Saint Petersburg State University

Mikhail R. Starchak

Quasi-Quantifier Elimination Algorithms and Definability Problems in Arithmetics with Divisibility

1.1.5. Mathematical logic, algebra, number theory and discrete mathematics

Thesis for the degree of
Candidate of Physical and Mathematical Sciences

Scientic supervisor:
Doctor of Physical and Mathematical Sciences
Tatiana M. Kosovskaya

St. Petersburg — 2022

Contents

Introduction

This thesis is primarily going to focus on the relationship between two important tools applied in theoretical computer science: quantifier elimination algorithms and the theorem on decidability of the existential theory of the natural numbers with unit, addition and divisibility. The questions of definability using the relations, which can be defined in terms of addition and divisibility of the integers, are directly related to these problems.

In the first chapter, we will introduce the notion of quasi-quantifier elimination (quasi-QE) algorithm, which is in some sense a generalization of quantifier elimination algorithm. Next, we construct two quasi-QE algorithms, which form a new decidability proof for the existential theory of the natural numbers with unit, addition and divisibility. The language of addition and divisibility is rather rich and difficult to study; in the second part of the thesis, a quasi-QE algorithm is also used to obtain results about definability in weaker structures. In the third chapter, from such questions of quasi-elimination we move towards some closely related definability problems.

0.1 Arithmetic of Addition and Divisibility and Quantifier Elimination Algorithms

Decidability of the positive existential theory of the natural numbers with unit, addition and divisibility was independently proved by A.P. Bel'tyukov [3] and L. Lipshitz [44] in 1976. In other words, there is an algorithm for satisfiability in the natural numbers of systems of the form $f_i(\overline{x}) \mid g_i(\overline{x})$ for every $i = 1..m$, where $\overline{x} = x_1...x_n$ and $f_i(\overline{x})$, $g_i(\overline{x})$ are linear polynomials with non-negative integer coefficients. It is not difficult to show that this problem is inter-reducible with the problem of satisfiability in the integers of systems of linear inequalities and divisibilities of linear polynomials with integer coefficients. From a logical point-of-view this means that the positive existential theory (P$\exists$Th) of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ is decidable. Here, the word «positive» means that we do not have indivisibilities in our systems. To avoid this restriction, we introduce new variables in order to rewrite every indivisibility via the formula

$$x \nmid y \Leftrightarrow (x = 0 \wedge 1 \leqslant |y|) \vee \exists z (1 \leqslant z \wedge z \leqslant |x| - 1 \wedge x \mid y + z). \tag{1}$$

It is now only left to express $x = 0$ and the absolute values of y and x using the other symbols of the signature.

Let us mention another way to reformulate the theorem of Bel'tyukov and Lipshitz (the BL-Theorem). Let the ternary relation GCD(x,y) = z be the graph of the GCD function over the integers such that GCD(0,0) = 0. Then $x \mid y \Leftrightarrow$ GCD(x,y) = $x \vee$ GCD(x,y) = $-x$. On the other

hand, from Euclid's algorithm, we obtain the following existential definitions:

$$\begin{aligned} \mathrm{GCD}(x,y) = z \;&\Leftrightarrow\; 0 \leqslant z \wedge z \mid x \wedge z \mid y \wedge \exists u\,(x \mid u \wedge y \mid u + z) \\ \neg\mathrm{GCD}(x,y) = z \;&\Leftrightarrow\; z + 1 \leqslant 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v\,(v \mid x \wedge v \mid y \wedge z + 1 \leqslant v)\,. \end{aligned} \tag{2}$$

Hence, whether we deal with the divisibility relation or the ternary relation GCD, the corresponding decision problems are inter-reducible. Exactly in this form, by considering the relation GCD instead of the divisibility, the BL-Theorem was proved by V.I. Mart'yanov [50] a year after the appearance of the original proofs. In the following we will call each of the considered reformulations as the BL-Theorem; which particular variation we are talking about will be easy to determine from the context.

The appearance of this theorem was preceded by the proof of the undecidability of the Hilbert's tenth problem, which was obtained in the works by M. Davis, H. Putnam, J. Robinson and Yu.V. Matiyasevich [51; 52] (the DPRM-Theorem). N.K. Kosovskii [37] showed in 1974 that this problem is reducible to the question of solvability in the natural numbers of systems of linear divisibilities and expressions of the form $T(f(\overline{x}),g(\overline{x}))$, where T is some predicate of fixed-power growth and $f(\overline{x})$, $g(\overline{x})$ are linear polynomials with natural coefficients. More formally, we can say that he proved undecidability of the theory $\exists\mathrm{Th}\langle\mathbb{N}; 1, +\,, \mid, T\rangle$. Now we see that the BL-Theorem gives us a negative answer to the question of whether the problem is still undecidable if we exclude T from the signature.

A number of problems of theoretical computer science were shown to be decidable by a reduction to the decision problem for $\exists\mathrm{Th}\langle\mathbb{N}; 1, +\,, |\rangle$, while the DPRM-Theorem often serves the opposite purpose, namely, to prove undecidability. For example, in 1996, A. Degtyarev, Yu.V. Matiyasevich and A. Voronkov [19] showed decidability of the problem of simultaneous rigid E-unification for the language with a signature containing one unary function symbol and a countable number of constants. Almost at the same time, A. Degtyarev and A. Voronkov [20] proved undecidability of the general problem of simultaneous rigid E-unification. In 2009, C. Haase, S. Kreutzer, J. Ouaknine, and J. Worrell [60] applied the BL-Theorem to prove decidability of reachability problem for parametric one-counter automata. In the same year, M. Bozga, R. Iosif and Y. Lakhnech [9] used the DPRM-Theorem in their undecidability proof of the reachability problem for flat parametric counter automata. In this sense, the BL-Theorem and the DPRM-Theorem complement each other.

In fact, for the decidable problems from the previous paragraph there is also an inverse reduction to the decision problem for $\exists\mathrm{Th}\langle\mathbb{N}; 1, +\,, |\rangle$. Moreover, the reductions in both directions can be performed in non-deterministic polynomial time (see [42]). A. Lechner, J. Ouaknine, and J. Worrell [43] showed in 2015 that every such problem is NP-hard and in **NEXPTIME**, however, a more precise characterization of time-complexity is not known. The upper complexity bound was obtained as a result of a number of improvements to Lipshitz's algorithm, which made the decision procedure similar to the algorithm of V.I. Mart'yanov. Thus, there are only four essentially similar presentations of the algorithm for $\exists\mathrm{Th}\langle\mathbb{N}; 1, +\,, |\rangle$. A. Lechner and co-authors remark that „[...] the considerable mathematical depth and intricacy of Lipshitz's proof, making it diffcult to read and understand [...]“, and that this leads to multiple mistakes concerning L. Lipshitz's results from [45].

The main idea of all known proofs can be briefly described as follows. For a given system of linear inequalities and divisibilities $\varpi(x_1,...,x_n)$, we construct a disjunction of systems of divisibilities $\varpi_i(x_1,...,x_n)$ of a special form, such that this disjunction is satisfiable in $\mathbb{Z}$ if and only if $\varpi(x_1,...,x_n)$ is satisfiable. For every $\varpi_i(x_1,...,x_n)$, according to the structure of the formula, we can constructively find a constant ν_i such that $\varpi_i(x_1,...,x_n)$ is satisfiable in the integers if and only if it is satisfiable in the p-adic integers $\mathbb{Z}_p$ for every prime $p \leqslant \nu_i$. The decidability result now follows from the decidability of $\exists\mathrm{Th}\langle\mathbb{Q}_p; 1, +, -, =, \mathrm{div}\rangle$ for the relation $\alpha \text{ div } \beta \rightleftharpoons v_p(\alpha) \leqslant v_p(\beta)$, where $v_p(x)$ is the greatest power of p that divides x.

Decidability of the latter theory can be proved via the quantifier elimination (QE) algorithms of V. Weispfenning [83] or T. Sturm [78]. For every formula of the form $\exists x\varphi(x,\overline{y})$, where $\varphi(x,\overline{y})$ is quantifier-free, such algorithms construct an equivalent (in a given structure) quantifier-free formula $\varphi(\overline{y})$ of the same language. Note that in the same paper Weispfenning used his QE algorithms to study complexity of the decision problem for $\exists\mathrm{Th}\langle\mathbb{Q}_p; 1, +, -, =, \mathrm{div}\rangle$ and proved that this problem is NP-hard and is in **EXPTIME**. He also conjectured that the problem is actually in **NP**; in 2019, F. Guépin, C. Haase and J. Worrell [28] answered this question in the affirmative by using an automata-theoretic approach. Another work that should be mentioned in this context is recent result of C. Haase and A. Mansutti [31]. They treat p as a parameter, and prove that the problem of deciding whether a given existential formula is satisfiable *for some* $p \geqslant 2$ is in **NEXPTIME** and the analogous question *for every* $p \geqslant 2$ is in **co-NEXPTIME**.

Arithmetical theories offer a convenient language for describing the properties of a wide range of objects, see e.g. [79], and quantifier elimination is a standard approach when we consider definability and decidability problems for these theories. Quantifier elimination algorithms were implemented in such packages as RedLog [22] for computer algebra system REDUCE or SyNRAC [34] for Maple. The main examples of theories with QE algorithms are the arithmetic of the natural numbers with unit, addition and equality, which is also called Presburger arithmetic, as well as the arithmetic of the reals with addition and order. Properties of a given object are described by using some formulas of the corresponding signatures, and then the satisfiability of these formulas is verified using QE algorithms, such as Cooper's algorithm [18] for the linear integer arithmetic and Loos-Weispfenning quantifier elimination [48] for the linear arithmetic over the reals, see e.g. [55] and [80]. Clearly, the crucial thing in such algorithms is the size of the formula obtained as a result of elimination.

Quantifier elimination approach is also applied to study decidable extensions of Presburger arithmetic. A significant contribution to the development of this field was made by A.L. Semënov [69]. In particular, he proved decidability of the elementary theory of the structure $\langle\mathbb{N}; 1, +, P_2, =\rangle$, where $P_2(x) \Leftrightarrow \exists y(x = 2^y)$, and even more general $\mathrm{Th}\langle\mathbb{N}; 1, +, 2^x, =\rangle$ is also decidable. These results were obtained using a quantifier elimination approach; a detailed presentation of QE algorithm for deciding formulas of $\mathrm{Th}\langle\mathbb{N}; 1, +, 2^x, =\rangle$ is given in the preprint [58] by F. Point. Regarding these results, it is natural to ask whether we can generalize the BL-Theorem by including in the signature P_2 or 2^x? The negative answer to the second question follows from the theorem of Kosovskii mentioned above; while decidability of the existential theory of the natural numbers with unit, addition, divisibility, and the relation P_2

remains an important open problem [71]. If we intend to find such kinds of generalizations of the BL-Theorem, it is useful to have an algorithm for $\exists\mathrm{Th}\langle\mathbb{N};1,+,\perp\rangle$. Decidability of this theory is a straightforward consequence from the BL-Theorem (this statement was explicitly formulated and proved A. Woods [85, Chapter 2, Corollary 1.6]), however, it does not seem an easy task to extract this case from the proofs of the BL-Theorem.

In 1999, V. Weispfenning [84] considered a natural generalization of linear programming and integer linear programming. He constructed a quantifier elimination algorithm for the structure $\langle\mathbb{R};1,+,-,[\,],\{c\cdot\}_{c\in\mathbb{Q}},=,<\rangle$, where $[\,]$ corresponds to the integer part operation over the reals, and unary function symbols $c\cdot$ are introduced for multiplication by rational constants c. Additionally, for the integer divisibility relation $x \mid y \rightleftharpoons \exists z(y = x\cdot z \wedge z \in \mathbb{Z})$ he proved undecidability of the theory $\mathrm{Th}\langle\mathbb{R};1,+,-,[\,],=,<,|\rangle$ and asked whether the positive existential theory of this structure is decidable. This result could be a generalization of the BL-Theorem, since the relation «to be an integer» can be defined, for example using the formula $x = [x]$.

0.2 Generalizations of the BL-Theorem and Definability Problems

Another line of research on finding generalizations of the BL-Theorem could be the usage of different quantifiers. However, already the set of all true in the natural numbers formulas of the language with the signature $\langle 1,+,|\rangle$ and quantifier prefix of the form $\exists...\exists\forall$ was shown to be undecidable by L. Lipshitz [45]. This result is a straightforward combination of the DPRM-Theorem and the following formula for the graph of squaring function:

$$y = x^2 \Leftrightarrow x \mid y \wedge x+1 \mid x+y \wedge \forall z(x \mid z \wedge x+1 \mid x+z \Rightarrow x+y \mid x+z). \tag{3}$$

Therefore, already $\exists\forall$- and $\forall\exists$-theories of the structures $\langle\mathbb{N};1,+,|\rangle$ and $\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ are undecidable. In this sense, M. Bozga and R. Iosif [8, p. 126] remark that the BL-Theorem „[...] remains one of the strongest decidability results in integer arithmetic [...]“.

However, in various formal verification problems we need to decide over the integers the truth of formulas with such quantifier prefixes, but also with some restrictions on the expressions under the quantifiers. In another paper [7], M. Bozga and R. Iosif introduced a family of positive $\exists\forall$-formulas with order and divisibility, where each linear divisibility has the form $f(\overline{x}) \mid g(\overline{x},\overline{y})$, and the variables $\overline{x}$ are existentially quantified, while the variables $\overline{y}$ are from the block of universal quantifiers. After they sketch a proof of the decidability for this family of formulas, this result is used to prove decidability of some verification problems concerning programs with lists.

A. Lechner [41] relies on the decidability of this fragment of arithmetic of the integers with addition, order and divisibility to investigate decidability and complexity of the linear temporal logic (LTL) synthesis problem for parametric one-counter automata. This work uses the way of expressing the reachability property for parametric one-counter automata in terms of addition and divisibility of the integers from the paper by C. Haase *et al.* [60]. However, as A. Lechner remarks in her thesis [42], there is a gap in the proof of decidability by M. Bozga and R. Iosif [7]. Recent

preprint of G.A. Pérez and R. Raha [57] is devoted to correction of this proof and improving the Lechner's results. They define a more restricted class of formulas such that the problem of deciding these formulas in the integers becomes decidable. This fragment is still sufficient to express various synthesis problems for parametric one-counter automata.

Therefore, we have an important problem of determining as wide as possible decidable fragments of $\exists\forall$-theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. On the other hand, it is desirable to have a suitable description of the relations, which can be defined by using such formulas. These descriptions might be helpful in order to show that some relations are *not* definable. For example, M. Bozga and R. Iosif [7, Remark 2] remark, that it is not clear whether the order relation $x \leqslant y$ is existentially definable ($\exists$-definable) in $\langle \mathbb{Z}; 1, +, -, | \rangle$. Formula (3) immediately yields $\exists$-definability of $y \neq x^2$ is in the structure $\langle \mathbb{N}; 1, +, | \rangle$, but this is not the case for $y = x^2$. In view of this definition, L. van den Dries and A. Wilkie [23] ask whether the relation $\neg Sq$ «not to be a square of a natural number» is $\exists$-definable.

Regarding formula (1), we can ask whether the negation of coprimeness is positively existentially definable (P$\exists$-definable) in $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$ and whether we can show that it is not P$\exists$-definable if we exclude the order relation from the signature. It is fair to say that existentially definable relations in similar structures are not rather well understood. In the paper [45], L. Lipshitz provides some examples of $\exists$-definable predicates for the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$, in particular formula (2). Moreover, he shows that every set $S \subseteq \mathbb{N}$, which is $\exists$-definable in this structure, is a union of some finite set and (possibly empty or infinite) union of arithmetic progressions. For the same structure, L. van den Dries and A. Wilkie [23] studied growth properties of functions whose graphs were $\exists$-definable.

Quantifier elimination algorithms give us a description of the relations, definable in some structure by arbitrary formulas, as a class of the relations, which are quantifier-free definable in some extension of this structure. From the classical Presburger's theorem [59] (see also [30]) we know that every relation is definable in the structure $\langle \mathbb{Z}; 1, +, -, \leqslant \rangle$ if and only if it is quantifier-free definable in the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, 2 \mid, 3 \mid, 4 \mid, \ldots \rangle$, where the unary predicate symbols $d \mid$ stand for the divisibilities by fixed integers $d \geqslant 2$. V. Weispfenning [84] proved that the sets, which are definable in the structure $\langle \mathbb{Q}; 1, +, -, =, <, Int \rangle$, where Int is a unary predicate symbol for the property «to be an integer», are exactly the sets, which are quantifier-free definable in $\langle \mathbb{Q}; 1, +, -, [\,], \{c\cdot\}_{c\in\mathbb{Q}}, =, < \rangle$.

It is important to mention that in all these cases it is sufficient to construct a positive quantifier-free formula $\psi(\overline{y})$, which is equivalent in the corresponding structure to a given positive existential formula (P$\exists$-formula) $\exists x \varphi(x, \overline{y})$, since every negated atomic formula could be defined by some positive quantifier-free formula. As a corollary, we obtain decidability of the elementary theories of these structures. On the other hand, D. Richard [61] and A. Woods [85] independently proved undecidability already for the elementary theory of the structure $\langle \mathbb{N}; S, \perp \rangle$, where we have the successor function $Sx = x + 1$ instead of addition, and divisibility is replaced by the coprimeness relation. For the arithmetic of the integers, D. Richard later proved [63] undecidability of $\mathrm{Th}\langle \mathbb{Z}; 1, +, \perp \rangle$. Thus, the BL-Theorem implies that for such kind of structures a straightforward manner of characterization of the $\exists$-definable relations using QE algorithms is not possible. This

follows from the fact that such QE algorithm would give us a decision procedure for the elementary theory.

A possible solution to this problem for any of the structures mentioned above, can be described as follows. We first extend the signature of a given structure with some P$\exists$-definable relations; next, for the resulting structure, we construct an algorithm assigning to every positive formula $\exists x \varphi(x,\overline{y})$ an equivalent positive quantifier-free formula $\psi(\overline{y})$. Note that the extended signature must contain a predicate symbol for the relation whose negation is not P$\exists$-definable, since otherwise our algorithm becomes a quantifier elimination algorithm, and this implies decidability of the corresponding elementary theory. An example of a relation with this property is $y \neq x^2$: formulas (1) and (3) imply that it is positively existentially definable in $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$, while the negation of this relation is not P$\exists$-definable.

0.3 Completeness with Respect to Definability

The last statement of the previous paragraph is just an easy corollary from the BL-Theorem and the DPRM-Theorem since we have the following elementary fact: $z = x \cdot y \Leftrightarrow (x+y)^2 = x^2 + y^2 + 2z$. Note that in the proof of the undecidability of $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, |, T \rangle$, N.K. Kosovskii [37] exactly defines the graph of squaring $y = x^2$ using some quantifier-free formula. On the other hand, it is not difficult to show that the graph of addition is quantifier-free definable in the structure $\langle \mathbb{N}; 0, S, \cdot, = \rangle$.

Similar results are important for the following reason. It is often more convenient to prove the algorithmic undecidability of a certain problem via a reduction from the decision problem for a theory with possibly stronger restrictions on the form of formulas. Thus, the main difficulty in proving undecidability is transferred to an essentially purely number-theoretic problem. As an example, we can consider the undecidability proof for the family of formulas, defined by M. Bozga and R. Iosif [7; 57], by using the theory $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, \mathrm{LCM} \rangle$, where LCM corresponds to the least common multiple function. Such definability and decidability questions are included in the context of research on the so-called weak arithmetics [64].

A systematic research of definability problems in weak arithmetics was initiated by J. Robinson [65] in 1949. She proved that every arithmetical relation (that is, definable in the structure $\langle \mathbb{N}; +, \cdot, = \rangle$) is definable in the structure $\langle \mathbb{N}; S, | \rangle$. In order to more easily formulate the fact that this property holds, the structures that have the specified property were called by I. Korec [36] as *complete with respect to definability* (Def-complete). In a similar vein one can introduce the notion of $\exists$Def-completeness for the structures $\langle \mathbb{N}; \sigma \rangle$, where the graphs of addition and multiplication are *existentially* definable. Here, the predicate symbols and graphs of the function symbols from σ correspond to some enumerable relations over $\mathbb{N}$.

Formula (3) allows us to prove Def-completeness of the structure $\langle \mathbb{N}; 1, +, | \rangle$. This result is «weaker» than theorem by J. Robinson, since in this structure the relation $y = Sx$ is obviously definable, while it does not seem a trivial task to define the graph of addition in the structure

$\langle \mathbb{N}; S, | \rangle$. Similarly, the coprimeness relation is «weaker» than divisibility, since definitions (2) imply that $\perp$ and its negation are (already) existentially definable in the structure $\langle \mathbb{N}; S, | \rangle$. In view of these definitions, J. Robinson asks whether the structure $\langle \mathbb{N}; S, \perp \rangle$, or at least $\langle \mathbb{N}; 1, +, \perp \rangle$ are Def-complete. A positive answer to the second question was obtained by A. Woods [85] who provided two different proofs of this fact. In addition, notice that in order to prove undecidability of the elementary theory of the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$, D. Richard [63] shows definability of the order relation. However, Def-completeness of the first structure remains an open problem closely related to the so-called Woods-Erdös conjecture (see an overview of the main results of A. Woods by P. Cégielski and D. Richard [17]).

Def-completeness of a structure implies undecidability of its elementary theory. In the case where it is difficult to prove Def-completeness, it is sometimes possible to define a sub-structure, which is isomorphic to some Def-complete. Using this technique, the undecidability proof for the theory $\mathrm{Th}\langle \mathbb{N}; S, \perp \rangle$ was independently obtained by A. Woods [85] and D. Richard [61]; moreover, they constructed different substructures isomorphic to $\langle \mathbb{N}; +, \cdot \rangle$. In the paper by P. Cégielski, Yu.V. Matiyasevich and D. Richard [16] it was introduced a special concept of *structure with isomorphic reinterpretation property*, and they also presented an example of a structure with isomorphic reinterpretation property, which is not Def-complete.

Now consider some properties of formulas with the successor function and divisibility. The **NEXPTIME** upper bound on the complexity of the decision problem for $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, | \rangle$ was obtained by A. Lechner, J. Ouaknine, and J. Worrell [43] as a direct consequence of the following fact: for every system of linear divisibilities, satisfiable over $\mathbb{N}$, there is an assignment with binary length bounded exponentially in the size of the system assuming binary encoding of the coefficients from linear divisibilities. On the other hand, they proposed a simple example demonstrating that the upper bound on the size of the smallest satisfying assignment cannot be improved. Every solution to the system

$$\bigwedge_{i=1}^{m} x_{i-1} \mid x_i \wedge Sx_{i-1} \mid x_i \wedge x_i \mid Sx_{m+1} \tag{4}$$

satisfies the following inequalities: $x_0 \geqslant 1$, $x_1 \geqslant x_0^2 + x_0 \geqslant 2$, ..., $x_m \geqslant x_{m-1}^2 + x_{m-1} \geqslant 2^{2^{m-1}}$. Therefore, the binary length of x_m is at least 2^{m-1}. In this formula we used the successor function instead of addition in order to show that a similar fact already holds for the theory $\exists\mathrm{Th}\langle \mathbb{N}; S, | \rangle$.

I. Korec [36] classified most of the Def-complete structures known at the time (2001), among them there were also very exotic ones. If we introduce the relation of divisibility by two consecutive numbers

$$x \,{}^{S}|\, y \rightleftharpoons x \mid y \wedge x+1 \mid y, \tag{5}$$

then the formula (3) almost immediately yields Def-completeness of the structure $\langle \mathbb{N}; +, {}^{S}| \rangle$, since

$$x \mid y \wedge x+1 \mid x+y \Leftrightarrow x \,{}^{S}|\, x+y.$$

This relation is also the basis of example (4). It is interesting to study definability and decidability questions for ${}^{S}|$ since this relation combines the successor function and divisibility. Also notice that there are no examples of relations similar to ${}^{S}|$ in the classification by I. Korec.

0.4 Goals and Main Results of the Thesis

Our **main goal** in this thesis is to introduce new concepts and techniques in order to improve the quality of understanding of the proof of the Bel'tyukov-Lipshitz theorem. We aim to obtain some definability and decidability results for the related structures and also further generalizations of this theorem. To achieve these goals we had to solve the following **problems**:

1. Construct a new decidability proof for the existential theory of the structure $\langle \mathbb{N}; 1, +, | \rangle$, different from the proofs by A.P. Bel'tyukov, L. Lipshitz and V.I. Mart'yanov and in a similar spirit to the process of quantifier elimination. This new decision procedure must be convenient enough to give us a possibility to easily extract the decision procedures for the existential theories of weaker structures, in particular for $\langle \mathbb{N}; 1, +, \perp \rangle$.
2. Give examples of some structures with decidable (due to the BL-Theorem) existential theories and undecidable elementary theories such that for these structures we can describe all P$\exists$-definable relations by applying a method similar to quantifier elimination.
3. Study some definability, Def-completeness, and $\exists$Def-completeness questions for the structures with the relation of divisibility by two consecutive integers $x \overset{S}{|} y \rightleftharpoons x(x+1) \mid y$.

Scientific novelty. Presented results are new and were obtained independently by the author. This thesis makes the following novel **contributions**:

1. Introduced the notion of a quasi-quantifier (quasi-QE) algorithm close to the notion of quantifier elimination algorithm. Then we construct in terms of quasi-elimination a new proof of decidability of the existential theory of the natural numbers with unit, addition and divisibility.
2. A quasi-QE algorithm is constructed for the existential theory of the natural numbers with unit, addition and coprimeness as well as for the simpler positive case.
3. Proved the matching of the following two classes of relations: positively existentially definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$ and positively quantifier-free definable in the structure $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \ldots \rangle$, where $\mathrm{GCD}_d(x,y) \rightleftharpoons \mathrm{GCD}(x,y) = d$. As a corollary, we obtain that the dis-coprimeness relation $\not\perp$ is not P$\exists$-definable in $\langle \mathbb{Z}; 1, +, \perp \rangle$. The result was obtained using a quasi-QE algorithm.
4. Two fragments of the $\forall\exists$-theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ are proved decidable. In particular, we construct an algorithm for deciding over the integers formulas of the form

$$\forall\, \overline{x}\, \exists\, \overline{y} \bigvee_{j \in J} \Big(\overline{y} \geqslant 0 \wedge \varphi_j(\overline{x}) \wedge \bigwedge_{i \in I_j} \left(\mathrm{GCD}(f_i(\overline{x}), g_i(\overline{x},\overline{y})) = h_i(\overline{x}) \wedge f_i(\overline{x}) > 0 \wedge h_i(\overline{x}) > 0 \right) \Big).$$

   Here, $f_i(\overline{x})$, $g_i(\overline{x},\overline{y})$, $h_i(\overline{x})$ are linear polynomials with integer coefficients, and $\varphi_j(\overline{x})$ are systems of linear inequalities and divisibilities. This is a generalization of a recent result by G.A. Pérez and R. Raha [57].
5. Existential theory of the structure $\langle \mathbb{R}; 1, +, -, [\,], =, <, | \rangle$ is decidable. This gives a positive answer to one V. Weispfenning's question [84, Remark, p.135].

6. The structures $\langle \mathbb{N}; {}^{S}|, | \rangle$ and $\langle \mathbb{N}; S, 2^x, {}^{S}| \rangle$ are Def-complete; we also prove undecidability of the theory $\mathrm{Th}\langle \mathbb{N}; <, {}^{S}|, P_2 \rangle$. Next, the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$ was shown to be $\exists$Def-complete, and thus the existential theory of this structure is undecidable.

Methodology and research methods. In this work we use quantifier elimination techniques, elementary methods of number theory, weak arithmetics, linear algebra, theory of computation and graph theory.

The algorithm for $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, | \rangle$, which is constructed in the first chapter, has two stages. We have two corresponding variations of quasi-QE algorithms for these stages. The first one reduces the decision problem for the existential theory of the structure $\langle \mathbb{Z}; 0,1, +, -, \leqslant, \mathrm{GCD} \rangle$ to the decision problem for the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a \in \mathbb{Z}_{>0}}, \mathrm{GCD} \rangle$, where $a\cdot$ is a unary function symbol for multiplication by some fixed positive integer a. The second quasi-QE algorithm yields decidability of the latter theory. The transformations of formulas are based on a generalization of the Chinese remainder theorem to systems of the form $\bigwedge_{i \in [1..m]} \mathrm{GCD}(a_i, b_i + x) = d_i$, where a_i, b_i, d_i are some integers such that $a_i \neq 0$, $d_i > 0$ for every $i \in [1..m]$. This proposition is an elementary result of modular arithmetic and will be called GCD-Lemma. In the first algorithm, the step of variable isolation uses one lemma by J. von zur Gathen and M. Siefking [26]; L. Lipshitz [44, Lemma 1] also applies an analogous statement. The second algorithm does not use this lemma; for every given formula we construct an oriented graph in which we detect and eliminate cycles.

GCD-Lemma is a key tool used for describing the relations, which are P$\exists$-definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$. The fact that dis-coprimeness $x \not\perp y$ is not P$\exists$-definable now follows from the main theorem of Chapter 2 and from the undecidability result by D. Richard [63] for the elementary theory of this structure. We prove decidability of $\exists\mathrm{Th}\langle \mathbb{R}; 0,1, +, -, [\,], =, <, | \rangle$ by reduction to the decidable $\exists$-theory of the structure with the same signature but with the set of rational numbers $\mathbb{Q}$ as a domain.

The third chapter deals with classical concepts and techniques for proving Def-completeness and $\exists$Def-completeness of arithmetic structures. Def-completness of $\langle \mathbb{N}; |\ , {}^{S}| \rangle$ follows from the definability in this structure of the graph of the successor function S and theorem of J. Robinson [65] on Def-completeness of $\langle \mathbb{N}; S, | \rangle$. In order to prove $\exists$Def-completeness of $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$, we show existential definability of the graph of the successor function and then use quantifier-free definability of addition in terms of S and multiplication. Undecidability of the $\exists$-theory of this structure now follows from the DPRM-Theorem. By combining the result of D. Richard [62] on Def-completeness of the structure $\langle \mathbb{N}; S, 2^x, \perp \rangle$ and definability of the coprimeness relation, we obtain Def-completeness of $\langle \mathbb{N}; S, 2^x, {}^{S}| \rangle$. Undecidability proof for the theory $\mathrm{Th}\langle \mathbb{N}; <, {}^{S}|, P_2 \rangle$ is carried out by proving the existence of a substructure isomorphic to the Def-complete structure $\langle \mathbb{N}; <, | \rangle$.

Theoretical and practical applications. We may note the following areas of applications of the results of the thesis.

In a recent preprint by G.A. Pérez and R. Raha [57] it is shown that there is a gap in the proof of a generalization of the BL-Theorem obtained by I. Bozga and R. Iosif [7]; in fact, a somewhat more restricted fragment of $\forall\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ turns out to be decidable. These

kinds of mistakes could be avoided if we had a formalized proof of the BL-Theorem obtained using interactive theorem provers, such as Isabelle, Coq or Lean. The construction of such proofs is an intensively developing area of research, which connects functional programming with proof theory. For example, in 2018, the process of proving the DPRM-Theorem was initiated in Isabelle [81], in the same year M. Carneiro [13] formalized the proof of Matiyasevich's theorem in Lean proof assistant, and in 2020 was announced [38] a complete formalization of the DPRM-Theorem in Coq. The proof of the BL-Theorem, proposed in the first chapter in terms of quasi-elimination, is probably more suitable for the purposes of formalization in interactive theorem provers, since it is based on the idea of quantifier elimination, familiar to specialists in such areas of theoretical computer science as symbolic computation and formal verification.

On the other hand, the very concept of *quasi-quantifier elimination* may be useful in attempts to further generalize this theorem, for example, to solve the problem of the possibility of adding the relation P_2 to the structure, preserving decidability. In addition, when studying the complexity of the decision problem for $\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leqslant, |\rangle$, it will be natural to try to prove that at least the weaker theory $\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leqslant, \perp\rangle$ is in **NP** (or **EXPTIME**). The quasi-QE algorithm, which is constructed for this theory in the second chapter, can contribute to solving of this question as well as to proving decidability of the existential theory of the structure $\langle\mathbb{Z}; 1, +, -, \leqslant, \perp, P_2\rangle$.

We have seen that the questions of existential definability in the structure $\langle\mathbb{Z}; 1, +, -, \leqslant, |\rangle$ admit various reformulations, and they often appear in research on algorithmic decidability of problems of theoretical computer science. At the same time, we do not have a satisfactory description of the relations $\exists$-definable in this structure. In any case, the author does not know the results similar to the description of all relations, P$\exists$-definable in $\langle\mathbb{Z}; 1, +, \perp\rangle$ from Chapter 2. This result can serve as a starting point of the search for descriptions of broader classes of P$\exists$-definable relations.

Talks. The main results of the thesis were presented at the following conferences:

1. International conference «Journées sur les Arithmétiques Faibles 37 (JAF37)», Florence, Italy, 29.05.2018;
2. Russian conference «SPISOK-2019», St. Petersburg State University, St. Petersburg, Russia, 25.04.2019;
3. Seminar «City seminar on Mathematical Logic», St. Petersburg, Russia, 31.05.2019;
4. International conference «Polynomial Computer Algebra 2020 (PCA 2020)», St. Petersburg, Russia, 12.10.2020;
5. International conference «International Symposium on Symbolic and Algebraic Computation 2021 (ISSAC'21)», St. Petersburg, Russia, 22.07.2021.
6. International conference «Journées sur les Arithmétiques Faibles 40 (JAF40)», Athens, Greece, 25.10.2021;

and were primarily presented in 4 **publications**, 1 of which is published in journals recommended by VAK [76], 3 — in scientific journals and in conference proceedings indexed by Web of Science or SCOPUS [74; 75; 77].

Structure of this work. The thesis consists of an introduction, 3 chapters and a conclusion. The first chapter combines the results from the papers [74] and [75]. Chapter 2 is based on the

paper [77], which was published in the proceedings of conference ISSAC'21, and is complemented by the results presented at the conference PCA'20. The third chapter is an extended version of the paper [76]. The thesis text consists of 88 pages. The list of references contains 85 items.

The author is grateful to his scientific supervisors N.K. Kosovskii and T.M. Kosovskaya for their attention, advices and support in this work for a long time. In addition, the author expresses his gratitude to anonymous reviewers of the papers on the topic of the thesis for very useful comments and advices, which contributed to a significant improvement of the quality of presentation.

Chapter 1. A Proof of Bel'tyukov–Lipshitz Theorem by quasi-Quantifier Elimination

> This is just the Chinese Remainder Theorem (see [M]). Of course g.c.d.(f_i,f_j) is not in our language so we have not actually eliminated x_n...
>
> L. Lipshitz [45] (1981)

In this chapter, we give a new proof of decidability of the existential theory of the natural numbers with unit, addition and divisibility. This theorem was independently proved by A.P. Bel'tyukov [3] and L. Lipshitz [44], and will be further referred to as the BL-Theorem. In order to prove this theorem in quantifier elimination spirit, we introduce the notion of quasi-quantifier elimination algorithm and then construct two such algorithms. At the beginning of the chapter, we recall some basic definitions, which will be used in this and subsequent chapters.

1.1 Existential Arithmetic of the Natural Numbers with Unit, Addition and Divisibility

1.1.1 Definitions and Examples

Let σ be some signature, and let M be some non-empty set. An assignment to every function symbol from σ some function over M and to every predicate symbol from σ some predicate over M of a corresponding arity is called an *interpretation of the signature* σ *over* M.

A *structure* is defined by a signature σ, a set M, and an interpretation of σ over M. The set M is called the *domain*, or the *base set* of the structure.

In this thesis, we will consider different signatures, however, the base set will be either the set of the natural numbers $\mathbb{N} = \{0,1,2,...\}$, the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, or the p-adic numbers $\mathbb{Q}_p$, and to every function and predicate symbol there will be assigned some naturally defined function and predicate. The structure of a signature σ with a domain M will be denoted by $\langle M; \sigma \rangle$.

The first-order language of a signature σ will be denoted by L_σ; a formula of the language $L \subseteq L_\sigma$ is an L-formula. A prenex L_σ-formula is a formula of the form $Q_1 y_1 ... Q_m y_m \varphi(x_1,...,x_n,y_1,...,y_m)$, where $\varphi(x_1,...,x_n,y_1,...,y_m)$ is a quantifier-free L_σ-formula, and Q_i are quantifiers. Grouping similar quantifiers into blocks, the formulas with a single existential block define the language $\exists L_\sigma$, and in the case of universal quantifiers, the language $\forall L_\sigma$. In a similar manner, we can define the languages $\forall\exists L_\sigma$, $\exists\forall L_\sigma$, etc. $\exists L_\sigma$-formulas are called *existential* and $\forall L_\sigma$-formulas — *universal* L_σ*-formulas.*

A quantifier-free formula is *positive*, if it is constructed from atomic formulas using only logical connectives of conjunction and disjunction. If in the definitions above the formula $\varphi(x_1,...,x_n,y_1,...,y_m)$ is positive, then we add prefix "P" to the notation of the corresponding languages, and the formulas of these languages will be called *positive*. For example, $\mathrm{P}\exists L_\sigma$ is the set of all positive existential L_σ-formulas.

Let φ be some L_σ-formula. We say that *«φ is true in M»* instead of «true in the structure $\langle M;\sigma\rangle$». The set of all closed L_σ-formulas, true in M, is called the *elementary theory of the structure* $\langle M;\sigma\rangle$ and denoted by $\mathrm{Th}\langle M;\sigma\rangle$. If we consider only existential L_σ-formulas, then we define the existential theory ($\exists$Th) and for the universal L_σ-formulas — the universal theory ($\forall$Th) of the structure $\langle M;\sigma\rangle$. In general, for every language $L \subseteq L_\sigma$ the set of all closed L-formulas, true in M, is, by definition, the *L-theory of the structure* $\langle M;\sigma\rangle$, denoted by $L\text{-}\mathrm{Th}\langle M;\sigma\rangle$. The *decision problem for some L-theory of the structure* $\langle M;\sigma\rangle$ is the problem of deciding formulas of this theory, i.e., of L-formulas, true in M.

In order to illustrate these notions consider different variations of the BL-Theorem that we mentioned in the introduction. First consider the structure $\langle \mathbb{N};1,+,|\rangle$, where the divisibility relation is defined by the formula $x \mid y \Leftrightarrow \exists z(y = z\cdot x)$. In particular, $0 \mid y \Leftrightarrow y = 0$.

It is clear that to prove decidability of $\mathrm{P}\exists\mathrm{Th}\langle \mathbb{N};1,+,|\rangle$ it is sufficient to construct an algorithm for satisfiability in the natural numbers of systems of the form

$$\bigwedge_{i\in[1..m]} f_i(\overline{x}) \mid g_i(\overline{x}), \tag{1.1}$$

where $\overline{x}$ is a list of variables $x_1,...,x_n$ and $f_i(\overline{x})$,$g_i(\overline{x})$ are linear polynomials $a_{i,0} + a_{i,1}x_1 + ... + a_{i,n}x_n$ with natural coefficients. By using distributive laws for conjunction and disjunction, we can transform any given $\mathrm{P}\exists L_{\langle 1,+,|\rangle}$-formula into a disjunction of systems of the form (1.1).

We can use Definition (1) and consider not only positive, but also arbitrary existential formulas. In every $\exists L_{\langle 1,+,|\rangle}$-formula push the negations inward and once more apply the distributive law. By introducing new variables, we can now rewrite indivisibilities in the resulting systems using the formula

$$x \nmid y \Leftrightarrow (x = 0 \wedge 1 \leqslant y) \vee \exists z(1 \leqslant z \wedge z \leqslant x-1 \wedge x \mid y+z), \tag{1.2}$$

where $x \leqslant y$ is, by definition, $\exists z(y = x+z)$ and $x = y \Leftrightarrow x \mid y \wedge y \mid x$. Note that the relation $x \leqslant y$ can be rewritten as $\exists z(x+z \mid y)$.

We can now show that for the structure $\langle \mathbb{Z};1,+,-,\leqslant,|\rangle$ the decision problem for $\mathrm{P}\exists$-theory is reducible to the decision problem for $\exists\mathrm{Th}\langle \mathbb{N};1,+,|\rangle$ and vice versa. The reduction from the integers to the natural numbers is obvious, since it is sufficient to add to a given formula $\varphi(x_1,...,x_n)$ the following system of inequalities $\bigwedge\limits_{i\in[1..n]} x_i \geqslant 0$.

For constructing a reduction in the other direction, replace every integer variable x_i by $x_i' - x_i''$, where x_i', x_i'' are new natural variables. We can now avoid using negative coefficients in linear polynomials. It is obvious for linear inequalities, and for linear divisibilities consider the following conjunction:

$$\varphi(\overline{x},\overline{y}) \wedge f(\overline{x}) - g(\overline{y}) \mid h(\overline{x},\overline{y}), \tag{1.3}$$

where $\varphi(\overline{x},\overline{y})$ is some system of linear inequalities and divisibilities, $h(\overline{x},\overline{y})$ is some linear polynomial with integer coefficients, $f(\overline{x})$ and $g(\overline{y})$ are linear polynomials with non-negative integer coefficients. Formula (1.3) is equivalent over the natural numbers to the following existential formula:

$$\varphi(\overline{x},\overline{y}) \wedge \exists z\,(z \mid h(\overline{x},\overline{y}) \wedge (f(\overline{x}) = g(\overline{y}) + z \vee f(\overline{x}) + z = g(\overline{y})))\,.$$

Continue this process for every linear polynomial which has some coefficients negative. It remains to rewrite inequalities and equations using divisibility in the same way as it is done above.

It is not difficult to see how we can use (1) to omit the positivity restriction in the case of the integers. Thus we obtain the following result.

