}(\mathbf{a})$. □

3.3 First-order Formulas and Their Characteristic Functions

Let $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ be a language. We fix another set of special symbols

$$\mathcal{Y} = \big\{ \boxed{=}, \boxed{\texttt{true}}, \boxed{\texttt{false}}, \boxed{\neg}, \boxed{\wedge}, \boxed{\vee}, \boxed{\rightarrow}, \boxed{\leftrightarrow}, \boxed{\exists}, \boxed{\forall} \big\}, \tag{3.15}$$

which are spelled out as "equals", "true", "false", "not", "and", "or", "implies", "implies in both directions", "exists", and "for all", respectively. We use the alphabet $\bar{\mathcal{Z}} = \mathcal{Y} \cup \mathcal{Z}$ from now on. We again assume that $\mathcal{Y} \cap \mathcal{Z} = \varnothing$ and that no composite word in $\bar{\mathcal{Z}}^*$ equals any alphabet character.

The set $\mathcal{A} \subseteq \bar{\mathcal{Z}}^*$ of *atomic $\mathcal{L}$-formulas* is defined as follows:

(i) *Equations:* If $t_1, t_2 \in \mathcal{T}$, then $t_1 \boxed{=} t_2 \in \mathcal{A}$.

(ii) *Predicates:* If $R^{(m)} \in \mathcal{R}$ and $t_1, \ldots, t_m \in \mathcal{T}$, then $R \boxed{(} t_1 \boxed{,} \ldots \boxed{,} t_m \boxed{)} \in \mathcal{A}$.

Let $\alpha \in \mathcal{A}$, let $\mathcal{V}(\alpha)$ be the finite set of variables occurring in α, let $\mathcal{V}(\alpha) \subseteq \{x_1, \ldots, x_n\}$, and set $\mathbf{x} = (x_1, \ldots, x_n)$. Let $\mathbf{A}$ be an $\mathcal{L}$-structure. Then the *extended atomic formula* $\alpha(\mathbf{x})$ specifies a *characteristic function* $\alpha^{\mathbf{A}} : A^n \to \{\top, \bot\}$, which is defined at $\mathbf{a} \in A^n$ as follows:

(i) If φ is an equation $t_1 = t_2$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = \top$ if and only if $t_1^{\mathbf{A}}(\mathbf{a}) = t_2^{\mathbf{A}}(\mathbf{a})$ using extended terms $t_1(\mathbf{x}), t_2(\mathbf{x})$.

(ii) If φ is a predicate $R(t_1, \ldots, t_m)$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = R^{\mathbf{A}}(t_1^{\mathbf{A}}(\mathbf{a}), \ldots, t_m^{\mathbf{A}}(\mathbf{a}))$ using extended terms $t_1(\mathbf{x}), \ldots, t_m(\mathbf{x})$.

Note that the equality sign $\boxed{=}$ never appears as a relation symbol in $\mathcal{R}$, while equations are always available as atomic formulas.

The set $\mathcal{FOF} \subseteq \bar{\mathcal{Z}}^*$ of *first-order $\mathcal{L}$-formulas*, or simply $\mathcal{L}$-formulas for short, is recursively defined as follows:

(i) *Atomic formulas:* If $\varphi_1 \in \mathcal{A}$, then $\varphi_1 \in \mathcal{FOF}$.

(ii) *Truth values:* $\boxed{\texttt{false}}, \boxed{\texttt{true}} \in \mathcal{FOF}$.

(iii) *Negations:* If $\varphi_1 \in \mathcal{FOF}$, then $\boxed{\neg}\,\boxed{(}\,\varphi_1\,\boxed{)} \in \mathcal{FOF}$.

(iv) *Conjunctions:* If $\varphi_1, \ldots, \varphi_n \in \mathcal{FOF}$, then $\boxed{(}\,\varphi_1\,\boxed{)}\,\boxed{\wedge}\,\ldots\,\boxed{\wedge}\,\boxed{(}\,\varphi_n\,\boxed{)} \in \mathcal{FOF}$.

(v) *Disjunctions:* If $\varphi_1, \ldots, \varphi_n \in \mathcal{FOF}$, then $\boxed{(}\,\varphi_1\,\boxed{)}\,\boxed{\vee}\,\ldots\,\boxed{\vee}\,\boxed{(}\,\varphi_n\,\boxed{)} \in \mathcal{FOF}$.

(vi) *Implications:* If $\varphi_1, \varphi_2 \in \mathcal{FOF}$, then $\boxed{(}\,\varphi_1\,\boxed{)}\,\boxed{\rightarrow}\,\boxed{(}\,\varphi_2\,\boxed{)} \in \mathcal{FOF}$.

(vii) *Biconditionals:* If $\varphi_1, \varphi_2 \in \mathcal{FOF}$, then $\boxed{(}\,\varphi_1\,\boxed{)}\,\boxed{\leftrightarrow}\,\boxed{(}\,\varphi_2\,\boxed{)} \in \mathcal{FOF}$.

(viii) *Existentially quantified formulas:* If $\varphi_1 \in \mathcal{FOF}$, $x \in \mathcal{V}$, then $\boxed{\exists}\,x\,\boxed{(}\,\varphi_1\,\boxed{)} \in \mathcal{FOF}$.

(ix) *Universally quantified formulas:* If $\varphi_1 \in \mathcal{FOF}$, $x \in \mathcal{V}$, then $\boxed{\forall}\,x\,\boxed{(}\,\varphi_1\,\boxed{)} \in \mathcal{FOF}$.

The set of *literals* is defined using only rules (i) and (iii). A *positive literal* is an atomic formula and a *negative literal* is a negated atomic formula. The set of *quantifier-free formulas* is recursively defined using only rules (i)–(vii).

The following words occurring in the definition of $\mathcal{FOF}$ are called *logical operators*:

$$\boxed{=},\quad \boxed{\texttt{true}},\quad \boxed{\texttt{false}},\quad \boxed{\neg},\quad \boxed{\wedge},\quad \boxed{\vee},\quad \boxed{\rightarrow},\quad \boxed{\leftrightarrow},\quad \boxed{\exists}\,x,\quad \boxed{\forall}\,x. \tag{3.16}$$

The logical operators $\boxed{\exists}\,x$ and $\boxed{\forall}\,x$ are called *quantifiers*. The *quantifier symbols* $\boxed{\exists}$ and $\boxed{\forall}$ are not logical operators or quantifiers by themselves. For saving parentheses we agree that the logical infix operators take precedence from strongest to weakest as follows:

$$\boxed{=} \;\succ\; \boxed{\wedge} \;\succ\; \boxed{\vee} \;\succ\; \boxed{\rightarrow} \;\succ\; \boxed{\leftrightarrow}. \tag{3.17}$$

Furthermore, implication is *right associative*, which means that $\varphi_1 \longrightarrow \varphi_2 \longrightarrow \varphi_3$ stands for $\varphi_1 \longrightarrow (\varphi_2 \longrightarrow \varphi_3)$. We allow infix notation of common relation symbols $R^{(2)} \in \mathcal{R}$ as a shorthand, which then have the same precedence as equality.

An *occurrence* of a variable $x \in \mathcal{V}$ in a first-order formula φ is defined as an occurrence inside a term within φ, in contrast to an occurrence after a quantifier symbol. An occurrence of x within a subformula $\exists x(\psi)$ or $\forall x(\psi)$ of φ is called a *bound occurrence* of x; all other occurrences of x in φ are called *free occurrences* . We define $\mathcal{V}_{\text{free}}(\varphi)$ and $\mathcal{V}_{\text{bound}}(\varphi)$ as the sets of variables with free and bound occurrences in φ, respectively. The set of all variables occurring in φ is $\mathcal{V}(\varphi) = \mathcal{V}_{\text{free}}(\varphi) \cup \mathcal{V}_{\text{bound}}(\varphi)$.

Example 3.8 (Free and bound occurrences of variables)**.**

1. Let $\mathcal{L}_1 = (0, 1, +, -^{(1)}, \cdot, |\_|^{(1)}, f^{(1)}; <)$ and consider the first-order formula

$$\varphi_1 \;=\; \forall\varepsilon(0 < \varepsilon \longrightarrow \exists\delta(0 < \delta \wedge \forall x(|x - x_0| < \delta \longrightarrow |f(x) - f(x_0)| < \varepsilon))). \tag{3.18}$$

   We have $\mathcal{V}_{\text{free}}(\varphi_1) = \{x_0\}$, $\mathcal{V}_{\text{bound}}(\varphi_1) = \{\delta, \varepsilon, x\}$, and $\mathcal{V}(\varphi_1) = \{\delta, \varepsilon, x, x_0\}$.

2. Let $\mathcal{L}_2 = (f^{(1)}, g^{(2)})$ and consider the first-order formula:

$$\varphi_2 \;=\; \neg\, w = y \longrightarrow \forall x \exists y \forall z (f(x) = g(w, y)). \tag{3.19}$$

   We have $\mathcal{V}_{\text{free}}(\varphi_2) = \{w, y\}$, $\mathcal{V}_{\text{bound}}(\varphi_2) = \{x, y\}$, and $\mathcal{V}(\varphi_2) = \{w, x, y\}$. Notice that $\mathcal{V}_{\text{free}}(\varphi_2) \cap \mathcal{V}_{\text{bound}}(\varphi_2) \neq \emptyset$, since there is both a free and a bound occurrence of y in φ_2. Furthermore, the variable z does not occur in φ_2 at all. ⌟

Let $\mathcal{V}_{\text{free}}(\varphi) \subseteq \{x_1, \ldots, x_n\}$ and set $\mathbf{x} = (x_1, \ldots, x_n)$. Let $\mathbf{A}$ be an $\mathcal{L}$-structure. Then the *extended first-order formula* $\varphi(\mathbf{x})$ specifies a *characteristic function* $\varphi^{\mathbf{A}} : A^n \to \{\top, \bot\}$, which is recursively defined at $\mathbf{a} \in A^n$ as follows:

(i) The case of an atomic formula φ has been discussed above.

(ii) $\text{TRUE}^{\mathbf{A}}(\mathbf{a}) = \top$ and $\text{FALSE}^{\mathbf{A}}(\mathbf{a}) = \bot$ using extended formulas $\text{TRUE}(\mathbf{x})$ and $\text{FALSE}(\mathbf{x})$.

(iii) If $\varphi = \neg(\varphi_1)$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = \top$ if and only if $\varphi_1^{\mathbf{A}}(\mathbf{a}) = \bot$ using the extended formula $\varphi_1(\mathbf{x})$.

(iv) If $\varphi = (\varphi_1) \wedge \cdots \wedge (\varphi_m)$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = \min\{\varphi_1^{\mathbf{A}}(\mathbf{a}), \ldots, \varphi_m^{\mathbf{A}}(\mathbf{a})\}$ using extended formulas $\varphi_1(\mathbf{x}), \ldots, \varphi_m(\mathbf{x})$.

(v) If $\varphi = (\varphi_1) \vee \cdots \vee (\varphi_m)$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = \max\{\varphi_1^{\mathbf{A}}(\mathbf{a}), \ldots, \varphi_m^{\mathbf{A}}(\mathbf{a})\}$ using extended formulas $\varphi_1(\mathbf{x}), \ldots, \varphi_m(\mathbf{x})$.

(vi) If $\varphi = (\varphi_1) \longrightarrow (\varphi_2)$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = \top$ if and only if $\varphi_1^{\mathbf{A}}(\mathbf{a}) \leq \varphi_2^{\mathbf{A}}(\mathbf{a})$ using extended formulas $\varphi_1(\mathbf{x})$ and $\varphi_2(\mathbf{x})$.

(vii) If $\varphi = (\varphi_1) \longleftrightarrow (\varphi_2)$, then $\varphi^{\mathbf{A}}(\mathbf{a}) = \top$ if and only if $\varphi_1^{\mathbf{A}}(\mathbf{a}) = \varphi_2^{\mathbf{A}}(\mathbf{a})$ using extended formulas $\varphi_1(\mathbf{x})$ and $\varphi_2(\mathbf{x})$.

(viii) If $\varphi = \exists x(\varphi_1)$, then $\varphi_1^{\mathbf{A}}(\mathbf{a}) = \max\{\, \varphi_1^{\mathbf{A}}(\mathbf{a}, a) \in \{\top, \bot\} \mid a \in A \,\}$ using the extended formula $\varphi_1(\mathbf{x}, x)$.

(ix) If $\varphi = \forall x(\varphi_1)$, then $\varphi_1^{\mathbf{A}}(\mathbf{a}) = \min\{\, \varphi_1^{\mathbf{A}}(\mathbf{a}, a) \in \{\top, \bot\} \mid a \in A \,\}$ using the extended formula $\varphi_1(\mathbf{x}, x)$.

Lemma 3.9 (Formulas under restriction and expansion)**.** Let $\mathcal{L}' \subseteq \mathcal{L}$, let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $\varphi(x_1, \ldots, x_n)$ be an extended $\mathcal{L}'$-formula. Then $\varphi^{\mathbf{A}|_{\mathcal{L}'}} = \varphi^{\mathbf{A}}$.

Proof. Induction on the length of φ. Compare Lemma 3.7. □

If $\mathcal{V}_{\text{free}}(\varphi) = \varnothing$, then we call φ a *sentence*. Assume that $\mathcal{V}_{\text{free}}(\varphi) = \{x_1, \ldots, x_n\}$. The *existential closure* $\underline{\exists}\,\varphi$ of φ is defined as the sentence $\exists x_1 \ldots \exists x_n \varphi$. Similarly, the *universal closure* $\underline{\forall}\,\varphi$ of φ is defined as $\forall x_1 \ldots \forall x_n \varphi$. Existential and universal closure are uniquely determined up to the order of the quantifiers added, and modifying that order would not change the constant characteristic functions $(\underline{\exists}\,\varphi)^{\mathbf{A}}$ and $(\underline{\forall}\,\varphi)^{\mathbf{A}}$.

3.4 Models and Axioms

Let $\mathbf{A}$ be an $\mathcal{L}$-structure, let $\varphi(\mathbf{x})$ be an extended $\mathcal{L}$-formula with $\mathbf{x} \in \mathcal{V}^n$, and let $\mathbf{a} \in A^n$. If $\varphi^{\mathbf{A}}(\mathbf{a}) = \top$, then we write $\mathbf{A} \vDash \varphi(\mathbf{a})$, and we say that φ *holds* in $\mathbf{A}$ at $\mathbf{a}$. If $\mathbf{A} \vDash \varphi(\mathbf{a})$ for all $\mathbf{a} \in A^n$, then we write $\mathbf{A} \vDash \varphi$, and we say that φ holds in $\mathbf{A}$.

The definition of $\mathbf{A} \vDash \varphi$ does not depend on the chosen extension $\mathbf{x}$. Therefore, it can be generalized to sets Φ of formulas and classes $\mathfrak{A}$ of $\mathcal{L}$-structures: $\mathbf{A} \vDash \Phi$ if $\mathbf{A} \vDash \varphi$ for all $\varphi \in \Phi$. Similarly, $\mathfrak{A} \vDash \varphi$ if $\mathbf{A} \vDash \varphi$ for all $\mathbf{A} \in \mathfrak{A}$, and $\mathfrak{A} \vDash \Phi$ if $\mathbf{A} \vDash \varphi$ for all $\mathbf{A} \in \mathfrak{A}$ and all $\varphi \in \Phi$. Finally, we shortly write $\nvDash$ when the corresponding model relation does not hold.

Example 3.10 (Model relations)**.** Consider the language $\mathcal{L}_{Rings}$ of rings, and consider $\mathbf{R} = (\mathbb{R};\ 0, 1, +, -, \cdot)$ and $\mathbf{Z} = (\mathbb{Z};\ 0, 1, +, -, \cdot)$.

1. Let φ_1 be the $\mathcal{L}_{Rings}$-formula $\neg\, x = 0 \longrightarrow \exists y(x \cdot y = 1)$. Then $\mathbf{R} \vDash \varphi_1$ but $\mathbf{Z} \nvDash \varphi_1$. Nevertheless, using the extended formula $\varphi_1(x)$, we have, e.g., $\mathbf{Z} \vDash \varphi_1(-1)$.

2. Let φ_2 be the the universal closure $\forall x \varphi_1$. By definition, we have for every $\mathcal{L}_{Rings}$-structure $\mathbf{A}$ that $\mathbf{A} \vDash \varphi_2$ if and only if $\mathbf{A} \vDash \varphi_1$. In particular, $\mathbf{R} \vDash \varphi_2$ and $\mathbf{Z} \nvDash \varphi_2$. We have $\mathcal{V}_{\text{free}}(\varphi_2) = \varnothing$, and $\varphi_2(x)$ is an extended formula. However, $\mathbf{Z} \nvDash \varphi_2(-1)$.

3. We have $\mathbf{R} \vDash \varphi_1(\sqrt{2})$. The corresponding statement with $\mathbf{Z}$ in place of $\mathbf{R}$ is meaningless because $\sqrt{2} \notin \mathbb{Z}$.

4. $\{\mathbf{R},\ \mathbf{Z}\} \vDash \{x + (y + z) = (x + y) + z,\ x + y = y + x,\ x + 0 = x,\ x + -x = 0\}$ ⌟

Let Φ be a set of $\mathcal{L}$-formulas. If there exists an $\mathcal{L}$-structure $\mathbf{A}$ such that $\mathbf{A} \vDash \Phi$, then we say that Φ is *satisfiable*. If $\mathbf{A} \vDash \Phi$ for all $\mathcal{L}$-structures $\mathbf{A}$, then we write $\vDash \Phi$, and we say that Φ is *valid*. The same definitions apply to a single formula φ instead of Φ. For a single formula φ it is easy to see that φ is valid if and only if $\neg\varphi$ is unsatisfiable, and φ is satisfiable if and only if $\neg\varphi$ is not valid.

Example 3.11 (Satisfiability and Validity)**.** Consider φ_1, φ_2 as in Example 3.10. Both φ_1 and φ_2 are satisfiable but not valid. The same holds for $\{\varphi_1, \varphi_2\}$. We will discuss a large number of valid formulas in Section 3.6. ⌟

If $\mathbf{A}$ is an $\mathcal{L}$-structure such that $\mathbf{A} \vDash \Phi$, then we say that $\mathbf{A}$ is a *model* of Φ. The class $\mathrm{Mod}(\Phi) = \{\, \mathbf{A} \mid \mathbf{A} \vDash \Phi \,\}$ is the *model class* of Φ.

A class $\mathfrak{A}$ of $\mathcal{L}$-structures is *elementary* if there exists a set Ξ of $\mathcal{L}$-formulas such that $\mathfrak{A} = \mathrm{Mod}(\Xi)$. We then call Ξ an *axiomatization* of $\mathfrak{A}$, and we call the elements of Ξ *axioms*.

Example 3.12 (Axiomatizations of rings and fields)**.** Consider the language $\mathcal{L}_{Rings}$ and define the axioms of rings and the axioms of fields:

$$\begin{aligned}\Xi_{Rings} \;=\; &\{x + (y + z) = (x + y) + z,\ x + y = y + x,\ x + 0 = x,\ x + -x = 0,\\ &x \cdot (y \cdot z) = (x \cdot y) \cdot z,\ x \cdot y = y \cdot x,\ x \cdot 1 = x,\\ &x \cdot (y + z) = (x \cdot y) + (x \cdot z)\},\\ \Xi_{Fields} \;=\; &\Xi_{Rings} \cup \{\neg\, 1 = 0,\ \neg\, x = 0 \longrightarrow \exists y(x \cdot y = 1)\}.\end{aligned} \tag{3.20}$$

These axioms axiomatize the class *Rings* = Mod(Ξ_{Rings}) of all rings and the class *Fields* = Mod(Ξ_{Fields}) of all fields as $\mathcal{L}_{Rings}$-structures, respectively. ⌟

In the language $\mathcal{L}_{Rings}$ we can use arbitrary non-zero integers within terms as shorthands for $1 + \cdots + 1$ and $-(1 + \cdots + 1)$. Furthermore, we allow ourselves to use *big operators* for the convenient notation of conjunctions and disjunctions. Our formal framework developed so far allows a concise reformulation of Example 2.7:

Example 3.13 (Systems of bivariate linear equations revisited)**.** Choose the language $\mathcal{L}_{Rings}$ and consider the following formulas:

$$\begin{aligned}\varphi &= a_{11} \neq 0 \wedge a_{21}a_{12} - a_{11}a_{22} \neq 0 \wedge \\ &\qquad \exists x_1 \exists x_2 \bigwedge_{i=1}^{m} a_{i1}x_1 + a_{i2}x_2 + b_i = 0, \\ \varphi' &= a_{11} \neq 0 \wedge a_{21}a_{12} - a_{11}a_{22} \neq 0 \wedge \\ &\qquad \bigwedge_{i=3}^{m} (a_{i1}a_{11} - a_{11}a_{i2})(a_{21}b_1 - a_{11}b_2) = (a_{21}a_{12} - a_{11}a_{22})(a_{i1}b_1 - a_{11}b_i).\end{aligned} \tag{3.21}$$

Then *Fields* $\models \varphi \longleftrightarrow \varphi'$. In particular $(\mathbb{R};\ 0, 1, +, -, \cdot) \models \varphi \longleftrightarrow \varphi'$. ⌟

3.5 Substitution

Fix a language $\mathcal{L}$. A *substitution* is a map $\theta : \mathcal{V} \to \mathcal{T}$ with $\theta(x) = x$ for almost all $x \in \mathcal{V}$. We shortly write $\theta = [t_1/x_1, \ldots, t_n/x_n]$ with $x_i \in \mathcal{V}$ pairwise distinct and $t_i \in \mathcal{T}$, and use postfix notation. A substitution θ induces a map $\theta : \mathcal{T} \to \mathcal{T}$. We recursively define $t\theta$ for $t \in \mathcal{T}$:

(i) If $t \in \mathcal{V} \setminus \{x_1, \ldots, x_n\}$, then $t\theta = t$.

(ii) If $t = x_i$, then $t\theta = t_i$.

(iii) If $t = f^{(0)} \in \mathcal{F}$, then $t\theta = t$.

(iv) If $t = f(u_1, \ldots, u_m)$ with $f^{(m)} \in \mathcal{F}$ and $u_1, \ldots, u_m \in \mathcal{T}$, then $t\theta = f(u_1\theta, \ldots, u_m\theta)$.

Example 3.14 (Substitution into terms)**.** Consider $\mathcal{L} = (f^{(3)}, g^{(1)})$. Then

1. $f\big(x, g(y), g(g(z))\big)\big[f(x, y, z)/x, z/y, x/z\big] = f\big(f(x, y, z), g(z), g(g(x))\big)$
2. $f\big(x, g(y), g(g(z))\big)\big[f(x, y, z)/x\big]\big[z/y, x/z\big] = f\big(f(x, z, x), g(z), g(g(x))\big)$. ⌟

Lemma 3.15 (Semantics of term substitution)**.** Consider an $\mathcal{L}$-structure $\mathbf{A}$ and a substitution $\theta = [t_1/x_1, \ldots, t_n/x_n]$. Choose $\mathbf{y} \in \mathcal{V}^m$ such that $t_1(\mathbf{y}), \ldots, t_n(\mathbf{y})$ are extended $\mathcal{L}$-terms and let $\mathbf{a} \in A^m$. Let t be another $\mathcal{L}$-term with $\mathcal{V}(t) \subseteq \{x_1, \ldots, x_n\}$. Then $t(x_1, \ldots, x_n)$ and $t\theta(\mathbf{y})$ are extended $\mathcal{L}$-terms and $t\theta^{\mathbf{A}}(\mathbf{a}) = t^{\mathbf{A}}\big(t_1^{\mathbf{A}}(\mathbf{a}), \ldots, t_n^{\mathbf{A}}(\mathbf{a})\big)$. □

Going further, a substitution $\theta[t_1/x_1, \ldots, t_n/x_n]$ induces a map $\theta : \mathcal{FOF} \to \mathcal{FOF}$, where some care must be taken in order to obtain a result on the semantics similar to Lemma 3.15. We define $\mathcal{V}_x(\theta) = \{x_1, \ldots, x_n\}$, $\mathcal{V}_t(\theta) = \mathcal{V}(t_1) \cup \cdots \cup \mathcal{V}(t_n)$, and $\mathcal{V}(\theta) = \mathcal{V}_x(\theta) \cup \mathcal{V}_t(\theta)$. For $\varphi \in \mathcal{FOF}$ we define $\mathcal{V}_q(\varphi)$ as the set of variables appearing in quantifiers within φ, and we recursively define $\varphi\theta$ as follows:

(i) $(u_1 = u_2)\theta = (u_1\theta = u_2\theta)$ and $R(u_1, \ldots, u_m)\theta = R(u_1\theta, \ldots, u_m\theta)$,

(ii) $\mathrm{TRUE}\,\theta = \mathrm{TRUE}$ and $\mathrm{FALSE}\,\theta = \mathrm{FALSE}$,

(iii) $(\neg\varphi_1)\theta = \neg(\varphi_1\theta)$,

(iv) $\big(\varphi_1 \wedge \cdots \wedge \varphi_m\big)\theta = (\varphi_1\theta \wedge \cdots \wedge \varphi_m\theta)$,

(v) $\big(\varphi_1 \vee \cdots \vee \varphi_m\big)\theta = (\varphi_1\theta \vee \cdots \vee \varphi_m\theta)$,

(vi) $\big(\varphi_1 \longrightarrow \varphi_2\big)\theta = (\varphi_1\theta \longrightarrow \varphi_2\theta)$,

(vii) $\big(\varphi_1 \longleftrightarrow \varphi_2\big)\theta = (\varphi_1\theta \longleftrightarrow \varphi_2\theta)$.

(viii) Consider $(\exists x\varphi_1)\theta$. Choose $x' \in \mathcal{V}$ such that $x' \notin \mathcal{V}(\theta) \cup \mathcal{V}(\varphi_1) \cup \mathcal{V}_q(\varphi_1)$ and define a modified substitution $\theta' : \mathcal{V} \to \mathcal{T}$ with $\theta'(x) = x'$ and $\theta'(v) = \theta(v)$ for $v \in \mathcal{V} \setminus \{x\}$. Then $(\exists x\varphi_1)\theta = \exists x'(\varphi_1\theta')$.

(ix) $(\forall x\varphi_1)\theta = \forall x'(\varphi_1\theta')$ with x' and θ' as in (viii).

Due to the non-deterministic choice of x', the substitution result is not uniquely determined. However, all possible results have the same semantics. In practice, one avoids the renaming of bound variables in (viii) and (ix) whenever possible.

Example 3.16 (Substitution into first-order formulas)**.** Consider $\mathcal{L}_{Rings}$.

1. $\big(x = a \wedge \exists x(ax + b = 0)\big)\big[b + 1/a\big] = \big(x = b + 1 \wedge \exists x'((b + 1)x' + b = 0)\big)$,
2. $\big(x = a \wedge \exists x(ax + b = 0)\big)\big[b + 1/x\big] = \big(b + 1 = a \wedge \exists x'(ax' + b = 0)\big)$,
3. $\big(x = a \wedge \exists x(ax + b = 0)\big)\big[x + 1/a\big] = \big(x = x + 1 \wedge \exists x'((x + 1)x' + b = 0)\big)$. ⌟

Lemma 3.17 (Semantics of first-order substitution)**.** Consider an $\mathcal{L}$-structure $\mathbf{A}$ and a substitution $\theta = [t_1/x_1, \ldots, t_n/x_n]$. Choose $\mathbf{y} \in \mathcal{V}^m$ such that $t_1(\mathbf{y}), \ldots, t_n(\mathbf{y})$ are extended $\mathcal{L}$-terms and let $\mathbf{a} \in A^m$. Let φ be an $\mathcal{L}$-formula with $\mathcal{V}_{\mathrm{free}}(\varphi) \subseteq \{x_1, \ldots, x_n\}$. Then $\varphi(x_1, \ldots, x_n)$ and $\varphi\theta(\mathbf{y})$ are extended $\mathcal{L}$-formulas and $\mathbf{A} \vDash \varphi\theta(\mathbf{a})$ if and only if $\mathbf{A} \vDash \varphi\big(t_1^{\mathbf{A}}(\mathbf{a}), \ldots, t_n^{\mathbf{A}}(\mathbf{a})\big)$. □

Corollary 3.18. *Consider an $\mathcal{L}$-structure $\mathbf{A}$. Let φ_1, φ_2 be $\mathcal{L}$-formulas, and let θ be a substitution. If $\mathbf{A} \vDash \varphi_1 \longleftrightarrow \varphi_2$ then $\mathbf{A} \vDash \varphi_1\theta \longleftrightarrow \varphi_2\theta$.* □

3.6 Entailment and Semantic Equivalence

Let φ_1, φ_2 be $\mathcal{L}$-formulas. If $\mathbf{A}$ is an $\mathcal{L}$-structure and $\mathbf{A} \models \varphi_1 \longrightarrow \varphi_2$, then we say that φ_1 *entails* φ_2 in $\mathbf{A}$, and we call φ_2 a *logical consequence* of φ_1 in $\mathbf{A}$. The same definition applies to classes $\mathfrak{A}$ of $\mathcal{L}$-structures instead of $\mathbf{A}$. If φ_1 entails φ_2 in all $\mathcal{L}$-structures, i.e. $\models \varphi_1 \longrightarrow \varphi_2$, then we simply say that φ_1 entails φ_2.

If $\mathbf{A}$ is an $\mathcal{L}$-structure and $\mathbf{A} \models \varphi_1 \longleftrightarrow \varphi_2$, then we say that φ_1 and φ_2 are *equivalent* in $\mathbf{A}$. The same definition applies to classes $\mathfrak{A}$ of $\mathcal{L}$-structures instead of $\mathbf{A}$. If φ_1 and φ_2 are equivalent in all $\mathcal{L}$-structures, i.e. $\models \varphi_1 \longleftrightarrow \varphi_2$, then we say that φ_1 and φ_2 are *semantically equivalent*.

Lemma 3.19 (Characterization of semantic equivalence)**.** Consider a language $\mathcal{L}$. Let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let φ_1, φ_2 be $\mathcal{L}$-formulas. Then the following are equivalent:

(i) φ_1 and φ_2 are equivalent in $\mathbf{A}$, i.e. $\mathbf{A} \models \varphi_1 \longleftrightarrow \varphi_2$;

(ii) φ_1 and φ_2 entail each other in $\mathbf{A}$, i.e. $\mathbf{A} \models \varphi_1 \longrightarrow \varphi_2$ and $\mathbf{A} \models \varphi_2 \longrightarrow \varphi_1$;

(iii) φ_1 and φ_2 have the same semantics in $\mathbf{A}$, i.e. $\varphi_1^{\mathbf{A}} = \varphi_2^{\mathbf{A}}$.

In particular, φ_1 and φ_2 are semantically equivalent if and only if φ_1 has the same semantic as φ_2 in all $\mathcal{L}$-structures. □

Lemma 3.20 (Propositional semantic equivalences)**.** Let $\mathcal{L}$ be a language, and let φ_1, φ_2, φ_3 be $\mathcal{L}$-formulas. Then the following semantic equivalences hold:

involution:	$\models$	$\neg\neg\varphi_1$	$\longleftrightarrow$	φ_1
neutral elements:	$\models$	$\varphi_1 \wedge \mathrm{TRUE}$	$\longleftrightarrow$	φ_1
	$\models$	$\varphi_1 \vee \mathrm{FALSE}$	$\longleftrightarrow$	φ_1
definiteness:	$\models$	$\varphi_1 \vee \mathrm{TRUE}$	$\longleftrightarrow$	TRUE
	$\models$	$\varphi_1 \wedge \mathrm{FALSE}$	$\longleftrightarrow$	FALSE
tertium non datur:	$\models$	$\varphi_1 \wedge \neg\varphi_1$	$\longleftrightarrow$	FALSE
	$\models$	$\varphi_1 \vee \neg\varphi_1$	$\longleftrightarrow$	TRUE
commutativity:	$\models$	$\varphi_1 \wedge \varphi_2$	$\longleftrightarrow$	$\varphi_2 \wedge \varphi_1$
	$\models$	$\varphi_1 \vee \varphi_2$	$\longleftrightarrow$	$\varphi_2 \vee \varphi_1$
associativity:	$\models$	$\varphi_1 \wedge (\varphi_2 \wedge \varphi_3)$	$\longleftrightarrow$	$(\varphi_1 \wedge \varphi_2) \wedge \varphi_3$
	$\models$	$\varphi_1 \vee (\varphi_2 \vee \varphi_3)$	$\longleftrightarrow$	$(\varphi_1 \vee \varphi_2) \vee \varphi_3$
distributivity:	$\models$	$\varphi_1 \wedge (\varphi_2 \vee \varphi_3)$	$\longleftrightarrow$	$(\varphi_1 \wedge \varphi_2) \vee (\varphi_1 \wedge \varphi_3)$
	$\models$	$\varphi_1 \vee (\varphi_2 \wedge \varphi_3)$	$\longleftrightarrow$	$(\varphi_1 \vee \varphi_2) \wedge (\varphi_1 \vee \varphi_3)$
idempotence:	$\models$	$\varphi_1 \wedge \varphi_1$	$\longleftrightarrow$	φ_1
	$\models$	$\varphi_1 \vee \varphi_1$	$\longleftrightarrow$	φ_1
absorption:	$\models$	$\varphi_1 \wedge (\varphi_2 \vee \varphi_1)$	$\longleftrightarrow$	φ_1
	$\models$	$\varphi_1 \vee (\varphi_2 \wedge \varphi_1)$	$\longleftrightarrow$	φ_1

de Morgan's laws:	$\models$	$\neg(\varphi_1 \wedge \varphi_2)$	$\longleftrightarrow$	$\neg\varphi_1 \vee \neg\varphi_2$	
	$\models$	$\neg(\varphi_1 \vee \varphi_2)$	$\longleftrightarrow$	$\neg\varphi_1 \wedge \neg\varphi_2$	
contrapositive:	$\models$	$(\varphi_1 \longrightarrow \varphi_2)$	$\longleftrightarrow$	$(\neg\varphi_2 \longrightarrow \neg\varphi_1)$	
	$\models$	$(\varphi_1 \longleftrightarrow \varphi_2)$	$\longleftrightarrow$	$(\neg\varphi_2 \longleftrightarrow \neg\varphi_1)$	
reduction to $\neg$, $\vee$, $\wedge$:	$\models$	$(\varphi_1 \longleftrightarrow \varphi_2)$	$\longleftrightarrow$	$(\varphi_1 \longrightarrow \varphi_2) \wedge (\varphi_2 \longrightarrow \varphi_1)$	
	$\models$	$(\varphi_1 \longrightarrow \varphi_2)$	$\longleftrightarrow$	$(\neg\varphi_1 \vee \varphi_2)$	□

Lemma 3.21 (Semantic equivalences with quantifiers)**.** Let $\mathcal{L}$ be a language, and let φ_1, φ_2 be $\mathcal{L}$-formulas. Then the following semantic equivalences hold:

trivial elimination:	$\models$	$\exists x(\varphi_1)$	$\longleftrightarrow$	φ_1	if $x \notin \mathcal{V}_{\text{free}}(\varphi_1)$
	$\models$	$\forall x(\varphi_1)$	$\longleftrightarrow$	φ_1	if $x \notin \mathcal{V}_{\text{free}}(\varphi_1)$
commutation of quantifiers:	$\models$	$\exists x \exists y(\varphi)$	$\longleftrightarrow$	$\exists y \exists x(\varphi)$	
	$\models$	$\forall x \forall y(\varphi)$	$\longleftrightarrow$	$\forall y \forall x(\varphi)$	
negation of quantifiers:	$\models$	$\neg\exists x(\varphi_1)$	$\longleftrightarrow$	$\forall x(\neg\varphi_1)$	
	$\models$	$\neg\forall x(\varphi_1)$	$\longleftrightarrow$	$\exists x(\neg\varphi_1)$	
compatibility with $\vee$, $\wedge$:	$\models$	$\exists x(\varphi_1 \vee \varphi_2)$	$\longleftrightarrow$	$\exists x(\varphi_1) \vee \exists x(\varphi_2)$	
	$\models$	$\forall x(\varphi_1 \wedge \varphi_2)$	$\longleftrightarrow$	$\forall x(\varphi_1) \wedge \forall x(\varphi_2)$	
miniscoping:	$\models$	$\exists x(\varphi_1 \wedge \varphi_2)$	$\longleftrightarrow$	$\exists x(\varphi_1) \wedge \varphi_2$	if $x \notin \mathcal{V}_{\text{free}}(\varphi_2)$
	$\models$	$\forall x(\varphi_1 \vee \varphi_2)$	$\longleftrightarrow$	$\forall x(\varphi_1) \vee \varphi_2$	if $x \notin \mathcal{V}_{\text{free}}(\varphi_2)$
renaming:	$\models$	$\exists x(\varphi_1)$	$\longleftrightarrow$	$\exists y(\varphi_1[y/x])$	if $y \notin \mathcal{V}_{\text{free}}(\varphi_1)$
	$\models$	$\forall x(\varphi_1)$	$\longleftrightarrow$	$\forall y(\varphi_1[y/x])$	if $y \notin \mathcal{V}_{\text{free}}(\varphi_1)$

□

It is noteworthy that quantifiers do not commute in general. Furthermore, disjunctions are compatible with existential quantifiers and conjunctions are compatible with universal quantifiers but not vice versa.

Lemma 3.22 (Entailments with quantifiers)**.** Let $\mathcal{L}$ be a language, and let φ_1, φ_2 be $\mathcal{L}$-formulas. Then the following entailments hold:

commutation of $\exists x$ *and* $\forall y$:	$\models$	$\exists x \forall y(\varphi_1)$	$\longrightarrow$	$\forall y \exists x(\varphi_1)$	
compatibility with $\vee$, $\wedge$:	$\models$	$\exists x(\varphi_1 \wedge \varphi_2)$	$\longrightarrow$	$\exists x(\varphi_1) \wedge \exists x(\varphi_2)$	
	$\models$	$\forall x(\varphi_1) \vee \forall x(\varphi_2)$	$\longrightarrow$	$\forall x(\varphi_1 \vee \varphi_2)$	□

The converse entailments in Lemma 3.22 do not hold:

Example 3.23 (Some counterexamples)**.** Consider the $(0^{(0)})$-structure $\mathbf{R} = (\mathbb{R};\ 0)$:

1. $\mathbf{R} \not\models \forall y \exists x(x = y) \longrightarrow \exists x \forall y(x = y)$
2. $\mathbf{R} \not\models \exists x(x = 0) \wedge \exists x(\neg\, x = 0) \longrightarrow \exists x(x = 0 \wedge \neg\, x = 0)$
3. $\mathbf{R} \not\models \forall x(x = 0 \vee \neg\, x = 0) \longrightarrow \forall x(x = 0) \vee \forall x(\neg\, x = 0)$ ⌟

3.7 Normal Forms

Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures and a set Γ of $\mathcal{L}$-formulas. A system of *normal forms* for Γ in $\mathfrak{A}$ is a subset $\Gamma' \subseteq \Gamma$ such that for all $\varphi \in \Gamma$ there is some $\varphi' \in \Gamma'$ with $\mathfrak{A} \vDash \varphi \longleftrightarrow \varphi'$. Normal forms are not necessarily uniquely determined.

We use $Q, Q_1, Q_2, \ldots$ and $S, S_1, S_2, \ldots$ to denote quantifier symbols $\exists$ and $\forall$. We define $\overline{\exists} = \forall$ and $\overline{\forall} = \exists$. We call $\overline{Q}$ the *dual quantifier symbol* of Q. A first-order formula φ is in *prenex normal form (PNF)* if it is of the form $Q_1 x_1 \ldots Q_n x_n(\psi)$ with ψ quantifier-free.

Theorem 3.24 (Prenex normal form)**.** *There is an algorithm computing for each first-order formula a semantically equivalent formula in PNF.*

Proof. Let φ be a formula. If φ is quantifier-free, then φ is in PNF. Assume now that there is at least one quantifier in φ. Reduce φ to $\neg$, $\vee$, $\wedge$, and distinguish three cases:

(a) $\varphi = Qx\varphi_1$: Recursively compute a PNF φ_1' of φ_1. Then φ is semantically equivalent to $Qx\varphi_1'$, which is in PNF.

(b) $\varphi = \neg\varphi_1$: Recursively compute a PNF $Q_1 x_1 \ldots Q_n x_n \psi$ of φ_1. Then φ is semantically equivalent to $\neg Q_1 x_1 \ldots Q_n x_n \psi$. This is, in turn, semantically equivalent to $\overline{Q_1} x_1 \ldots \overline{Q_n} x_n \neg\psi$, which is in PNF.

(c) $\varphi = \varphi_1 \sqcup \varphi_2$ with $\sqcup \in \{\wedge, \vee\}$: Recursively compute a PNF $Q_1 x_1 \ldots Q_n x_n(\psi_1)$ of φ_1 and a PNF $S_1 y_1 \ldots S_m y_m(\psi_2)$ of φ_2. Then φ is semantically equivalent to $Q_1 x_1 \ldots Q_n x_n(\psi_1) \sqcup S_1 y_1 \ldots S_m y_m(\psi_2)$. This is, in turn semantically equivalent to

$$Q_1 x_1' \ldots Q_n x_n'(\psi_1) \sqcup S_1 y_1' \ldots S_m y_m'(\psi_2) \tag{3.22}$$

with $x_i' \notin \mathcal{V}(\psi_2)$, and $y_j' \notin \mathcal{V}(\psi_1)$, and $\{x_1', \ldots, x_n'\} \cap \{y_1', \ldots, y_m'\} = \varnothing$. On these grounds, (3.22) is semantically equivalent to $Q_1 x_1' \ldots Q_n x_n' S_1 y_1' \ldots S_m y_m'(\psi_1 \sqcup \psi_2)$, which is in PNF.

The recursion terminates because the word length of the input formula strictly decreases with each recursion level. □

After conversion to prenex normal form $Q_1 x_1 \ldots Q_n x_n(\psi)$, the quantifiers $Q_i x_i$ are nicely separated from the quantifier-free formula ψ. We now concentrate on normal forms for such quantifier-free formulas. A quantifier-free formula is in *negation normal form (NNF)* if it is built from TRUE, FALSE, and literals using only $\vee$ and $\wedge$.

Theorem 3.25 (Negation normal form)**.** *There is an algorithm computing for each quantifier-free formula a semantically equivalent formula in NNF.*

Proof. Let ψ be a quantifier-free formula. Reduce φ to $\neg$, $\vee$, $\wedge$. Iteratively apply de Morgan's laws to move all $\neg$ inside the scopes of $\vee$ and $\wedge$. Use involution to reduce sequences of $\neg$ to at most one $\neg$. □

A *disjunctive normal form (DNF)* is a disjunction of conjunctions of FALSE, TRUE, and literals. Similarly, a *conjunctive normal form (CNF)* is a conjunction of disjunctions of TRUE, FALSE, and literals.