Proposition 1.1.1. *The decision problems for the existential theories of the structures* $\langle \mathbb{N}; 1, +\,, |\rangle$ *and* $\langle \mathbb{Z}; 1, +\,, -\,, \leqslant\,, |\rangle$ *are inter-reducible.*

Before we consider relationships between the divisibility relation and GCD, let us formally define the notion of first-order definability.

For a language $L \subseteq L_\sigma$ we say that an n-ary relation R on M is *«L-definable in the structure* $\langle M; \sigma\rangle$*»* if and only if there exists an L-formula $\varphi(\overline{x})$ such that for every $\overline{a} \in M^n$ we have $R(\overline{a}) \Leftrightarrow \varphi(\overline{a})$. When L is one of the classes of formulas, defined using L_σ with prefixes "P", "$\exists$", "$\forall$", we can omit L in its notation. In particular, the relations, P$\exists L_\sigma$-definable in the structure $\langle M; \sigma\rangle$, will be called *positively existentially definable in the structure* $\langle M; \sigma\rangle$, or P$\exists$-definable. If the structure we are working in is clear from the context, we will just write L-theory and L-definable.

One year after the appearance of the original proofs, the BL-Theorem was proved by V. I. Mart'yanov [50]. He obtained an equivalent result by considering instead of divisibility the ternary predicate GCD such that $\mathrm{GCD}(x,y,z)$ is true if and only if $\pm z$ is the greatest common divisor of x and y. It seems more natural to use the GCD function, which computes the greatest common divisor (a non-negative integer) of two integers and is equal to zero if and only if both arguments are equal to zero. For the graph of this function $\mathrm{GCD}(x,y) = z$ we see that $x \mid y \Leftrightarrow \mathrm{GCD}(x,y) = x \vee \mathrm{GCD}(x,y) = -x$. Conversely, Euclidean algorithm implies that the relation GCD and its negation are $\exists$-definable in the structure $\langle \mathbb{Z}; 1, +\,, -\,, \leqslant\,, |\rangle$:

$$\begin{aligned} \mathrm{GCD}(x,y) = z \;&\Leftrightarrow\; 0 \leqslant z \wedge z \mid x \wedge z \mid y \wedge \exists u\,(x \mid u \wedge y \mid u + z) \\ \neg\mathrm{GCD}(x,y) = z \;&\Leftrightarrow\; z + 1 \leqslant 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v\,(v \mid x \wedge v \mid y \wedge z + 1 \leqslant v)\,. \end{aligned} \tag{1.4}$$

In the structures that we consider in the thesis GCD will be a ternary predicate symbol associated with the graph of the corresponding function. We can now generalize Proposition 1.1.1.

Proposition 1.1.2. *The decision problems for the existential theories of the following structures:* $\langle \mathbb{N}; 1, +\,, |\rangle$, $\langle \mathbb{N}; 1, +\,, \mathrm{GCD}\rangle$, $\langle \mathbb{Z}; 1, +\,, -\,, \leqslant\,, |\rangle$, *and* $\langle \mathbb{Z}; 1, +\,, -\,, \leqslant\,, \mathrm{GCD}\rangle$ *are inter-reducible.*

Constructing quantifier elimination algorithms is a classical approach when we study definability and decidability properties of arithmetic structures. A *quantifier elimination (QE) algorithm for the language* L_σ *in the structure* $\langle M; \sigma\rangle$ is an algorithm assigning to every L_σ-formula of the form $\exists x \varphi(x,y_1,\ldots,y_n)$, where $\varphi(x,y_1,\ldots,y_n)$ is quantifier-free, an equivalent in this structure

quantifier-free L_σ-formula $\psi(y_1,...,y_n)$. As a corollary, we see that by using a quantifier elimination algorithm, for every L_σ-formula we can construct an equivalent in the corresponding structure quantifier-free L_σ-formula. Note that the algorithm from this corollary is commonly called a quantifier elimination algorithm (see e.g. [30] or [83]), and its construction is reduced to a construction of a quantifier elimination algorithm in our terms. „As usual, it is sufficient to consider a formula with a single existential quantifier [...]“, — with this phrase N.K. Vereschagin and A. Shen [70] start their presentation of a QE algorithm for the first-order language of the signature $\sigma = \langle 0,1,+,\cdot,=,<\rangle$ in the structure $\langle \mathbb{R}; \sigma\rangle$.

In Subsection 1.2.3 this definition of QE algorithm will be generalized to the notion of quasi-quantifier elimination algorithms. In terms of quasi-elimination we will prove the following theorem.

Theorem 1 (A.P. Bel'tyukov [3], L. Lipshitz [44], V.I. Mart'yanov [50])**.** *The existential theory of the structure* $\langle \mathbb{Z}; 0,1,+,-,\leqslant,\mathrm{GCD}\rangle$ *is decidable.*

Note that $\neg\mathrm{GCD}(x,y) = z \Leftrightarrow \exists t\,(\mathrm{GCD}(x,y) = t \wedge t \neq z)$ for $t \neq z \Leftrightarrow t \leqslant z-1 \vee z+1 \leqslant t$ and, moreover, $\neg x \leqslant y \Leftrightarrow y+1 \leqslant x$. It will also be convenient to have in formulas separately equalities and inequalities represented in matrix form. Thus, introducing, if necessary, some new variables, we can reduce the general problem to the problem of satisfiability in $\mathbb{Z}$ of formulas of the form

$$\varphi(\overline{x}) \rightleftharpoons A\overline{x} = b \wedge C\overline{x} \geqslant d \wedge \bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{x}),g_i(\overline{x})) = h_i(\overline{x}), \tag{1.5}$$

where $\overline{x}$ is a list of variables $x_1,...,x_n$; $f_i(\overline{x})$, $g_i(\overline{x})$, $h_i(\overline{x})$ are linear polynomials with integer coefficients; A and C are integer matrices and b, d are some integer vectors. Expressions of the form $\mathrm{GCD}(f(\overline{x}),g(\overline{x})) = h(\overline{x})$ will be further called *gcd-expressions.*

1.1.2 Structure of the Chapter

This chapter is organised as follows. In Section 1.2, we introduce the notion of quasi-Quantifier Elimination (quasi-QE) algorithm, in some sense a generalization of Quantifier Elimination algorithm. Then we sketch the proof and construct two quasi-QE algorithms $\mathcal{R}$ and $\mathcal{D}$. The first one reduces the decision problem for the existential theory of the structure $\langle \mathbb{Z}; 0,1,+,-,\leqslant,\mathrm{GCD}\rangle$ to the decision problem for the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD}\rangle$, where $a\cdot$ is a unary function symbol for multiplication by a positive integer a. In Section 1.7, quasi-QE algorithm $\mathcal{D}$ gives a decidability proof for the latter theory. The main algorithm $\mathcal{R}$ is described in Sections 1.4 and 1.5. We then show in Section 1.6 that the resulting algorithm is actually a quasi-QE algorithm.

A.P. Bel'tyukov [4] remarks about the theorem, proved at the same time by L. Lipshits, that «in fact, our solution was a very deep generalization of the well-known Chinese remainder theorem...». After we give a sketch of the proof, in Section 1.3 we generalize the Chinese remainder

theorem to the systems $\bigwedge_{i\in[1..m]} \mathrm{GCD}(a_i,b_i+x) = d_i$, where a_i,b_i,d_i are some integers such that $a_i \neq 0$, $d_i > 0$ for all $i \in [1..m]$. This result will be the basic tool in transformations of formulas in quasi-QE algorithm $\mathcal{R}$. A special case of this generalization will be used in algorithm $\mathcal{D}$.

1.2 General Description of the Algorithm

1.2.1 LS-Lemma and Simple Transformations of Formulas

The problem of consistency in $\mathbb{Z}$ of system (1.5) will be reduced to satisfiability in the non-negative integers $\mathbb{N}$ of a disjunction of systems $\widetilde{\varphi}_j$. In each system $\widetilde{\varphi}_j$ there will be a variable $\widetilde{x}_j$ such that this variable appears only in gcd-expressions of the form $\mathrm{GCD}(f(\overline{z}),g(\overline{z})+c\widetilde{x}_j) = h(\overline{z})$ for a list of variables $\overline{z}$ not containing $\widetilde{x}_j$. These transformations can be performed using the following Linear Systems Lemma (LS-Lemma) taken in a weaker form from the paper by A. Lechner et al. [43, Theorem 3]. It was proved by J. von zur Gathen and M. Sieveking [26]; L. Lipshitz used an analogous statement (see [44, Lemma 1]).

Lemma 1.2.1 (Linear Systems Lemma (LS-Lemma) [44, Lemma 1] and [26] in a form similar to [43, Theorem 3])**.** *Let A be an $p\times n$ integer matrix of rank r and let C be a $q\times n$ integer matrix. Let b and d be integer vectors of size respectively p and q. Then we can constructively find a finite set of $n\times(n-r)$ integer matrices $E^{(j)}$ and $n\times 1$ vectors $u^{(i)}$ for $j\in J$ such that*

$$\{\overline{x}\in\mathbb{Z}^n \,:\, A\overline{x}=b\wedge C\overline{x}\geqslant d\} = \bigcup_{j\in J}\left\{E^{(j)}\overline{y}+u^{(j)} \,:\, \overline{y}\in\mathbb{N}^{n-r}\right\}.$$

Split the list $\overline{x}$ into two parts $\overline{s} = x_1,\ldots,x_l$ and $\overline{t} = x_{l+1},\ldots,x_n$, and let the system $A\overline{x}=b\wedge C\overline{x}\geqslant d$ be split into two subsystems: $S(\overline{s}) \rightleftharpoons A_1\overline{s}=b_1\wedge C_1\overline{s}\geqslant d_1$ and $T(\overline{x}) \rightleftharpoons A_2\overline{x}=b_2\wedge C_2\overline{x}\geqslant d_2$ with matrix A_1 of rank r_1. Then by *«application of LS-Lemma to the subsystem $S(\overline{s})$ of the formula $\varphi(\overline{x})$»* we assume the following. Suppose that we have already constructed integer matrices $E^{(j)}$ and vectors $u^{(j)}, j\in J$ for the system $S(\overline{s})$. Now construct a set of formulas $\{\psi_j\}_{j\in J}$, where

$$\psi_j(\overline{y},\overline{t}) \rightleftharpoons \widetilde{T}(\overline{y},\overline{t})\wedge\overline{y}\geqslant 0\wedge\bigwedge_{i\in[1..m]}\mathrm{GCD}(\widetilde{f}_{i,j}(\overline{y},\overline{t}),\widetilde{g}_{i,j}(\overline{y},\overline{t})) = \widetilde{h}_{i,j}(\overline{y},\overline{t}) \tag{1.6}$$

as a result of substitution $E^{(j)}\overline{y}+u^{(j)}$ for $\overline{s}$ in

$$T(\overline{s},\overline{t})\wedge\bigwedge_{i\in[1..m]}\mathrm{GCD}(f_i(\overline{s},\overline{t}),g_i(\overline{s},\overline{t})) = h_i(\overline{s},\overline{t}).$$

Thus, we have transformed $\varphi(\overline{x})$ into an equi-satisfiable over the integers disjunction $\bigvee_{j\in J}\psi_j(\overline{y},\overline{t})$ with r_1 fewer number of variables.

Applying LS-Lemma to the subsystem $\bigwedge\limits_{i\in[1..m]} h_i(\overline{x}) \geqslant 0 \wedge A\overline{x} = b \wedge C\overline{x} \geqslant d$ of the formula $\bigwedge\limits_{i\in[1..m]} h_i(\overline{x}) \geqslant 0 \wedge \varphi(\overline{x})$ (which is equi-satisfiable over $\mathbb{Z}$ with $\varphi(\overline{x})$), we obtain the following auxiliary lemma.

Lemma 1.2.2. *For every formula of the form (1.5) we can construct an equi-satisfiable over $\mathbb{Z}$ disjunction of formulas of the form*

$$\overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}), \tag{1.7}$$

where $\overline{y}$ is a list of variables $y_1,...,y_k$, $k \leqslant n$; $f_i(\overline{y}),g_i(\overline{y}),h_i(\overline{y})$ are linear polynomials with integer coefficients, and, moreover, the coefficients of $h_i(\overline{y})$ are non-negative.

We apply a similar approach in the step of variable isolation (i.e., when we construct formulas $\widetilde{\varphi}_j$) to obtain non-negative coefficients in linear polynomials using LS-Lemma. These transformations will be described in Section 1.4.

1.2.2 GCD-Lemma

By the Chinese remainder theorem we mean the theorem [67], which states that the system of divisibilities $\bigwedge\limits_{i\in[1..m]} d_i \mid b_i + x$ has an integer solution if and only if $\bigwedge\limits_{i,j\in[1..m]} \mathrm{GCD}(d_i,d_j) \mid b_i - b_j$. In Section 1.3 we prove the following generalization of the Chinese remainder theorem, which we use in Step 2 of quasi-elimination for the systems $\widetilde{\varphi}_j$. This step will be described in Section 1.5.

For every positive integer x and prime p let $v_p(x)$ be the p-valuation of x, i.e., the maximal k such that $p^k \mid x$. We also write $\mathrm{GCD}(x,y,z)$ for $\mathrm{GCD}(\mathrm{GCD}(x,y),z)$. Then for the system

$$\bigwedge_{i\in[1..m]} \mathrm{GCD}(a_i,b_i + x) = d_i, \tag{1.8}$$

we can prove the following lemma.

Lemma 1.2.3 (GCD-Lemma)**.** *For the system (1.8) with $a_i,b_i,d_i \in \mathbb{Z}$, $a_i \neq 0$, and $d_i > 0$ for every $i \in [1..m]$, we define for every prime p the integer $M_p = \max\limits_{i\in[1..m]} v_p(d_i)$ and the index sets $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ and $I_p = \{i \in J_p : v_p(a_i) > M_p\}$. Then (1.8) has a solution in $\mathbb{Z}$ if and only if the following conditions simultaneously hold:*

(i) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$

(ii) $\bigwedge\limits_{i,j\in[1..m]} \mathrm{GCD}(d_i,d_j) \mid b_i - b_j$

(iii) $\bigwedge\limits_{i,j\in[1..m]} \mathrm{GCD}(a_i,d_j,b_i - b_j) \mid d_i$

(iv) For every prime $p \leqslant m$ and every $I \subseteq I_p$ such that $|I| = p$ there are such $i,j \in I$, $i \neq j$ that $v_p(b_i - b_j) > M_p$.

Consider the subsystem $\widetilde{\varphi}_j$ with all the gcd-expressions with an isolated variable. It is not difficult to see that we can assume that the coefficients of this variable are all equal to one. This subsystem will be of the form (1.8), where there will be some linear polynomials with integer coefficients $f_i(\overline{z})$, $g_i(\overline{z})$, and $h_i(\overline{z})$ instead of a_i, b_i, and d_i, respectively. Application of GCD-Lemma will require introduction of new positive integer variables. For these variables we use the letters of the Greek alphabet, while for the variables introduced by LS-Lemma we use Latin letters. Greek variables will only appear in polynomials of the form $a\zeta$.

This idea can be illustrated via the following example of rewriting condition (ii). In this case, for each pair (i,j), for $1 \leqslant i < j \leqslant m$, we introduce a new variable $\zeta_{i,j}$, such that the corresponding divisibility can be rewritten as

$$\exists\zeta_{i,j}\,(\mathrm{GCD}(h_i(\overline{z}),h_j(\overline{z})) = \zeta_{i,j} \wedge \mathrm{GCD}(\zeta_{i,j},g_i(\overline{z}) - g_j(\overline{z})) = \zeta_{i,j})\,.$$

Lemmas 1.2.1 and 1.2.3 form two steps, which are repeatedly applied in order to obtain a disjunction of systems of gcd-expressions without occurrences of Latin variables. Thus, each linear polynomial will have the form either $a\zeta$ or a for some positive integer a. This reduction can be formalized using the notion of quasi-quantifier elimination algorithm.

1.2.3 Definition of quasi-Quantifier Elimination Algorithm

Let S_1 and S_2 be two disjoint sorts of variables. For the variables from S_1 we use Latin letters (and will be named «Latin variables») and Greek letters for the variables from S_2 («Greek variables»). Let $L_\sigma^{1,2}$ be the first-order language with the signature σ and variables from $S_1 \cup S_2$. Denote L_σ^1 and L_σ^2 the first-order languages with the signature σ and variables from S_1 and S_2, respectively.

Denote by $[\varphi]_t^x$ the result of substitution of term t for every free occurrences of the variable x in the formula φ. A set of formulas $L \subset L_\sigma$ is called *decidable* if there is an algorithm that determines whether a given formula is an L-formula.

Definition 1. *Let $\langle M;\sigma\rangle$ be some structure with a signature σ, and we have some decidable set of existential formulas $L \subset L_\sigma^{1,2}$ such that all occurrences of Latin variables are free and all occurrences of Greek variables are bound. Let also for some variable $x \in S_1$ be defined a decidable set $L^x \subseteq L$ of* ***L-formulas of elimination form*** *and are given the following two steps:*

Step 1. *Transformation of every L-formula $\exists\overline{\alpha}\varphi(\overline{y},\overline{\alpha})$ into an equi-satisfiable in $\langle M;\sigma\rangle$ disjunction $\bigvee\limits_{j\in J}\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})$ for some finite index set J and lists of Latin variables $\overline{y_j}$ such that for every $j \in J$ we have the following:*

1. *Every $\overline{y_j}$ for $j \in J$ comprises at most the same number of variables as $\overline{y}$.*
2. *If the list of variables $\overline{y_j}$ is non-empty, then there is a variable $\widetilde{x}_j \in \overline{y_j}$ such that $[\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})]_x^{\widetilde{x}_j} \in L^x$.*

Step 2. *Transformation of every formula* $\exists x \exists \overline{\alpha} \widetilde{\varphi}(x,\overline{z},\overline{\alpha})$*, where* $\exists \overline{\alpha} \widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ *is some* L^x*-formula, into an equivalent in the structure* $\langle M; \sigma \rangle$ *L-formula* $\exists \overline{\alpha} \exists \overline{\beta} \psi(\overline{z},\overline{\alpha},\overline{\beta})$*.*

Now $\mathcal{A}$ ***is a quasi-quantifier elimination algorithm (quasi-QE) for the language*** *L* ***in the structure*** $\langle M; \sigma \rangle$ *if for a given L-formula* $\exists \overline{\alpha} \varphi(y_1,...,y_k,\overline{\alpha})$ *it first applies Step 1 and then Step 2 to every formula* $\exists x \, [\exists \overline{\alpha} \widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})]_x^{\widetilde{x}_j}$*. Thus we construct an equi-satisfiable disjunction of L-formulas, where the number of Latin variables is less than k.*

The language L will be called ***the language of quasi-QE algorithm*** $\mathcal{A}$*.*

Consider some properties of a quasi-QE algorithm $\mathcal{A}$ for $L_{\mathcal{A}}$ in $\langle M; \sigma \rangle$.

For a subset L of quantifier-free L_σ-formulas define a language $\exists L$ as the set of formulas of the form $\exists \overline{x} \varphi(\overline{x},\overline{y})$ for every (quantifier-free) L-formula $\varphi(\overline{x},\overline{y})$. Denote by $E(L)$ the set of all closed $\exists L$-formulas.

The main purpose of $\mathcal{A}$ can be described as follows. Since $L_{\mathcal{A}} \cap L_\sigma^1$ comprises only quantifier-free L_σ-formulas, we can define $E(L_{\mathcal{A}} \cap L_\sigma^1)$, which will be denoted $L_{\mathcal{A}}^1$. Also let $L_{\mathcal{A}}^2 \rightleftharpoons L_{\mathcal{A}} \cap L_\sigma^2$. Then the algorithm $\mathcal{A}$ performs a reduction from the decision problem for $L_{\mathcal{A}}^1$-theory to the decision problem for $L_{\mathcal{A}}^2$-theory. Indeed, for every (quantifier-free) $(L_{\mathcal{A}} \cap L_\sigma^1)$-formula φ, by repeatedly applying algorithm $\mathcal{A}$ to every $L_{\mathcal{A}}$-formula of the resulting disjunctions, we construct a disjunction of (closed) $L_{\mathcal{A}}^2$-formulas. This disjunction is true in $\langle M; \sigma \rangle$ if and only if φ is satisfiable in this structure.

Consider three important variations of quasi-QE algorithms when $S_2 = \varnothing$. In this case, the definition implies that $L_{\mathcal{A}}$ is a subset of quantifier-free L_σ-formulas.

Example 1.2.1. *Let* S_2 *be the empty sort of variables and let the problem of validity of ground* L_σ*-formulas in* $\langle M; \sigma \rangle$ *be decidable. Then algorithm* $\mathcal{A}$ *provides a decision procedure for* $E(L_{\mathcal{A}})$*-theory of the structure* $\langle M; \sigma \rangle$*, since for a given formula we obtain an equivalent (in this structure) ground formula.*

Algorithm $\mathcal{D}$ from Section 1.7 and two algorithms from Section 2.6 will be examples of such quasi-QE algorithms.

Example 1.2.2. *If* S_2 *is the empty sort of variables and* $L_{\mathcal{A}}^x = L_{\mathcal{A}}$ *(Step 1 of algorithm* $\mathcal{A}$ *becomes trivial) then the set of all the relations,* $\exists L_{\mathcal{A}}$*-definable in* $\langle M; \sigma \rangle$*, is equal to the set of relations, (quantifier-free)* $L_{\mathcal{A}}$*-definable in* $\langle M; \sigma \rangle$*.*

The only step of the algorithm eliminates each quantifier of a given $\exists L_{\mathcal{A}}$-formula, and we obtain an equivalent in $\langle M; \sigma \rangle$ $L_{\mathcal{A}}$-formula, which is a quantifier-free L_σ-formula. In Chapter 2, this kind of quasi-QE will give us a description of all relations, which are positively existentially definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$.

Example 1.2.3. *Moreover, if* $L_{\mathcal{A}}$ *is the set of all quantifier-free* L_σ*-formulas then* $\mathcal{A}$ *is exactly a quantifier elimination algorithm for* L_σ *in* $\langle M; \sigma \rangle$*.*

1.2.4 The Main quasi-QE Algorithm

We going to construct two quasi-QE algorithms $\mathcal{R}$ and $\mathcal{D}$. The first one reduces the problem of satisfiability in $\mathbb{Z}$ of formulas (1.5) to the problem of decidability of the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$, while the second one gives us a decidability proof for this theory. In this subsection we describe algorithm $\mathcal{R}$, the main quasi-QE algorithm, and $\mathcal{D}$ will be constructed in Section 1.7.

Define the language $L_{\mathcal{R}}$ of quasi-QE algorithm $\mathcal{R}$ as the set of formulas $\exists\overline{\alpha} \bigvee\limits_{j\in J_1} \varphi_j(\overline{y_j},\overline{\alpha})$ for some finite index set J_1 and formulas $\varphi_j(\overline{y},\overline{\alpha})$ of the form

$$\overline{\alpha} \geqslant 1 \wedge \overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..m_j]} \mathrm{GCD}(f_{i,j}(\overline{y},\overline{\alpha}),g_{i,j}(\overline{y},\overline{\alpha})) = h_{i,j}(\overline{y},\overline{\alpha}), \tag{1.9}$$

where all linear polynomials $h_{i,j}(\overline{y},\overline{\alpha})$ have non-negative integer coefficients, and every gcd-expression takes one of the following forms:

($\mathcal{R}$-1) $\mathrm{GCD}(f(\overline{y}),g(\overline{y})) = h(\overline{y})$

($\mathcal{R}$-2) $\mathrm{GCD}(f(\overline{y}),g(\overline{y})) = a\zeta$

($\mathcal{R}$-3) $\mathrm{GCD}(a\zeta,g(\overline{y})) = b\eta$

($\mathcal{R}$-4) $\mathrm{GCD}(a\zeta,b\eta) = c\theta$,

where ζ,η,θ are Greek variables (they can be the same) and a, b, c are positive integers. Moreover, every Greek variable ζ, occurring in gcd-expression of the form ($\mathcal{R}$-2), appears on the right-hand sides of ($\mathcal{R}$-3) and ($\mathcal{R}$-4) only in gcd-expressions of the form $\mathrm{GCD}(a\zeta,g(\overline{y})) = b\zeta$ or $\mathrm{GCD}(a\zeta,b\zeta) = c\zeta$.

The latter restriction is necessary for the following reason. Suppose we obtain an equality $l(\overline{y}) = a\zeta$ from some gcd-expression ($\mathcal{R}$-2). Substitute $\frac{l(\overline{y})}{a}$ for all occurrences of ζ in (1.9) and multiply corresponding gcd-expressions by a. Our restriction ensures that after this substitution the resulting formula is an $L_{\mathcal{R}}$-formula.

We will call gcd-expressions $\mathrm{GCD}(f(\overline{z},\overline{\alpha}),g(\overline{z},\overline{\alpha}) + cx) = h(\overline{z},\overline{\alpha})$ *regular gcd-expressions*, if linear polynomials $f(\overline{z},\overline{\alpha})$ and $h(\overline{z},\overline{\alpha})$ have one of the following forms: either $a\zeta$ for some Greek variable ζ and positive integer a, or linear polynomial $l(\overline{z})$ with non-negative integer coefficients and positive constant term. Since in $L_{\mathcal{R}}$-formulas we have $\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0$, the polynomials $f(\overline{z},\overline{\alpha})$ and $h(\overline{z},\overline{\alpha})$ can take only positive values. Thus we can apply GCD-Lemma to system of regular gcd-expressions.

The set of formulas of elimination form $L^x_{\mathcal{R}} \subseteq L_{\mathcal{R}}$ comprise formulas $\exists\overline{\alpha} \bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x,\overline{z_j},\overline{\alpha})$ for some finite index set J_2 and formulas $\widetilde{\varphi}_j(x,\overline{z},\overline{\alpha})$ of the form

$$\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}_j(\overline{z},\overline{\alpha}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} \mathrm{GCD}(\widetilde{f}_{i,j}(\overline{z},\overline{\alpha}),\widetilde{g}_{i,j}(\overline{z}) + c_{i,j}x) = \widetilde{h}_{i,j}(\overline{z},\overline{\alpha}), \tag{1.10}$$

such that x does not appear in $\overline{z}$, $c_{i,j} > 0$, every gcd-expression with x is a regular gcd-expression, and $\widetilde{\widetilde{\varphi}}_j(\overline{z},\overline{\alpha})$ is a system of gcd-expressions without occurrences of x.

In Section 1.6 we show that transformations, described in Sections 1.4 and 1.5, actually define Step 1 and Step 2 of a quasi-QE algorithm for $L_{\mathcal{R}}$. Therefore, from the definition of $L_{\mathcal{R}}$ it follows that the proof of Theorem 1 will be completed if we prove decidability of the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$. In Section 1.7 we will show that LS-Lemma is not used in $\mathcal{D}$ and only a special case of GCD-Lemma is needed.

1.3 Proof of GCD-Lemma

Before proceeding to the proof of Lemma 1.2.3, it will be convenient to slightly reformulate its forth condition. Define the condition

((iv)) For every prime p there is $x_p \in \mathbb{Z}$ such that $\bigwedge\limits_{i\in I_p} v_p(b_i + x_p) = M_p$

to get the following auxiliary lemma.

Lemma 1.3.1. *Suppose we have a system of the form (1.8) with a_i, b_i, d_i, M_p, I_p, as defined in Lemma 1.2.3. Assume condition (ii) holds, then condition (iv) is equivalent to ((iv)).*

Proof. Consider prime p, natural number M_p, and index set I_p. Condition (ii) implies consistency of the system $\bigwedge\limits_{i\in I_p} p^{M_p} \mid b_i + x$. Take $x_0 \in [0, p^{M_p})$ such that $x_0 \equiv -b_i (\mathrm{mod}\ p^{M_p})$ for $i \in I_p$. Then we have that $x = x_0 + kp^{M_p}$ is a solution for every $k \in \mathbb{Z}$ and thus

$$\exists x \left(\bigwedge_{i\in I_p} v_p(b_i + x) = M_p \right) \Leftrightarrow \exists k \left(\bigwedge_{i\in I_p} p \nmid \left(\frac{b_i + x_0}{p^{M_p}} + k\right) \right). \tag{1.11}$$

The right-hand side of (1.11) is true if and only if $\left\{ \frac{b_i+x_0}{p^{M_p}} \right\}_{i\in I_p}$ does not contain a complete residue system modulo p. Hence it is true for every $p > m$, and for $p \leqslant m$ this condition is equivalent to the fact that for every $I \subseteq I_p$ such that $|I| = p$ there are such $i,j \in I$, $i \neq j$ that $p \mid \frac{b_i+x_0}{p^{M_p}} - \frac{b_j+x_0}{p^{M_p}}$, or, in terms of the p-valuation function, $v_p(b_i - b_j) > M_p$. This implies the lemma. □

Now we prove Lemma 1.2.3 assuming condition (iv) replaced by ((iv)).

Proof of Lemma 1.2.3. **Necessity**. Condition (i) is obviously necessary. Since for every $i,j \in [1..m]$ we have $d_i \mid b_i + x$ and $d_j \mid b_j + x$, it follows that $\mathrm{GCD}(d_i,d_j) \mid b_i + x - (b_j + x)$. Thus we also obtain (ii).

To prove (iii), consider for every $i,j \in [1..m]$ the following chain of equalities:

$$\begin{aligned} \mathrm{GCD}(a_i,d_j,b_i - b_j) &= \mathrm{GCD}(a_i,\mathrm{GCD}(a_j,b_j + x),b_i - b_j) \\ &= \mathrm{GCD}(a_i,a_j,\mathrm{GCD}(b_i + x,b_j + x)) = \mathrm{GCD}(d_i,d_j). \end{aligned}$$

For every prime number p we have $v_p(\mathrm{GCD}(a_i,b_i + x)) = v_p(d_i)$ for every $i \in [1..m]$. In particular, if $i \in I_p$ then $\min(v_p(a_i),v_p(b_i + x)) = v_p(\mathrm{GCD}(a_i,b_i + x)) = M_p$ and also $v_p(a_i) > M_p$. Therefore, $v_p(b_i + x) = M_p$ and necessity of ((iv)) is proved.

Sufficiency. Let P_0 be the (finite) set of all primes p such that $p \mid a_i$ for some $i \in [1..m]$. Condition (i) implies that $v_p(a_i) \geqslant v_p(d_i)$ for every $i \in [1..m]$ and $p \in P_0$. Now we rewrite (1.8) as a system of divisibilities and indivisibilities

$$\bigwedge_{i\in[1..m]} \left(\bigwedge_{p\in P_0 \wedge v_p(a_i)=v_p(d_i)} p^{v_p(d_i)} \mid b_i + x \right) \wedge \left(\bigwedge_{p\in P_0 \wedge v_p(a_i)>v_p(d_i)} p^{v_p(d_i)} \mid b_i + x \wedge p^{v_p(d_i)+1} \nmid b_i + x \right). \tag{1.12}$$

For every prime $p \in P_0$ consider the subsystem of (1.12) with all the divisibilities and indivisibilities having p in some degree as a divisor. Define the index set $K_p = \{i \in [1..m] \setminus J_p : v_p(a_i) > v_p(d_i)\}$ and the following system of divisibilities and indivisibilities

$$\Phi_p(x) \rightleftharpoons \bigwedge_{i\in[1..m]\setminus J_p} p^{v_p(d_i)} \mid b_i + x \wedge \bigwedge_{i\in K_p} p^{v_p(d_i)+1} \nmid b_i + x. \tag{1.13}$$

Thus we get that the conjunction (1.12) can be rewritten as follows:

$$\bigwedge_{p\in P_0} \left(\Phi_p(x) \wedge \bigwedge_{i\in J_p} p^{M_p} \mid b_i + x \wedge \bigwedge_{i\in I_p} p^{M_p+1} \nmid b_i + x \right). \tag{1.14}$$

By the Chinese remainder theorem it is sufficient to find independently for every prime $p \in P_0$ a solution to the corresponding subsystem.

Fix some $p \in P_0$. We first construct a solution x_p to the subsystem of divisibilities and indivisibilities with indexes from J_p and then prove that $\Phi_p(x_p)$ holds.

If $I_p = \varnothing$, as by (ii) we have $b_i \equiv b_j (\mathrm{mod}\ p^{M_p})$ for every $i,j \in J_p$, it is sufficient to take an arbitrary index $j_p \in J_p$ and define $x_p \in [0,p^{M_p})$ congruent to $-b_{j_p}$ modulo p^{M_p}.

When the index set I_p is not empty, condition ((iv)) implies that there exists $x_p \in \mathbb{Z}$ such that

$$\bigwedge_{i\in I_p} p^{M_p} \mid b_i + x_p \wedge \bigwedge_{i\in I_p} p^{M_p+1} \nmid b_i + x_p. \tag{1.15}$$

It is convenient to assume that $x_p \in [0,p^{M_p+1})$. Condition (ii) implies that in the system of divisibilities from (1.15) the index set I_p can be replaced by J_p.

It now remains to prove that x_p satisfies the system of divisibilities and indivisibilities (1.13). Let j_p be an arbitrary index from J_p. Condition (ii) implies that $b_k \equiv b_{j_p} (\mathrm{mod}\ p^{v_p(d_k)})$ for every $k \in [1..m] \setminus K_p$ and therefore $p^{v_p(d_k)} \mid b_k + x_p$ as $v_p(d_k) < M_p$. It follows that x_p satisfies the subsystem of divisibilities from (1.13).

To prove that x_p is also a solution to the subsystem of indivisibilities, suppose that $p^{v_p(d_k)+1}$ divides $b_k + x_p$ for some $k \in K_p$. Then we have $v_p(b_k - b_{j_p}) \geqslant \min\left\{v_p(b_k + x_p), v_p(b_{j_p} + x_p)\right\} \geqslant v_p(d_k) + 1$. It follows that

$$\min\left\{\min\left\{v_p(a_k), M_p\right\}, v_p(b_k - b_{j_p})\right\} \geqslant v_p(d_k) + 1.$$

But this is a contradiction to (iii) as the left-hand side must be not greater than $v_p(d_k)$.

Finally, we obtain a solution by the Chinese remainder theorem from a system of the form

$$\bigwedge_{p\in P_0} x \equiv x_p (\mathrm{mod}\ p^{\beta_p}), \tag{1.16}$$

where $\beta_p = M_p + 1$ if the index set I_p is not empty and $\beta_p = M_p$ otherwise. □

The resulting system of congruences gives us the following remark.

Remark 1.3.1. *If x is a solution to the system (1.8) then $x + k \operatorname*{LCM}_{i\in[1..m]}(d_i) \cdot \mathrm{rad}\left(\prod_{i\in[1..m]} \frac{a_i}{d_i}\right)$ is also a solution for every $k \in \mathbb{Z}$, where $\mathrm{rad}(n)$ is the radical of a non-zero integer n, i.e., the product of the distinct prime factors of n.*

1.4 Step 1: Latin Variable Isolation

Omitting the indexes j in (1.9), consider $L_{\mathcal{R}}$-formula $\exists\overline{\alpha}\varphi(\overline{y},\overline{\alpha})$, where

$$\varphi(\overline{y},\overline{\alpha}) \rightleftharpoons \overline{\alpha} \geqslant 1 \wedge \overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{y},\overline{\alpha}),g_i(\overline{y},\overline{\alpha})) = h_i(\overline{y},\overline{\alpha}). \tag{1.17}$$

Recall that in $L_{\mathcal{R}}$-formulas the coefficients of $h_i(\overline{y},\overline{\alpha})$ are non-negative. In the same way as in subsection 1.2.1, we split the list $\overline{y}$ into $\overline{s} = y_1,...,y_l$ and $\overline{t} = y_{l+1},...,y_n$. We have the following remarks.

Remark 1.4.1. *The result of application of LS-Lemma to a subsystem $A\overline{s} = b \wedge C\overline{s} \geqslant d \wedge \overline{s} \geqslant 0$ of the formula $A\overline{s} = b \wedge C\overline{s} \geqslant d \wedge \varphi(\overline{y},\overline{\alpha})$ is a disjunction of the formulas $\psi_j(\overline{z},\overline{t},\overline{\alpha})$ such that $\exists\overline{\alpha}\psi_j(\overline{z},\overline{t},\overline{\alpha})$ is an $L_{\mathcal{R}}$-formula. Moreover, for every regular gcd-expression in $\varphi(\overline{y},\overline{\alpha})$ with an isolated variable from $\overline{t}$ there will be a corresponding regular gcd-expression in $\psi_j(\overline{z},\overline{t},\overline{\alpha})$.*

Proof. Indeed, since the subsystem of linear equalities and inequalities contains $\overline{s} \geqslant 0$, then every variable from $\overline{s}$ is replaced by a linear polynomial $l(\overline{z})$ with non-negative integer coefficients. Hence every linear polynomial $f(\overline{y})$ with non-negative coefficients preserves this property, when we substitute $E^{(j)}\overline{z} + u^{(j)}$ for $\overline{s}$, and moreover, if the constant term of $f(\overline{y})$ was positive, it remains positive. □

Remark 1.4.2. *We can assume that in the system (1.17) there are no gcd-expressions of the form ($\mathcal{R}$-1) and ($\mathcal{R}$-2) such that $k_1 f_i(\overline{y}) = k_2 g_i(\overline{y})$ for some integers k_1 and k_2, which are not simultaneously equal to zero.*

Proof. Suppose that $k_1 f_i(\overline{y}) = k_2 g_i(\overline{y})$ for $k_1 \neq 0$. In this case we can compute the greatest common divisor and consider a disjunction over $\sigma \in \{-1,1\}$, substituting in (1.17) the corresponding gcd-expression for an equality $\sigma\mathrm{GCD}(k_1,k_2)g_i(\overline{y}) = k_1 h_i(\overline{y},\overline{\alpha})$. For gcd-expressions of the form ($\mathcal{R}$-1) this equality is either always true, or can be used to obtain a disjunction of systems with

one fewer number of variables as a result of application of LS-Lemma to the subsystem $\overline{y} \geqslant 0 \wedge \sigma\mathrm{GCD}(k_1,k_2)g_i(\overline{y}) = k_1 h_i(\overline{y})$ of the formula (1.17).

In the case where $h_i(\overline{y},\overline{\alpha}) = a_i\zeta_i$, we exclude $\sigma\mathrm{GCD}(k_1,k_2)g_i(\overline{y}) = a_i k_1 \zeta_i$ from the system, substitute $\frac{\sigma\mathrm{GCD}(k_1,k_2)g_i(\overline{y})}{a_i k_1}$ for all occurrences of ζ_i, and multiply linear expressions by $a_i k_1$. In particular, instead of $\zeta_i \geqslant 1$ there will be an inequality $\sigma\mathrm{GCD}(k_1,k_2)g_i(\overline{y}) \geqslant a_i k_1$. By definition of the language $L_{\mathcal{R}}$, after the substitution every gcd-expression again will have one of the forms: ($\mathcal{R}$-1)–($\mathcal{R}$-4). It remains to apply LS-Lemma to the subsystem $\overline{y} \geqslant 0 \wedge \sigma\mathrm{GCD}(k_1,k_2)g_i(\overline{y}) \geqslant a_i k_1$. □

We now show how to construct an equi-satisfiable over the integers disjunction of formulas of the form (1.10).

The first case is when there is a Latin variable x that does not occur on the right-hand side of any gcd-expression of (1.17). Using the Euclidean algorithm, every gcd-expression of the form ($\mathcal{R}$-1) or ($\mathcal{R}$-2) $\mathrm{GCD}(f(\overline{z}) + ax, g(\overline{z}) + bx) = h(\overline{z},\overline{\alpha})$, where $a,b \neq 0$ and $f(\overline{z})$, $g(\overline{z})$ are linear polynomials, can be rewritten such that the coefficient of x is non-zero only in one of the polynomials. Let $a > b > 0$ and $a = qb + r$ for $r \in [0,b)$. Then we have

$$\mathrm{GCD}(f(\overline{z}) + ax, g(\overline{z}) + bx) = \mathrm{GCD}(f(\overline{z}) - qg(\overline{z}) + rx, g(\overline{z}) + bx).$$

Repeating this step, we obtain a formula of the form $\mathrm{GCD}(\widetilde{f}(\overline{z}),\widetilde{g}(\overline{z}) + cx) = h(\overline{z},\overline{\alpha})$. Remark 1.4.2 implies that $\widetilde{f}(\overline{z})$ is not identically zero.

In the other case, every Latin variable appears in at least one of the right-hand side polynomials. Isolating in (1.17) a subsystem of gcd-expressions of the form ($\mathcal{R}$-1), rewrite (1.17) as follows:

$$\begin{aligned} \overline{\alpha} \geqslant 1 \wedge \overline{y} \geqslant 0 \wedge & \bigwedge_{i\in[1..l]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}) \\ & \wedge \bigwedge_{i\in[l+1..m]} \mathrm{GCD}(f_i(\overline{y},\overline{\alpha}),g_i(\overline{y},\overline{\alpha})) = h_i(\overline{\alpha}). \end{aligned} \tag{1.18}$$

For every variable $x \in \overline{y}$ there is an index $i_x \in [1..l]$ such that this variable appears with non-zero coefficient in $h_{i_x}(\overline{y})$ (that is, $h_{i_x}(\overline{y}) = h'_{i_x}(\overline{y} \setminus x) + c_{i_x}x$ for some positive integer c_{i_x}). Remark 1.4.2 implies that we do not have simultaneously $u_1 f_{i_x}(\overline{y}) = v_1 h_{i_x}(\overline{y})$ and $u_2 g_{i_x}(\overline{y}) = v_2 h_{i_x}(\overline{y})$ for some integers u_1,v_1,u_2,v_2. Assume that $u f_{i_x}(\overline{y}) \neq v h_{i_x}(\overline{y})$ for every integers u and v. Then the system (1.17) is equivalent to the following disjunction:

$$\bigvee_{x\in\overline{y}} \left(\bigvee_{-S_x\leqslant k\leqslant S_x} \overline{\alpha} \geqslant 1 \wedge \Psi_{x,k}(\overline{y}) \wedge \bigwedge_{i\in[1..m]\wedge i\neq i_x} \mathrm{GCD}(f_i(\overline{y},\overline{\alpha}),g_i(\overline{y},\overline{\alpha})) = h_i(\overline{y},\overline{\alpha}) \right), \tag{1.19}$$

for

$$\Psi_{x,k}(\overline{y}) \rightleftharpoons \overline{y} \geqslant 0 \wedge \bigwedge_{x'\in\overline{y}} x \geqslant x' \wedge k(h_{i_x}(\overline{y})) = f_{i_x}(\overline{y}),$$

where S_x is the sum of the absolute values of the coefficients of $f_{i_x}(\overline{y})$. This follows from the fact that all the coefficients of $h_{i_x}(\overline{y})$ are non-negative, $c_{i_x} > 0$, the variables $\overline{y}$ are non-negative and x takes the maximum value among the variables from $\overline{y}$.