Theorem 3.26 (Disjunctive and conjunctive normal form)**.**

(i) There is an algorithm computing for each quantifier-free formula a semantically equivalent formula in DNF.

(ii) There is an algorithm computing for each quantifier-free formula a semantically equivalent formula in CNF.

Proof. Compute an NNF according to Theorem 3.25, and then apply the laws of distributivity according to Lemma 3.20. □

Our normal forms for quantifier-free formulas discussed so far all involve reduction to $\neg$, $\vee$, $\wedge$. A quantifier-free formula is *positive* if it is even reduced to $\vee$, $\wedge$.

Lemma 3.27. Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. Assume that for every literal λ one can compute an equivalent positive formula in $\mathfrak{A}$. Then there is an algorithm computing for every quantifier-free formula an equivalent positive formula in $\mathfrak{A}$.

Proof. Compute an NNF according to Theorem 3.25 and equivalently replace all negative literals with their positive equivalents. □

Accordingly, we have *positive normal form* and, more importantly *positive negation normal form*, *positive conjunctive normal form*, and *positive disjunctive normal form*.

Example 3.28. Consider the relational language $\mathcal{L}_{Losets} = (<)$ of *linear ordered sets*. The *axioms of linear ordered sets* are given by

$$\Xi_{Losets} = \{\neg\, x < x,\ x < y \vee x = y \vee y < x,\ x < y \wedge y < z \longrightarrow x < z\}, \tag{3.23}$$

which yields the class $Losets = \mathrm{Mod}(\Xi_{Losets})$ of linear ordered sets. All literals in $\mathcal{L}_{Losets}$ are of one of the forms $t_1 = t_2$ or $t_1 < t_2$ with terms t_1, t_2. We have

$$Losets \models \neg\, t_1 = t_2 \longleftrightarrow t_1 < t_2 \vee t_2 < t_1, \quad Losets \models \neg\, t_1 < t_2 \longleftrightarrow t_2 < t_1 \vee t_2 = t_1. \tag{3.24}$$

By Lemma 3.27, every quantifier-free formula has a positive normal form in *Losets*. The same holds for all subclasses of *Losets*. ⌟

4 Quantifier Elimination, Completeness, and Decidability

4.1 Quantifier Elimination

Let $\mathcal{L}$ be a language, let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures, and let Γ a set of first-order $\mathcal{L}$-formulas. We say that $\mathfrak{A}$ admits *quantifier elimination (QE)* for Γ if for all $\varphi \in \Gamma$ there exists a quantifier-free $\mathcal{L}$-formula φ' such that $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$. We say that $\mathfrak{A}$ admits *effective quantifier elimination* if there is an algorithm computing φ' from φ. Such an algorithm is called a *quantifier elimination procedure*. If Γ is not mentioned explicitly, then Γ is the set of all first-order $\mathcal{L}$-formulas. If $\mathfrak{A} = \{\mathbf{A}\}$ contains only a single $\mathcal{L}$-structure, we allow ourselves to refer to $\mathbf{A}$ instead of $\mathfrak{A}$ and say that $\mathbf{A}$ admits QE for Γ, etc.

Lemma 4.1. Assume that $\mathfrak{A}$ admits QE for Γ, and let $\mathfrak{A}' \subseteq \mathfrak{A}$. Then also $\mathfrak{A}'$ admits QE for Γ, and every QE procedure for $\mathfrak{A}$ and Γ is also a QE procedure for $\mathfrak{A}'$ and Γ. This holds in particular for $\mathfrak{A}' = \{\mathbf{A}\}$ with $\mathbf{A} \in \mathfrak{A}$. □

Let ψ be a quantifier-free formula. An *existential formula* is of the form $\exists x_1 \dots \exists x_k(\psi)$ and a *1-existential formula* is of the form $\exists x(\psi)$. Existential and 1-existential formulas are called *positive* if ψ is positive. Let $\lambda_1, \dots, \lambda_m$ be literals. A *primitive formula* is of the form $\exists x_1 \dots \exists x_n(\lambda_1 \wedge \dots \wedge \lambda_m)$, and a *1-primitive formula* is of the form $\exists x(\lambda_1 \wedge \dots \wedge \lambda_m)$. Primitive and 1-primitive formulas are called *positive* if $\lambda_1, \dots, \lambda_m$ are positive literals.

Theorem 4.2 (Reduction to 1-primitive Formulas)**.** *Let $\mathcal{L}$ be a language, and let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures that admits QE for 1-primitive formulas. Then $\mathfrak{A}$ admits QE. Every QE procedure for $\mathfrak{A}$ and 1-primitive formulas induces a QE procedure for $\mathfrak{A}$.*

Proof. Let φ be a formula. We apply Theorem 3.24 to equivalently transform φ into a PNF $Q_1 x_1 \dots Q_n x_n \psi$. We proceed by induction on the number n of quantifiers. If $n = 0$, then there is nothing to do. Let $n > 0$. We are going to eliminate $Q_n x_n$ from $Q_n x_n \psi$. Since $\forall x_n \psi$ is semantically equivalent to $\neg \exists x_n \neg \psi$, we may assume that $Q_n = \exists$, possibly preceded by a negation symbol, which we write here as $[\neg]\,\exists$. Apply Theorem 3.26 to transform ψ or $\neg\psi$, respectively, into DNF, yielding

$$[\neg]\,\exists x_n \bigvee_i \bigwedge_j \lambda_{ij}, \tag{4.1}$$

which is semantically equivalent to

$$[\neg] \bigvee_i \exists x_n \bigwedge_j \lambda_{ij}. \tag{4.2}$$

By the hypothesis of the theorem we can eliminate the existential quantifiers from the 1-primitive formulas $\exists x_n \bigwedge_j \lambda_{ij}$ in (4.2), yielding quantifier-free formulas ψ_i'. Together we obtain

$$\mathfrak{A} \models Q_1 x_1 \dots Q_n x_n \psi \longleftrightarrow Q_1 x_1 \dots Q_{n-1} x_{n-1} \, [\neg] \bigvee_i \psi_i', \tag{4.3}$$

and the remaining quantifiers can be eliminated by the induction hypothesis. □

Corollary 4.3 (Reduction to normal forms of 1-primitive formulas)**.**

(i) It is sufficient in Theorem 4.2 to consider only 1-primitive formulas where the quantified variable occurs in all literals.

(ii) If $\mathfrak{A}$ has positive normal forms, then it is sufficient in Theorem 4.2 to consider only positive 1-primitive formulas.

Proof. In part (i), all other literals can be semantically equivalently removed from the scope of the existential quantifier before applying the proof of Theorem 4.2. Part (ii) is obvious. □

Obviously, Theorem 4.2 holds also on the stronger assumption that QE is available for 1-existential formulas instead of 1-primitive formulas. It is easy to see that the DNF computation in the proof can then be avoided, which is interesting from a complexity point of view. The proof of the following lemma is an example for such a reduction.

Lemma 4.4 (Effective QE via substitution in a finite setting)**.** Let $\mathcal{L}$ be a language, and let $\mathbf{A}$ be a finite $\mathcal{L}$-structure. Assume that all elements of the finite universe A can be represented as variable-free terms. Then $\mathbf{A}$ admits effective QE.

Proof. Let $A = \{ t^{\mathbf{A}} \in A \mid t \in T \}$ for a finite set T of variable-free terms. Consider a 1-existential formula $\varphi = \exists x(\psi)$. Then $\mathbf{A} \models \varphi \longleftrightarrow \bigvee_{t \in T} \psi[t/x]$. □

Example 4.5. Let $1 < m \in \mathbb{N}$. Consider the $\mathcal{L}_{Rings}$-structure $\mathbf{Z}_m = (\mathbb{Z}/m;\ 0, 1, +, -, \cdot)$. Let $T_m = \{0,\ 1,\ 1+1,\ \dots,\ (m-1) \odot 1\}$, where $(m-1) \odot 1$ denotes the $(m-1)$-fold addition $1 + \dots + 1$. Then $\mathbb{Z}/m = \{ t^{\mathbf{Z}_m} \in \mathbb{Z}/m \mid t \in T_m \}$. According to Lemma 4.4, $\mathbf{Z}_m$ admits effective QE.

As an example consider the formula $\varphi = \exists x(a \cdot x = 1)$, which states that a has a multiplicative inverse in $\mathbb{Z}/m$. The QE procedure suggested in the proof of Lemma 4.4 yields a necessary and sufficient condition on a as a quantifier-free formula:

$$\mathbf{Z}_m \models \varphi \longleftrightarrow \bigvee_{t \in T_m} a \cdot t = 1. \tag{4.4}$$

⌟

It is noteworthy that one can, more generally, reduce to existential, in contrast to 1-existential, formulas. In some domains, including the real numbers, there are asymptotically fast methods available that eliminate entire existential quantifier blocks at once. However, for our purposes here, we will mostly use reduction to 1-primitive formulas. The proof of the following lemma gives a first impression.

Lemma 4.6 (Effective QE for some classes of sets)**.** Let $\mathcal{L} = (\ )$. That is, all terms are variables and all atoms are equations between those variables. Then the following hold:

(i) $\mathfrak{A} = \{ \mathbf{A} \mid A \text{ is infinite} \}$ admits effective QE.

(ii) $\mathbf{B}_1 = (\{1\})$ admits effective QE.

(iii) $\mathbf{B}_2 = (\{1, 2\})$ admits effective QE.

Proof. Consider a 1-primitive formula

$$\exists x \left[\bigwedge_{i=1}^{n} x = y_i \wedge \bigwedge_{j=1}^{m} \neg\, x = z_j \right], \tag{4.5}$$

where $y_i, z_i \in \mathcal{V}$. Equations $x = x$ can be deleted from the conjunctions in (4.5) via semantic equivalence to TRUE. Similarly, if there is a literal $\neg\, x = x$, then that literal and thus the entire 1-primitive formula (4.5) is semantically equivalent to FALSE. We may now assume that $x \notin \{y_1, \ldots, y_n, z_1, \ldots, z_m\}$. If $n > 0$, then (4.5) is semantically equivalent to

$$\exists x (x = y_1) \wedge \bigwedge_{i=2}^{n} y_1 = y_i \wedge \bigwedge_{j=1}^{m} \neg\, y_1 = z_j, \tag{4.6}$$

which is in turn semantically equivalent to the quantifier-free formula

$$\bigwedge_{i=2}^{n} y_1 = y_i \wedge \bigwedge_{j=1}^{m} \neg\, y_1 = z_j. \tag{4.7}$$

Assume now that $n = 0$. If also $m = 0$, then (4.5) is semantically equivalent to TRUE. Otherwise we obtain

$$\exists x \left[\bigwedge_{j=1}^{m} \neg\, x = z_j \right] \quad \text{with} \quad m > 0. \tag{4.8}$$

We have reduced our QE problem from an arbitrary 1-primitive formula in (4.5) to a formula of the form (4.8).

(i) In $\mathfrak{A}$, (4.8) is equivalent to TRUE.

(ii) In $\mathbf{B}_1$, (4.8) is equivalent to FALSE.

(iii) In $\mathbf{B}_2$, (4.8) is equivalent to $\bigwedge_{j=2}^{m} z_1 = z_j$. □

Quantifier elimination is quite sensitive to the underlying language $\mathcal{L}$. In general, adding or removing function or relation symbols can both enable and prevent quantifier eliminability. The next lemma shows that quantifier eliminability is preserved when adding only constant symbols to the language. The idea is based on abstraction: In the input replace all new constants with fresh free variables, perform QE, and in the result substitute the constants back into variables introduced before.

Lemma 4.7 (QE and language extension by constants)**.** Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures that admits QE. Let $\mathcal{L}'$ be an extension language obtained from $\mathcal{L}$ by adding constant symbols. Let $\mathfrak{A}'$ be a class of $\mathcal{L}'$-structures such that $\mathbf{A}'|_{\mathcal{L}} \in \mathfrak{A}$ for all $\mathbf{A}' \in \mathfrak{A}'$. Then also $\mathfrak{A}'$ admits QE, and every QE procedure for $\mathfrak{A}$ induces a QE procedure for $\mathfrak{A}'$.

Proof. Let φ be an $\mathcal{L}'$-formula. Then there exist constant symbols $c_1, \ldots, c_n$ in $\mathcal{L}'$, variables $y_1, \ldots, y_n \in \mathcal{V} \setminus \mathcal{V}(\varphi)$, and an $\mathcal{L}$-formula ψ such that $\varphi = \psi[c_1/y_1, \ldots, c_n/y_n]$. Let $\psi' \in \mathfrak{A}$ such that $\mathfrak{A} \vDash \psi \longleftrightarrow \psi'$. It follows that $\mathfrak{A}' \vDash \psi \longleftrightarrow \psi'$ and thus $\mathfrak{A}' \vDash \psi[c_1/y_1, \ldots, c_n/y_n] \longleftrightarrow \psi'[c_1/y_1, \ldots, c_n/y_n]$, i.e., $\mathfrak{A}' \vDash \varphi \longleftrightarrow \varphi'$. □

Consider the elimination of a quantifier $\exists x$ from a 1-existential formula $\varphi = \exists x(\psi)$, yielding an equivalent quantifier-free equivalent φ'. It might seem quite natural that the variable x vanishes along with the quantifier in the course of the elimination and that finally the variables occurring in φ' would be a subset of the variables occurring free in φ. However, this is not always the case! The following example illustrates a situation where the introduction of a new variable in the course of the elimination of a quantifier is inevitable.

Example 4.8 (QE-introduced variables)**.** Consider the relational language $\mathcal{L} = (P^{(1)})$ and the $\mathcal{L}$-structures $\mathbf{A}_1 = (\{1\};\ P_1)$ with $P_1(1) = \top$ and $\mathbf{A}_2 = (\{2\};\ P_2)$ with $P_2(2) = \bot$. Consider the sentence $\varphi = \exists x(P(x))$, and note that $\mathbf{A}_1 \vDash \varphi$ and $\mathbf{A}_2 \nvDash \varphi$.

Let $\varphi' = P(y)$ with $y \in \mathcal{V}$, and consider the extended formula $(\varphi \longleftrightarrow \varphi')(y)$. Then $\mathbf{A}_1 \vDash (\varphi \longleftrightarrow \varphi')(1)$ and $\mathbf{A}_2 \vDash (\varphi \longleftrightarrow \varphi')(2)$, and therefore $\{\mathbf{A}_1, \mathbf{A}_2\} \vDash \varphi \longleftrightarrow \varphi'$.

Assume for a contradiction that there exists a quantifier-free formula φ'' such that $\{\mathbf{A}_1, \mathbf{A}_2\} \vDash \varphi \longleftrightarrow \varphi''$ and $\mathcal{V}(\varphi'') \subseteq \mathcal{V}_{\text{free}}(\varphi) = \varnothing$. Since there are no constant symbols in $\mathcal{L}$ and no variables in φ'', there are no terms in φ''. As a consequence, there are no equations and no predicates in φ''. Instead, φ'' is a Boolean combination of TRUE and FALSE. It follows that φ'' is semantically equivalent to either TRUE or FALSE. Since φ'' is equivalent to φ in $\{\mathbf{A}_1, \mathbf{A}_2\}$, it follows further that also φ is equivalent to either TRUE or FALSE in $\{\mathbf{A}_1, \mathbf{A}_2\}$. This contradicts our observation that $\mathbf{A}_1 \vDash \varphi$ and $\mathbf{A}_2 \nvDash \varphi$ above. ⌟

We are now going to show that, even with the elimination of several quantifiers, generally at most one new variable need be introduced. We will furthermore give sufficient conditions that allow to avoid the introduction of new variables altogether in most practical situations. We start with a technical lemma and subsequently state our result as a theorem.

Lemma 4.9. Let $\mathcal{L}$ be a language, let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures, let φ be a formula, and let φ' be a quantifier-free formula such that $\mathfrak{A} \vDash \varphi \longleftrightarrow \varphi'$. Let $\{z_1, \ldots, z_n\} = \mathcal{V}(\varphi') \setminus \mathcal{V}_{\text{free}}(\varphi)$, and let $t_1, \ldots, t_n$ be terms. Then $\mathfrak{A} \vDash \varphi \longleftrightarrow \varphi'[t_1/z_1, \ldots, t_n/z_n]$.

Proof. Define pairwise disjoint tuples of variables $\mathbf{z} = (z_1, \ldots, z_n)$ with $\{z_1, \ldots, z_n\}$ as above, $\mathbf{y} = (y_1, \ldots, y_m)$ with $\{y_1, \ldots, y_m\} = \mathcal{V}_{\text{free}}(\varphi)$, and $\mathbf{w} = (w_1, \ldots, w_k)$ with $\{w_1, \ldots, w_k\} = \bigcup_i \mathcal{V}(t_i) \setminus \{y_1, \ldots, y_m, z_1, \ldots, z_n\}$. Consider extended formulas $\varphi(\mathbf{y}, \mathbf{z}, \mathbf{w})$ and $\varphi'(\mathbf{y}, \mathbf{z}, \mathbf{w})$. Let $\mathbf{A} \in \mathfrak{A}$. Then we have $\mathbf{A} \vDash \varphi \longleftrightarrow \varphi'$, which is defined as

$$\varphi^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \varphi'^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) \tag{4.9}$$

for all $\mathbf{a} \in A^m$, $\mathbf{b} \in A^n$, $\mathbf{c} \in A^k$. Since the variables $\mathbf{z}$ and $\mathbf{w}$ do not occur free in φ, we can switch to the extended formula $\varphi(\mathbf{y})$ and obtain

$$\varphi'^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \varphi^{\mathbf{A}}(\mathbf{a}) \tag{4.10}$$

for all $\mathbf{a} \in A^m$, $\mathbf{b} \in A^n$, $\mathbf{c} \in A^k$. For $\mathbf{t} = (t_1, \dots, t_n)$ we consider the extended formula $\varphi'[\mathbf{t}/\mathbf{z}](\mathbf{y}, \mathbf{z}, \mathbf{w})$ and obtain

$$\varphi'[\mathbf{t}/\mathbf{z}]^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \varphi'^{\mathbf{A}}(\mathbf{a}, t_1^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}), \dots, t_m^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}), \mathbf{c}) = \varphi^{\mathbf{A}}(\mathbf{a}) \tag{4.11}$$

for all $\mathbf{a} \in A^m$, $\mathbf{b} \in A^n$, $\mathbf{c} \in A^k$. We finally switch back to the extended formula $\varphi(\mathbf{y}, \mathbf{z}, \mathbf{w})$ and obtain

$$\varphi^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \varphi'[\mathbf{t}/\mathbf{z}]^{\mathbf{A}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) \tag{4.12}$$

for all $\mathbf{a} \in A^m$, $\mathbf{b} \in A^n$, $\mathbf{c} \in A^k$, which is by definition equivalent to $\mathbf{A} \models \varphi \longleftrightarrow \varphi'[\mathbf{t}/\mathbf{z}]$. □

Theorem 4.10 (Conservative QE)**.** *Let $\mathcal{L}$ be a language, let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures that admits QE for a set Γ of formulas, and let $\varphi \in \Gamma$. Then the following hold:*

(i) There exists a quantifier-free formula φ' such that $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ and $|\mathcal{V}(\varphi') \setminus \mathcal{V}_{free}(\varphi)| \leq 1$. Furthermore, if $\varphi(y_1, \dots, y_n)$ is an extended formula with $n \geq 1$, then $\varphi'(y_1, \dots, y_n)$ is an extended quantifier-free formula.

(ii) If $\mathcal{L}$ contains at least one constant symbol, then there exists a quantifier-free formula φ' such that $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ and $\mathcal{V}(\varphi') \subseteq \mathcal{V}_{free}(\varphi)$.

(iii) If $\mathcal{V}_{free}(\varphi) \neq \varnothing$, then there exists a quantifier-free formula φ' such that $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ and $\mathcal{V}(\varphi') \subseteq \mathcal{V}_{free}(\varphi)$.

If $\mathfrak{A}$ admits effective QE for Γ, then φ' in (i)–(iii) can be effectively computed.

Proof. Since $\mathfrak{A}$ admits QE, there is a quantifier-free formula $\bar{\varphi}$ such that $\mathfrak{A} \models \varphi \longleftrightarrow \bar{\varphi}$. Let $\{z_1, \dots, z_n\} = \mathcal{V}(\bar{\varphi}) \setminus \mathcal{V}_{\text{free}}(\varphi)$. It follows that $\mathcal{V}(\bar{\varphi}) \subseteq \mathcal{V}_{\text{free}}(\varphi) \cup \{z_1, \dots, z_n\}$.

(i) Let $\varphi(y_1, \dots, y_n)$ be an extended formula with $n \geq 1$. Such an extended formula always exists. Set $\varphi' = \bar{\varphi}[y_1/z_1, \dots, y_1/z_n]$. Then $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ by Lemma 4.9. Furthermore, $\mathcal{V}(\varphi') \subseteq \mathcal{V}_{\text{free}}(\varphi) \cup \{y_1\}$. It follows that $|\mathcal{V}(\varphi') \setminus \mathcal{V}_{\text{free}}(\varphi)| \leq 1$ and that $\varphi'(y_1, \dots, y_n)$ is an extended quantifier-free formula.

(ii) Let c be a constant symbol in $\mathcal{L}$ and set $\varphi' = \bar{\varphi}[c/z_1, \dots, c/z_n]$. Then $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ by Lemma 4.9. Furthermore, $\mathcal{V}_{\text{free}}(\varphi') \subseteq \mathcal{V}_{\text{free}}(\varphi)$.

(iii) Let $y \in \mathcal{V}_{\text{free}}(\varphi)$ and set $\varphi' = \bar{\varphi}[y/z_1, \dots, y/z_n]$. Then $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ by Lemma 4.9. Furthermore, $\mathcal{V}_{\text{free}}(\varphi') \subseteq \mathcal{V}_{\text{free}}(\varphi) \cup \{y\} = \mathcal{V}_{\text{free}}(\varphi)$. □

Wrapping up, Theorem 4.10 states that in the course of quantifier elimination with input φ and quantifier-free output φ' it is never necessary to introduce more than one new variable. Furthermore, the introduction of a new variable can become necessary only when there is no constant in the language and the input φ is a sentence. Even in this critical case it is well possible that there exist QE without introduction of a new variable, e.g., our QE procedures for sets over $\mathcal{L} = (\,)$ in Lemma 4.6.

If a new variable is introduced for an input sentence φ, then $\varphi(\,)$ is an extended formula but $\varphi'(\,)$ is not. Otherwise we may generally assume that admissible extensions $(y_1, \ldots, y_n)$ of φ are also admissible extensions of φ'. Notice that in (ii) and (iii) of the theorem it follows from $\mathcal{V}(\varphi') \subseteq \mathcal{V}_{\text{free}}(\varphi)$ that $\varphi'(y_1, \ldots, y_n)$ is an extended quantifier-free formula for all extended formulas $\varphi(y_1, \ldots, y_n)$. This includes $\varphi(\,)$, where $n = 0$.

Lemma 4.11 (A negative result on QE for another class of sets)**.** Let $\mathcal{L} = (\,)$, let $\mathbf{B}_1 = (\{1\})$, and let $\mathbf{B}_2 = (\{1, 2\})$. Recall from Lemma 4.6 that both $\mathbf{B}_1$ and $\mathbf{B}_2$ admit effective QE. However, $\mathfrak{B} = \{\mathbf{B}_1, \mathbf{B}_2\}$ does not admit QE.

Proof. Consider $\varphi = \exists x(\neg\, x = z_1)$. Then $\neg\varphi$ is semantically equivalent to $\forall x(x = z_1)$. Since $\mathbf{B}_1 \models \neg\varphi$ and $\mathbf{B}_2 \models \varphi$, it follows that φ is not equivalent to one of TRUE, FALSE in $\mathfrak{B}$. Assume for a contradiction that φ has a quantifier-free equivalent φ' in $\mathfrak{B}$. According to Theorem 4.10 we may assume without loss of generality that $\mathcal{V}(\varphi') \subseteq \mathcal{V}_{\text{free}}(\varphi) = \{z_1\}$. Then the only possible atom occurring in φ' is $z_1 = z_1$, which is semantically equivalent to TRUE. It follows that φ' is semantically equivalent to either TRUE or FALSE, a contradiction. □

4.2 Definable Sets and Projection

Let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $\varphi(\mathbf{x})$ be an extended formula with $\mathbf{x} \in \mathcal{V}^n$, $n \geq 1$. Then the set

$$[\varphi]^{\mathbf{A}} = \{\, \mathbf{a} \in A^n \mid \mathbf{A} \models \varphi(\mathbf{a}) \,\} \tag{4.13}$$

is *defined* by $\varphi(\mathbf{x})$ in $\mathbf{A}$. We say that a set $B \subseteq A^n$ is *definable* in $\mathbf{A}$ if there exists an extended formula $\varphi(\mathbf{x})$ such that $B = [\varphi]^{\mathbf{A}}$. We call B *quantifier-free definable* if $\varphi(\mathbf{x})$ can be chosen quantifier-free.

Theorem 4.12 (Characterization of QE)**.** *Let* $\mathbf{A}$ *be an* $\mathcal{L}$*-structure. Then* $\mathbf{A}$ *admits QE if and only if every definable set is quantifier-free definable.*

Proof. Assume that $\mathbf{A}$ admits QE, and let $B \subseteq \mathbf{A}^n$ be a definable set, i.e., $B = [\varphi]^{\mathbf{A}}$ for an extended formula $\varphi(\mathbf{x})$ with $\mathbf{x} \in \mathcal{V}^n$. Let φ' be a quantifier-free formula such that $\mathbf{A} \models \varphi \longleftrightarrow \varphi'$. Then $\varphi'(\mathbf{x})$ is an extended formula as well, and $[\varphi']^{\mathbf{A}} = [\varphi]^{\mathbf{A}} = B$. Assume vice versa that every definable set is quantifier-free definable. Consider a formula φ. There is a quantifier-free formula φ' such that $[\varphi']^{\mathbf{A}} = [\varphi]^{\mathbf{A}}$ for extended formulas $\varphi(\mathbf{x})$ and $\varphi'(\mathbf{x})$ with $\mathbf{x} \in \mathcal{V}^n$. It follows that $\mathbf{A} \models \varphi \longleftrightarrow \varphi'$. □

A typical application of Theorem 4.12 is in proving negative results about QE. One finds formulas whose definable sets cannot be represented by quantifier-free formulas. The proof of the following theorem is an example. The language of rings is used also for fields, because the multiplicative inverse in fields is a partial function, defined only for non-zero elements.

Theorem 4.13. *Consider* $\mathcal{L}_{Rings}$*. The field* $\mathbf{R} = (\mathbb{R};\ 0, 1, +, -, \cdot\,)$ *does not admit QE.*

Proof. The extended formula $\varphi = \exists x(x^2 = y)(y)$ defines the set $[\varphi]^{\mathbf{R}} = [0, \infty)$. Assume for a contradiction that $\mathbf{R}$ admits QE. Let $\varphi'(y)$ be an extended quantifier-free formula, without loss of

generality in NNF, such that $\mathbf{R} \models \varphi \longleftrightarrow \varphi'$. Each atom α in φ' describes a univariate polynomial equation in y, which has at most finitely many solutions. Thus $[\alpha]^{\mathbf{R}}$ is finite. Accordingly, every negative literal λ defines a cofinite set $[\lambda]^{\mathbf{R}}$. It is easy to see that $[\varphi_1 \vee \varphi_2]^{\mathbf{R}} = [\varphi_1]^{\mathbf{R}} \cup [\varphi_2]^{\mathbf{R}}$ and $[\varphi_1 \wedge \varphi_2]^{\mathbf{R}} = [\varphi_1]^{\mathbf{R}} \cap [\varphi_2]^{\mathbf{R}}$, and it is not hard to see that unions and intersections among finite and cofinite sets yield again finite or cofinite sets. Hence $[\varphi']^{\mathbf{R}}$ is either finite or cofinite. However, $[\varphi]^{\mathbf{R}} = [0, \infty)$ is neither, a contradiction. □

Conversely, if an $\mathcal{L}$-structure $\mathbf{A}$ admits QE, then all definable sets can be described with quantifier-free formulas. This aids in understanding structural properties of definable sets in the given structure $\mathbf{A}$.

Let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $m, n \in \mathbb{N}$ with $m, n \geq 1$. The *graph* of a function $f : A^n \to A^m$ is defined as

$$\operatorname{graph}(f) = \{ (\mathbf{a}, \mathbf{b}) \in A^{n+m} \mid f(\mathbf{a}) = \mathbf{b} \}. \tag{4.14}$$

We call f a *(quantifier-free) definable function* in $\mathbf{A}$ if $\operatorname{graph}(f)$ is a (quantifier-free) definable set. For $D \subseteq A^n$, the *image* of D under f is defined as

$$f(D) = \{ \mathbf{b} \in A^m \mid \text{exists } \mathbf{a} \in D \text{ such that } f(\mathbf{a}) = \mathbf{b} \}. \tag{4.15}$$

Lemma 4.14. Consider $f : A^n \to A^m$ and $D \subseteq A^n$.

(i) If both f and D are definable, then $f(D)$ is definable.

(ii) If $f(\mathbf{a}) = \left(t_1^{\mathbf{A}}(\mathbf{a}), \ldots, t_m^{\mathbf{A}}(\mathbf{a})\right)$ for $\mathbf{a} \in A^n$ and using extended terms $t_i(\mathbf{x})$ with $\mathbf{x} \in \mathcal{V}^n$, then f is quantifier-free definable.

Proof. (i) Let $\operatorname{graph}(f) = [\gamma]^{\mathbf{A}}$ using the extended formula $\gamma(\mathbf{x}, \mathbf{y})$ with $\mathbf{x} \in \mathcal{V}^n$, $\mathbf{y} \in \mathcal{V}^m$, and let $D = [\delta]^{\mathbf{A}}$ using the extended formula $\delta(\mathbf{x})$. Define $\iota = \exists \mathbf{x}(\delta \wedge \gamma)$. Then $\iota(\mathbf{y})$ is an extended formula and $f(D) = [\iota]^{\mathbf{A}}$.

(ii) Consider $\gamma = y_1 = t_1 \wedge \ldots \wedge y_m = t_m$ and the extended quantifier-free formula $\gamma(\mathbf{x}, \mathbf{y})$ with $\mathbf{y} = (y_1, \ldots, y_m)$. Then $\operatorname{graph}(f) = [\gamma]^{\mathbf{A}}$. □

The *projection function* along the $(n+1)$-st coordinate is quantifier-free definable:

$$\pi_{n+1} : A^{n+1} \to A^n, \quad \pi_{n+1}(a_1, \ldots, a_{n+1}) = (a_1, \ldots, a_n). \tag{4.16}$$

Let $\mathbf{x} = (x_1, \ldots, x_{n+1})$, $\mathbf{y} = (y_1, \ldots, y_n)$, and $\gamma = (y_1 = x_1 \wedge \cdots \wedge y_n = x_n)$. Then $\operatorname{graph}(\pi_{n+1}) = [\gamma]^{\mathbf{A}}$ using the extended quantifier-free formula $\gamma(\mathbf{x}, \mathbf{y})$. For $D \subseteq A^{n+1}$ the *projection of D* along the $(n+1)$-st coordinate is defined as the image

$$\pi_{n+1}(D) = \{ \mathbf{b} \in A^n \mid \text{exists } \mathbf{a} \in D \text{ such that } \pi_{n+1}(\mathbf{a}) = \mathbf{b} \}. \tag{4.17}$$

Assume that D is definable, say, $D = [\delta]^{\mathbf{A}}$ using an extended formula $\delta(\mathbf{x})$. Then the projection of D is definable by Lemma 4.14 as follows. Let $\iota = \exists \mathbf{x}(\delta \wedge \gamma)$. Then $\pi_{n+1}(D) = [\iota]^{\mathbf{A}}$ using the extended formula $\iota(\mathbf{y})$. More explicitly, we have

$$\iota = \exists x_1 \ldots \exists x_{n+1}(\delta \wedge x_1 = y_1 \wedge \cdots \wedge x_n = y_n), \tag{4.18}$$

and we can eliminate the quantifiers $\exists x_1 \ldots \exists x_n$, because ι is semantically equivalent to

$$\iota' = \exists x_{n+1}(\delta[y_1/x_1, \ldots, y_n/x_n]). \tag{4.19}$$

Any defined set $[\varphi]^{\mathbf{A}}$ using an extended formula $\varphi(\mathbf{y})$ is invariant under renaming of variables of φ in the following sense. Recall that $\mathbf{y} = (y_1, \ldots, y_n)$, let $\bar{\mathbf{x}} = (x_1, \ldots, x_n)$, and let $\bar{\varphi} = \varphi[\bar{\mathbf{x}}/\mathbf{y}]$, then $[\varphi]^{\mathbf{A}} = [\bar{\varphi}]^{\mathbf{A}}$ using extended formulas $\varphi(\mathbf{y})$ and $\bar{\varphi}(\bar{\mathbf{x}})$, respectively. In particular,

$$\pi_{n+1}(D) = [\iota]^{\mathbf{A}} = [\iota']^{\mathbf{A}} = [\exists x_{n+1}(\delta)]^{\mathbf{A}}, \tag{4.20}$$

using extended formulas $\iota(\mathbf{y})$, $\iota'(\mathbf{y})$, and $\exists x_{n+1}(\delta)(\bar{\mathbf{x}})$, respectively.

Theorem 4.15 (Characterization of QE)**.** *Let* $\mathbf{A}$ *be an* $\mathcal{L}$*-structure. The following are equivalent:*

(i) $\mathbf{A}$ *admits QE.*

(ii) For every quantifier-free definable set $D \subseteq A^n$ *and every definable function* $f : A^n \to A^m$*, the image* $f(D) \subseteq A^m$ *is quantifier-free definable.*

(iii) For every quantifier-free definable set $D \subseteq A^{n+1}$*, the projection* $\pi_{n+1}(D) \subseteq A^n$ *is quantifier-free definable.*

Proof. Assume (i). Let $\delta(\mathbf{x})$ be a quantifier-free extended formula such that $[\delta]^{\mathbf{A}} = D \subseteq A^n$, and let $\gamma(\mathbf{x}, \mathbf{y})$ be an extended formula such that $[\gamma]^{\mathbf{A}} = \mathrm{graph}(f)$. Define $\iota = \exists \mathbf{x}(\delta \wedge \gamma)$ and consider the extended formula $\iota(\mathbf{y})$. Then $[\iota]^{\mathbf{A}} = f(D)$. Since $\mathbf{A}$ admits QE, there is a quantifier-free extended formula $\iota'(\mathbf{y})$ with $\mathbf{A} \models \iota \longleftrightarrow \iota'$, and it follows that $[\iota']^{\mathbf{A}} = [\iota]^{\mathbf{A}} = f(D)$.

Assume (ii). Let D be a quantifier-free definable set. Recall that $\pi_{n+1} : A^{n+1} \to A^n$ is a definable function. Now (ii) states that $\pi_{n+1}(D)$ is quantifier-free definable.

Assume (iii). Consider a 1-existential formula $\varphi = \exists x(\psi)$. Let $\varphi(\bar{\mathbf{x}})$ and $\psi(\bar{\mathbf{x}}, x)$ be extended formulas, where $\bar{\mathbf{x}} = (x_1, \ldots, x_n)$. Set $D = [\psi]^{\mathbf{A}} \subseteq A^{n+1}$. Recall from (4.20) that $\pi_{n+1}(D) = [\varphi]^{\mathbf{A}} \subseteq A^n$. By (iii) there exists an extended quantifier-free formula $\varphi'(\bar{\mathbf{x}})$ with $\pi_{n+1}(D) = [\varphi']^{\mathbf{A}}$. It follows that $[\varphi]^{\mathbf{A}} = [\varphi']^{\mathbf{A}}$ and hence $\mathbf{A} \models \varphi \longleftrightarrow \varphi'$. □

Example 4.16 (Real Algebraic Geometry)**.** An *algebraic set* in $\mathbb{R}^n$ is a set $\{ \mathbf{a} \in \mathbb{R}^n \mid f_1(\mathbf{a}) = \cdots = f_m(\mathbf{a}) = 0 \}$ of all real solutions of a finite system of multivariate polynomial equations with $f_i \in \mathbb{Z}[\mathbf{x}]$. Figure 4.1 shows an algebraic set in $\mathbb{R}^3$, which is called the Whitney Umbrella. It is defined by one single equation $x^2 - y^2 z = 0$. By Theorem 4.13, the $\mathcal{L}_{Rings}$-structure $(\mathbb{R};\ 0, 1, +, -, \cdot)$ does not admit QE. By Theorem 4.15, it follows that projections of algebraic sets are not algebraic sets in general. In fact, our proof of Theorem 4.13 introduced an algebraic set defined by $x^2 = y$, which is a parabola, and then argued that its projection $[0, \infty)$ along the x-axis is not an algebraic set. It is noteworthy that the projection of the parabola along the y-axis yields $\mathbb{R}$, which is an algebraic set, defined by $0 = 0$. Another popular example is the hyperbola $xy = 1$, whose projection along either axis is $\mathbb{R} \setminus \{0\}$, which is not algebraic. The parabola and the hyperbola are plotted in Figure 4.2.

A *basic semialgebraic set* in $\mathbb{R}^n$ is a set of all real solutions of a finite system of multivariate polynomial equations and inequalities. A *semialgebraic set* in $\mathbb{R}^n$ is a finite union of basic

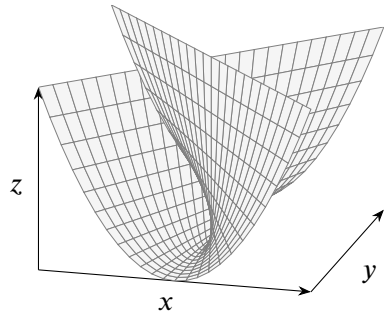


Figure 4.1: The Whitney Umbrella defined by $x^2 - y^2 z = 0$ in $\mathbb{R}^3$

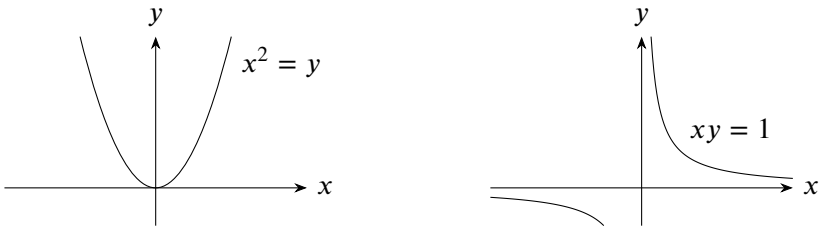


Figure 4.2: Two algebraic sets, a parabola and a hyperbola, in $\mathbb{R}^2$

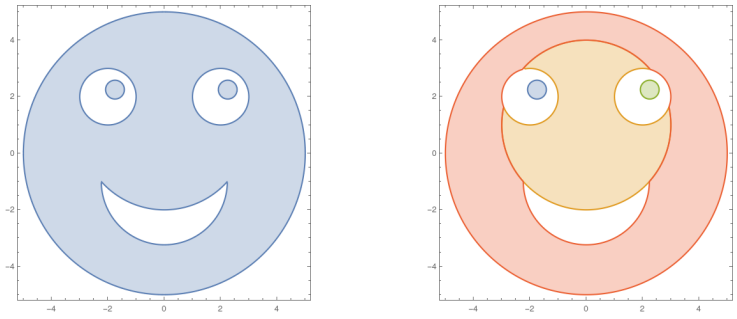


Figure 4.3: A semialgebraic set in $\mathbb{R}^2$ defined by the formula in (4.21)

semialgebraic sets. Figure 4.3 pictures a semialgebraic set defined by

$$\begin{aligned}&\left(\tfrac{7}{4}+x\right)^2+\left(-\tfrac{9}{4}+y\right)^2<\tfrac{1}{9}\vee\left(-\tfrac{9}{4}+x\right)^2+\left(-\tfrac{9}{4}+y\right)^2<\tfrac{1}{9}\vee\\&\quad\Big(x^2+y^2<25\wedge(-2+x)^2+(-2+y)^2\geq 1\wedge(2+x)^2+(-2+y)^2\geq 1\wedge\\&\qquad(x^2+(1+y)^2\geq 5\vee x^2+(-1+y)^2<9)\Big),\end{aligned}\tag{4.21}$$

which is essentially an $\mathcal{L}_{Rings_<}$-formula.[1] The *Tarski–Seidenberg Theorem* states that projections of semialgebraic sets are again semialgebraic sets. By Theorem 4.15, it follows that the $\mathcal{L}_{Rings_<}$-structure $\mathbf{R} = (\mathbb{R};\ 0, 1, +, -, \cdot\,; <)$ admits QE. Historically, both Tarski in 1948 and Seidenberg in 1954 proposed QE procedures for $\mathbf{R}$ and, conversely, concluded the Tarski–Seidenberg Theorem from quantifier eliminability. ⌟

4.3 Completeness and Decidability

Let $\mathcal{L}$ be a language, $\mathfrak{A}$ a class of $\mathcal{L}$-structures, and Θ a set of $\mathcal{L}$-sentences. We say that $\mathfrak{A}$ is *complete* for Θ if for all $\vartheta \in \Theta$ either $\mathfrak{A} \models \vartheta$ or $\mathfrak{A} \models \neg\vartheta$. Otherwise $\mathfrak{A}$ is *incomplete* for Θ.[2] A *decision procedure* for $\mathfrak{A}$ and Θ is an algorithm that takes a sentence $\vartheta \in \Theta$ as input. If $\mathfrak{A} \models \vartheta$, then the output is YES, else the output is NO. We say that $\mathfrak{A}$ is *decidable* for Θ if there exists a decision procedure for $\mathfrak{A}$ and Θ. Otherwise $\mathfrak{A}$ is *undecidable* for Θ. If $\mathfrak{A} = \{\mathbf{A}\}$ contains only one $\mathcal{L}$-structure, we allow ourselves to refer to $\mathbf{A}$ instead of $\mathfrak{A}$. If Θ is not mentioned explicitly, then Θ is the set of all $\mathcal{L}$-sentences. Note that a single $\mathcal{L}$-structure $\mathbf{A}$ can be decidable or undecidable, but $\{\mathbf{A}\}$ is always complete.

Let T be set set of all Turing machines. A *Gödel numbering* is an injective function $g : T \to \mathbb{N}$ such that g is computable, the image $g(T)$ is recursive, and the inverse $g^{-1} : g(T) \to T$ is computable. Given a Turing machine $m \in T$, the value $g(m) \in \mathbb{N}$ is the *Gödel number* of m. There exist infinitely many Gödel numberings, of which we fix one.

Example 4.17 (An undecidable structure)**.** Consider the language $\mathcal{L} = (0, 1, \ldots;\ H^{(1)})$. Let $\mathbf{A} = (\mathbb{N};\ 0, 1, \ldots;\ H)$ with $H^{\mathbf{A}}(n) = \top$ if and only if n is the Gödel number of a Turing machine that halts. Then $\mathbf{A}$ is undecidable for $\Theta = \{H(0), H(1), \ldots\}$. However, $\{\mathbf{A}\}$ is trivially complete, which reflects the fact that every Turing machine either holds or not. As an exercise, show that $\mathbf{A}$ admits effective QE. ⌟

Example 4.18 (An incomplete decidable class)**.** Consider $\mathcal{L}_{Rings}$, the class $\mathfrak{A} = \{\mathbf{Z}_2, \mathbf{Z}_3\}$ with $\mathbf{Z}_m = (\mathbb{Z}/m;\ 0, 1, +, -, \cdot\,)$ and the set Θ of all variable-free equations. Then $\mathfrak{A}$ is not complete for Θ because neither $\mathfrak{A} \models 1 + 1 = 0$ nor $\mathfrak{A} \models \neg\, 1 + 1 = 0$. However, $\mathfrak{A}$ is decidable for Θ, because all variable-free equations can be effectively evaluated to either $\bot$ or $\top$ in both $\mathbf{Z}_2$ and $\mathbf{Z}_3$. For our $1 + 1 = 0$ we obtain $(1 + 1 = 0)^{\mathbf{Z}_2} = \top$ and $(1 + 1 = 0)^{\mathbf{Z}_3} = \bot$. The output of a decision procedure on input of $1 + 1 = 0$ would be NO. ⌟

[1] Denominators can be equivalently removed by applying the laws of distributivity and then multiplying with the positive least common multiple of the denominators in each atomic formula.

[2] This notion of completeness of a model class should not be confused with the notion of completeness of a logical calculus. It is noteworthy that Gödel's *Incompleteness Theorems* refer to the former, while his *Completeness Theorem* refers to the latter.

Lemma 4.19 (Decidable restrictions)**.** Let $\mathcal{L}$ be a language, and let $\mathbf{A}$ be an $\mathcal{L}$-structure. If $\mathbf{A}$ is decidable, then $\mathbf{A}|_{\mathcal{L}'}$ is decidable for all $\mathcal{L}' \subseteq \mathcal{L}$.

Proof. Assume that $\mathbf{A}$ is decidable. Let $\mathcal{L}' \subseteq \mathcal{L}$, and let ϑ be an $\mathcal{L}'$-sentence. Then ϑ is also an $\mathcal{L}$-sentence, and $\vartheta^{\mathbf{A}|_{\mathcal{L}'}} = \vartheta^{\mathbf{A}} \in \{\top, \bot\}$ by Lemma 3.9. In other words, $\mathbf{A}|_{\mathcal{L}'} \vDash \vartheta$ if and only if $\mathbf{A} \vDash \vartheta$. Hence we can use the existing decision procedure for $\mathbf{A}$ also for $\mathbf{A}|_{\mathcal{L}'}$. □

Corollary 4.20 (Undecidable expansions)**.** *Let $\mathcal{L}$ be a language, and let $\mathbf{A}$ be an $\mathcal{L}$-structure. If $\mathbf{A}$ is undecidable, then $\mathbf{A}'$ is undecidable for all $\mathcal{L}' \supseteq \mathcal{L}$ and all $\mathcal{L}'$-expansions $\mathbf{A}'$ of $\mathbf{A}$.*

Proof. Assume that $\mathbf{A}$ is undecidable. Let $\mathcal{L}' \supseteq \mathcal{L}$, and let $\mathbf{A}'$ be an $\mathcal{L}'$-expansion of $\mathbf{A}$, i.e., $\mathbf{A}'|_{\mathcal{L}} = \mathbf{A}$. Assume for a contradiction that $\mathbf{A}'$ is decidable. Then $\mathbf{A}$ is decidable by Lemma 4.19. □

The following two results are concerned with the somewhat subtle connections between completeness and decidability of classes vs. completeness and decidability of their members.

Lemma 4.21. Let $\mathfrak{A}$ be a finite set of $\mathcal{L}$-structures, and let Θ be a set of sentences. If each $\mathbf{A} \in \mathfrak{A}$ is decidable for Θ, then $\mathfrak{A}$ is decidable for Θ.

Proof. Let $\vartheta \in \Theta$. We must produce the output YES if $\mathfrak{A} \vDash \vartheta$, and the output NO else. For each of the finitely many $\mathbf{A} \in \mathfrak{A}$, we apply the existing decision procedure for $\mathbf{A}$ and Θ to ϑ with output $r_{\mathbf{A}} \in \{\text{YES}, \text{NO}\}$. If $r_{\mathbf{A}} = \text{YES}$ for all $\mathbf{A} \in \mathfrak{A}$, then our output is YES, else our output is NO. □

Example 4.22 (An infinite undecidable class of decidable structures)**.** Consider the language $\mathcal{L} = (0, 1, \ldots; \bar{H}^{(1)})$. Let $\mathfrak{A} = \{\mathbf{A}_1, \mathbf{A}_2, \ldots\}$ with $\mathbf{A}_i = (\mathbb{N}; 0, 1, \ldots; \bar{H}^{\mathbf{A}_i})$, where $\bar{H}^{\mathbf{A}_i}(n) = \top$ if and only if n is the Gödel number of a Turing machine that does not halt within its first i steps. Let $\Theta = \{\bar{H}(0), \bar{H}(1), \ldots\}$. Then each $\mathbf{A}_i \in \mathfrak{A}$ is decidable for Θ but $\mathfrak{A}$ is undecidable for Θ. ⌟

Theorem 4.23. *Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures, and let Θ be a set of sentences. If $\mathfrak{A}$ is complete and decidable for Θ, then every $\mathbf{A} \in \mathfrak{A}$ is decidable for Θ.*

Proof. Let $\mathbf{A} \in \mathfrak{A}$, and let $\vartheta \in \Theta$. We must produce the output YES if $\mathbf{A} \vDash \vartheta$, and the output NO else. We apply the existing decision procedure for $\mathfrak{A}$ to ϑ. If the output of that application is YES, then we know that $\mathfrak{A} \vDash \vartheta$, in particular $\mathbf{A} \vDash \vartheta$, and our output is YES. Else, we know by the completeness of $\mathfrak{A}$ that $\mathfrak{A} \vDash \neg\vartheta$, in particular $\mathbf{A} \vDash \neg\vartheta$, and our output is NO. □

Example 4.24 (An incomplete decidable class of undecidable structures)**.** Consider the language $\mathcal{L} = (0, 1, \ldots; R^{(1)})$. Let $M \subseteq \mathbb{N}$ be a non-recursive set. It follows that $\mathbb{N} \setminus M$ is non-recursive as well. Let $\mathfrak{A} = \{\mathbf{A}, \mathbf{B}\}$ with $\mathbf{A} = (\mathbb{N}; 0, 1, \ldots; R^{\mathbf{A}})$ and $\mathbf{B} = (\mathbb{N}; 0, 1, \ldots; R^{\mathbf{B}})$ where $R^{\mathbf{A}}(n) = \top$ if and only if $n \in M$, and $R^{\mathbf{B}}(n) = \top$ if and only if $n \in \mathbb{N} \setminus M$. We define sentences $\vartheta_n = R(n)$ and $\Theta = \{\, \vartheta_n \mid n \in \mathbb{N} \,\}$. We distinguish two cases:

(a) If $n \in M$, then $\mathbf{B} \nvDash \vartheta_n$, and it follows that $\mathfrak{A} \nvDash \vartheta_n$.

(b) If $n \in \mathbb{N} \setminus M$, then $\mathbf{A} \nvDash \vartheta_n$, and it follows that $\mathfrak{A} \nvDash \vartheta_n$.

Hence $\mathfrak{A}$ is decidable for Θ. On any input, the decision procedure will simply output NO. However, neither $\mathbf{A}$ nor $\mathbf{B}$ are decidable, because neither M nor $\mathbb{N} \setminus M$ are recursive. ⌟

The next two theorems give sufficient conditions for completeness and decidability of classes of $\mathcal{L}$-structures, respectively. Their hypotheses originate from Theorem 4.10. Both these theorems are going to play an important role for deriving completeness and decidability results based on QE results for concrete model classes in the following chapters.

Theorem 4.25 (Sufficient conditions for completeness)**.** *Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures, and assume that $\mathfrak{A}$ admits QE. Then the following hold:*

(i) If each atom that contains at most one variable is equivalent to either TRUE *or* FALSE *in $\mathfrak{A}$, then $\mathfrak{A}$ is complete.*

(ii) If $\mathcal{L}$ contains at least one constant symbol, and $\mathfrak{A}$ is complete for the set of all atomic sentences, then $\mathfrak{A}$ is complete.

Proof. Let ϑ be a sentence. We must show that either $\mathfrak{A} \models \vartheta$ or $\mathfrak{A} \models \neg\vartheta$.

(i) Assume that each atom that contains at most one variable is equivalent to either TRUE or FALSE in $\mathfrak{A}$. Quantifier elimination yields a quantifier-free formula φ' with $\mathfrak{A} \models \vartheta \longleftrightarrow \varphi'$ and $\mathcal{V}(\varphi') \subseteq \{x\}$ by Theorem 4.10. For each atomic formula α in φ', the function $\alpha^{\mathbf{A}} : A \to \{\top, \bot\}$, using the extended formula $\alpha(x)$, is constant and has the same value for all $\mathbf{A} \in \mathfrak{A}$. It follows that also $\varphi'^{\mathbf{A}} : A \to \{\top, \bot\}$, using the extended formula $\varphi'(x)$, is constant and has the same value for all $\mathbf{A} \in \mathfrak{A}$. The same holds for $\vartheta^{\mathbf{A}} = \varphi'^{\mathbf{A}}$, using the extended atomic formula $\vartheta(x)$.

(ii) Assume that $\mathcal{L}$ contains at least one constant symbol, and $\mathfrak{A}$ is complete for the set of all atomic sentences. Quantifier elimination yields a quantifier-free sentence ϑ' with $\mathfrak{A} \models \vartheta \longleftrightarrow \vartheta'$ and $\mathcal{V}(\vartheta') = \varnothing$ by Theorem 4.10. Each atomic formula α in ϑ' is an atomic sentence that has the same value $\alpha^{\mathbf{A}} \in \{\top, \bot\}$, using the extended formula $\alpha(\,)$ for all $\mathbf{A} \in \mathfrak{A}$. The same holds for $\vartheta^{\mathbf{A}} = \vartheta'^{\mathbf{A}}$, using the extended formula $\vartheta(\,)$. □

Theorem 4.26 (Sufficient conditions for decidability)**.** *Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures, and assume that $\mathfrak{A}$ admits effective QE. Then the following hold:*

*(i) If there is an algorithm taking atomic formulas α with most one variable as input and computing $\tau \in \{$*TRUE*, FALSE$\}$ such that $\mathfrak{A} \models \alpha \longleftrightarrow \tau$, then $\mathfrak{A}$ is complete and decidable.*

(ii) If $\mathcal{L}$ contains at least one constant symbol and $\mathfrak{A}$ is complete and decidable for the set of all atomic sentences, then $\mathfrak{A}$ is complete and decidable.

Proof. In both (i) and (ii), the completeness of $\mathfrak{A}$ follows by Theorem 4.25. It remains to be shown that $\mathfrak{A}$ is decidable. Let ϑ be a sentence. We must produce the output YES if $\mathfrak{A} \models \vartheta$, and the output NO else.

(i) Assume that there is an algorithm taking atomic formulas α with most one variable as input and computing $\tau \in \{$TRUE, FALSE$\}$ such that $\mathfrak{A} \models \alpha \longleftrightarrow \tau$. Use effective QE to compute a quantifier-free formula φ' with $\mathfrak{A} \models \vartheta \longleftrightarrow \varphi'$ and $\mathcal{V}(\varphi') \subseteq \{x\}$ by Theorem 4.10. For each of the finitely many atoms α in φ' apply the existing algorithm to compute $\tau \in \{$TRUE, FALSE$\}$ with $\mathfrak{A} \models \alpha \longleftrightarrow \tau$ and equivalently replace all occurrences of α in φ' with τ. At the end, φ' is

a Boolean combination of TRUE and FALSE, which can be simplified to either TRUE or FALSE. Output YES or NO, respectively.

(ii) Assume that $\mathcal{L}$ contains at least one constant symbol and that $\mathfrak{A}$ is decidable for atomic sentences. Use effective QE to compute a quantifier-free sentence ϑ' with $\mathfrak{A} \models \vartheta \longleftrightarrow \vartheta'$ and $\mathcal{V}(\vartheta') = \varnothing$ by Theorem 4.10. For each of the finitely many atoms α in φ' proceed as follows: Due to completeness, we know that either $\mathfrak{A} \models \alpha$ or $\mathfrak{A} \models \neg\alpha$. The assumed decision procedure will output YES for either α or $\neg\alpha$, respectively. Equivalently replace all occurrences of α in φ' with TRUE or FALSE, respectively. At the end, φ' is a Boolean combination of TRUE and FALSE, which can be simplified to either TRUE or FALSE. Output YES or NO, respectively. □

Example 4.27 (Infinite sets revisited)**.** Consider $\mathcal{L} = (\ )$ and recall from Lemma 4.6 that the class $\mathfrak{A} = \{\, \mathbf{A} \mid A \text{ is infinite} \,\}$ of $\mathcal{L}$-structures admits effective QE. All atomic $\mathcal{L}$-formulas with at most one variable are of the form $x = x$ with $x \in \mathcal{V}$, which is semantically equivalent to TRUE. Hence $\mathfrak{A}$ is complete and decidable by Theorem 4.26. ⌟

Corollary 4.28. *Let $\mathcal{L}$ be a finite language. Then every finite $\mathcal{L}$-structure is decidable.*

Proof. Let $\mathbf{A}$ be a finite $\mathcal{L}$-structure with universe $A = \{a_1, \ldots, a_n\}$, where $n \geq 1$. We switch to an extension language $\mathcal{L}' \supseteq \mathcal{L}$ with constant symbols for $a_1, \ldots, a_n$. The corresponding $\mathcal{L}'$-expansion $\mathbf{A}'$ of $\mathbf{A}$ admits effective QE by Lemma 4.4, $\mathcal{L}'$ has at least one constant symbol, $\{\mathbf{A}'\}$ is trivially complete, and atomic $\mathcal{L}'$-sentences in $\mathbf{A}'$ are decidable because all of the finitely many functions and relations in $\mathbf{A}'$ have suitable finite representations. It follows that $\mathbf{A}'$ is decidable by Theorem 4.26, and further that $\mathbf{A}$ is decidable by Lemma 4.19. □

Example 4.29 (A finite undecidable structure in an infinite language)**.** Consider the language $\mathcal{L} = (0^{(0)}, 1^{(0)};\ H_0^{(1)}, H_1^{(2)}, \ldots)$. Let $\mathbf{A} = (\{0,1\};\ 0, 1;\ H_0, H_1, \ldots)$ with $H_n^{\mathbf{A}}(a_n, \ldots, a_0) = \top$ if and only if $\sum_{i=0}^{n}(a_i \cdot 2^i)$ is the Gödel number of a Turing machine that halts. In other words, $a_n \ldots a_0 \in \{0,1\}^*$ is a binary representation of such a number. Then $\mathbf{A}$ is undecidable for the set $\Theta = \{\, H_n(\mathbf{c}) \mid n \in \mathbb{N} \setminus \{0\},\ \mathbf{c} \in \{0,1\}^n \,\}$ of all variable-free predicates. ⌟

The following result, which we state without a proof, is a well-known consequence of Gödel's Completeness Theorem. In contrast to Gödel's original theorem it does not refer to any deduction calculus.[3]

Theorem 4.30 (Gödel, 1929)**.** *Let $\mathcal{L}$ be a countable language, let Ξ be a recursively enumerable set of $\mathcal{L}$-sentences, and let $\mathfrak{A} = \mathrm{Mod}(\Xi)$. Then the set $\{\, \vartheta \in \mathcal{L}\text{-sentences} \mid \mathfrak{A} \models \vartheta \,\}$ is recursively enumerable.* □

Corollary 4.31. *Let $\mathcal{L}$ be a countable language, let Ξ be a recursively enumerable set of $\mathcal{L}$-sentences, and let $\mathfrak{A} = \mathrm{Mod}(\Xi)$. Let Θ be another set of $\mathcal{L}$-sentences. If $\mathfrak{A}$ is complete for Θ, then $\mathfrak{A}$ is decidable for Θ.*

Proof. Let $\vartheta \in \Theta$. We must produce the output YES if $\mathfrak{A} \models \vartheta$, and the output NO else. Let $(\nu_n)_{n\in\mathbb{N}}$ be an effective enumeration of the valid sentences of $\mathfrak{A}$, which exists by Theorem 4.30. Since $\mathfrak{A}$ is complete, there exists $n \in \mathbb{N}$ such that one of the following holds:

[3] We attribute the result to Gödel, as it is not too hard to prove from his Completeness Theorem. Significant contributions around Gödel's Completeness Theorem from a model theory perspective were made by Henkin in his PhD thesis in 1947.

(a) $\nu_n = \vartheta$ and for all $m \in \mathbb{N}$ with $m \neq n$ we have $\vartheta_m \neq \neg\vartheta$.

(b) $\nu_n = \neg\vartheta$ and for all $m \in \mathbb{N}$ with $m \neq n$ we have $\vartheta_m \neq \vartheta$.

We run the enumeration $(\nu_n)_{n\in\mathbb{N}}$ until, after finitely many steps, either ϑ or $\neg\vartheta$ occurs and output YES or NO, respectively. □

5 Quantifier Elimination for Sets and Linear Orders

5.1 Sets

We are going to use $t_1 \neq t_2$ as a shorthand for $\neg\, t_1 = t_2$ throughout this section. In Lemma 4.6 we have considered the empty language $\mathcal{L} = (\,)$ and showed that the class $\mathfrak{A}$ of all $\mathcal{L}$-structures with infinite universe as well as single $\mathcal{L}$-structures $\mathbf{B}_1$ with $|B_1| = 1$ and $\mathbf{B}_2$ with $|B_2| = 2$ admit effective QE. We have then shown in Lemma 4.11 that the class $\mathfrak{B} = \{\mathbf{B}_1, \mathbf{B}_2\}$ does not admit QE. The proof argument was essentially that the formula $\exists x(x \neq z_1)$ states that the universe has at least cardinality 2, which cannot be expressed as a quantifier-free $\mathcal{L}$-formula.

Our following definitions address this issue. We switch to a non-empty relational language $\mathcal{L}_{Sets}$, which has relation symbols $C_n^{(0)}$ for $n \in \{2, 3, \dots\}$. We introduce axioms Ξ_{Sets} stating that C_n holds if and only if there are at least n pairwise different elements in the universe:

$$\begin{aligned} \mathcal{L}_{Sets} &= \left(C_2^{(0)}, C_3^{(0)}, \dots\right), \\ \Xi_{Sets} &= \left\{ C_n \longleftrightarrow \exists x_1 \dots \exists x_n \bigwedge_{i=1}^{n} \bigwedge_{j=i+1}^{n} x_i \neq x_j \;\middle|\; n \in \{2, 3, \dots\} \right\}, \\ Sets &= \mathrm{Mod}(\Xi_{Sets}). \end{aligned} \tag{5.1}$$

With these definitions we have formally fixed that *Sets* is the class of all non-empty sets as $\mathcal{L}_{Sets}$-structures, where for all $\mathbf{S} \in Sets$ and for all $n \in \{2, 3, \dots\}$ we have $\mathbf{S} \vDash C_n$ if and only if $|S| \geq n$.

Theorem 5.1. *The class Sets admits effective QE.*

Proof. Following the reduction in the proof of Lemma 4.4 it suffices to consider formulas of the form (4.8) there, i.e.,

$$\varphi = \exists x \left[\bigwedge_{j=1}^{m} x \neq z_j \right] \tag{5.2}$$

where $m > 0$ and $z_1, \dots, z_m \in \mathcal{V}$. For $k \in \{1, \dots, m\}$ the following quantifier-free formula states that the variables $z_1, \dots, z_m$ take exactly k different values:

$$\eta_k = \bigvee_{h_1=1}^{m} \cdots \bigvee_{h_k=1}^{m} \left[\bigwedge_{j=1}^{m} \bigvee_{i=1}^{k} z_j = z_{h_i} \wedge \bigwedge_{i=1}^{k} \bigwedge_{l=i+1}^{k} z_{h_i} \neq z_{h_l} \right]. \tag{5.3}$$

The quantifier-free formula $\eta_k \wedge C_{k+1}$ additionally states that the universe is large enough to accommodate these k different values along with another value for the quantified variable x. We

finally obtain a quantifier-free equivalent

$$\varphi' = \bigvee_{k=1}^{m} (\eta_k \wedge C_{k+1}) \tag{5.4}$$

of φ by expressing a finite case distinction on k. □

Naturally, we are now interested in decidability and completeness. The following theorem can be viewed as a strong version of decidability. We will subsequently conclude decidability and a couple of related properties of the class *Sets* as corollaries.

Theorem 5.2. *Consider $\mathcal{L}_{Sets}$. For each sentence ϑ one can compute a finite union of disjoint intervals $M_\vartheta \subseteq \mathbb{N} \setminus \{0\}$ such that the following holds:*

(i) For all finite $\mathbf{S} \in Sets$ we have $\mathbf{S} \models \vartheta$ if and only if $|S| \in M_\vartheta$.

(ii) For all infinite $\mathbf{S} \in Sets$ we have $\mathbf{S} \models \vartheta$ if and only if M_ϑ is unbounded from above.

Proof. Let $y \in \mathcal{V}$. Then $\vartheta(y)$ is an extended sentence. Since *Sets* admits effective QE, we can compute an extended quantifier-free formula $\varphi'(y)$ such that $Sets \models \vartheta \longleftrightarrow \varphi'$, using Theorem 4.10(i). Next, we compute a DNF $\delta = \bigvee_i \gamma_i$ with $\gamma_i = \bigwedge_j \lambda_{ij}$ such that $\models \varphi' \longleftrightarrow \delta$. Again $\delta(y)$, $\gamma_i(y)$, and $\lambda_{ij}(y)$ are extended formulas, because δ contains the same atomic formulas and thus the same variables as φ'. For each λ_{ij} we compute

$$M_{\lambda_{ij}} = \begin{cases} [1\,..\,\infty) & \text{if} \quad \lambda_{ij} \in \{\text{TRUE},\ y = y\} \\ \varnothing & \text{if} \quad \lambda_{ij} \in \{\text{FALSE},\ y \neq y\} \\ [n\,..\,\infty) & \text{if} \quad \lambda_{ij} = C_n \\ [1\,..\,n-1] & \text{if} \quad \lambda_{ij} = \neg C_n. \end{cases} \tag{5.5}$$

For each γ_i we compute $M_{\gamma_i} = \bigcap_j M_{\lambda_{ij}}$, and for δ we compute $M_\delta = \bigcup_i M_{\gamma_i}$ with properties (i) and (ii). Since ϑ and δ are equivalent in *Sets*, we can set $M_\vartheta = M_\delta$. □

Corollary 5.3. *The class Sets is decidable but not complete.*

Proof. For decidability, let ϑ be a sentence. We must produce the output YES if $Sets \models \vartheta$, and the output NO else. Compute M_ϑ according to Theorem 5.2. If $M_\vartheta = [1\,..\,\infty)$, then output YES, else output NO.

Sets is complete if and only if for all sentences ϑ either $M_\vartheta = [1\,..\,\infty)$ or $M_\vartheta = \varnothing$. However, $M_{C_2} = [2\,..\,\infty)$. □

We leave the proof of the following consequences of Theorem 5.2 as an exercise. Notice that $Sets_\infty$ is the class $\mathfrak{A}$ from Lemma 4.6.

Corollary 5.4 (Complete and decidable subclasses of *Sets*)**.**

(i) $Sets_n = \{\, \mathbf{S} \in Sets : |S| = n \,\}$ is complete and decidable for all $n \in \mathbb{N} \setminus \{0\}$.

(ii) $Sets_\infty = \{\, \mathbf{S} \in Sets : S \text{ is infinite} \,\}$ is complete and decidable. □

Let $\mathcal{L}$ be an arbitrary language. A class $\mathfrak{A}$ of $\mathcal{L}$-structures has a *small model property* if there exists a computable function $k : \mathcal{L}\text{-sentences} \to \mathbb{N} \setminus \{0\}$ such that every sentence ϑ that is satisfiable in $\mathfrak{A}$ has a model $\mathbf{A} \in \mathfrak{A}$ with $|A| = k(\vartheta)$. The small model property entails the *finite model property*: If ϑ is satisfiable in $\mathfrak{A}$, then ϑ has a finite model in $\mathfrak{A}$.

Corollary 5.5 (Small model property)**.** *Consider $\mathcal{L}_{Sets}$ and let ϑ be a sentence. Assume that there is an infinite $\mathbf{S} \in Sets$ with $\mathbf{S} \vDash \vartheta$. Then one can compute $k_\vartheta \in \mathbb{N} \setminus \{0\}$ such that $\mathbf{T} \vDash \vartheta$ for all $\mathbf{T} \in Sets$ with $|T| \geq k_\vartheta$.*

Proof. Compute M_ϑ according to Theorem 5.2. From $\mathbf{S} \vDash \vartheta$ it follows that M_ϑ is unbounded from above. Hence one and only one of the disjoint intervals in M_ϑ is of the form $[n \,..\, \infty)$ with $n \in \mathbb{N} \setminus \{0\}$. Choose $k_\vartheta \in [n \,..\, \infty)$. □

Notice that even with the choice $k_\vartheta = n$ in the proof, $|T| \geq k_\vartheta$ is only a sufficient condition for $\mathbf{T} \vDash \vartheta$.

5.2 Use Case: Graph Coloring

Figure 5.1 shows a map of Europe and lists the member countries of the European Union. We identify the countries with their numbers $V = \{1, \ldots, 27\} \subseteq \mathbb{N}$. For each country $i \in V$ we introduce a variable c_i and define constraints $\gamma_i = \bigwedge_j c_i \neq c_j$ where j runs over all countries that share a border with country i:

$$
\begin{aligned}
\gamma_1 &= \textstyle\bigwedge_{j\in\{11,6,24,13,25,15\}} c_1 \neq c_j, & \gamma_2 &= \textstyle\bigwedge_{j\in\{20,11,18,10\}} c_2 \neq c_j,\\
\gamma_3 &= \textstyle\bigwedge_{j\in\{23,12\}} c_3 \neq c_j, & \gamma_4 &= \textstyle\bigwedge_{j\in\{25,13\}} c_4 \neq c_j,\\
\gamma_5 &= \text{TRUE}, & \gamma_6 &= \textstyle\bigwedge_{j\in\{11,21,24,1\}} c_6 \neq c_j,\\
\gamma_7 &= (c_7 \neq c_{11}), & \gamma_8 &= (c_8 \neq c_{16}),\\
\gamma_9 &= (c_9 \neq c_{27}), & \gamma_{10} &= \textstyle\bigwedge_{j\in\{2,18,11,15,26\}} c_{10} \neq c_j,\\
\gamma_{11} &= \textstyle\bigwedge_{j\in\{7,21,6,1,10,18,2,20\}} c_{11} \neq c_j, & \gamma_{12} &= (c_{12} \neq c_3),\\
\gamma_{13} &= \textstyle\bigwedge_{j\in\{24,23,4,25,1\}} c_{13} \neq c_j, & \gamma_{14} &= \text{TRUE},\\
\gamma_{15} &= \textstyle\bigwedge_{j\in\{10,1,25\}} c_{15} \neq c_j, & \gamma_{16} &= \textstyle\bigwedge_{j\in\{8,17\}} c_{16} \neq c_j,\\
\gamma_{17} &= \textstyle\bigwedge_{j\in\{16,21\}} c_{17} \neq c_j, & \gamma_{18} &= \textstyle\bigwedge_{j\in\{2,11,10\}} c_{18} \neq c_j,\\
\gamma_{19} &= \text{TRUE}, & \gamma_{20} &= \textstyle\bigwedge_{j\in\{11,2\}} c_{20} \neq c_j,\\
\gamma_{21} &= \textstyle\bigwedge_{j\in\{17,25,6,11\}} c_{21} \neq c_j, & \gamma_{22} &= (c_{22} \neq c_{26}),\\
\gamma_{23} &= \textstyle\bigwedge_{j\in\{3,13\}} c_{23} \neq c_j, & \gamma_{24} &= \textstyle\bigwedge_{j\in\{21,13,1,6\}} c_{24} \neq c_j,\\
\gamma_{25} &= \textstyle\bigwedge_{j\in\{1,13,4,15\}} c_{25} \neq c_j, & \gamma_{26} &= \textstyle\bigwedge_{j\in\{10,22\}} c_{26} \neq c_j,\\
\gamma_{27} &= (c_{27} \neq c_9).
\end{aligned}
\tag{5.6}
$$

Let $\psi = \bigwedge_{i\in V} \gamma_i$. Quantifier elimination on $\varphi_1 = (\exists c_i)_{i\in V}\, \psi$ yields $\varphi_1' = C_4$. Since $Sets \vDash \varphi \longleftrightarrow \varphi'$ it follows that $\mathbf{A} \vDash \varphi$ if and only if $|A| \geq 4$ for all $\mathbf{A} \in Sets$. We can consider the elements of the universe A of each $\mathbf{A} \in Sets$ as colors. In this view we have deduced that all

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czechia
7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Ireland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Malta
20. Netherlands
21. Poland
22. Portugal
23. Romania
24. Slovakia
25. Slovenia
26. Spain
27. Sweden

Figure 5.1: The member countries of the European Union (as of 2023)

pairs of countries with a common border can be colored differently on our map if and only if there are at least 4 different colors available altogether.

More abstractly, we have solved an instance of the *vertex coloring problem* for graphs, where the vertices are the countries V and the undirected edges are the neighborhood relation on the countries. Other applications of vertex coloring include scheduling problems, register allocation in compiler optimization, and Sudoku puzzles. While there are certainly more efficient algorithms for graph coloring, including heuristic ones, our quantifier elimination approach is more general. First, there are not only existential quantifiers available but also universal quantifiers, which admits quantifier alternation. Second, we can use free variables and consider parametric problems.

As an example for the use of universal quantifiers and quantifier alternation consider the following problem: Find the smallest number of colors necessary such that any admissible coloring of $W = \{6, 13, 24, 25\} \subseteq V$, i.e., of Czechia, Hungary, Slovakia, Slovenia, can be extended to an admissible coloring of the complete map V. We formalize our problem as follows, where χ specifies admissible colorings of W:

$$\varphi_2 = (\forall c_i)_{i\in W}\big[\chi \longrightarrow (\exists c_j)_{j\in V\setminus W}\,\psi\big], \quad \chi = (c_6 \neq c_{24} \wedge c_{24} \neq c_{13} \wedge c_{13} \neq c_{25}). \tag{5.7}$$

Quantifier elimination on φ_2 yields $\varphi_2' = \neg C_2 \vee C_5$. The condition $\neg C_2$ covers the degenerate case that χ is unsatisfiable, i.e., there is no admissible coloring of W. This case can be formally excluded by considering $(\exists c_i)_{i\in W}\,\chi \wedge \varphi_2$ instead of φ_2. The condition C_5 tells us that we need at least five colors.

As an example of a parametric problem consider $\varphi_3 = (\exists c_j)_{j\in V\setminus W}\,\psi$, which leaves the colors of W as free variables. Quantifier elimination yields

$$\varphi_3' = (\chi \wedge c_6 = c_{25} \wedge C_4) \vee (\chi \wedge c_6 = c_{13} \wedge C_4) \vee (\chi \wedge c_{24} = c_{25} \wedge C_4) \vee (\chi \wedge C_5). \tag{5.8}$$

This again states that five colors are generally sufficient. Furthermore, it provides three equational constraints on the colors of W each of which independently admits a coloring with only four colors.

5.3 Dense Linear Orders Without Endpoints

We consider the relational language $\mathcal{L}_{Losets} = (<)$ of linear ordered sets and $\mathbf{R} = (\mathbb{R};\ <)$ with the natural strict order on $\mathbb{R}$. As a linear ordered set, $\mathbf{R}$ has positive normal forms according to Example 3.28.

Lemma 5.6. $\mathbf{R} = (\mathbb{R};\ <)$ admits effective QE.

Proof. Consider a positive 1-primitive formula

$$\varphi = \exists x \left[\bigwedge_{i=1}^{m} x = u_i \wedge \bigwedge_{j=1}^{n} v_j < x \wedge \bigwedge_{k=1}^{p} x < w_k\right], \tag{5.9}$$

where $u_i,\ v_j,\ w_k \in \mathcal{V}$. Equations $x = x$ can be deleted from the conjunctions in (5.9) via semantic equivalence to TRUE. Similarly, if there is a literal $x < x$, then that literal and

thus the entire formula φ in (5.9) is equivalent to FALSE in $\mathbf{R}$. We may now assume that $x \notin \{u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots, w_p\}$. If $m > 0$, then (5.9) is semantically equivalent to the quantifier-free formula

$$\varphi' = \bigwedge_{i=2}^{m} u_1 = u_i \wedge \bigwedge_{j=1}^{n} v_j < u_1 \wedge \bigwedge_{k=1}^{p} u_1 < w_k. \tag{5.10}$$

Assume now that $m = 0$. Then (5.9) is of the form

$$\exists x \left[\bigwedge_{j=1}^{n} v_j < x \wedge \bigwedge_{k=1}^{p} x < w_k \right]. \tag{5.11}$$

If $n = 0$, then (5.11) is equivalent to TRUE, because $\mathbb{R}$ has no minimum. Similarly, If $p = 0$, then (5.11) is equivalent to TRUE, because $\mathbb{R}$ has no maximum. Assume now that both $n > 0$ and $p > 0$. Then (5.11) is equivalent to the quantifier-free formula

$$\bigwedge_{j=1}^{n} \bigwedge_{k=1}^{p} v_j < w_k. \tag{5.12}$$

From (5.11) to (5.12) one uses the transitivity of the order. Conversely, from (5.12) to (5.11) one uses the density of $\mathbb{R}$: If $\max_j v_j < \min_k w_k$, then there exists $x \in \mathbb{R}$ such that $\max_j v_j < x < \min_k w_k$, e.g., $x = \frac{1}{2}(\max_j v_j + \min_k w_k)$. □

An analysis of the proof shows that we have used only the following *elementary properties* of $\mathbf{R}$, in the sense that those properties can be formulated as first-order formulas:

(i) $\mathbf{R}$ is a linear ordered set, which is irreflexive, connected, and transitive:

$$\Xi_{Losets} = \{\neg\, x < x,\ x < y \vee x = y \vee y < x,\ x < y \wedge y < z \longrightarrow x < z\}; \tag{5.13}$$

(ii) $\mathbf{R}$ is dense:

$$\Xi_{Dense} = \{x < y \longrightarrow \exists z(x < z \wedge z < y)\}; \tag{5.14}$$

(iii) $\mathbf{R}$ has no minimum and maximum, which we call *endpoints*:

$$\Xi_{NoEndpoints} = \{\exists y(x < y),\ \exists y(y < x)\}. \tag{5.15}$$

This yields the axioms and the class of all *dense linear orders without endpoints*:

$$\Xi_{DensLo} = \Xi_{Losets} \cup \Xi_{Dense} \cup \Xi_{NoEndpoints}, \quad DensLo = \mathrm{Mod}(\Xi_{DensLo}). \tag{5.16}$$

Our axiomatization allows to apply the proof of Lemma 5.6 to the class *DensLo* instead of the single structure $\mathbf{R} \in DensLo$, which gives us the following theorem.

Theorem 5.7. *The class DensLo admits effective QE.* □

Corollary 5.8. *The class DensLo is complete and decidable.*

Proof. In $\mathcal{L}_{Losets}$ all atomic formulas with at most one variable are of one of the forms $y = y$ or $y < y$ with $y \in \mathcal{V}$. We have $\vDash y = y \longleftrightarrow$ TRUE and $\mathit{DensLo} \vDash y < y \longleftrightarrow$ FALSE. Hence *DensLo* is complete and decidable by Theorem 4.26(i). □

Example 5.9 (Dense linear orders without endpoints)**.** Of course, $(\mathbb{R};\ <) \in \mathit{DensLo}$. Further examples are

$$(\mathbb{Q};\ <), \quad (\mathbb{R} \setminus \mathbb{Q};\ <), \quad (\mathbb{Q} \cup (0,1);\ <) \in \mathit{DensLo}, \tag{5.17}$$

where $(0, 1)$ denotes the open real interval. However,

$$(\mathbb{N};\ <), \quad (\mathbb{Z};\ <), \quad ([0,1];\ <) \notin \mathit{DensLo}, \tag{5.18}$$

where $[0, 1]$ denotes the closed real interval. The linear ordered sets $(\mathbb{N};\ <)$ and $(\mathbb{Z};\ <)$ are not dense; both $(\mathbb{N};\ <)$ and $([0, 1];\ <)$ have endpoints. Another positive example is

$$(\mathbb{N} \times \mathbb{R};\ <_{\text{lex}}) \in \mathit{DensLo}, \tag{5.19}$$

where the *lexicographic order* is defined as $(x_1, x_2) <_{\text{lex}} (y_1, y_2)$ if and only if $x_1 < y_1$ or $x_1 = y_1$ and $x_2 < y_2$. However,

$$(\mathbb{R} \times \mathbb{N};\ <_{\text{lex}}) \notin \mathit{DensLo}, \tag{5.20}$$

because $(\mathbb{R} \times \mathbb{N};\ <_{\text{lex}})$ is not dense. ⌟

As an exercise, decide the sentence $\forall x \exists y (x < y \wedge \forall z (x < z \longrightarrow y = z \vee y < z))$ in *DensLo*.

5.4 Discrete Linear Orders with Left Endpoint

We stay with the relational language $\mathcal{L}_{Losets} = (<)$ of linear ordered sets and consider now $\mathbf{N}_0 = (\mathbb{N};\ <)$ as a discrete counterpart of $\mathbf{R} = (\mathbb{R};\ <)$ in the previous section. As a linear ordered set, $\mathbf{N}_0$ also has positive normal forms according to Example 3.28. In contrast to $\mathbf{R}$, we obtain a negative result regarding QE for $\mathbf{N}_0$.

Theorem 5.10. $\mathbf{N}_0 = (\mathbb{N};\ <)$ *does not admit QE.*

Proof. According to Theorem 4.12 it is sufficient to find a definable set that is not quantifier-free definable. Consider the extended formula

$$\varphi(y) \ = \ \forall x (x = y \vee y < x)(y), \tag{5.21}$$

which defines $[\varphi]^{\mathbf{N}_0} = \{0\}$. Let $\varphi'(y)$ be an extended quantifier-free formula. Then $\mathcal{V}(\varphi) \subseteq \{y\}$, and the only possible atomic formulas in φ' are $y = y$ and $y < y$. We have $\vDash y = y \longleftrightarrow$ TRUE and $\mathbf{N}_0 \vDash y < y \longleftrightarrow$ FALSE. It follows that $\mathbf{N}_0 \vDash \varphi' \longleftrightarrow$ TRUE or $\mathbf{N}_0 \vDash \varphi' \longleftrightarrow$ FALSE and thus $[\varphi']^{\mathbf{N}_0} = \mathbb{N}$ or $[\varphi']^{\mathbf{N}_0} = \varnothing$. □

This proof suggests to add a constant symbol 0 and switch to the language $\mathcal{L}_1 = (0;\ <)$ and the $\mathcal{L}$-structure $\mathbf{N}_1 = (\mathbb{N};\ 0;\ <)$. This obviously allows a quantifier-free definition of $\{0\}$. However, it also adds to the expressiveness on the side of the quantified formulas. We again obtain a negative result.

Theorem 5.11. $\mathbf{N}_1 = (\mathbb{N};\ 0;\ <)$ *does not admit QE.*

Proof. Again, we use Theorem 4.12 and find a definable set that is not quantifier-free definable. Consider the extended formula $\varphi(y)$ with

$$\varphi \ = \ 0 < y \wedge \forall x(0 < x \longrightarrow x = y \vee y < x), \tag{5.22}$$

which defines $[\varphi]^{\mathbf{N}_1} = \{1\}$. Let $\varphi'(y)$ be an extended quantifier-free formula, without loss of generality, in positive normal form. For all atomic formulas α in φ' we have

$$\alpha \in \{0 = 0,\ 0 = y,\ y = 0,\ y = y,\ 0 < 0,\ 0 < y,\ y < 0,\ y < y\}, \tag{5.23}$$

and for corresponding extended atomic formulas $\alpha(y)$ we obtain

$$[\alpha]^{\mathbf{N}_1} \in D, \quad D = \big\{\varnothing,\ \{0\},\ \mathbb{N} \setminus \{0\},\ \mathbb{N}\big\}. \tag{5.24}$$

Since φ' is reduced to $\vee$, $\wedge$, the set $[\varphi']^{\mathbf{N}_1}$ is formed from the sets in D via unions and intersections. However, D is closed under unions and intersections. It follows that also $[\varphi']^{\mathbf{N}_1} \in D$. Hence $[\varphi]^{\mathbf{N}_1} = \{1\}$ is not quantifier-free definable. □

If we now added another constant symbol 1 yielding $\mathcal{L}_1' = (0, 1;\ <)$ and considered the $\mathcal{L}_1'$-structure $(\mathbb{N};\ 0, 1;\ <)$, we would find that $\{2\}$ is definable but not quantifier-free definable, and so on. In fact, it easily follows by induction that $\{n\}$ is definable for all $n \in \mathbb{N}$ already in $\mathbf{N}_0$.

The most economic way to have terms available for all elements of $\mathbb{N}$ is the introduction of the successor function known from Peano arithmetic. We define $\mathcal{L}_2 = (0, s^{(1)};\ <)$ and consider $\mathbf{N}_2 = (\mathbb{N};\ 0, s;\ <)$ with $s^{\mathbf{N}_2}(n) = n + 1$. As a shorthand notation for terms we define s^n as the n-fold application of the function symbol s, formally $s^0(t) = t$ and $s^{n+1}(t) = s(s^n(t))$. This yields $s^n(t)^{\mathbf{N}_2} = t^{\mathbf{N}_2} + n$, in particular $s^n(0)^{\mathbf{N}_2} = n$.

Lemma 5.12. $\mathbf{N}_2 = (\mathbb{N};\ 0, s;\ <)$ admits effective QE.