Application of LS-Lemma to the subsystem $\Psi_{x,k}(\overline{y})$ of every disjunct of (1.19) gives us a disjunction of systems of the form (1.17) with one fewer Latin variable and one fewer gcd-expression. If we denote this disjunction $\psi(\overline{z},\overline{\alpha})$, by Remark 1.4.1, we have $\exists\overline{\alpha}\psi(\overline{z},\overline{\alpha}) \in L_{\mathcal{R}}$.

This concludes the consideration of the second case. Now in every system from $\psi(\overline{z},\overline{\alpha})$ again we try to isolate a Latin variable which have no occurrences in the right-hand side of any gcd-expression. Finally we obtain a disjunction of formulas of the form (1.10).

We assume that the desired disjunction is constructed. Omit the indexes j in (1.10) and denote this formula by $\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$. Transform $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ into an equi-satisfiable over the integers disjunction of formulas of the same form (1.10) but with regular gcd-expressions. Thus we will construct an $L^x_{\mathcal{R}}$- formula.

Since $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ is an $L_{\mathcal{R}}$-formula, non-regular gcd-expressions can only be of the form ($\mathcal{R}$-1) or ($\mathcal{R}$-2). Let the gcd-expressions from $\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ with indexes $i = 1..k$ comprise all non-regular gcd-expressions of the form ($\mathcal{R}$-1) and all non-regular gcd-expressions ($\mathcal{R}$-2), assuming $\widetilde{h}_i(\overline{z},\overline{\alpha}) = a_i\zeta_i$, have indexes $i = k+1..l$.

Rewrite $\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ in the form $\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \Delta(x,\overline{z},\overline{\alpha})$, where

$$\begin{aligned}\Delta(x,\overline{z},\overline{\alpha}) \rightleftharpoons & \bigwedge_{i\in[1..k]} \mathrm{GCD}(\widetilde{f}_i(\overline{z}),\quad \widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z}) \\ \wedge & \bigwedge_{i\in[k+1..l]} \mathrm{GCD}(\widetilde{f}_i(\overline{z}),\quad \widetilde{g}_i(\overline{z}) + c_i x) = a_i\zeta_i \\ \wedge & \bigwedge_{i\in[l+1..m]} \mathrm{GCD}(\widetilde{f}_i(\overline{z},\overline{\alpha}),\widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z},\overline{\alpha})\end{aligned}$$

and for the formula $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ construct an equi-satisfiable formula

$$\exists\overline{\alpha}\Big(\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha}) \vee \widetilde{\Phi}_1(\overline{z_1},\overline{\alpha}) \vee \widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})\Big).$$

Here $\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha})$ and $\widetilde{\Phi}_1(\overline{z_1},\overline{\alpha})$ are disjunctions of systems of the form (1.17) such that the list $\overline{z_0}$ contains two and $\overline{z_1}$ one fewer variable than $x,\overline{z}$. In these systems again we isolate a Latin variable and then make regular the gcd-expressions with this variable. Since the number of Latin variables always decreases, this process will definitely terminate. In the meantime, $\widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})$ will be a disjunction of the desired form, that is, $\exists\overline{\alpha}\widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})$ will be some $L^x_{\mathcal{R}}$-formula.

Disjunctions $\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha})$ and $\widetilde{\Phi}_1(\overline{z_1},\overline{\alpha})$ correspond to the cases when polynomials $\widetilde{f}_i(\overline{z})$ are equal to zero, for $i = 1..k$ and $i = k+1..l$, respectively. We construct these disjunctions in a similar way as in the cases from Remark 1.4.2. That is,

$$\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha}) \rightleftharpoons \bigvee_{i\in[1..k]} \bigvee_{\sigma\in\{-1,1\}} \Omega_{i,\sigma}(\overline{z_0},\overline{\alpha})$$

and

$$\widetilde{\Phi}_1(\overline{z_1},\overline{\alpha}) \rightleftharpoons \bigvee_{i\in[k+1..l]} \bigvee_{\sigma\in\{-1,1\}} \Omega_{i,\sigma}(\overline{z_1},\overline{\alpha}),$$

where $\Omega_{i,\sigma}(\overline{z_0},\overline{\alpha})$ and $\Omega_{i,\sigma}(\overline{z_1},\overline{\alpha})$ are disjunctions, which can be obtained by using LS-Lemma.

Denote by $\Delta_i(x,\overline{z},\overline{\alpha})$ the systems that we get after excluding a gcd-expression with index $i \in [1..l]$ from $\Delta(x,\overline{z},\overline{\alpha})$. Then for every $i = 1..k$, we obtain a disjunction $\Omega_{i,\sigma}(\overline{z_0},\overline{\alpha})$ as a result of application of LS-Lemma to the subsystem

$$\Phi_{i,\sigma}(x,\overline{z}) \rightleftharpoons \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{f_i}(\overline{z}) = 0 \wedge c_i x = \sigma\widetilde{h_i}(\overline{z}) - \widetilde{g_i}(\overline{z})$$

of the formula $\overline{\alpha} \geqslant 1 \wedge \Phi_{i,\sigma}(x,\overline{z}) \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \Delta_i(x,\overline{z},\overline{\alpha})$.

The result of substitution of $\frac{\sigma(\widetilde{g_i}(\overline{z})+c_i x)}{a_i}$ for ζ_i in the formula $\overline{\alpha}\backslash\zeta_i \geqslant 1 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \Delta_i(x,\overline{z},\overline{\alpha})$ and multiplication of the resulting expressions by a_i will be denoted by $\widetilde{\Delta}_{i,\sigma}(x,\overline{z},\overline{\alpha})$, where $i = k+1..l$. Applying LS-Lemma to the subsystem

$$\Phi_{i,\sigma}(x,\overline{z}) \rightleftharpoons \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{f_i}(\overline{z}) = 0 \wedge \sigma(\widetilde{g_i}(\overline{z}) + c_i x) \geqslant a_i$$

of the formula $\Phi_{i,\sigma}(x,\overline{z}) \wedge \widetilde{\Delta}_{i,\sigma}(x,\overline{z},\overline{\alpha})$, we obtain a disjunction $\Omega_{i,\sigma}(\overline{z_1},\overline{\alpha})$. It remains to notice that the lists $\overline{z_0}$ and $\overline{z_1}$ have fewer variables since every polynomial $\widetilde{f_i}(\overline{z})$ is not identically zero for $i = 1..l$.

Now consider the case when the values of polynomials $\widetilde{f_i}(\overline{z})$ are non-zero:

$$\bigvee_{\overline{\sigma}\in\{-1,1\}^l} \Bigg(\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \bigwedge_{i\in[1..k]} \Big(\sigma_i \widetilde{f_i}(\overline{z}) \geqslant 1 \wedge \widetilde{h_i}(\overline{z}) \geqslant 1\Big) \\ \wedge \bigwedge_{i\in[k+1..l]} \sigma_i \widetilde{f_i}(\overline{z}) \geqslant 1 \wedge \bigwedge_{i\in[1..m]} \mathrm{GCD}(\widetilde{f_i}(\overline{z},\overline{\alpha}),\widetilde{g_i}(\overline{z}) + c_i x) = \widetilde{h_i}(\overline{z},\overline{\alpha}) \Bigg). \tag{1.20}$$

The disjunction $\widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})$ is a result of application of LS-Lemma to the subsystems with all linear equalities and inequalities over $\overline{z}$ in every disjunct from (1.20). Remark 1.4.1 yields regularity of every gcd-expression with x in the resulting systems.

1.5 Step 2: GCD-Lemma Application

Now consider the subsystem of (1.10) with an isolated variable x. Without loss of generality, we can assume that all $c_{i,j}$ equal 1 as we can compute $C = \operatorname{LCM}_{i=1..\widetilde{m}_j}(c_{i,j})$, multiply every gcd-expression by $\frac{C}{c_{i,j}}$, replace all occurrences of Cx by $\widetilde{x}$ and add the gcd-expression $\mathrm{GCD}(C,\widetilde{x}) = C$.

Introducing some new positive integer Greek variables $\overline{\beta}$, rewrite the formula $\exists x \widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ for $L^x_{\mathcal{R}}$-formula $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$, where

$$\widetilde{\varphi}(x,\overline{z},\overline{\alpha}) \rightleftharpoons \overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \\ \wedge \bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{z},\overline{\alpha}),g_i(\overline{z}) + x) = h_i(\overline{z},\overline{\alpha}) \tag{1.21}$$

to get an equivalent in $\mathbb{Z}$ formula of the form $\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ such that $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ is some $L_{\mathcal{R}}$-formula. This transformation will define Step 2 of the quasi-QE algorithm $\mathcal{R}$.

Denote the list of variables $\overline{z}$,$\overline{\alpha}$ by $\overline{u}$ and consider conditions (i) – (iv) of GCD-Lemma.

(i). In this case introduction of new variables is not needed. We get the conjunction $\bigwedge\limits_{i\in[1..m]} \mathrm{GCD}(h_i(\overline{u}),f_i(\overline{u})) = h_i(\overline{u})$.

(ii). For every ordered pair (i,j) with $1 \leqslant i < j \leqslant m$, a new variable $\zeta_{i,j}$ is introduced such that the second condition can be written in the form:

$$\bigwedge_{1\leqslant i<j\leqslant m} \exists\zeta_{i,j}\,(\mathrm{GCD}(h_i(\overline{u}),h_j(\overline{u})) = \zeta_{i,j} \wedge \mathrm{GCD}(\zeta_{i,j},g_i(\overline{z}) - g_j(\overline{z})) = \zeta_{i,j})\,.$$

This formula can be put in prenex form, as the corresponding variables appear only in a single pair of gcd-expressions.

(iii). For every ordered pair (i,j), $i,j \in [1..m]$, we introduce two new variables $\eta_{i,j}$ and $\theta_{i,j}$ to rewrite the divisibility $\mathrm{GCD}(f_i(\overline{u}),h_j(\overline{u}),g_i(\overline{z}) - g_j(\overline{z})) \mid h_i(\overline{u})$ in the following form:

$$\begin{aligned}\exists\eta_{i,j}\exists\theta_{i,j}(\mathrm{GCD}(f_i(\overline{u}),h_j(\overline{u})) = \eta_{i,j}\\ \wedge \mathrm{GCD}(\eta_{i,j},g_i(\overline{z}) - g_j(\overline{z})) = \theta_{i,j} \wedge \mathrm{GCD}(\theta_{i,j},h_i(\overline{u})) = \theta_{i,j}).\end{aligned}$$

(iv). We have to rewrite the fact that for every prime $p \leqslant m$ and index set $I \subseteq [1..m]$ such that $|I| = p$ either the condition

$$\bigwedge_{i\in I}\left(v_p(h_i(\overline{u})) = \max_{j\in[1..m]} v_p(h_j(\overline{u})) \wedge v_p(f_i(\overline{u})) > v_p(h_i(\overline{u}))\right),$$

is false, or there are such $i,j \in I, i \neq j$ that $v_p\,(g_i(\overline{z}) - g_j(\overline{z})) > v_p\,(h_i(\overline{u}))$. Let us construct a formula $\Omega_{p,I}(\overline{u})$ to write this condition in the form of the following conjunction:

$$\bigwedge_{p\leqslant m\wedge p\in\mathbb{P}}\left(\bigwedge_{I\subseteq[1..m]\wedge|I|=p}\Omega_{p,I}(\overline{u})\right),$$

where $\mathbb{P}$ is the set of the prime numbers.

The first case is when the index set I is not a subset of J_p: either not for all $i \in I$ the value of $v_p(h_i(\overline{u}))$ is the same, or not the maximal $\bigvee\limits_{i\in I\wedge j\in[1..m]} v_p(h_i(\overline{u})) < v_p(h_j(\overline{u}))$. Here the relation $v_p(x) < v_p(y)$ is definable by the formula

$$\exists\iota\,(\mathrm{GCD}(\iota,x) = \iota \wedge \mathrm{GCD}(p\iota,x) = \iota \wedge \mathrm{GCD}(\iota,y) = \iota \wedge \mathrm{GCD}(p\iota,y) = p\iota)\,. \tag{1.22}$$

Now exclude the sets I with $\bigvee\limits_{i\in I} v_p(f_i(\overline{u})) = v_p(h_i(\overline{u}))$, since otherwise I is not a subset of I_p. For the relation of equality of p-valuations $v_p(x) = v_p(y)$ we have the existential formula

$$\exists\iota\,(\mathrm{GCD}(\iota,x) = \iota \wedge \mathrm{GCD}(\iota,y) = \iota \wedge \mathrm{GCD}(p\iota,x) = \iota \wedge \mathrm{GCD}(p\iota,y) = \iota)\,. \tag{1.23}$$

If neither of the disjunctions is true (i.e. $I \subseteq I_p$), we only need to write the condition «there are such $i,j \in I$, $i \neq j$ that $v_p(g_i(\overline{z}) - g_j(\overline{z})) > v_p(h_i(\overline{u}))$». Combine the disjunctions to get $\Omega_{p,I}(\overline{u})$.

$$\begin{aligned}\Omega_{p,I}(\overline{u}) \rightleftharpoons \bigvee_{i\in I\wedge j\in[1..m]} v_p(h_i(\overline{u})) < v_p(h_j(\overline{u})) \vee \bigvee_{i\in I} v_p(h_i(\overline{u})) = v_p(f_i(\overline{u}))\\ \vee \bigvee_{i,j\in I\wedge i\neq j} v_p(g_i(\overline{z}) - g_j(\overline{z})) > v_p(h_i(\overline{u})).\end{aligned}$$

Introducing new Greek variables for every disjunct, using (1.22) and (1.23), we rewrite this formula in the desired form. This completes the transformation of (1.21) using GCD-Lemma. Since all gcd-expressions with x in (1.21) are regular, the variables $\overline{\beta}$ can take only positive values. Adding $\overline{\beta} \geqslant 1$ to the resulting formula, we get a desired formula $\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$.

1.6 The Reduction Theorem

We can now prove the following theorem. Recall that P$\exists$ThS denotes the positive existential theory of some structure S; for multiplication by a positive integer a introduce a unary function symbol $a\cdot$.

Theorem 2. *The decision problem for* $\exists\mathrm{Th}\langle\mathbb{Z};0,1,+,-,\leqslant,\mathrm{GCD}\rangle$ *is reducible to the decision problem for* $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD}\rangle$.

Proof. From Lemma 1.2.2, it follows that it is sufficient to check satisfiability in $\mathbb{Z}$ of formulas of the form (1.7). Since (1.7) is an $L_{\mathcal{R}}$-formula, let us prove that Step 1 and Step 2 from Sections 1.4 and 1.5 actually define a quasi-QE algorithm $\mathcal{R}$.

By construction, Section 1.4 satisfy the definition of Step 1 of the algorithm $\mathcal{R}$.

For Step 2 first note that condition (i) introduces gcd-expressions, each of which has form either ($\mathcal{R}$-1), ($\mathcal{R}$-3) or ($\mathcal{R}$-4). Rewriting (ii) and (iii), we obtain gcd-expressions of the following forms: ($\mathcal{R}$-2), ($\mathcal{R}$-3) or ($\mathcal{R}$-4) and for condition (iv) — gcd-expressions ($\mathcal{R}$-3) or ($\mathcal{R}$-4).

Let us now check that gcd-expressions with a Greek variable from some gcd-expression of the form ($\mathcal{R}$-2) satisfy the restrictions from the definition of $L_{\mathcal{R}}$. This is obvious for the *new* Greek variables, introduced while rewriting conditions (ii) and (iii). While for every Greek variable ζ from a gcd-expression of the form ($\mathcal{R}$-2) in system (1.21), its occurrence in the right-hand side of some gcd-expression, which was obtained in Step 2, can only be connected with condition (i). Since $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ is an $L^x_{\mathcal{R}}$-formula, every gcd-expression with x and some Greek variable ζ in the right-hand side has form either $\mathrm{GCD}(f(\overline{z}),g(\overline{z})+x)=a\zeta$, or $\mathrm{GCD}(a\zeta,g(\overline{z})+x)=b\zeta$. In this case, from (i) we obtain gcd-expressions of the form $\mathrm{GCD}(a\zeta,f(\overline{z}))=a\zeta$ or $\mathrm{GCD}(b\zeta,a\zeta)=b\zeta$. Hence, after application of transformations from Section 1.5, the formula $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ is actually an $L_{\mathcal{R}}$-formula.

To complete the proof it is sufficient to notice that every $L^2_{\mathcal{R}}$-formula is a formula of the form $\exists\overline{\alpha}\left(\overline{\alpha}\geqslant 1\wedge\bigvee\limits_{j\in J}\varphi_j(\overline{\alpha})\right)$ for some finite index set J, where every $\varphi_j(\overline{\alpha})$ is a conjunction of atomic formulas of the form $\mathrm{GCD}(a',b')=c'$, $\mathrm{GCD}(a',b')=c\zeta$, $\mathrm{GCD}(a\zeta,b')=c\eta$ or $\mathrm{GCD}(a\zeta,b\eta)=c\theta$ for some positive integers a,b,c and non-negative integers a',b',c'. To get a positive $L_{\langle 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD}\rangle}$-formula, we exclude the cases when a',b',c' are equal to zero.

The expression $\mathrm{GCD}(a',b')=c'$ can be directly computed and we either exclude this gcd-expression from $\varphi_j(\overline{\alpha})$, or conclude that the system is not satisfiable. The case when we have an expression of the form $\mathrm{GCD}(0,0)=c\zeta$ also implies unsatisfiablilty of $\varphi_j(\overline{\alpha})$ in the positive

integers. Finally, exclude the expressions $\mathrm{GCD}(a,0) = c\zeta$ and $\mathrm{GCD}(a\zeta,0) = c\eta$, substituting in the first case $\frac{a}{c}$ for all occurrences of ζ, and in the second case $\frac{a}{c}\zeta$ for η, and then multiplying these gcd-expressions by c. □

1.7 Systems of GCD-Expressions with a Single non-Zero Coefficient

In this section, using a quasi-quantifier elimination algorithm, we will prove decidability of the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$. Thus, the proof of Theorem 1 will be completed.

If we suppose that our aim was only to solve the original problem of decidability of the $\exists$-theory of the structure $\langle \mathbb{Z}; 0, 1, +, -, \leqslant, \mathrm{GCD}\rangle$, then it would be sufficient to combine Theorem 2 with the decidability result for Skolem arithmetic with constants. Recall that Skolem arithmetic is the elementary theory of the structure $\langle \mathbb{Z}_{>0}; \cdot, =\rangle$, i.e., the arithmetic of multiplication. T. Skolem presented an informal proof of decidability using quantifier elimination technique [5; 72]. Relying on the notion of direct product of structures, A. Mostowski [53] in 1952 presented a complete proof. Alternative proofs were later obtained by P. Cégielski [14] and B.R. Hodgson [33]. Since the relations $x = a$ for every natural $a \geqslant 2$ are not definable in the structure $\langle \mathbb{Z}_{>0}; \cdot, =\rangle$ (see [5]), we need a slightly more general result. A decidability proof for $\mathrm{Th}\langle \mathbb{Z}_{>0}; \{a\}_{a\in\mathbb{Z}_{>0}}, \cdot, =\rangle$ can be obtained by reduction to Skolem arithmetic [24]. Now, since the relation GCD is definable by the formula

$$\mathrm{GCD}(x,y) = z \Leftrightarrow z \mid x \wedge z \mid y \wedge \forall t(t \mid x \wedge t \mid y \Rightarrow t \mid z), \tag{1.24}$$

by definition of the divisibility relation $x \mid y \rightleftharpoons \exists z(y = z \cdot x)$ we prove decidability of the elementary theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$.

Nevertheless, to complete the proof of Theorem 1, it is sufficient to prove decidability of the positive existential theory of the aforementioned structure. Let us show how to apply quasi-quantifier elimination approach to obtain this decidability result. It is clear that we can consider the problem of satisfiability in the positive integers of a system of gcd-expressions with linear polynomials of the form either a or ax for some positive integer a. For this problem we construct a quasi-QE algorithm $\mathcal{D}$. In Step 2 of $\mathcal{D}$ we use the following corollary of GCD-Lemma.

Lemma 1.7.1. *The system* $\bigwedge\limits_{i\in[1..m]} \mathrm{GCD}(a_i,x) = d_i$ *for* $a_i, d_i \in \mathbb{Z}$ *and* $a_i \neq 0$, $d_i > 0$ *for every* $i \in [1..m]$ *has a solution in* $\mathbb{Z}$ *if and only if the following conditions simultaneously hold:*

(a) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$

(b) $\bigwedge\limits_{1\leqslant i<j\leqslant m} \mathrm{GCD}(a_i,d_j) = \mathrm{GCD}(a_j,d_i) = \mathrm{GCD}(d_i,d_j)$

Proof. Since in our case all the values of b_i from GCD-Lemma are equal to zero, it is sufficient to consider only conditions (i) and (iii). The first one remains unchanged and condition (iii) has the

form of a system of the following pairs of divisibilities:

$$\mathrm{GCD}(a_i,d_j) \mid d_i \wedge \mathrm{GCD}(a_j,d_i) \mid d_j$$

for any $1 \leqslant i < j \leqslant m$. The divisibilities obviously follow from (b). The converse direction follows from the chain of equalities:

$$\mathrm{GCD}(a_i,d_j) = \mathrm{GCD}\,(d_i,\mathrm{GCD}(a_i,d_j)) = \mathrm{GCD}\,(\mathrm{GCD}(d_i,a_i),d_j)) = \mathrm{GCD}\,(d_i,d_j)\,.$$

□

Now consider the structure $\langle \mathbb{Z}_{>0}; 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD}\rangle$ and define qiasi-QE algorithm $\mathcal{D}$. In this algorithm S_2 will be the empty sort of variables. The language $L_{\mathcal{D}}$ of algorithm $\mathcal{D}$ will be the set of formulas $\bigvee\limits_{j\in J_1} \varphi_j(\overline{y_j})$ for some finite index set J_1 and conjunctions of gcd-expressions $\varphi_j(\overline{y})$ such that every gcd-expression has one of the following forms:

($\mathcal{D}$-1) $\mathrm{GCD}(au,bv) = dw$

($\mathcal{D}$-2) $\mathrm{GCD}(au,bv) = d$

($\mathcal{D}$-3) $\mathrm{GCD}(a,bv) = d$

($\mathcal{D}$-4) $\mathrm{GCD}(a,b) = d$,

where u and v are different variables, w can be the same as u or v, and a,b,d are positive integers. Moreover, each conjunction $\varphi_j(\overline{y})$ for every pair of variables $u,v \in \overline{y}$ contains some gcd-expression with left-hand side of the form $\mathrm{GCD}(au,bv)$ for some positive integers a and b.

The set of formulas of elimination form $L^x_{\mathcal{D}} \subseteq L_{\mathcal{D}}$ comprise formulas $\bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x,\overline{z_j})$ for some finite index set J_2 and every $\widetilde{\varphi}_j(x,\overline{z})$ of the form

$$\widetilde{\widetilde{\varphi}}_j(\overline{z}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} \mathrm{GCD}(\widetilde{f}_{i,j}(\overline{z}),c_{i,j}x) = \widetilde{h}_{i,j}(\overline{z}) \tag{1.25}$$

such that x does not appear in $\overline{z}$, $c_{i,j} > 0$, and $\widetilde{\widetilde{\varphi}}_j(\overline{z})$ is a system of gcd-expressions with variables from $\overline{z}$.

Before we define Steps 1 and 2 of the algorithm $\mathcal{D}$, let us prove the following lemma.

Lemma 1.7.2. *The decision problem for* $\mathrm{P}\exists\mathrm{Th}\langle \mathbb{Z}_{>0}; 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD}\rangle$ *is reducible to the decision problem for* $L^1_{\mathcal{D}}$*-theory.*

Proof. Consider a system of gcd-expressions

$$\bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}) \tag{1.26}$$

for $f_i(\overline{y}),g_i(\overline{y}),h_i(\overline{y})$ of the form either au or a, where a is a positive integer and $u \in \overline{y}$.

In the case of $\mathrm{GCD}(au,bu) = h(\overline{y})$ the greatest common divisor can be directly computed, and we can eliminate one of the variables. For the gcd-expressions of the form $\mathrm{GCD}(a,g(\overline{y})) = du$ with $a,d > 0$, the system (1.26) is equivalent to a disjunction over all positive divisors d' of $\frac{a}{d}$ of the systems, that we obtain from (1.26) replacing every occurrence of u by d'.

Consider pairs of variables $u,v \in \overline{y}$ such that in (1.26) the value of $\mathrm{GCD}(au,bv)$ is not specified for any positive integers a and b. Introduce a new variable $t_{\{u,v\}}$ for every such pair (u,v) and add to the system (1.26) the expression $\mathrm{GCD}(u,v) = t_{\{u,v\}}$. We continue this process for the new variables and introduce at most 2^n variables t_Y for the greatest common divisors of various subsets Y of $\overline{y}$ (since for every two variables t_{Y_1} and t_{Y_2} we have $\mathrm{GCD}(t_{Y_1},t_{Y_2}) = t_{Y_1 \cup Y_2}$). $\square$

Theorem 3. $\mathrm{P}\exists\mathrm{Th}\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$ *is decidable.*

Proof. From Lemma 1.7.2 it follows that if we define a quasi-QE algorithm $\mathcal{D}$ for the language $L_{\mathcal{D}}$ in $\mathbb{Z}_{>0}$ then we will get a decision procedure for $\mathrm{P}\exists\mathrm{Th}\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$. Define the two Steps of $\mathcal{D}$.

Step 1. Let us have an $L_{\mathcal{D}}$-formula of the form (1.26). Construct a directed graph whose vertices are the variables of the system (1.26), and every arc from the vertex u to the vertex v corresponds to a gcd-expression with $h_i(\overline{y})$ of the form du, and either $f_i(\overline{y})$ or $g_i(\overline{y})$ of the form av. In the resulting graph we will detect cycles and rewrite (1.26) as equivalent disjunction of systems with fewer number of variables. We see that if the graph constructed by the system (1.26) has no cycles, then $L_{\mathcal{D}}$-formula (1.26) contains variables that do not appear on the right-hand side of any of the gcd-expressions, and thus this formula is a $L^x_{\mathcal{D}}$-formula.

Assume that there is some cycle $y_1 \to y_2 \to \ldots \to y_s \to y_1$. It corresponds to a sequence of divisibilities of the form

$$a_1y_1 \mid b_1y_2, \ldots, a_{s-1}y_{s-1} \mid b_{s-1}y_s, \gamma y_s \mid \delta y_1.$$

The first $(s-1)$ divisibilities yield a divisibility of the form $\alpha y_1 \mid \beta y_s$. Thus, we have $\beta y_s = k\alpha y_1$ for some positive integer k. The divisibility $\gamma y_s \mid \delta y_1$ implies that $\gamma\beta y_s \mid \delta\beta y_1$ and hence $\gamma k\alpha y_1 \mid \delta\beta y_1$. Since $y_1 > 0$, there is a finite set of such k and we can eliminate one of the variables, for example y_s. We continue this process to eliminate all the variables from this cycle except for y_1.

Step 2. Consider the subsystem of (1.25) with an isolated variable x. As in Section 1.5, we can assume that all $c_{i,j}$ equal 1, and we have the following $L^x_{\mathcal{D}}$-formula

$$\widetilde{\widetilde{\varphi}}(\overline{z}) \wedge \bigwedge_{i\in[1..m]} \left(\mathrm{GCD}(f_i(\overline{z}),x) = h_i(\overline{z})\right). \tag{1.27}$$

Applying Lemma 1.7.1, consider every item separately.

(a). In this case we obtain the conjunction $\bigwedge\limits_{i\in[1..m]} \mathrm{GCD}(h_i(\overline{z}),f_i(\overline{z})) = h_i(\overline{z})$.

(b). For every pair $1 \leqslant i < j \leqslant m$ we have to rewrite the chain of equalities

$$\mathrm{GCD}(f_i(\overline{z}),h_j(\overline{z})) = \mathrm{GCD}(f_j(\overline{z}),h_i(\overline{z})) = \mathrm{GCD}(h_i(\overline{z}),h_j(\overline{z})).$$

We have two cases. If $h_i(\overline{z}) = d_i$ or $h_j(\overline{z}) = d_j$ for some positive integers d_i,d_j, we get the following disjunction over all positive divisors of d_i (assuming the first equality holds):

$$\bigvee_{d\mid d_i} \big(\mathrm{GCD}(f_i(\overline{z}),h_j(\overline{z})) = d \wedge \mathrm{GCD}(f_j(\overline{z}),d_i) = d \wedge \mathrm{GCD}(d_i,h_j(\overline{z})) = d\big).$$

Suppose that the gcd-expressions with numbers i and j are of the form ($\mathcal{D}$-1). We can rewrite this condition for $h_i(\overline{z}) = d_iz_i$ and $h_j(\overline{z}) = d_jz_j$ as follows.

If $z_i = z_j$ we get a conjunction

$$\mathrm{GCD}(f_i(\overline{z}),d_jz_j) = \mathrm{GCD}(d_i,d_j)z_i \wedge \mathrm{GCD}(f_j(\overline{z}),d_iz_i) = \mathrm{GCD}(d_i,d_j)z_i.$$

Now let $z_i \neq z_j$. Then (1.27) must have a gcd-expression of the form $\mathrm{GCD}(az_i,bz_j) = h(\overline{z})$. Therefore, $\mathrm{GCD}(z_i,z_j) = \frac{h(\overline{z})}{\mathrm{GCD}(a,b)l}$ for some divisor l of $\mathrm{LCM}(a,b)$ and hence $\mathrm{GCD}(h_i(\overline{z}), h_j(\overline{z}))$ must be equal to $\frac{\mathrm{GCD}(d_i,d_j)k}{\mathrm{GCD}(a,b)l}h(\overline{z})$ for some $k \mid \mathrm{LCM}(d_i,d_j)$.

Define $M_{k,l} = \frac{\mathrm{GCD}(d_i,d_j)k}{\mathrm{GCD}(a,b)l}$ and rewrite condition (b) for the pair (i,j) using the following disjunction:

$$\bigvee_{k|\mathrm{LCM}(d_i,d_j)} \left(\bigvee_{l|\mathrm{LCM}(a,b)} \mathrm{GCD}(h_i(\overline{z}),h_j(\overline{z})) = M_{k,l}h(\overline{z}) \right.$$
$$\left. \wedge\, \mathrm{GCD}(f_i(\overline{z}),h_j(\overline{z})) = M_{k,l}h(\overline{z}) \wedge \mathrm{GCD}(f_j(\overline{z}),h_i(\overline{z})) = M_{k,l}h(\overline{z}) \right).$$

The resulting formula is obviously an $L_{\mathcal{D}}$-formula, and we have thus defined a quasi-QE algorithm $\mathcal{D}$. This concludes the proof. □

Theorem 1 now follows from Theorem 2 and Theorem 3.

1.8 Conclusion and Connections with Chapter 2

The decision problem for the existential theory of the structure $\langle \mathbb{Z}; 0,1, +, -, \leqslant, \mathrm{GCD}\rangle$ was reduced to the decision problem for the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$. Then the decidability of the latter theory was proved. The ideas of both reduction and decidability proof were essentially the same: to isolate a variable and then transform the resulting formula using GCD-Lemma, a generalization of the Chinese remainder theorem. To formalize this idea, we introduced the notion of quasi-quantifier elimination algorithm, and then constructed quasi-QE algorithms $\mathcal{R}$ and $\mathcal{D}$ to solve the two problems above.

Presented algorithm does not use complex arguments and is actually completely described in section 1.2, while the other sections only provide technical details. It is not difficult to extract from our algorithm a decision procedure for the existential theory such structures as $\langle \mathbb{N}; 0, S, | \rangle$ and $\langle \mathbb{Z}; 0, S, \leqslant, \mathrm{GCD}\rangle$, where S stands for the successor function $Sx = x+1$. These structures are interesting, since in their languages we can rewrite system (4). Therefore, there is no polynomial *poly* such that for every $L_{\langle 0,S,|\rangle}$-formula φ, satisfiable over the natural numbers $\mathbb{N}$, there is a satisfying assignment, bounded by $poly(|\varphi|)$, where $|\varphi|$ is the size of the formula φ. The same holds for $L_{\langle 0,S,\leqslant,\mathrm{GCD}\rangle}$-formulas satisfiable over the integers. It is an interesting problem to investigate whether any of these theories is in **NP**. An effort to answer on these questions seems to be a natural approach when we study algorithmic complexity of $\exists\mathrm{Th}\langle \mathbb{Z}; 0,1, +, -, \leqslant, \mathrm{GCD}\rangle$.

The notion of quasi-quantifier elimination can be helpful in attempts to prove decidability of $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, |, P_2\rangle$. A. Sirokofskich remarks [71] that J. Robinson and L. Lipshitz tried to find

an answer to a related question: „J. Robinson asked in a personal communication with L. Lipshitz whether the existential theory of $\mathbb{Z}$ in the language of addition, divisibility and the predicate for powers of 2 is decidable“. Note also that this problem is inter-reducible with the decision problem for the existential Büchi arithmetic of base 2 with divisibility. The latter theory is the existential theory of the structure $\langle \mathbb{N}; 1, +, | , V_2 \rangle$, where V_2 is a binary predicate such that $V_2(x,y)$ if and only if y is the greatest power of 2 that divides x. We see that $V_2(x,y) \Leftrightarrow P_2(y) \wedge y \mid x \wedge 2y \nmid x$ and $P_2(x) \Leftrightarrow V_2(x,x)$. Even in the case when these theories are undecidable, we can further ask whether at least $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, \perp , P_2 \rangle$ is decidable. In order to answer this question it is necessary to understand particularities of decision procedures for $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, \perp \rangle$.

Substituting the relation GCD in Theorem 1 for the coprimeness relation, we considerably simplify Step 1 of algorithm $\mathcal{R}$. In this case, either all gcd-expressions are of the form $\mathrm{GCD}(f(\overline{x}),g(\overline{x})) = d$ for the expressions with coprimeness, or $\mathrm{GCD}(f(\overline{x}),g(\overline{x})) = a\zeta$ for their negations, where $\zeta \geqslant 2$ and a,d are positive integers. Moreover, we can avoid using Greek variables in algorithm $\mathcal{R}$ if we consider only positive existential formulas of the first-order language of the signature $\sigma_\perp = \langle 0,1, +, -, \neq , \mathrm{GCD}_1, \mathrm{GCD}_2, ... \rangle$, where $\mathrm{GCD}_d(x,y) \rightleftharpoons \mathrm{GCD}(x,y) = d$. Similar to the case from Example 1.2.2, the algorithm can be easily transformed into an algorithm which to every positive existential $L_{\sigma_\perp}$-formula assigns an equivalent in $\mathbb{Z}$ positive quantifier-free $L_{\sigma_\perp}$-formula. In the next chapter in this way we obtain a description of every relation, P$\exists$-definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$.

Chapter 2. Positive Existential Definability with Unit, Addition and Coprimeness

> For instance, it is not clear whether one can define the order relation in the existential fragment of $\langle \mathbb{Z}; +, | ,0,1\rangle$, hence we will work with $\langle \mathbb{Z}; +, | , \leqslant ,0,1\rangle$ instead of it, whenever needed.
>
> M. Bozga and R. Iosif [7] (2005)

In this chapter, we consider applications of quasi-quantifier elimination algorithms to some definability problems. The main result is that every relation is positively existentially definable in the structure $\langle \mathbb{Z}; 1, + , \perp\rangle$ if and only if it is positively quantifier-free definable in the structure $\langle \mathbb{Z}; 1, + , - , \neq , \perp ,\mathrm{GCD}_2,\mathrm{GCD}_3,\mathrm{GCD}_4,...\rangle$, where $\mathrm{GCD}_d(x,y) \rightleftharpoons \mathrm{GCD}(x,y) = d$. This implies that the negation of coprimeness and the order relation are not positively existentially definable in $\langle \mathbb{Z}; 1, + , \perp\rangle$. We then obtain three generalizations of the BL-Theorem. At the end of this chapter, we construct quasi-QE algorithms for $\exists\mathrm{Th}\langle \mathbb{Z}; 1, + , - , \leqslant , \perp\rangle$ and for a much more simple positive fragment of this theory.

2.1 Arithmetic of the Integers with Unit, Addition and Coprimeness

When we describe properties of some objects (such as programs with lists [7] or parametric one-counter automata [29]) using formulas of the first-order language with unit, addition, order and divisibility, it is convenient to have any description of the relations, definable in this language. However, apart from some examples, we do not have any significant general results on the existential definability in the structure $\langle \mathbb{Z}; 1, + , - , \leqslant , |\rangle$. In the first chapter we have shown that the graph of the GCD function and its negation are $\exists$-definable (1.4), and thus the coprimeness relation $x \perp y$ together with its negation are also $\exists$-definable. Moreover, since we know that the indivisibility relation is P$\exists$-definable in this structure (1.2), it would be interesting to ask an analogous question: is the negation of coprimeness P$\exists$-definable in $\langle \mathbb{Z}; 1, + , - , \leqslant , \perp\rangle$? M. Bozga and R. Iosif [7, Remark 2 on p. 428] raised another natural question of whether the order relation is $\exists$-definable in the structure $\langle \mathbb{Z}; 1, + , - , |\rangle$.

Among the general results on $\exists$-definability in $\langle \mathbb{Z}; 1, + , - , \leqslant , |\rangle$, we can mention one result by L. Lipshitz [45] who proved that every set $S \subseteq \mathbb{N}$, $\exists$-definable in this structure, is a union of some finite set and (perhaps empty or infinite) union of arithmetic progressions. L. van den Dries and A. Wilkie [23] studied growth properties of functions whose graphs were $\exists$-definable in $\langle \mathbb{Z}; 1, + , - , \leqslant , |\rangle$, however these results do not seem helpful answering the aforementioned definability questions.

Constructing quantifier elimination algorithms is a classical approach to the problem of describing the predicates, definable in some structure $\langle M; \sigma \rangle$. Let us only mention some well-known results related to the structures considered in this chapter: the integer arithmetic with unit, addition and order, and the arithmetic of the p-adic integers with unit, addition, equality and strict divisibility $x \parallel y \rightleftharpoons v_p(x) < v_p(y)$. In the first case, M. Presburger [59] (see also [30]) showed that every relation is definable in $\langle \mathbb{Z}; 1, +, -, \leqslant \rangle$ if and only if it is quantifier-free definable in $\langle \mathbb{Z}; 1, +, -, \leqslant, 2 \mid, 3 \mid, 4 \mid, ... \rangle$ with unary predicate symbols $d \mid$ for divisibility by constants $d \geqslant 2$. V. Weispfenning [83] and T. Sturm [78] presented quantifier elimination algorithms for the structure $\langle \mathbb{Q}_p; 1, +, -, =, \| \rangle$ and thus obtained a characterization of the predicates, definable in this structure, i.e., these predicates are exactly the predicates, which are definable in this structure by some quantifier-free formulas.

This pioneering paper by V. Weispfenning [83] played a key role in the intensive development of quantifier elimination techniques using the so-called virtual substitution. The implementation of these methods in practice was initiated by the students of V. Weispfenning, mainly by A. Dolzmann and T. Sturm. They developed the RedLog [22] package for the computer algebra system REDUCE, which has found a lot of applications and continues to evolve nowadays (see the overview by T. Sturm [80], as well as the RedLog project page[1]). In particular, RedLog implements quantifier elimination in the linear theory of the p-adic numbers; for Presburger arithmetic it uses quantifier elimination algorithms developed by A. Lazaruk and T. Sturm [39; 40].

Analogues of quantifier elimination algorithm for Presburger arithmetic are also used for other structures, as for example, in the recent work of P. Backeman, P. Rummer and A. Zeljic [2] on the elimination of quantifiers in machine arithmetic (bit-vector arithmetic). Note that while there is a well-known relationship between operations over bit-vectors and over the 2-adic numbers [35], quantifier elimination algorithms in linear theories of the 2-adic numbers (to the knowledge of the author) do not seem to attract significant interest in the formal verification community.

Another important example is the following result, obtained by V. Weispfenning [84] in 1999. Using quantifier elimination, he proved that the sets, definable in the structure $\langle \mathbb{Q}; 1, +, -, =, <, Int \rangle$, where Int is a unary predicate symbol for the property «to be an integer», are exactly the sets, quantifier-free definable in $\langle \mathbb{Q}; 1, +, -, [\,], \{c\cdot\}_{c \in \mathbb{Q}}, =, < \rangle$. Here, $[\,]$ is a unary function symbol for the integer part operation and $c\cdot$ are unary function symbols for multiplication by rational constants c. Note that this result was already known to C. Smorynski in 1991, but he probably did not consider this proposition important enough for publication and included it in his book «Logical Number Theory I» as an exercise [73, III.4, Exercise 15].