Proof. Consider a positive 1-primitive formula

$$\varphi \ = \ \exists x \left[\bigwedge_{i=1}^{m} s^{a_i}(x) = t_i \wedge \bigwedge_{j=1}^{n} u_j < s^{b_j}(x) \wedge \bigwedge_{k=1}^{p} s^{c_k}(x) < v_k \wedge \bigwedge_{l=1}^{r} s^{d_l}(x) \underset{=}{\leq} s^{e_l}(x) \right], \tag{5.25}$$

where $a_i, b_j, c_k, d_l, e_l \in \mathbb{N}$, and t_i, u_j, v_k are terms of the form $s^h(0)$ or $s^h(y)$, where $h \in \mathbb{N}$ and y is variable different from x. We have

$$\mathbf{N}_2 \vDash s^{d_l}(x) \underset{=}{\leq} s^{e_l}(x) \longleftrightarrow \begin{cases} \text{TRUE} \\ \text{FALSE} & \text{if} \quad d_l < e_l \\ \text{FALSE} \\ \text{TRUE} & \text{if} \quad d_l = e_l \\ \text{FALSE} \\ \text{FALSE} & \text{if} \quad d_l > e_l. \end{cases} \tag{5.26}$$

Therefore, the last conjunction $\bigwedge_l s^{d_l}(x) \underset{=}{\leq} s^{e_l}(x)$ in (5.25) can be equivalently replaced with either FALSE or TRUE. In the former case, $\varphi' = \text{FALSE}$ is a quantifier-free equivalent for φ and we are finished. Otherwise, we have reduced our QE problem from (5.25) to

$$\exists x \left[\bigwedge_{i=1}^{m} s^{a_i}(x) = t_i \wedge \bigwedge_{j=1}^{n} u_j < s^{b_j}(x) \wedge \bigwedge_{k=1}^{p} s^{c_k}(x) < v_k \right]. \tag{5.27}$$

Let $\mu = \max_{i,j,k}\{a_i, b_j, c_k\}$, and let $t'_i = s^{\mu-a_i}(t_i)$, $u'_j = s^{\mu-b_j}(u_j)$, and $v'_k = s^{\mu-c_k}(v_k)$. Then (5.27) is equivalent to

$$\exists x \left[\bigwedge_{i=1}^{m} s^{\mu}(x) = t'_i \wedge \bigwedge_{j=1}^{n} u'_j < s^{\mu}(x) \wedge \bigwedge_{k=1}^{p} s^{\mu}(x) < v'_k \right]. \tag{5.28}$$

If $m > 0$, then (5.28) is equivalent to

$$\exists x (s^{\mu}(x) = t'_1) \wedge \bigwedge_{i=2}^{m} t'_1 = t'_i \wedge \bigwedge_{j=1}^{n} u'_j < t'_1 \wedge \bigwedge_{k=1}^{p} t'_1 < v'_k, \tag{5.29}$$

which is in turn equivalent to the quantifier-free formula

$$\varphi' \;=\; \left[s^{\mu}(0) = t'_1 \vee s^{\mu}(0) < t'_1 \right] \wedge \bigwedge_{i=2}^{m} t'_1 = t'_i \wedge \bigwedge_{j=1}^{n} u'_j < t'_1 \wedge \bigwedge_{k=1}^{p} t'_1 < v'_k, \tag{5.30}$$

and we are finished. Otherwise, we have reduced our QE problem from (5.28) to

$$\exists x \left[\bigwedge_{j=1}^{n} u'_j < s^{\mu}(x) \wedge \bigwedge_{k=1}^{p} s^{\mu}(x) < v'_k \right]. \tag{5.31}$$

If $p = 0$, then (5.31) is equivalent to the quantifier-free formula

$$\varphi' = \text{TRUE}, \tag{5.32}$$

because $\mathbb{N}$ has no maximum, and we are finished. Assume now that $p > 0$. If $n = 0$, then (5.31) is equivalent to the quantifier-free formula

$$\varphi' = \bigwedge_{k=1}^{p} s^{\mu}(0) < v'_k, \tag{5.33}$$

and we are finished. The difference between (5.32) and (5.33) is due to the fact that $\mathbb{N}$ has a minimum. Therefore we cannot make the term function $s^{\mu}(x)^{\mathbf{N}_2} : \mathbb{N} \to \mathbb{N}$ arbitrarily small by choosing $x \in \mathbb{N}$. Its range of possible values is bounded from below by $\mu = s^{\mu}(x)^{\mathbf{N}_2}(0) = s^{\mu}(0)^{\mathbf{N}_2}$, and (5.33) guarantees that $\mu < {v'_k}^{\mathbf{N}_2}$ for all k. Finally, assume that also $n > 0$. Then (5.31) is equivalent to the quantifier-free formula

$$\varphi' = \bigwedge_{j=1}^{n} \bigwedge_{k=1}^{p} s(u'_j) < v'_k \wedge \bigwedge_{k=1}^{p} s^{\mu}(0) < v'_k. \tag{5.34}$$

The first part of (5.34) resembles (5.12) in the proof of Lemma 5.6 for $(\mathbb{R}; <)$. In the absence of density of $\mathbb{N}$, we put $s(u'_j)$ instead of u'_j to ensure that there is a gap between $\max_j {u'_j}^{\mathbf{N}_2}$ and $\min_k {v'_k}^{\mathbf{N}_2}$ that can accommodate $s^{\mu}(0)^{\mathbf{N}_2}$. □

Similarly to **R** in the previous section, an analysis of the proof shows that we have used only certain elementary properties of $\mathbf{N}_2$, which are the following:

(i) $\mathbf{N}_2$ is a linear ordered set, for which the axioms Ξ_{Losets} have been introduced in (5.13);

(ii) $\mathbf{N}_2$ has a minimum, which we call *left endpoint*:

$$\Xi_{LeftEndpoint} \;=\; \{0 = x \vee 0 < x\}; \tag{5.35}$$

(iii) $s^{\mathbf{N}_2}$ is the successor function:

$$\Xi_{Succ} \;=\; \{x < s(x),\; x < y \longrightarrow s(x) = y \vee s(x) < y,\; 0 < y \longrightarrow \exists x(s(x) = y)\}. \tag{5.36}$$

From $x < s(x)$ it follows that there is no right endpoint. Furthermore, one can prove $x < y \longleftrightarrow s(x) < s(y)$ and the injectivity $s(x) = s(y) \longrightarrow x = y$ of the successor function.

This yields the axioms and the class of all *discrete linear orders with left endpoint*:

$$\Xi_{DiscrLo} = \Xi_{Losets} \cup \Xi_{LeftEndpoint} \cup \Xi_{Succ}, \quad DiscrLo = \mathrm{Mod}(\Xi_{DiscrLo}). \tag{5.37}$$

One can now generalize and apply the proof of Lemma 5.12 to the class *DiscrLo* instead of the single $\mathcal{L}_2$-structure $\mathbf{N}_2 \in DiscrLo$. This yields the following theorem.

Theorem 5.13. *The class DiscrLo admits effective QE.* □

Corollary 5.14. *The class DiscrLo is complete and decidable.*

Proof. The language $\mathcal{L}_2$ has a constant symbol 0. All atomic sentences in $\mathcal{L}_2$ are of the form $s^m(0) \mathrel{\substack{<\\=}} s^n(0)$ with $m, n \in \mathbb{N}$. We have

$$DiscrLo \vDash s^m(0) \mathrel{\substack{<\\=}} s^n(0) \longleftrightarrow \begin{cases} \begin{smallmatrix}\text{TRUE}\\ \text{FALSE}\end{smallmatrix} & \text{if} \quad m < n \\ \begin{smallmatrix}\text{FALSE}\\ \text{TRUE}\end{smallmatrix} & \text{if} \quad m = n \\ \begin{smallmatrix}\text{FALSE}\\ \text{FALSE}\end{smallmatrix} & \text{if} \quad m > n. \end{cases} \tag{5.38}$$

Hence *DiscrLo* is complete and decidable for the set of all atomic sentences, and general completeness and decidability follow by Theorem 4.26(ii). □

Consider the language $\mathcal{L}_{Losets}$ and linear ordered sets $\mathbf{A} = (A;\, <)$ and $\mathbf{B} = (B;\, <)$ with $A \cap B = \varnothing$. We define the *sum* of the linear orders $\mathbf{A}$ and $\mathbf{B}$ as $\mathbf{A} \oplus \mathbf{B} = (A \dot\cup B;\, <)$, where

$$<^{\mathbf{A}\oplus\mathbf{B}}(x, y) \;=\; \begin{cases} <^{\mathbf{A}}(x, y) & \text{if} \quad x, y \in A \\ \top & \text{if} \quad x \in A,\; y \in B \\ <^{\mathbf{B}}(x, y) & \text{if} \quad x, y \in B \\ \bot & \text{else.} \end{cases} \tag{5.39}$$

It is easy to see that $\mathbf{A} \oplus \mathbf{B}$ is again a linear ordered set. Going further, we can generalize the sum of linear orders to $\mathbf{A}, \mathbf{B} \in DiscrLo$, where we define

$$0^{\mathbf{A}\oplus\mathbf{B}} \;=\; 0^{\mathbf{A}}, \qquad s^{\mathbf{A}\oplus\mathbf{B}}(x) \;=\; \begin{cases} s^{\mathbf{A}}(x) & \text{if} \quad x \in A \\ s^{\mathbf{B}}(x) & \text{if} \quad x \in B. \end{cases} \tag{5.40}$$

With these definitions, $\mathbf{A} \oplus \mathbf{B}$ might or might not be a discrete linear order with left endpoint. In other words, the class *DiscrLo* is not closed under our generalized sum of linear orders. Nevertheless, $\mathbf{A} \oplus \mathbf{B}$ is always a well-defined $\mathcal{L}_2$-structure.

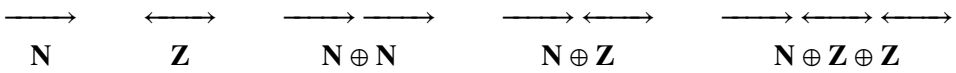
Example 5.15 (Some sums of linear orders with left endpoint)**.** Consider the language $\mathcal{L}_2$. Let $\mathbf{N} = (\mathbb{N};\ 0, s;\ <)$, $\mathbf{Z} = (\mathbb{Z};\ 0, s;\ <)$. Then

$$\mathbf{N} \oplus \mathbf{Z} \in \mathit{DiscrLo}, \quad \mathbf{N} \oplus \mathbf{Z} \oplus \mathbf{Z} \in \mathit{DiscrLo} \tag{5.41}$$

assuming without loss of generality that $\mathbb{N} \cap \mathbb{Z} = \varnothing$. However,

$$\mathbf{Z}, \quad \mathbf{N} \oplus \mathbf{N} \notin \mathit{DiscrLo}, \tag{5.42}$$

where $\mathbf{N} \oplus \mathbf{N}$ should be read as adding two isomorphic copies of $\mathbf{N}$ with disjoint universes. The linear orders considered here can be visualized as follows:



(5.43)

The picture suggests that $\mathbf{Z}$ has no left endpoint and that the zero of the second summand of $\mathbf{N} \oplus \mathbf{N}$ is not a successor. ⌟

6 Substructures

6.1 Substructures

Let $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ be a language, and let $\mathbf{S}$ and $\mathbf{A}$ be $\mathcal{L}$-structures such that the following holds:

(i) $S \subseteq A$,

(ii) $f^{\mathbf{S}} = f^{\mathbf{A}}|_{S^n}$ for all $f^{(n)} \in \mathcal{F}$,

(iii) $R^{\mathbf{S}} = R^{\mathbf{A}}|_{S^n}$ for all $R^{(n)} \in \mathcal{R}$.

Then we call $\mathbf{S}$ a *substructure* of $\mathbf{A}$, we call $\mathbf{A}$ an *extension structure* of $\mathbf{S}$, and we write $\mathbf{S} \subseteq \mathbf{A}$.

Given an $\mathcal{L}$-structure $\mathbf{A}$, universes of substructures of $\mathbf{A}$ can be characterized among the subsets of A as follows.

Lemma 6.1 (Universes of substructures)**.** Let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $\varnothing \subsetneq S \subseteq A$. Then S is the universe of a substructure $\mathbf{S}$ of $\mathbf{A}$ if and only if S is closed under the functions $f^{\mathbf{A}}$ for $f \in \mathcal{F}$. In the positive case, $\mathbf{S}$ is uniquely determined by $\mathbf{A}$ and S. □

Proof. Let $\mathbf{S} \subseteq \mathbf{A}$ with universe S, let $f^{(n)} \in \mathcal{F}$, and let $\mathbf{s} \in S^n$. Then $f^{\mathbf{A}}|_{S^n} = f^{\mathbf{S}}$ and $f^{\mathbf{S}} : S^n \to S$. It follows that $f^{\mathbf{A}}(\mathbf{s}) = f^{\mathbf{S}}(\mathbf{s}) \in S$.

Conversely, assume that S is closed under the functions $f^{\mathbf{A}}$. We define an $\mathcal{L}$-structure $\mathbf{S}$ with universe S as follows: For $f^{(n)} \in \mathcal{F}$ and $\mathbf{s} \in S^n$ set $f^{\mathbf{S}}(\mathbf{s}) = f^{\mathbf{A}}(\mathbf{s})$, and for $R^{(n)} \in \mathcal{R}$ and $\mathbf{s} \in S^n$ set $R^{\mathbf{S}}(\mathbf{s}) = R^{\mathbf{A}}(\mathbf{s})$. Then $\mathbf{S} \subseteq \mathbf{A}$, and it is easy to see that this is the only possible definition of $\mathbf{S}$ that yields $\mathbf{S} \subseteq \mathbf{A}$. □

The following lemma states that the defining conditions (ii) and (iii) for substructures generalize to term functions and characteristic functions of quantifier-free formulas. We leave the proof as an exercise.

Lemma 6.2. Let $\mathbf{S} \subseteq \mathbf{A}$ be $\mathcal{L}$-structures. Then the following hold:

(i) Let $t(\mathbf{x})$ be an extended term with $\mathbf{x} \in \mathcal{V}^n$. Then $t^{\mathbf{S}} = t^{\mathbf{A}}|_{S^n}$. For all $\mathbf{s} \in S^n$ it follows that $t^{\mathbf{S}}(\mathbf{s}) = t^{\mathbf{A}}(\mathbf{s})$.

(ii) Let $\varphi(\mathbf{x})$ be an extended quantifier-free formula with $\mathbf{x} \in \mathcal{V}^n$. Then $\varphi^{\mathbf{S}} = \varphi^{\mathbf{A}}|_{S^n}$. For all $\mathbf{s} \in S^n$ it follows that $\mathbf{S} \models \varphi(\mathbf{s})$ if and only if $\mathbf{A} \models \varphi(\mathbf{s})$. □

The following example illustrates the relevance of the assumption that φ is quantifier-free in part (ii) of the previous lemma:

Example 6.3. Consider $\mathcal{L}_{Rings}$, and let $\mathbf{Q} = (\mathbb{Q};\ 0, 1, +, -, \cdot)$, $\mathbf{R} = (\mathbb{R};\ 0, 1, +, -, \cdot)$. Then $\mathbf{Q} \subseteq \mathbf{R}$. For $\varphi = \exists x(x^2 = y)$ we obtain $\mathbf{Q} \nvDash \varphi(2)$ and $\mathbf{R} \vDash \varphi(2)$, using the extended formula $\varphi(y)$. For $\bar{\varphi} = \forall x(x^2 \neq y)$, which is semantically equivalent to the logical negation of φ, we obtain $\mathbf{Q} \vDash \bar{\varphi}(2)$ and $\mathbf{R} \nvDash \bar{\varphi}(2)$, using the extended formula $\bar{\varphi}(y)$. ⌟

Recall that an existential formula is of the form $\exists x_1 \dots \exists x_k(\psi)$ with ψ quantifier-free. We define *universal formulas* to be of the form $\forall x_1 \dots \forall x_k(\psi)$ with ψ quantifier-free.

Lemma 6.4 (Existential statements go up – universal statements go down)**.** Let $\mathbf{S} \subseteq \mathbf{A}$ be $\mathcal{L}$-structures. Then the following hold:

(i) Let $\varphi(\mathbf{y})$ be an extended existential formula with $\mathbf{y} \in \mathcal{V}^n$, and let $\mathbf{s} \in S^n$. Then it follows from $\mathbf{S} \vDash \varphi(\mathbf{s})$ that also $\mathbf{A} \vDash \varphi(\mathbf{s})$.

(ii) Let $\varphi(\mathbf{y})$ be an extended universal formula with $\mathbf{y} \in \mathcal{V}^n$, and let $\mathbf{s} \in S^n$. Then it follows from $\mathbf{A} \vDash \varphi(\mathbf{s})$ that also $\mathbf{S} \vDash \varphi(\mathbf{s})$.

Proof. (i) Let $\varphi = \exists x_1 \dots \exists x_k(\psi)$ with ψ quantifier-free, and consider the extended formula $\psi(\mathbf{y}, x_1, \dots, x_k)$. Assume that $\mathbf{S} \vDash \varphi(\mathbf{s})$. Using the semantics of the existential quantifier and Lemma 6.2(ii) we obtain

$$\top = \varphi^{\mathbf{S}}(\mathbf{s}) = \max_{\mathbf{s}' \in S^k} \psi^{\mathbf{S}}(\mathbf{s}, \mathbf{s}') = \max_{\mathbf{s}' \in S^k} \psi^{\mathbf{A}}(\mathbf{s}, \mathbf{s}') \leq \max_{\mathbf{s}' \in A^k} \psi^{\mathbf{A}}(\mathbf{s}, \mathbf{s}') = \varphi^{\mathbf{A}}(\mathbf{s}), \tag{6.1}$$

hence $\varphi^{\mathbf{A}}(\mathbf{s}) = \top$, in other words $\mathbf{A} \vDash \varphi(\mathbf{s})$. The proof of part (ii) is analogous. □

A substructure $\mathbf{S}$ of $\mathbf{A}$ is *definable* if the universe of $\mathbf{S}$ is a definable set in $\mathbf{A}$, i.e., if there is an extended formula $\chi_S(x)$ such that $[\chi_S]^{\mathbf{A}} = S$. The following lemma is a technical result, which we need for the proof of the subsequent theorem.

Lemma 6.5. Let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $\mathbf{S} \subseteq \mathbf{A}$ be a definable substructure, and let $\chi_S(z)$ be an extended formula with $S = [\chi_S]^{\mathbf{A}}$. Let $\psi(\mathbf{y}, x)$, $\varphi(\mathbf{y}, x)$ be extended formulas with $\mathbf{y} \in \mathcal{V}^n$, $x \in \mathcal{V}$ such that $\mathbf{S} \vDash \psi(\mathbf{s}, r)$ if and only if $\mathbf{A} \vDash \varphi(\mathbf{s}, r)$, for all $\mathbf{s} \in S^n$, $r \in S$. Then the following hold:

(i) For all $\mathbf{s} \in S^n$ we have $\mathbf{S} \vDash \exists x(\psi)(\mathbf{s})$ if and only if $\mathbf{A} \vDash \exists x(\chi_S[x/z] \wedge \varphi)(\mathbf{s})$, using extended formulas $\exists x(\psi)(\mathbf{y})$ and $\exists x(\chi_S[x/z] \wedge \varphi)(\mathbf{y})$.

(ii) For all $\mathbf{s} \in S^n$ we have $\mathbf{S} \vDash \forall x(\psi)(\mathbf{s})$ if and only if $\mathbf{A} \vDash \forall x(\chi_S[x/z] \longrightarrow \varphi)(\mathbf{s})$, using extended formulas $\forall x(\psi)(\mathbf{y})$ and $\forall x(\chi_S[x/z] \longrightarrow \varphi)(\mathbf{y})$.

Proof. (i) Let $\mathbf{s} \in S^n$. Using the definition of the semantics of first-order formulas we obtain

$$\begin{aligned}
&\exists x(\chi_S[x/z] \wedge \varphi)^{\mathbf{A}}(\mathbf{s}) \\
&\quad = \max_{a \in A} \min\{\chi_S[x/z]^{\mathbf{A}}(a),\ \varphi^{\mathbf{A}}(\mathbf{s}, a)\} \\
&\quad = \max\Big\{\max_{a \in S} \min\{\chi_S[x/z]^{\mathbf{A}}(a),\ \varphi^{\mathbf{A}}(\mathbf{s}, a)\},\ \max_{a \in A \setminus S} \min\{\chi_S[x/z]^{\mathbf{A}}(a),\ \varphi^{\mathbf{A}}(\mathbf{s}, a)\}\Big\} \\
&\quad = \max\Big\{\max_{a \in S} \min\{\top,\ \varphi^{\mathbf{A}}(\mathbf{s}, a)\},\ \max_{a \in A \setminus S} \min\{\bot,\ \varphi^{\mathbf{A}}(\mathbf{s}, a)\}\Big\} \qquad (6.2) \\
&\quad = \max_{a \in S} \varphi^{\mathbf{A}}(\mathbf{s}, a) \\
&\quad = \max_{a \in S} \psi^{\mathbf{S}}(\mathbf{s}, a) \\
&\quad = \exists x(\psi)^{\mathbf{S}}(\mathbf{s}).
\end{aligned}$$

(ii) Let $\mathbf{s} \in S^n$, $r \in \mathbf{S}$. Using the assumptions of the lemma it follows that

$$\mathbf{S} \models \neg\psi(\mathbf{s}, r) \quad \text{iff} \quad \mathbf{S} \not\models \psi(\mathbf{s}, r) \quad \text{iff} \quad \mathbf{A} \not\models \varphi(\mathbf{s}, r) \quad \text{iff} \quad \mathbf{A} \models \neg\varphi(\mathbf{s}, r). \qquad (6.3)$$

This allows us to apply part (i) of the lemma to $\neg\psi$ and $\neg\varphi$ in place of ψ and φ, respectively. In combination with some semantic equivalence transformations we obtain

$$\begin{aligned}
\mathbf{S} \models \forall x(\psi)(\mathbf{s}) \quad &\text{iff} \quad \mathbf{S} \models \neg\exists x(\neg\psi)(\mathbf{s}) \\
&\text{iff} \quad \mathbf{S} \not\models \exists x(\neg\psi)(\mathbf{s}) \\
&\text{iff} \quad \mathbf{A} \not\models \exists x(\chi_S[x/z] \wedge \neg\varphi)(\mathbf{s}) \qquad (6.4) \\
&\text{iff} \quad \mathbf{A} \models \neg\exists x(\chi_S[x/z] \wedge \neg\varphi)(\mathbf{s}) \\
&\text{iff} \quad \mathbf{A} \models \forall x(\chi_S[x/z] \longrightarrow \varphi)(\mathbf{s}).
\end{aligned}$$

□

Theorem 6.6 (Decidability of definable substructures)**.** *Let* $\mathbf{A}$ *be an* $\mathcal{L}$*-structure. If* $\mathbf{A}$ *is decidable, then every definable substructure of* $\mathbf{A}$ *is decidable.*

Proof. Assume that $\mathbf{A}$ is decidable, let $\mathbf{S} \subseteq \mathbf{A}$ be a definable substructure, and let $\chi_S(z)$ be an extended formula with $[\chi_S]^{\mathbf{A}} = S$. Let $\vartheta = Q_n x_n \dots Q_1 x_1(\psi)$ be a sentence, without loss of generality in prenex normal form with ψ quantifier-free. We must produce the output YES if $\mathbf{S} \models \vartheta$, and NO else. Define $\vartheta_i = Q_i x_i \dots Q_1 x_1(\psi)$ for $i \in \{0, \dots, n\}$ and construct

$$\tilde{\vartheta}_0 = \psi, \quad \tilde{\vartheta}_{i+1} = \begin{cases} \exists x_{i+1}(\chi_S[x_{i+1}/z] \wedge \tilde{\vartheta}_i) & \text{if } Q_{i+1} = \exists \\ \forall x_{i+1}(\chi_S[x_{i+1}/z] \longrightarrow \tilde{\vartheta}_i) & \text{if } Q_{i+1} = \forall, \end{cases} \quad i \in \{0, \dots, n-1\}. \qquad (6.5)$$

We consider extended formulas $\vartheta_i(\mathbf{x})$, $\tilde{\vartheta}_i(\mathbf{x})$ with $\mathbf{x} = (x_1, \dots, x_n)$ and show by induction on i that for all $i \in \{0, \dots, n\}$ the following holds:

$$\mathbf{S} \models \vartheta_i(\mathbf{s}) \quad \text{iff} \quad \mathbf{A} \models \tilde{\vartheta}_i(\mathbf{s}), \quad \text{for} \quad \mathbf{s} \in S^n. \qquad (6.6)$$

If $i = 0$, then $\vartheta_i = \psi = \tilde{\vartheta}_i$ is quantifier-free, and (6.6) follows by Lemma 6.2(ii). Assume now that (6.6) holds for $i \in \{0, \dots, n-1\}$ and consider $\vartheta_{i+1} = \exists_{i+1} x_{i+1}(\vartheta_i)$ and $\tilde{\vartheta}_{i+1}$ as in (6.5). Then Lemma 6.5 yields $\mathbf{S} \models \vartheta_{i+1}(\mathbf{s})$ if and only if $\mathbf{A} \models \tilde{\vartheta}_{i+1}(\mathbf{s})$, for all $\mathbf{s} \in S^n$.

Since both ϑ_n and $\tilde{\vartheta}_n$ are sentences and $\vartheta_n = \vartheta$, it follows that $\mathbf{S} \models \vartheta$ if and only if $\mathbf{A} \models \tilde{\vartheta}_n$. We can finally apply an existing decision procedure for $\mathbf{A}$ to $\tilde{\vartheta}_n$ in order to decide ϑ in $\mathbf{S}$. □

The assumption that the input sentence is in prenex normal form keeps the proof of the previous theorem a bit simpler. It is not hard to see that in practice the encoding in (6.5) can be applied to arbitrary first-order input sentences as a local transformation of each quantified subformula, without any prenex normal form computation.

Example 6.7. Consider $\mathcal{L} = (0, 1, +; <)$, and let $\mathbf{N} = (\mathbb{N};\ 0, 1, +; <)$ and $\mathbf{Z} = (\mathbb{Z};\ 0, 1, +; <)$. Then $\mathbf{N} \subseteq \mathbf{Z}$, and $\mathbf{N}$ is definable by $\chi_{\mathbb{N}}(z)$ with $\chi_{\mathbb{N}} = (0 < z + 1)$. Consider the following sentence:

$$\vartheta \;=\; \forall x_1 \forall x_2 (x_1 + 1 < x_2 \longrightarrow \exists y (x_1 < y \wedge y < x_2)). \tag{6.7}$$

For deciding ϑ in $\mathbf{N}$, we can define

$$\begin{aligned} \tilde{\vartheta} \;&=\; \forall x_1 (\chi_{\mathbb{N}}[x_1/z] \longrightarrow \forall x_2 (\chi_{\mathbb{N}}[x_2/z] \longrightarrow \\ &\qquad\qquad x_1 + 1 < x_2 \longrightarrow \exists y (\chi_{\mathbb{N}}[y/z] \wedge x_1 < y \wedge y < x_2))) \\ &=\; \forall x_1 (0 < x_1 + 1 \longrightarrow \forall x_2 (0 < x_2 + 1 \longrightarrow \\ &\qquad\qquad x_1 + 1 < x_2 \longrightarrow \exists y (0 < y + 1 \wedge x_1 < y \wedge y < x_2))) \end{aligned} \tag{6.8}$$

and apply a decision procedure for $\mathbf{Z}$ to $\tilde{\vartheta}$.[1] ⌟

Our proofs of Theorem 6.6 and Lemma 6.5 are quite technical, while the construction in (6.5) is rather common and intuitive. However, the overall situation is more subtle than it might appear. As an example for a possible fallacy note that in the positive case we have $\mathbf{S} \models \vartheta$ and $\mathbf{A} \models \tilde{\vartheta}$ but not necessarily $\mathbf{S} \models \tilde{\vartheta}$. For instance, $\chi_{\mathbb{N}}$ in Example 6.7 could be replaced with $0 < z + 1 \wedge \exists x (x < 0)$.

6.2 Elementary Equivalence and Substructure Completeness

Let $\mathcal{L}$ be a language, and let $\mathbf{A}$, $\mathbf{B}$ be $\mathcal{L}$-structures. Assume that for all sentences ϑ we have $\mathbf{A} \models \vartheta$ if and only if $\mathbf{B} \models \vartheta$. Then we call $\mathbf{A}$ and $\mathbf{B}$ *elementary equivalent*, and we write $\mathbf{A} \equiv \mathbf{B}$.

Theorem 6.8. *Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. Then $\mathfrak{A}$ is complete if and only if $\mathbf{A} \equiv \mathbf{B}$ for all $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$.*

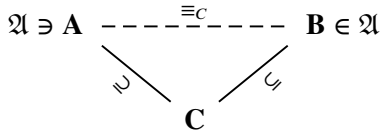
Proof. Assume that $\mathfrak{A}$ is complete, and let $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$. Let ϑ be a sentence. Then either $\mathfrak{A} \models \vartheta$ or $\mathfrak{A} \models \neg\vartheta$. If $\mathfrak{A} \models \vartheta$, then both $\mathbf{A} \models \vartheta$ and $\mathbf{B} \models \vartheta$. If $\mathfrak{A} \models \neg\vartheta$, then both $\mathbf{A} \models \neg\vartheta$ and $\mathbf{B} \models \neg\vartheta$, and it follows that both $\mathbf{A} \not\models \vartheta$ and $\mathbf{B} \not\models \vartheta$. Hence $\mathbf{A} \equiv \mathbf{B}$.

Conversely, assume that $\mathfrak{A}$ is not complete. Then there is a sentence ϑ such that $\mathfrak{A} \not\models \vartheta$ and $\mathfrak{A} \not\models \neg\vartheta$. It follows that there are $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ such that $\mathbf{A} \not\models \vartheta$ and $\mathbf{B} \not\models \neg\vartheta$. It follows that $\mathbf{B} \models \vartheta$, hence $\mathbf{A} \not\equiv \mathbf{B}$. □

Let $\mathcal{L}$ be a language, let $\mathbf{A}$, $\mathbf{B}$ be $\mathcal{L}$-structures, and let $\varnothing \subsetneq C \subseteq A \cap B$. Assume that for all $n \geq 1$, all extended formulas $\varphi(\mathbf{x})$ with $\mathbf{x} \in \mathcal{V}^n$, and all $\mathbf{c} \in C^n$ we have $\mathbf{A} \models \varphi(\mathbf{c})$ if and only if $\mathbf{B} \models \varphi(\mathbf{c})$. Then we call $\mathbf{A}$ and $\mathbf{B}$ *elementary equivalent over C*, and we write $\mathbf{A} \equiv_C \mathbf{B}$.

[1] $(\mathbb{Z};\ 0, 1, +, -; <)$ is decidable according to Example 8.34 in the next chapter. Decidability of its $\mathcal{L}$-restriction $\mathbf{Z}$ follows by Lemma 4.19.

Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. We call $\mathfrak{A}$ *substructure complete* if $\mathbf{A} \equiv_C \mathbf{B}$ for all $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ and all $\mathcal{L}$-structures $\mathbf{C}$ with $\mathbf{C} \subseteq \mathbf{A}$ and $\mathbf{C} \subseteq \mathbf{B}$. Note that it is not required that $\mathbf{C} \in \mathfrak{A}$.



(6.9)

Theorem 6.9. *Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. If $\mathfrak{A}$ is substructure complete and there is an $\mathcal{L}$-structure $\mathbf{C}$ such that $\mathbf{C} \subseteq \mathbf{A}$ for all $\mathbf{A} \in \mathfrak{A}$, then $\mathfrak{A}$ is complete.*

Proof. Let $\mathbf{A}$, $\mathbf{B}$ in $\mathfrak{A}$, and let $\mathbf{C}$ be an $\mathcal{L}$-structure such that $\mathbf{C} \subseteq \mathbf{A}$ and $\mathbf{C} \subseteq \mathbf{B}$. Let $\vartheta(x)$ be an extended sentence. For $c \in C$ it follows that $\mathbf{A} \models \vartheta$ if and only if $\mathbf{A} \models \vartheta(c)$ if and only if $\mathbf{B} \models \vartheta(c)$ if and only if $\mathbf{B} \models \vartheta$. We have shown that $\mathbf{A}$ and $\mathbf{B}$ are elementary equivalent. Hence $\mathfrak{A}$ is complete by Theorem 6.8. □

The assumption of a common substructure of all $\mathbf{A} \in \mathfrak{A}$ in the previous theorem cannot formally hold for elementary classes $\mathfrak{A} \neq \varnothing$, because then for any $\mathbf{A} \in \mathfrak{A}$ there are arbitrarily many $\mathbf{A}' \in \mathfrak{A}$ that are isomorphic to $\mathbf{A}$ but have disjoint universes with $\mathbf{A}$. However, it is not hard to see that it is sufficient to assume in the theorem that $\mathbf{C} \subseteq \mathbf{A}$ for all $\mathbf{A} \in \mathfrak{A}$ only up to isomorphism.

The following theorem reveals that substructure completeness provides a semantic characterization of quantifier eliminability. We will prove only part (i) of the theorem. The proof of part (ii) requires some results and techniques of algebraic model theory not covered here, namely the Compactness Theorem for first-order logic and Robinson's Diagram Method.

Theorem 6.10 (A. Robinson, ∼1965)**.** *Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. Then the following hold:*

(i) If $\mathfrak{A}$ admits QE, then $\mathfrak{A}$ is substructure complete.

(ii) If $\mathfrak{A}$ is elementary and substructure complete, then $\mathfrak{A}$ admits QE.

Proof. (i) Assume that $\mathfrak{A}$ admits QE. Let $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$, and let $\mathbf{C}$ be an $\mathcal{L}$-structure such that $\mathbf{C} \subseteq \mathbf{A}$ and $\mathbf{C} \subseteq \mathbf{B}$. Let $n \geq 1$, let $\varphi(\mathbf{x})$ be an extended formula with $\mathbf{x} \in \mathcal{V}^n$, and let $\mathbf{c} \in C^n$. There is an extended quantifier-free formula $\varphi'(\mathbf{x})$ with $\mathfrak{A} \models \varphi \longleftrightarrow \varphi'$ by Lemma 4.10(i). It follows that

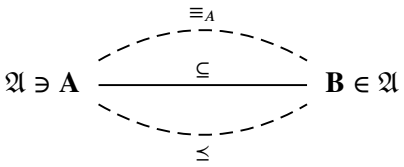
$$\mathbf{A} \models \varphi(\mathbf{c}) \quad \text{iff} \quad \mathbf{A} \models \varphi'(\mathbf{c}) \quad \text{iff} \quad \mathbf{C} \models \varphi'(\mathbf{c}) \quad \text{iff} \quad \mathbf{B} \models \varphi'(\mathbf{c}) \quad \text{iff} \quad \mathbf{B} \models \varphi(\mathbf{c}). \tag{6.10}$$

Hence $\mathbf{A} \equiv_C \mathbf{B}$. □

6.3 Elementary Substructures and Model Completeness

Let $\mathcal{L}$ be a language, and let $\mathbf{A}$, $\mathbf{B}$ be $\mathcal{L}$-structures. If both $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{A} \equiv_A \mathbf{B}$, then we call $\mathbf{A}$ an *elementary substructure* of $\mathbf{B}$, we call $\mathbf{B}$ an *elementary extension structure* of $\mathbf{A}$, and we write $\mathbf{A} \preceq \mathbf{B}$.

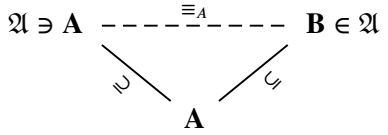
Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. We call $\mathfrak{A}$ *model complete* if for all $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ with $\mathbf{A} \subseteq \mathbf{B}$ it follows that $\mathbf{A} \equiv_A \mathbf{B}$, from which in turn follows that $\mathbf{A} \preceq \mathbf{B}$. This is sometimes phrased as "all extensions are elementary in $\mathfrak{A}$".



(6.11)

Theorem 6.11. *Let $\mathcal{L}$ be a language, and let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures. If $\mathfrak{A}$ is substructure complete, then $\mathfrak{A}$ is model complete.*

Proof. Assume that $\mathfrak{A}$ is substructure complete. Let $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ with $\mathbf{A} \subseteq \mathbf{B}$. Since obviously also $\mathbf{A} \subseteq \mathbf{A}$, it follows that $\mathbf{A} \equiv_A \mathbf{B}$ and thus $\mathbf{A} \preceq \mathbf{B}$.



(6.12)

□

Similarly to substructure completeness, model completeness can be characterized in terms of elimination of quantifiers. The following result is commonly known as Robinson's Test. We omit the proof step from (i) to (ii) as it requires results that are not covered here, namely the First Persistence Theorem of model theory.

Theorem 6.12 (A. Robinson, ∼1965)**.** *Let $\mathfrak{A}$ be an elementary class of $\mathcal{L}$-structures. Then the following are equivalent:*

(i) $\mathfrak{A}$ is model complete.

(ii) For every universal formula φ there is an existential formula φ' such that $\mathfrak{A} \vDash \varphi \longleftrightarrow \varphi'$.

(iii) For every formula φ there is an existential formula φ' such that $\mathfrak{A} \vDash \varphi \longleftrightarrow \varphi'$.

Proof. Assume (ii). For $Q \in \{\exists, \forall\}$ and $\mathbf{x} = (x_1, \ldots, x_k) \in \mathcal{V}^k$ we write $Qx_1 \ldots Qx_k$ shortly as $Q\mathbf{x}$. Let φ be a formula, without loss of generality, in PNF, i.e.,

$$\varphi = Q_1\mathbf{x}_1 \ldots Q_n\mathbf{x}_n(\psi), \tag{6.13}$$

where $Q_i \neq Q_{i+1}$ and ψ is quantifier-free. We proceed by induction on the number n of quantifier blocks. The case $n = 0$ is trivial. Assume now that $n \geq 1$. We distinguish two cases:

(a) $Q_1 = \exists$: By the induction hypothesis, $Q_2\mathbf{x}_2 \ldots Q_n\mathbf{x}_n(\psi)$ is equivalent to an existential formula $\exists\mathbf{x}(\psi')$ in $\mathfrak{A}$, and it follows that also φ is equivalent to an existential formula in $\mathfrak{A}$.

(b) $Q_1 = \forall$: The formula $\neg Q_2\mathbf{x}_2 \dots Q_n\mathbf{x}_n(\psi)$ is semantically equivalent to the prenex formula $\bar{Q}_2\mathbf{x}_2 \dots \bar{Q}_n\mathbf{x}_n(\neg\psi)$, which is by the induction hypothesis equivalent to an existential formula $\exists\mathbf{x}(\psi')$ in $\mathfrak{A}$. It follows that $Q_2\mathbf{x}_2 \dots Q_n\mathbf{x}_n(\psi)$ is equivalent to $\forall\mathbf{x}(\neg\psi')$ and that φ is equivalent to the universal formula $\forall\mathbf{x}_1\forall\mathbf{x}(\neg\psi')$ in $\mathfrak{A}$. Hence φ is equivalent to an existential formula in $\mathfrak{A}$ by (ii).

Assume (iii), and let $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ with $\mathbf{A} \subseteq \mathbf{B}$. We must show $\mathbf{A} \equiv_A \mathbf{B}$. Let $n \geq 1$, and let $\varphi(\mathbf{x})$ be an extended formula with $\mathbf{x} \in \mathcal{V}^n$. Then φ is equivalent to an existential formula $\varphi_\exists$ in $\mathfrak{A}$ by (iii). Furthermore, $\neg\varphi$ is equivalent to an existential formula in $\mathfrak{A}$ by (iii), and it follows that φ is equivalent also to a universal formula $\varphi_\forall$ in $\mathfrak{A}$. Both $\varphi_\exists(\mathbf{x})$ and $\varphi_\forall(\mathbf{x})$ are extended formulas. Let $\mathbf{a} \in A^n$. If $\mathbf{A} \models \varphi(\mathbf{a})$, then $\mathbf{A} \models \varphi_\exists(\mathbf{a})$, thus $\mathbf{B} \models \varphi_\exists(\mathbf{a})$ by Lemma 6.4(i), hence $\mathbf{B} \models \varphi(\mathbf{a})$. Conversely, we can conclude from $\mathbf{B} \models \varphi(\mathbf{a})$ that $\mathbf{A} \models \varphi(\mathbf{a})$ using $\varphi_\forall$ and Lemma 6.4(ii). □

Condition (iii) of the theorem is sometimes phrased as "$\mathfrak{A}$ admits quantifier elimination down to existential formulas".

7 Quantifier Elimination for Divisible Abelian Groups

7.1 Non-trivial Abelian Groups

We consider the algebraic language $\mathcal{L}_{Groups} = (0^{(0)}, +^{(2)}, -^{(1)})$ of additive groups. The axioms and the model class of all groups are defined as follows:

$$\begin{aligned} \Xi_{Groups} &= \{(x+y)+z = x+(y+z),\ x+0=x,\ x+(-x)=0\}, \\ \mathit{Groups} &= \mathrm{Mod}(\Xi_{Groups}). \end{aligned} \tag{7.1}$$

Let $\mathbf{A} \in \mathit{Groups}$. If $|A| = 1$, then $\mathbf{A}$ is a called a *trivial group*, else $|A| > 1$ and $\mathbf{A}$ is called a *non-trivial group*. If $\mathbf{A}$ is a trivial group, say $A = \{a\}$, then the only possible definition of the functions of $\mathbf{A}$ is given by $0^{\mathbf{T}} = a$, $a +^{\mathbf{T}} a = a$, and $-^{\mathbf{T}} a = a$. In other words, all trivial groups are isomorphic.

The following lemma clarifies quantifier eliminability for subclasses of *Groups* that contain at least one trivial group.

Lemma 7.1 (QE in classes with trivial groups)**.** Let $\mathfrak{A} \subseteq \mathit{Groups}$.

(i) If $|A| = 1$ for all $\mathbf{A} \in \mathfrak{A}$, then $\mathfrak{A}$ admits effective QE.

(ii) If there are $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ with $|A| = 1$ and $|B| > 1$, then $\mathfrak{A}$ does not admit QE.

In particular *Groups* does not admit QE.

Proof. (i) Consider a 1-existential formula $\varphi = \exists x(\psi)$. Then $\mathbf{A} \models \varphi \longleftrightarrow \psi[0/x]$. This is a special case of Lemma 4.4.