In all these cases it was sufficient to construct a positive quantifier-free formula $\psi(\overline{y})$, which was equivalent in the corresponding structure to a given positive existential formula (P$\exists$-formula) $\exists x \varphi(x, \overline{y})$, as every negated atomic formula could be defined by some positive quantifier-free formula. As a corollary, we obtain decidability of the elementary theories of these structures.

In the same paper V. Weispfenning [84] remarks: «By way of contrast, quantifier elimination definitely breaks down if one admits scalar multiplication by a real parameter or integer divisibility in the language» and in connection with the BL-Theorem, he asks whether P$\exists$Th$\langle \mathbb{R}; 1, +, -, [\,], | \rangle$

[1] https://www.redlog.eu/references/

is decidable, where $x \mid y \rightleftharpoons \exists z(Int(z) \wedge y = xz)$. The fact that we cannot eliminate quantifiers in the case when we add an integer divisibility relation to the signature is a consequence of a simple remark by L. Lipshitz [45]. He showed that every enumerable set is definable in the structure $\langle \mathbb{N}; 1, +, | \rangle$ using a formula with a single universal quantifier that follows a block of existential quantifiers: $\exists ... \exists \forall$. Indeed, it is not difficult to show (a similar reasoning will be used in the proof of Corollary 3.4.1.1) that this fact follows from the definability of the graph of squaring function using the following universal formula:

$$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z(x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z). \tag{2.1}$$

Thus, the $\forall\exists$- and $\exists\forall$-theories of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ turn out to be undecidable. Note that if we introduce the relation of divisibility by two consecutive numbers $x \,{}^{S}|\, y \rightleftharpoons x \mid y \wedge x+1 \mid y$ then the formula (2.1) almost immediately implies definability of the graph of squaring function in the structure $\langle \mathbb{N}; 1, +, {}^{S}| \rangle$. We turn to the problems of definability in structures with the relation ${}^{S}|$ in Chapter 3.

Due to this negative result, an important problem is to find the widest possible decidable fragments of $\forall\exists \mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. In the preprint [57], G.A. Pérez and R. Raha (building on the works by M. Bozga and R. Iosif [7] and especially on the papers by C. Haase, S. Kreutzer, J. Ouaknine, J. Worrell [60] and A. Lechner [43]) defined a family of $\forall\exists$-formulas in the language with unit, addition, and divisibility; proved its decidability and used this result to study decidability and complexity of synthesis problems for parametric one-counter automata (P1CA). Note that decidability of the reachability problem for P1CA was established in 2009 by C. Haase et al. [60] using the BL-Theorem. It turns out that the reachability property for P1CA can be expressed by an existential $L_{\langle 1,+,-,\leqslant,| \rangle}$-formula and, in addition, there is an inverse reduction [29, Lemma 4.2.1].

Considering the relationship between automata and definability problems for arithmetic structures, we can note the following. In some structures, such as $\langle \mathbb{N}; 0,1, +, P_k, = \rangle$ or in k-Büchi arithmetic $\langle \mathbb{N}; 0,1, +, V_k, = \rangle$, where $k \geqslant 2$ and $V_k(x,y) \Leftrightarrow (P_k(y) \wedge \mathrm{GCD}(ky,x) = y)$, definability problems can successfully be solved using automata-theoretic tools. According to a well-known theorem of R.J. Büchi [10; 47], every relation over the natural numbers encoded in positional number systems base $k \geqslant 2$ is recognizable by a deterministic k-automaton if and only if this relation is definable in the structure $\langle \mathbb{N}; 0,1, +, V_k, = \rangle$. However, as was shown by A.L. Semënov [68], there are relations, definable in this structure but not in $\langle \mathbb{N}; 0,1, +, P_k, = \rangle$. In 1992, R. Villemaire [82] proved that every relation, which is definable in k-Büchi arithmetic, is also definable in this structure using some $\exists\forall\exists$-formula. C. Haase and J. Różycki [32] note that a slight modification of Villemaire's proof will allow us to construct $\forall\exists$-formula, however, existential Büchi arithmetic turns out to be less expressive.

Denote by $L_{k\text{-}BA}$ the language of Büchi arithmetic of base k. The aforementioned descriptions of all the relations, definable in k-Büchi arithmetic, were obtained as follows: by Büchi's theorem, for every $L_{k\text{-}BA}$-formula $\varphi(x_1,...,x_n)$, we can constructively find a deterministic finite k-automaton $\mathcal{A}$ that recognizes exactly those $(a_1,...,a_n) \in \mathbb{N}^n$ such that the formula $\varphi(a_1,...,a_n)$ is true. Next, for every such automaton $\mathcal{A}$ we construct a $\forall\exists L_{k\text{-}BA}$-formula $\psi(x_1,...,x_n)$ that encodes

the computation of $\mathcal{A}$, i.e., this formula ψ is now true for some $(a_1,...,a_n)$ if and only if $\mathcal{A}$ accepts $(a_1,...,a_n)$. Therefore, informally speaking, in the case of k-Büchi arithmetic, the *elimination form* of a given formula is the k-automaton that was constructed for this formula. Probably an automata-theoretic approach to the arithmetic of the natural numbers with unit, addition and divisibility [11; 29; 42; 60] will yield us as significant definability results as in the case of Büchi arithmetic (see the reviews [5; 47]). However, in this thesis we will only use an arithmetic approach to study definability, and we further will not return to an automata-theoretic approach.

Considering definability and decidability questions from a practical point of view, it is not obvious whether quantifier elimination or automata-theoretic approach to arithmetic theories is more successful. Let us quote a remark of C. Haase [30] regarding decision procedures for Presburger arithmetic: «While to the best of the author's knowledge the automata-based approach is not widely applied in practice these days, it is worth mentioning that it can empirically be more efficient compared to quantifier elimination. For instance, even on small instances of the Frobenius problem presented in the introduction, a straight-forward implementation of the automata-based decision procedure outperforms the quantifier-elimination procedure implemented in the SMT-solver Z3 [54] by orders of magnitudes». In the last statement, C. Haase refers to an informal discussion of the problem with M. Blondin.

It does not seem to be an easy task to understand how we can use quasi-quantifier elimination algorithms from Chapter 1 to describe all the relations, existentially definable in the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. As stated above, this class coincides with all P$\exists$-definable relations. However, in the case when the second sort of variables in a quasi-quantifier elimination algorithm is empty, as in the case considered in Example 1.2.2, it is possible to apply quantifier elimination to describe the predicates that are definable by existential formulas of the language of this algorithm. It thus seems natural to consider intermediate languages between $\exists L_{\langle 1,+,-,\leqslant \rangle}$ and $\exists L_{\langle 1,+,-,\leqslant,| \rangle}$, and then construct quasi-quantifier elimination algorithms over $\mathbb{Z}$ for these languages. In this chapter we study P$\exists$-definability in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$ and some related questions.

In 1989, D. Richard [63] proved that the graph of multiplication is first-order definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$. The main difficulty in proving this result was to define the order relation (or equivalently, the set of non-negative integers), since definability of every arithmetical relation in $\langle \mathbb{N}; 1, +, \perp \rangle$ was earlier proved by A. Woods [85] (moreover, in two different ways). Woods also noted that another proof was independently obtained by J. Robinson but remained unpublished.

The study of arithmetical definability problems, in particular for the structures with coprimeness relation, was initiated by J. Robinson [65]. She proved that every arithmetical relation, i.e., definable in the structure $\langle \mathbb{N}; +, \cdot, = \rangle$, is definable in the structure $\langle \mathbb{N}; S, | \rangle$, where S is a unary function symbol that corresponds to the successor function $x \mapsto x + 1$, and $|$ stands for the binary divisibility relation. Such kind of structures were called *Def-complete* by I. Korec [36], who presented a list of various Def-complete structures. Replacing the divisibility relation by coprimeness, J. Robinson asks whether $\langle \mathbb{N}; S, \perp \rangle$ is Def-complete, or whether we can at least prove that the elementary theory of the structure $\langle \mathbb{N}; S, \perp \rangle$ is undecidable. An positive answer to the last question was independently given by D. Richard [61] and A. Woods [85], while Def-completeness remains an open problem. It is well-known that this problem is closely related to the

so-called Woods-Erdös conjecture (see an overview of the main results of A. Woods by P. Cégielski and D. Richard [17]). The definition of Def-completeness, similar definitions and examples will be given in Chapter 3.

The main result of this chapter is the proof that every relation, which is P$\exists$-definable in $\langle \mathbb{Z}; 1, +, \perp \rangle$, is positively quantifier-free definable in the structure $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \ldots \rangle$, and vice versa. Here GCD_d for every $d \geqslant 2$ is a binary predicate symbol for the relation $\mathrm{GCD}_d(x,y) \rightleftharpoons \mathrm{GCD}(x,y) = d$. First, in Section 2.2 we show why the signature must be extended in order the elimination be possible. Then in Section 2.3 for every P$\exists$-formula $\exists x \varphi(x, y_1, \ldots, y_n)$ of the language with thus extended signature we construct an equivalent in $\mathbb{Z}$ positive quantifier-free formula of the same language. This construction is based on GCD-Lemma and defines a quasi-quantifier elimination algorithm. Note that rewriting the fourth condition of GCD-Lemma for each prime p we can see some traces of the quantifier elimination algorithms for the structure $\langle \mathbb{Q}_p; 1, +, -, =, \| \rangle$.

In Section 2.4 we prove that the negation of the coprimeness relation is not P$\exists$-definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$, since otherwise $\mathrm{Th}\langle \mathbb{Z}; 1, +, \perp \rangle$ would be decidable. Then close results will be obtained on P$\exists$-definability for structures $\langle \mathbb{N}; S, \perp \rangle$ and $\langle \mathbb{Q}; 1, +, -, \{c\cdot\}_{c \in \mathbb{Q}}, \perp \rangle$. Combining the main theorem of this chapter with the BL-Theorem, in Section 2.5 we construct a decidable fragment of $\forall\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. We also show how to apply GCD-Lemma in order to generalize the decidability result by G.A. Pérez and R. Raha [57]. In the same section we obtain another generalization of the BL-Theorem, namely, the existential theory of the structure $\langle \mathbb{R}; 1, +, -, [\,], <, | \rangle$ turns out to be decidable. This gives a positive answer to a question by V. Weispfenning [84, Remark, p.135].

At the end of this chapter we construct quasi-QE algorithms for the positive case and for the general case of the existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$. The quantifier elimination algorithm from the main theorem of Section 2.3 and these two algorithms can be considered as three cases, which successively generalize each other when the signature is extended by the order relation and the negation of the coprimeness relation. These constructions demonstrate the following. Quasi-QE algorithms turn to be a convenient tool for constructing decision procedures for the theories that are intermediate between existential arithmetic of addition and $\exists$-arithmetic with addition and divisibility. Note that for $\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant \rangle$ the strong form of the LS-Lemma almost immediately yields an algorithm from the class **NP** (see [26] and [42, Section 2.3, Corollary 2]). In addition, these algorithms will show significant differences between these intermediate P$\exists$-theories when we extend the signatures.

2.2 Positive Quantifier-Free Undefinability Results

In this section, we show that in order to apply quantifier elimination in the case of positive existential formulas, the signature of the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$ must be extended with some

P∃-definable predicates. The following lemma gives us the main examples of the relations, P∃-definable in this structure.

Lemma 2.2.1. *The relations $x = 0$, $y = -x$, $x = y$, $x \neq 0$, $x \neq y$, and* $\mathrm{GCD}(x,y) = d$ *for every integer $d \geqslant 2$ are positively existentially definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$.*

Proof. For the first two relations, we have the following quantifier-free definitions: $x = 0 \Leftrightarrow x+1 \perp x+1 \wedge 3 \perp x+2$ and $y = -x \Leftrightarrow x + y = 0$.

The formula $\exists t\,(x \perp t \wedge x \perp t+4)$ defines the relation $x \neq 0$. It is obviously false when $x = 0$. If we suppose that $x \neq 0$, then there is a finite set P_x of prime divisors of x. To construct t, it is sufficient to use the Chinese remainder theorem to solve the following system of congruences:

$$t \equiv 1(\mathrm{mod}\ 2) \wedge t \equiv 1(\mathrm{mod}\ 3) \wedge \bigwedge_{p \in P_x \setminus \{2,3\}} t \equiv 2(\mathrm{mod}\ p).$$

Indeed, for every prime divisor p of the integer x, we have $p \nmid t \wedge p \nmid t+4$.

Thus we get $x = y \Leftrightarrow \exists t(t = -y \wedge x + t = 0)$ and $x \neq y \Leftrightarrow \exists t(t = -y \wedge x + t \neq 0)$. The relation $\mathrm{GCD}(x,y) = d$ is definable by the formula $\exists u \exists v\,(x = du \wedge y = dv \wedge u \perp v)$. □

It is convenient to include in our signature unary function symbol '$-$', and further suppose that every term is a linear polynomial with integer coefficients. The equality relation is now quantifier-free definable in $\langle \mathbb{Z}; 1, +, -, \perp \rangle$ and dis-equality $\neq$ is quantifier-free definable in $\langle \mathbb{Z}; 1, +, -, \neq 0, \perp \rangle$. In the following two propositions we will show that the signature of $\langle \mathbb{Z}; 1, +, -, \perp \rangle$ must be extended to define every relation from Lemma 2.2.1 by some quantifier-free formula.

Before we begin with questions of quantifier-free undefinability, let us more formally describe the standard transformation, which we use in Section 1.4. Every expression of the form $\mathrm{GCD}(f(\overline{y})+ax, g(\overline{y}) + bx) = d$, where $a, b \neq 0$, and $f(\overline{y})$, $g(\overline{y})$ are linear polynomials with integer coefficients, can be rewritten using Euclid's algorithm such that the coefficient of the variable x is non-zero only in one of the polynomials of the expression. Let $a > b > 0$ and $a = qb + r$, where $r \in [0, b)$. Then

$$\mathrm{GCD}(f(\overline{y}) + ax, g(\overline{y}) + bx) = d \Leftrightarrow$$
$$\mathrm{GCD}(f(\overline{y}) - qg(\overline{y}) + rx, g(\overline{y}) + bx) = d.$$

Repeating this process until one of the coefficients of x becomes a divisor of the other and then again applying the specified step, we obtain a formula of the form $\mathrm{GCD}(\widetilde{f}(\overline{y}), \widetilde{g}(\overline{y}) + cx) = d$.

Lemma 2.2.2. *For every linear polynomials with integer coefficients $f(\overline{y}) + ax$, $g(\overline{y}) + bx$ we can construct such linear polynomials $\widetilde{f}(\overline{y})$ and $\widetilde{g}(\overline{y}) + cx$ that* $\mathrm{GCD}(f(\overline{y}) + ax, g(\overline{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\overline{y}), \widetilde{g}(\overline{y}) + cx)$.

Proposition 2.2.1. *The relation $x \neq 0$ is not positively quantifier-free definable in the structure $\langle \mathbb{Z}; 1, +, -, \perp \rangle$.*

Proof. Assume that there is a formula

$$\varphi(x) \rightleftharpoons \bigvee_{j\in J}\left(\bigwedge_{i\in I_j} a_i \perp b_i + c_i x\right),$$

where every $c_i > 0$, that defines the relation $x \neq 0$. Then $\varphi(0)$ must be false; therefore, for every $j \in J$ there is an index $i \in I_j$ such that $a_i \not\perp b_i$. This index will be denoted by i_j. If for all $j \in J$ we have $a_{i_j} = 0$, then the formula $\varphi(x)$ is obviously false for every $x > \max\limits_{j\in J} |b_{i_j}| + 1$. For the case when at least one of the numbers a_{i_j} is non-zero, define $A = \prod\limits_{j\in J\wedge a_{i_j}\neq 0} a_{i_j}$. We see that A is positive, however $\neg\varphi(A)$. This contradicts the definition of φ. □

We now prove that the extension of the signature by a predicate symbol for dis-equality is still not sufficient.

Proposition 2.2.2. *The relation* GCD(x,y) $= d$ *for every fixed integer* $d \geqslant 2$ *is not positively quantifier-free definable in the structure* $\langle \mathbb{Z}; 1, +, -, \neq, \perp\rangle$.

Proof. We are going to show that the statement is already true for the relation $p \parallel x \rightleftharpoons p \mid x \wedge p^2 \nmid x$ for any prime p. This relation is a special case of the formula GCD(x,y) $= d$ for $d = p$ and $y = p^2$.

Suppose we have for the relation $p \parallel x$ the following formula:

$$\varphi(x) \rightleftharpoons \bigvee_{j\in J}\left(\bigwedge_{i\in I_j} a_i \perp b_i + c_i x \wedge \bigwedge_{i\in K_j} x \neq d_i\right).$$

Let D be the maximum of all the numbers d_i from dis-equalities of the formula. It is clear that for any $x > D$ we have $\varphi(x) \Leftrightarrow \bigvee\limits_{j\in J}\bigwedge\limits_{i\in I_j} a_i \perp b_i + c_i x$. Choose $k > 1$ such that $p^k > D$. Then the formula $\varphi(p^k)$ must be false. We are going to construct an integer A such that $p \parallel A$, but at the same time $\neg\varphi(A)$.

Since $\neg\varphi(p^k)$, for every $j \in J$ it is true that for at least one index $i \in I_j$ we have $a_i \not\perp b_i + c_i p^k$. Denote the corresponding index i_j for every $j \in J$. Split the index set J into two sets J_1 and J_2, the first of which will contain such indexes that $p \nmid a_{i_j} \vee p \nmid b_{i_j}$, and the other indexes will form J_2, i.e., those j with $p \mid a_{i_j} \wedge p \mid b_{i_j}$. We see that for any $x > D$ if $p \mid x$, then $\varphi(x) \Leftrightarrow \bigvee\limits_{j\in J_1}\bigwedge\limits_{i\in I_j} a_i \perp b_i + c_i x$.

Let $a_{i_j} = p^{\alpha_j}\widetilde{a_{i_j}}$, where $\widetilde{a_{i_j}} \perp p$ for every $j \in J_1$. Define $A = p^k + p \cdot \prod\limits_{j\in J_1} \widetilde{a_{i_j}}$. It is clear that $p \parallel A$, but at the same time for every $j \in J_1$ we have the following chain of equalities:

$$\mathrm{GCD}(a_{i_j}, b_{i_j} + c_{i_j}p^k) = \mathrm{GCD}(\widetilde{a_{i_j}}, b_{i_j} + c_{i_j}p^k) = \mathrm{GCD}(\widetilde{a_{i_j}}, b_{i_j} + c_{i_j}A).$$

The first equality follows from the fact that for $j \in J_1$, if $\alpha_j \neq 0$ then $p \perp b_{i_j}$, and hence since $k > 1$, $b_{i_j} + c_{i_j}p^k$ is not divisible by p. As the residue class of A modulo a_{i_j} is p^k for every $j \in J_1$, we obtain the second equality.

Since $a_{i_j} \not\perp b_{i_j} + c_{i_j}p^k$, we have $a_{i_j} \not\perp b_{i_j} + c_{i_j}A$ and hence $\neg\varphi(A)$. □

The relation $p \parallel x$ is obviously quantifier-free definable in $\langle \mathbb{Z}; 1, +, -, 2\mid, 3\mid, 4\mid, ... \rangle$ using the formula $p \mid x \wedge p^2 \nmid x$. Moreover, for every fixed integer a such that $a = cd$ for some integer c, the relation $\mathrm{GCD}(a,x) = d$ is definable by the formula $\bigvee\limits_{k\perp c \wedge 1 \leqslant k \leqslant c} a \mid x - dk$. Indeed, it is sufficient and necessary for the residue class of x modulo a to be divisible by d and coprime with c.

It might be an interesting question whether $\mathrm{GCD}(x,y) = d$ for $d \geqslant 2$ is quantifier-free definable in $\langle \mathbb{Z}; 1, +, -, \perp, 2\mid, 3\mid, 4\mid, ... \rangle$, but it will be convenient for us to use further simultaneously with coprimeness the relations $\mathrm{GCD}(x,y) = d$ for every $d \geqslant 2$.

2.3 The Main Definability Result

In order to prove that after the extension of the signature $\langle 1, +, -, \perp \rangle$ by the predicate symbols for the relations from Propositions 2.2.1 and 2.2.2 there will be no analogues examples of quantifier-free undefinablilty, we use GCD-Lemma from Section 1.2.2. For convenience we recall GCD-Lemma, which is a criterion of solvability in the integers of systems of the form

$$\bigwedge_{i\in[1..m]} \mathrm{GCD}(a_i, b_i + x) = d_i. \tag{2.2}$$

Lemma 2.3.1 (GCD-Lemma)**.** *For the system (2.2) with $a_i, b_i, d_i \in \mathbb{Z}$, $a_i \neq 0$, and $d_i > 0$ for every $i \in [1..m]$, we define for every prime p the integer $M_p = \max\limits_{i\in[1..m]} v_p(d_i)$ and the index sets $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ and $I_p = \{i \in J_p : v_p(a_i) > M_p\}$.*

Then (2.2) has a solution in $\mathbb{Z}$ if and only if the following conditions simultaneously hold:

(i) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$

(ii) $\bigwedge\limits_{i,j\in[1..m]} \mathrm{GCD}(d_i, d_j) \mid b_i - b_j$

(iii) $\bigwedge\limits_{i,j\in[1..m]} \mathrm{GCD}(a_i, d_j, b_i - b_j) \mid d_i$

(iv) For every prime $p \leqslant m$ and every $I \subseteq I_p$ such that $|I| = p$ there are such $i,j \in I$, $i \neq j$ that $v_p(b_i - b_j) > M_p$.

Fix the signature $\sigma = \langle 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, ... \rangle$. By applying Lemma 2.3.1, we will show how to eliminate an existential quantifier in a P$\exists L_\sigma$-formula. The following theorem will be intensively used in Sections 2.4 and 2.5.

Theorem 4. *There is an algorithm assigning to every L_σ-formula of the form $\exists x \varphi(x, \overline{y})$, where $\varphi(x, \overline{y})$ is positive quantifier-free, a positive quantifier-free L_σ-formula $\psi(\overline{y})$ that is equivalent to $\exists x \varphi(x, \overline{y})$ in $\mathbb{Z}$.*

Proof. Taking into account Lemma 2.2.2, we need to show how to construct for a formula of the form

$$\exists x \left(\bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{y}), g_i(\overline{y}) + c_i x) = d_i \wedge \bigwedge_{i\in[m+1..l]} f_i(\overline{y}) \neq c_i x \right) \tag{2.3}$$

an equivalent in $\mathbb{Z}$ quantifier-free formula $\psi(\overline{y})$. Here, $f_i(\overline{y})$ and $g_i(\overline{y})$ are linear polynomials with integer coefficients and $c_i > 0$ for every $i \in [1..m]$. Let $\varphi(x, \overline{y})$ denote the matrix of the formula (2.3). As in the first chapter, expressions of the form $\mathrm{GCD}(f(\overline{z}),g(\overline{z})) = d$ will be further called *gcd-expressions*.

Note that we can without loss of generality assume that all c_i equal 1 as we can compute $C = \underset{i=1..l}{\mathrm{LCM}}(c_i)$, multiply every expression with index $i \in [1..l]$ by $\frac{C}{c_i}$, replace all occurrences of Cx by $\widetilde{x}$ and adjoin the gcd-expression $\mathrm{GCD}(C,\widetilde{x}) = C$.

Our goal now is to construct a formula $\psi_{GCD}(\overline{y})$ such that

$$\exists x \varphi(x,\overline{y}) \Leftrightarrow \bigvee_{i\in[1..m]} \left(f_i(\overline{y}) = 0 \wedge \bigvee_{s\in\{-1,1\}} \varphi(s \cdot d_i - g_i(\overline{y}),\overline{y}) \right) \vee \left(\bigwedge_{i\in[1..m]} f_i(\overline{y}) \neq 0 \wedge \psi_{GCD}(\overline{y}) \right).$$

Here we have separately considered the cases for which the first arguments of gcd-expressions are equal to zero and hence the value of x can be immediately determined. To get an L_σ-formula we rewrite linear equalities using Lemma 2.2.1.

For the last case note that since $\bigwedge\limits_{i\in[1..m]} f_i(\overline{y}) \neq 0$, according to Remark 1.3.1, the existence of a solution to the subsystem of gcd-expressions of $\varphi(\overline{y}, x)$ implies the existence of such a solution that simultaneously satisfies the subsystem of dis-equalities $\bigwedge\limits_{i\in[m+1..l]} f_i(\overline{y}) \neq c_i x$.

Now consider the system $\bigwedge\limits_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{y}), g_i(\overline{y}) + x) = d_i$ with non-zero first arguments in every gcd-expression. We will show that the fact that such system has a solution in $\mathbb{Z}$ can be rewritten as a certain quantifier-free L_σ-formula.

Consider sequentially the conditions from Lemma 2.3.1. Expressions from (i) can be rewritten using $\mathrm{GCD}(d_i,f_i(\overline{y})) = d_i$ for every $i \in [1..m]$. For condition (ii) denote $D_{i,j} = \mathrm{GCD}(d_i,d_j)$ to use an analogous formula:

$$\mathrm{GCD}(D_{i,j},g_i(\overline{y}) - g_j(\overline{y})) = D_{i,j}$$

for every index pair $i,j \in [1..m]$.

For condition (iii) we have a conjunction over all pairs of indexes $i,j \in [1..m]$ of expressions of the form

$$\mathrm{GCD}\left(\mathrm{GCD}\left(f_i(\overline{y}), d_j\right), g_i(\overline{y}) - g_j(\overline{y})\right) \mid d_i.$$

We see that this formula is equivalent to the disjunction

$$\bigvee_{a|d_j} \left(\mathrm{GCD}(f_i(\overline{y}), d_j) = a \wedge \bigvee_{d|d_i} \mathrm{GCD}(a,g_i(\overline{y}) - g_j(\overline{y})) = d \right).$$

Rewriting condition (iv) more formally, we get an expression of the following form:

$$\bigwedge_{p\in\mathbb{P}\wedge p\leqslant m}\left(\bigwedge_{I\subseteq J_p\wedge|I|=p}\left(\bigvee_{i\in I}v_p(f_i(\overline{y}))\leqslant M_p\right.\right.$$
$$\left.\left.\vee\bigvee_{i,j\in I\wedge i\neq j}\mathrm{GCD}(p^{M_p+1},g_i(\overline{y})-g_j(\overline{y}))=p^{M_p+1}\right)\right). \tag{2.4}$$

In every disjunction from (2.4) the corresponding index set I is either not a subset of I_p, or there are such $i,j\in I\wedge i\neq j$ that $v_p(g_i(\overline{y})-g_j(\overline{y}))>M_p$. Since we have already required in (i) that $\mathrm{GCD}(d_i,f_i(\overline{y}))=d_i$ for every index $i\in[1..m]$, then instead of $v_p(f_i(\overline{y}))\leqslant M_p$ it is enough to require $v_p(f_i(\overline{y}))=M_p$. This relation can be expressed by the formula $\mathrm{GCD}(p^{M_p+1},f_i(\overline{y}))=p^{M_p}$.

Thus we have constructed the formula $\psi_{GCD}(\overline{y})$ and hence the desired formula $\psi(\overline{y})$. □

This algorithm is essentially a quasi-quantifier elimination algorithm for the case when the sort of variables S_2 is empty, and the set of formulas of elimination form is equal to the language of this algorithm. Here, the language of such algorithm is the set of all positive quantifier-free L_σ-formulas. Combining Theorem 4 and Lemma 2.2.1, we get a characterization of all relations, P$\exists$-definable in $\langle\mathbb{Z};1,+,\perp\rangle$.

Theorem 5. *A relation is positively existentially definable in the structure $\langle\mathbb{Z};1,+,\perp\rangle$ iff it is positively quantifier-free definable in the structure $\langle\mathbb{Z};1,+,-,\neq,\perp,\mathrm{GCD}_2,\mathrm{GCD}_3,\mathrm{GCD}_4,...\rangle$.*

We will demonstrate quantifier elimination from Theorem 4 via the following example. In the resulting quantifier-free formula it is convenient to use the equality relation since by Lemma 2.2.1 it is quantifier-free definable in the structure $\langle\mathbb{Z};1,+,-,\perp\rangle$.

Example 2.3.1. *Consider the formula*

$$\exists x\,(2x+y\perp 3y+z\ \wedge\ x+3z\perp 2x+3\ \wedge\ 5x+3y\perp 2x+y+2z+1)\,. \tag{2.5}$$

It is convenient to supplement our quantifier elimination algorithm with some simplifications, similar to those applied in the case of Presburger arithmetic in RedLog package for computer algebra system REDUCE [21]. In particular, we assume that after quantifier elimination, the resulting formula satisfies the following conditions:

(1) Every linear equality has form $l(\overline{x})=0$ and the greatest common divisor of coefficients of $l(\overline{x})$ is one.

(2) Every linear equality without any integer satisfying assignments evaluates to false*. For example, applying* rlqe *function to the formula $\varphi:=2x+1=0$ we obtain* false*.*

(3) Every gcd-expression has form $\mathrm{GCD}(f(\overline{x}),g(\overline{x}))=d$, where the greatest common divisor of all the coefficients from $f(\overline{x})$ and $g(\overline{x})$ is equal to one. That is, in the case when the greatest common divisor of the coefficients of the linear polynomials does not divide d, this gcd-expression evaluates to false*.*

(4) Every gcd-expression of the form $\mathrm{GCD}(1,g(\overline{x}))=d$ or $\mathrm{GCD}(f(\overline{x}),1)=d$ evaluates to true *if $d=1$, and to* false *otherwise.*

(5) In every linear expression $l(\overline{x})$, the variables $\overline{x}$ are sorted in lexicographic order and the first non-zero coefficient is positive.

We first rewrite (2.5) such that this formula has form (2.3) and then apply the transformations from Lemma 2.2.2:

$$\exists x\,(\ \mathrm{GCD}(3y+z,y+2x)=1\ \wedge\ \mathrm{GCD}(-6z+3,3z+x)=1 \\ \wedge\ \mathrm{GCD}(y-10z-5,y-4z-2+x)=1\ )\,. \tag{2.6}$$

Now we construct an equivalent formula, where coefficients of the eliminated variable are equal to 1*. Immediately replace the new variable by x.*

$$\exists x \begin{cases} \mathrm{GCD}(3y+z, & y+ & x)=1 \\ \mathrm{GCD}(12z-6, & 6z+ & x)=2 \\ \mathrm{GCD}(2y-20z-10, & 2y-8z-4+ & x)=2 \\ \mathrm{GCD}(2, & & x)=2 \end{cases} \tag{2.7}$$

It is convenient to consider the resulting quantifier-free formula as a combination of the following three formulas: $\varphi_1(y,z)\vee\varphi_2(y,z)\wedge\varphi_3(y,z)$. The formula $\varphi_1(y,z)$ corresponds to the case when the first argument of one of the gcd-expressions from (2.7) equals zero. The second and the third formulas are the results of application of GCD-Lemma when in every gcd-expression the first argument is non-zero. Here we first rewrite conditions (i)–(iii) in $\varphi_2(y,z)$ and then separately condition (iv) by the formula $\varphi_3(y,z)$.

Since the equations $12z-6=0$ and $2=0$ have no integer solutions, in $\varphi_1(y,z)$ we only handle the cases $3y+z=0$ and $2y-20z+10=0$. By substituting in the first case either $-y+1$ or $-y-1$ for x, and either $-2y+8z+6$ or $-2y+8z+2$ for x in the second case, we obtain the following:

$$\begin{aligned} \varphi_1(y,z) \rightleftharpoons 3y+z=0\wedge\Big(\big(&\mathrm{GCD}(12z-6,y-6z-1)=2\ \wedge\ \mathrm{GCD}(2y-20z-10,y-8z-3)=2 \\ &\wedge\ \mathrm{GCD}(2,y-1)=2\big)\vee \\ \vee\big(&\mathrm{GCD}(12z-6,y-6z+1)=2\ \wedge\ \mathrm{GCD}(2y-20z-10,y-8z-5)=2 \\ &\wedge\ \mathrm{GCD}(2,y+1)=2\big)\Big)\vee \\ \vee\, y-10z-5=0\wedge\Big(\big(&\mathrm{GCD}(3y+z,y-8z-6)=1\ \ \wedge\ \mathrm{GCD}(6z-3,y-7z-3)=1 \\ \vee\big(&\mathrm{GCD}(3y+z,y-8z-2)=1\ \ \wedge\ \mathrm{GCD}(6z-3,y-7z-1)=1\big)\Big). \end{aligned}$$

In the case when $3y+z\neq 0\wedge y-10z-5\neq 0$, we can apply GCD-Lemma. Since (2.6) contains only coprimeness relations, formula (2.7) obviously satisfy conditions (i) and (ii). Thus,

in order to construct formula $\varphi_2(y,z)$*, we must rewrite only (iii).*

$$\begin{aligned}\varphi_2(y,z) \rightleftharpoons 3y+z\neq 0 \wedge y-10z-5\neq 0 \wedge \big(&\mathrm{GCD}(3y+z,2)=1 \vee\\ &\vee \mathrm{GCD}(3y+z,2)=2 \wedge \mathrm{GCD}(2,y-6z)=1\big)\wedge\\ &\big(\mathrm{GCD}(3y+z,2)=1 \vee\\ &\vee \mathrm{GCD}(3y+z,2)=2 \wedge \mathrm{GCD}(2,y-8z-4)=1\big)\wedge\\ &\big(\mathrm{GCD}(3y+z,2)=1 \vee\\ &\vee \mathrm{GCD}(3y+z,2)=2 \wedge \mathrm{GCD}(2,y)=1\big).\end{aligned}$$

Here we see that (iii) is always satisfied for the second and third, for the second and fourth, for the third and forth gcd-expressions.

Finally, we are going to rewrite condition (iv). For $p=2$*, we have* $M_2=1$*,* $J_2=\{2,3,4\}$*, and* I_2 *can only contain indexes* 2 *and* 3*. When* $p=3$*,* $M_3=0$ *and thus* $J_3=\{1,2,3,4\}$*, and the only possible subset of* I_3 *with three elements is* $I=\{1,2,3\}$*. Now we obtain the following formula:*

$$\begin{aligned}\varphi_3(y,z) \rightleftharpoons \big(&\mathrm{GCD}(2,6z-3)=1 \vee \mathrm{GCD}(2,y-10z-5)=1 \vee \mathrm{GCD}(2,y-7z-2)=2\big)\wedge\\ &\big(\mathrm{GCD}(3,3y+z)=1 \vee \mathrm{GCD}(3,2y-20z-10)=1 \vee\\ &\vee \mathrm{GCD}(3,y-6z)=3 \vee \mathrm{GCD}(3,2y-14z-4)=3 \vee \mathrm{GCD}(3,y-8z-4)=3\big).\end{aligned}$$

We conclude that existential formula (2.5) is equivalent over the integers to the quantifier-free formula $\varphi_1(y,z)\vee\varphi_2(y,z)\wedge\varphi_3(y,z)$*.*

2.4 Some Corollaries and Related Definabililty Problems

Having a description of the relations, P$\exists$-definable in the structure $\langle\mathbb{Z};1,+,\perp\rangle$, we can obtain some P$\exists$-undefinability results.

If we assume that the relation $x\not\perp y$ is P$\exists$-definable in $\langle\mathbb{Z};1,+,\perp\rangle$, then, since

$$\begin{aligned}\neg\mathrm{GCD}(x,y)=d \Leftrightarrow d\nmid x \vee d\nmid y&\\ \vee \exists u\exists v\,(x=du\wedge y=dv\wedge u\not\perp v)&\end{aligned}$$

and $d\nmid x \Leftrightarrow \bigvee\limits_{k=1..d-1} d\mid x+k$, by Theorem 5 the negations of $x\perp y$ and $\mathrm{GCD}(x,y)=d$ for any $d\geqslant 2$ are definable in the structure $\langle\mathbb{Z};1,+,-,=,\neq,\perp,\mathrm{GCD}_2,\mathrm{GCD}_3,\ldots\rangle$ by some positive quantifier-free formulas. But in this case Theorem 4 implies that we can eliminate all the quantifiers, and thus prove dicidability of $\mathrm{Th}\langle\mathbb{Z};1,+,\perp\rangle$. This contradicts D. Richard's undecidability result for this theory [63] and hence we get the following corollary.

Corollary 5.1. *The relation* $x\not\perp y$ *is not positively existentially definable in the structure* $\langle\mathbb{Z};1,+,\perp\rangle$*.*

It is not surprising that the order relation (or equivalently, $x \geqslant 0$) is also not P$\exists$-definable in $\langle \mathbb{Z}; 1, +, \perp \rangle$. We can prove it using Theorem 5 the same way as we prove quantifier-free undefinability in Section 2.2.

Indeed, if we assume that some quantifier-free formula $\varphi(x)$ defines $x \geqslant 0$ in the structure $\langle \mathbb{Z}; 1, +, -, =, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \ldots \rangle$, then this formula has form

$$\bigwedge_{i \in [1..m]} \mathrm{GCD}(a_i, b_i + cx) = d_i \wedge \bigwedge_{i \in [m+1..l]} a_i \neq cx. \tag{2.8}$$

for some integers a_i, b_i, d_i and positive integer c. By Remark 1.3.1, if the subsystem of all gcd-expressions from (2.8) has any solutions for cx then it has infinitely many negative integer solutions for cx. Therefore, since $\varphi(x)$ is true for some integer (in fact for every non-negative integer), it is true for infinitely many negative integers.

Corollary 5.2. *The order relation $\leqslant$ is not positively existentially definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$.*

Now consider P$\exists$-definability questions in some related structures.

For the structure $\langle \mathbb{N}; S, \perp \rangle$ first we see that the relation $x \neq 0$ is P$\exists$-definable by the formula $\exists y\,(x \perp SSy)$ while, for the same reasons as in Proposition 2.2.1, this relation is not positively quantifier-free definable in $\langle \mathbb{N}; S, \perp \rangle$. For this structure there is the following analogue of Theorem 5.

Proposition 2.4.1. *A relation is positively existentially definable in the structure $\langle \mathbb{N}; S, \perp \rangle$ if and only if it is positively quantifier-free definable in the structure $\langle \mathbb{N}; S, \neq 0, \perp \rangle$.*

To prove this proposition it is sufficient to use a special case of Lemma 2.3.1, where all $d_i = 1$.

Lemma 2.4.1. *Let $\bigwedge_{i \in [1..m]} a_i \perp b_i + x$ be a system such that $a_i, b_i \in \mathbb{N}$ and $a_i > 0$ for every $i \in [1..m]$. Define the index set $I_p = \{i \in [1..m] : p \mid a_i\}$. Then the system has a solution in $\mathbb{Z}$ if and only if for every prime $p \leqslant m$ and every set $I \subseteq I_p$ such that $|I| = p$ there are such $i,j \in I$, $i \neq j$ that $p \mid b_i - b_j$.*

Proof of Proposition 2.4.1. We can assume that in atomic formulas there are terms of the form $SS\ldots S0$, as $a \perp b + x \Leftrightarrow a + b + x \perp b + x$.

Consider the formula

$$\varphi(x, \overline{y}) \rightleftharpoons \bigwedge_{i \in [1..m]} f_i(\overline{y}) \perp b_i + x \wedge \bigwedge_{i \in [m+1..l]} a_i + x \neq 0, \tag{2.9}$$

where $f_i(\overline{y})$ are expressions of the form either $y_j + a$, or a for some $y_j \in \overline{y}$ and natural number a.

Note that $f_i(\overline{y})$ in (2.9) can only be equal to zero if $x = 0$ or $x = 1$, since otherwise the values of the expressions $b_i + x$ are at least 2 for every $i \in [1..m]$. By Remark 1.3.1, in the case $\bigwedge_{i \in [1..m]} f_i(\overline{y}) \neq 0$ we can omit dis-equalities in (2.9).

Therefore, applying Lemma 2.4.1, we have the following equivalence in $\mathbb{N}$:

$$\exists x \varphi(x,\overline{y}) \Leftrightarrow \varphi(0,\overline{y}) \vee \varphi(S0,\overline{y}) \vee \bigwedge_{i\in[1..m]} f_i(\overline{y}) \neq 0 \wedge \psi(\overline{y})$$

for

$$\psi(\overline{y}) \rightleftharpoons \bigwedge_{p\in\mathbb{P}\wedge p\leqslant m} \left(\bigwedge_{System(p,I)} \left(\bigvee_{i\in I} p \perp f_i(\overline{y}) \right) \right),$$

where $System(p,I) \rightleftharpoons I \subseteq [1..m] \wedge |I| = p \wedge \bigwedge_{i,j\in I\wedge i\neq j} p \nmid b_i - b_j$. Here for every prime p the condition $System(p,I)$ is true for such index sets I that $\{b_i\}_{i\in I}$ is a complete residue system modulo p. □

Now let $v_p(x)$ be the p-valuation of a rational number x (recall that $v_p(0) = \infty$). Then we define the divisibility $x \mid y$ on the rationals by $\bigwedge_{p\in\mathbb{P}} v_p(x) \leqslant v_p(y)$, and therefore $\mathrm{GCD}(x,y) = \prod_{p\in\mathbb{P}} p^{\min(v_p(x),v_p(y))}$, assuming that $\mathrm{GCD}(0,0) = 0$. If we define $x \perp y \rightleftharpoons \mathrm{GCD}(x,y) = 1$, then for a pair of rational numbers their coprimeness means that these numbers are coprime integers.

For these relations we can prove the following generalization of Lemma 2.3.1.

Lemma 2.4.2. *Lemma 2.3.1 remains true if we substitute in its statement $\mathbb{Q}$ for all occurrences of $\mathbb{Z}$.*

Proof. Consider (2.2), where $a_i, b_i, d_i \in \mathbb{Q}$ and $a_i \neq 0$, $d_i > 0$ for all $i \in [1..m]$.

Multiply every gcd-expression $\mathrm{GCD}(a_i,b_i + x) = d_i$ by the common denominator of a_i, b_i, d_i (denote it c_i) to obtain a system with only integer parameters and some integer coefficients c_i of the variable x. Let $C = \mathrm{LCM}_{i\in[1..m]}(c_i)$. Multiply each expression with index $i \in [1..m]$ by $\frac{C}{c_i}$ to get the same coefficient C of x. Since we are looking for a solution $x \in \mathbb{Q}$, replace Cx in every expression by a new rational variable $\widetilde{x}$.

Substitute $\frac{y}{z}$ for $\widetilde{x}$ and multiply each expression by $z \neq 0$. Thus we obtain the following system

$$\bigwedge_{i\in[1..m]} \mathrm{GCD}(a_iCz,b_iCz + y) = d_iCz. \tag{2.10}$$

By Lemma 2.3.1, there exist a solution $y \in \mathbb{Z}$ to the system (2.10) if and only if conditions (i) – (iv) hold for the parameters a_iCz, b_iCz and d_iCz.

For the first three conditions we can take the multiplier $Cz \neq 0$ from each parameter and reduce by it. To rewrite (iv), note that since $Cz \neq 0$ its p-valuation is some integer and we have $v_p(d_i) = v_p(d_iCz) - v_p(C) - v_p(z)$. Therefore, for every prime p the index sets J_p and I_p will be the same and $v_p(b_iCz - b_jCz) > \max_{i\in[1..m]} v_p(d_iCz)$ iff $v_p(b_i - b_j) > \max_{i\in[1..m]} v_p(d_i)$. □

Corollary 5.3. *A relation is positively existentially definable in the structure $\langle \mathbb{Q}; 1, +, -, \{c\cdot\}_{c\in\mathbb{Q}}, \perp \rangle$ if and only if it is positively quantifier-free definable in the structure $\langle \mathbb{Q}; 1, +, -, \neq, \{c\cdot\}_{c\in\mathbb{Q}}, \perp \rangle$.*

Proof. Consider a formula of the form (2.3), where the coefficients of linear polynomials are some rational numbers.

The same way as in Lemma 2.4.2, we make the coefficients of linear polynomials to be integers and the coefficient of x equal to C in every gcd-expression. We eliminate an existential quantifier the same way as in Theorem 4, but now Lemma 2.4.2 is used instead of Lemma 2.3.1. Conditions (i) and (ii) imply that the values of $f_i(\overline{y})$ and $(g_i(\overline{y}) - g_j(\overline{y}))$ must be integers, hence the process of rewriting (iii) and (iv) coincides with the one described in Theorem 4.

It remains to note that every expression of the form GCD(x,y) = d, where d is some rational number, is definable by the formula $\frac{x}{d} \perp \frac{y}{d}$. □

2.5 Three Generalizations of the BL-Theorem

2.5.1 Decidability of a Theory from Weispfenning's Remark

Probably, a more natural way to define integer divisibility over the rational numbers is to say that $x \in \mathbb{Q}$ divides $y \in \mathbb{Q}$ if and only if there exists some $z \in \mathbb{Z}$ such that $y = zx$. V. Weispfenning [84] considered mixed real-integer linear problems with two different divisibility relations over the reals. The first one is a generalization of our integer divisibility over the rationals $x \mid y \rightleftharpoons \exists z(z \in \mathbb{Z} \wedge y = zx)$, and the second one was defined as follows: $x \parallel y \rightleftharpoons x \in \mathbb{Z} \wedge \exists z(z \in \mathbb{Z} \wedge y = zx)$. Then he shows that the elementary theories of the structures $\langle \mathbb{R}; 0,1, +, -, [\,], =, <, \parallel \rangle$ and $\langle \mathbb{R}; 0,1, +, -, [\,], =, <, \mid \rangle$ are undecidable, while the positive existential theory of the first structure is decidable. Here, $[\,]$ stands for the integer-part operation whose graph is quantifier-free definable in both structures, for example,

$$x = [y] \Leftrightarrow (x = y \vee x < y) \wedge y < x + 1 \wedge 1 \mid x. \tag{2.11}$$

Note that undecidability results were obtained using the DPRM-Theorem, while the BL-Theorem was applied to prove decidability. After this proof, V. Weispfenning remarks that «We do not know whether a corresponding theorem holds in the analogous language L'_{div}», that is, whether the structure with $\mid$ also has decidable positive existential theory.

The first result of this section is the positive answer to Weispfenning's question. Moreover, we can avoid the restriction of positiveness and prove that the existential theory of the structure $\langle \mathbb{R}; 0,1, +, -, [\,], =, <, \mid \rangle$ is decidable. This result can be considered as a generalization of the BL-Theorem. The idea of the proof is straightforward. Denote by L_{div} the first-order language of the signature $\langle 0,1, +, -, =, <, \mid \rangle$; L'_{div} is the extension of L_{div} by a unary function symbol for the integer-part operation. First we show that if the domain is the set of the rational numbers, then the decision problem is reducible to the integer case and is thus decidable by the BL-Theorem. Then we prove that every quantifier-free L_{div}-formula is satisfiable over the reals if and only if it is satisfiable over the rational numbers.

Lemma 2.5.1. *The positive existential theory of the structure* $\langle \mathbb{Q}; 0,1, +, -, =, <, \mid \rangle$ *is decidable.*

Proof. In the same way as in Lemma 2.4.2, for every $i \in [1..n]$ we substitute the fraction $\frac{y_i}{z}$ for x_i in a given quantifier-free formula $\varphi(x_1,...,x_n)$. We see that

$$\exists x_{1\in\mathbb{Q}}...\exists x_{n\in\mathbb{Q}}\varphi(x_1,...,x_n) \Leftrightarrow \exists y_{1\in\mathbb{Z}}...\exists y_{n\in\mathbb{Z}}\exists z_{\in\mathbb{Z}}\left(z > 0 \wedge \varphi(\frac{y_1}{z},...,\frac{y_n}{z})\right).$$

Atomic formulas of $\varphi(x_1,...,x_n)$ have the form $f(x_1,...,x_n) = c$, or $f(x_1,...,x_n) < c$, or $f(x_1,...,x_n) + c \mid g(x_1,...,x_n) + d$, where $f(x_1,...,x_n)$ and $g(x_1,...,x_n)$ are linear forms with integer coefficients, and c, d are some integers. Multiplying every linear equality, inequality and divisibility from $\varphi(\frac{y_1}{z},...,\frac{y_n}{z})$ by z, we obtain a quantifier-free L_{div}-formula $\varphi'(y_1,...,y_n,z)$ with atomic formulas of the form $f(y_1,...,y_n) = cz$, or $f(y_1,...,y_n) < cz$, or $f(y_1,...,y_n) + cz \mid g(y_1,...,y_n) + dz$. Now $\exists x_1...\exists x_n\varphi(x_1,...,x_n)$ is true in the rationals if and only if $\exists y_1...\exists y_n\exists z\,(z > 0 \wedge \varphi'(y_1,...,y_n,z))$ is true in the integers. The decidability result now follows from the BL-Theorem. □

Lemma 2.5.2. *Every positive quantifier-free L_{div}-formula is satisfiable over $\mathbb{R}$ if and only if it is satisfiable over $\mathbb{Q}$.*

Proof. Let the formula

$$\varphi(\overline{x}) \rightleftharpoons \bigwedge_{i=1..k} g_i(\overline{x}) = 0 \wedge \bigwedge_{i=k+1..l} f_i(\overline{x}) \mid g_i(\overline{x}) \wedge \bigwedge_{i=l+1..m} g_i(\overline{x}) < 0$$

be satisfiable over $\mathbb{R}$, where $\overline{x}$ is a list of variables $x_1,..., x_n$; $g_i(\overline{x})$ for $i \in [1..m]$, $f_i(\overline{x})$ for $i \in [k+1..l]$ are linear polynomials with integer coefficients. We are going to show that $\varphi(\overline{x})$ is satisfiable over the rational numbers.

Suppose this formula is true for some real values $\alpha_1,...,\alpha_n$. Let $g_i(\alpha_1,...,\alpha_n) = 0$ for $i = k + 1..k'$, and $g_i(\alpha_1,...,\alpha_n) \neq 0$ for every $i \in [k' + 1..l]$. Now define the formula

$$\varphi'(\overline{x}) \rightleftharpoons \bigwedge_{i=1..k'} g_i(\overline{x}) = 0 \wedge \bigwedge_{i=k'+1..l} f_i(\overline{x}) \mid g_i(\overline{x}) \wedge \bigwedge_{i=k'+1..l} \sigma_i \cdot g_i(\overline{x}) < 0 \wedge \bigwedge_{i=l+1..m} g_i(\overline{x}) < 0,$$

where $\sigma_i = 1$ if $g_i(\alpha_1,...,\alpha_n) < 0$ and $\sigma_i = -1$ if $g_i(\alpha_1,...,\alpha_n) > 0$ for $i = k' + 1..l$.

Consider the system of linear equalities with integer coefficients $\bigwedge_{i=1..k'} g_i(\overline{x}) = 0$. Let $A\overline{y} + b$ be the solution set of this system for some rational matrix A, rational vector b and new variables $\overline{y} = y_1,...,y_t$. Substituting $A\overline{y} + b$ for $\overline{x}$, we obtain an equi-satisfiable over the reals system of linear inequalities and divisibilities with rational coefficients

$$\varphi''(\overline{y}) \rightleftharpoons \bigwedge_{i=k'+1..l} \widetilde{f}_i(\overline{y}) \mid \widetilde{g}_i(\overline{y}) \wedge \bigwedge_{i=k'+1..l} \sigma_i \cdot \widetilde{g}_i(\overline{y}) < 0 \wedge \bigwedge_{i=l+1..m} \widetilde{g}_i(\overline{y}) < 0$$

such that for every rational solution of $\varphi''(\overline{y})$ we can construct a rational solution of $\varphi'(\overline{x})$ and thus of $\varphi(\overline{x})$. Moreover, by construction $\varphi''(\overline{y})$ is satisfiable over $\mathbb{R}$.

Let $\beta_1,...,\beta_t$ be some real satisfying assignment of $\varphi''(\overline{y})$. Let the real numbers $\{1,\gamma_1,...,\gamma_s\}$ for some $s \leqslant t$ be a basis of the linear space over $\mathbb{Q}$ generated by the reals $\{1,\beta_1,...,\beta_t\}$. Each element β_i is uniquely represented as $c_{i,0} \cdot 1 + c_{i,1} \cdot \gamma_1 + ... + c_{i,s} \cdot \gamma_s$ for $i = 1..t$, where all $c_{i,j} \in \mathbb{Q}$. Define $\chi_i(z_1,...,z_s) = c_{i,0} + c_{i,1}z_1 + ... + c_{i,s}z_s$ for $i = 1..t$ and substitute $\chi_i(z_1,...,z_s)$ for y_i in $\varphi''(\overline{y})$. We obtain the following formula:

$$\psi(\overline{z}) = \varphi''(\chi_1(\overline{z}),...,\chi_t(\overline{z})).$$

Thus, for every rational satisfying assignment of $\psi(\overline{z})$, we can get a rational satisfying assignment of $\varphi''(\overline{y})$, and moreover $\psi(\gamma_1,...,\gamma_s)$ holds, since $\psi(\gamma_1,...,\gamma_s) = \varphi''(\beta_1,...,\beta_t)$.

Rewrite $\psi(\overline{z})$ in the following form:

$$\bigwedge_{i=1..l'} \widetilde{\widetilde{f}}_i(\overline{z}) \mid \widetilde{\widetilde{g}}_i(\overline{z}) \wedge \bigwedge_{i=1..m'} \widetilde{\widetilde{g}}_i(\overline{z}) < 0$$

for some $l' \leqslant m'$. Consider separately each divisibility $\widetilde{\widetilde{f}}(\overline{z}) \mid \widetilde{\widetilde{g}}(\overline{z})$ in $\psi(\overline{z})$. Here, $\widetilde{\widetilde{f}}(\overline{z}) = a_0 + a_1 z_1 + ... + a_s z_s$ and $\widetilde{\widetilde{g}}(\overline{z}) = b_0 + b_1 z_1 + ... + b_s z_s$ are some linear polynomials with raticonal coefficients and $\widetilde{\widetilde{g}}(\overline{z})$ is a non-zero polynomial. We will show that $\widetilde{\widetilde{g}}(\overline{z})$ is actually an integer multiple of $\widetilde{\widetilde{f}}(\overline{z})$ and thus the divisibility holds for every values of $\overline{z}$.

Let $w \cdot f(\gamma_1,...,\gamma_s) = g(\gamma_1,...,\gamma_s)$ for some integer w. For convenience, define $\gamma_0 = 1$. If we assume that $w \cdot a_i \gamma_i \neq b_i \gamma_i$ for some $i \in [0..s]$, then we have the equality $\gamma_i(w \cdot a_i - b_i) = \sum_{j=0..s \wedge j \neq i} \gamma_j (b_j - w \cdot a_j)$. But this is impossible because $1,\gamma_1,...,\gamma_s$ are linearly independent over $\mathbb{Q}$.

We conclude that every solution to the subsystem of linear inequalities $\bigwedge_{i=1..m'} \widetilde{\widetilde{g}}_i(\overline{z}) < 0$ with rational coefficients is also a satisfying assignment for $\psi(\overline{z})$. Since this subsystem has real solution $\gamma_1,...,\gamma_s$, there is some rational solution $q_1,...,q_s$. Finally, $\chi_1(q_1,...,q_s),...,\chi_t(q_1,...,q_s)$ is a rational satisfying assignment for $\varphi''(\overline{y})$, and thus $\varphi(\overline{x})$ is satisfiable over $\mathbb{Q}$. □

Theorem 6. *The existential theory of the structure* $\langle \mathbb{R}; 0,1, +, -, [\,], =, <, | \rangle$ *is decidable.*

Proof. Using formula (2.11), we can introduce some existentially quantified variables to transform a given $\exists L'_{div}$-formula into an equivalent over the reals $\exists L_{div}$-formula. Then, the negation of divisibility is positively existentially definable by the formula

$$x \nmid y \Leftrightarrow (x = 0 \wedge (y < 0 \vee 0 < y)) \vee \exists z\, (0 < z \wedge (z < x \vee z < -x) \wedge x \mid y + z)\,.$$

The desired decidability result now follows from Lemmas 2.5.1 and 2.5.2. □

2.5.2 Two Decidable Fragments of the ∀∃-Theory

Denote by L_{PA} the language of Presburger arithmetic, i.e., the first-order language over the signature $\langle 1, +, -, \leqslant, 2 \mid, 3 \mid, 4 \mid, ... \rangle$. Substituting all the unary divisibility predicate symbols for a binary predicate symbol for the divisibility relation, we get the language L_{PAD}. We know that $\exists\forall \mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ is undecidable. In this subsection, we define two families of closed $\forall\exists L_{PAD}$-formulas and prove decidability of the corresponding fragments of the $\exists\forall$-theory.

Our first result will be a generalization of a theorem by G.A. Pérez and R. Raha [57]. In their preprint, they show that the fragment of $\exists\forall \mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$, which was defined by M. Bozga and R. Iosif [7], is actually undecidable. Then they introduce some restrictions on the formulas of this fragment such that this new fragment becomes decidable. This decidable fragment comprises

all true in the integers formulas of the form

$$\forall\,\overline{x}\,\exists\,\overline{y}\bigvee_{j\in J}\Big(\overline{y}\geqslant 0\wedge\varphi_j(\overline{x})\wedge\bigwedge_{i\in[1..m_j]}(\mathrm{GCD}(f_i(\overline{x}),g_i(\overline{x},\overline{y}))=f_i(\overline{x})\wedge f_i(\overline{x})>0)\Big),\tag{2.12}$$

where $f_i(\overline{x})$, $g_i(\overline{x},\overline{y})$ are some linear polynomials with integer coefficients and $\varphi_j(\overline{x})$ are some quantifier-free L_{PAD}-formulas.

In this case we can easily isolate an existentially quantified variable, while (as we have seen in Step 1 of $\mathcal{R}$ in Section 1.4) in the general situation we have to apply LS-Lemma. Moreover, the system of gcd-expressions in (2.12) is already prepared for application of the Chinese remainder theorem, since every divisor is positive. Using GCD-Lemma instead of the Chinese remainder theorem, we are able to prove a more general statement.

Define a family of formulas, where in every gcd-expression the right-hand side polynomial may differ from the first argument of GCD.

$$\forall\,\overline{x}\,\exists\,\overline{y}\bigvee_{j\in J}\Big(\overline{y}\geqslant 0\wedge\varphi_j(\overline{x})\wedge\bigwedge_{i\in[1..m_j]}(\mathrm{GCD}(f_i(\overline{x}),g_i(\overline{x},\overline{y}))=h_i(\overline{x})\wedge f_i(\overline{x})>0\wedge h_i(\overline{x})>0)\Big),\tag{2.13}$$

Here, $h_i(\overline{x})$ are also some linear polynomials with integer coefficients. Then we have the following theorem.

Theorem 7. *There is an algorithm that decides in the integers formulas of the form (2.13).*

Before we begin with the proof of this theorem, for convenience we slightly modify the GCD-Lemma. Define the condition

((iii)) $\displaystyle\bigwedge_{1\leqslant i<j\leqslant m}\mathrm{GCD}(a_i,d_j,b_i-b_j)=\mathrm{GCD}(a_j,d_i,b_i-b_j)=\mathrm{GCD}(d_i,d_j)$

to get the following auxiliary lemma.

Lemma 2.5.3. *Suppose we are given a system of the form (2.2) with a_i, b_i, d_i as defined in Lemma 2.3.1. Assume condition (i) holds, then conditions (ii) and (iii) are equivalent to ((iii)).*

Proof. We see that (ii) obviously follows from ((iii)). Condition (iii) has the form of a system of the following pairs of divisibilities:

$$\mathrm{GCD}(a_i,d_j,b_i-b_j)\mid d_i\wedge\mathrm{GCD}(a_j,d_i,b_i-b_j)\mid d_j$$

for any $1\leqslant i<j\leqslant m$. Now ((iii)) also implies theses divisibilities.

Conversely, consider the chain of equalities:

$$\begin{aligned}\mathrm{GCD}(a_i,d_j,b_i-b_j)&=\mathrm{GCD}\,(d_i,\mathrm{GCD}(a_i,d_j,b_i-b_j))\\&=\mathrm{GCD}\,(\mathrm{GCD}(d_i,a_i),\mathrm{GCD}(d_j,b_i-b_j))=\mathrm{GCD}\,(d_i,d_j)\,.\end{aligned}$$

The first equality is just condition (iii) and the last equality immediately follows from (i) and (ii). This concludes the proof of this lemma. □

Remark 2.5.1. *If we allow $i=j$ in ((iii)), then we have $GCD\,(d_i,a_i)=GCD\,(d_i,d_i)$, that is, $d_i\mid a_i$. Therefore, we can replace in GCD-Lemma a pair of conditions (i) and (iii) by ((iii)), where indexes i and j may be the same. But this reformulation seems somewhat unclear since it hides the obviously expected condition (i).*

Proof of Theorem 7. Our aim is to construct for every formula of the form (2.13) an equivalent over the integers universal L_{PAD}-formula. Then, since $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ is decidable if and only if the universal theory of this structure is decidable, the BL-Theorem yields the desired algorithm.

In order to simplify this construction, we introduce in our signature a binary function symbol for the GCD function and unary function symbols for the V_p functions from p-Büchi arithmetic for every prime number p. We will assume that $\mathrm{GCD}(0,0)=0$ and $V_p(0)=0$.

It follows from definitions (2) that the relation $\mathrm{GCD}(x,y)=z$ with its negation are also universally definable in the structure $\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$. The function symbols V_p in the resulting $\forall L_{PAD}$-formula will only appear in atomic formulas of the form either $V_p(t_1(\overline{x}))\mid t_2(\overline{x})$ or $V_p(t_1(\overline{x}))=V_p(t_2(\overline{x}))$, where $t_1(\overline{x})$ and $t_2(\overline{x})$ are some terms constructed using variables from $\overline{x}$, unit, addition, subtraction and GCD. Then we can exclude V_p from our formula using the equivalence

$$V_p(x)\mid y\Leftrightarrow V_p(\mathrm{GCD}(x,y))=V_p(x) \tag{2.14}$$

and the following quantifier-free definition:

$$V_p(x)=V_p(y)\Leftrightarrow \mathrm{GCD}(x,py)=\mathrm{GCD}(x,y)\wedge\mathrm{GCD}(px,y)=\mathrm{GCD}(x,y). \tag{2.15}$$

Let X and Y be two disjoint sets of variables, and let $L^Y_{(2.16)}$ be the set of quantifier-free formulas $\bigvee\limits_{j\in J}\psi_j(\overline{x},\overline{y})$ for some finite index set J and formulas $\psi_j(\overline{x},\overline{y})$ of the form

$$\overline{y}\geqslant 0\wedge\varphi_j(\overline{x})\wedge\bigwedge_{k\in[1..m_j]}f_k(\overline{x})>0\wedge h_k(\overline{x})>0\wedge\bigwedge_{i\in[1..l_j]}\mathrm{GCD}(F_i(\overline{x}),g_i(\overline{x},\overline{y}))=H_i(\overline{x}), \tag{2.16}$$

where $\overline{x}$ is a finite set of variables from X; $\overline{y}$ is a finite set of variables from Y; $f_k(\overline{x})$, $h_k(\overline{x})$ for $k\in[1..m_j]$ and $g_i(\overline{x},\overline{y})$ for $i\in[1..l_j]$ are linear polynomials with integer coefficients. The expressions $F_i(\overline{x})$ and $H_i(\overline{x})$ are constructed using only $f_1(\overline{x})$, $h_1(\overline{x})$,...,$f_{m_j}(\overline{x})$, $h_{m_j}(\overline{x})$ and function symbols GCD and V_p for every prime number p with the following auxiliary restriction: for every $i\in[1..l_j]$ a function symbol V_p appears in $F_i(\overline{x})$ only if it appears in $H_i(\overline{x})$. Finally, every $\varphi_j(\overline{x})$ is a formula of the form

$$\widetilde{\varphi_j}(\overline{x})\wedge\bigwedge_{i\in[1..\widetilde{m}_j]}V_{p_i}\left(t_{i,1}(\overline{x})\right)\mid t_{i,2}(\overline{x})\wedge\bigwedge_{i\in[1..\widetilde{\widetilde{m}}_j]}V_{q_i}\left(\widetilde{t}_{i,1}(\overline{x})\right)=V_{q_i}\left(\widetilde{t}_{i,2}(\overline{x})\right), \tag{2.17}$$

where $\widetilde{\varphi_j}(\overline{x})$ is some quantifier-free $L_{\langle1,+,-,\mathrm{GCD},\leqslant,|\rangle}$-formula and $t_{i,1}(\overline{x})$, $t_{i,2}(\overline{x})$, $\widetilde{t}_{i,1}(\overline{x})$, $\widetilde{t}_{i,2}(\overline{x})$ are some terms of the same language.

The following lemma finishes the proof of this theorem. □

Lemma 2.5.4. *Let X and Y be two disjoint sets of variables, $\overline{x}$ are from X and $(\overline{y},z)$ are from Y. Then, for every formula of the form $\exists z\psi(\overline{x},\overline{y},z)$, where $\psi(\overline{x},\overline{y},z)$ is some $L^Y_{(2.16)}$-formula, we can constructively find an $L^Y_{(2.16)}$-formula $\theta(\overline{x},\overline{y})$ that is equivalent to $\exists z\psi(\overline{x},\overline{y},z)$ in $\mathbb{Z}$.*

Proof. Analogously to Step 2 of $\mathcal{R}$ in Section 1.5 and to Theorem 4, we can assume that the coefficients of the eliminated variable z in every expression are equal to one. In every conjunct of

$\psi(\overline{x},\overline{y},z)$, a subsystem with only those atomic formulas that have any occurrences of z now has form

$$z \geqslant 0 \wedge \bigwedge_{i\in[1..l]} \mathrm{GCD}(F_i(\overline{x}), g_i(\overline{x},\overline{y}) + z) = H_i(\overline{x}). \tag{2.18}$$

By definition of $L^Y_{(2.16)}$, every expression $F_i(\overline{x})$ and $H_i(\overline{x})$ can take only positive values. Thus, we are now able to apply GCD-Lemma to rewrite the fact that there exists such a solution z to the system (2.18). By Remark 1.3.1, if there is any such z then we can find infinitely many positive solutions to (2.18), and thus inequality $z \geqslant 0$ can be excluded. Consider separately every condition of GCD-Lemma, assuming that a pair of conditions (ii) and (iii) be replaced by ((iii)). By Lemma 2.5.3, this replacement is correct.

It is not difficult to rewrite conditions (i) and ((iii)). For (i) we have the conjunction of divisibilities

$$\bigwedge_{i\in[1..l]} H_i(\overline{x}) \mid F_i(\overline{x}), \tag{2.19}$$

and condition ((iii)) is just the formula

$$\bigwedge_{1\leqslant i<j\leqslant l} \Big(\mathrm{GCD}(\mathrm{GCD}(F_i(\overline{x}),H_j(\overline{x})), g_i(\overline{x},\overline{y}) - g_j(\overline{x},\overline{y})) = \mathrm{GCD}(H_i(\overline{x}),H_j(\overline{x}))\wedge$$
$$\mathrm{GCD}(\mathrm{GCD}(F_j(\overline{x}),H_i(\overline{x})), g_i(\overline{x},\overline{y}) - g_j(\overline{x},\overline{y})) = \mathrm{GCD}(H_i(\overline{x}),H_j(\overline{x}))\Big). \tag{2.20}$$

We treat (iv) in the same way as in Step 2 of quasi-QE algorithm $\mathcal{R}$ in Section 1.5. The only difference is that every equality and inequality with p-valuation functions are now replaced by equalities and divisibilities with V_p. Namely, we have the following conjunction:

$$\bigwedge_{p\leqslant l\wedge p\in\mathbb{P}} \left(\bigwedge_{I\subseteq[1..l]\wedge|I|=p} \Omega_{p,I}(\overline{x},\overline{y}) \right), \tag{2.21}$$

where $\mathbb{P}$ is the set of the prime numbers and

$$\Omega_{p,I}(\overline{x},\overline{y}) \rightleftharpoons \bigvee_{i\in I\wedge j\in[1..l]} V_p(pH_i(\overline{x})) \mid H_j(\overline{x}) \vee \bigvee_{i\in I} V_p(H_i(\overline{x})) = V_p(F_i(\overline{x}))$$
$$\vee \bigvee_{i,j\in I\wedge i\neq j} V_p(H_i(\overline{x})) \mid g_i(\overline{x},\overline{y}) - g_j(\overline{x},\overline{y}). \tag{2.22}$$

Note that every divisibility in (2.22) with variables from $\overline{y}$ can be rewritten in the obvious way:

$$\mathrm{GCD}(V_p(H_i(\overline{x})), g_i(\overline{x},\overline{y}) - g_j(\overline{x},\overline{y})) = V_p(H_i(\overline{x})).$$

In order to construct $\theta(\overline{x},\overline{y})$, in every conjunct of $\psi(\overline{x},\overline{y},z)$ we replace a subsystem of the form (2.18) by the corresponding conjunction (2.19)$\wedge$(2.20)$\wedge$(2.21). Then we apply the distributive law to move all disjunctions to the outer level. It remains to prove that in every conjunct the expressions without variables from $\overline{y}$ are equivalent to some formulas of the form (2.17). This follows from the equalities $\mathrm{GCD}(V_p(x),y) = V_p(\mathrm{GCD}(x,y))$ and $\mathrm{GCD}(V_p(x),V_q(y)) = 1$. $\square$

Decidability of the second fragment of $\forall\exists$-theory of $\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ follows as an immediate consequence from Theorem 4. In this case, we consider formulas of the following form

$$\forall\,\overline{x}\,\exists\,\overline{y}\bigvee_{j\in J}\Big(\varphi_j(\overline{x})\wedge\bigwedge_{i\in[1..m_j]}\mathrm{GCD}(f_i(\overline{x},\overline{y}),g_i(\overline{x},\overline{y}))=d_i\Big),\tag{2.23}$$

where $f_i(\overline{x},\overline{y})$, $g_i(\overline{x},\overline{y})$ are some linear polynomials with integer coefficients and $\varphi_j(\overline{x})$ are some quantifier-free L_{PAD}-formulas. That these formulas are some $\forall\exists L_{PAD}$-formulas follows from definitions (2). Here, for every gcd-expression with variables from $\overline{y}$ there are no restrictions on the left-hand side polynomials, but the right-hand side polynomials are some positive integers. Moreover, the variables from $\overline{y}$ do not appear in linear inequalities. Theorem 4 gives us the following corollary for this family of formulas.

Corollary 4.1. *There is an algorithm that decides in the integers formulas of the form (2.23).*

Proof. Apply Theorem 4 to eliminate all the existential quantifiers. Rewrite dis-equalities using the order relation to obtain a universal formula of the first-order language of the signature $\langle 1,+,-,\mathrm{GCD},\leqslant,|\rangle$. Again, with the help of definitions (2), we can exclude GCD from the formula and then apply the BL-Theorem in order to construct the desired algorithm. □

2.6 Quasi-QE Algorithm for the Existential Arithmetic of the Natural Numbers with Unit, Addition and Coprimeness

It is not known whether we still have a decidable problem if in (2.23) we allow linear inequalities $f(\overline{x},\overline{y})\geqslant 0$. Nevertheless, it seems natural to consider the problem of existence of integer solutions of systems of the form

$$\varphi_+(\overline{z})\rightleftharpoons A\overline{z}=B\wedge C\overline{z}\geqslant D\wedge\bigwedge_{i\in[1..m]}\mathrm{GCD}(f_i(\overline{z}),g_i(\overline{z}))=d_i,\tag{2.24}$$

where A and C are integer matrices and B, D are some integer vectors.

By Corollary 5.1, the dis-coprimeness relation is not P$\exists$-definable in the structure $\langle\mathbb{Z};1,+,-,\perp\rangle$, but this says nothing about P$\exists$-definability of this relation if we have the order relation in our structure. In order to decide arbitrary formulas of the existential Presburger arithmetic with coprimeness $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ (denote the corresponding first-order language by L_{PAC}), we consider the problem of satisfiability over $\mathbb{Z}$ of formulas of the form

$$\begin{aligned}\varphi(\overline{z})\rightleftharpoons\overline{\delta}\geqslant 2\wedge A\overline{z}=B\wedge C\overline{z}\geqslant D\wedge&\bigwedge_{i\in[1..m]}\mathrm{GCD}(f_i(\overline{z}),g_i(\overline{z}))=d_i\\&\wedge\bigwedge_{i\in[m+1..l]}\mathrm{GCD}(f_i(\overline{z}),g_i(\overline{z}))=d_i\delta_i.\end{aligned}\tag{2.25}$$

Using Theorem 4, we construct a quasi-QE algorithm that decides closed P$\exists L_{PAC}$-formulas in the integers $\mathbb{Z}$. This algorithm, called $\mathcal{C}^+$, is much simpler than the combination of algorithms

$\mathcal{R}$ and $\mathcal{D}$ for the BL-theorem from the first chapter. Then, for arbitrary $\exists L_{PAC}$-formulas we construct a quasi-QE algorithm $\mathcal{C}$ that performs a reduction from the decision problem for $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ to the decision problem for a fragment of $\exists\mathrm{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD},=\rangle$, where GCD is treated as a binary function symbol for the corresponding function. A slight modification of quasi-QE algorithm $\mathcal{D}$ completes the desired decidability proof.

2.6.1 The Positive Case

By Lemma 1.2.2, in order to construct a decision procedure for the positive existential theory of the structure $\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ it is sufficient to solve the problem of satisfiability over the integers of systems of the form

$$\overline{y}\geqslant 0\wedge\bigwedge_{i\in[1..m]}\mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y}))=d_i. \tag{2.26}$$

We now define the languages of quasi-quantifier elimination algorithm $\mathcal{C}^+$.

The sort S_2 will be empty, and the language $L_{\mathcal{C}^+}$ comprises quantifier-free formulas $\bigvee\limits_{j\in J_1}\varphi_j(\overline{y_j})$ for some finite index set J_1 and formulas $\varphi_j(\overline{y_j})$ of the form (2.26). The set of formulas of elimination form $L^x_{\mathcal{C}^+}$ for a Latin variable x is the set of $L_{\mathcal{C}^+}$-formulas $\bigvee\limits_{j\in J_2}\widetilde{\varphi}_j(x,\overline{z_j})$ for some finite index set J_2 and $\widetilde{\varphi}_j(x,\overline{z})$ of the following form:

$$\overline{z}\geqslant 0\wedge x\geqslant 0\wedge\widetilde{\widetilde{\varphi}}(\overline{z})\wedge\bigwedge_{i\in[1..\widetilde{m}]}\mathrm{GCD}(\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z})+c_ix)=\widetilde{d}_i, \tag{2.27}$$

where x does not appear in the list $\overline{z}$, $c_i>0$; every $\widetilde{f}_i(\overline{z})$ is a linear polynomial with non-negative integer coefficients and positive constant terms, and $\widetilde{\widetilde{\varphi}}(\overline{z})$ is a system of gcd-expressions.

Step 1 of algorithm $\mathcal{C}^+$ is much simpler than Step 1 of $\mathcal{R}$ from Section 1.4 since linear polynomials on the right-hand side of gcd-expressions are always some positive constants. Moreover, in our formulas there are no Greek variables. As we are going to show below, in algorithm $\mathcal{C}$ such variables are used to rewrite the dis-coprimeness relations. The following lemma provides us with the desired transformations.

Lemma 2.6.1. *There is an algorithm assigning to every $L_{\mathcal{C}^+}$-formula $\varphi(\overline{z})$ an equi-satisfiable over the integers disjunction $\bigvee\limits_{j\in J}\varphi_j(\overline{z_j})$ for some finite index set J, where for every $j\in J$ $\overline{z_j}$ has at most the same number of variables than $\overline{z}$, and $\varphi_j(\overline{z_j})$ is an $L^{x_j}_{\mathcal{C}^+}$-formula for some variable $x_j\in\overline{z_j}$.*

Proof. In the proof we will again use LS-Lemma from Subsection 1.2.1. In addition, we will also consider a special case of *«application of LS-Lemma to the subsystem $S(\overline{s})$ of the formula $\varphi(\overline{z})$»*. That is, we say that some disjunction is obtained as a result of *«application of LS-Lemma to the formula $\varphi(\overline{z})$»* if the subsystem $S(\overline{s})$ comprises all the linear equalities and inequalities from $\varphi(\overline{z})$.

Suppose we have applied Lemma 2.2.2 to every disjunct of a given $L_{\mathcal{C}^+}$-formula. We get a disjunction of formulas of the form (2.27). For this formula we are going to construct an equisatisfiable over the integers formula $\widetilde{\Phi}_1(\overline{z_1}) \vee \widetilde{\Phi}_2(x,\overline{z_2})$ in which $\widetilde{\Phi}_1(\overline{z_1})$ is a disjunction of formulas of the form (2.27) with fewer number of variables and $\widetilde{\Phi}_2(x,\overline{z_2})$ is a disjunction of $L^x_{\mathcal{C}^+}$-formulas. By repeatedly applying this step to the first disjunct until its list of variables becomes empty, we construct a disjunction of the desired form.

The formula $\widetilde{\Phi}_1(\overline{z_1})$ is a result obtained for the cases when $\widetilde{f}_i(\overline{z}) = 0$. Let $\Phi(x,\overline{z})$ be the conjunction $\overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z})$, then $\widetilde{\Phi}_1(\overline{z_1})$ is a result of application of LS-Lemma to every system of the following disjunction:

$$\bigvee_{j\in[1..\widetilde{m}]} \bigvee_{\sigma\in\{-1,1\}} \Bigg(\Phi(x,\overline{z}) \wedge \widetilde{f}_j(\overline{z}) = 0 \wedge \widetilde{g}_j(\overline{z}) + c_j x = \sigma \widetilde{d}_j \\ \wedge \bigwedge_{i\in[1..\widetilde{m}]\wedge i\neq j} \mathrm{GCD}(\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{d}_i \Bigg).$$

The case of non-zero first arguments of gcd-expressions will be described by the formula $\widetilde{\Phi}_2(x,\overline{z_2})$. Consider the formula

$$\bigvee_{\overline{\sigma}\in\{-1,1\}^{\widetilde{m}}} \Bigg(\Phi(x,\overline{z}) \wedge \bigwedge_{i\in[1..\widetilde{m}]} \Big(\sigma_i \widetilde{f}_i(\overline{z}) \geqslant 1 \wedge \mathrm{GCD}(\sigma_i \widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{d}_i \Big) \Bigg). \tag{2.28}$$

Applying LS-Lemma to the subsystems with all linear equalities and inequalities in $\overline{z}$ in each disjunct of (2.28), we get a disjunction of $L^x_{\mathcal{C}^+}$-formulas. This completes the definition of $\widetilde{\Phi}_2(x,\overline{z_2})$ and hence the proof of the lemma. □

Now we are able to prove the following proposition.

Proposition 2.6.1. *The positive existential theory of the structure* $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$ *is decidable.*

Proof. It is sufficient to define Step 2 of quasi-QE algorithm $\mathcal{C}^+$. Let us have an $L^x_{\mathcal{C}^+}$-formula $\bigvee\limits_{j\in J} \varphi_j(x,\overline{z_j})$ for some finite index set J and $L^x_{\mathcal{C}^+}$-formulas $\varphi_j(x,\overline{z_j})$. In Step 2 we apply Lemma 2.3.1 to the formulas $\exists x \varphi_j(x,\overline{z_j})$ for every $j \in J$ in the same way as in Theorem 4. Here we do not consider the cases when the first arguments of gcd-expressions are equal to zero, because by definition of the language $L^x_{\mathcal{C}^+}$ they can take only positive values. Again, Remark 1.3.1 implies that the restriction of non-negativeness on the eliminated variable can be omitted.

Thus we have constructed an equivalent in the integers disjunction $\bigvee\limits_{j\in J} \psi_j(\overline{z_j})$, where $\psi_j(\overline{z_j})$ are some $L_{\mathcal{C}^+}$-formulas. This concludes the description of algorithm $\mathcal{C}^+$ and thus gives us the desired decidability result. □

This proposition itself is not a new result, since it follows from the BL-Theorem. However, we do not know any explicit descriptions of an algorithm for $\mathrm{P}\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$, as well as for the case when the formulas are not required to be positive. This generalization will be considered in the next subsection.

2.6.2 Generalization to Arbitrary Existential Formulas

For the problem of satisfiability in $\mathbb{Z}$ of quantifier-free L_{PAC}-formulas it is sufficient to check that there are integer solutions to the system (2.24), where we also allow expressions of the form $\mathrm{GCD}(f(\overline{x}),g(\overline{x})) \neq 1$. It is not difficult to reduce this problem to satisfiability over $\mathbb{Z}$ of formulas of the form

$$\overline{\delta} \geqslant 2 \wedge \overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = d_i \wedge \bigwedge_{i\in[m+1..l]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = d_i\delta_i. \tag{2.29}$$

Let us fix this transformation in the following lemma.

Lemma 2.6.2. *The decision problem for* $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ *is reducible to the problem of satisfiability in* $\mathbb{Z}$ *of systems of the form (2.29).*

Proof. Suppose that $\varpi(\overline{z}) \rightleftharpoons \varphi_+(\overline{z}) \wedge \bigwedge_{i\in[m+1..k]} \mathrm{GCD}(f_i(\overline{z}),g_i(\overline{z})) \neq 1$, where $\varphi_+(\overline{z})$ has form (2.24). Each gcd-expression for $i \in [m+1..l]$ is true if and only if for some integer δ_i we have

$$(f_i(\overline{z}) = 0 \wedge g_i(\overline{z}) = 0) \vee (\delta_i \geqslant 2 \wedge \mathrm{GCD}(f_i(\overline{z}),g_i(\overline{z})) = \delta_i)\,.$$

Rewriting every such gcd-expression, for the formula $\varpi(\overline{z})$ we obtain an equi-satisfiable over the integers disjunction of formulas of the form (2.25). It remains to apply LS-Lemma to the subsystems with all linear equalities and inequalities over $\overline{z}$ in each disjunct in order to obtain the desired result. □

Now we are going to construct a quasi-QE algorithm $\mathcal{C}$, which reduces the problem of satisfiability in the integers of formulas of the form (2.29) to the decision problem for a fragment of the existential theory of the structure $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD},=\rangle$, where GCD is a binary function symbol. Decidability of the latter theory can easily be proved by using algorithm $\mathcal{D}$ from Section 1.7. We obtain the following generalization of Theorem 3.

Lemma 2.6.3. *The existential theory of the structure* $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD},=\rangle$ *is decidable.*

Proof. This lemma still follows from the decidability of Skolem arithmetic with constants $\mathrm{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\cdot,=\rangle$. But we can prove it using quasi-QE algorithm as follows.

Any given existential formula after introducing some auxiliary variables can be rewritten as a disjunction of formulas of the form

$$\exists\overline{y} \bigwedge_{i\in[1..m]} f_i(\overline{y}) \neq g_i(\overline{y}) \wedge \bigwedge_{i\in[m+1..l]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}) \tag{2.30}$$

for $f_i(\overline{y})$, $g_i(\overline{y})$, $h_i(\overline{y})$ of the form au or a, where a is a positive integer and $u \in \overline{y}$.

First apply the transformations of this formula from Lemma 1.7.2. In our case, after replacements of variables in some conjunction of the form (2.30) we can get a contradiction $f(\overline{y}) \neq f(\overline{y})$, and this conjunction evaluates to false.