(ii) Consider $\vartheta = \exists x(x \neq 0)$. Then $\mathbf{A} \models \vartheta \longleftrightarrow$ FALSE and $\mathbf{B} \models \vartheta \longleftrightarrow$ TRUE. Assume for a contradiction that $\mathfrak{A}$ admits QE. Since $\mathcal{L}_{Groups}$ has a constant symbol, there is a quantifier-free sentence ϑ' such that $\mathfrak{A} \models \vartheta \longleftrightarrow \vartheta'$, using Theorem 4.10(iii). All atomic sentences in ϑ' can be equivalently rewritten as $0 = 0$. Since $\models 0 = 0 \longleftrightarrow$ TRUE, we obtain either $\mathfrak{A} \models \vartheta' \longleftrightarrow$ TRUE, which contradicts $\mathbf{A} \models \vartheta \longleftrightarrow$ FALSE, or $\mathfrak{A} \models \vartheta' \longleftrightarrow$ FALSE, which contradicts $\mathbf{B} \models \vartheta \longleftrightarrow$ TRUE. □

It remains to study quantifier eliminability for subclasses of *Groups* that contain exclusively non-trivial groups. Non-triviality can be axiomatized by

$$\Xi_{NonTrivial} = \{\exists x(\neg\, x = 0)\}. \tag{7.2}$$

We restrict our attention to non-trivial *Abelian groups*. An additive group is called Abelian if the addition is commutative, which is axiomatized by

$$\Xi_{Abelian} \;=\; \{x + y = y + x\}. \tag{7.3}$$

In summary, we have the following axioms and model class of non-trivial Abelian groups:

$$\Xi_{NtAGroups} \;=\; \Xi_{NonTrivial} \cup \Xi_{Abelian} \cup \Xi_{Groups}, \quad NtAGroups = \mathrm{Mod}(\Xi_{NtAGroups}). \tag{7.4}$$

The class *NtAGroups* and its subclasses admit normal forms of terms and atomic formulas as follows. For $k \in \mathbb{Z} \setminus \{0\}$ and $t \in \mathcal{T}$ we introduce a notation $k \odot t = \pm(t + \cdots + t)$, which can be shorter written as kt. Then each term t can be equivalently rewritten as either 0 or

$$k_1 \odot x_1 + \cdots + k_n \odot x_n, \qquad k_i \in \mathbb{Z} \setminus \{0\}, \quad x_i \in \mathcal{V}(t). \tag{7.5}$$

In particular, all variable-free terms can be rewritten as 0.

All atomic formulas α are equations, which can be rewritten in the following normal form suitable for the general presentation of atoms: Either $0 = 0$ or

$$k_1 \odot x_1 + \sum_{j=2}^{n} k_j \odot x_j = 0, \qquad k_1 \in \mathbb{N} \setminus \{0\}, \quad k_j \in \mathbb{Z} \setminus \{0\}, \quad x_1, x_j \in \mathcal{V}(\alpha). \tag{7.6}$$

For $i \in \{1, \ldots, n\}$ we can rewrite (7.6) in *x_i-elimination form*, which isolates a particular variable x_i on the left hand side:

$$k_i \odot x_i = \sum_{j=1}^{i-1} k_j \odot x_j + \sum_{j=i+1}^{n} k_j \odot x_j, \qquad k_i \in \mathbb{N} \setminus \{0\}, \quad k_j \in \mathbb{Z} \setminus \{0\}. \tag{7.7}$$

From a mathematical perspective it is often sufficient for QE that the left hand sides of equations have a form $k_i \odot x_i$ as in (7.7) while the right hand side can be any term in which x_i does not occur. We call this *weak x_i-elimination form*. All atomic sentences can be rewritten as $0 = 0$. For negated equations $\neg\, t_1 = t_2$ we shortly write $t_1 \neq t_2$.

Lemma 7.2. The class *NtAGroups* does not admit QE.

Proof. Consider $\mathbf{Z} = (\mathbb{Z};\ 0, +, -)$, $\mathbf{R} = (\mathbb{R};\ 0, +, -) \in$ *NtAGroups* and the sentence $\vartheta = \forall x \exists y (2 \odot y = x)$. Then $\mathbf{Z} \models \vartheta \longleftrightarrow$ FALSE and $\mathbf{R} \models \vartheta \longleftrightarrow$ TRUE. Now use the same arguments as in the proof of Lemma 7.1. □

7.2 Divisible Torsion-free Abelian Groups

Similar to our explorations of linear orders in Chapter 5, we begin with the real numbers. Our strategy is to consider $\mathbf{R} = (\mathbb{R};\ 0, +, -)$ and try to find a QE procedure that uses only elementary properties of $\mathbf{R}$. In the positive case, such a procedure can be generalized to a subclass of *NtAGroups* along with a suitable axiomatization.

Lemma 7.3. $\mathbf{R} = (\mathbb{R};\ 0, +, -)$ admits effective QE.

Proof. Consider a 1-primitive formula in weak x-elimination form:

$$\varphi \;=\; \exists x \left[\bigwedge_{i=1}^{m} k_i x = t_i \wedge \bigwedge_{j=1}^{n} l_j x \neq u_j \right]. \tag{7.8}$$

Let $\lambda = \mathrm{lcm}_{i,j}\{k_i, l_j\} > 0$. We set $k'_i = \lambda / k_i \in \mathbb{N} \setminus \{0\}$, and we set $t'_i = k'_i t_i$. In the same way we obtain l'_j and u'_j. Then (7.8) is equivalent to

$$\exists x \left[\bigwedge_{i=1}^{m} \lambda x = t'_i \wedge \bigwedge_{j=1}^{n} \lambda x \neq u'_j \right]. \tag{7.9}$$

Since $\beta : \mathbb{R} \to \mathbb{R}$ with $\beta(x) = \lambda x$ is left-total, as a function, and right-total, i.e. surjective, (7.9) is equivalent to

$$\exists y \left[\bigwedge_{i=1}^{m} y = t'_i \wedge \bigwedge_{j=1}^{n} y \neq u'_j \right]. \tag{7.10}$$

We can now continue exactly as in the proof of Lemma 4.6(i) on effective QE for infinite sets. Our formula (7.10) matches the formula (4.5) there. □

An analysis of the proof shows that we have used the following elementary properties of **R**:

(i) **R** is a non-trivial Abelian group. Corresponding formal axioms $\Xi_{NtAGroups}$ have been given in (7.4).

(ii) The proof step from (7.8) to (7.9) requires that $k_i x = t_i$ is equivalent to $k'_i k_i x = k'_i t_i$ for $k'_i \in \mathbb{N} \setminus \{0\}$. An analogous equivalence is required for $l_j x \neq u_j$. Those equivalence hold in **R** but, e.g., not in $(\mathbb{Z}/6;\ 0, +, -) \in \mathit{NtAGroups}$, where we have $3 \neq 0$ but $2 \odot 3 = 2 \odot 0$. The proof uses the fact that **R** is *torsion-free*:

$$\Xi_{Torsion_0} \;=\; \{\, nx = 0 \longrightarrow x = 0 \mid n \in \mathbb{N} \setminus \{0\} \,\}. \tag{7.11}$$

(iii) The proof step from (7.9) to (7.10) requires that the function $\beta(x) = \lambda x$ is surjective, which is not the case, e.g., in $(\mathbb{Z};\ 0, +, -) \in \mathit{NtAGroups}$. The proof uses the fact that **R** is *divisible*:

$$\Xi_{Divisible} \;=\; \{\, \exists y(ny = x) \mid n \in \mathbb{N} \setminus \{0\} \,\}. \tag{7.12}$$

(iv) Finally, the reduction to Lemma 4.6(i) requires that the universe is infinite. This follows from $\Xi_{Torsion_0}$.

We define the class $\mathit{NtDAGroups}_0$ of all non-trivial torsion-free divisible Abelian groups:

$$\Xi_{NtDAGroups_0} \;=\; \Xi_{NtAGroups} \cup \Xi_{Torsion_0} \cup \Xi_{Divisible}, \tag{7.13}$$

$$\mathit{NtDAGroups}_0 \;=\; \mathrm{Mod}(\Xi_{NtDAGroups_0}). \tag{7.14}$$

One can now generalize and apply the proof of Lemma 7.3 to the class $\mathit{NtDAGroups}_0$ instead of the single structure $\mathbf{R} \in \mathit{NtDAGroups}_0$. This yields the following theorem.

Theorem 7.4. *The class NtDAGroups$_0$ admits effective QE.* □

Corollary 7.5. *The class NtDAGroups$_0$ is complete and decidable.*

Proof. The language $\mathcal{L}_{Groups}$ has a constant symbol 0. All atomic sentences have the normal form $0 = 0$ in *NtAGroups* $\supseteq$ *NtDAGroups*$_0$. Since $\vDash 0 = 0 \longleftrightarrow$ TRUE, *NtDAGroups*$_0$ is complete and decidable for the set of all atomic sentences. General completeness and decidability follows by Theorem 4.26(ii). □

Let us remind ourselves of some results of the previous section. The following corollary holds for every class that admits QE.

Corollary 7.6. *The class NtDAGroups$_0$ is substructure complete and model complete.*

Proof. Substructure completeness follows from quantifier eliminability, using Theorem 6.10. Model completeness follows from substructure completeness, using Theorem 6.11. □

Substructure completeness provides us with an alternative approach to proving completeness: The trivial group $(\{0\};\ 0, +, -) \notin$ *NtDAGroups*$_0$ is a common substructure of all $\mathbf{A} \in$ *NtDAGroups*$_0$, up to isomorphism. Completeness follows essentially via Theorem 6.9. Recall the remarks following that theorem.

Lemma 7.7. Let $\mathbf{A} \in$ *NtDAGroups*$_0$. Let $a \in A$ with $a \neq 0$, and let $m, n \in \mathbb{N}$ with $m \neq n$. Then $ma \neq na$. In particular, $\mathbf{A}$ is infinite.

Proof. Assume without loss of generality that $m < n$. Since $\mathbf{A}$ is torsion-free, it follows that $(n - m)a \neq 0$ and hence $na \neq ma$. □

Example 7.8 (Non-trivial torsion-free divisible Abelian groups)**.** Of course, $\mathbf{R} = (\mathbb{R};\ 0, +, -) \in$ *NtDAGroups*$_0$. Further examples are

$$(\mathbb{R}^n;\ 0, +, -), \quad (\mathbb{Q}^n;\ 0, +, -) \in \textit{NtDAGroups}_0 \tag{7.15}$$

for $n \in \mathbb{N} \setminus \{0\}$. More generally, we have the set of all functions from a non-empty set S to $\mathbb{R}$ with the constant zero-function as 0 and point-wise addition:

$$(\mathbb{R}^S;\ 0, +, -) \in \textit{NtDAGroups}_0. \tag{7.16}$$

For $S = \mathbb{R}$ we obtain as a special case the additive group of all real functions and its subgroups of $k \in (\mathbb{N} \setminus \{0\}) \cup \{\infty\}$ times continuously differentiable functions:

$$(\mathbb{R}^{\mathbb{R}};\ 0, +, -), \quad (\mathscr{C}^k(\mathbb{R}, \mathbb{R});\ 0, +, -) \in \textit{NtDAGroups}_0. \tag{7.17}$$

This yields an infinite chain of extensions of $(\mathbb{Q};\ 0, +, -)$ in *NtDAGroups*$_0$, which are all elementary via model completeness:

$$\begin{aligned}(\mathbb{Q};\ 0, +, -) \preceq (\mathbb{R};\ 0, +, -) \preceq (\mathscr{C}^\infty(\mathbb{R}, \mathbb{R});\ 0, +, -) \preceq \ldots \\ \preceq (\mathscr{C}^2(\mathbb{R}, \mathbb{R});\ 0, +, -) \preceq (\mathscr{C}(\mathbb{R}, \mathbb{R});\ 0, +, -) \preceq (\mathbb{R}^{\mathbb{R}};\ 0, +, -).\end{aligned} \tag{7.18}$$

Additive groups of polynomials with real or rational coefficients and indeterminates $X_1, \ldots, X_n$:

$$(\mathbb{R}[X_1, \ldots, X_n];\ 0, +, -), \quad (\mathbb{Q}[X_1, \ldots, X_n];\ 0, +, -) \in \mathit{NtDAGroups}_0. \tag{7.19}$$

For $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ we have multiplicative group of the field of complex numbers:

$$(\mathbb{C}^*;\ 1, \cdot, ^{-1}) \in \mathit{NtDAGroups}_0. \tag{7.20}$$

Divisibility here corresponds to the existence of n-th roots for all $n \in \mathbb{N} \setminus \{0\}$ and all $c \in \mathbb{C}^*$. For $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ it follows that the corresponding multiplicative groups are not divisible, thus

$$(\mathbb{R}^*;\ 1, \cdot, ^{-1}), \quad (\mathbb{Q}^*;\ 1, \cdot, ^{-1}) \notin \mathit{NtDAGroups}_0. \tag{7.21}$$

Consider now $\mathbb{R}^+ = \{\, r \in \mathbb{R} \mid r > 0 \,\}$. Then the corresponding multiplicative group is isomorphic to $\mathbf{R}$ via the exponential function $\mathbb{R} \to \mathbb{R}^+$, thus

$$(\mathbb{R}^+;\ 1, \cdot, ^{-1}) \in \mathit{NtDAGroups}_0. \tag{7.22}$$

The corresponding multiplicative group for $\mathbb{Q}^+ = \{\, q \in \mathbb{Q} \mid q > 0 \,\}$ is again not divisible, thus

$$(\mathbb{Q}^+;\ 1, \cdot, ^{-1}) \notin \mathit{NtDAGroups}_0. \tag{7.23}$$

Finally, we have seen in Lemma 7.7 that finite groups are generally not torsion-free, e.g.,

$$(\mathbb{Z}/m;\ 0, +, -) \notin \mathit{NtDAGroups}_0 \tag{7.24}$$

for $m \in \{2, 3, \ldots\}$. ⌟

7.3 Infinite Divisible Abelian Groups with Prime Torsion

We keep the language $\mathcal{L}_{\mathit{Groups}}$ and turn to infinite Abelian groups that are not torsion-free. For $a, b \in \mathbb{Z}$ we define $a \bmod b \in \{0, \ldots, |b| - 1\}$ as the positive remainder upon division of a by b. Let $p \in \mathbb{N}$ be a *prime number*, i.e., $p \notin \{0, 1\}$ and for all $m, n \in \mathbb{N}$ the following holds: If p divides mn, then p divides m or p divides n.

(i) We still have $\Xi_{\mathit{NtAGroups}}$ as in in (7.4).

(ii) We replace Ξ_{Torsion_0} with the following axiom:

$$\Xi_{\mathit{Torsion}_p} \ = \ \{\, px = 0 \,\}. \tag{7.25}$$

(iii) In contrast to Ξ_{Torsion_0}, our new Ξ_{Torsion_p} does not model infinity of the universe. We explicitly add suitable axioms as follows:

$$\Xi_\infty \ = \ \Big\{\, \exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{n} \bigwedge_{j=i+1}^{n} x_i \neq x_j \ \Big|\ n \in \{2, 3, \ldots\} \,\Big\}, \tag{7.26}$$

(iv) Consider $\mathfrak{E} = \mathrm{Mod}(\Xi_{NtAGroups} \cup \Xi_{Torsion_p} \cup \Xi_{Divisible})$ and let $\mathbf{A} \in \mathfrak{E}$. Then $A \setminus \{0^{\mathbf{A}}\} \neq \varnothing$. Let $a \in A \setminus \{0^{\mathbf{A}}\}$. By $\Xi_{Torsion_p}$ we have $pb = 0^{\mathbf{A}}$ for all $b \in A$, while by $\Xi_{Divisible}$ there is $b \in A$ with $pb = a \neq 0^{\mathbf{A}}$, a contradiction. It follows that $\mathfrak{E} = \varnothing$, equivalently, $\Xi_{NtAGroups} \cup \Xi_{Torsion_p} \cup \Xi_{Divisible}$ is inconsistent.

We replace $\Xi_{Divisible}$ with the following axioms:

$$\Xi_{Divisible_p} = \{\, \exists y(ry = x) \mid r \in \{1, \ldots, p-1\} \,\}. \tag{7.27}$$

We define the axioms and the class of non-trivial infinite divisible Abelian groups with p-torsion as follows:

$$\Xi_{NtDAGroups_p} = \Xi_{NtAGroups} \cup \Xi_{\infty} \cup \Xi_{Divisible_p} \cup \Xi_{Torsion_p}, \tag{7.28}$$

$$NtDAGroups_p = \mathrm{Mod}(\Xi_{NtDAGroups_p}). \tag{7.29}$$

We immediately provide examples for structures in $NtDAGroups_p$. Verification of the axioms $\Xi_{NtDAGroups_p}$ for at least one example proves that $NtDAGroups_p \neq \varnothing$, equivalently, $\Xi_{NtDAGroups_p}$ is consistent.

Example 7.9 (Infinite divisible Abelian groups with p-torsion)**.** Let p be a prime number, consider an infinite vector space $\mathbf{V}$ over the finite field $\mathbb{Z}/p$. Then the additive group of $\mathbf{V}$ is divisible with p-torsion:

$$(V;\ 0, +, -) \in NtDAGroups_p. \tag{7.30}$$

Recall that a vector space over a finite field is finite if and only it has finite dimension.

Concrete examples include infinite sequences of elements of $\mathbb{Z}/p$:

$$(\mathbb{Z}/p^{\mathbb{N}};\ 0, +, -) \in NtDAGroups_p. \tag{7.31}$$

Furthermore, polynomials with coefficients in $\mathbb{Z}/p$ and indeterminates $X_1, \ldots, X_n$:

$$(\mathbb{Z}/p[X_1, \ldots, X_n];\ 0, +, -). \in NtDAGroups_p. \tag{7.32}$$

As a field, $\mathbb{Z}/p$ has an algebraic closure with universe $\overline{\mathbb{Z}/p} \supseteq \mathbb{Z}/p$ in which every non-constant polynomial has a zero. Algebraic closures are generally infinite and unique up to isomorphism. Furthermore, as an extension field, $\overline{\mathbb{Z}/p}$ is a vector space over $\mathbb{Z}/p$. For the additive group of the algebraic closure we have

$$\left(\overline{\mathbb{Z}/p};\ 0, +, -\right) \in NtDAGroups_p. \tag{7.33}$$

⌟

The following lemma explains the choice of $r \in \{1, \ldots, p-1\}$ in $\Xi_{Divisible_p}$.

Lemma 7.10. Let p be a prime number, let $n \in \mathbb{N}$ and set $r = n \bmod p$. Then $r \in \{0, \ldots, p-1\}$, in particular, $r = 0$ if and only if $p \mid n$, and $NtDAGroups_p \vDash nx = rx$.

Proof. Let $\mathbf{A} \in NtDAGroups_p$, and let $a \in A$. There is $q \in \mathbb{Z}$ such that $ra = (n - qp)a = na - p(qa)$. Due to $\Xi_{Torsion_p}$ we have $p(qa) = 0$ and therefore $ra = na$. □

The normal forms for terms and atoms introduced in Section 7.1 require only the axioms $\Xi_{NtAGroups}$ and therefore remain valid here. Our previous lemma admits even stronger normal forms that restrict the range of all coefficients k_1, k_i, k_j in (7.5)–(7.7) to $\{1, \ldots, p-1\}$.

Theorem 7.11. *Let p be a prime number. Then the class $NtDAGroups_p$ admits effective QE.*

Proof. Consider a 1-primitive formula in weak x-elimination form

$$\varphi \;=\; \exists x \left[\bigwedge_{i=1}^{m} k_i x = t_i \wedge \bigwedge_{j=1}^{n} l_j x \neq u_j \right]. \tag{7.34}$$

where $k_i, l_j \in \{1, \ldots, p-1\}$, using Lemma 7.10 and thus $\Xi_{Torsion_p}$. The right hand sides t_i and u_j are terms in which the variable x does not occur. Let

$$\pi = \left[\prod_{i=1}^{m} k_i \cdot \prod_{j=1}^{n} l_j \right] \bmod p. \tag{7.35}$$

Since the prime p is not a divisor of any of the k_i, l_j, it follows that p is not a divisor of $\prod_i k_i \prod_j l_j$ either, and thus $\pi \in \{1, \ldots, p-1\}$. We set $k'_i = \pi k_i^{-1} \bmod p$, we note that $k'_i \in \{1, \ldots, p-1\}$, and we set $t'_i = k'_i t_i$. In the same way we obtain l'_j and u'_j. Then (7.34) is equivalent to

$$\exists x \left[\bigwedge_{i=1}^{m} \pi x = t'_i \wedge \bigwedge_{j=1}^{n} \pi x \neq u'_j \right]. \tag{7.36}$$

Let $\mathbf{A} \in NtDAGroups_p$ and consider $\beta : A \to A$ with $\beta(x) = \pi x$. For each $b \in A$, there is $a \in A$ with $\pi a = b$, using $\Xi_{Divisible_p}$. Thus β is surjective. It follows that (7.36) is equivalent in $NtDAGroups_p$ to

$$\exists y \left[\bigwedge_{i=1}^{m} y = t'_i \wedge \bigwedge_{j=1}^{n} y \neq u'_j \right]. \tag{7.37}$$

Due to Ξ_∞ we can now continue exactly as in the proof of Lemma 4.6(i) on effective QE for infinite sets. Our formula (7.37) matches (4.5) there. □

The proof of the following corollary is literally the same as the proofs of the corresponding corollaries 7.5 and 7.6 for $NtDAGroups_0$. It is noteworthy that groups in $NtDAGroups_p$ also share the trivial group as a common substructure up to isomorphism.

Corollary 7.12. *Let p be a prime number. Then the class $NtDAGroups_p$ is substructure complete, model complete, complete, and decidable.* □

7.4 Dense Ordered Abelian Groups

We want to combine our results for dense linear orders without endpoints back in Section 5.3 with our results for torsion-free divisible Abelian groups in 7.2 above. We introduce the language $\mathcal{L}_{Groups_<} = (0, +, -; <)$ of linear ordered additive groups and use $t > t'$ as a notational variant for

atomic formulas $t' < t$. We start with the ordered additive group $\mathbf{R} = (\mathbb{R};\ 0, +, -;\ <)$ of the real numbers, for which we have studied restrictions $\mathbf{R}|_{\mathcal{L}_{Losets}} = (\mathbb{R};\ <)$ and $\mathbf{R}|_{\mathcal{L}_{Groups}} = (\mathbb{R};\ 0, +, -)$ in Lemma 5.6 and Lemma 7.3, respectively.

The normal forms (7.5)–(7.7) for terms and equations introduced in Section 7.1 require only the axioms $\Xi_{NtAGroups}$ and therefore remain valid in $\mathbf{R}$. Furthermore, $\mathbf{R}$ admits the following normal forms for inequalities α:

$$0 < 0, \quad k_1 x_1 + \sum_{j=2}^{n} k_j x_j \gtrless 0, \qquad k_1 \in \mathbb{N} \setminus \{0\}, \quad k_j \in \mathbb{Z} \setminus \{0\}, \quad x_1, x_j \in \mathcal{V}(\alpha). \tag{7.38}$$

For $i \in \{1, \ldots, n\}$, the second form in (7.38) can be rewritten in x_i-elimination form :

$$k_i x_i \gtrless \sum_{j=1}^{i-1} k_j x_j + \sum_{j=i+1}^{n} k_j x_j, \qquad k_i \in \mathbb{N} \setminus \{0\}, \quad k_j \in \mathbb{Z} \setminus \{0\}. \tag{7.39}$$

Again, there is a *weak* x_i-elimination form, which requires a left hand side as in (7.39) with an arbitrary right hand side term t in which x_i does not occur. Positive normal forms are available from Example 3.28.

Lemma 7.13 (Fourier, 1826; Motzkin, 1936)**.** $\mathbf{R} = (\mathbb{R};\ 0, +, -;\ <)$ admits effective QE.

Proof. Consider a positive 1-primitive formula in weak x-elimination form:

$$\varphi \ = \ \exists x \left[\bigwedge_{i=1}^{m} a_i x = t_i \wedge \bigwedge_{j=1}^{n} u_j < b_j x \wedge \bigwedge_{k=1}^{p} c_k x < v_k \right]. \tag{7.40}$$

Let $\lambda = \mathrm{lcm}_{i,j,k}\{a_i, b_j, c_k\}$ and compute t'_i, u'_j, v'_k as in the proof of Lemma 7.3. Then (7.40) is equivalent to

$$\exists x \left[\bigwedge_{i=1}^{m} \lambda x = t'_i \wedge \bigwedge_{j=1}^{n} u'_j < \lambda x \wedge \bigwedge_{k=1}^{p} \lambda x < v'_k \right]. \tag{7.41}$$

Using the same argument as in the proof of Lemma 7.3, it follows that (7.41) is equivalent to

$$\exists y \left[\bigwedge_{i=1}^{m} y = t'_i \wedge \bigwedge_{j=1}^{n} u'_j < y \wedge \bigwedge_{k=1}^{p} y < v'_k \right]. \tag{7.42}$$

We can now continue exactly as in the proof of Lemma 5.6 on effective QE for $(\mathbb{R};\ <)$. Our formula (7.42) matches the formula (5.9) there. □

Corollary 7.14 (Definable sets)**.** *A set $S \subseteq \mathbb{R}$ is definable in $\mathbf{R} = (\mathbb{R};\ 0, +, -;\ <)$ if and only if*

$$S \in \big\{ \varnothing,\ \{0\},\ (-\infty, 0),\ (0, \infty),\ (-\infty, 0],\ [0, \infty),\ \mathbb{R} \setminus \{0\},\ \mathbb{R} \big\}. \tag{7.43}$$

Proof. Since $\mathbf{R}$ admits QE, $S \subseteq \mathbb{R}$ is definable if and only if S is quantifier-free definable, using Theorem 4.12. Let $\varphi'(x)$ be an extended quantifier-free formula in positive normal form. Let α be an atom in φ'. Using our normal forms for atoms we may assume that

$$\alpha \in \big\{\, 0 = 0,\ kx = 0,\ 0 < 0,\ kx < 0,\ 0 < kx \ \big|\ k \in \mathbb{N} \setminus \{0\} \,\big\}. \tag{7.44}$$

For the corresponding extended atoms $\alpha(x)$ we obtain

$$[\alpha]^{\mathbf{R}} \in D, \quad D = \big\{\{0\},\ \mathbb{R},\ (-\infty, 0),\ \varnothing,\ (0, \infty)\big\}. \tag{7.45}$$

Since φ' is reduced to $\vee$, $\wedge$, the set $[\varphi']^{\mathbf{R}}$ is formed from sets in D via unions and intersections. We newly obtain

$$\begin{aligned} D' &= \big\{(-\infty, 0) \cup \{0\},\ (0, \infty) \cup \{0\},\ (-\infty, 0) \cup (0, \infty)\big\} \\ &= \big\{(-\infty, 0],\ [0, -\infty),\ \mathbb{R} \setminus \{0\}\big\}; \end{aligned} \tag{7.46}$$

then $D \cup D'$ is closed under unions and intersections. Hence $[\varphi']^{\mathbf{R}} = D \cup D'$. □

Our next goal is to identify axioms that allow us to define a model class to which the proof of Lemma 7.13 can be generalized.

(i) The proof starts with a 1-primitive formula in (7.40), which contains inequalities in normal form according to (7.38) and (7.39). In addition to $\Xi_{Abelian}$, those normal forms depend on the monotonicity of the order:

$$\Xi_{Monotone} = \{x < y \longrightarrow x + z < y + z\}. \tag{7.47}$$

(ii) The proof then follows the ideas of the proof of Lemma 7.3, which requires the axioms of non-trivial torsion-free divisible Abelian groups as introduced in (7.13):

$$\Xi_{NtDAGroups_0} = \Xi_{NtAGroups} \cup \Xi_{Torsion_0} \cup \Xi_{Divisible}. \tag{7.48}$$

In addition, the step from (7.40) to (7.41) once more requires monotonicity.

(iii) The proof finally delegates (7.42) to Lemma 5.6, the proof of which, in turn, depends on the axioms of dense linear orders as introduced in (5.16):

$$\Xi_{DensLo} = \Xi_{Losets} \cup \Xi_{Dense} \cup \Xi_{NoEndpoints}. \tag{7.49}$$

Monotonicity plays quite an important role here. On the one hand, it forms the bridge between the group structure and the order structure. On the other hand, in combination with other axioms, it entails torsion-freeness on the group side and density and the absence of endpoints on the order side.

Lemma 7.15 (Redundant axioms)**.** Let $\mathbf{A} = (A;\ 0, +, -;\ <)$ be such that

$$\mathbf{A} \models \Xi_{NtAGroups} \cup \Xi_{Divisible} \cup \Xi_{Losets} \cup \Xi_{Monotone}. \tag{7.50}$$

Then the following hold:

(i) $\mathbf{A} \models \Xi_{Torsion_0}$

(ii) $\mathbf{A} \models \Xi_{Dense}$

(iii) $\mathbf{A} \models \Xi_{NoEndpoints}$.

Proof. (i) Let $x \in A$ with $x \neq 0$. We show by induction on $n \in \mathbb{N} \setminus \{0\}$ that $nx \neq 0$. Assume without loss of generality that $0 < x$, using connectivity. For $n = 1$ we have $0 < x = 1 \odot x$. Assume now that $0 < nx$ holds for $n \in \mathbb{N} \setminus \{0\}$. Then $0 < x < nx + x = (n+1)x$, using the induction hypothesis, monotonicity, and transitivity.

(ii) Let $x, y \in A$ with $x < y$. It follows that $0 < y - x$, using monotonicity. Since $\mathbf{A}$ is divisible, there is $z \in A$ such that $2z = x + y$, which can be rewritten as $2(z-x) - y + x = 0$. Monotonicity with the inequality $0 < y - x$ from above and the summand $2(z-x) - y + x$ yields

$$0 = 2(z-x) - y + x < 2(z-x) - y + x + y - x = 2(z-x). \tag{7.51}$$

If $z - x < 2(z-x)$, then $0 = (z-x) - (z-x) < 2(z-x) - (z-x) = z - x$, using monotonicity; else $0 < 2(z-x) \leq z - x$, using transitivity. Monotonicity finally yields $x < z$. Similarly, one shows that $z < y$.

(iii) Let $x \in A$. Since $\mathbf{A}$ is not trivial, there is $a \in A$ with $a \neq 0$, without loss of generality $0 < a$, using connectivity. Monotonicity yields $-a < a - a = 0$. Hence $x < a + x$ and $-a + x < x$, again using monotonicity. □

Our analysis of the proof of Lemma 7.13 in (i)–(iii) above along with the redundancies identified in the previous lemma yield the following axioms and model class of all *divisible ordered Abelian groups*:

$$\Xi_{NtDAGroups_<} = \Xi_{NtAGroups} \cup \Xi_{Divisible} \cup \Xi_{Losets} \cup \Xi_{Monotone}, \tag{7.52}$$

$$NtDAGroups_< = \mathrm{Mod}(\Xi_{NtDAGroups_<}). \tag{7.53}$$

We can now apply the proof of Lemma 7.13 to the class $NtDAGroups_<$ instead of the single structure $\mathbf{R} \in NtDAGroups_<$, which yields the following theorem.

Theorem 7.16. *The class $NtDAGroups_<$ admits effective QE.* □

It immediately follows that $NtDAGroups_<$ is substructure complete and thus also model complete. Groups in $NtDAGroups_<$ share the *trivial ordered group* $(\{0\};\ 0, +, -;\ <)$ as a common substructure up to isomorphism. In combination with substructure completeness, completeness follows via Theorem 6.9. An alternative completeness proof comes with the following corollary, in the course of proving decidability.

Corollary 7.17. *The class $NtDAGroups_<$ is complete and decidable.*

Proof. The language $\mathcal{L}_{Groups_<}$ has a constant symbol 0. Recall that all atomic sentences have the normal form $0 = 0$ or $0 < 0$. Since $\models 0 = 0 \longleftrightarrow$ TRUE and $NtDAGroups_< \models 0 < 0 \longleftrightarrow$ FALSE, $NtDAGroups_<$ is complete and decidable for the set of all atomic sentences, and general completeness and decidability follows by Theorem 4.26(i). □

Example 7.18 (Divisible ordered Abelian groups)**.** $\mathbf{R} = (\mathbb{R};\ 0, +, -;\ <) \in NtDAGroups_<$. Further examples are

$$(\mathbb{R}^n;\ 0, +, -;\ <_{\mathrm{lex}}), \quad (\mathbb{Q}^n;\ 0, +, -;\ <_{\mathrm{lex}}) \in NtDAGroups_< \tag{7.54}$$

for $n \in \mathbb{N} \setminus \{0\}$ with component-wise operations and the lexicographic order. In contrast to the lexicographic order $<_{\text{lex}}$, the component-wise order $<$ on $\mathbb{R}^n$, $\mathbb{Q}^n$ is not connected, thus

$$(\mathbb{R}^n;\ 0, +, -;\ <), \quad (\mathbb{Q}^n;\ 0, +, -;\ <) \notin \mathit{NtDAGroups}_<. \tag{7.55}$$

Given indeterminates $X_1, \ldots, X_n$, every term order[1] on $\{ X_1^{e_1} \cdots X_n^{e_n} \mid (e_1, \ldots, e_n) \in \mathbb{N}^n \}$ induces an order on polynomials with coefficients from a linear ordered set and indeterminates $X_1, \ldots, X_n$. With such an order $<$ we have, e.g.,

$$(\mathbb{R}[X_1, \ldots, X_n];\ 0, +, -;\ <), \quad (\mathbb{Q}[X_1, \ldots, X_n];\ 0, +, -;\ <) \in \mathit{NtDAGroups}_<. \tag{7.56}$$

Recall that $\mathbb{R}^+ = \{ r \in \mathbb{R} \mid r > 0 \}$. The corresponding ordered multiplicative group is isomorphic to $\mathbf{R}$ via the exponential function $\mathbb{R} \to \mathbb{R}^+$, thus

$$(\mathbb{R}^+;\ 1, \cdot, ^{-1};\ <) \in \mathit{NtDAGroups}_<. \tag{7.57}$$

⌟

7.5 Use Case: Linear Programming

Consider the following linear programming problem over the real numbers:

$$\begin{array}{llrcrcr} \text{maximize:} & 3x_1 + 4x_2 & \text{subject to:} & 3x_1 & + & 2x_2 & \leq & 500 \\ & & & -x_1 & & & \leq & 0 \\ & & & x_1 & & & \leq & 100 \\ & & & & & -x_2 & \leq & 0 \\ & & & & & x_2 & \leq & 200. \end{array} \tag{7.58}$$

Using $t_1 \leq t_2$ as a shorthand for $t_1 < t_2 \vee t_1 = t_2$ this translates into an $\mathcal{L}_{\mathit{Groups}_<}$-formula with two free variables ζ and υ as follows:

$$\begin{aligned} \varphi \ = \exists x_1 \exists x_2 (\zeta \leq 3x_1 + 4x_2 \wedge \\ 3x_1 + 2x_2 \leq 500\upsilon \wedge -x_1 \leq 0 \wedge x_1 \leq 100\upsilon \wedge -x_2 \leq 0 \wedge x_2 \leq 200\upsilon). \end{aligned} \tag{7.59}$$

The variable ζ models an upper bound on the defining term of the objective function. This encoding of the objective function as another constraint is a well-known technique in linear programming. However, it requires algorithms that can take free variables, which is not always the case, specifically not with the simplex method. The constraints in (7.58) have plain numbers $z \in \mathbb{Z}$ on their right hand sides. We cannot express such numbers in our language $\mathcal{L}_{\mathit{Groups}_<}$. However, we can express zx_i on the left hand sides as $\pm(x_i + \cdots + x_i)$, as we have regularly done with our normal forms throughout this section. Accordingly, we express the right hand sides as $z\upsilon$. Quantifier elimination results will be equivalent to φ for all choices of υ in $\mathbb{Q}$, including the choice 1 that we are actually interested in.

[1] also called *monomial order* or *admissible order*

Following Theorem 4.2, we reduce to 1-primitive formulas by eliminating prenex quantifiers from the inside to the outside, starting with $\exists x_2$ in our case, and removing constraints not containing x_2 from the scope of the quantifier.

$$\begin{aligned}&\exists x_1(-x_1 \leq 0 \wedge x_1 \leq 100v \wedge \\ &\quad \exists x_2(\zeta \leq 3x_1 + 4x_2 \wedge 3x_1 + 2x_2 \leq 500v \wedge -x_2 \leq 0 \wedge x_2 \leq 200v)).\end{aligned} \tag{7.60}$$

The following positive 1-primitive formula corresponds to (7.40) in the proof of Lemma 7.13. It is easy to see that this proof works also with weak inequalities:

$$\exists x_2 \begin{bmatrix} & -3x_1 + \zeta & \leq & 4x_2 & & \\ \wedge & 0 & \leq & x_2 & & \\ \wedge & & & 2x_2 & \leq & -3x_1 + 500v \\ \wedge & & & x_2 & \leq & 200v \end{bmatrix}. \tag{7.61}$$

We multiply all the constraints with positive integers such that all occurrences of x_2 get a common factor 4, which is the least common multiple of the original factors $\{1,\ 2,\ 4\}$. The result matches (7.41):

$$\exists x_2 \begin{bmatrix} & -3x_1 + \zeta & \leq & 4x_2 & & \\ \wedge & 0 & \leq & 4x_2 & & \\ \wedge & & & 4x_2 & \leq & -6x_1 + 1000v \\ \wedge & & & 4x_2 & \leq & 800v \end{bmatrix}. \tag{7.62}$$

Since our group of the reals is divisible, every rational number can be represented as an integer multiple of 4. This allows us to take an abstract view of the term $4x$ as a variable y. The result matches (7.42):

$$\exists y \begin{bmatrix} & -3x_1 + \zeta & \leq & y & & \\ \wedge & 0 & \leq & y & & \\ \wedge & & & y & \leq & -6x_1 + 1000v \\ \wedge & & & y & \leq & 800v \end{bmatrix}. \tag{7.63}$$

The proof of Lemma 7.13 now redirects us to Lemma 5.6. Indeed, our (7.63) matches also (5.11) in the proof of Lemma 5.6, where we have $n = p = 2$. Again, it is not hard to see that the proof of Lemma 5.6 also works with weak inequalities. Following that proof, we combine all upper bounds on y with all lower bounds on y and obtain the following formula. The result matches (5.12):

$$\begin{bmatrix} & -3x_1 + \zeta & \leq & -6x_1 + 1000v \\ \wedge & -3x_1 + \zeta & \leq & 800v \\ \wedge & 0 & \leq & -6x_1 + 1000v \\ \wedge & 0 & \leq & 800v \end{bmatrix}. \tag{7.64}$$

We can now equivalently replace the subformula starting with $\exists x_2$ in (7.60) with our quantifier-free (7.64). After some obvious simplifications this yields

$$\begin{aligned}&0 \leq 800v \wedge \exists x_1(-x_1 \leq 0 \wedge x_1 \leq 100v \wedge \\ &\qquad 3x_1 + \zeta \leq 1000v \wedge -3x_1 + \zeta \leq 800v \wedge 6x_1 \leq 1000v).\end{aligned} \tag{7.65}$$

We now iterate QE for the next quantifier $\exists x_1$. Compute a positive 1-primitive formula in normal form:

$$\exists x_1 \left[\begin{array}{rcrcl} & 0 & \leq & x_1 & \\ \wedge & \zeta - 800\upsilon & \leq & 3x_1 & \\ \wedge & & & x_1 & \leq & 100\upsilon \\ \wedge & & & 3x_1 & \leq & -\zeta + 1000\upsilon \\ \wedge & & & 6x_1 & \leq & 1000\upsilon \end{array}\right]. \tag{7.66}$$

Multiply with the co-factors of $\operatorname{lcm}\{1,3,6\}$:

$$\exists x_1 \left[\begin{array}{rcrcl} & 0 & \leq & 6x_1 & \\ \wedge & 2\zeta - 1600\upsilon & \leq & 6x_1 & \\ \wedge & & & 6x_1 & \leq & 600\upsilon \\ \wedge & & & 6x_1 & \leq & -2\zeta + 2000\upsilon \\ \wedge & & & 6x_1 & \leq & 1000\upsilon \end{array}\right]. \tag{7.67}$$

Combine all upper bounds with all lower bounds:

$$\left[\begin{array}{rcrcl} & 0 & \leq & & 600\upsilon \\ & 0 & \leq & -2\zeta & + 2000\upsilon \\ & 0 & \leq & & 1000\upsilon \\ \wedge & 2\zeta - 1600\upsilon & \leq & -2\zeta & + 2000\upsilon \\ \wedge & 2\zeta - 1600\upsilon & \leq & & 600\upsilon \\ \wedge & 2\zeta - 1600\upsilon & \leq & & 1000\upsilon \end{array}\right]. \tag{7.68}$$

Finally, simplification yields a quantifier-free equivalent of (7.59):

$$\varphi' \;=\; 0 \leq \upsilon \wedge \zeta \leq 900\upsilon \wedge \zeta \leq 1300\upsilon. \tag{7.69}$$

We now leave our formal QE framework and choose $\upsilon = 1$ in (7.69). The result is a condition on ζ describing the range of the objective function subject to the constraints. We obtain $\zeta \leq 900$. Next, we choose $\upsilon = 1$ and $\zeta = 900$ in (7.65) and obtain

$$\text{TRUE}, \quad 0 \leq x_1, \quad x_1 \leq 100, \quad 3x_1 \leq 100, \quad 100 \leq 3x_1, \quad 3x_1 \leq 500, \tag{7.70}$$

which yields $x_1 = 100/3$. Finally, we get back to (7.60) and choose $\upsilon = 1$, $\zeta = 900$, and $x_1 = 100/3$ instead of the existential quantification of x_1. This yields

$$\text{TRUE}, \quad \text{TRUE}, \quad 200 \leq x_2, \quad x_2 \leq 200, \quad 0 \leq x_2, \quad x_2 \leq 200, \tag{7.71}$$

which can be simplified to $x_2 = 200$. Hence, in (7.58) the maximum of the objective function subject to the constraints is 900. Is is assumed exclusively at the point $(x_1, x_2) = (100/3, 200)$.

In general, one will obtain not a unique value but an interval for the first variable x_1 in (7.70). One can then choose any value from that interval, which in general leads to another interval for the subsequent variable x_2, and so on. This allows to sample the solution space, where choices for coordinates have to be made in the order of the quantifier elimination for the corresponding variables.

8 Quantifier Elimination for Z-Groups

We choose the extension language $\mathcal{L}_0 = (0, 1, +, -; <)$ of the language $\mathcal{L}_{Groups_<} = (0, +, -; <)$ of ordered groups and consider the $\mathcal{L}$-structure $\mathbf{Z}_0 = (\mathbb{Z};\ 0, 1, +, -; <)$ as a discrete counterpart of the divisible ordered Abelian group $\mathbf{R} = (\mathbb{R};\ 0, +, -; <)$ in Section 7.4. Recall our definition $kt = \pm(t + \cdots + t)$ for $k \in \mathbb{Z} \setminus \{0\}$ and $t \in \mathcal{T}$.