Now we allow dis-equalities in algorithm $\mathcal{D}$. It is obvious that Step 2 is the same since by Remark 1.3.1 we can always choose a solution to a given system of gcd-expression that satisfies all the dis-equalities. Applying the transformations from Step 1, similarly to the case of modified Lemma 1.7.2, we can obtain a contradiction $f(\overline{y}) \neq f(\overline{y})$. Here, the corresponding disjunct can be excluded from the formula since it is always false. This concludes the modification of quasi-QE algorithm $\mathcal{D}$ and the proof of the lemma. □

We call terms of the language $L_{\langle 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD},=\rangle}$ *primitive gcd-terms*. If $T(\overline{\alpha})$ is a primitive gcd-term and p is a prime number, we call terms of the form $V_p(T(\overline{\alpha}))$ *p-valuated primitive gcd-terms*. The language $L_{\mathcal{C}}$ of quasi-QE algorithm $\mathcal{C}$ comprises existential formulas $\exists\overline{\delta} \bigvee\limits_{j\in J_1} \varphi_j(\overline{y_j},\overline{\delta})$ for some finite index set J_1 and formulas $\varphi_j(\overline{y_j},\overline{\delta})$ of the form

$$\begin{aligned}\overline{\delta^{(1)}} \geqslant 2 \wedge \overline{\delta^{(2)}} \geqslant 2 \wedge \overline{y} \geqslant 0 \wedge & \bigwedge_{i\in[1..k]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = d_i \\ \wedge & \bigwedge_{i\in[k+1..l]} \mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})) = d_i\delta_i \\ \wedge & \bigwedge_{i\in[l+1..m]} \mathrm{GCD}(\mathrm{GCD}(f_i(\overline{y}),F_i(\overline{\delta^{(2)}})),g_i(\overline{y})) = H_i(\overline{\delta^{(2)}}),\end{aligned} \tag{2.31}$$

where $\overline{\delta^{(1)}} = \delta_{k+1},\ldots,\delta_l$ and $\overline{\delta^{(2)}} = \delta_{l+1},\ldots,\delta_m$ are disjoint sets of Greek variables; as usual, $f_i(\overline{y})$, $g_i(\overline{y})$ denote linear polynomials with integer coefficients, and $F_i(\overline{\delta^{(2)}})$, $H_i(\overline{\delta^{(2)}})$ are either primitive gcd-terms or for some prime number p simultaneously p-valuated primitive gcd-terms. Further we call *gcd-expression* every expression of the form $\mathrm{GCD}(u,v) = w$ for any terms u,v,w and not only for linear polynomials.

The set of formulas of elimination form $L^x_{\mathcal{C}}$ for a Latin variable x is the set of $L_{\mathcal{C}}$-formulas $\exists\overline{\delta} \bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x,\overline{z_j},\overline{\delta})$ for some finite index set J_2 and $\widetilde{\varphi}_j(x,\overline{z},\overline{\delta})$ of the following form:

$$\overline{\delta} \geqslant 2 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta}) \wedge \bigwedge_{i\in[1..\widetilde{m}]} \mathrm{GCD}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{H}_i(\overline{\delta}), \tag{2.32}$$

where x does not appear in the list $\overline{z}$, $c_i > 0$; every $\widetilde{F}_i(\overline{z},\overline{\delta})$ is either a linear polynomial with non-negative integer coefficients and positive constant terms or $\mathrm{GCD}(f(\overline{z}),F(\overline{\delta}))$, where $F(\overline{\delta})$ is some primitive gcd-term or p-valuated primitive gcd-term; and $\widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta})$ is a system of gcd-expressions without occurrences of x.

We now ready to prove the main result of this section.

Proposition 2.6.2. *The existential theory of the structure $\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ is decidable.*

Proof. Since in an $L_{\mathcal{C}}$-formula without Latin variables we can avoid using p-valuated primitive gcd-terms by using equality $\mathrm{GCD}(V_p(x),y) = V_p(\mathrm{GCD}(x,y))$ and formula (2.15), it is clear that quasi-QE algorithm $\mathcal{C}$ reduces the problem of satisfiability in the integers $\mathbb{Z}$ of systems of the form (2.29) to the decision problem for a fragment of the existential theory of the structure $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD},=\rangle$. In Lemma 2.6.3 we presented a quasi-QE algorithm for this theory,

and from Lemma 2.6.2 it follows that in order to complete the proof it remains to define Steps 1 and 2 of quasi-QE algorithm $\mathcal{C}$.

Step 1. This step is a generalization of Step 1 of $\mathcal{C}^+$. Applying Lemma 2.2.2 to every gcd-expression in a given system of the form (2.31), we obtain a system of the form (2.32). Note that in the case of gcd-expressions with primitive gcd-terms, we first put together linear polynomials: $\mathrm{GCD}(\mathrm{GCD}(f_i(\overline{y}),F_i(\overline{\delta^{(2)}})),g_i(\overline{y})) = \mathrm{GCD}(\mathrm{GCD}(f_i(\overline{y}),g_i(\overline{y})),F_i(\overline{\delta^{(2)}}))$, then apply Lemma 2.2.2, and finally rewrite this expression in the standard form.

We can now consider the system $\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ of the form: $\overline{\delta^{(1)}} \geqslant 2 \wedge \overline{\delta^{(2)}} \geqslant 2 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta}) \wedge \Delta(x,\overline{z},\overline{\delta})$, where

$$\begin{aligned}\Delta(x,\overline{z},\overline{\delta}) \rightleftharpoons & \bigwedge_{i\in[1..k]} \mathrm{GCD}(\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z})+c_ix) = d_i \\ & \wedge \bigwedge_{i\in[k+1..l]} \mathrm{GCD}(\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z})+c_ix) = d_i\delta_i \\ & \wedge \bigwedge_{i\in[l+1..m]} \mathrm{GCD}(\mathrm{GCD}(\widetilde{f}_i(\overline{z}),\widetilde{F}_i(\overline{\delta^{(2)}})),\widetilde{g}_i(\overline{z})+c_ix) = \widetilde{H}_i(\overline{\delta^{(2)}}).\end{aligned}$$

For the formula $\exists\overline{\delta}\widetilde{\varphi}(x,\overline{z},\overline{\delta})$, analogously to Step 1 of algorithm $\mathcal{R}$ from Section 1.4, we construct an equi-satisfiable formula

$$\exists\overline{\delta}\Big(\widetilde{\Phi}_0(\overline{z_0},\overline{\delta}) \vee \widetilde{\Phi}_1(\overline{z_1},\overline{\delta}) \vee \widetilde{\Phi}_2(x,\overline{z_2},\overline{\delta})\Big),$$

where $\widetilde{\Phi}_0(\overline{z_0},\overline{\delta})$ and $\widetilde{\Phi}_1(\overline{z_1},\overline{\delta})$ are disjunctions of systems of the form (2.32) such that the list $\overline{z_0}$ contains two and $\overline{z_1}$ one fewer variable than the list $(x,\overline{z})$. At the same time, $\widetilde{\Phi}_2(x,\overline{z_2},\overline{\delta})$ will be a disjunction of the desired form, that is, $\exists\overline{\delta}\,\widetilde{\Phi}_2(x,\overline{z_2},\overline{\delta})$ will be some $L^x_{\mathcal{C}}$-formula.

These disjunctions can be constructed in the same way as described at the end of Section 1.4. Note that for the formula $\widetilde{\Phi}_1(\overline{z_1},\overline{\delta})$, we do not need the restrictions on gcd-expressions of the form ($\mathcal{R}$-2) since now the lists of Greek variables $\overline{\delta^{(1)}}$ and $\overline{\delta^{(2)}}$ are disjoint. Thus, for every $i \in [k+1..l]$, the substitution of $\frac{\sigma(\widetilde{g}_i(\overline{z})+c_ix)}{d_i}$ for δ_i only replaces $\delta_i \geqslant 2$ with $\sigma(\widetilde{g}_i(\overline{z})+c_ix) \geqslant 2d_i$.

Step 2. As usual, we can without loss of generality assume that in the subsystem of (2.32) with an isolated variable x all c_i are equal to 1.

In this step, for $L^x_{\mathcal{C}}$-formula $\exists\overline{\delta}\widetilde{\varphi}(x,\overline{z},\overline{\delta})$, where

$$\widetilde{\varphi}(x,\overline{z},\overline{\delta}) \rightleftharpoons \overline{\delta} \geqslant 2 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta}) \wedge \bigwedge_{i\in[1..\widetilde{m}]} \mathrm{GCD}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{g}_i(\overline{z})+x) = \widetilde{H}_i(\overline{\delta}), \qquad (2.33)$$

we rewrite the formula $\exists x\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ to get an equivalent in $\mathbb{Z}$ formula $\psi(\overline{z},\overline{\delta})$ such that $\exists\overline{\delta}\psi(\overline{z},\overline{\delta})$ is some $L_{\mathcal{C}}$-formula.

The first argument of every gcd-expression with x can only have positive values: this is obvious when $\widetilde{F}_i(\overline{z},\overline{\delta})$ are linear polynomials over $\overline{z}$, and the same is true for the expressions $\mathrm{GCD}(f(\overline{z}),F(\overline{\delta}))$, since $F(\overline{\delta})$ is always positive. Therefore, we can apply GCD-Lemma; it is technically convenient to replace a pair of conditions (ii) and (iii) by ((iii)). By Remark 2.5.1, we can also allow $i = j$ in ((iii)) instead of rewriting separately condition (i).

((iii)) for every $i,j \in [1..\widetilde{m}]$. For this condition we have the following conjunction:

$$\bigwedge_{1\leqslant i,j\leqslant \widetilde{m}} \mathrm{GCD}(\mathrm{GCD}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{H}_j(\overline{\delta})),\widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z})) = \mathrm{GCD}(\widetilde{H}_i(\overline{\delta}),\widetilde{H}_j(\overline{\delta})). \tag{2.34}$$

Next we show that (2.34) can be rewritten as a system of gcd-expressions from an $L_{\mathcal{C}}$-formula.

If $\widetilde{F}_i(\overline{z},\overline{\delta})$ is a linear polynomial over $\overline{z}$, this can be done in the obvious way. In the case $\widetilde{F}_i(\overline{z},\overline{\delta}) = \mathrm{GCD}(f_i(\overline{z}),F_i(\overline{\delta}))$, we have

$$\mathrm{GCD}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{H}_j(\overline{\delta})) = \mathrm{GCD}(f_i(\overline{z}),\mathrm{GCD}(F_i(\overline{\delta}),\widetilde{H}_j(\overline{\delta})).$$

To satisfy the restrictions on p-valuated primitive gcd-terms, we again use the equalities $\mathrm{GCD}(V_p(x),y) = V_p(\mathrm{GCD}(x,y))$ and $\mathrm{GCD}(V_p(x),V_q(y)) = V_p(1) = V_q(1) = 1$ for different prime numbers p and q. Rewriting (iv), we will implicitly use these two formulas and the obvious equality $V_p(V_q(x)) = 1$ to move V_p to the outer level of terms of the first-order language of the signature $\langle 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\{V_p\}_{p\in\mathbb{P}},\mathrm{GCD},=\rangle$, where $\mathbb{P}$ is the set of prime numbers.

(iv). Considering this condition the same way as in the proof of Lemma 2.5.4, we have the following conjunction:

$$\bigwedge_{p\leqslant\widetilde{m}\wedge p\in\mathbb{P}} \left(\bigwedge_{I\subseteq[1..\widetilde{m}]\wedge|I|=p} \Omega_{p,I}(\overline{z},\overline{\delta}) \right), \tag{2.35}$$

where

$$\Omega_{p,I}(\overline{z},\overline{\delta}) \rightleftharpoons \bigvee_{i\in I\wedge j\in[1..\widetilde{m}]} V_p(p\widetilde{H}_i(\overline{\delta})) \mid \widetilde{H}_j(\overline{\delta}) \vee \bigvee_{i\in I} V_p(\widetilde{H}_i(\overline{\delta})) = V_p(\widetilde{F}_i(\overline{z},\overline{\delta})) \vee \bigvee_{i,j\in I\wedge i\neq j} V_p(\widetilde{H}_i(\overline{\delta})) \mid \widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z}).$$

In order to obtain gcd-expressions from an $L_{\mathcal{C}}$-formula, we first use formula (2.14) to rewrite every divisibility $V_p(p\widetilde{H}_i(\overline{\delta})) \mid \widetilde{H}_j(\overline{\delta})$. This gives us the following equality:

$$V_p(\mathrm{GCD}(p\widetilde{H}_i(\overline{\delta}),\widetilde{H}_j(\overline{\delta}))) = V_p(p\widetilde{H}_i(\overline{\delta})).$$

Next, for every equality $V_p(\widetilde{H}_i(\overline{\delta})) = V_p(\widetilde{F}_i(\overline{z},\overline{\delta}))$ we apply (2.15) and (2.34) for the case $i = j$, i.e., we have

$$V_p(\widetilde{H}_i(\overline{\delta})) = V_p(\widetilde{F}_i(\overline{z},\overline{\delta})) \Leftrightarrow \begin{cases} \mathrm{GCD}(\widetilde{H}_i(\overline{\delta}),p\widetilde{F}_i(\overline{z},\overline{\delta})) = \widetilde{H}_i(\overline{\delta}) \\ \mathrm{GCD}(p\widetilde{H}_i(\overline{\delta}),\widetilde{F}_i(\overline{z},\overline{\delta})) = \widetilde{H}_i(\overline{\delta}). \end{cases}$$

Finally, every divisibility $V_p(\widetilde{H}_i(\overline{\delta})) \mid \widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z})$ can be rewritten by its definition:

$$\mathrm{GCD}(V_p(\widetilde{H}_i(\overline{\delta})),\widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z})) = V_p(\widetilde{H}_i(\overline{\delta})).$$

Since we introduced only gcd-expressions with primitive gcd-terms (or p-valuated primitive gcd-terms) on their left-hand sides, Greek variables that appear in $\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ in gcd-expressions of the form $\mathrm{GCD}(f_i(\overline{z}),g_i(\overline{z}) + x) = d_i\delta_i$ will be excluded from the list $\overline{\delta^{(1)}}$ and will be included in the list $\overline{\delta^{(2)}}$. Therefore, moving all disjunctions to the outer level, we obtain a desired $L_{\mathcal{C}}$-formula. This concludes the construction of quasi-QE algorithm $\mathcal{C}$ and the proof of Proposition 2.6.2. $\square$

2.7 Conclusion and Connections with Chapter 3

We believe that quasi-QE algorithms $\mathcal{C}^+$ and $\mathcal{C}$ might be helpful when trying to prove decidability of the existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp, P_2 \rangle$ or prove this at least for its positive fragment. It seems natural to consider these theories if we hope to answer positively to J. Robinson's question about decidability of $\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, |, P_2 \rangle$. The functions V_p for prime numbers p have extensively been used in $\mathcal{C}$, and we know that the graph of V_k is quantifier-free definable in $\langle \mathbb{Z}; 1, +, -, \leqslant, |, P_k \rangle$ for every integer $k \geqslant 2$. This suggests the following question: whether the existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, |, P_2, P_3, P_4, \ldots \rangle$ is decidable. In Example 3.1.3 from Chapter 3 we observe that if we replace all the predicates P_k in this structure by a single binary predicate $Pow_x(y) \rightleftharpoons \exists z(y = x^z)$, the resulting structure will have undecidable existential theory. Note that it would be interesting to consider this predicate together with multiplication instead of addition. If we could prove that $\exists\mathrm{Th}\langle \mathbb{Z}_{>0}, \{a\}_{a \in \mathbb{Z}_{>0}}, \cdot, Pow, = \rangle$ is decidable, this result would be an analogue of the BL-theorem in multiplication world.

The question of M. Bozga and R. Iosif from the epigraph motivated the research on some general results on existential definability within the arithmetic of addition and divisibility. In Theorem 5, we have presented a characterization of the relations that are positively existentially definable in the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$. However, the problem seems to be rather difficult if we include the order relation in this structure. For example, in the case of the structure $\langle \mathbb{N}; 0, S, \leqslant, \perp \rangle$, a straightforward substitution of $[x,y] \not\perp [u,v] \rightleftharpoons \exists u \exists v\, (u \in [x,y] \wedge v \in [z,t] \wedge u \perp v)$ for coprimeness does not give the desired characterization. We deal with the order relation in $\mathcal{C}^+$ and $\mathcal{C}$ by using LS-Lemma. These algorithms show that the decision procedure becomes more complicated for the cases when we allow the order relation and the dis-coprimeness relation. It would be interesting to find out whether we can extract any information on positive existential definability in some structures using quasi-QE algorithms for the P$\exists$-theories of these structures.

In this chapter we considered definability and decidability problems since our aim was to demonstrate various applications of two main tools from Chapter 1: GCD-Lemma and quasi-quantifier elimination algorithms. However, we did not consider computational complexity of these problems. Studying complexity of arithmetical theories is almost always a challenging task, and it is highly doubtful that a straightforward analysis of quasi-QE algorithms $\mathcal{R}$ or $\mathcal{C}$ would give us a better result than the **NEXPTIME** upper bound for $\exists L_{PAD}$-formulas from [41]. Since this chapter mainly focuses on Presburger arithmetic with coprimeness, let us mention the following questions: whether for every true $\exists L_{PAC}$-formula there is a satisfying assignment of size at most polynomial in the size of the formula, and whether the problem of existence of integer solutions to systems of the form (2.24) can be solved in polynomial time for every fixed number of variables in $\overline{z}$. It is well-known that the answers to similar questions are affirmative in the case of $\exists L_{PA}$-formulas [6; 26; 66] and negative for $\exists L_{PAD}$-formulas [41; 45]. In fact, L. Lipshitz presented in [45] an NP-complete family of systems with five linear divisibilities and four variables. In the next chapter we will prove an analogue to this result for the predicate of divisibility by two consecutive integers, and the Lipshitz's proof will be given in Example 3.4.1.

In Section 2.5 we proved decidability of the existential mixed real-integer linear arithmetic with integer divisibility. Considering possible generalizations of V. Weispfenning's quantifier elimination for mixed real-integer linear arithmetic [84], it is interesting to study definability and decidability properties of the structure $\langle \mathbb{R}; 1, +, -, [\,], 2^{[\,]}, =, < \rangle$, where $2^{[\,]}$ is a unary function symbol for the function that maps a real number x to $2^{[x]}$. In 1983, A.L. Semënov [69] proved that the structure $\langle \mathbb{N}; 1, +, 2^x, = \rangle$ has quantifier elimination in a certain extension and thus the elementary theory of this structure is decidable; this quantifier elimination algorithm was explicitly shown by F. Point in the preprint [58]. Observe that if we use the function symbol 2^x instead of $2^{[\,]}$, we can easily define multiplication in our structure. We do not know whether $\mathrm{Th}\langle \mathbb{R}; 1, +, -, [\,], 2^{[\,]}, =, < \rangle$ is decidable, however, Example 3.1.4 from the next chapter implies that $\exists\mathrm{Th}\langle \mathbb{R}; 1, +, -, [\,], 2^{[\,]}, =, <, | \rangle$ is already undecidable.

In the same section we also presented two decidable fragments of $\forall\exists$-theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$, however, we know that $\forall\exists$-theory in general is undecidable. This follows from the definability of the graph of squaring function (by using one simple universal formula) and the DPRM-theorem. This universal definition of squaring uses the predicate of divisibility by two consecutive integers $x \,{}^{S}\!|\, y \rightleftharpoons x \mid y \wedge 1 + x \mid y$, and we can even prove that $\forall\exists$-theory of the structure $\langle \mathbb{N}; +, {}^{S}\!| \rangle$ is undecidable. We investigate various relationships between divisibility and ${}^{S}\!|$ from definability and decidability point-of-view in the next chapter.

Chapter 3. Definability and Decaidbility Problems for the Predicate of Divisibility by Two Consecutive Integers

> On the other hand, formulas of the form $\exists \mathbf{x} \forall t \psi(\mathbf{x},t)$ where $\mathbf{x}$ is several variables and t just one variable and ψ is open in the language $\langle +, -, \mid, 0, 1\rangle$ are undecidable.
>
> ...ψ is constructed using the following devices.
>
> $$w = z^2 \Leftrightarrow z \mid w \wedge z+1 \mid w+z \wedge$$
> $$\forall t(z \mid t \wedge z+1 \mid t+z \Rightarrow w+z \mid t+z).$$
>
> L. Lipshitz [45] (1981)

The definition of the graph of squaring provided by Lipshitz implicitly uses the predicate of divisibility by two consecutive integers $x\,{}^S|y \rightleftharpoons x \mid y \wedge 1+x \mid y$. Now we can show that every arithmetical relation is definable in the structure $\langle \mathbb{N}; +, {}^S| \rangle$. In this chapter, we prove that the same holds for the structures $\langle \mathbb{N}; \mid, {}^S| \rangle$ and $\langle \mathbb{N}; S, 2^x, {}^S| \rangle$. We also study existential definability with ${}^S|$ and show, in particular, that the graphs of addition and multiplication are existentially definable in $\langle \mathbb{N}; \cdot, {}^S| \rangle$ and $\langle \mathbb{N}; 1, +, Sq, {}^S| \rangle$. At the end of this chapter, we obtain some difinability results for the structure $\langle \mathbb{N}; <, {}^S| \rangle$.

3.1 Definability in Arithmetic, Def-Completeness and ∃Def-Completeness

3.1.1 Definitions and Examples

In addition to the definitions introduced in Section 1.1.1, we use the following notions.

To formulate the results of this chapter it will be convenient to use the notion of Def-completeness of a certain structure introduced by I. Korec [36]. For any arithmetic predicates $X_1,...,X_n$ that are definable in the structure $\langle \mathbb{N}; +, \cdot, = \rangle$, the structure $\langle \mathbb{N}; X_1,..., X_n \rangle$ is called *complete with respect to the first-order definability* (*Def-complete*) if the graphs of addition and multiplication functions (ternary predicates $x+y=z$ and $x \cdot y = z$) are definable in this structure. Analogously for every *enumerable* predicates $X_1,...,X_n$ we say that the structure $\langle \mathbb{N}; X_1,...,X_n \rangle$ is $\exists$*Def-complete* if in this structure the graphs of addition and multiplication functions are *existentially* definable. An arbitrary structure $\langle \mathbb{N}; \sigma \rangle$ is called Def-complete ($\exists$Def-complete) if it becomes Def-complete ($\exists$Def-complete) after replacement in its signature σ every function symbol by some predicate symbols for the graphs of this functions.

In 2001, I. Korec [36] presented a list of the most well-known Def-complete structures at that time. It is clear that elementary theories of Def-complete structures are undecidable. Among the most interesting examples of Def-complete structures are $\langle \mathbb{N}; S, | \rangle$, proved by J. Robinson [65], and $\langle \mathbb{N}; < , \perp \rangle$, the result of A. Woods [85]. A direct consequence of the DPRM-Theorem [52] is that the existential theory of every $\exists$Def-complete structure is undecidable. For example, from the formula [65]

$$z = x + y \Leftrightarrow (x = 0 \wedge y = 0 \wedge z = 0) \vee (z \neq 0 \wedge S(zx)S(zy) = S(z^2 S(xy))), \tag{3.1}$$

we see that the structure $\langle \mathbb{N}; S, \cdot \rangle$ is $\exists$Def-complete. Let us consider another examples.

Example 3.1.1. *The structure* $\langle \mathbb{N}; {}^\wedge, = \rangle$ *is* $\exists$*Def-complete.*

Proof. We are going to show that the graphs of addition and multiplication are existentially definable using exponentiation and equality. First, define the constants 0 and 1 using quantifier-free formulas: $x = 1 \Leftrightarrow x^\wedge x = x$ and $x = 0 \Leftrightarrow x^\wedge x = 1 \wedge \neg x = 1$. It is not difficult to see that

$$\begin{aligned} z = x \cdot y &\Leftrightarrow \exists t(\neg t = 0 \wedge \neg t = 1 \wedge t^\wedge z = (t^\wedge x)^\wedge y) \\ z = x + y &\Leftrightarrow \exists t(\neg t = 0 \wedge \neg t = 1 \wedge t^\wedge z = (t^\wedge x) \cdot (t^\wedge y)). \end{aligned}$$

□

The BL-Theorem shows that the structure $\langle \mathbb{N}; 1, + , | \rangle$ is not $\exists$Def-complete. From the existential definitions (2) for the relation GCD$(x,y) = z$ and its negation, we obtain that every relation is $\exists$-definable in the structures $\langle \mathbb{N}; 1, + , | \rangle$ if and only if it is $\exists$-definable in $\langle \mathbb{N}; 1, + ,\text{GCD} \rangle$. Therefore, the latter structure is also not $\exists$Def-complete. In contrast to the graph of the GCD function, for the graph of the least common multiple LCM we have the following:

Example 3.1.2. *The structure* $\langle \mathbb{N}; 1, + ,\text{LCM} \rangle$ *is* $\exists$*Def-complete.*

Indeed, since $z = x \cdot y \Leftrightarrow (x + y)^2 = x^2 + y^2 + 2z$ it is sufficient to define the relation $y = x^2$ using the formula LCM$(x,x + 1) = x + y$.

In the previous chapters, we noticed that it is not known whether the existential theory of the structure $\langle \mathbb{N}; 1, + , | , P_2 \rangle$ is decidable, where $P_2(y) \rightleftharpoons \exists z(y = 2^z)$. The relation P_2 can be generalized as follows: $Pow_x(y) \rightleftharpoons \exists z(y = x^z)$. We are going to show that the existential theory of natural numbers with addition and Pow is undecidable.

Example 3.1.3. *The structure* $\langle \mathbb{N}; 1, + , Pow \rangle$ *is* $\exists$*Def-complete.*

Proof. As usual, since $x = y \Leftrightarrow Pow_x y \wedge Pow_y x$, it is sufficient to define by some existential formula the graph of squaring function. Indeed, for this relation there is a quantifier-free formula:

$$y = x^2 \Leftrightarrow Pow_x y \wedge Pow_{2x} 4y \wedge Pow_{3x} 9y. \tag{3.2}$$

Suppose $y = x^k$ for some $k \in \mathbb{N}$. Then $4x^k = (2x)^l$ for $l \in \mathbb{N}$. By representing x as $2^\alpha z$, where $z \perp 2$, we obtain the following:

$$2^{\alpha k+2} z^k = 2^{\alpha l+l} z^l.$$

If $z = 0$ then $x = y = 0$. In the case where $z > 1$, it is necessary that $k = l = 2$, and thus $y = x^2$. For the case $x = 2^\alpha$, consider the last conjunct of (3.2), where we have $9 \cdot 2^{\alpha k} = (3 \cdot 2^\alpha)^m$ for some non-negative integer m. It is obvious that $m = 2$, hence $k = 2$ and $y = x^2$. □

Now consider the following example. N.K. Kosovskii [37] showed that for every predicate of fixed-power growth $T(x,y)$ the structure $\langle \mathbb{N}; 1, +, |, T\rangle$ is $\exists$Def-complete. A binary predicate T, defined over the natural numbers, is called a *fixed-power growth predicate* if there are such positive rational constants C,D,c,d, that $d > 1$ and the following two conditions simultaneously hold:

1. for every x,$y \in \mathbb{N}$, if $T(x,y) \wedge x > 0$ then $y \leqslant Cx^D$,
2. for every $x \in \mathbb{N}$ there is $y \in \mathbb{N}$ such that $y \geqslant cx^d \wedge T(x,y)$.

Using this result, we can now prove the following statement.

Example 3.1.4. *The structure* $\langle \mathbb{N}; 1, +, |, 2^x\rangle$ *is* $\exists$*Def-complete.*

Proof. We will show that the relation $|y| \leqslant 2|x|$ is existentially definable, where $|x|$ is the length of binary representation of a given natural number x. This predicate is a predicate of a fixed-power growth since on the one hand, if $|y| \leqslant 2|x|$ and $x \neq 0$, then $y \leqslant 4x^2$, and on the other hand, it is obvious that $|x^2| \leqslant 2|x|$, and we can choose the constants $C = 4$, $D = 2$, $c = 1$, $d = 2$.

The definitions $x = y \Leftrightarrow x \mid y \wedge y \mid x$; $x = 0 \Leftrightarrow x + x = x$; $x \leqslant y \Leftrightarrow \exists z(y = x + z)$ imply that it is sufficient to define the relation $x = |y|$ using the formula

$$x = |y| \Leftrightarrow (x = 1 \wedge y = 0) \vee \exists t(t + 1 = x \wedge 2^t \leqslant y \wedge y + 1 \leqslant 2^x). \qquad \square$$

3.1.2 Divisibility by Two Consecutive Integers

In the introduction, we defined the predicate $x \,{}^S|\, y \rightleftharpoons x \mid y \wedge 1+x \mid y$, which was used by L. van den Dries and A. Wilkie in the study of growth of functions whose graphs are existentially definable in the structure $\langle \mathbb{N}; 1, +, |\rangle$. They showed that for every such function $f : S \to \mathbb{N}$ for $S \subseteq \mathbb{N}^n$ there is $c \geqslant 1$ such that for every non-zero vector $(x_1,...,x_n) \in S$ we have $f(x_1,...,x_n) \leqslant c\,(x_1 + ... + x_n)$. Moreover, for every unbounded function f there is a real number $c \in (0,1)$ such that for an infinite number of vectors $(x_1,...,x_n) \in S$, it holds $f(x_1,...,x_n) > (x_1 + ... + x_n)^c$. A final remark [23, p. 526] provides a simple example showing that it is not possible to improve the lower bound to a linear one. It is sufficient to consider the predicate ${}^S|$ and the following function:

$$f(x,y) = \begin{cases} x, & x > 0 \wedge y > 0 \wedge x \,{}^S|\, y \\ 0, & \text{otherwise} \end{cases}. \tag{3.3}$$

We see that $f(x,y)$ is an unbounded function such that $f(x,y) < (x + y)^{\frac{1}{2}}$ for any $(x,y) \in \mathbb{N}^2$.

It was implicitly used by L. Lipshitz [45] for defining the graph of the squaring function in the structure $\langle \mathbb{N}; 1, +, |\rangle$ with only one universal quantifier. Note also that Example (4) from [43], which demonstrates that it is impossible to obtain a polynomial upper bound on the smallest satisfying assignment for systems of divisibilities and inequalities of linear polynomials in $\mathbb{Z}$, can easily be rewritten using only the predicate ${}^S|$.

Thus, it would be interesting to study this predicate independently in the sense of arithmetical definability and also decidability problems for the theories containing this predicate

such as, for example, $\exists\mathrm{Th}\langle\mathbb{N};\cdot,{}^{S}|\rangle$. In the survey paper by I. Korec [36] we do not see any structures with predicates related to ${}^{S}|$, hence it would also be interesting to consider some definability (and, in particular, existential definability) problems for this predicate. Note that Lipshitz's definition (3) almost immediately yields Def-completeness of the structure $\langle\mathbb{N};+,{}^{S}|\rangle$.

Observe that there is a possible connection between ${}^{S}|$ and the coprimeness relation. We can generalize coprimeness to increasing factorial powers (see for example [27]) as follows:

$$x \perp_k y \rightleftharpoons \mathrm{GCD}(x^{\overline{k}},y^{\overline{k}}) = 1^{\overline{k}}, \tag{3.4}$$

where $x^{\overline{k}} = x(x+1)...(x+k-1)$. In particular, the case of $k = 1$ is the usual relation of coprimeness, and for $k = 2$ we have $x \perp_2 y \rightleftharpoons \mathrm{GCD}(x(x+1),y(y+1)) = 2$. Although the definability of coprimeness in $\langle\mathbb{N};<,{}^{S}|\rangle$ does not seem obvious, for the case of $k = 2$ this relation is definable in the structure $\langle\mathbb{N};S,{}^{S}|\rangle$ by the formula $\exists z(x\,{}^{S}|z \wedge y\,{}^{S}|SSz)$. Indeed, the Chinese remainder theorem implies that the specified formula can be rewritten as:

$$\exists z \begin{cases} z \equiv \quad 0 \,(\mathrm{mod}\ x(x+1)) \\ z \equiv -2 \,(\mathrm{mod}\ y(y+1)) \end{cases} \Leftrightarrow \mathrm{GCD}(x(x+1),y(y+1)) \mid 2, \tag{3.5}$$

and on the right-hand side we actually have an equality, since both arguments of GCD are even. We will use this predicate to prove Def-completeness of the structure $\langle\mathbb{N};S,2^x,{}^{S}|\rangle$.

3.2 Def-Completeness for ${}^{S}|$ and Divisibility

First introduce some simple predicates that can be defined using only ${}^{S}|$.

Lemma 3.2.1. *The properties $x = 0$, $x = 1$ and the relation $x = y$ are definable in the structure $\langle\mathbb{N};{}^{S}|\rangle$.*

Proof. It is clear that $x = 0 \Leftrightarrow x\,{}^{S}|x$; $x = 1 \Leftrightarrow \forall y\forall z(z\,{}^{S}|y \Rightarrow x\,{}^{S}|y)$. Indeed, if $y = 2$ and $z = 1$, then it is necessary that $x = 1$, while for any y such that $z\,{}^{S}|y$ for some z, the formula $1\,{}^{S}|y$ is always true. Finally, $x = y \Leftrightarrow \forall z(x\,{}^{S}|z \Longleftrightarrow y\,{}^{S}|z)$. In the case of $x = 0$ and $y > 0$, it is sufficient to consider $z = y(y+1)$. If both arguments are positive and when, for example, $x < y$, then take $z = x(x+1)$. □

Now consider definability and decidability problems for structures with ${}^{S}|$ and some arithmetic predicates, which are definable using only multiplication and equality.

Proposition 3.2.1. *The structure $\langle\mathbb{N};|\,,{}^{S}|\rangle$ is Def-complete.*

Proof. By the well-known theorem of J. Robinson [65], the structure $\langle\mathbb{N};S,|\rangle$ is Def-complete. Therefore, we only need to define the relation $y = Sx$.

The relation $x \perp y$ is definable by the formula $\forall t(t \mid x \wedge t \mid y \Rightarrow t = 1)$. Thus we obtain the following definition:

$$y = Sx \Leftrightarrow (x = 0 \wedge y = 1) \vee (\neg x = 0 \wedge x \perp y \wedge \forall z(x \,{}^{S}|z \Leftrightarrow x \mid z \wedge y \mid z)).$$

It is obvious that this formula is true when $y = Sx$. We are going to show that such pairs of natural numbers are the only ones that satisfy the formula. Let $x \neq 0$. Then for $z = x(x+1)$, since $y \mid z$ and $x \perp y$, it is necessary that $y \neq 0$ and $y \mid Sx$. Thus, we have $0 < y \leqslant Sx$. If we assume that $y < Sx$, then we obtain a contradiction for $z = x \cdot y$, since simultaneously $x \cdot y < x(x+1)$ and $x(x+1) \mid z$. □

The elementary theory of natural numbers with divisibility $\mathrm{Th}\langle \mathbb{N}; | \rangle$ and the elementary theory with coprimeness $\mathrm{Th}\langle \mathbb{N}; \perp \rangle$ are decidable. This follows from the definability of these predicates using multiplication and equality (for the predicate of coprimeness we can use the formula from the proof of Proposition 3.2.1 and $x = 1 \Leftrightarrow \forall y(x \cdot y = y)$) and decidability of Skolem Arithmetic $\mathrm{Th}\langle \mathbb{N}; \cdot, = \rangle$, proved by A. Mostowski [53]. Thus, for the predicate $x \,{}^{S}|y$ we have the following corollary from Proposition 3.2.1.

Corollary 3.2.1.1. *The relation* ${}^{S}|$ *is not definable in the structure* $\langle \mathbb{N}; \cdot, = \rangle$.

3.3 Undecidability of the Existential Arithmetic with ${}^{S}|$ and Multiplication

If we now proceed to only existential theories, then we see that decidability of $\exists\mathrm{Th}\langle \mathbb{N}; | \,, {}^{S}| \rangle$ is obvious, since every formula of this theory is a formula of the decidable $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, | \rangle$. Consider the problem of decidability of $\exists\mathrm{Th}\langle \mathbb{N}; \cdot, {}^{S}| \rangle$. In this section we will show that the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$ is $\exists$Def-complete. First we would like to define existentially the relations $x = 1$ and $x = y$ in $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$. To this end, we prove the following lemma.

Lemma 3.3.1. *For every integer* $x \geqslant 1$ *and integer* $y \geqslant 0$ *the divisibility* $y(x+1)+1 \mid x^2$ *holds if and only if* $y = 0$ *or* $y = x - 1$.

Proof. It is obvious that $y = 0$ and $y = x - 1$ satisfy the divisibility. We are going to show that there are no other solutions.

It follows from the divisibility that $y \in [0,x-1]$. Let $y = x - k$ for some $k \in [1,x)$, then

$$y(x+1)+1 \mid x^2 \Leftrightarrow \exists k(y(y+k+1)+1 \mid (y+k)^2 \wedge y = x - k).$$

Rewrite the divisibility under the quantifier, subtracting the left argument from the right one. In the resulting expression $(k-1)y + k^2 - 1$, factoring out the common multiple $(k-1)$ we obtain the formula

$$y(y+k+1)+1 \mid (y+k)^2 \Leftrightarrow y(y+k+1)+1 \mid (k-1)(y+k+1).$$

Since $y > 0$, we have $y(y+k+1)+1 \perp y+k+1$ and thus $y(y+k+1)+1 \mid k-1$. Moreover, $y(y+k+1)+1 > k+1$, and hence $k = 1$ and $y = x-1$. This concludes the proof of Lemma. □

Note that in Lemma 3.2.1 we have defined a quantifier-free formula for $x = 0$. Let us now prove the following auxiliary statement.

Lemma 3.3.2. *The properties $x \neq 1$, $x = 1$, and the relations $x = y$, $y = x^2 - 1$, $x \mid y$ are existentially definable in the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$.*

Proof. For the first predicate, we can use the negation of the definition of $x = 1$ from Lemma 3.2.1: $x \neq 1 \Leftrightarrow \exists y \exists z (z \, {}^{S}|y \wedge \neg x \, {}^{S}|y)$. Next, from Lemma 3.3.1, it follows that

$$x > 1 \wedge y > 1 \wedge y = x^2 - 1 \Leftrightarrow x \neq 0 \wedge y \neq 0 \wedge x \, {}^{S}|xy \wedge y \, {}^{S}|yx^2). \tag{3.6}$$

Indeed, $x \, {}^{S}|xy \Leftrightarrow x+1 \mid y$, but $y \, {}^{S}|yx^2 \Leftrightarrow y+1 \mid x^2$ for positive x and y, and we obtain equivalence (3.6). Now using thus defined predicate $x > 1 \wedge y > 1 \wedge y = x^2 - 1$, we have the following formula:

$$x > 1 \wedge y > 1 \wedge x = y \Leftrightarrow \exists u \exists v \begin{pmatrix} x > 1 \wedge u > 1 \wedge u = x^2 - 1 \wedge u \, {}^{S}|y^2 u \\ \wedge y > 1 \wedge v > 1 \wedge v = y^2 - 1 \wedge v \, {}^{S}|x^2 v \end{pmatrix}.$$

This «restricted» version of equality gives us a definition of the second of the desired predicates:

$$x = 1 \Leftrightarrow \exists y \exists z (y > 1 \wedge z > 1 \wedge y = z \wedge y > 1 \wedge xz > 1 \wedge y = xz).$$

Now we can define the equality relation $x = y \Leftrightarrow (x = 0 \wedge y = 0) \vee (x = 1 \wedge y = 1) \vee (x > 1 \wedge y > 1 \wedge x = y)$, and also, by using expression (3.6) in the analogous way we define the relation $y = x^2 - 1$. Having equality, divisibility is obtained by definition $x \mid y \Leftrightarrow \exists z (y = xz)$. □

To prove $\exists$Def-completeness of the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$, it is sufficient to define by some existential formula the relation $y = Sx$, since $\langle \mathbb{N}; S, \cdot \rangle$ is already $\exists$Def-complete as it was noticed in the first section. First, we prove another auxiliary lemma.

Lemma 3.3.3. *For every integer $x > 1$ and integer $y \geqslant 0$ the divisibility $yx + 1 \mid x^2 - 1$ holds if and only if $y = 0$ or $y = 1$.*

Proof. The values $y = 0$ and $y = 1$ obviously satisfy the divisibility. We can show that there are no other integers y.

Let $y \geqslant 2$. Since $y \leqslant x - 1$, then $y = x - k$ for some $k \in [1, x-2]$. Add the left argument of the divisibility to the right one and factor out the common multiple $(y + k)$:

$$yx + 1 \mid x^2 - 1 \Leftrightarrow y(y+k) + 1 \mid (y+k)^2 - 1 \Leftrightarrow y(y+k) + 1 \mid (y+k)(2y+k).$$

Since $y > 0$, we have that $y(y+k)+1 \perp y+k$. Therefore, it is required that $y(y+k)+1 \mid 2y+k$, where the first argument is positive and less than $y^2 + ky + 1$ for every $y \geqslant 2$. Thus we conclude that for $y \geqslant 2$ the divisibility is not satisfiable. □

We can now define the following «restricted» version of the relation $y = Sx$.

Lemma 3.3.4. *The relation $x > 2 \wedge y = Sx$ is existentially definable in the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$.*

Proof. We will use the predicates from Lemma 3.3.2. The property $x > 1$ is definable by the formula $x \neq 0 \wedge x \neq 1$.

We are going to show that

$$\begin{gathered} x > 2 \wedge y = Sx \Leftrightarrow \\ \exists z \exists t \left(z > 1 \wedge x > 1 \wedge x \,{}^{S}|xy \wedge yz = x^2 - 1 \wedge t = z^2 - 1 \wedge x \mid t \right). \end{gathered} \tag{3.7}$$

If $y = x + 1$ for some $x > 2$ then take $z = x - 1$ and $t = (x-1)^2 - 1$.