Theorem 8.1. $\mathbf{Z}_0 = (\mathbb{Z};\ 0, 1, +, -; <)$ *does not admit QE.*

Proof. It is sufficient to find a definable set that is not quantifier-free definable, using Theorem 4.12. Consider the extended formula $\varphi(y)$ with

$$\varphi \ = \ \exists x(2x = y), \tag{8.1}$$

which defines the set $[\varphi]^{\mathbf{Z}_0} = 2\mathbb{Z}$ of all even integers. Let $\varphi'(y)$ be an extended quantifier-free formula, without loss of generality, in positive normal form. Let α be an atom in φ'. Then

$$\alpha \in \big\{\, 0 = 0,\ l1 = 0,\ ky = 0,\ ky = l1,\ 0 < 0,\ l1 < 0,\ ky < 0,\ ky < l1 \\ \big|\ k, l \in \mathbb{Z} \setminus \{0\} \,\big\}, \tag{8.2}$$

up to equivalence in $\mathbf{Z}_0$. For the corresponding extended atom $\alpha(y)$ we obtain

$$[\alpha]^{\mathbf{Z}_0} \in D, \quad D = \big\{\, \varnothing,\ \{z\},\ (-\infty\,..\,z],\ [z\,..\,\infty),\ \mathbb{Z} \mid z \in \mathbb{Z} \,\big\}. \tag{8.3}$$

Since φ' is reduced to $\vee$, $\wedge$, the set $[\varphi']^{\mathbf{Z}_0}$ is formed from the sets in D via unions and intersections. This yields a finite disjoint union of integer intervals. Hence $[\varphi]^{\mathbf{Z}_0}$ is not quantifier-free definable. □

8.1 Presburger Arithmetic

The proof of the negative result in Theorem 8.1 can be adapted to definable sets $m\mathbb{Z}$ instead of $2\mathbb{Z}$ for arbitrary $m \in \{2, 3, \dots\}$. We thus switch to the infinite language

$$\mathcal{L}_{PrA} = (0, 1, +, -; <, \equiv_1^{(2)}, \equiv_2^{(2)}, \dots) \tag{8.4}$$

of *Presburger Arithmetic* and consider an $\mathcal{L}_{PrA}$-structure

$$\mathbf{Z}_{PrA} = (\mathbb{Z};\ 0, +, -; <, \equiv_1, \equiv_2, \dots), \tag{8.5}$$

where the new relations are defined as follows: For $z_1, z_2 \in \mathbb{Z}$ we say that z_1 *divides* z_2 and we write $z_1 \mid z_2$ if there exists $q \in \mathbb{Z}$ such that $qz_1 = z_2$. In these terms,

$$\equiv_m^{\mathbf{Z}_{PrA}}(z_1, z_2) \ = \ \begin{cases} \top & \text{if} \quad m \mid z_1 - z_2 \\ \bot & \text{else,} \end{cases} \qquad m \in \mathbb{N} \setminus \{0\}. \tag{8.6}$$

It follows that $\mathbf{Z}_{PrA} \vDash x \equiv_1 y \longleftrightarrow \text{TRUE}$. With regard to the proof of Theorem 8.1 we obtain

$$\mathbf{Z}_{PrA} \vDash \exists x(mx = y) \longleftrightarrow y \equiv_m 0, \qquad m \in \mathbb{N} \setminus \{0\}. \tag{8.7}$$

The following three lemmas recall some basic facts about $\equiv_m$ in $\mathbf{Z}_{PrA}$. The proofs, which are essentially direct applications of the axioms of Abelian groups along with definition (8.6), are left as exercises.

Lemma 8.2 (Equivalence relation)**.** Let $m \in \mathbb{N} \setminus \{0\}$. Then the following hold:

(i) reflexivity: $\mathbf{Z}_{PrA} \vDash x \equiv_m x$

(ii) transitivity: $\mathbf{Z}_{PrA} \vDash x \equiv_m y \wedge y \equiv_m z \longrightarrow x \equiv_m z$

(iii) symmetry: $\mathbf{Z}_{PrA} \vDash x \equiv_m y \longrightarrow y \equiv_m x$. □

Hence $\equiv_n$ is an equivalence relation.

Lemma 8.3 (Congruence relation)**.** Let $m \in \mathbb{N} \setminus \{0\}$. Then $\equiv_m$ is compatible with the non-constant functions of $\mathbf{Z}_{PrA}$ in the following sense:

(i) addition: $\mathbf{Z}_{PrA} \vDash x \equiv_m x' \wedge y \equiv_m y' \longrightarrow x + y \equiv_m x' + y'$

(ii) additive inverse: $\mathbf{Z}_{PrA} \vDash x \equiv_m x' \longrightarrow -x \equiv_m -x'$. □

Hence $\equiv_m$ is even a congruence relation. For $z_1, z_2 \in \mathbb{Z}$ with $z_1 \equiv_m z_2$ we say that z_1 is *congruent z_2 modulo n*. Note that compatibility with the constant function 0 in the sense of Lemma 8.3 amounts to an instance $\mathbf{Z}_{PrA} \vDash 0 \equiv_m 0$ of reflexivity, which we have already stated in Lemma 8.2.

Lemma 8.4 (Computing with congruences)**.** Let $m, k \in \mathbb{N} \setminus \{0\}$. Then the following hold:

(i) $\mathbf{Z}_{PrA} \vDash x \equiv_m y \longleftrightarrow x + z \equiv_m y + z$

(ii) $\mathbf{Z}_{PrA} \vDash x \equiv_m y \longleftrightarrow x - y \equiv_m 0$

(iii) $\mathbf{Z}_{PrA} \vDash x \equiv_m y \longleftrightarrow kx \equiv_{km} ky$

(iv) $\mathbf{Z}_{PrA} \vDash x \equiv_{km} y \longrightarrow x \equiv_m y$

(v) If $\gcd(k, m) = 1$, then $\mathbf{Z}_{PrA} \vDash kx \equiv_m ky \longleftrightarrow x \equiv_m y$. □

We generalize the normal forms for terms and equations introduced in Section 7.1 and 7.4 with regard to the constant symbol 1 in $\mathcal{L}_{PrA}$:

(i) Each term t can be written in one of the following forms:

$$0, \quad k1, \quad k_1x_1 + \cdots + k_nx_n, \quad k_1x_1 + \cdots + k_nx_n + k_{n+1}1, \tag{8.8}$$

where $n \geq 1$, $k, k_1, \ldots, k_{n+1} \in \mathbb{Z} \setminus \{0\}$ and $x_1, \ldots, x_n \in \mathcal{V}(t)$.

(ii) Each equation α can be equivalently rewritten in one of the following forms:

$$0 = 0, \quad k1 = 0, \quad k_1x_1 + \sum_{j=2}^{n} k_jx_j = 0, \quad k_1x_1 + \sum_{j=2}^{n} k_jx_j + k_{n+1}1 = 0, \tag{8.9}$$

where $k, k_1 \in \mathbb{N} \setminus \{0\}$, $k_j \in \mathbb{Z} \setminus \{0\}$, and $x_1, x_j \in \mathcal{V}(\alpha)$.

Alternatively, in x_i-elimination form:

$$k_ix_i = \sum_{\substack{j=1 \\ j\neq i}}^{n} k_jx_j, \quad k_ix_i = \sum_{\substack{j=1 \\ j\neq i}}^{n} k_jx_j + k_{n+1}1, \tag{8.10}$$

where $k_i \in \mathbb{N} \setminus \{0\}$, $k_j, k_{n+1} \in \mathbb{Z} \setminus \{0\}$, and $x_i, x_j \in \mathcal{V}(\alpha)$.

(iii) Each inequality α can be equivalently rewritten in one of the following forms, where we use $t_1 > t_2$ as a notational variant of $t_2 < t_1$:

$$0 < 0, \quad k1 \gtrless 0, \quad k_1x_1 + \sum_{j=2}^{n} k_jx_j \gtrless 0, \quad k_1x_1 + \sum_{j=2}^{n} k_jx_j + k_{n+1}1 \gtrless 0, \tag{8.11}$$

where $k, k_1 \in \mathbb{N} \setminus \{0\}$, $k_j \in \mathbb{Z} \setminus \{0\}$, and $x_1, x_j \in \mathcal{V}(\alpha)$.

Alternatively, in x_i-elimination form:

$$k_ix_i \gtrless \sum_{\substack{j=1 \\ j\neq i}}^{n} k_jx_j, \quad k_ix_i \gtrless \sum_{\substack{j=1 \\ j\neq i}}^{n} k_jx_j + k_{n+1}1, \tag{8.12}$$

where $k_i \in \mathbb{N} \setminus \{0\}$, $k_j, k_{n+1} \in \mathbb{Z} \setminus \{0\}$, and $x_i, x_j \in \mathcal{V}(\alpha)$.

(iv) Each congruence α with modulus $m \in \mathbb{N} \setminus \{0\}$ can be equivalently rewritten in one of the following forms:

$$0 \equiv_m 0, \quad k1 \equiv_m 0, \quad k_1x_1 + \sum_{j=2}^{n} k_jx_j \equiv_m 0, \quad k_1x_1 + \sum_{j=2}^{n} k_jx_j + k_{n+1}1 \equiv_m 0, \tag{8.13}$$

where $k, k_j, k_{n+1} \in \{1, \ldots, m-1\}$ and $x_1, x_j \in \mathcal{V}(\alpha)$.

Alternatively, in x_i-elimination form:

$$k_ix_i \equiv_m \sum_{\substack{j=1 \\ j\neq i}}^{n} k_jx_j, \quad k_ix_i \equiv_m \sum_{\substack{j=1 \\ j\neq i}}^{n} k_jx_j + k_{n+1}1, \tag{8.14}$$

where $k_i, k_j, k_{n+1} \in \{1, \ldots, m-1\}$ and $x_i, x_j \in \mathcal{V}(\alpha)$.

Recall that corresponding *weak x_i-elimination forms* isolate k_ix_i with positive k_i one side of a constraint but do not require any special form of the term on the other side of the constraint.

For the sake of a concise notation we admit summands $k1$ within in terms where k can become zero. Unless stated otherwise, the corresponding summand is considered not to be present.

Lemma 8.5 (Euclidean properties)**.** Let $m \in \mathbb{N} \setminus \{0\}$. Then the following hold:

(i) $\mathbf{Z}_{PrA} \models \bigvee_{k=0}^{m-1} x \equiv_m k1$, where $0 \odot 1$ denotes the constant symbol 0

(ii) $\mathbf{Z}_{PrA} \models \bigvee_{k=0}^{m-1} x \equiv_m y + k1$

(iii) $\mathbf{Z}_{PrA} \models \neg\, x \equiv_m y \longleftrightarrow \bigvee_{k=1}^{m-1} x \equiv_m y + k1$

(iv) $\mathbf{Z}_{PrA} \models x \equiv_m y \longleftrightarrow \bigwedge_{k=1}^{m-1} \neg\, x \equiv_m y + k1 \wedge \bigwedge_{k=1}^{m-1} \neg\, x \equiv_m y - k1$.

Proof. (i) Let $z \in \mathbb{Z}$. Division of z by m yields $z = qm + r$ with $r \in \{0, \dots, m-1\}$. It follows that $m \mid z - r$ and thus $z \equiv_m r$.

(ii) Let $z_1, z_2 \in \mathbb{Z}$. Then there is $k \in \{0, \dots, m-1\}$ with $z_1 - z_2 \equiv_m k$ by part (i). It follows that $z_1 \equiv_m z_2 + k$ by Lemma 8.4(i).

(iii) $\mathbf{Z}_{PrA} \models \neg\, x \equiv_m y \longrightarrow \bigvee_{k=1}^{m-1} x \equiv_m y + k1$ follows from part (ii) via rewriting $x \equiv_m y$ for $k = 0$ as $\neg\neg\, x \equiv_m y$. Conversely, let $z_1, z_2 \in \mathbb{Z}$ and $k \in \{1, \dots, m-1\}$ such that $z_1 \equiv_m z_2 + k$. Assume for a contradiction that $z_1 \equiv_m z_2$. Then $z_2 \equiv_m z_2 + k$. It follows that $k \equiv_m 0$ by Lemma 8.4(i), and thus $m \mid k$ by (8.6). This contradicts our choice of k.

(iv) First, note that $\mathbf{Z}_{PrA} \models x \equiv_m y \longleftrightarrow \bigwedge_{k=1}^{m-1} \neg\, x \equiv_m y + k1$ is the contrapositive of part (iii). Second, substitution of $y - m$ for y into this contrapositive yields $\mathbf{Z}_{PrA} \models x \equiv_m y - m \longleftrightarrow \bigwedge_{k=1}^{m-1} \neg\, x \equiv_m y - k1$, and it is easy to see that $\mathbf{Z}_{PrA} \models x \equiv_m y - m \longleftrightarrow x \equiv_m y$. Hence also $\mathbf{Z}_{PrA} \models x \equiv_m y \longleftrightarrow \bigwedge_{k=1}^{m-1} \neg\, x \equiv_m y - k1$. Together these two results entail (iv). □

Part (i) of the lemma can be read as follows: Upon division of x by positive m one can obtain a positive remainder k with $k < m$. This observation is closely related to the the validity of the Euclidean algorithm in $\mathbb{Z}$. Its proof indeed used division with remainder, which goes beyond the axioms of Abelian groups and definition (8.6). The proofs of parts (ii)–(iv) are based on this part (i). Part (iii) provides us with positive normal forms for congruences. Recall that positive normal forms for equations and inequalities are available from Example 3.28.

Theorem 8.6 (Presburger, 1929)**.** $\mathbf{Z}_{PrA} = (\mathbb{Z};\ 0, 1, +, -;\ <, \equiv_1, \equiv_2, \dots)$ *admits effective QE.*

Proof. Consider a positive 1-primitive formula in weak x-elimination form:

$$\varphi \;=\; \exists x \left[\bigwedge_{i=1}^{m} a_i x = t_i \wedge \bigwedge_{j=1}^{n} u_j < b_j x \wedge \bigwedge_{k=1}^{p} c_k x < v_k \wedge \bigwedge_{l=1}^{r} d_l x \equiv_{s_l} w_l \right]. \tag{8.15}$$

Let $\lambda = \operatorname{lcm}_{i,j,k,l}\{a_i, b_j, c_k, d_l\}$, compute t_i', u_j', v_k' as in the proof of Lemma 7.3, and compute s_l' and w_l' analogously. Then $d_l x \equiv_{s_l} w_l$ is equivalent to $\lambda x \equiv_{s_l'} w_l'$ by Lemma 8.4(iii), and thus (8.15) is equivalent to

$$\exists x \left[\bigwedge_{i=1}^{m} \lambda x = t_i' \wedge \bigwedge_{j=1}^{n} u_j' < \lambda x \wedge \bigwedge_{k=1}^{p} \lambda x < v_k' \wedge \bigwedge_{l=1}^{r} \lambda x \equiv_{s_l'} w_l' \right]. \tag{8.16}$$

We equivalently introduce a new variable y that stands for λx:

$$\exists x \exists y \left[y = \lambda x \wedge \bigwedge_{i=1}^{m} y = t_i' \wedge \bigwedge_{j=1}^{n} u_j' < y \wedge \bigwedge_{k=1}^{p} y < v_k' \wedge \bigwedge_{l=1}^{r} y \equiv_{s_l'} w_l' \right]. \tag{8.17}$$

This is semantically equivalent to

$$\exists y \left[\bigwedge_{i=1}^{m} y = t_i' \wedge \bigwedge_{j=1}^{n} u_j' < y \wedge \bigwedge_{k=1}^{p} y < v_k' \wedge \bigwedge_{l=1}^{r} y \equiv_{s_l'} w_l' \wedge \exists x(\lambda x = y) \right]. \tag{8.18}$$

Now we can use the equivalence (8.7) to eliminate the quantifier $\exists x$:

$$\exists y \left[\bigwedge_{i=1}^{m} y = t_i' \wedge \bigwedge_{j=1}^{n} u_j' < y \wedge \bigwedge_{k=1}^{p} y < v_k' \wedge \bigwedge_{l=1}^{r} y \equiv_{s_l'} w_l' \wedge y \equiv_\lambda 0 \right]. \tag{8.19}$$

If $m > 0$, then (8.19) is semantically equivalent to the quantifier-free formula

$$\varphi' \;=\; \bigwedge_{i=2}^{m} t_1' = t_i' \wedge \bigwedge_{j=1}^{n} u_j' < t_1' \wedge \bigwedge_{k=1}^{p} t_1' < v_k' \wedge \bigwedge_{l=1}^{r} t_1' \equiv_{s_l'} w_l' \wedge t_1' \equiv_\lambda 0. \tag{8.20}$$

Assume now that $m = 0$. Let $s = \operatorname{lcm}\{s_1', \ldots, s_r', \lambda\}$. Then (8.19) is equivalent to

$$\exists y \left[\bigwedge_{j=1}^{n} u_j' < y \wedge \bigwedge_{k=1}^{p} y < v_k' \wedge \bigvee_{h \in \{0,1,\ldots,(s-1)1\}} \left[y \equiv_s h \wedge \bigwedge_{l=1}^{r} h \equiv_{s_l'} w_l' \wedge h \equiv_\lambda 0 \right] \right]. \tag{8.21}$$

In order to see this, let $\mu \in \{s_1', \ldots, s_r', \lambda\}$ and $t \in \{w_1', \ldots, w_r', 0\}$, and assume that $y \equiv_\mu t$. Then there is $h \in \{0, \ldots, s-1\}$ such that $y \equiv_s h$. It follows that $\mu \mid s \mid y - h$, thus $y \equiv_\mu h$, and transitivity yields $h \equiv_\mu y \equiv_\mu t$. Conversely, let $h \in \{0, \ldots, s-1\}$ such that $y \equiv_s h$ and $h \equiv_\mu t$. Again, it follows that $y \equiv_\mu h$ and transitivity yields $y \equiv_\mu h \equiv_\mu t$. Next, (8.21) is semantically equivalent to

$$\bigvee_{h \in \{0,1,\ldots,(s-1)1\}} \left[\exists y \left[\bigwedge_{j=1}^{n} u_j' < y \wedge \bigwedge_{k=1}^{p} y < v_k' \wedge y \equiv_s h \right] \wedge \bigwedge_{l=1}^{r} h \equiv_{s_l'} w_l' \wedge h \equiv_\lambda 0 \right]. \tag{8.22}$$

We can thus restrict our attention to positive 1-primitive formulas of the form

$$\exists y \left[\bigwedge_{j=1}^{n} u_j' < y \wedge \bigwedge_{k=1}^{p} y < v_k' \wedge y \equiv_s h \right]. \tag{8.23}$$

If $n = 0$ or $p = 0$, then (8.23) is equivalent to $\varphi' = \text{TRUE}$, because $\mathbb{Z}$ has no minimum or maximum and y can be chosen as $h \mp qs$ for sufficiently large $q \in \mathbb{N}$. Assume now that $n > 0$ and $p > 0$. Then (8.23) is equivalent to the quantifier-free formula

$$\varphi' \;=\; \bigvee_{i=1}^{n} \left[\bigwedge_{j=1}^{n} u_j' < u_i' + 1 \wedge \bigvee_{l=1}^{s} \left[\bigwedge_{k=1}^{p} u_i' + l < v_k' \wedge u_i' + l \equiv_s h \right] \right]. \tag{8.24}$$

The idea of (8.24) is to find $u_i' = \max_j u_j'$ by means of a finite case distinction and try $u_i' + 1$, $\ldots$, $u_i' + s$ as candidates for y. □

Corollary 8.7. $\mathbf{Z}_{PrA} = (\mathbb{Z};\ 0, 1, +, -;\ <, \equiv_1, \equiv_2, \dots)$ *is decidable.*

Proof. The language $\mathcal{L}_{PrA}$ has a constant symbol 0. All atomic sentences have a normal form in

$$\Theta = \Big\{\, 0 = 0,\ k1 = 0,\ 0 < 0,\ k1 < 0,\ 0 < k1,\ 0 \equiv_m 0,\ k'1 \equiv_m 0 \\ \Big|\ k, m \in \mathbb{N} \setminus \{0\},\ k' \in \{1, \dots, m-1\} \,\Big\}. \quad (8.25)$$

There is an algorithm taking $\vartheta \in \Theta$ as input and computing $\tau \in \{\text{TRUE}, \text{FALSE}\}$ such that $\mathbf{Z}_{PrA} \vDash \vartheta \longleftrightarrow \tau$. Hence $\mathbf{Z}_{PrA}$ is decidable. □

8.2 Use Case: Integer Programming

Consider the following linear programming problem over the integers:

$$\text{maximize:}\quad x_1 + 3x_2 \quad \text{subject to:}\quad \begin{array}{rcrcl} 7x_1 & + & x_2 & \leq & 10 \\ -2x_1 & & & \leq & -1 \\ & & -x_2 & \leq & 0. \end{array} \quad (8.26)$$

Using $t_1 \leq t_2$ as a shorthand for $t_1 < t_2 \vee t_1 = t_2$ this translates into an $\mathcal{L}_{PrA}$-formula with one free variable ζ as follows:

$$\varphi \;=\; \exists x_1 \exists x_2 (\zeta \leq x_1 + 3x_2 \wedge 7x_1 + x_2 \leq 10 \wedge -2x_1 \leq -1 \wedge -x_2 \leq 0). \quad (8.27)$$

We have discussed the role of the variable ζ as an upper bound on the defining term of the objective function already in the context of QE-based linear programming over the reals in Section 7.5. In contrast to the situation there, the constant symbol 1 in $\mathcal{L}_{PrA}$ allows us here to express plain integer numbers directly. We again use $\leq$ instead of $<$ throughout the elimination, keeping an eye on possible issues.

We remove $-2x_1 \leq -1$ from the scope of $\exists x_2$ in (8.27), which yields

$$\exists x_1 (-2x_1 \leq -1 \wedge \exists x_2 (\zeta \leq x_1 + 3x_2 \wedge 7x_1 + x_2 \leq 10 \wedge -x_2 \leq 0)), \quad (8.28)$$

Step 1 (Elimination of $\exists x_2$)**.** Our input is the subformula of (8.28) starting with $\exists x_2$. It corresponds to (8.15) in the proof of Theorem 8.6:

$$\exists x_2 \left[\begin{array}{rcrcl} & -x_1 + \zeta & \leq & 3x_2 & \\ \wedge & 0 & \leq & x_2 & \\ \wedge & & & x_2 & \leq\ -7x_1 + 10 \end{array}\right]. \quad (8.29)$$

Multiplication with the co-factors of $\lambda = \operatorname{lcm}\{1, 3\} = 3$ yields the following instance of (8.16):

$$\exists x_2 \left[\begin{array}{rcrcl} & -x_1 + \zeta & \leq & 3x_2 & \\ \wedge & 0 & \leq & 3x_2 & \\ \wedge & & & 3x_2 & \leq\ -21x_1 + 30 \end{array}\right]. \quad (8.30)$$

We introduce a new variable y for $3x_2$ and obtain the following instance of (8.19) with $m = 0$, $n = 2$, $p = 1$, and $r = 0$:

$$\exists y \left[\begin{array}{llllll} & -x_1+\zeta & \leq & y & & \\ \wedge & 0 & \leq & y & & \\ \wedge & & & y & \leq & -21x_1+30 \\ \wedge & & & y & \equiv_3 & 0 \end{array}\right]. \tag{8.31}$$

We compute $s = a = 3$ and obtain the following instance of (8.22), in which the quantified subformula corresponds to (8.23) with $n = 2$ and $p = 1$:

$$\bigvee_{h=0}^{2} \exists y \left[\begin{array}{llllll} & -x_1+\zeta & \leq & y & & \\ \wedge & 0 & \leq & y & & \\ \wedge & & & y & \leq & -21x_1+30 \\ \wedge & & & y & \equiv_3 & h \end{array}\right] \wedge\ h \equiv_3 0. \tag{8.32}$$

There are two possible candidates for the maximum of the lower bounds on y, which we both try, expressing the case distinction as a disjunction:

$$\begin{aligned} \bigvee_{h=0}^{2} \Bigg[\Bigg[0 \leq -x_1+\zeta \ \wedge \bigvee_{l=0}^{2} \left[\begin{array}{llll} & -x_1+\zeta+l & \leq & -21x_1+30 \\ \wedge & -x_1+\zeta+l & \equiv_3 & h \end{array}\right] \\ \vee\ -x_1+\zeta \leq 0 \ \wedge \bigvee_{l=0}^{2} \left[\begin{array}{llll} & l & \leq & -21x_1+30 \\ \wedge & l & \equiv_3 & h \end{array}\right] \Bigg] \wedge\ h \equiv_3 0 \Bigg]. \end{aligned} \tag{8.33}$$

This case distinction within (8.33) essentially matches (8.23) with $n = 2$, $s = 3$, and $p = 1$. However, our use of $\leq$ instead of $<$ causes two subtle differences:

1. With the two cases $0 \leq -x_1+\zeta$ and $-x_1+\zeta \leq 0$ we drop a summand $+1$ on the respective right hand sides.

2. When substituting the candidate terms $-x_1+\zeta+l$ or l for the variable y, we must start from $l = 0$ instead of $l = 1$. We adapt the ranges of the disjunctions over l accordingly.

This concludes the elimination of $\exists x_2$ from the corresponding subformula of (8.28) following the proof of Theorem 8.6. ⌟

The last atom $h \equiv_3 0$ in (8.33), and generally the last atom $h \equiv_\lambda 0$ in (8.22), acts as a filter on the disjunction over h. In our instance (8.33), only $h = 0$ survives.[1] This in turn entails $l = 0$ in the second case of (8.33). With some obvious simplifications this gives us the following equivalent of (8.33):

$$\bigvee_{l=0}^{2} (x_1-\zeta \leq 0 \wedge 20x_1+\zeta \leq 30-l \wedge x_1-\zeta \equiv_3 l) \vee (0 \leq x_1-\zeta \wedge 7x_1 \leq 10). \tag{8.34}$$

[1] This was already visible in (8.32). A corresponding simplification there would just undo the transformation of (8.31) into (8.32). In fact, the introduction of h in (8.32) is not necessary in our case. The reason is that we started without any congruences in (8.29).

We equivalently replace the subformula starting with $\exists x_2$ in (8.28) with our quantifier-free formula (8.34) and arrive at the following equivalent of (8.28):

$$\exists x_1 \left[-2x_1 \leq -1 \wedge \left[\bigvee_{l=0}^{2} (x_1 - \zeta \leq 0 \wedge 20x_1 + \zeta \leq 30 - l \wedge x_1 - \zeta \equiv_3 l) \right.\right. \\ \left.\left. \vee \ (0 \leq x_1 - \zeta \wedge 7x_1 \leq 10) \right] \right]. \tag{8.35}$$

This can be rewritten as a disjunction of four 1-primitive formulas:

$$\bigvee_{l=0}^{2} \exists x_1 (-2x_1 \leq -1 \wedge x_1 - \zeta \leq 0 \wedge 20x_1 + \zeta \leq 30 - l \wedge x_1 - \zeta \equiv_3 l) \tag{8.36}$$

$$\vee \ \exists x_1 (-2x_1 \leq -1 \wedge 0 \leq x_1 - \zeta \wedge 7x_1 \leq 10). \tag{8.37}$$

Step 2a (Uniform elimination of $\exists x_1$ in (8.36))**.** We treat l like a regular variable and start with the following instance of (8.15):

$$\exists x_1 \begin{bmatrix} 1 & \leq & 2x_1 & & \\ \wedge & & 20x_1 & \leq & -\zeta + 30 - l \\ \wedge & & x_1 & \leq & \zeta \\ \wedge & & x_1 & \equiv_3 & \zeta + l \end{bmatrix}. \tag{8.38}$$

Multiplication with the co-factors of $\lambda = \operatorname{lcm}\{1, 2, 20\} = 20$ yields the following instance of (8.16):

$$\exists x_1 \begin{bmatrix} 10 & \leq & 20x_1 & & \\ \wedge & & 20x_1 & \leq & -\zeta + 30 - l \\ \wedge & & 20x_1 & \leq & 20\zeta \\ \wedge & & 20x_1 & \equiv_{60} & 20\zeta + 20l \end{bmatrix}. \tag{8.39}$$

We introduce a new variable y for $20x_1$ and obtain the following instance of (8.19) with $m = 0$, $n = 1$, $p = 2$, and $r = 1$:

$$\exists y \begin{bmatrix} 10 & \leq & y & & \\ \wedge & & y & \leq & -\zeta + 30 - l \\ \wedge & & y & \leq & 20\zeta \\ \wedge & & y & \equiv_{60} & 20\zeta + 20l \\ \wedge & & y & \equiv_{20} & 0 \end{bmatrix}. \tag{8.40}$$

We compute $s = \operatorname{lcm}\{20, 60\} = 60$ and obtain the following instance of (8.22):

$$\bigvee_{h=0}^{59} \exists y \begin{bmatrix} 10 & \leq & y & & \\ \wedge & & y & \leq & -\zeta + 30 - l \\ \wedge & & y & \leq & 20\zeta \\ \wedge & & y & \equiv_{60} & h \end{bmatrix} \wedge \ h \equiv_{60} 20\zeta + 20l \ \wedge \ h \equiv_{20} 0. \tag{8.41}$$

Clearly, 10 is the maximum of the lower bounds, which we must plug in to arrive at (8.24):

$$\bigvee_{h=0}^{59}\bigvee_{l'=0}^{59}\begin{bmatrix} & 10+l' & \leq & -\zeta+30-l \\ \wedge & 10+l' & \leq & 20\zeta \\ \wedge & 10+l' & \equiv_{60} & h \end{bmatrix} \wedge\ h \equiv_{60} 20\zeta+20l \ \wedge\ h \equiv_{20} 0. \tag{8.42}$$

This concludes the uniform elimination of $\exists x_1$ from the three corresponding subformulas of (8.36), following the proof of Theorem 8.6. ⌟

The last atom $h \equiv_{20} 0$ of (8.42) filters the relevant choices for h in the outer disjunction such that only $h = 0$, $h = 20$, and $h = 40$ remain. For each of these remaining choices, the atom $10 + l' \equiv_{60} h$ yields a unique relevant choice for l' in the inner disjunction. Those choices for l' are $l' = 50$, $l' = 10$, and $l' = 30$, respectively. With some obvious simplifications this gives us the following equivalent of (8.36):

$$\bigvee_{\substack{l\in\{0,1,2\}\\(h,l')\in\{(0,50),(20,10),(40,30)\}}} 10+l' \leq 20\zeta \wedge \zeta \leq 20-l'-l \wedge 20\zeta \equiv_{60} h-20l. \tag{8.43}$$

This unfolds as follows, where the rows are choices of (h, l') and the columns are choices of l:

$$\begin{aligned} &(\ \ 3\leq\zeta\leq -30\wedge\zeta\equiv_3 0)\vee(\ \ 3\leq\zeta\leq -31\wedge\zeta\equiv_3 2)\vee(\ \ 3\leq\zeta\leq -32\wedge\zeta\equiv_3 1)\\ \vee&(\ \ 1\leq\zeta\leq\ \ 10\wedge\zeta\equiv_3 1)\vee(\ \ 1\leq\zeta\leq\ \ 9\wedge\zeta\equiv_3 0)\vee(\ \ 1\leq\zeta\leq\ \ 8\wedge\zeta\equiv_3 2)\\ \vee&(-1\leq\zeta\leq -10\wedge\zeta\equiv_3 2)\vee(-1\leq\zeta\leq -11\wedge\zeta\equiv_3 1)\vee(-1\leq\zeta\leq -12\wedge\zeta\equiv_3 0) \end{aligned} \tag{8.44}$$

The first and the last row of (8.44) are equivalent to FALSE due to the inequalities. The second row gives us $\zeta \in \{1, 4, 7, 10\} \cup \{3, 6, 9\} \cup \{2, 5, 8\}$, which can be written in $\mathcal{L}_{PrA}$ as

$$1 \leq \zeta \wedge \zeta \leq 10. \tag{8.45}$$

Step 2b (Elimination of $\exists x_1$ in (8.37))**.** We start with the following instance of (8.15):

$$\exists x_1 \begin{bmatrix} & 1 & \leq & 2x_1 & \\ \wedge & \zeta & \leq & x_1 & \\ \wedge & & & 7x_1 & \leq\ 10 \end{bmatrix}. \tag{8.46}$$

Multiplication with the co-factors of $a = \operatorname{lcm}\{1, 2, 7\} = 14$ yields an instance of (8.16):

$$\exists x_1 \begin{bmatrix} & 7 & \leq & 14x_1 & \\ \wedge & 14\zeta & \leq & 14x_1 & \\ \wedge & & & 14x_1 & \leq\ 20 \end{bmatrix}. \tag{8.47}$$

We introduce y for $14x_1$ and obtain an following instance of (8.19) with $m = 0$, $n = 2$, $p = 1$, and $r = 0$:

$$\exists y \begin{bmatrix} & 7 & \leq & y & \\ \wedge & 14\zeta & \leq & y & \\ \wedge & & & y & \leq\ 20 \\ \wedge & & & y & \equiv_{14}\ 0 \end{bmatrix}. \tag{8.48}$$

We compute $s = \lambda = 14$ and obtain the following instance of (8.22), in which the quantified subformula corresponds to (8.23) with $n = 2$ and $p = 1$:

$$\bigvee_{h=0}^{13} \exists y \left[\begin{array}{llllll} & 7 & \leq & y & & \\ \wedge & 14\zeta & \leq & y & & \\ \wedge & & & y & \leq & 20 \\ \wedge & & & y & \equiv_{14} & h \end{array}\right] \wedge\ h \equiv_{14} 0. \tag{8.49}$$

There are two possible candidates for the maximum of the lower bounds on y, which we both try in a case distinction:

$$\begin{aligned} \bigvee_{h=0}^{13} \Bigg[\Bigg[14\zeta \leq 7 \ \wedge \bigvee_{l=0}^{13} \left[\begin{array}{llll} & 7+l & \leq & 20 \\ \wedge & 7+l & \equiv_{14} & h \end{array}\right] \\ \vee\ 7 \leq 14\zeta \ \wedge \bigvee_{l=0}^{13} \left[\begin{array}{llll} & 14\zeta+l & \leq & 20 \\ \wedge & 14\zeta+l & \equiv_{14} & h \end{array}\right] \Bigg] \wedge\ h \equiv_{14} 0 \Bigg]. \end{aligned} \tag{8.50}$$

This concludes the elimination of $\exists x_1$ from (8.37) following the proof of Theorem 8.6. ⌟

The only possible solution for the last constraint $h \equiv_{14} 0$ in (8.50) is $h = 0$. It follows that the only possible solutions of $7 + l \equiv_{14} 0$ and $14\zeta + l \equiv_{14} 0$ are $l = 7$ and $l = 0$, respectively. With some obvious simplifications (8.50) is equivalent to $2\zeta \leq 1 \vee (1 \leq 2\zeta \wedge 7\zeta \leq 10)$, which is in turn equivalent to

$$\zeta \leq 1. \tag{8.51}$$

Taking our elimination results in (8.45) and (8.51) together, we obtain a quantifier-free equivalent of (8.35) and hence also of our original input formula (8.27):

$$\zeta \leq 10. \tag{8.52}$$

The final QE result in (8.52) makes a statement about the integer linear programming problem in (8.26): The maximum value of the objective function x_1+3x_2 subject to the constraints equals 10. For constructing a point where the maximum is assumed, we get back to the result (8.35) of the elimination of $\exists x_2$. We drop the quantifier $\exists x_1$, substitute $[10/\zeta]$, and simplify. This yields $x_1 = 1$. Next, we get back to our initial input (8.27), drop both quantifiers, substitute $[10/\zeta, 1/x_1]$, and simplify. This yields $x_2 = 3$. Hence, the maximum is assumed exclusively at the point $(x_1, x_2) = (1, 3)$.

8.3 Definable Sets in Presburger Arithmetic

A set $A \subseteq \mathbb{Z}$ is called *periodic* if there exists $p \in \mathbb{N} \setminus \{0\}$ such that for all $z \in \mathbb{Z}$ the following condition holds:

$$z \in A \quad \text{iff} \quad z + p \in A. \tag{8.53}$$

Suitable numbers p are then called a *period* of A. It is easy to see that within the definition, (8.53) can be equivalently phrased as

$$\text{if} \quad z \in A \quad \text{then} \quad z \pm p \in A. \tag{8.54}$$

Example 8.8 (Periodic sets)**.** The sets $\varnothing$, $2\mathbb{Z}$, $6\mathbb{Z}$, and $2\mathbb{Z} \cup (3\mathbb{Z}+1)$ are periodic. All those sets have period 6. The set $2\mathbb{Z}$ also has period 2, and $\varnothing$ has period p for all $p \in \mathbb{N} \setminus \{0\}$. ⌟

For a set $A \subseteq \mathbb{Z}$ we define the *complement* of A as $\mathbb{Z} \setminus A$. We write $\complement A$ for $\mathbb{Z} \setminus A$ and agree that the unary operator $\complement$ binds stronger than all binary operators.

Lemma 8.9 (Closedness under Boolean operations)**.** Let A, $B \subseteq \mathbb{Z}$ be periodic. Then also $\complement A$, $A \cup B$, and $A \cap B$ are periodic.

Proof. Let $a, b \in \mathbb{N} \setminus \{0\}$ be periods of A and B, respectively. Starting with $\complement A$, we have $z \in A$ if and only if $z + a \in A$ by (8.53) and therefore $z \in \complement A$ if and only if $z + a \in \complement A$. Next, consider $A \cup B$. Let $l = \operatorname{lcm}\{a, b\}$, and let $a' = l/a$ and $b' = l/b$. Let $z \in A \cup B$. If $z \in A$, then $z \pm l = z \pm a'a \in A$. If $z \in B$, then $z \pm l = z \pm b'b \in B$. In both cases, $z \pm l \in A \cup B$. Finally, $A \cap B = \complement\big(\complement A \cup \complement B\big)$ by de Morgan's law, and it follows that $A \cap B$ is periodic with a period l. □

We agree that $\gcd(a, b) \geq 0$ for a, $b \in \mathbb{Z}$. The following lemma is commonly known as *Bézout's identity*. It has been stated for the integers by Bachet de Méziriac in 1624 and proved by Bézout for polynomials in 1779. We give a proof over the integers, which is the relevant domain here.

Lemma 8.10 (Bézout, 1779)**.** Let a, $b \in \mathbb{Z}$ with $\gcd(a, b) = g$. Then there exist u, $v \in \mathbb{Z}$ such that $ua + vb = g$. Moreover, the integers of the form $as + bt$ with $s, t \in \mathbb{Z}$ are exactly the multiples of g. □

Proof. If $a = 0$, then $g = \pm b$, and we can choose $u = 0$ and $v = \pm 1$. Assume now that $a \neq 0$. Let $\langle a, b\rangle = \{\, ua + vb \in \mathbb{Z} \mid u, v \in \mathbb{Z} \,\}$ and denote $\langle a, b\rangle^* = \langle a, b\rangle \cap [1\,..\,\infty)$. It is easy to see that $\langle a, b\rangle^* \neq \varnothing$. Let $d = \min \langle a, b\rangle^*$. It is easy to see that $g \mid d$. Division with remainder yields $a = qd + r$ with $r \in [0\,..\,d-1]$. It follows that $a = q(ua + vb) + r$, thus $r = (1 - qu)a + (-qv)b$, and therefore $r = 0$, due to the minimality of $d \in \langle a, b\rangle^*$. Hence $d \mid a$, analogously $d \mid b$, and together $d \mid g$. We have shown that $g \mid d$ and $d \mid g$, and with $g \geq 0$ it follows that $d = g$.

For the second part of the lemma, let $d = kg$ be a multiple of $g = ua + vb$. Then $d = kua + kvb \in \langle a, b\rangle$. Conversely, for $d \in \langle a, b\rangle$ it is easy to see that $g \mid d = ua + vb$. □

From a modern point of view, and using concepts that were not available to Bézout at the time, the lemma states that, as a Euclidean domain, $\mathbb{Z}$ is also a principal ideal domain and that $\langle a, b\rangle = \langle g\rangle$. Of course, the first part of the lemma has its algorithmic counterpart in the extended Euclidean algorithm, which was published by Saunderson in 1740. Our proof of the following theorem requires both parts.

Theorem 8.11 (Linear congruence in one variable)**.** *Let a, $b \in \mathbb{Z}$, let $m \in \mathbb{N} \setminus \{0\}$, and let $g = \gcd(a, m) > 0$. Then the following hold:*

(i) $\mathbf{Z}_{PrA} \vDash \exists x(ax \equiv_m b)$ *if and only if* $g \mid b$.

(ii) Assume that $g \mid b$. Then $ax \equiv_m b$ has exactly g solutions in $\{0, \ldots, m-1\}$. All those g solutions are congruent modulo m/g.

Proof. (i) By definition, $\exists x(ax \equiv_m b)$ is equivalent to $\exists x \exists y(ax + my = b)$, and we can apply the second part of Bézout's Lemma 8.10.

(ii) Let $a' = a/g$, $b' = b/g$, $m' = m/g$. Then $ax \equiv_m b$ is equivalent to

$$a'x \equiv_{m'} b' \tag{8.55}$$

by Lemma 8.4(iii). It is easy to see that $\gcd(a', m') = 1$. Thus by Bézout's Lemma 8.10 there are $u, v \in \mathbb{Z}$ with $a'u + m'v = 1$, from which it follows that $a'u \equiv_{m'} 1$. Moreover, $\gcd(u, m') \mid 1$, thus $\gcd(u, m') = 1$, and multiplication of (8.55) with u equivalently yields

$$x \equiv_{m'} b'u, \tag{8.56}$$

using Lemma 8.4(v). Division with remainder yields $b'u = qm' + r$ with a unique remainder $r \in \{0, \ldots, m' - 1\}$. Since $b'u \equiv_{m'} r$, it follows that (8.56) is equivalent to

$$x \equiv_{m'} r. \tag{8.57}$$

The set of all solutions of (8.57), and thus of the original congruence $a \equiv_m b$, is $m'\mathbb{Z} + r$. Finally,

$$(m'\mathbb{Z} + r) \cap \{0, \ldots, m - 1\} = \{r, r + m', \ldots, r + (g - 1)m'\}. \tag{8.58}$$

Regarding the equality in (8.58), notice that $m'(g - 1) + r = m - (m' - r) \leq m - 1$ and $m'g + r = m + r > m - 1$. From the right hand side of (8.58) we can read off the cardinality of the set, which is g. □

The solutions in (8.58) are called *essentially different* solutions of $a \equiv_m b$. The following corollary is an immediate consequence of Theorem 8.11.