Conversely, for $x > 1$, we have $x \,{}^{S}|xy \Leftrightarrow x + 1 \mid y$ and hence $y = k(x+1)$ for some $k \geqslant 0$ and $k(x+1)z = (x+1)(x-1)$. Therefore, $kz = x - 1$. We obtain that $kz + 1 \mid z^2 - 1$ for some $k \geqslant 0$, and this, by Lemma 3.3.3, implies that k is equal to zero or one. Since $k = 0$ implies $x = 1$, it is only possible that $k = 1$ and $z = x - 1$, which means that $y = x + 1$. □

Theorem 8. *The relations $x = y$ and $y = Sx$ are existentially definable in the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$, hence the structure $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$ is $\exists$Def-complete and its existential theory is undecidable.*

Proof. It is sufficient to define the property $x = 2$ since $y = 3 \Leftrightarrow \exists x (x = 2 \wedge y = x^2 - 1)$, and for the case $x > 2$ we already have definition (3.7) from Lemma 3.3.4. We show that

$$x = 2 \Leftrightarrow \exists y \exists z \exists t \left(zx > 2 \wedge y = Szx \wedge x \mid z \wedge t = y^2 - 1 \wedge z \,{}^{S}|t \right).$$

For $x = 2$, we can take $z = 2$, $y = 5$ and $t = 24$.

To prove the equivalence in the other direction, rewrite the expression in brackets in the following form:

$$zx > 2 \wedge z(z+1) \mid (zx+1)^2 - 1 \wedge x \mid z.$$

Since $z \neq 0$, divide through by z the first divisibility: $z + 1 \mid x(zx + 2)$. From the divisibility $x \mid z$ we obtain that $z+1 \perp x$ and hence $z+1 \mid zx+2$. This divisibility is true if and only if $z+1 \mid 2-x$, or, in terms of congruences $x \equiv 2 (\mathrm{mod}\ z+1)$, but $0 < x < z + 1$ and hence $x = 2$.

Finally, by Lemma 3.3.2, the equality relation $x = y$ is existentially definable in $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$, and the existential definability of $y = Sx$ follows from the definitions of $x = 0$, $x = 1$ from Lemma 3.3.2, the formulas for $x = 2$ and $x = 3$, and $x > 2 \wedge y = Sx$ from Lemma 3.3.4. Thus, we get the desired result from $\exists$Def-completeness of the structure $\langle \mathbb{N}; S, \cdot \rangle$. □

3.4 Def-Completeness, Decidability and Complexity Problems for ${}^{S}|$ with Addition

3.4.1 Addition and ${}^{S}|$

Before we proceed to the problems of definability and decidability for the structures and theories of the natural numbers with ${}^{S}|$ and some predicates, definable with addition, we first prove the following proposition.

Proposition 3.4.1. *The structure* $\langle \mathbb{N}; +, {}^{S}| \rangle$ *is Def-complete.*

Proof. As usual, it is sufficient to define the graph of the squaring function $y = x^2$. Using the fact that $x \leqslant y \Leftrightarrow \exists z(x + z = y)$, we obtain the following definition:

$$y = x^2 \Leftrightarrow x \,{}^{S}|x + y \wedge \forall z(x \,{}^{S}|x + z \Rightarrow y \leqslant z). \tag{3.8}$$

Since $x \,{}^{S}|x + y$ we get that x and y can be equal to zero only simultaneously. For non-zero values of the parameters y is the least natural number such that $x(x+1) \mid x+y$, thus $x^2+x = x+y$. □

In the introduction to the chapter, we have already noted that formula (3.8) is analogous to the L. Lipshitz's definition [45] of the graph of squaring function in the structure $\langle \mathbb{N}; 1, + , | \rangle$:

$$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z(x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z). \tag{3.9}$$

We see that $x \mid y \wedge x + 1 \mid x + y \Leftrightarrow x \,{}^{S}|x + y$. Using definition (3.8), we obtain a corollary from Proposition 3.4.1. Recall that $\exists\forall\mathrm{Th}\langle \mathbb{N}; +, {}^{S}| \rangle$ is the set of all closed prenex formulas of the language $L_{\langle +, \leqslant, {}^{S}| \rangle}$ with quantifier prefixes of the form $\exists x_1 ... \exists x_n \forall y_1 ... \forall y_m$, true in the natural numbers. First prove an auxiliary lemma.

Lemma 3.4.1. *The properties* $x = 0$ *and* $x = 1$ *are quantifier-free definable in the structure* $\langle \mathbb{N}; +, {}^{S}| \rangle$*, and the relations* $x = y$ *and* $x \leqslant y$ *are existentially definable in this structure.*

Proof. Indeed, $x = 0 \Leftrightarrow x \,{}^{S}|x$ and $x = 1 \Leftrightarrow \neg x \,{}^{S}|x \wedge x \,{}^{S}|x + x$. For the equality relation we can use the following existential formula:

$$x = y \Leftrightarrow \exists z \left(x \,{}^{S}|z + x \wedge x \,{}^{S}|z + y \wedge y \,{}^{S}|z + x \wedge y \,{}^{S}|z + y \right). \tag{3.10}$$

When one of the arguments is equal to zero, the other also equals zero. If x,$y \neq 0$ then the first two expressions imply that $x \equiv y (\mathrm{mod}\ x(x + 1))$, and from the third and forth it follows that $x \equiv y (\mathrm{mod}\ y(y + 1))$. We can easily see that now x and y are equal, and thus we obtain $\exists$-definability of the relation $x \leqslant y$. □

Corollary 3.4.1.1. *The theory* $\exists\mathrm{Th}\langle \mathbb{N}; +, {}^{S}| \rangle$ *is decidable and* $\exists\forall\mathrm{Th}\langle \mathbb{N}; +, {}^{S}| \rangle$ *is undecidable.*

Proof. The first part of this proposition follows immediately from the BL-Theorem. The second part follows from the DPRM-Theorem and formula (3.8) in a similar way as in the undecidability proof of $\exists\forall\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$ by L. Lipshitz [45]. Let us describe this proof in more detail.

We will show that every set, which is $\exists$-definable in the structure $\langle\mathbb{N};+,\cdot,=\rangle$, is $\exists\forall$-definable in the structure $\langle\mathbb{N};+,{}^{S}|\rangle$. It is well-known (see a textbook by Yu.V. Matijasevich [52]) that every such set is definable via some formula of the form $\exists\overline{y}(P(\overline{x},\overline{y})=0)$, where $P(\overline{x},\overline{y})$ is a polynomial with integer coefficients. The formula $z=xy\Leftrightarrow(x+y)^2=x^2+y^2+2z$ implies that for every such polynomial equation we can construct an $L_{\langle+,=\rangle}$-formula $\chi(\overline{x},\overline{y},\overline{u},\overline{v})$, where $\overline{u}=u_1,...,u_m$, $\overline{v}=v_1,...,v_m$ and

$$\exists\overline{y}(P(\overline{x},\overline{y})=0)\Leftrightarrow\exists\overline{y}\exists\overline{u}\exists\overline{v}\left(\chi(\overline{x},\overline{y},\overline{u},\overline{v})\wedge\bigwedge_{i\in[1..m]}v_i=u_i^2\right). \tag{3.11}$$

Introduce new variables and rewrite the formula $\chi(\overline{x},\overline{y},\overline{u},\overline{v})$, using (3.10) as an existential $L_{\langle+,{}^{S}|\rangle}$-formula.

It remains to rewrite every expression $v_i=u_i^2$ for $i=1..m$ using some universal $L_{\langle+,{}^{S}|\rangle}$-formulas. To this end, we have to show that $x\leqslant y$ is $\forall$-definable in the structure $\langle\mathbb{N};+,{}^{S}|\rangle$ and then apply formula (3.8). We see that $x\leqslant y\Leftrightarrow\forall z(1+y+z\neq x)$, and the universal definability of the relations $x=1$ and $x\neq y$ follows from Lemma 3.4.1. □

3.4.2 NP-hard Addition and ${}^{S}|$ Family

In a conference paper by L. Lipshitz [45], the predicate ${}^{S}|$ was implicitly used in the proof of NP-hardness of the problem of satisfiablilty in the natural numbers of systems with only five divisibilities and four variables.

We assume that natural parameters of our formulas are encoded in binary. It is important to notice that L. Lipshitz actually constructed not an NP-hard set, existentially definable in the structure $\langle\mathbb{N};1,+,|\rangle$, but an NP-hard family. Since Lipschitz's proof is quite simple, however published in hard-to-access conference proceedings [45], we give it as an example. Then we will define a notion of addition and divisibility family.

Introduce the following problems in the same way as it is done in the list of NP-hard problems from the book by M. Gary and D. Johnson [25]:

QUADRATIC CONGRUENCES (QC)

INPUT: Positive integers a,b and c.

QUESTION: Is there a positive integer $x\leqslant c$ such that $x^2\equiv a(\mathrm{mod}\ b)$?

NP-completeness of this problem was proved by K. Manders and L. Adleman [49].

SIMULTANEOUS DIVISIBILITY of LINEAR POLYNOMIALS (SDLP)

INPUT: Non-negative integer vectors $a_i=a_{i,0},...,a_{i,n}$ and $b_i=b_{i,0},...,b_{i,n}$ for $i\in[1..m]$.

QUESTION: Do there exist non-negative integers $x_1,x_2,\ldots,x_n$ such that for all $i\in[1..m]$ we have $a_{i,0}+\sum_{j=1}^{n}a_{i,j}x_j\mid b_{i,0}+\sum_{j=1}^{n}b_{i,j}x_j$?

L. Lipshitz [45] proved that SDLP is in **NP** for every fixed number of divisibilities m. He also showed that the problem is NP-hard for $m = 5$ and $n = 4$ via a polynomial reduction of QC to this problem. This proof allows us to obtain a similar result for the predicate of divisibility by two consecutive numbers.

Example 3.4.1 (L. Lipshitz [45, Proposition 2])**.** *The problem SDLP is NP-hard for the case when $n = 4$ and $m = 5$.*

Proof. We can assume that in QC the variable x takes its values from the interval $[0..c]$, and that $a < b$. We are going to show that we have the following equivalence over the natural numbers:

$$\exists x \begin{cases} x^2 \equiv a \,(\mathrm{mod}\ b) \\ x \in [0..c] \end{cases} \Leftrightarrow \exists x \exists y \exists u \exists v \begin{cases} b \mid y + (b - a) \\ x + c \mid y + 2cx + c^2 \\ x + (c + 1) \mid y + 2(c + 1)x + (c + 1)^2 \\ y + u \mid c^2 \\ x + v \mid c \end{cases} \tag{3.12}$$

We use the variables u and v to rewrite the fact that $x \in [0..c]$ and $y \in [0..c^2]$. By the Chinese remainder theorem, it follows from the second and the third divisibility that there is a unique solution for y to this subsystem (of two divisibilities) from the interval $[0,(x + c)(x + c + 1))$. We obviously have that $y = x^2$ is a solution to this subsystem; but now we see that since $(x+c)(x+c+1) > c^2$, there are no other solutions in the interval $[0..c^2]$. This implies the equivalence (3.12). □

For the formulas similar to (3.12), we can introduce the following notion.

Definition 2. ***Addition and divisibility family*** *is every set $S \subseteq \mathbb{N}^n$ for which there exists a quantifier-free $L_{\langle 1,+,\cdot,|\rangle}$-formula $\varphi(\overline{x},\overline{y})$, linear over $\overline{y}$, such that $\overline{a} \in S \Leftrightarrow \exists \overline{y} \varphi(\overline{a},\overline{y})$.*

Thus, we presented an NP-hard addition and divisibility family in Example 3.4.1.

It is obvious that every addition and divisibility family is existentially definable in the structure $\langle \mathbb{N}; +, \cdot\ , = \rangle$. Definition 2 can be generalized over arbitrary arithmetical structures, but this will lead us far from the main topic of the chapter. Now we introduce an analogue to Definition 2 for the relation of divisibility by two consecutive integers.

Definition 3. ***$\langle +, {}^{S}| \rangle$-family*** *is every set $S \subseteq \mathbb{N}^n$ for which there exists a quantifier-free $L_{\langle +,\cdot,\, {}^{S}| \rangle}$-formula $\varphi(\overline{x},\overline{y})$, linear over $\overline{y}$, such that $\overline{a} \in S \Leftrightarrow \exists \overline{y} \varphi(\overline{a},\overline{y})$.*

We say that a family S is NP-hard if the problem of deciding $\overline{a} \in S$ is NP-hard, where we assume that all natural numbers from vector $\overline{a}$ are encoded in binary. We can now prove the following proposition.

Proposition 3.4.2. *There exists an NP-hard $\langle +, {}^{S}| \rangle$-family.*

Proof. We prove this statement by constructing a polynomial reduction from NP-complete problem of solvability of quadratic congruence $x^2 \equiv a (\mathrm{mod}\ b)$ in the interval $[2..c]$ for positive integer

parameters a, b and c, where $c \geqslant 2$. NP-completeness of the latter problem follows as a direct consequence of the NP-completeness of QC.

We can construct an existential $L_{\langle +,\cdot,{}^S| \rangle}$-formula $\exists \overline{y} \varphi(a,b,c,\overline{y})$ that defines a $\langle +, {}^S| \rangle$-family of triples of natural numbers (a,b,c) with the following property. If a, b and c are positive integers and $c \geqslant 2$, then

$$\exists x \left(x^2 \equiv a (\mathrm{mod}\ b) \wedge x \in [2..c] \right) \Leftrightarrow \exists \overline{y} \varphi(a,b,c,\overline{y}).$$

This reduction will obviously be polynomial since we will construct an explicit formula in the same way as in Example 3.4.1.

We are going to show that we have the following equivalence over the natural numbers:

$$\exists x \begin{cases} x^2 \equiv a \,(\mathrm{mod}\ b) \\ x \in [2..c] \end{cases} \Leftrightarrow \exists x \exists y \begin{cases} b \mid y + (b-a) \\ cx+1 \mid c^2 y + 3cx + 2 \\ cx+2 \mid c^2 y + 3cx + 2 \\ x \in [2..c] \\ y \in [4..c^2] \end{cases} \tag{3.13}$$

To complete the proof of the proposition, we use the following steps. Using the formula $b \,{}^S|(b+1)y + (b+1)(b-a)$, we can rewrite the first divisibility. Conjunction of the second and the third divisibility is exactly the expression $cx+1 \,{}^S| c^2 y + 3cx + 2$, and the last two expressions of the system can be rewritten using existential formulas for the relation $\leqslant$ from Lemma 3.4.1.

Necessity of every condition of the right-hand side system of (3.13) is obvious. Let us prove that this system has the only solution $y = x^2$.

We see that $cx+1 \perp c^2$, while we have $\mathrm{GCD}(cx+2, c^2) = 2$ when c is even, and $cx+2 \perp c^2$ when c is odd. By the Chinese remainder theorem, the subsystem of the second and the third divisibility has a unique solution in the interval $\left[0, \frac{(cx+1)(cx+2)}{2}\right)$, when c is even and, otherwise, a unique solution in the interval $[0, (cx+1)(cx+2))$. Since $x \geqslant 2$, we have $\frac{(cx+1)(cx+2)}{2} > 2c^2$. Therefore, the only solution for $y \in [4..c^2]$ is $y = x^2$. This concludes the proof. □

Since by L. Lipshitz's theorem [45], every addition and divisibility family is in **NP**, our NP-hard family will be NP-complete. It is clear that the set of all the relations, $\exists$-definable in the structure $\langle \mathbb{N}; 1, +, | \rangle$, is a proper subset of the set of all such families. Studying properties of addition and divisibility families seems to be rather interesting problem.

3.4.3 The Set of Squares, Addition and ${}^S|$

In connection with definition of the graph of squaring function (3.9), L. van den Dries and A. Wilkie ask [23, p. 505] whether the relation $\neg Sq(x) \rightleftharpoons \forall y (y \neq x^2)$ is existentially definable in the structure $\langle \mathbb{N}; 1, +, | \rangle$. On the other hand, while the question of $\exists$Def-completeness of the structure $\langle \mathbb{N}; 1, +, Sq \rangle$ remains an open problem (see [46; 56], a positive answer would follow from

the truth of Büchi's five-squares problem), it seems that L. van den Dries and A. Wilkie knew that the structure $\langle \mathbb{N}; 1, +, Sq, | \rangle$ was $\exists$Def-complete. Since we did not find a reference to this result, we are going to show that the relation $y = x^2$ is definable in this structure by a simple quantifier-free formula. A slight transformation of this proof will give us a proof of $\exists$Def-completeness of the structure $\langle \mathbb{N}; 1, +, Sq, {}^S| \rangle$.

Proposition 3.4.3. *The relation $y = x^2$ is quantifier-free definable in the structure $\langle \mathbb{N}; 1, +, Sq, | \rangle$. Thus, this structure is $\exists$Def-complete, and its existential theory is undecidable.*

Proof. Let us show that

$$y = x^2 \Leftrightarrow Sq(y) \wedge Sq(y + 2x + 1) \wedge x \mid y \wedge 1 + x \mid y + 2x + 1. \tag{3.14}$$

We can rewrite the last divisibility as $1 + x \mid y - 1$. Let $y = z^2$. Then it follows from the divisibility $x \mid y$ that $z^2 = xu$ for some $u > 0$ (if $u = 0$ then $y = 0$; thus $1 + x \mid x$ and $x = 0$).

Rewrite the divisibility $1 + x \mid y - 1$ as $1 + x \mid xu - 1$, or equivalently, $1 + x \mid u + 1$. Let $u + 1 = (x + 1)v$ for some $v > 0$. We obtain the following chain of equalities:

$$\begin{aligned} y + 2x + 1 = xu + 2x + 1 &= x((x + 1)v - 1) + 2x + 1 \\ &= x(x + 1)v + (x + 1) = (x + 1)(xv + 1). \end{aligned}$$

It remains to show that v can only be equal to 1.

Assume that $v > 1$ and the following holds:

$$Sq((x + 1)(xv + 1) - 2x - 1) \wedge Sq((x + 1)(xv + 1)).$$

Suppose that $t^2 = (x + 1)(xv + 1)$. Since $v > 1$, we have $t > x + 1$. But in this case we obtain $t^2 - (t - 1)^2 > 2(x + 1) - 1 = 2x + 1$, where $(t - 1)^2$ is obviously the greatest square, less than t^2. Thus $\neg Sq(t^2 - 2x - 1)$ and our assumption is false. We conclude that $v = 1$ and $y = x^2$. □

A direct consequence of this result is that the relation $Sq(x)$ is not existentially definable in the structure $\langle \mathbb{N}; 1, +, | \rangle$. From the formula (3.14) and equivalence $x \mid y \wedge 1 + x \mid y + 2x + 1 \Leftrightarrow x \, {}^S| x + y$ we obtain the following statement.

Corollary 3.4.3.1. *The structure $\langle \mathbb{N}; 1, +, Sq, {}^S| \rangle$ is $\exists$Def-complete.*

3.5 Some Definability Results for ${}^S|$ with Order and Successor

A natural generalization of Proposition 3.4.1 could be the proof of Def-completeness of the structure $\langle \mathbb{N}; <, {}^S| \rangle$. This problem seems to be more challenging, and we will find a sufficient condition of Def-completeness and will prove definability in this structure of the relations $y = 2x$ and $y = x^2$.

In the proof of Theorem 9 we do not need the full strength of J. Robinson's theorem on Def-completeness of the structure $\langle \mathbb{N}; S, | \rangle$. Since the graph of the successor function $y = Sx$ is definable via the formula $x < y \wedge \forall z(x < z \Rightarrow y = z \vee y < z)$, the structure $\langle \mathbb{N}; <, | \rangle$ is also Def-complete. We will implicitly use definability of $y = Sx$ in all subsequent propositions.

Theorem 9. *If the property $P_2(x) \rightleftharpoons \exists y(x = 2^y)$ is definable in the structure $\langle \mathbb{N}; <, {}^S| \rangle$, then the theory $\mathrm{Th}\langle \mathbb{N}; <, {}^S| \rangle$ is undecidable. If we can define the relation $x = 2^y$ in this structure, then $\langle \mathbb{N}; <, {}^S| \rangle$ is Def-complete.*

Proof. We will use the well-known fact [12] that for every $\alpha > \beta \geqslant 0$ such that $\alpha \perp \beta$ and $x > y \geqslant 0$, the following equality holds: $\mathrm{GCD}(\alpha^x - \beta^x, \alpha^y - \beta^y) = \alpha^{\mathrm{GCD}(x,y)} - \beta^{\mathrm{GCD}(x,y)}$. In particular, $\mathrm{GCD}(2^x - 1, 2^y - 1) = 2^{\mathrm{GCD}(x,y)} - 1$ and thus $\mathrm{GCD}(x,y) = x \Leftrightarrow \mathrm{GCD}(2^x - 1, 2^y - 1) = 2^x - 1$. This implies that

$$(2^x - 1)2^x \mid (2^y - 1)2^y \Leftrightarrow 2^x - 1 \mid 2^y - 1 \wedge 2^x \mid 2^y \Leftrightarrow x \mid y. \tag{3.15}$$

The relation $L_1(x,y) \rightleftharpoons y = x^2 + x$ can be defined using the formula

$$(x = 0 \wedge y = 0) \vee \neg y = 0 \wedge x\, {}^S|y \wedge \forall z(\neg z = 0 \wedge x\, {}^S|z \Rightarrow y = z \vee y < z).$$

The divisibility $x(x+1) \mid y(y+1)$ is now definable via the formula $\exists z(L_1(y,z) \wedge x\, {}^S|z)$. If we assume that the relation $x = 2^y$ is definable in the structure $\langle \mathbb{N}; <, {}^S| \rangle$, then we obtain from (3.15) that $x \mid y \Leftrightarrow \exists u \exists v\, (Su = 2^x \wedge Sv = 2^y \wedge u(u+1) \mid v(v+1))$. Now the second part of the theorem follows from the Def-completeness of the structure $\langle \mathbb{N}; <, | \rangle$.

Let us prove the first part of the theorem. To this end, we introduce a substructure of $\langle \mathbb{N}; <, {}^S| \rangle$, isomorphic to $\langle \mathbb{N}; <, | \rangle$. That is, we will define a subset $A \subseteq \mathbb{N}$ and some relations $y \widetilde{<} x$ and $x \widetilde{|} y$ over A such that there is a bijection $f : \mathbb{N} \to A$ with $x < y \Leftrightarrow f(x) \widetilde{<} f(y)$ and $x \mid y \Leftrightarrow f(y) \widetilde{|} f(x)$. From the definability of the relations $x \in A$, $y \widetilde{<} x$ and $x \widetilde{|} y$ in the structure $\langle \mathbb{N}; <, | \rangle$ we will obtain undecidability of $\mathrm{Th}\langle \mathbb{N}; <, {}^S| \rangle$.

Let $A = \{2^x - 1 : x \geqslant 0\}$ and $f : x \mapsto 2^x - 1$. Then, since we assume definability of the property P_2, the relation $x \in A$ is definable via the formula $\exists y(P_2(y) \wedge Sx = y)$. We see that $x < y \Leftrightarrow 2^x - 1 < 2^y - 1$, and thus, by defining $x \widetilde{|} y \rightleftharpoons x(x+1) \mid y(y+1)$, the formula (3.15) implies that the structure $\langle A; <, \widetilde{|} \rangle$ is isomorphic to $\langle \mathbb{N}; <, | \rangle$. □

The approach that has been used to prove undecidability of the elementary theory of the structure $\langle \mathbb{N}; <, P_2, {}^S| \rangle$ is widely applied in the cases where it is difficult to prove Def-completeness of a given structure. For example, it is still an open question whether the structure $\langle \mathbb{N}; S, \perp \rangle$ is Def-complete, while A. Woods [85] and D. Richard [61] independently constructed for this structure different substructures that are isomorphic to $\langle \mathbb{N}; +, \cdot, = \rangle$. Note that for this purpose there was introduced by P. Cégielski, Yu.V. Matiyasevich and D. Richard [16] the notion of *structure with isomorphic reinterpretation property*. They also presented an example of a structure with isomorphic reinterpretation property, which is not Def-complete.

If we now consider the structure $\langle \mathbb{N}; S, {}^S| \rangle$, then using the relation $x \perp_2 y$ defined in Subsection 3.1.2, we can show that definability of the relation $y = 2^x$ in $\langle \mathbb{N}; S, {}^S| \rangle$ also implies Def-completeness. Since by Lemma 3.2.1 the equality relation is definable in $\langle \mathbb{N}; {}^S| \rangle$, we include in our structure a unary function symbol for the function $x \mapsto 2^x$, which will be denoted 2^x.

Proposition 3.5.1. *The structure* $\langle \mathbb{N}; S, 2^x, {}^S| \rangle$ *is Def-complete.*

Proof. We will use another result by D. Richard [62] on the Def-completeness of the structure $\langle \mathbb{N}; S, 2^x, \perp \rangle$. In order to prove our proposition, it is sufficient to define the relation of coprimeness in the structure $\langle \mathbb{N}; S, 2^x, {}^S| \rangle$.

We will again use the fact that $\mathrm{GCD}(2^x - 1, 2^y - 1) = 2^{\mathrm{GCD}(x,y)} - 1$, which implies that $x \perp y \Leftrightarrow 2^x - 1 \perp 2^y - 1$. Now we show that for the predicate $\perp_2$ we have

$$x \perp y \Leftrightarrow (x = 0 \wedge y = 1) \vee 2^{2^x - 1} - 1 \perp_2 2^{2^y} - 2 \tag{3.16}$$

for all non-negative integers x and y. We thus get the desired result from the formula $y = x - 1 \Leftrightarrow \exists z(x = Sy)$ and the fact that the predicate $x \perp_2 y$ is definable in the structure $\langle \mathbb{N}; S, {}^S| \rangle$.

Assume $x \neq 0$. Omit the first disjunct on the right-hand side of (3.16) and, using the definition of $\perp_2$, rewrite it as

$$2^{2^x - 1} - 1 \perp_2 2(2^{2^y - 1} - 1) \Leftrightarrow \mathrm{GCD}((2^{2^x - 1} - 1)2^{2^x - 1}, 2(2^{2^y - 1} - 1)(2^{2^y} - 1)) = 2. \tag{3.17}$$

First we divide the expression by 2; moreover, we can exclude the power of 2 in the first argument of GCD and rewrite the result using the coprimeness symbol in the form $(2^{2^x - 1} - 1) \perp (2^{2^y - 1} - 1)(2^{2^y} - 1)$. This is obviously equivalent to the following conjunction:

$$2^{2^x - 1} - 1 \perp 2^{2^y - 1} - 1 \wedge 2^{2^x - 1} - 1 \perp 2^{2^y} - 1.$$

Applying twice the fact mentioned above, we get $x \perp y \wedge 2^x - 1 \perp 2^y$. This completes the proof of the proposition. □

We do not know whether the relation $y = 2^x$ is definable in the structure $\langle \mathbb{N}; S, {}^S| \rangle$, or at least P_2 in $\langle \mathbb{N}; <, {}^S| \rangle$. Propositions 3.5.2 and 3.5.3 might prove helpful in constructing formulas that define these relations in the latter structure.

Proposition 3.5.2. *The relation* $y = 2x$ *is definable in the structure* $\langle \mathbb{N}; <, {}^S| \rangle$.

Proof. If in the definition of L_1 from Theorem 9 we introduce the notation $M_0(x,y) \rightleftharpoons \neg y = 0$, then

$$L_1(x,y) \Leftrightarrow (x = 0 \wedge y = 0) \vee M_0(x,y) \wedge \forall z(M_0(x,z) \wedge x\,{}^S|z \Rightarrow y = z \vee y < z).$$

Now we can define $L_k(x,y) \rightleftharpoons y = kx^2 + kx$ successively for the indexes $k = 2,3,4$ by using the formulas

$$L_k(x,y) \Leftrightarrow (x = 0 \wedge y = 0) \vee M_{k-1}(x,y) \wedge \forall z(M_{k-1}(x,z) \wedge x\,{}^S|z \Rightarrow y = z \vee y < z),$$

where $M_{k-1}(x,y) \rightleftharpoons M_{k-2}(x,y) \wedge \neg L_{k-1}(x,y)$. Hence we define $y = (2x+1)^2$ in the obvious way, and for the relation $x > 0 \wedge y = (2x-1)^2$ we have the existential formula $\exists z \exists t(Sz = x \wedge L_4(z,t) \wedge y = St)$.

The following formula defines the desired predicate:

$$\begin{aligned} y = 2x \Leftrightarrow (x = 0 \wedge y = 0) \vee \exists z_1 \exists z_2 \exists z_3 \exists z_4 \big(& x > 0 \\ & \wedge z_1 = (2x - 1)^2 \wedge z_2 = y(y - 1) \\ & \wedge z_3 = y(y + 1) \wedge z_4 = (2x + 1)^2 \\ & \wedge z_1 < z_2 \wedge z_3 < z_4 \big). \end{aligned}$$

The expression on the right-hand side requires $y \geqslant 2x \wedge y \leqslant 2x$. □

In order to prove that the graph of squaring function is definable in the structure $\langle \mathbb{N}; <, {}^{S}| \rangle$, we first prove the following lemma.

Lemma 3.5.1. *The relation $y = x(x+1)(x+2)(x+3)$ is definable in the structure $\langle \mathbb{N}; <, {}^{S}| \rangle$.*

Proof. If $y \neq 0$ satisfies $x\,{}^{S}|y \wedge SSx\,{}^{S}|y$, then it can easily be seen that in the case of $3 \mid x$ we have $y = \frac{k}{6}x(x+1)(x+2)(x+3)$, and when $3 \nmid x$ we have $y = \frac{k}{2}x(x+1)(x+2)(x+3)$ for some $k \in \mathbb{N}$.

First define the property $3 \mid x$. Using $x = 0$ and S, we obtain $6 \mid x \Leftrightarrow \exists y(y = 0 \wedge SSy\,{}^{S}|x)$. Thus: $3 \mid x \Leftrightarrow 6 \mid x \vee 6 \mid SSSx$.

Following the same approach as in Proposition 3.5.2, we define

$$S_1(x,y) \Leftrightarrow \neg y = 0 \wedge x\,{}^{S}|y \wedge SSx\,{}^{S}|y \wedge \forall z(\neg z = 0 \wedge x\,{}^{S}|z \wedge SSx\,{}^{S}|z \Rightarrow y \leqslant z),$$

and further, for $i = 2,...,6$ we sequentially add conjunctively to the formula and in the premise of the implication the expression $\neg S_{i-1}(x,y)$ and $\neg S_{i-1}(x,z)$, respectively. Likewise, we define the relations «y is the i-th positive integer, which is divisible by $x(x+1)(x+2)(x+3)$». As a result, we obtain the following:

$$y = x(x+1)(x+2)(x+3) \Leftrightarrow (x = 0 \wedge y = 0) \vee (3 \mid x \wedge S_6(x,y)) \vee (3 \nmid x \wedge S_2(x,y)).$$

□

Proposition 3.5.3. *The relation $y = x^2$ is definable in the structure $\langle \mathbb{N}; <, {}^{S}| \rangle$.*

Proof. We are going to show that the following definition holds:

$$\begin{aligned} y = x^2 \;\Leftrightarrow\; & (x = 0 \wedge y = 0) \vee (x = 1 \wedge y = 1) \vee (x = 2 \wedge y = 4) \\ & \vee \Big(x > 2 \wedge y > 2 \wedge \forall z \big(z = y(y-1) \Rightarrow x\,{}^{S}|z \wedge x-1\,{}^{S}|z \wedge \\ & \wedge (x-2)(x-1)x(x+1) < z \wedge z < (x-1)x(x+1)(x+2) \big) \Big). \end{aligned} \tag{3.18}$$

The conclusion of the implication under the quantifier should ensure that $z = x^2(x^2-1)$. To this end, we require divisibility of z by $x-1, x, x+1$ and enclose z between $x^2(x^2-1) - 2x(x^2-1)$ and $x^2(x^2-1) + 2x(x^2-1)$.

It is clear that $y = x^2$ satisfies the formula. We can prove that only such pairs of values of x and y satisfy this formula.

Let $x, y \geqslant 3$. The expression $x\,{}^{S}|z \wedge x-1\,{}^{S}|z$ implies that $z = \frac{k}{2}(x-1)x(x+1)$; thus we have $(x-2) < \frac{k}{2} < x+2$. Therefore, we obtain the following three possibilities: $z = (x-1)^2x(x+1)$, $z = (x-1)x^2(x+1)$, and $z = (x-1)x(x+1)^2$.

First assume that $y > x^2$. If $z = y(y-1)$ then $z > x^2(x^2-1)$, and the only possibility is $y(y-1) = (x-1)x(x+1)^2 = (x^2-1)(x^2+x)$. Since it is clear that $y < x^2+x$, suppose $y = x^2+k$ for some $k \in [1, x-1]$. Therefore, we have a divisibility $x^2-1 \mid (x^2+k)(x^2+k-1)$, which can be rewritten as

$$(x^2+k)(x^2+k-1) \equiv (k+1)k \equiv 0 \,(\mathrm{mod}\; x^2-1).$$

Now we see that such a number k does not exist, since from the definition of k and the constraint $x \geqslant 3$ we get the following chain of inequalities $0 < k(k+1) \leqslant x(x-1) < x^2 - 1$.

If we now assume that $y < x^2$ then for $z = y(y-1)$ the only possibility is $y(y-1) = (x-1)^2 x(x+1) = (x^2 - x)(x^2 - 1)$, which implies $y > x^2 - x$. Again assuming that $y = x^2 - k$ for some $k \in [1,x-1]$, we obtain that

$$(x^2 - k)(x^2 - k - 1) \equiv (k-1)k \equiv 0 \,(\mathrm{mod}\ x^2 - 1).$$

If $k = 1$ then the original equality has form $(x^2 - 1)(x^2 - 2) = (x^2 - 1)(x^2 - x)$. It follows that either $x = 1$, or $x = 2$, but we have excluded these cases. If $k > 1$ then $0 < k(k-1) < x^2 - 1$, which implies the absence of such k and y. This completes the proof of the statement. $\square$

Conclusion

In essence, the main contribution of this thesis is GCD-Lemma and the notion of quasi-quantifier elimination algorithm from the first chapter, and the main results from Chapters 1 and 2 are obtained using these tools. While Chapter 3 gives some insight into similarities between integer divisibility and divisibility by two consecutive integers from definability and decidability point-of-view, this chapter uses standard techniques and all results look quite predictable.

It was difficult to find an appropriate formulation for fourth condition of GCD-Lemma, since it was easier to prove this lemma using ((iv)), whereas in applications we always use (iv). Moreover, (i) and (ii) echo the Chinese remainder theorem, while it is sometimes more convenient (e.g. in quasi-QE algorithm $\mathcal{C}$ from Proposition 2.6.2) to replace three conditions (i), (ii) and (iii) by a single condition ((iii)) for every $i,j \in [1..m]$. Overall, it is surprising that there exists such a generalization of the Chinese remainder theorem and, moreover, that it can be applied to solve various definability and decidability problems. The results of Section 2.6 were obtained when Chapter 1 was finished. Similarly to quasi-QE algorithm $\mathcal{C}$, Step 2 of algorithm $\mathcal{R}$ can be transformed in order to be "closer" to quantifier elimination. That is, by using binary function symbol GCD, we can introduce less Greek variables (or even do not introduce them at all). At the same time, auxiliary Greek variables greatly simplify the form of gcd-expressions, and thus we can easier reason about formulas with gcd-expressions of this kind.

We believe that a proof of the BL-theorem from The Book [1, Preface] must also give us a description of all the P$\exists$-definable predicates. In Theorem 5, we were able to solve this problem in the case where the order relation is excluded from the structure and divisibility is replaced by coprimeness. Among intermediate structures, the most important ones are the following: $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$ and $\langle \mathbb{Z}; 1, +, -, | \rangle$. For the second structure, it might be helpful to use a result of P. Cégielski [15], who applied model-theoretic methods to prove that there is a quantifier elimination algorithm for a certain extension of $\langle \mathbb{Z}_{>0}; | \rangle$ with some predicates definable in this structure. Note that in our case it is sufficient to consider only P$\exists$-definable relations. A solution to any of these P$\exists$-definability problems would give us a new decidable fragment of the $\forall\exists$-theory of the structure $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Thus, the decidable fragments from Theorem 7 and Corollary 4.1 may appear to be two special cases of a single decidable fragment.

Robinson's question about decidability of $\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, |, P_2 \rangle$ forms the main branch of further research. L. van den Dries (see [58]) gave a model-theoretic proof that there is a quantifier elimination algorithm for a certain extension of the structure $\langle \mathbb{N}; 1, +, \leqslant, P_2 \rangle$ with some functions whose graphs are definable in this structure. For our purposes, it is important to explicitly construct such an algorithm, or at least a quasi-QE algorithm for the existential theory of this structure. Next, if we want to give a positive answer to the generalized Robinson's question from section 2.7, we should first consider the decision problem for $\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, P_2, P_3, P_4, \ldots \rangle$ (note that it is a long-standing open problem of whether $\mathrm{Th}\langle \mathbb{N}; 1, +, \leqslant, P_2, P_3 \rangle$ is decidable [5]). However, these questions are already far from the main topic of this thesis. Concerning possible further directions of research this may suffice.

Bibliography

1. *Aigner*, *M.*, *Ziegler*, *G. M.* Proofs from THE BOOK. — Springer Berlin Heidelberg, 2010.
2. *Backeman*, *P.*, *Rümmer*, *P.*, *Zeljić*, *A.* Interpolating bit-vector formulas using uninterpreted predicates and Presburger arithmetic // Formal Methods in System Design. — 2021. — May.
3. *Bel'tyukov*, *A. P.* Decidability of the universal theory of natural numbers with addition and divisibility // Zapiski Nauchnyh Seminarov LOMI. — 1976. — Vol. 60. — P. 15—28. — (in Russian).
4. *Bel'tyukov*, *A. P.* To the anniversary of Yuri Vladimirovich Matiyasevich // Computer Tools in Education. — 2017. — Dec. — No. 6. — P. 5—11. — (in Russian).
5. *Bès*, *A.* A survey of arithmetical definability // Société mathématique de Belgique. — 2002. — P. 1—54.
6. *Borosh*, *I.*, *Treybig*, *L. B.* Bounds on positive integral solutions of linear diophantine equations // Proceedings of the American Mathematical Society. — 1976. — Vol. 55. — P. 299—304.
7. *Bozga*, *M.*, *Iosif*, *R.* On decidability within the arithmetic of addition and divisibility // Proceedings of FoSSaCS, ser. Lecture Notes in Computer Science. Vol. 3441. — 2005. — P. 425—439.
8. *Bozga*, *M.*, *Iosif*, *R.* On flat programs with lists // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2007. — P. 122—136.
9. *Bozga*, *M.*, *Iosif*, *R.*, *Lakhnech*, *Y.* Flat parametric counter automata // Fundamenta Informaticae. — 2009. — Vol. 91. — P. 275—303.
10. *Büchi*, *J. R.* Weak second-order arithmetic and finite automata // Zeitschrift für Mathematische Logik und Grundlagen der Mathematik. — 1960. — Vol. 6, no. 1—6. — P. 66—92.
11. *Bundala*, *D.*, *Ouaknine*, *J.* On parametric timed automata and one-counter machines // Information and Computation. — 2017. — Vol. 253. — P. 272—303.
12. *Carmichael*, *L.* On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$ // Ann. Math. — 1913. — Vol. 15, no. 2. — P. 30—69.
13. *Carneiro*, *M.* A Lean formalization of Matiyasevič's theorem // arXiv:1802.01795v1. — 2018. — Feb. — arXiv: 1802.01795v1 [math.LO].
14. *Cégielski*, *P.* Théorie élémentaire de la multiplication des entiers naturels // Lecture Notes in Mathematics. — Springer Berlin Heidelberg, 1981. — P. 44—89.
15. *Cégielski*, *P.* La théorie élémentaire de la divisibilité est finiment axiomatisable // Comptes rendus de l'Académie des sciences. Série I, Mathématique. — 1984. — Vol. 299. — P. 367—369.

16. *Cégielski, P., Matiyasevich, Y., Richard, D.* Definability and decidability issues in extensions of the integers with the divisibility predicate // The Journal of Symbolic Logic. — 1996. — Vol. 61, no. 2. — P. 515—540.

17. *Cégielski, P., Richard, D.* In memoriam of Alan Robert Woods // New Studies in Weak Arithmetics, Lecture Notes 211 / ed. by P. Cégielski, C. Cornaros, C. Dimitracopoulos. — CSLI Publications, Stanford, 2013. — P. 15—31.

18. *Cooper, D. C.* Theorem proving in arithmetic without multiplication // Machine intelligence. — 1972. — Vol. 7, no. 91—99. — P. 300.

19. *Degtyarev, A., Matiyasevich, Y., Voronkov, A.* Simultaneous rigid E-unification and related algorithmic problems // Proceedings 11th Annual IEEE Symposium on Logic in Computer Science. — IEEE Comput. Soc. Press, 1996.

20. *Degtyarev, A., Voronkov, A.* Simultaneous rigid E-unification is undecidable // Computer Science Logic. — Springer Berlin Heidelberg, 1996. — P. 178—190.

21. *Dolzmann, A., Seidl, A., Sturm, T.* Redlog user manual, edition 3.0 // Tech. Rep., University of Passau. — 2004. — URL: http://andreasseidl.com/publications/DSS04b.pdf.

22. *Dolzmann, A., Sturm, T.* REDLOG: computer algebra meets computer logic // ACM SIGSAM Bulletin. — 1997. — June. — Vol. 31, no. 2. — P. 2—9.

23. *Dries, L. van den, Wilkie, A.* The laws of integer divisibility, and solution sets of linear divisibility conditions // The Journal of Symbolic Logic. — 2003. — Vol. 68, no. 2. — P. 503—526.

24. Emptiness problems for integer circuits / D. Barth [et al.] // Electronic Colloquium on Computational Complexity. — 2017. — No. 12. — URL: https://eccc.weizmann.ac.il/report/2017/012/ ; Article Number: TR17-012.