Corollary 8.12 (Sets generated by congruences)**.** *Let $a, b \in \mathbb{Z}$, let $m \in \mathbb{N} \setminus \{0\}$, and let $g = \gcd(a, m)$. Consider the extended formula $\alpha(x)$ with $\alpha = (ax \equiv_m b)$. Then $[\alpha]^{\mathbf{Z}_{\mathrm{PrA}}}$ is a periodic set with period m/g, possibly empty.* □

A set $A \subseteq \mathbb{Z}$ is called *ultimately periodic* if there exist $n \in \mathbb{N} \setminus \{0\}$ and periodic sets A^+ and A^- such that

$$A \cap (-\infty \,..\, -n] = A^- \cap (-\infty \,..\, -n] \quad \text{and} \quad A \cap [n \,..\, \infty) = A^+ \cap [n \,..\, \infty). \tag{8.59}$$

Example 8.13 (Ultimately periodic sets)**.**

(i) The following set is ultimately periodic:

$$A = \big(5\mathbb{Z} \cap (-\infty \,..\, 233]\big) \cup \{2, 3, 5, 8, 13, 21, 34, 55\} \cup \big(89\mathbb{Z} \cap [144 \,..\, \infty)\big). \tag{8.60}$$

For instance, $n = 1000$, $A^- = 5\mathbb{Z}$, and $A^+ = 89\mathbb{Z}$.

(ii) Consider a directed graph (V, E). For $v, w \in V$ the set of all possible lengths of paths from v to w is an ultimately periodic set. The intuition is that a path with a length greater than $|E|$ can only be constructed by iterating loops of certain lengths within that path. This in turn allows arbitrarily many iterations.

(iii) Consider a a context-free language L. The set of all possible word lengths in L is an ultimately periodic set. This observation is related to the Pumping Lemma. ⌟

Lemma 8.14 (Sufficient conditions for ultimate periodicity)**.** Let $A \subseteq \mathbb{Z}$.

(i) If A is periodic, then A is ultimately periodic.

(ii) If A is bounded, then A is ultimately periodic.

(iii) Assume that A is periodic, and let z, $z' \in \mathbb{Z}$. Then $A \cap [z\,..\,z']$, $A \cap (-\infty\,..\,z')$, and $A \cap [z\,..\,\infty)$ are ultimately periodic. Notice that our choice of z, z' admits $z > z'$ with $[z\,..\,z'] = \varnothing$.

Proof. (i) Assume that A is periodic. Then we can choose $A^- = A^+ = A$ and any $n \in \mathbb{N} \setminus \{0\}$.

(ii) Assume that A is bounded with lower bound $l \in \mathbb{Z}$ and upper bound $u \in \mathbb{Z}$. Then $A \subseteq [l\,..\,u]$. For $n = \max\{|l|, |u|\} + 1$ we obtain $A \subseteq [-n+1\,..\,n-1]$, and we can choose $A^- = A^+ = \varnothing$, which is periodic.

(iii) To start with, $A \cap [z\,..\,z']$ is bounded so that ultimate periodicity follows from (ii). Next, for $A \cap (-\infty\,..\,z')$ we can choose $n = |z'| + 1$, $A^- = A$, and $A^+ = \varnothing$. Similarly, for $A \cap [z\,..\,\infty)$ we choose $n = |z| + 1$, $A^- = \varnothing$, and $A^+ = A$. □

Lemma 8.15 (Closedness under Boolean operations)**.** Let A, $B \subseteq \mathbb{Z}$ be ultimately periodic. Then also $\complement A$, $A \cup B$, and $A \cap B$ are ultimately periodic.

Proof. Let $n, m \in \mathbb{N} \setminus \{0\}$, and let A^+, A^-, B^+, B^- be periodic sets such that

$$\begin{aligned} A \cap [n\,..\,\infty) &= A^+ \cap [n\,..\,\infty), & A \cap (-\infty\,..\,-n] &= A^- \cap (-\infty\,..\,-n], \\ B \cap [m\,..\,\infty) &= B^+ \cap [m\,..\,\infty), & B \cap (-\infty\,..\,-m] &= B^- \cap (-\infty\,..\,-m]. \end{aligned} \tag{8.61}$$

Starting with $\complement A$, it follows from (8.61) that also

$$\begin{aligned} \complement A \cap [n\,..\,\infty) &= \big(\complement A \cap [n\,..\,\infty)\big) \cup \big(\complement [n\,..\,\infty) \cap [n\,..\,\infty)\big) \\ &= \big(\complement A \cup \complement [n\,..\,\infty)\big) \cap [n\,..\,\infty) \\ &= \complement\big(A \cap [n\,..\,\infty)\big) \cap [n\,..\,\infty) \\ &= \complement\big(A^+ \cap [n\,..\,\infty)\big) \cap [n\,..\,\infty) \\ &= \complement A^+ \cap [n\,..\,\infty) \end{aligned} \tag{8.62}$$

and, analogously, $\complement A \cap (-\infty\,..\,-n] = \complement A^- \cap (-\infty\,..\,-n]$. According to Lemma 8.9, $\complement A^+$ and $\complement A^-$ are periodic sets. Therefore, $\complement A$ is ultimately periodic. Next, consider $A \cup B$. Let $\mu = \max\{n, m\}$. It follows from (8.61) that

$$\begin{aligned} A \cap [\mu\,..\,\infty) &= A^+ \cap [\mu\,..\,\infty), & A \cap (-\infty\,..\,-\mu] &= A^- \cap (-\infty\,..\,-\mu], \\ B \cap [\mu\,..\,\infty) &= B^+ \cap [\mu\,..\,\infty), & B \cap (-\infty\,..\,-\mu] &= B^- \cap (-\infty\,..\,-\mu]. \end{aligned} \tag{8.63}$$

From (8.63) it follows in turn that also

$$\begin{aligned} \big(A \cup B\big) \cap [\mu\,..\,\infty) &= \big(A \cup B\big) \cap [\mu\,..\,\infty) \cap [\mu\,..\,\infty) \\ &= \big(\big(A \cap [\mu\,..\,\infty)\big) \cup \big(B \cap [\mu\,..\,\infty)\big)\big) \cap [\mu\,..\,\infty) \\ &= \big(\big(A^+ \cap [\mu\,..\,\infty)\big) \cup \big(B^+ \cap [\mu\,..\,\infty)\big)\big) \cap [\mu\,..\,\infty) \\ &= \big(A^+ \cup B^+\big) \cap [\mu\,..\,\infty) \end{aligned} \tag{8.64}$$

and, analogously, $(A \cup B) \cap (-\infty \,..\, -\mu] = (A^- \cup B^-) \cap (-\infty \,..\, -\mu]$. According to Lemma 8.9, $A^+ \cup B^+$ and $A^- \cup B^-$ are periodic sets. Therefore, $A \cup B$ is ultimately periodic. Finally, $A \cap B = \complement\big(\complement A \cup \complement B\big)$ by de Morgan's law, and it follows that also $A \cap B$ is ultimately periodic. □

The main result of this section is a special case of a result by Ginsburg and Spanier, who more generally considered subsets of $\mathbb{Z}^n$ defined by extended Presburger formulas $\varphi(x_1, \ldots, x_n)$ along with a generalization of ultimately periodic sets in $\mathbb{Z}$ to *semi-linear sets* in $\mathbb{Z}^n$.

Theorem 8.16 (Ginsburg–Spanier, 1964)**.** *A set $A \subseteq \mathbb{Z}$ is definable in $\mathbf{Z}_{PrA}$ if and only if A is ultimately periodic.*

Proof. Assume that A is definable. Let $\varphi(x)$ be an extended formula with $[\varphi]^{\mathbf{Z}_{PrA}} = A$. There is a positive extended quantifier-free formula $\varphi'(x)$ with $\mathbf{Z}_{PrA} \vDash \varphi \longleftrightarrow \varphi'$. Since

$$\mathbf{Z}_{PrA} \vDash x = y \longleftrightarrow x - 1 < y \wedge y < x + 1, \tag{8.65}$$

we can assume that there are no equations in φ'. It follows that all atomic formulas in φ' are either atomic sentences or have one of the following normal forms

(a) $kx \gtrless 0$ or $kx \gtrless l1$ with $k \in \mathbb{N} \setminus \{0\}$ and $l \in \mathbb{Z} \setminus \{0\}$

(b) $kx \equiv_m 0$ or $kx \equiv_m l1$ with $m \in \mathbb{N} \setminus \{0\}$ and $k, l \in \{1, \ldots, m-1\}$.

According to Theorem 8.11, the normal forms in (b) are either equivalent to FALSE or to a disjunction of atomic formulas where each one is of the form

(b′) $x \equiv_m 0$ or $x \equiv_m l1$ with $m \in \mathbb{N} \setminus \{0\}$ and $l \in \{1, \ldots, m-1\}$.

All atomic sentences are equivalent to either TRUE or FALSE, and all occurrences of TRUE, FALSE in φ' can be equivalently eliminated. Hence φ' is either equivalent to one of TRUE, FALSE with $[\text{TRUE}]^{\mathbf{Z}_{PrA}} = \mathbb{Z}$ and $[\text{FALSE}]^{\mathbf{Z}_{PrA}} = \varnothing$ periodic, or to a disjunctive normal form $\bigvee_i \varphi'_i$, where each φ'_i is of the form

$$\bigwedge_{j=1}^{n} u_j < b_j x \wedge \bigwedge_{k=1}^{p} c_k x < v_k \wedge \bigwedge_{l=1}^{r} x \equiv_{s_l} w_l \tag{8.66}$$

with $b_j, c_k, s_l \in \mathbb{N} \setminus \{0\}$, $u_j, v_k \in \{\, 0,\ k1 \mid k \in \mathbb{Z} \setminus \{0\} \,\}$, $w_l \in \{0, 1, \ldots, (s_l - 1)1\}$. We may assume that $r > 0$, since one can equivalently add to φ'_i, e.g., $x \equiv_1 0$. Let $s = \operatorname{lcm}\{s_1, \ldots s_r\}$. Then (8.66) is equivalent to

$$\bigvee_{h \in \{0,1,\ldots,(s-1)1\}} \left[\bigwedge_{j=1}^{n} u_j < b_j x \wedge \bigwedge_{k=1}^{p} c_k x < v_k \wedge x \equiv_s h \wedge \bigwedge_{l=1}^{r} h \equiv_{s_l} w_l \right]. \tag{8.67}$$

Each $\bigwedge_l h \equiv_{s_l} w_l$ is a sentence and thus equivalent to either TRUE or FALSE. It follows that φ' is either equivalent to FALSE, again with $[\text{FALSE}]^{\mathbf{Z}_{PrA}} = \varnothing$ periodic, or to a disjunctive normal form $\bigvee_i \varphi''_i$, where each φ''_i is of the form

$$\bigwedge_{j=1}^{n} u_j < b_j x \wedge \bigwedge_{k=1}^{p} c_k x < v_k \wedge x \equiv_s h. \tag{8.68}$$

Let $\mu = \max_j \left\lfloor u_j^{\mathbf{Z}_{PrA}} / b_j^{\mathbf{Z}_{PrA}} \right\rfloor$ and $\nu = \min_k \left\lceil v_k^{\mathbf{Z}_{PrA}} / c_k^{\mathbf{Z}_{PrA}} \right\rceil$. Using the extended formula $\varphi_i''(x)$, we obtain

$$[\varphi_i'']^{\mathbf{Z}_{PrA}} = \begin{cases} [x \equiv_s h]^{\mathbf{Z}_{PrA}} & \text{if} \quad n = p = 0 \\ [x \equiv_s h]^{\mathbf{Z}_{PrA}} \cap (-\infty \,..\, \nu] & \text{if} \quad n = 0,\ p > 0 \\ [x \equiv_s h]^{\mathbf{Z}_{PrA}} \cap [\mu \,..\, \infty) & \text{if} \quad n > 0,\ p = 0 \\ [x \equiv_s h]^{\mathbf{Z}_{PrA}} \cap [\mu \,..\, \nu] & \text{if} \quad n > 0,\ p > 0, \end{cases} \tag{8.69}$$

where possibly $[\mu \,..\, \nu] = \varnothing$. According to Corollary 8.12, $[x \equiv_s h]^{\mathbf{Z}_{PrA}}$ is periodic, and using Lemma 8.14 it follows that $[\varphi_i'']^{\mathbf{Z}_{PrA}}$ is ultimately periodic. Finally,

$$A = [\varphi]^{\mathbf{Z}_{PrA}} = [\varphi']^{\mathbf{Z}_{PrA}} = \left[\bigvee\nolimits_i \varphi_i''\right]^{\mathbf{Z}_{PrA}} = \bigcup\nolimits_i [\varphi_i'']^{\mathbf{Z}_{PrA}} \tag{8.70}$$

is ultimately periodic by Lemma 8.15.

Conversely, assume that A is ultimately periodic. Let $n \in \mathbb{N} \setminus \{0\}$, and let A^-, $A^+ \subseteq \mathbb{Z}$ be periodic sets such that $A \cap (-\infty \,..\, -n] = A^- \cap (-\infty \,..\, -n]$ and $A \cap [n \,..\, \infty) = A^+ \cap [n \,..\, \infty)$. It follows that

$$A = \big(A^- \cap (-\infty \,..\, -n]\big) \cup \big(A \cap [-n+1 \,..\, n-1]\big) \cup \big(A^+ \cap [n \,..\, \infty)\big). \tag{8.71}$$

Let p^+ be a period of A^+ and consider the finite set $A^+ \cap [1 \,..\, p^+] = \{z_1^+, \ldots, z_m^+\}$. Then $z \in A^+$ if and only if there is $z_i^+ \in \{z_1^+, \ldots, z_m^+\} \subseteq \mathbb{N} \setminus \{0\}$ and $k \in \mathbb{Z}$ with $z = z_i^+ + kp^+$. Thus

$$A^+ = [\varphi^+]^{\mathbf{Z}_{PrA}} \quad \text{with} \quad \varphi^+ = \bigvee_{i=1}^{m} \exists k (x = z_i^+ 1 + p^+ k), \tag{8.72}$$

using the extended formula $\varphi^+(x)$. We analogously construct $\varphi^- = \bigvee_j \exists k (x = z_j^- 1 + p^- k)$ such that $A^- = [\varphi^-]^{\mathbf{Z}_{PrA}}$. Finally, consider the finite set $A \cap [-n+1 \,..\, n-1] = \{a_1, \ldots, a_r\}$:

$$A \cap [-n+1 \,..\, n-1] = [\varphi_0]^{\mathbf{Z}_{PrA}} \quad \text{with} \quad \varphi_0 = \bigvee_{i=1}^{r} \begin{cases} x = 0 & \text{if} \quad a_i = 0 \\ x = a_i 1 & \text{else,} \end{cases} \tag{8.73}$$

using the extended formula $\varphi_0(x)$. Hence

$$A = [\varphi]^{\mathbf{Z}_{PrA}} \quad \text{for} \quad \varphi = (x < -n+1 \wedge \varphi^-) \vee \varphi_0 \vee (n-1 < x \wedge \varphi^+), \tag{8.74}$$

using the extended formula $\varphi(x)$. □

8.4 The Ring and the Ordered Ring of the Integers

Our next goal is to add multiplication and investigate the ring and the ordered ring of integers. While both are certainly interesting from a practical point of view, we will obtain negative results. We need two well-known theorems, which we present here without proofs. The first one is the undecidability of *Peano Arithmetic*, i.e., the natural numbers in the language $\mathcal{L}_{PeA} = (+, \cdot)$.

Theorem 8.17 (Gödel, 1931; Rosser 1936)**.** $\mathbf{N}_{PeA} = (\mathbb{N};\ +, \cdot)$ *is undecidable.* □

It is easy to see that $0, 1 \in \mathbb{N}$, ordering, and congruences are definable in $\mathbf{N}_{PeA}$. Recall that expansion structures of undecidable structures are undecidable as well, by Corollary 4.20. Therefore it is generally interesting to formulate undecidability results for small languages.

The second result we need is Lagrange's Four-square Theorem. It provides an integer counterpart to the observation that every non-negative real number can be represented as a square of a real number, which we have used, e.g., in the proof of Theorem 4.13.

Theorem 8.18 (Lagrange, 1770)**.** *Every non-negative integer can be represented as a sum of four squares of integers.* □

We are now equipped to consider the integers $\mathbb{Z}$ instead of $\mathbb{N}$ in the Peano language $\mathcal{L}_{PeA}$.

Theorem 8.19. $\mathbf{Z}_{PeA} = (\mathbb{Z};\ +,\ \cdot\ )$ *is undecidable.*

Proof. Assume for a contradiction that $\mathbf{Z}_{PeA}$ is decidable. Using Lagrange's Four-square Theorem 8.18, the substructure $\mathbf{N}_{PeA} \subseteq \mathbf{Z}_{PeA}$ is definable by $\chi_{\mathbb{N}}(x)$ with

$$\chi_{\mathbb{N}} \ = \ \exists y_1 \exists y_2 \exists y_3 \exists y_4 (x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4). \tag{8.75}$$

It follows that $\mathbf{N}_{PeA}$ is decidable by Theorem 6.6, which contradicts the Gödel–Rosser Theorem 8.17. □

Corollary 8.20. *Every expansion structure of $\mathbf{Z}_{PeA}$ is undecidable. This holds in particular for the ring and the ordered ring of the integers:*

(i) $\mathbf{Z}_{Rings} = (\mathbb{Z};\ 0, 1, +, -, \cdot\ )$ *is undecidable.*

(ii) $\mathbf{Z}_{Rings_<} = (\mathbb{Z};\ 0, 1, +, -, \cdot\ ;\ <)$ *is undecidable.*

Proof. This is a direct application of Corollary 4.20. □

So far, we have derived quite a number of decidability results via Theorem 4.26, which combines effective quantifier eliminability with effective equivalence to $\tau \in \{\text{TRUE}, \text{FALSE}\}$ of atomic formulas in one or zero variables, depending on the availability of a constant symbol in the language. We are now in a situation where we have derived undecidability of the ring and the ordered ring of integers not via effective QE but via reduction to another known undecidability result, namely the Gödel–Rosser Theorem for Peano Arithmetic. On these grounds we can use the contrapositive of Theorem 4.26 to disprove effective quantifier eliminability.

Corollary 8.21. *Consider the ring of integers and the ordered ring of integers.*

(i) $\mathbf{Z}_{Rings} = (\mathbb{Z};\ 0, 1, +, -, \cdot\ )$ *does not admit effective QE.*

(ii) $\mathbf{Z}_{Rings_<} = (\mathbb{Z};\ 0, 1, +, -, \cdot\ ;\ <)$ *does not admit effective QE.*

Proof. (i) Note that $\mathcal{L}_{Rings}$ has a constant symbol. Assume for a contradiction that $\mathbf{Z}_{Rings}$ admits effective QE. All atomic sentences have a normal form in $\Theta = \{\ 0 = 0,\ k1 = 0 \mid k \in \mathbb{N} \setminus \{0\}\ \}$. There is an algorithm taking $\vartheta \in \Theta$ as input and computing $\tau \in \{\text{TRUE}, \text{FALSE}\}$ such that $\mathbf{Z}_{Rings} \vDash \vartheta \longleftrightarrow \tau$. Hence $\mathbf{Z}_{Rings}$ is decidable by Theorem 4.26(i). This contradicts our corresponding undecidability result in Corollary 8.20 above.

(ii) The same argument as in (i) holds for $\mathbf{Z}_{Rings_<}$ instead of $\mathbf{Z}_{Rings}$, considering also normal forms of inequalities, i.e., $\Theta = \{\ 0 = 0,\ k1 = 0,\ 0 < 0,\ k1 < 0,\ 0 < k1 \mid k \in \mathbb{N} \setminus \{0\}\ \}$. □

8.5 Presburger Arithmetic with Divisibility

We now leave multiplication aside and consider the additive ordered group of the integers along with several flavors of divisibility relations instead of congruences. As a preparation, we remind ourselves of the Fundamental Theorem of Arithmetic, the first complete proof of which has been given by Gauss. This came surprisingly late, taking into consideration that the *existence* of prime decompositions in a geometric setting was known to Euclid around 300 BC and proved by Kamāl al-Dīn al-Fārisī around 1300.

Theorem 8.22 (Gauss, 1801)**.** *Every integer greater than* 1 *can be represented uniquely as a product of prime numbers, up to the order of the factors.* □

To start with, we consider $\mathcal{L}_{DivP} = (0, 1, +, -; <, {}_1|^{(1)}, {}_2|^{(1)}, \dots)$ along with $\mathbf{Z}_{DivP}$ where

$$ {}_n|^{\mathbf{Z}_{DivP}}(z) \;=\; \begin{cases} \top & \text{if} \quad n \mid z \\ \bot & \text{else,} \end{cases} \qquad n \in \mathbb{N} \setminus \{0\}, \quad z \in \mathbb{Z}. \tag{8.76} $$

We refer to ${}_n|$ as a *passive divisibility*.[2] It is quite obvious that $\mathbf{Z}_{DivP}$ is $\mathbf{Z}_{PrA}$ in disguise, and thus our results are positive. Nevertheless, it is worth having a look at the exact proof argument.

Theorem 8.23. $\mathbf{Z}_{DivP} = (\mathbb{Z};\ 0, 1, +, -;\ <, {}_1|, {}_2|, \dots)$ *admits effective QE.*

Proof. Let $n \in \mathbb{N} \setminus \{0\}$, and let $z_1, z_2 \in \mathbb{Z}$. Recall from (8.6) that $\equiv_n^{\mathbf{Z}_{PrA}}(z_1, z_2) = \top$ if and only if $n \mid z_1 - z_2$. It follows that passive $\mathcal{L}_{DivP}$ divisibilities ${}_n|(t)$ can be translated into $\mathcal{L}_{PrA}$ congruences $\equiv_n$, and vice versa:

$$ \mathbf{Z}_{DivP} \vDash {}_n|(t) \quad \text{iff} \quad \mathbf{Z}_{PrA} \vDash t \equiv_n 0, \qquad \mathbf{Z}_{PrA} \vDash t_1 \equiv_n t_2 \quad \text{iff} \quad \mathbf{Z}_{DivP} \vDash {}_n|(t_1 - t_2), \tag{8.77} $$

where t, t_1, t_2 are terms over the common algebraic sublanguage $(0, 1, +, -)$ of $\mathcal{L}_{DivP}$ and $\mathcal{L}_{PrA}$. On these grounds, a quantifier elimination procedure for $\mathbf{Z}_{DivP}$ is obtained as follows. Let $\varphi(\mathbf{x})$ be an extended $\mathcal{L}_{DivP}$-formula with $\mathbf{x} \in \mathcal{V}^k$. Compute an $\mathcal{L}_{PrA}$-formula $\bar{\varphi}$ by translating every passive divisibility in φ into a congruence. Apply QE in $\mathbf{Z}_{PrA}$ to compute a quantifier-free $\mathcal{L}_{PrA}$-formula $\bar{\varphi}'$ with $\mathbf{Z}_{PrA} \vDash \bar{\varphi} \longleftrightarrow \bar{\varphi}'$, using Theorem 8.6. Finally, compute a quantifier-free $\mathcal{L}_{DivP}$-formula φ' by translating every congruence in $\bar{\varphi}'$ back into a passive divisibility. For $\mathbf{z} \in \mathbb{Z}^k$ we have

$$ \mathbf{Z}_{DivP} \vDash \varphi(\mathbf{z}) \quad \text{iff} \quad \mathbf{Z}_{PrA} \vDash \bar{\varphi}(\mathbf{z}) \quad \text{iff} \quad \mathbf{Z}_{PrA} \vDash \bar{\varphi}'(\mathbf{z}) \quad \text{iff} \quad \mathbf{Z}_{DivP} \vDash \varphi'(\mathbf{z}), \tag{8.78} $$

using extended formulas $\varphi(\mathbf{x})$, $\bar{\varphi}(\mathbf{x})$, $\bar{\varphi}'(\mathbf{x})$, and $\varphi'(\mathbf{x})$. Hence, $\mathbf{Z}_{DivP} \vDash \varphi \longleftrightarrow \varphi'$. □

Decidability of $\mathbf{Z}_{DivP}$ follows similarly to Corollary 8.7 for Presburger Arithmetic.

Corollary 8.24. $\mathbf{Z}_{DivP} = (\mathbb{Z};\ 0, 1, +, -;\ <, {}_1|, {}_2|, \dots)$ *is decidable.* □

[2] The argument term t of ${}_n|(t)$ is passive in the sense that it is being trial divided by n.

Having coined the notion of passive divisibilities it is natural to think about active divisibilities for a moment. We consider the language $\mathcal{L}_{DivA} = (0, 1, +, -; <, |_1{}^{(1)}, |_2{}^{(1)}, \dots)$ along with $\mathbf{Z}_{DivA}$ where

$$|_n{}^{\mathbf{Z}_{DivA}}(z) = \begin{cases} \top & \text{if} \quad z \mid n \\ \bot & \text{else,} \end{cases} \qquad n \in \mathbb{N} \setminus \{0\}, \quad z \in \mathbb{Z}. \tag{8.79}$$

We refer to $|_n$ as an *active divisibility*. We encounter a situation where QE is not admissible but decidability holds.

Theorem 8.25. $\mathbf{Z}_{DivA} = (\mathbb{Z};\ 0, 1, +, -; <,\ |_1,\ |_2,\ \dots)$ *does not admit QE.*

Proof. Let $n \in \mathbb{N} \setminus \{0\}$ with prime decomposition $n = p_1^{e_1} \cdots p_k^{e_k}$, and let $P_1 = \{1, p_1, \dots, p_1^{e_1}\}$, $\dots$, $P_k = \{1, p_k, \dots, p_k^{e_k}\}$. Then the finite set of all integer divisors of n can be computed as

$$D = \{ \pm q_1 \cdots q_k \in \mathbb{Z} \mid q_1 \in P_1, \dots, q_k \in P_k \}. \tag{8.80}$$

Thus active divisibilities $|_n(t)$ with terms t can be equivalently rewritten as disjunctions of equations by means of the equivalence

$$\mathbf{Z}_{DivA} \vDash |_n(t) \longleftrightarrow \bigvee_{k \in D} t = k1. \tag{8.81}$$

It follows that the quantifier-free definable sets in $\mathbf{Z}_{DivA}$ are the same as in $\mathbf{Z}_0$. Hence $\mathbf{Z}_{DivA}$ does not admit QE, according to the proof of Theorem 8.1. □

Theorem 8.26. $\mathbf{Z}_{DivA} = (\mathbb{Z};\ 0, 1, +, -; <,\ |_1,\ |_2,\ \dots)$ *is decidable.*

Proof. Let ϑ be an $\mathcal{L}_{DivA}$-sentence. We rewrite all active divisibilities $|_n(t)$ in ϑ according to (8.81) and obtain an $\mathcal{L}_0$-sentence $\bar{\vartheta}$ with $\mathbf{Z}_{DivA} \vDash \vartheta \longleftrightarrow \bar{\vartheta}$. Since $\mathbf{Z}_{DivA}|_{\mathcal{L}_0} = \mathbf{Z}_0 = \mathbf{Z}_{PrA}|_{\mathcal{L}_0}$, we can decide ϑ in $\mathbf{Z}_{DivA}$ by applying to $\bar{\vartheta}$ any decision procedure for $\mathbf{Z}_{PrA}$. □

We finally generalize from active and passive divisibilities to the regular binary *divisibility* relation in $\mathbb{Z}$. Consider $\mathcal{L}_{Div} = \left(0, 1, +, -; <, |^{(2)}\right)$ along with $\mathbf{Z}_{Div}$ where

$$|^{\mathbf{Z}_{Div}}(z_1, z_2) = \begin{cases} \top & \text{if} \quad z_1 \mid z_2 \\ \bot & \text{else,} \end{cases} \qquad z_1, z_2 \in \mathbb{Z}. \tag{8.82}$$

We are heading for negative results regarding both quantifier eliminability and decidability of $\mathbf{Z}_{Div}$. Recall that we have obtained corresponding negative results for $\mathbf{Z}_{Rings}$ via step-wise reduction to the undecidable structure $\mathbf{N}_{PeA}$ known from the Gödel–Rosser Theorem 8.17. For establishing a similar chain of arguments for $\mathbf{Z}_{Div}$, we consider the language $\mathcal{L}_{Rob} = (+; \mid)$ along with $\mathbf{N}_{Rob} = (\mathbb{N};\ +;\ \mid)$ as a foundational undecidable structure. We attribute the following theorem to Julia Robinson. Robinson has actually shown a slightly stronger result considering $(\mathbb{N};\ s;\ \mid)$ with the successor function instead of addition, using essentially the proof given below.

Theorem 8.27 (J. Robinson, 1949)**.** $\mathbf{N}_{Rob} = (\mathbb{N};\ +;\ \mid)$ *is undecidable.*

Proof. We show that the graph of the multiplication in $\mathbb{N}$ is definable in $\mathbf{N}_{Rob}$. Define the extended formula $\lambda(x_1, x_2, y)$ with

$$\lambda \;=\; x_1 \mid y \wedge x_2 \mid y \wedge \forall y'(0 < y' \wedge x_1 \mid y' \wedge x_2 \mid y' \longrightarrow y \mid y'). \tag{8.83}$$

For $n_1, n_2, m \in \mathbb{N} \setminus \{0\}$ we have $\mathbf{N}_{Rob} \vDash \lambda(n_1, n_2, m)$ if and only if $\operatorname{lcm}(n_1, n_2) = m$. As an intermediate step, define $\eta(x_1, y)$ with

$$\eta = \lambda[x_1 + 1/x_2]. \tag{8.84}$$

For $n_1, m \in \mathbb{N} \setminus \{0\}$ we have $\mathbf{N}_{Rob} \vDash \eta(n_1, m)$ if and only if $m = \operatorname{lcm}(n_1, n_1 + 1) = n_1(n_1 + 1) = n_1^2 + n_1$. We use η for constructing $\sigma(x_1, y)$ with

$$\sigma = \eta[x_1 + y/y]. \tag{8.85}$$

Then for $n_1, m \in \mathbb{N} \setminus \{0\}$ we have $\mathbf{N}_{Rob} \vDash \sigma(n_1, m)$ if and only if $n_1^2 = m$. Next, define $\mu^*(x_1, x_2, y)$ with

$$\begin{aligned} \mu^* \;=\; \exists x_1' \exists x_2' \exists s(\sigma[x_1'/y] \wedge \sigma[x_2/x_1, x_2'/y] \wedge \sigma[x_1 + x_2/x_1, s/y] \\ \wedge\; s = x_1' + 2y + x_2'). \end{aligned} \tag{8.86}$$

For $n_1, n_2, m \in \mathbb{N} \setminus \{0\}$ we have $\mathbf{N}_{Rob} \vDash \mu^*(n_1, n_2, m)$ if and only if there exist $n_1', n_2', n_s \in \mathbb{Z}$ such that

$$n_1' = n_1^2, \quad n_2' = n_2^2, \quad n_s = (n_1 + n_2)^2, \quad \text{and} \quad n_s = n_1' + 2m + n_2'. \tag{8.87}$$

This is equivalent to $n_1 n_2 = m$ by the binomial identity $(n_1 + n_2)^2 = n_1^2 + 2n_1 n_2 + n_2^2$. Finally, let $\nu \;=\; x_1 \neq 0 \wedge x_2 \neq 0 \wedge y \neq 0$ and define $\mu(x_1, x_2, y)$ with

$$\mu \;=\; (\nu \wedge \mu^*(x_1, x_2, y)) \vee (\neg\nu \wedge (y = 0 \longleftrightarrow x_1 = 0 \vee x_2 = 0)). \tag{8.88}$$

Then for all $n_1, n_2, m \in \mathbb{N}$ we have $\mathbf{N}_{Rob} \vDash \mu(n_1, n_2, m)$ if and only if $n_1 n_2 = m$.

Next, let $\mathcal{L} = (+, \cdot; \mid)$, and let $\mathbf{N} = (\mathbb{N}; +, \cdot; \mid)$. Then $\mathbf{N}$ is an $\mathcal{L}$-expansion of both $\mathbf{N}_{PeA}$ and $\mathbf{N}_{Rob}$. We have shown above that $\mathbf{N} \vDash x_1 \cdot x_2 = y \longleftrightarrow \mu$. We now show that for all $\mathcal{L}$-sentences ϑ one can compute an $\mathcal{L}_{Rob}$-sentence ϑ' such that $\mathbf{N} \vDash \vartheta \longleftrightarrow \vartheta'$. We proceed by induction on the number n of occurrences of the function symbol $\cdot$ in ϑ. If $n = 0$, then we can choose $\vartheta' = \vartheta$. Else, let v_1, v_2, w be variables that do not occur in μ, ϑ. Select any subterm of the form $t_1 \cdot t_2$ in ϑ and let φ be the $\mathcal{L}$-formula obtained from ϑ by replacing that subterm with w. Then

$$\mathbf{N} \vDash \vartheta \longleftrightarrow \tilde{\vartheta}', \quad \tilde{\vartheta}' = \exists v_1 \exists v_2 \exists w(v_1 = t_1 \wedge v_2 = t_2 \wedge \mu[v_1/x_1, v_2/x_2, w/y] \wedge \varphi), \tag{8.89}$$

and by the induction hypothesis one can compute an $\mathcal{L}_{Rob}$-sentence ϑ' such that $\mathbf{N} \vDash \tilde{\vartheta}' \longleftrightarrow \vartheta'$.

Finally, assume for a contradiction that $\mathbf{N}_{Rob}$ is decidable. We give a decision procedure for $\mathbf{N}_{PeA}$. Let ϑ be an $\mathcal{L}_{PeA}$-sentence. Compute an $\mathcal{L}_{Rob}$-sentence ϑ' with $\mathbf{N} \vDash \vartheta \longleftrightarrow \vartheta'$. Using a decision procedure for $\mathbf{N}_{Rob}$, compute $\tau \in \{\text{TRUE}, \text{FALSE}\}$ such that $\mathbf{N}_{Rob} \vDash \vartheta' \longleftrightarrow \tau$. Since $\mathbf{N}_{Rob} = \mathbf{N}|_{\mathcal{L}_{Rob}}$, it follows that also $\mathbf{N} \vDash \vartheta' \longleftrightarrow \tau$, and thus also $\mathbf{N} \vDash \vartheta \longleftrightarrow \tau$. Since $\mathbf{N}_{PeA} = \mathbf{N}|_{\mathcal{L}_{PeA}}$, it follows that $\mathbf{N}_{PeA} \vDash \vartheta \longleftrightarrow \tau$. This contradicts Theorem 8.17. □

Theorem 8.28. $\mathbf{Z}_{Rob_<} = (\mathbb{Z};\ +;\ <,\ |\ )$ *is undecidable.*

Proof. Assume for a contradiction that $\mathbf{Z}_{Rob_<}$ is decidable. Denote $\mathbf{N}_{Rob_<} = (\mathbb{N};\ +;\ <,\ |\ )$. Then the substructure $\mathbf{N}_{Rob_<} \subseteq \mathbf{Z}_{Rob_<}$ is definable by $\chi_{\mathbb{N}}(x)$ with

$$\chi_{\mathbb{N}} \ = \ \forall y(y = y + x \vee y < y + x). \tag{8.90}$$

It follows that $\mathbf{N}_{Rob_<}$ is decidable by Theorem 6.6 and further that the $\mathcal{L}_{Rob}$-restriction $\mathbf{N}_{Rob}$ of $\mathbf{N}_{Rob_<}$ is decidable, by Lemma 4.19. This contradicts Robinson's Theorem 8.27. □

Corollary 8.29. *Every expansion structure of* $\mathbf{Z}_{Rob_<}$ *is undecidable. In particular,* $\mathbf{Z}_{Div} = (\mathbb{Z};\ 0, 1, +, -;\ <,\ |\ )$ *is undecidable.*

Proof. This is a direct application of Corollary 4.20. □

Corollary 8.30. $\mathbf{Z}_{Div} = (\mathbb{Z};\ 0, 1, +, -;\ <,\ |\ )$ *does not admit effective QE.*

Proof. Note that $\mathcal{L}_{Div}$ has a constant symbol. Assume for a contradiction that $\mathbf{Z}_{Div}$ admits effective QE. Since $z_1 \mid z_2$ for $z_1, z_2 \in \mathbb{Z}$ is equivalent to divisibility of the respective absolute values, all atomic sentences have a normal form in

$$\Theta = \Big\{\, 0 = 0,\ k1 = 0,\ 0 < 0,\ k1 < 0,\ 0 < k1,\ 0 \mid 0,\ k1 \mid 0,\ 0 \mid k1,\ k1 \mid l1 \\ \Big|\ k,\ l \in \mathbb{N} \setminus \{0\} \,\Big\}. \tag{8.91}$$

There is an algorithm taking $\vartheta \in \Theta$ as input and computing $\tau \in \{\text{TRUE}, \text{FALSE}\}$ such that $\mathbf{Z}_{Div} \vDash \vartheta \longleftrightarrow \tau$, where for $k1 \mid l1$ one can employ, e.g., the Euclidean algorithm. Hence $\mathbf{Z}_{Div}$ is decidable by Theorem 4.26(i). This contradicts Corollary 8.29. □

8.6 Z-Groups

Throughout this section we have studied a variety of concrete structures, which were all related to $\mathbf{Z}_{PrA} = (\mathbb{Z};\ 0, 1, +, -;\ <, \equiv_1, \equiv_2, \dots)$ in Theorem 8.6. We finally get back to $\mathbf{Z}_{PrA}$ and its language $\mathcal{L}_{PrA}$ and axiomatize an elementary class that contains $\mathbf{Z}_{PrA}$ and admits effective QE following the proof of Theorem 8.6. An analysis of the proof shows that we have used only the following elementary properties of $\mathbf{Z}_{PrA}$:

(i) $\mathbf{Z}_{PrA}$ is a non-trivial Abelian group, corresponding formal axioms $\Xi_{NtAGroups}$ have been given in (7.4);

(ii) 1 is a smallest positive element:

$$\Xi_1 \ = \ \{0 < x \longleftrightarrow x = 1 \vee 1 < x\}; \tag{8.92}$$

(iii) the definition the congruences

$$\Xi_{\equiv} \ = \ \{\, x \equiv_m y \longleftrightarrow \exists z(mz = x - y) \mid m \in \mathbb{N} \setminus \{0\} \,\}; \tag{8.93}$$

(iv) Lemma 8.5(i) along with consequences of it in combination with the other axioms:

$$\Xi_{Euclidean} \;=\; \Big\{ \bigvee_{i=0}^{m-1} x \equiv_m i1 \;\Big|\; m \in \mathbb{N} \setminus \{0\} \Big\},^{3} \tag{8.94}$$

where $0 \odot 1$ denotes the constant symbol 0.

We define the class *ZGroups* of all *Z-groups*[4] as follows:

$$\Xi_{ZGroups} \;=\; \Xi_{NtAGroups} \cup \Xi_1 \cup \Xi_{\equiv} \cup \Xi_{Euclidean}, \quad ZGroups \;=\; \mathrm{Mod}(\Xi_{ZGroups}). \tag{8.95}$$

One can now generalize and apply the proofs of Theorem 8.6 and Corollary 8.7 to the class *ZGroups* instead of the single $\mathcal{L}_{PrA}$-structure $\mathbf{Z}_{PrA} \in ZGroups$. This yields the following corollary:

Corollary 8.31. *The class ZGroups admits effective QE. It follows that ZGroups is substructure complete and model complete. Furthermore, ZGroups is complete and decidable.* □

Example 8.32 (Z-groups)**.** Of course, $\mathbf{Z}_{PrA} \in ZGroups$. Furthermore, we have

$$(\mathbb{Q} \times \mathbb{Z};\ (0,0),\ (0,1),\ +,\ -;\ <_{\mathrm{lex}},\ \equiv_1,\ \equiv_2,\ \dots) \in ZGroups, \tag{8.96}$$

where addition and additive inverse are defined component-wise, and $(q_1, z_1) \equiv_m (q_2, z_2)$ if and only if $z_1 \equiv_m z_2$. It is easy to see that $\{0\} \times \mathbb{Z} \subseteq \mathbb{Q} \times \mathbb{Z}$ is the universe of a substructure of (8.96), which is isomorphic to $\mathbf{Z}_{PrA}$. More generally, we have

$$(\mathbb{Q} \times \cdots \times \mathbb{Q} \times \mathbb{Z};\ (0,\dots,0),\ (0,\dots,0,1),\ +,\ -;\ <_{\mathrm{lex}},\ \equiv_1,\ \equiv_2,\ \dots) \in ZGroups. \tag{8.97}$$

Alternatively, one can consider, e.g., $\mathbb{R} \times \mathbb{Z}$ instead of $\mathbb{Q} \times \mathbb{Z}$. ⌟

Let us once more return to the language $\mathcal{L}_0 = (0, 1, +, -; <)$ from the beginning of the chapter and consider the class $ZGroups'$ of all Z-groups as $\mathcal{L}_0$-structures:

$$ZGroups' = \Big\{ \mathbf{A}|_{\mathcal{L}_0} \;\Big|\; \mathbf{A} \in ZGroups \Big\}. \tag{8.98}$$

For each $\mathbf{A} \in ZGroups$ there is, by definition, a unique $\mathbf{A}|_{\mathcal{L}_0} \in ZGroups'$. Conversely, for each $\mathbf{A}' \in ZGroups'$ there is a unique $\mathbf{A} \in ZGroups$ with $\mathbf{A}|_{\mathcal{L}_0} = \mathbf{A}'$, in which the congruences are defined according to (iii). An axiomatization of the class $ZGroups'$ can be derived from the axiomatization of *ZGroups* above as follows.

(i′) Leave (i) unchanged.

(ii′) Leave (ii) unchanged.

(iii′) Drop the defining axioms (iii) of the congruences.

[3] The formulas $\bigvee_{i=0}^{m-1} x \equiv_m i1$ can be read as follows: *Upon division of x by positive m one can obtain a positive remainder i with $i < m$.* This observation is closely related to the Eucidean algorithm and to so-called Euclidean domains, which motivates the naming $\Xi_{Euclidean}$.

[4] Care must be taken, because the term Z-group refers to a number of distinct types of groups.

(iv′) Adapt (iv) as follows:

$$\Xi'_{Euclidean} \;=\; \Big\{\, \exists z \bigvee_{i=0}^{m-1} mz = x - i1 \;\Big|\; m \in \mathbb{N} \setminus \{0\} \,\Big\}. \tag{8.99}$$

Recall that the existential quantifier can be semantically equivalently moved inside the disjunction, which might be more intuitive.

This yields the following set of axioms:

$$\Xi'_{ZGroups} \;=\; \Xi_{NtAGroups} \cup \Xi_1 \cup \Xi'_{Euclidean}. \tag{8.100}$$

It is not hard to see that $\mathrm{Mod}(\Xi'_{ZGroups}) = ZGroups'$ as in (8.98), and it follows that $ZGroups'$ is an elementary class.

Corollary 8.33. *The class ZGroups′ has the following properties:*

(i) ZGroups′ does not admit QE.

(ii) ZGroups′ is not substructure complete.

(iii) ZGroups′ is complete.

(iv) ZGroups′ is decidable.

(v) ZGroups′ admits effective QE down to existential quantifiers.

(vi) ZGroups′ is model complete.

Proof. (i) The class $ZGroups'$ does not admit QE, because $\mathbf{Z}_0 \in ZGroups'$ does not admit QE, according to Theorem 8.1.

(ii) We have observed that $ZGroups'$ is an elementary class, and we know that $ZGroups'$ does not admit QE by (i). It follows that $ZGroups'$ is not substructure complete, using the contrapositive of Theorem 6.10.

(iii) Let ϑ be an $\mathcal{L}_0$-sentence. Assume that $ZGroups \models \vartheta$, and let $\mathbf{A}' \in ZGroups'$. By the definition of $ZGroups'$ there is $\mathbf{A} \in ZGroups$ with $\mathbf{A}' = \mathbf{A}|_{\mathcal{L}_0}$. Since $\mathbf{A} \models \vartheta$, it follows that $\mathbf{A}' \models \vartheta$, using Lemma 3.9, and we have shown that $ZGroups' \models \vartheta$. Conversely assume that $ZGroups' \models \vartheta$, and let $\mathbf{A} \in ZGroups$. Then $\mathbf{A}|_{\mathcal{L}_0} \in ZGroups'$ and thus $\mathbf{A}|_{\mathcal{L}_0} \models \vartheta$. It follows that $\mathbf{A} \models \vartheta$, again using Lemma 3.9, and we have shown that $ZGroups \models \vartheta$. Hence for all $\mathcal{L}_0$-sentences ϑ,

$$ZGroups' \models \vartheta \quad \text{iff} \quad ZGroups \models \vartheta, \tag{8.101}$$

and completeness of $ZGroups'$ follows from the completeness of $ZGroups$ in Corollary 8.31.

(iv) Let ϑ be an $\mathcal{L}_0$-sentence. According to (8.101), we can decide $ZGroups' \models \vartheta$ using a decision procedure for $ZGroups$, which exists by Corollary 8.31.

(v) Let $\varphi(\mathbf{x})$ be an extended $\mathcal{L}_0$-formula with $\mathbf{x} \in \mathcal{V}^n$. Apply effective QE in $ZGroups$, which is available by Corollary 8.31, to compute an extended positive quantifier-free $\mathcal{L}_{PrA}$-formula $\varphi'(\mathbf{x})$ such that $ZGroups \models \varphi \longleftrightarrow \varphi'$. From φ' compute an extended positive $\mathcal{L}_0$-formula $\varphi''(\mathbf{x})$ by replacing each congruence $t_1 \equiv_m t_2$ equivalently in $ZGroups$ by $\exists z(mz = t_1 - t_2)$, where

without loss of generality $z \notin \mathcal{V}(t_1 - t_2)$. Let now $\mathbf{A}' \in \mathit{ZGroups}'$. Then there is $\mathbf{A} \in \mathit{ZGroups}$ such that $\mathbf{A}' = \mathbf{A}|_{\mathcal{L}_0}$ and, by definition of the $\mathcal{L}_0$-restriction, $A' = A$. For $\mathbf{a} \in A'^n$ we obtain

$$\mathbf{A}' \models \varphi(\mathbf{a}) \quad \text{iff} \quad \mathbf{A} \models \varphi(\mathbf{a}) \quad \text{iff} \quad \mathbf{A} \models \varphi'(\mathbf{a}) \quad \text{iff} \quad \mathbf{A} \models \varphi''(\mathbf{a}) \quad \text{iff} \quad \mathbf{A}' \models \varphi''(\mathbf{a}), \tag{8.102}$$

and there is a semantically equivalent prenex normal form of φ'' which is an existential formula.

(vi) We have observed that $\mathit{ZGroups}'$ is an elementary class, and we know that $\mathit{ZGroups}'$ admits QE down to existential quantifiers by (v). It follows that $\mathit{ZGroups}'$ is model complete, using the equivalence between (i) and (iii) in Theorem 6.12. □

Example 8.34. We started this chapter with the $\mathcal{L}_0$-structure $\mathbf{Z}_0 = (\mathbb{Z};\ 0, 1, +, -;\ <)$ and found that $\varphi = \exists x(2x = y)$ has no quantifier-free equivalent. This motivated the introduction of $\mathcal{L}_{PrA}$ and $\mathbf{Z}_{PrA}$. Nevertheless, $\mathbf{Z}_0 \in \mathit{ZGroups}'$ and therefore $\mathbf{Z}_0$ is decidable, using Theorem 4.23. It should be noted that the decidability of $\mathbf{Z}_0 = \mathbf{Z}_{PrA}|_{\mathcal{L}_0}$ also follows directly from the decidability of $\mathbf{Z}_{PrA}$, using Lemma 4.19. ⌟

9 Quantifier Elimination for Fields

We are going to discuss various classes of fields using the language $\mathcal{L}_{Rings} = (0, 1, +, -, \cdot)$. We admit $t_1 \neq t_2$ as a shorthand for $\neg\, t_1 = t_2$. Recall Example 3.12. The axioms

$$\begin{aligned} \Xi_{Rings} &= \{x + (y + z) = (x + y) + z,\ x + y = y + x,\ x + 0 = x,\ x + -x = 0,\\ &\qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z,\ x \cdot y = y \cdot x,\ x \cdot 1 = x,\\ &\qquad x \cdot (y + z) = (x \cdot y) + (x \cdot z)\},\\ \Xi_{10} &= \{1 \neq 0\},\\ \Xi_{MultInv} &= \{x \neq 0 \longrightarrow \exists y(x \cdot y = 1)\} \end{aligned} \tag{9.1}$$

yield the axioms and the model class of fields:

$$\Xi_{Fields} = \Xi_{Rings} \cup \Xi_{10} \cup \Xi_{MultInv}, \qquad Fields = \mathrm{Mod}(\Xi_{Fields}). \tag{9.2}$$

Note that there is no function symbol for the multiplicative inverse, which is a partial function because $0^{\mathbf{K}}$ for $\mathbf{K} \in Fields$ has not multiplicative inverse. Our logical framework, in contrast, requires function symbols to be interpreted by total functions. Of course, multiplicative inverses and, more generally, division are definable in *Fields*.

Lemma 9.1. $Fields \models x \cdot y = 0 \longleftrightarrow x = 0 \vee y = 0$

Proof. Let $\mathbf{K} \in Fields$, and let $x^*, y^* \in K$. We start with the implication from the right to the left. Assume that, without loss of generality, $x^* = 0^{\mathbf{K}}$. Then, with the functions of $\mathbf{K}$,

$$x^* \cdot y^* = 0 \cdot y^* = (1 - 1) \cdot y^* = y^* - y^* = 0. \tag{9.3}$$

Conversely, assume for a contradiction that $x^* \cdot^{\mathbf{K}} y^* = 0^{\mathbf{K}}$ but $x^* \neq 0^{\mathbf{K}}$ and $y^* \neq 0^{\mathbf{K}}$. Let $\bar{x}^*, \bar{y}^*$ be multiplicative inverses of $x^*, y^* \in K$, respectively. Then, with the functions of $\mathbf{K}$,

$$1 = x^* \cdot y^* \cdot \bar{x}^* \cdot \bar{y}^* = 0 \cdot \bar{x}^* \cdot \bar{y}^* = 0. \tag{9.4}$$

□

Consider the extension language $\mathcal{L}_{Rings_<} = (0, 1, +, -, \cdot\,; <)$ of $\mathcal{L}_{Rings}$. Recall the axioms of linear ordered sets from (5.13) and of monotonicity with respect to addition from (7.47). We newly introduce $\Xi_{ProdPos}$, which states that the product of positive numbers is positive:

$$\begin{aligned} \Xi_{Losets} &= \{\neg\, x < x,\ x < y \vee x = y \vee y < x,\ x < y \wedge y < z \longrightarrow x < z\},\\ \Xi_{Monotone} &= \{x < y \longrightarrow x + z < y + z\},\\ \Xi_{ProdPos} &= \{0 < x \wedge 0 < y \longrightarrow 0 < x \cdot y\}. \end{aligned} \tag{9.5}$$

It is not hard to see that $\Xi_{ProdPos}$ could be equivalently replaced with monotonicity of the linear order with respect to multiplication by positive numbers:

$$\{x < y \wedge 0 < z \longrightarrow x \cdot z < y \cdot z\}. \tag{9.6}$$

In combination with the axioms of fields from above we obtain the axioms of ordered fields and the class of all ordered fields:

$$\Xi_{Fields_<} \;=\; \Xi_{Fields} \cup \Xi_{Losets} \cup \Xi_{Monotone} \cup \Xi_{ProdPos}, \qquad Fields_< \;=\; \mathrm{Mod}(\Xi_{Fields_<}). \tag{9.7}$$

9.1 The Field of the Rational Numbers

Consider the field of rational numbers $\mathbf{Q} = (\mathbb{Q};\ 0, 1, +, -, \cdot) \in Fields$. The following theorem states that $\mathbb{Z}$ is a definable set in $\mathbf{Q}$.

Theorem 9.2 (J. Robinson, 1949)**.** *Consider* $\mathbf{Q} = (\mathbb{Q};\ 0, 1, +, -, \cdot)$ *and the extended formula* $\chi_{\mathbb{Z}}(q)$ *with*

$$\begin{aligned}\chi_{\mathbb{Z}} \;=\; \forall a \forall b \Big(\big(\exists x \exists y \exists z (2 + bz^2 = x^2 + ay^2) \wedge \forall m \big(\exists x \exists y \exists z (2 + abm^2 + bz^2 = x^2 + ay^2) \\ \longrightarrow \exists x \exists y \exists z (2 + ab(m+1)^2 + bz^2 = x^2 + ay^2)\big)\big) \\ \longrightarrow \exists x \exists y \exists z (2 + abq^2 + bz^2 = x^2 + ay^2)\Big).\end{aligned} \tag{9.8}$$

Then for $q^* \in \mathbb{Q}$ *we have* $\mathbf{Q} \vDash \chi_{\mathbb{Z}}(q^*)$ *if and only if* $q^* \in \mathbb{Z}$*. In other words,* $[\chi_{\mathbb{Z}}]^{\mathbf{Q}} = \mathbb{Z}$*.* □

Thus the ring of integers $(\mathbb{Z};\ 0, 1, +, -, \cdot)$ is a definable substructure of $\mathbf{Q}$, and it follows that $\mathbf{Q}$ is undecidable. For general reasons, the same holds for all expansion structures of $\mathbf{Q}$, in particular for $\mathbf{Q}_< \in Fields_<$.

Corollary 9.3. *The field and the ordered field of rational numbers are undecidable:*

(i) $\mathbf{Q} = (\mathbb{Q};\ 0, 1, +, -, \cdot)$ *is undecidable.*

(ii) $\mathbf{Q}_< = (\mathbb{Q};\ 0, 1, +, -;\ <)$ *is undecidable.*

More generally, every expansion structure of $\mathbf{Q}$ *is undecidable.*

Proof. Assume for a contradiction that $\mathbf{Q}$ is decidable. Then $\mathbf{Z}_{Rings} \subseteq \mathbf{Q}$ is definable by $\chi_{\mathbb{Z}}(y)$ with $\chi_{\mathbb{Z}}$ as in (9.8). Therefore, $\mathbf{Z}_{Rings}$ is decidable, by Theorem 6.6. This contradicts Corollary 8.20. It follows further that every expansion structure of $\mathbf{Q}$ is undecidable, by Corollary 4.20, and $\mathbf{Q}_<$ is one such expansion structure. □

Corollary 9.4. *Consider the field and the ordered field of the rational numbers.*

(i) $\mathbf{Q} = (\mathbb{Q};\ 0, 1, +, -, \cdot)$ *does not admit effective QE.*

(ii) $\mathbf{Q}_< = (\mathbb{Q};\ 0, 1, +, -, \cdot;\ <)$ *does not admit effective QE.*

Proof. Analogous to the proof of Corollary 8.21 for the integers. □

As an important consequence, both the class of all fields and the class of all ordered fields do not admit effective QE. This motivates our interest in algebraically closed fields as an important subclass of *Fields* in the next section.

Corollary 9.5.

(i) The class Fields does not admit effective QE.

(ii) The class $\mathsf{Fields}_<$ does not admit effective QE. □

Proof. The class *Fields* does not admit effective QE, because $\mathbf{Q} \in \mathit{Fields}$ does not admit effective QE, according to Corollary 9.4. Analogously, the class $\mathit{Fields}_<$ does not admit effective QE, because $\mathbf{Q}_< \in \mathit{Fields}_<$. □

9.2 Algebraically Closed Fields

For Presburger Arithmetic we used normal forms of terms t in a language $(0, 1, +, -) \subseteq \mathcal{L}_{PrA}$ that were essentially integer linear combinations of variables plus a constant summand; compare (8.8) in the previous chapter:

$$k_1 x_1 + \ldots k_n x_n + k_{n+1}, \qquad k_i \in \mathbb{Z} \setminus \{0\}, \quad x_i \in \mathcal{V}(t). \tag{9.9}$$

The presence of multiplication in $\mathcal{L}_{Rings} = (0, 1, +, -, \cdot)$ more generally calls for multivariate polynomials as normal forms of terms t, e.g., in *distributive representation*

$$\sum_{\mathbf{e} \in S} k_{\mathbf{e}} x_1^{e_1} \cdots x_n^{e_n}, \qquad S \subseteq \mathbb{N}^n \text{ finite}, \quad k_{\mathbf{e}} \in \mathbb{Z} \setminus \{0\}, \quad \mathbf{e} = (e_1, \ldots, e_n), \quad x_i \in \mathcal{V}(t). \tag{9.10}$$

For $S = \varnothing$ we obtain the empty sum, which denotes the term 0. The set of all such distributive normal forms is the *polynomial ring* $\mathbb{Z}[x_1, \ldots, x_n]$, where the ring operations are respective term constructions with subsequent normal form computation.

For separating a certain variable, say x_1, from the others we use a *semi-distributive representation* of t as

$$\sum_{i=0}^{d} p_i x_1^i, \qquad p_i \in \mathbb{Z}[x_2, \ldots, x_n], \quad p_d \neq 0. \tag{9.11}$$

From an algebraic viewpoint, semi-distributive normal forms are elements of $\mathbb{Z}[x_2, \ldots, x_n][x_1]$, which is a univariate polynomial ring in x_1 with coefficients from a polynomial ring $\mathbb{Z}[x_2, \ldots, x_n]$.

Fix now $s \in \mathbb{N}$, $\mathbf{y} \in \mathcal{V}^s$, $x \in \mathcal{V}$, and consider $f = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}[\mathbf{y}][x]$. We define the *x-degree* of f as

$$\deg_x(f) = \begin{cases} m & \text{if} \quad f \neq 0 \\ -\infty & \text{else.} \end{cases} \tag{9.12}$$

We agree that $-\infty < m$ and $(-\infty) + (-\infty) = (-\infty) + m = m + (-\infty) = -\infty$ for $m \in \mathbb{N}$. In the special case that $f \in \mathbb{Z}[x]$ is univariate we speak of the *degree* of f and write $\deg(f)$.

Lemma 9.6. Let $f, g \in \mathbb{Z}[\mathbf{y}][x]$. Then the following hold:

(i) $\deg_x(fg) = \deg_x(f) + \deg_x(g)$

(ii) If $\deg_x(fg) < \deg(f)$ then $g = 0$. □

If $\deg_x(f) > 0$, then we define the *leading x-coefficient* and the *x-reductum* of f as

$$\mathrm{lc}_x(f) = a_m, \qquad \mathrm{red}_x(f) = \sum_{i=0}^{m-1} a_i x^i, \tag{9.13}$$

respectively. It is easy to see that $t = \mathrm{lc}_x(f)x^m + \mathrm{red}_x(f)$. The variable x does not occur in $\mathrm{lc}_x(f)$, and in $\mathrm{red}_x(f)$ it occurs only with powers smaller than $\deg_x(f)$.

Lemma 9.7. Let $f \in \mathbb{Z}[\mathbf{y}][x]$ with $\deg_x(f) > 0$. Then

$$\mathit{Fields} \vDash \mathrm{lc}_x(f) = 0 \wedge f = 0 \longleftrightarrow \mathrm{lc}_x(f) = 0 \wedge \mathrm{red}_x(f) = 0. \tag{9.14}$$

□

Consider $f, g \in \mathbf{Z}[\mathbf{y}][x]$ with $\deg_x(f) \geq \deg_x(g) \geq 0$, say

$$f = \sum_{i=0}^{m} a_i x^i, \quad g = \sum_{j=0}^{n} b_i x^i, \qquad m \geq n \geq 0. \tag{9.15}$$

We compute $h_1 \in \mathbf{Z}[\mathbf{y}][x]$ as follows:

$$h_1 = b_n f - a_m x^{m-n} g = \sum_{k=0}^{m-1} (b_n a_k - a_m b_{k-m+n}) x^k. \tag{9.16}$$

It is well possible that $b_n a_k = a_m b_{k-m+n}$ in $\mathbb{Z}[\mathbf{y}]$ so that not necessarily $\deg_x(h_1) = m - 1$. However, we generally have $\deg_x(h_1) < m$, including the case $h_1 = 0$ with $\deg_x(h_1) = -\infty$. We say that h_1 is obtained by *x-pseudo-reduction* of f modulo g, and we write $f \xrightarrow[g]{} h_1$. Note that h_1 is uniquely determined by f and g.

When iterating x-pseudo-reduction with the same divisor g, the degree strictly decreases with each reduction step. After finitely many steps we obtain

$$f \xrightarrow[g]{} h_1 \xrightarrow[g]{} \cdots \xrightarrow[g]{} h_r = h \quad \text{with} \quad \deg_x(h) < \deg_x(g), \tag{9.17}$$

and there is no further reduction possible. We say that h is *completely reduced* modulo g. By induction on $r \in \mathbb{N}$ there is a unique polynomial $q \in \mathbb{Z}[\mathbf{y}][x]$ such that

$$h = b_n^r f - qg. \tag{9.18}$$

We say that we have performed *x-pseudo-division* of f by g with *quotient* q and *remainder* h.

Lemma 9.8. Let $f, g \in \mathbb{Z}[\mathbf{y}][x]$ with $\deg_x(f) \geq \deg_x(g) > 0$. Let h be the remainder upon x-pseudo-division of f by g. Then

$$\mathit{Fields} \vDash \mathrm{lc}_x(g) \neq 0 \wedge g = 0 \wedge f = 0 \longleftrightarrow \mathrm{lc}_x(g) \neq 0 \wedge g = 0 \wedge h = 0. \tag{9.19}$$

Proof. Recall that $\mathbf{y} \in \mathcal{V}^s$. Let $\mathbf{K} \in \mathit{Fields}$ and let $x^* \in K$, $\mathbf{y}^* \in K^s$. Assume that $\mathrm{lc}_x(g)^{\mathbf{K}}(\mathbf{y}^*) \neq 0$ and $g^{\mathbf{K}}(x^*, \mathbf{y}^*) = 0$. We show that $f^{\mathbf{K}}(x^*, \mathbf{y}^*) = 0$ if and only if $h^{\mathbf{K}}(x^*, \mathbf{y}^*) = 0$. From $h = \mathrm{lc}_x(g)^r f - qg$ it follows that

$$h^{\mathbf{K}}(x^*, \mathbf{y}^*) = \mathrm{lc}_x(g)^{r\mathbf{K}}(\mathbf{y}^*) f^{\mathbf{K}}(x^*, \mathbf{y}^*) - q^{\mathbf{K}}(x^*, \mathbf{y}^*) g^{\mathbf{K}}(x^*, \mathbf{y}^*), \tag{9.20}$$

where $\mathrm{lc}_x(g)^{r\mathbf{K}}(\mathbf{y}^*) = \left(\mathrm{lc}_x(g)^{\mathbf{K}}(\mathbf{y}^*)\right)^r \neq 0$ and $q^{\mathbf{K}}(x^*, \mathbf{y}^*) g^{\mathbf{K}}(x^*, \mathbf{y}^*) = 0$. Hence

$$h^{\mathbf{K}}(x^*, \mathbf{y}^*) = \lambda f^{\mathbf{K}}(x^*, \mathbf{y}^*) \tag{9.21}$$

with $\lambda = \mathrm{lc}_x(g)^{r\mathbf{K}}(\mathbf{y}^*) \neq 0$. □

For equations we have normal forms $t = 0$ with $t \in \mathbb{Z}[\mathbf{y}][x]$. Recall that we shortly write $t \neq 0$ for $\neg\, t = 0$. We start with a quantifier elimination procedure for the field of complex numbers.

Theorem 9.9 (Tarski, 1935)**.** $\mathbf{C} = (\mathbb{C};\ 0, 1, +, -,\ \cdot\ )$ *admits effective QE.*

Proof. Consider a 1-primitive formula

$$\varphi \ = \ \exists x \left[\bigwedge_{i=1}^{M} f_i = 0 \wedge \bigwedge_{j=1}^{N} g_j \neq 0 \right], \qquad f_i,\ g_j \in \mathbb{Z}[\mathbf{y}][x]. \tag{9.22}$$

We may assume that x occurs in all atomic formulas and thus $\deg_x(f_i) > 0$ and $\deg_x(g_j) > 0$; compare the remark after Theorem 4.2. Formula (9.22) is equivalent to

$$\exists x \left[\bigwedge_{i=1}^{M} f_i = 0 \wedge g \neq 0 \right], \quad g = \prod_{j=1}^{N} g_j. \tag{9.23}$$

Recall that $g = 1$ for $N = 0$. Let $g = \sum_{j=0}^{n} b_j x^j$ with $b_j \in \mathbb{Z}[\mathbf{y}]$.

Case 1: $M = 0$. Then (9.23) is equivalent to $\exists x[g \neq 0]$. We show that this is equivalent to

$$\varphi' \ = \ \bigvee_{j=0}^{n} b_j \neq 0. \tag{9.24}$$

Let $\mathbf{y}^* \in \mathbb{C}^s$ and note that $g^* = g(x, \mathbf{y}^*) = \sum_{j=0}^{n} b_j(\mathbf{y}^*) x^j \in \mathbb{C}[x]$ is a univariate polynomial. According to the fundamental theorem of algebra, there exists $x^* \in \mathbb{C}$ with $g^*(x^*) \neq 0$ if and only if g^* is not the zero polynomial if and only if $\mathbf{C} \vDash \varphi'(\mathbf{y}^*)$.

Case 2: $M = 1$. Then (9.23) is equivalent to $\exists x[f_1 = 0 \wedge g \neq 0]$. Let $f_1 = \sum_{i=0}^{m} a_i x^i$ with $a_i \in \mathbb{Z}[\mathbf{y}]$. We show by strong induction on $m = \deg_x(f_1) > 0$ that we can construct a quantifier-free equivalent φ' of (9.23). We equivalently rewrite (9.23) as

$$\left(a_m \neq 0 \wedge \exists x\,[f_1 = 0 \wedge g \neq 0]\right) \vee \tag{9.25}$$
$$\left(a_m = 0 \wedge \exists x\,[\mathrm{red}_x(f_1) = 0 \wedge g \neq 0]\right), \tag{9.26}$$

using Lemma 9.7. For (9.26) we distinguish two cases regarding $m' = \deg_x(\operatorname{red}_x(f_1))$: If $m' \leq 0$, then (9.26) matches Case 1, and we can construct a quantifier-free equivalent following the proof there. Else we have $0 < m' < m$, and we can construct a quantifier-free equivalent by the induction hypothesis.

It remains to construct a quantifier-free equivalent for (9.25). Pseudo-division of g^m by f_1 yields a quotient $q \in \mathbb{Z}[x, \mathbf{y}]$ and a remainder

$$h = a_m^r g^m - q f_1 \in \mathbb{Z}[x, \mathbf{y}], \qquad \deg_x(h) < \deg_x(f_1). \tag{9.27}$$

Let $h = \sum_{k=0}^{p} c_k x^k$ with $c_k \in \mathbb{Z}[\mathbf{y}]$. We show that (9.25) is equivalent to

$$\varphi' \;=\; a_m \neq 0 \wedge \bigvee_{k=0}^{p} c_k \neq 0. \tag{9.28}$$

Let $\mathbf{y}^* \in \mathbb{C}^s$ with $a_m(\mathbf{y}^*) \neq 0$. We use notations $a_m^* = a_m(\mathbf{y}^*)$, $b_n^* = b_n(\mathbf{y}^*) \in \mathbb{C}$ and

$$f_1^* = f_1(x, \mathbf{y}^*), \quad g^* = g(x, \mathbf{y}^*), \quad h^* = h(x, \mathbf{y}^*), \quad q^* = q(x, \mathbf{y}^*) \;\in\; \mathbb{C}[x]. \tag{9.29}$$

Note that the evaluation homomorphism yields $h^* = {a_m^*}^r {g^*}^m - q^* f_1^*$ with

$$\deg_x(h^*) \leq \deg_x(h) < \deg_x(f_1) = \deg_x(f_1^*), \tag{9.30}$$

where $\deg_x(f_1^*) = \deg_x(f_1)$ follows from our choice of $\mathbf{y}^*$ with $a_m^* \neq 0$.

Assume that there exists $x^* \in \mathbb{C}$ such that $f_1^*(x^*) = 0$ and $g^*(x^*) \neq 0$. It follows that $h^*(x^*) = {a_m^*}^r {g^*}^m(x^*) \neq 0$. Thus h^* is not the zero polynomial, and it follows that $\mathbf{C} \vDash \varphi'(\mathbf{y}^*)$.

Conversely, assume that $\mathbf{C} \vDash \varphi'(\mathbf{y}^*)$. Univariate polynomial factorization yields

$$f_1^* = a_m^* \prod_{i=1}^{\mu} (x - \alpha_i)^{t_i}, \quad g^* = b_n^* \prod_{j=1}^{\nu} (x - \beta_j)^{u_j}, \tag{9.31}$$

where the $\alpha_i \in \mathbb{C}$ and $\beta_j \in \mathbb{C}$ are pairwise different, respectively, $0 < t_i \leq m$, and $0 < u_j < n$.

Assume for a contradiction that $\{\alpha_1, \ldots, \alpha_\mu\} \subseteq \{\beta_1, \ldots, \beta_\nu\}$, without loss of generality $(\alpha_1, \ldots, \alpha_\mu) = (\beta_1, \ldots, \beta_\mu)$. It follows that ${g^*}^m$ is divisible by f_1^* with a polynomial quotient

$${g^*}^m / f_1^* \;=\; {a_m^*}^{-1} {b_n^*}^m \prod_{i=1}^{\mu} (x - \beta_i)^{mu_i - t_i} \prod_{j=\mu+1}^{\nu} (x - \beta_j)^{mu_j} \;\in\; \mathbb{C}[x]. \tag{9.32}$$

With $q' = {a_m^*}^r {g^*}^m / f_1^* \in \mathbb{C}[x]$ this yields $q' f_1^* = {a_m^*}^r {g^*}^m = h^* + q^* f_1^*$, and it follows that

$$h^* = (q' - q^*) f_1^*. \tag{9.33}$$

With (9.30) and Lemma 9.6 it follows that $h^* = 0$. However, our assumption $\mathbf{C} \vDash \varphi'(\mathbf{y}^*)$ states that $h^* \neq 0$, a contradiction.

Hence, we can choose $x^* \in \{\alpha_1, \ldots, \alpha_\mu\} \setminus \{\beta_1, \ldots, \beta_\nu\} \neq \varnothing$, which satisfies $f_1^*(x^*) = 0$ and $g^*(x^*) \neq 0$.

Case 3: $m > 1$. We proceed by strong induction on $d = \sum_{i=1}^{M} \deg_x(f_i) \in \mathbb{N} \setminus \{0, 1\}$. Assume without loss of generality that

$$d > \deg_x(f_1) \geq \cdots \geq \deg_x(f_M) > 0. \tag{9.34}$$

Pseudo-division of f_1 by f_2 yields $h = \mathrm{lc}_x(f_2)^r f_1 - q f_2$ with $\deg_x(h) < \deg_x(f_2)$. Formula (9.23) is equivalent to

$$\exists x \left[\mathrm{lc}_x(f_2) \neq 0 \wedge h = 0 \wedge f_2 = 0 \wedge \bigwedge_{i=3}^{M} f_i = 0 \wedge g \neq 0 \right] \tag{9.35}$$

$$\vee \exists x \left[\mathrm{lc}_x(f_2) = 0 \wedge \mathrm{red}_x(f_2) = 0 \wedge f_1 = 0 \wedge \bigwedge_{i=3}^{M} f_i = 0 \wedge g \neq 0 \right] \tag{9.36}$$

by introducing a case distinction on the vanishing of $\mathrm{lc}_x(f_2)$ and applying Lemma 9.8 and 9.7 in (9.35) and (9.36), respectively.

In (9.35) the induction parameter d has decreased by $\deg_x(f_1) > 0$ if x does not occur in h, and by $\deg_x(f_1) - \deg_x(h) > 0$ else. Similarly, in (9.36) d has decreased by $\deg_x(f_2) > 0$ if x not in $\mathrm{red}_x(f_2)$, and by $\deg_x(f_2) - \deg_x(\mathrm{red}_x(f_2)) > 0$ else. In both cases we are either in Case 2, or we obtain a quantifier-free equivalent by the induction hypothesis. □

Corollary 9.10 (Tarski, 1935)**.** $\mathbf{C} = (\mathbb{C};\ 0, 1, +, -, \cdot)$ *is decidable.*

Proof. The language $\mathcal{L}_{Rings}$ has a constant symbol. All atomic sentences have a normal form in $\Theta = \{\, k = 0 \mid k \in \mathbb{Z} \,\}$. There is an algorithm taking $\vartheta \in \Theta$ as input and computing $\tau \in \{\mathrm{TRUE}, \mathrm{FALSE}\}$ such that $\mathbf{C} \vDash \vartheta \longleftrightarrow \tau$. Hence $\mathbf{C}$ is complete and decidable for the set of all atomic sentences. General decidability follows by Theorem 4.26(i). □

An analysis of the proof shows that we have used the following elementary properties of $\mathbf{C}$:

(i) $\mathbf{C}$ is a field; the field axioms Ξ_{Fields} are listed in (9.2);

(ii) $\mathbf{C}$ *algebraically closed*, i.e., every univariate polynomial $f \in \mathbb{C}[X]$ of positive degree has at least one zero:

$$\Xi_{AC} = \left\{ a_n \neq 0 \longrightarrow \exists x \sum_{i=0}^{n} a_i x^i = 0 \;\middle|\; n \in \mathbb{N} \setminus \{0\} \right\}. \tag{9.37}$$

We define the class *ACF* of all *algebraically closed fields* as follows:

$$\Xi_{ACF} = \Xi_{Fields} \cup \Xi_{AC}, \quad ACF = \mathrm{Mod}(\Xi_{ACF}). \tag{9.38}$$

Lemma 9.11 (Properties of algebraically closed fields)**.** Let $\mathbf{K} \in ACF$. Then the following hold:

(i) Every $f \in K[x]$ of degree $n \in \mathbb{N} \setminus \{0\}$ factors into n linear factors.

(ii) K is infinite.

Proof. (i) We proceed by strong induction on $\deg(f) = n \in \mathbb{N} \setminus \{0\}$. According to Ξ_{AC}, there is at least one $k \in K$ with $f(k) = 0$. Division with remainder yields $h = f - q(x - k)$ with $\deg(h) < \deg(x - k) = 1$ and thus $h \in K$. Furthermore, $h(k) = f(k) - q(k)(k - k) = 0$ and thus $h = 0$. Hence $f = q(x - k)$ and $\deg(q) = \deg(f) - 1$ using Lemma 9.6. If $\deg(q) = 1$, then we are finished, else we apply the induction hypothesis to q.

(ii) Assume for a contradiction that K is finite, say $K = \{k_1, \ldots, k_n\}$. Consider the polynomial $f = 1 + \prod_{i=1}^{n}(x - k_i)$. We have $f(k) = 1$ for all $k \in K$. According to (i), f factors into linear factors. It follows that there are $k \in K$ and $q \in K[x]$ such that $f = (x - k)q$ and thus $f(k) = 0$, a contradiction. □

One can now generalize and apply the proof of Theorem 9.9 to the class *ACF* instead of the single $\mathcal{L}_{Rings}$-structure $\mathbf{C} \in ACF$. This yields the following corollary of the Theorem 9.9.

Corollary 9.12 (Tarski, 1935)**.** *The class ACF admits effective QE.* □

Every field $\mathbf{K}$ has a *characteristic* $\mathrm{char}(\mathbf{K})$, which is the smallest number $n \in \mathbb{N} \setminus \{0\}$ such that $\mathbf{K} \vDash n \odot 1 = 0$, provided that such a number exists. Otherwise $\mathrm{char}(\mathbf{K}) = 0$. For instance, the finite fields $\mathbf{Z}/p$ have characteristic p, and $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ all have characteristic 0.

Lemma 9.13. Let $\mathbf{K}$ be a field with $\mathrm{char}(\mathbf{K}) = n \in \mathbb{N} \setminus \{0\}$. Then n is prime.

Proof. To start with, we show by induction on $r \in \mathbb{N} \setminus \{0\}$ that

$$\mathbf{K} \vDash (r \odot 1) \cdot (s \odot 1) = (r \times s) \odot 1, \qquad r,\ s \in \mathbb{N} \setminus \{0\}. \tag{9.39}$$

Notice that (9.39) combines three different notions of multiplication: The n-fold addition $\odot$, the function $\cdot^{\mathbf{K}}$ of the field $\mathbf{K}$, and meta-mathematical multiplication $\times$ of positive integers. For $r = 1$ we obtain

$$\big((1 \odot 1) \cdot (s \odot 1)\big)^{\mathbf{K}} = \big(1 \cdot (s \odot 1)\big)^{\mathbf{K}} = \big(s \odot 1\big)^{\mathbf{K}} = \big((1 \times s) \odot 1\big)^{\mathbf{K}}, \tag{9.40}$$

using the neutrality of 1 in both $\mathbf{K}$ and $\mathbb{N}$. For $r + 1$ we obtain

$$\begin{aligned} \big(((r+1) \odot 1) \cdot (s \odot 1)\big)^{\mathbf{K}} &= \big((r \odot 1 + 1) \cdot (s \odot 1)\big)^{\mathbf{K}} \\ &= \big((r \odot 1) \cdot (s \odot 1) + 1 \cdot (s \odot 1)\big)^{\mathbf{K}} \\ &= \big((r \times s) \odot 1 + s \odot 1\big)^{\mathbf{K}} \\ &= \big(((r+1) \times s) \odot 1\big)^{\mathbf{K}}, \end{aligned} \tag{9.41}$$

using the law of distributivity, the neutrality of 1, and the induction hypothesis.

Assume for a contradiction that $\mathrm{char}(\mathbf{K}) = n = r \times s$ with $r, s \in \mathbb{N} \setminus \{0, 1\}$. Using (9.39) above we obtain

$$\mathbf{K} \vDash (r \odot 1) \cdot (s \odot 1) = 0. \tag{9.42}$$

It follows that, without loss of generality, $\mathbf{K} \vDash r \odot 1 = 0$ and thus $\mathrm{char}(\mathbf{K}) \leq r < r \times s$. □

We define the class $ACF_0 = \{\, \mathbf{K} \in ACF \mid \mathrm{char}(\mathbf{K}) = 0 \,\}$, and for each prime p we define the class $ACF_p = \{\, \mathbf{K} \in ACF \mid \mathrm{char}(\mathbf{K}) = p \,\}$. This yields a partitioning of the class *ACF*. The following theorem resembles Theorem 5.2 for sets.

Theorem 9.14. *Let ϑ be an $\mathcal{L}_{Rings}$-sentence. Then one can compute a set P_ϑ of primes with the following properties:*

(i) P_ϑ is finite or cofinite;

(ii) $ACF_p \vDash \vartheta$ if and only if $p \in P_\vartheta$;

(iii) $ACF_0 \vDash \vartheta$ if and only if P_ϑ is cofinite.

Proof. Without loss of generality, ϑ is reduced to $\neg$, $\wedge$, and $\vee$. We proceed by strong induction on the word length $|\vartheta| \in \mathbb{N}$. If ϑ is atomic, then ϑ has a normal form $k = 0$ with $k \in \mathbb{Z}$. If $k = 0$, then P_ϑ is the set of all primes. Otherwise, $P_\vartheta = \{\, p \in \mathbb{Z} \mid p \text{ prime and } p \text{ divides } k \,\}$. If ϑ is of the form $\neg\vartheta_1$, then we can construct P_{ϑ_1} by the induction hypothesis, and P_ϑ is the complement of P_{ϑ_1} in the set of all primes, which has a finite representation. Similarly, if ϑ is of the form $\vartheta_1 \wedge \vartheta_2$ or $\vartheta_1 \vee \vartheta_2$, then we apply the induction hypothesis to ϑ_1 and ϑ_2 and compute $P_\vartheta = P_{\vartheta_1} \cap P_{\vartheta_2}$ or $P_\vartheta = P_{\vartheta_1} \cup P_{\vartheta_2}$, respectively. □

Corollary 9.15 (Completeness and decidability results for subclasses of *ACF*)**.**

(i) The class ACF_p is complete and decidable for each prime p.

(ii) The class ACF_0 is complete and decidable.

Proof. Both parts are direct applications of parts (ii) and (iii) of Theorem 9.14, respectively. □

Corollary 9.16. *The class ACF is decidable but not complete.*

Proof. Let ϑ be an $\mathcal{L}_{Rings}$-sentence. Then $ACF \vDash \vartheta$ if and only if both $ACF_0 \vDash \vartheta$ and $ACF_p \vDash \vartheta$ for all primes p, if and only if P_ϑ in Theorem 9.14 is the set of all primes. Regarding completeness, consider the sentence $\vartheta = (1 + 1 = 0)$. Then $P_\vartheta = \{2\}$ and $P_{\neg\vartheta}$ is the complement $\{3, 5, \dots\}$ of $\{2\}$ in the set of all primes. Thus

$$ACF_2 \vDash \vartheta, \quad ACF_3 \nvDash \vartheta, \quad ACF_2 \nvDash \neg\vartheta, \quad ACF_3 \vDash \neg\vartheta, \tag{9.43}$$

and it follows that neither $ACF \vDash \vartheta$ nor $ACF \vDash \neg\vartheta$. □

Example 9.17 (Algebraically closed fields)**.** We start with some negative examples:

$$\mathbf{R} \notin ACF, \quad \mathbf{Q} \notin ACF, \quad \mathbf{Z}/p \notin ACF. \tag{9.44}$$

The field $\mathbf{R}$ of real numbers is not algebraically closed, because $x^2 + 1$ has no zero in $\mathbb{R}$. The same argument holds for $\mathbb{Q}$. The fields $\mathbf{Z}/p$ with p prime are finite and therefore not algebraically closed by Lemma 9.11. More explicitly, e.g., $\mathbb{Z}/2$ is not algebraically closed, because $x^2 + x + 1$ has no zero in $\mathbb{Z}/2$.

$$\mathbf{C}[[t]] \notin ACF, \quad \mathbf{C}((t)) \notin ACF. \tag{9.45}$$

The ring $\mathbf{C}[[t]]$ of formal power series over $\mathbb{C}$ is not a field. A formal power series $\sum_{k=0}^{\infty} a_k t^k$ with $a_k \in \mathbb{C}$ has a multiplicative inverse if and only if $a_0 \neq 0$. The field $\mathbf{C}((t))$ of formal Laurent series $\sum_{k=z}^{\infty} a_k t^k$ with $z \in \mathbb{Z}$ and $a_k \in \mathbb{C}$ is not algebraically closed, because $x^2 - t$ has no zero in $\mathbb{C}((t))$.

According to a more general result by Steinitz (1910), every field possesses an algebraically closed extension field. For instance,

$$\mathbf{R} \subsetneq \mathbf{C} \in ACF_0, \qquad \mathbf{Q} \subsetneq \overline{\mathbf{Q}} \in ACF_0, \quad \overline{\mathbb{Q}} = \{\, a + ib \in \mathbb{C} \mid a, b \in \mathbb{A} \,\}. \tag{9.46}$$

The *real algebraic numbers* $\mathbb{A} = \{\, a \in \mathbb{R} \mid \text{exists } f \in \mathbb{Z}[x] \text{ with } f(a) = 0 \,\}$ used in the definition of $\overline{\mathbb{Q}}$ form themselves a field, which is not algebraically closed. It is noteworthy that real algebraic numbers have finite representations on which the ring operations are effective. For every prime p, the field $\mathbf{Z}/p$ has an infinite algebraically closed extension field

$$\mathbf{Z}/p \subsetneq \overline{\mathbf{Z}/p} \in ACF_p. \tag{9.47}$$

The field $\mathbf{C}((t))$ of formal Laurent series over $\mathbb{C}$ has the field of Puiseux series over $\mathbb{C}$ as an algebraically closed extension field:

$$\mathbf{C}[[t]] \subsetneq \mathbf{C}((t)) \subsetneq \mathbf{C}\langle\langle t \rangle\rangle \in ACF_0, \qquad \mathbb{C}\langle\langle t \rangle\rangle = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \mathbb{C}((t^{1/n})). \tag{9.48}$$

More generally, $\mathbf{K}\langle\langle t \rangle\rangle \in ACF$ whenever $\mathbf{K} \in ACF$, and then $\operatorname{char}(\mathbf{K}\langle\langle t \rangle\rangle) = \operatorname{char}(\mathbf{K})$. In particular, $\overline{\mathbf{Z}/p}\,\langle\langle t \rangle\rangle \in ACF_p$ for every prime p. ⌟

The following *Lefshetz principle* has been extensively used and cited in algebraic geometry. It reflects a common strategy, proving over the complex numbers, exploiting convenient topological properties there, and transferring the results and proofs to other domains of interest. We deliberately state the principle in an informal style, outside our logical framework.

Corollary 9.18 (Lefshetz, 1953)**.** *Let ϑ be an elementary statement that holds in $\mathbb{C}$. Then ϑ holds in all algebraically closed fields of characteristic* 0*. Furthermore, ϑ holds in all algebraically closed fields of sufficiently large prime characteristic. Lower bounds on the required characteristic can be computed.* □

In his original work, Lefshetz did not make precise to which kind of statements his principle would be applicable. Tarski's results on quantifier elimination and completeness for algebraically closed fields, which we have presented here, show that the Lefshetz principle is applicable at least to $\mathcal{L}_{Rings}$-sentences. This has been remarked by Seidenberg (1958).

Index