25. *Garey, M. R., Johnson, D. S.* Computers and intractability. A guide to the theory of NP-completeness. — NY, USA : W. H. Freeman, Co., 1979.

26. *Gathen, J. von zur, Sieveking, M.* Bounds on positive integral solutions of linear diophantine equations // Proceedings of the American Mathematical Society. — 1978. — Vol. 72. — P. 155—158.

27. *Graham, R., Knuth, D., Patashnik, O.* Concrete mathematics. A foundation for computer science. — Reading : Addison-Wesley, 1989.

28. *Guépin, F., Haase, C., Worrell, J.* On the exitential theories of Büchi arithmetic and linear p-adic fields // Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). — 2019. — P. 1—10. — (LICS '19).

29. *Haase, C.* On the complexity of model checking counter automata : Ph.D. Thesis. — University of Oxford, 2012.

30. *Haase, C.* A survival guide to Presburger arithmetic // ACM SIGLOG News. — 2018. — July. — Vol. 5, no. 3. — P. 67—82.

31. *Haase, C., Mansutti, A.* On deciding linear arithmetic constraints over p-adic integers for all primes //. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

32. *Haase, C., Różycki, J.* On the expressiveness of Büchi arithmetic // Lecture Notes in Computer Science. — Springer International Publishing, 2021. — P. 310—323.

33. *Hodgson, B. R.* On direct products of automaton decidable theories // Theoretical Computer Science. — 1982. — Sept. — Vol. 19, no. 3. — P. 331—335.

34. *Iwane, H., Yanami, H., Anai, H.* SyNRAC: A toolbox for solving real algebraic constraints // Mathematical Software – ICMS 2014. — Springer Berlin Heidelberg, 2014. — P. 518—522.

35. *Knuth, D. E.* The art of computer programming, Volume 4A, The: Combinatorial Algorithms, Part 1. — 1st. — Boston, MA : Addison-Wesley Professional, 2011.

36. *Korec, I.* A list of arithmetical structures complete with respect to the first-order definability // Theoretical Computer Science. — 2001. — Vol. 257, no. 1/2. — P. 115—151.

37. *Kosovskii, N. K.* On solutions of systems consisting both of word equationa and of word length inequalities // Zapiski Nauchnyh Seminarov LOMI. — 1974. — Vol. 40. — P. 24—29. — (in Russian).

38. *Larchey-Wendling, D., Forster, Y.* Hilbert's tenth problem in Coq // arXiv:2003.04604. — 2020. — Mar. — arXiv: 2003.04604 [cs.LO].

39. *Lasaruk, A., Sturm, T.* Weak quantifier elimination for the full linear theory of the integers // Applicable Algebra in Engineering, Communication and Computing. — 2007. — Oct. — Vol. 18, no. 6. — P. 545—574.

40. *Lasaruk, A., Sturm, T.* Effective quantifier elimination for Presburger arithmetic with infinity // Computer Algebra in Scientific Computing. — Springer Berlin Heidelberg, 2009. — P. 195—212.

41. *Lechner, A.* Synthesis problems for one-counter automata // Lecture Notes in Computer Science. — Springer International Publishing, 2015. — P. 89—100.

42. *Lechner, A.* Extensions of Presburger arithmetic and model checking one-counter automata : Ph.D. Thesis. — Oriel College University of Oxford, 2016.

43. *Lechner, A., Ouaknine, J., Worrell, J.* On the complexity of linear arithmetic with divisibility // 30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2015, Kyoto, Japan, July 6-10, 2015. — IEEE Computer Society, 2015. — P. 667—676. — URL: http://dx.doi.org/10.1109/LICS.2015.67.

44. *Lipshitz, L.* The diophantine problem for addition and divisibility // Trans. Amer. Math. Soc. — 1978. — Vol. 235. — P. 271—283.

45. *Lipshitz, L.* Some remarks on the diophantine problem for addition and divisibility // Bulletin de la Société mathématique de Belgique. Série B. — 1981. — Vol. 33, no. 1. — P. 41—52.

46. *Lipshitz, L.* Quadratic forms, the five square problem, and diophantine equations // The collected works of J. Richard Büchi / ed. by S. MacLane, D. Siefkes. — Springer, 1990. — P. 677—680.

47. Logic and p-recognizable sets of integers / V. Bruyère [et al.] // Bulletin of the Belgian Mathematical Society - Simon Stevin. — 1994. — Jan. — Vol. 1, no. 2. — P. 191—238.

48. *Loos, R., Weispfenning, V.* Applying linear quantifier elimination // The Computer Journal. — 1993. — May. — Vol. 36, no. 5. — P. 450—462.

49. *Manders, K., Adleman, L.* NP-Complete decision problems for binary quadratics // Journal of Computer and System Sciences. — 1978. — Vol. 16, no. 2. — P. 168—184.

50. *Mart'yanov, V. I.* Universal extended theories of integers // Algebra i Logika. — 1977. — Vol. 16, no. 5. — P. 588—602. — (in Russian).

51. *Matiyasevich, Y. V.* Enumerable sets are diophantine // Dokl. Akad. Nauk SSSR. — 1970. — Vol. 191, no. 2. — P. 279—282. — (in Russian).

52. *Matiyasevich, Y. V.* Hilbert's tenth problem. — Massachusetts : MIT Press, 1993.

53. *Mostowski, A.* On direct products of theories // The Journal of Symbolic Logic. — 1952. — Vol. 17, no. 1. — P. 1—31.

54. *Moura, L. de, Bjørner, N.* Z3: An efficient SMT solver // Tools and Algorithms for the Construction and Analysis of Systems. — Springer Berlin Heidelberg, 2008. — P. 337—340.

55. *Nipkow, T.* Linear quantifier elimination // Journal of Automated Reasoning. — 2010. — July. — Vol. 45, no. 2. — P. 189—212.

56. *Pasten, H., Pheidas, T., Vidaux, X.* A survey on Büchi's problem: new presentations and open problems // Zap. Nauchn. Sem. POMI. — 2010. — Vol. 377. — P. 111—140.

57. *Pérez, G. A., Raha, R.* Revisiting parameter synthesis for one-counter automata. — 2021. — arXiv: 2005.01071 [cs.LO].

58. *Point, F.* On the expansion $(\mathbb{N}, +, 2^x)$ of Presburger arithmetic // preprint. — 2007. — URL: http://www.logique.jussieu.fr/~point/papiers/Pres.pdf.

59. *Presburger, M.* Über die vollständigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchem die addition als einzige operation hervortritt // Comptes Rendus du I congrès de Mathématiciens des Pays Slaves. — 1929. — P. 92—101.

60. Reachability in succinct and parametric one-counter automata / C. Haase [et al.] // CONCUR 2009 - Concurrency Theory. — Springer Berlin Heidelberg, 2009. — P. 369—383.

61. *Richard, D.* La théorie sans égalité du successeur et de la coprimarité des entiers naturels est indécidable. Le prédicat de primarité est définissable dans le langage de cette théorie // Comptes Rendus de l'Académie des Sciences. Série I: Mathématique. — 1982. — Vol. 294. — P. 143—146.

62. *Richard, D.* All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate // Discrete Mathematics. — 1985. — Vol. 53. — P. 221—247.

63. *Richard, D.* Definability in terms of the successor function and the coprimeness predicate in the set of arbitrary integers // The Journal of Symbolic Logic. — 1989. — Vol. 54, no. 4. — P. 1253—1287.

64. *Richard, D.* What are weak arithmetics? // Theoretical Computer Science. — 2001. — Vol. 257. — P. 17—29.

65. *Robinson, J.* Definability and decision problems in arithmetic // The Journal of Symbolic Logic. — 1949. — Vol. 14. — P. 98—114.

66. *Scarpellini, B.* Complexity of subcases of Presburger arithmetic // Transactions of the American Mathematical Society. — 1984. — Vol. 284, no. 1. — P. 203—218.

67. *Schmid, H. L., Mahler, K.* On the Chinese remainder theorem // Mathematische Nachrichten. — 1958. — Vol. 18, no. 1—6. — P. 120—122.

68. *Semënov, A. L.* On certain extensions of the arithmetic of addition of natural numbers // Izv. Akad. Nauk SSSR Ser. Mat. — 1979. — Vol. 43, no. 5. — P. 1175—1195. — (in Russian).

69. *Semënov, A. L.* Logical theories of one-place functions on the set of natural numbers // Izv. Akad. Nauk SSSR Ser. Mat. — 1983. — Vol. 47, no. 3. — P. 623—658. — (in Russian).

70. *Shen, A., Vereshchagin, N.* Mathematical logic and computation theory. Languages and calculi. — Moscow : MCCME, 2012. — 240 p. — (in Russian).

71. *Sirokofskich, A.* On a weak form of divisibility // Definability and Decidability Problems in Number Theory. — 2016. — P. 2827—2829.

72. *Skolem, T.* Über gewisse satzfunktionen in der arithmetik // Skrifter utgit av Videnskapsselskapet i Kristiania. — 1930. — Vol. I. klasse, no. 7.

73. *Smoryński, C.* Logical number theory I. — Springer Berlin Heidelberg, 1991.

74. *Starchak, M. R.* A proof of Bel'tyukov–Lipshitz theorem by quasi-quantifier elimination. I. Definitions and GCD-Lemma // Vestnik St.Petersb. Univ. Math. — 2021. — Vol. 54, no. 3. — P. 264—272.

75. *Starchak, M. R.* A proof of Bel'tyukov–Lipshitz theorem by quasi-quantifier elimination. II. The main reduction // Vestnik St.Petersb. Univ. Math. — 2021. — Vol. 54, no. 4. — P. 372—380.

76. *Starchak, M.* Some decidability and definability problems for the predicate of divisibility by two consecutive numbers // Computer Tools in Education. — 2018. — Dec. — No. 6. — P. 5—15. — (in Russian).

77. *Starchak, M. R.* Positive existential definability with unit, addition and coprimeness // Proceedings of the International Symposium on Symbolic and Algebraic Computation 2021 (ISSAC '21). — ACM, 07/2021. — P. 353—360.

78. *Sturm, T.* Linear problems in valued fields // Journal of Symbolic Computation. — 2000. — Aug. — Vol. 30, no. 2. — P. 207—219.

79. *Sturm, T.* A survey of some methods for real quantifier elimination, decision, and satisfiability and their applications // Mathematics in Computer Science. — 2017. — Apr. — Vol. 11, no. 3/4. — P. 483—502.

80. *Sturm, T.* Thirty years of virtual substitution // Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC '18). — ACM, 07/2018.

81. The DPRM theorem in Isabelle (short paper) / J. Bayer [et al.] // 10th International Conference on Interactive Theorem Proving (ITP 2019). — Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik GmbH, Wadern/Saarbruecken, Germany, 2019.

82. *Villemaire, R.* The theory of $(\mathbb{N}; +, V_k, V_l)$ is undecidable // Theoretical Computer Science. — 1992. — Dec. — Vol. 106, no. 2. — P. 337—349.

83. *Weispfenning, V.* The complexity of linear problems in fields // Journal of Symbolic Computation. — 1988. — Vol. 5, no. 1/2. — P. 3—27.

84. *Weispfenning, V.* Mixed real-integer linear quantifier elimination // International Symposium on Symbolic and Algebraic Computation 1999 (ISSAC '99). — ACM Press, 1999. — P. 129—136.

85. *Woods, A.* Some problems in logic and number theory : Ph.D. Thesis. — University of Manchester, 1981.

Санкт-Петербургский Государственный Университет

На правах рукописи

Старчак Михаил Романович

Алгоритмы квазиэлиминации кванторов и вопросы выразимости в арифметиках с делимостью

1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Перевод с английского

Научный руководитель:
доктор физико-математических наук, профессор
Косовская Татьяна Матвеевна

Санкт-Петербург — 2022

Оглавление

Стр.

Стр.

Введение

Диссертация посвящена исследованию связи между двумя важными инструментами, применяемыми при изучении вопросов теоретической информатики: алгоритмами элиминации кванторов и теоремы о разрешимости экзистенциальной теории натуральных чисел с единицей, сложением и делимостью. К этой теме непосредственно примыкают вопросы выразимости с помощью отношений, которые можно определить в терминах сложения и делимости целых чисел.

В первой части работы будет введено понятие алгоритма квазиэлиминации кванторов (квази-ЭК), в некотором смысле обобщающее понятие алгоритма элиминации кванторов. Далее строятся два алгоритма квази-ЭК, которые формируют новое доказательство разрешимости экзистенциальной теории натуральных чисел с единицей, сложением и делимостью. Язык сложения и делимости достаточно богат и сложен для изучения; во второй главе понятие алгоритма квази-ЭК используется для получения результатов о выразимости с помощью более слабых средств. В третьей главе мы отходим от вопросов квазиэлиминации и рассматриваем некоторые близкие проблемы выразимости.

0.1 Арифметика со сложением и делимостью и алгоритмы элиминации кванторов

Разрешимость позитивной экзистенциальной теории натуральных чисел с единицей, сложением и делимостью была доказана независимо А.П. Бельтюковым [1] и Л. Липшицем [51] в 1976 году. Иными словами, существует алгоритм проверки совместности в натуральных числах систем вида $f_i(\overline{x}) \mid g_i(\overline{x})$ для всех $i = 1..m$, где $\overline{x} = x_1...x_n$, а $f_i(\overline{x})$ и $g_i(\overline{x})$ суть линейные полиномы с неотрицательными целыми коэффициентами. Несложно также показать, что этот результат сводится к проблеме разрешимости в целых числах систем неравенств и делимостей линейных полиномов с целыми коэффициентами, и наоборот. Или, с точки зрения математической логики, позитивная экзистенциальная теория ($\mathrm{P}\exists\mathrm{Th}$) структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ разрешима. Слово «позитивная» означает, что в системах не используется отношение неделимости. От этого ограничения можно избавиться введением новых переменных посредством формулы

$$x \nmid y \Leftrightarrow (x = 0 \wedge 1 \leqslant |y|) \vee \exists z (1 \leqslant z \wedge z \leqslant |x| - 1 \wedge x \mid y + z), \tag{1}$$

где необходимо лишь переписать равенство нулю и модуль y и x с помощью других символов сигнатуры.

Отметим ещё один способ переформулировать теорему Бельтюкова и Липшица (БЛ-теорему). Пусть трёхместное отношение НОД(x,y) $= z$ есть график функции, вычисляющей НОД целых чисел, причём НОД(0,0) $= 0$. Тогда $x \mid y \Leftrightarrow$ НОД(x,y) $= x \vee$ НОД(x,y) $= -x$. С

другой стороны, из алгоритма Евклида получаем следующие экзистенциальные определения:

$$\begin{aligned} \text{НОД}(x,y) = z \;&\Leftrightarrow\; 0 \leqslant z \wedge z \mid x \wedge z \mid y \wedge \exists u\,(x \mid u \wedge y \mid u + z) \\ \neg\text{НОД}(x,y) = z \;&\Leftrightarrow\; z + 1 \leqslant 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v\,(v \mid x \wedge v \mid y \wedge z + 1 \leqslant v)\,. \end{aligned} \tag{2}$$

Следовательно, используется ли отношение делимости или трёхместное отношение НОД, соответствующие проблемы разрешимости сводятся друг к другу. Именно в таком виде, используя отношение НОД вместо делимости, БЛ-теорема была доказана В. И. Мартьяновым [5] через год после появления оригинальных доказательств. Каждую из рассмотренных переформулировок мы будем далее называть БЛ-теоремой; из контекста несложно будет определить, о какой конкретно вариации идёт речь.

Появлению этой теоремы предшествовало доказательство неразрешимости десятой проблемы Гильберта, полученное в работах М. Дэвиса, Х. Патнэма, Дж. Робинсон и Ю.В. Матиясевича [6; 7] (ДПРМ-теорема). Как было показано в 1974 году Н.К. Косовским [4], эта проблема сводится к вопросу совместности в натуральных числах систем линейных делимостей и выражений вида $T(f(\overline{x}),g(\overline{x}))$, где T есть некоторый предикат степенного роста, а $f(\overline{x})$ и $g(\overline{x})$ являются линейными полиномами с натуральными коэффициентами. Более формально, была доказана неразрешимость $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, \mid, T\rangle$. Отсюда видим, что БЛ-теорема даёт отрицательный ответ на вопрос о том, останется ли проблема неразрешимой, если исключить T из сигнатуры.

Сведением к задаче разрешимости для $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, \mid\rangle$ удалось установить разрешимость ряда проблем теоретической информатики, в то время как ДПРМ-теорема часто служит обратной цели, а именно, доказательству неразрешимости. Например, в 1996 году А. Дегтярёвым, Ю.В. Матиясевичем и А. Воронковым [27] была доказана разрешимость проблемы одновременной жёсткой E-унификации (*simultaneous rigid E-unification*) для языка, сигнатура которого содержит один унарный функциональный символ и счётное число констант. Практически в то же время А. Дегтярёвым и А. Воронковым [28] была установлена неразрешимость общей проблемы одновременной жёсткой E-унификации. В работе 2009 года К. Хаасе, С. Крёйцера, Дж. Оакнина и Дж. Уоррелла [64] с помощью БЛ-теоремы была доказана разрешимость проблемы достижимости для параметрического односчётчикового автомата (*parametric one-counter automata*), а ДПРМ-теорема была применена М. Божгой, Р. Иосифом и Я. Лахнеком [17] для доказательства неразрешимости проблемы достижимости для параметрического плоского счётчикового автомата (*flat parametric counter automata*). В этом смысле БЛ-теорема и ДПРМ-теорема дополняют друг друга.

В действительности, для разрешимых проблем из предыдущего абзаца существует и обратное сведение к задаче разрешимости для $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, \mid\rangle$, и, кроме того, сведения в обоих направлениях можно выполнить за полиномиальное время на недетерминированной машине Тьюринга (см. [49]). Каждая из этих проблем NP-трудна и принадлежит классу **NEXPTIME**, как было установлено в 2015 году А. Лечнер, Дж. Оакнином и Дж. Уоррелом [50], однако более точной классификации временной сложности не известно. Верхняя оценка сложности была получена в результате ряда усовершенствований алгоритма Л. Липшица, что приблизило разрешающую процедуру к алгоритму В.И. Мартьянова. Таким

образом, имеется лишь четыре во многом схожих изложения алгоритма для $\exists\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$. А. Лечнер с соавторами отмечают трудность алгоритма („[...] the considerable mathematical depth and intricacy of Lipshitz's proof, making it diffcult to read and understand [...]“), что привело к неоднократным ошибкам в интерпретации результатов Л. Липшица [52].

Основная идея этих алгоритмов может быть изложена следующим образом. По данной системе линейных неравенств и делимостей $\varpi(x_1,...,x_n)$ строится дизъюнкция систем делимостей специального вида $\varpi_i(x_1,...,x_n)$, выполнимая в $\mathbb{Z}$ тогда и только тогда, когда выполнима $\varpi(x_1,...,x_n)$. Для каждой системы $\varpi_i(x_1,...,x_n)$, исходя из её структуры, можно построить константу ν_i такую, что $\varpi_i(x_1,...,x_n)$ выполнима в целых числах тогда и только тогда, когда она выполнима в целых p-адических числах $\mathbb{Z}_p$ для всякого простого числа $p \leqslant \nu_i$. Разрешимость теперь следует из разрешимости $\exists\mathrm{Th}\langle\mathbb{Q}_p;1,+,-,=,\mathrm{div}\rangle$ для отношения $\alpha \mathrm{\ div\ } \beta \rightleftharpoons v_p(\alpha) \leqslant v_p(\beta)$, где $v_p(x)$ есть наибольшая степень p, которая делит x.

Разрешимость последней теории можно установить с помощью алгоритмов элиминации кванторов (ЭК) В. Виспфеннинга [83] или Т. Штурма [78]. Такой алгоритм по всякой формуле вида $\exists x\varphi(x,\overline{y})$, где $\varphi(x,\overline{y})$ — бескванторная, строит эквивалентную в соответствующей структуре бескванторную формулу $\varphi(\overline{y})$ того же языка. Отметим, что в указанной работе В. Виспфеннинг изучал с помощью алгоритмов ЭК сложность $\exists\mathrm{Th}\langle\mathbb{Q}_p;1,+,-,=,\mathrm{div}\rangle$ и показал, что проблема распознавания формул этой теории NP-трудна и принадлежит классу **EXPTIME**. Им также было высказано предположение о принадлежности задачи классу **NP**; истинность этой гипотезы была доказана в 2019 году Ф. Гепеном, К. Хаасе и Дж. Уорреллом [36] с помощью теоретико-автоматных средств. В связи с этими вопросами отметим следующий результат, недавно полученный К. Хаасе и А. Мансутти [39]. Они рассматривают p в качестве параметра и доказывают следующее: классу **NEXPTIME** принадлежит проблема проверки того, что данная экзистенциальная формула является выполнимой *для некоторого* $p \geqslant 2$; аналогичный вопрос *для каждого* $p \geqslant 2$ оказывается в классе **co-NEXPTIME**.

Алгоритмы ЭК являются привычным инструментом при изучении арифметических теорий, которые в свою очередь предлагают удобный язык для описания свойств самых разнообразных объектов (см. обзор Т. Штурма [79]). Для элиминации кванторов были разработаны такие пакеты как RedLog для системы компьютерной алгебры REDUCE или SyNRAC [42] для Maple. Основными примерами теорий с алгоритмами ЭК являются арифметика натуральных чисел с единицей, сложением и равенством, которая называется также арифметикой Пресбургера, а так же арифметика вещественных чисел со сложением и отношением порядка. Свойства изучаемого объекта описываются с помощью формул соответствующих сигнатур, затем осуществляется проверка выполнимости формулы с помощью алгоритмов ЭК, таких как алгоритм Купера [26] для линейной целочисленной арифметики и элиминация кванторов Луса-Виспфеннинга [55] для вещественной линейной арифметики (см. обзоры Т. Нипкова [59] и Т. Штурма [80]). Ясно, что в результате элиминации желательно получить формулу как можно меньшего размера.

Аналоги алгоритмов ЭК применялись для изучения расширений арифметики Пресбургера, которые сохраняют свойство разрешимости. Значительный вклад в развитие этого

направления внёс А.Л. Семёнов [9]. Им была, в частности, установлена разрешимость элементарной теории структуры $\langle \mathbb{N}; 1, +, P_2, = \rangle$, где $P_2(x) \Leftrightarrow \exists y(x = 2^y)$, и даже более общей $\mathrm{Th}\langle \mathbb{N}; 1, +, 2^x, = \rangle$. Эти результаты были получены методом близким ЭК; детальное описание алгоритма ЭК, позволяющего установить разрешимость $\mathrm{Th}\langle \mathbb{N}; 1, +, 2^x, = \rangle$, представлено в препринте Ф. Пуан [62]. В связи с этим естественно спросить, можно ли обобщить БЛ-теорему добавлением в сигнатуру P_2 или 2^x? Отрицательный ответ на второй вопрос следует из указанной выше теоремы Косовского; в то же время, вопрос о разрешимости экзистенциальной теории натуральных чисел с единицей, сложением, делимостью и отношением P_2 остаётся важной открытой проблемой [72]. Отметим, что для попыток обобщения БЛ-теоремы, желательно иметь алгоритм для $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, \perp \rangle$. Разрешимость этой теории является несложным следствием БЛ-теоремы (утверждение было явно сформулировано и доказано А. Вудсом [85, Chapter 2, Corollary 1.6]), однако не выглядит простой задачей отделение этого случая от алгоритма из доказательства БЛ-теоремы.

Естественное с точки зрения приложений обобщение задач линейного программирования и целочисленного линейного программирования было изучено В. Виспфеннингом [84] в 1999 году. Был построен алгоритм элиминации кванторов для структуры $\left\langle \mathbb{R}; 1, +, -, [\,], \{c\cdot\}_{c\in\mathbb{Q}}, =, < \right\rangle$, где $[\,]$ соответствует функции вычисления целой части вещественного числа, а унарные функциональные символы $c\cdot$ вводятся для умножения на рациональные константы c. Кроме того, для отношения целочисленной делимости $x \mid y \rightleftharpoons \exists z(y = x \cdot z \wedge z \in \mathbb{Z})$ доказана неразрешимость $\mathrm{Th}\langle \mathbb{R}; 1, +, -, [\,], =, <, | \rangle$, а также задан вопрос о разрешимости позитивной экзистенциальной теории этой структуры. Этот результат был бы обобщением БЛ-теоремы, так как отношение «быть целым числом» выражается, например, с помощью формулы $x = [x]$.

0.2 Обобщения БЛ-теоремы и вопросы выразимости

Другим направлением поиска обобщений могло бы стать использование различных кванторов. Однако, как было показано Л. Липшицем [52], неразрешимым окажется уже множество истинных в натуральных числах формул языка сигнатуры $\langle 1, +, | \rangle$, в которых кванторная приставка имеет вид $\exists ... \exists \forall$. Этот результат является несложной комбинацией ДПРМ-теоремы и выразимости графика функции возведения в квадрат с помощью формулы

$$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z(x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z). \tag{3}$$

Следовательно, неразрешимыми оказываются уже $\exists\forall$- и $\forall\exists$-теории структур $\langle \mathbb{N}; 1, +, | \rangle$ и $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. В этом смысле, как отмечают М. Божга и Р. Иосиф [16, с. 126], БЛ-теорема является одним из самых сильных результатов о разрешимости в целочисленной арифметике („[...] remains one of the strongest decidability results in integer arithmetic [...]“).

В то же время, для ряда проблем формальной верификации требуется распознавать истинные в целых числах формулы с такими кванторными приставками, но с некоторыми

ограничениями на вид подкванторных выражений. М. Божга и Р. Иосиф в другой работе [15] определили семейство позитивных $\exists\forall$-формул с отношением порядка и делимостью, в которых каждая линейная делимость имеет вид $f(\overline{x}) \mid g(\overline{x},\overline{y})$, причём переменные из $\overline{x}$ замкнуты кванторами существования, а из $\overline{y}$ — кванторами всеобщности. После наброска доказательства разрешимости этого семейства, результат был применён в исследовании вопросов верификации программ со списками.

На разрешимость этого фрагмента арифметики целых чисел со сложением, порядком и делимостью опирается А. Лечнер [48] в изучении вопросов разрешимости и сложности проблемы синтеза по формуле линейной темпоральной логики (LTL) для параметрического односчётчикового автомата. Эта работа использует способ выражения свойства достижимости для указанных автоматов в терминах сложения и делимостей целых чисел из работы К. Хаасе и соавторов [64]. Однако, как отмечает А. Лечнер в своей диссертации [49], в доказательстве разрешимости М. Божги и Р. Иосифа [15] имеется ошибка. Исправлению этой ошибки и усовершенствованию полученных Лечнер результатов посвящена недавняя работа Г.А. Переса и Р. Рахи [61]. Ими был определён более узкий класс формул, для которых проблема проверки их истинности в целых числах уже будет разрешимой, и в то же время, этого фрагмента достаточно, чтобы записывать различные проблемы синтеза для параметрического односчётчикового автомата.

Таким образом, важной проблемой является нахождение достаточно широких разрешимых подмножеств формул $\exists\forall$-теории структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. С другой стороны, желательно обладать удобным описанием отношений, которые могут быть выражены подобными формулами. Такие описания должны дать возможность отвечать на вопросы о том, какие свойства *не* могут быть выражены. Например, М. Божга и Р. Иосиф [15, Remark 2] отмечают, что неизвестно является ли отношение $x \leqslant y$ экзистенциально выразимым ($\exists$-выразимым) в $\langle \mathbb{Z}; 1, +, -, | \rangle$. В качестве следствия из формулы (3) получаем, что $y \neq x^2$ является $\exists$-выразимым в структуре $\langle \mathbb{N}; 1, +, | \rangle$, что неверно для $y = x^2$. Ввиду этого определения Л. ван ден Дрис и А. Уилки [31] задают вопрос о $\exists$-выразимости отношения $\neg Sq$ «не быть квадратом натурального числа».

В связи с формулой (1) можно спросить, является ли позитивно экзистенциально выразимым (P$\exists$-выразимым) в $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$ отрицание отношения взаимной простоты и можно ли показать, что оно таковым не является, если мы запретим использование отношения порядка? Подобные вопросы экзистенциальной выразимости являются слабо изученными. В работе Л. Липшица [52] были приведены несколько примеров $\exists$-выразимых в структуре $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ предикатов, в частности, формулы (2). Кроме того, было доказано, что каждое множество $S \subseteq \mathbb{N}$, $\exists$-выразимое в этой структуре, представляет собой объединение некоторого конечного множества и (возможно, пустого или бесконечного) объединения арифметических прогрессий. Для этой же структуры Л. ван ден Дрис и А. Уилки [31] изучали свойства роста функций, графики которых являются экзистенциально выразимыми.

Алгоритмы ЭК позволяют описывать отношения, выразимые в некоторой структуре с помощью формул с кванторами, как класс отношений, выразимых бескванторными фор-

мулами в некотором расширении этой структуры. По известной теореме Пресбургера [63] (см. обзор К. Хаасе [38]), всякое отношение выразимо в $\langle \mathbb{Z}; 1, +, -, \leqslant \rangle$ тогда и только тогда, когда оно бесквантор но выразимо в $\langle \mathbb{Z}; 1, +, -, \leqslant, 2\mid, 3\mid, 4\mid, ... \rangle$, где унарным предикатным символам $d\mid$ сопоставляются отношения делимости на целочисленные константы $d \geqslant 2$. В. Виспфеннинг [84] доказал, что множества, выразимые в структуре $\langle \mathbb{Q}; 1, +, -, =, <, Int \rangle$, где Int есть унарный предикатный символ для свойства «быть целым числом», суть в точности множества, бесквантор но выразимые в $\langle \mathbb{Q}; 1, +, -, [\,], \{c\cdot\}_{c\in\mathbb{Q}}, =, < \rangle$.

Важно заметить, что в приведённых случаях достаточно построить позитивную бесквантор ную формулу $\psi(\overline{y})$, эквивалентную в соответствующей структуре данной позитивной экзистенциальной формуле (Р$\exists$-формуле) $\exists x \varphi(x, \overline{y})$, так как отрицание всякой атомарной формулы может быть выражено с помощью некоторой позитивной бесквантор ной формулы. Разрешимость элементарных теорий этих структур получается в качестве следствия. С другой стороны, известна неразрешимость элементарной теории структуры $\langle \mathbb{N}; S, \perp \rangle$, в которой вместо сложения имеется функция следования $Sx = x + 1$, а вместо делимости — отношение взаимной простоты. Этот результат был получен независимо Д. Ришаром [65] и А. Вудсом [85]. Для арифметики целых чисел Д. Ришар позже установил [67] неразрешимость $\mathrm{Th}\langle \mathbb{Z}; 1, +, \perp \rangle$. Таким образом, ввиду БЛ-теоремы, описания с помощью алгоритмов ЭК отношений, $\exists$-выразимых в подобных структурах, в общем случае невозможны. Это следует из того факта, что предполагаемый алгоритм ЭК позволил бы доказать разрешимость элементарной теории.

Вероятно, удовлетворительным решением для хотя бы одной из рассмотренных структур было бы найти способ расширить структуры некоторыми Р$\exists$-выразимыми отношениями, а затем для полученной структуры построить алгоритм, сопоставляющий всякой позитивной формуле $\exists x \varphi(x, \overline{y})$ эквивалентную позитивную бесквантор ную формулу $\psi(\overline{y})$. Заметим, что в расширенной сигнатуре должен содержаться предикатный символ для отношения, отрицание которого не является Р$\exists$-выразимым, так как иначе наш алгоритм превращается в алгоритм элиминации кванторов, что повлечёт разрешимость соответствующей элементарной теории. В качестве примера рассмотрим отношение $y \neq x^2$, позитивно экзистенциально выразимое в $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ ввиду формул (1) и (3), в то время как отрицание этого отношения таковым не является.

0.3 Полнота по выразимости

Последнее утверждение предыдущего раздела является очевидным следствием БЛ-теоремы и ДПРМ-теоремы ввиду элементарного факта: $z = x \cdot y \Leftrightarrow (x + y)^2 = x^2 + y^2 + 2z$. Отметим, что в теореме Н.К. Косовского о неразрешимости $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, \mid, T \rangle$ доказывается именно выразимость (причём бесквантор ная) графика возведения в квадрат $y = x^2$ в структуре $\langle \mathbb{N}; 1, +, \mid, T \rangle$. С другой стороны, несложно показать, что график сложения является бесквантор но выразимым в структуре $\langle \mathbb{N}; 0, S, \cdot, = \rangle$.

Подобные результаты важны в том смысле, что доказательство алгоритмической неразрешимости некоторой проблемы удобнее проводить сведением к ней задачи разрешимости для теории с возможно более сильными ограничениями на вид формул. Таким образом происходит перенос основной трудности в доказательстве неразрешимости на, по существу, чисто арифметический вопрос. Отметим в качестве примера доказательство неразрешимости семейства формул, определённого М. Божгой и Р. Иосифом [15; 61], с помощью теории $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, \mathrm{НОК}\rangle$, где НОК соответствует функции, вычисляющей наименьшее общее кратное. Такого рода вопросы о выразимости и разрешимости входят в контекст исследований по так называемым слабым арифметикам [68].

Систематическое исследование вопросов выразимости в слабых арифметиках начато Дж. Робинсон [69] в 1949 году. Было показано, что всякое арифметическое отношение (то есть, выразимое в структуре $\langle\mathbb{N}; +, \cdot, =\rangle$) является выразимым в $\langle\mathbb{N}; S, |\rangle$. Для структур, обладающих таким свойством, И. Корец [44] использует удобное для формулировки результатов понятие полноты по выразимости (Def-полноты). Аналогичным образом можно ввести понятие $\exists$Def-полноты для структур $\langle\mathbb{N}; \sigma\rangle$, в которых графики функций сложения и умножения являются *экзистенциально* выразимыми. В данном случае предикатные символы и графики функциональных символов из σ соответствуют некоторым перечислимым отношениям на $\mathbb{N}$.

Формула (3) позволяет доказать Def-полноту структуры $\langle\mathbb{N}; 1, +, |\rangle$. Этот результат будет более слабым, чем теорема Робинсон, так как в этой структуре $y = Sx$ выразимо очевидным образом, а вопрос выразимости графика сложения в $\langle\mathbb{N}; S, |\rangle$ является во всяком случае не самым тривиальным. Аналогично отношение взаимной простоты является более «слабым», чем отношение делимости, поскольку из определений (2) получаем уже экзистенциальную выразимость $\perp$ и его отрицания в структуре $\langle\mathbb{N}; S, |\rangle$. В связи с этим Дж. Робинсон спрашивает, будет ли Def-полной структура $\langle\mathbb{N}; S, \perp\rangle$ или хотя бы $\langle\mathbb{N}; 1, +, \perp\rangle$? Утвердительный ответ на второй вопрос удалось получить А. Вудсу [85], которым было предложено два доказательства этого факта. Кроме того отметим, что для доказательства неразрешимости элементарной теории структуры $\langle\mathbb{Z}; 1, +, \perp\rangle$ Д. Ришар доказывает выразимость отношения порядка. В то же время, вопрос о Def-полноте первой структуры остаётся открытым и связан с так называемой гипотезой Эрдёша-Вудса (см. обзор основных результатов А. Вудса, написанный П. Сигиельски и Д. Ришаром [25]).

Свойство Def-полноты структуры влечёт неразрешимость её элементарной теории. В тех случаях, когда затруднительно доказать Def-полноту, иногда возможно определить подструктуру, изоморфную некоторой Def-полной. Так было получено доказательство неразрешимости $\mathrm{Th}\langle\mathbb{N}; S, \perp\rangle$ независимо А. Вудсом и Д. Ришаром, причём были построены разные подструктуры, изоморфные $\langle\mathbb{N}; +, \cdot\rangle$. В работе П. Сигиельски, Ю.В. Матиясевича и Д. Ришара [24] вводится специальное понятие *структуры с изоморфной переинтерпретацией* (*structure with isomorphic reinterpretation property*) и предлагается пример структуры, обладающей свойством изоморфной переинтерпретации, но не являющейся Def-полной.

Возвращаясь к функции следования и делимости, отметим следующее. Доказательство принадлежности классу **NEXPTIME** проблемы разрешимости для $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, |\rangle$ было получено А. Лечнер, Дж. Оакнином и Дж. Уорреллом в качестве следствия того факта, что

для всякой совместной в $\mathbb{N}$ системы линейных делимостей существует решение, длина двоичной записи которого ограничена экспонентой от длины записи самой системы при условии двоичного кодирования коэффициентов линейных выражений. С другой стороны, ими был предложен простой пример, демонстрирующий, что верхняя оценка на наименьший выполняющий набор не может быть улучшена. Всякое решение системы

$$\bigwedge_{i=1}^{m} x_{i-1} \mid x_i \wedge Sx_{i-1} \mid x_i \wedge x_i \mid Sx_{m+1} \tag{4}$$

таково, что $x_0 \geqslant 1$, $x_1 \geqslant x_0^2 + x_0 \geqslant 2$, ..., $x_m \geqslant x_{m-1}^2 + x_{m-1} \geqslant 2^{2^{m-1}}$. Таким образом, длина бинарной записи x_m не меньше 2^{m-1}. В этой формуле используется функция следования вместо сложения, чтобы показать, что аналогичный факт имеет место уже для теории $\exists\mathrm{Th}\langle\mathbb{N}; S, |\rangle$.

И. Корец [44] систематизировал большинство известных на тот момент (2001 год) Def-полных структур, среди которых есть и весьма экзотичные. Если мы теперь введём отношение делимости на два последовательных числа

$$x \,{}^{S}|y \rightleftharpoons x \mid y \wedge x+1 \mid y, \tag{5}$$

то из формулы (3) почти непосредственно получается Def-полнота структуры $\langle\mathbb{N}; +, {}^{S}|\rangle$, так как

$$x \mid y \wedge x+1 \mid x+y \Leftrightarrow x \,{}^{S}|x+y.$$

Это же отношение лежит в основе примера (4). Изучение вопросов выразимости и разрешимости для ${}^{S}|$ любопытно в том смысле, что оно объединяет и функцию следования, и отношение делимости. В то же время, в классификации Кореца нет примеров отношений, схожих с ${}^{S}|$.

0.4 Задачи и список основных результатов

Целью данной работы является привлечение новых средств для повышения качества понимания доказательства БЛ-теоремы, получения результатов о выразимости и разрешимости, а также дальнейших обобщений этой теоремы. Для достижения поставленной цели нужно было решить следующие **задачи**:

1. Построить новое доказательство разрешимости $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, |\rangle$, отличное от доказательств, полученных А.П. Бельтюковым, Л. Липшицем и В.И. Мартьяновым, приближенное к процессу элиминации кванторов. Новая разрешающая процедура должна быть достаточно удобной, чтобы из неё несложно было выделить разрешающий алгоритм для экзистенциальных теорий более слабых структур, в частности, для $\langle\mathbb{N}; 1, +, \perp\rangle$.
2. Привести примеры структур с разрешимыми (ввиду БЛ-теоремы) экзистенциальными теориями и неразрешимыми элементарными теориями, для которых возможно описание всех Р$\exists$-выразимых отношений методом, близким к элиминации кванторов.

3. Изучить вопросы выразимости, Def-полноты и ∃Def-полноты для структур с отношением делимости на два последовательных числа $x\,{}^{S}|\,y \rightleftharpoons x(x+1) \mid y$.

Научная новизна: Результаты диссертации являются новыми и получены автором самостоятельно. Основные **результаты, выносимые на защиту**, следующие:

1. Введено понятие алгоритма квазиэлиминации кванторов (квази-ЭК), близкое к понятию алгоритма элиминации кванторов. В терминах квазиэлиминации построено новое доказательство разрешимости экзистенциальной теории натуральных чисел с единицей, сложением и делимостью.
2. Построен алгоритм квази-ЭК для экзистенциальной теории натуральных чисел с единицей, сложением и взаимной простотой, как и для более простого позитивного случая.
3. Доказано совпадение классов отношений, позитивно экзистенциально выразимых в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$ и позитивно бесквантворно выразимых в структуре $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \ldots \rangle$, где $\text{НОД}_d(x,y) \rightleftharpoons \text{НОД}(x,y) = d$. Отсюда следует, что отношение $\not\perp$ не является P∃-выразимым в $\langle \mathbb{Z}; 1, +, \perp \rangle$. Результат получен с помощью алгоритма квази-ЭК.
4. Построены два разрешимых фрагмента ∀∃-теории структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. В частности, разрешимой является проблема проверки истинности в целых числах формул вида

$$\forall\, \overline{x}\, \exists\, \overline{y} \bigvee_{j \in J} \Big(\overline{y} \geqslant 0 \wedge \varphi_j(\overline{x}) \wedge \bigwedge_{i \in I_j} (\text{GCD}(f_i(\overline{x}), g_i(\overline{x},\overline{y})) = h_i(\overline{x}) \wedge f_i(\overline{x}) > 0 \wedge h_i(\overline{x}) > 0) \Big),$$

   где $f_i(\overline{x})$, $g_i(\overline{x},\overline{y})$, $h_i(\overline{x})$ — линейные полиномы с целыми коэффициентами, а $\varphi_i(\overline{x})$ суть системы линейных неравенств и делимостей. Этот результат является обобщением теоремы, недавно полученной Г.А. Пересом и Р. Рахой [61].
5. Экзистенциальная теория структуры $\langle \mathbb{R}; 1, +, -, [\,], =, <, | \rangle$ разрешима, что даёт ответ на вопрос В. Виспфеннинга [84, Remark, p.135].
6. Доказана Def-полнота структур $\langle \mathbb{N}; {}^{S}|, | \rangle$ и $\langle \mathbb{N}; S, 2^x, {}^{S}| \rangle$; доказана неразрешимость $\text{Th}\langle \mathbb{N}; <, {}^{S}|, P_2 \rangle$. Далее, ∃Def-полной оказывается $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$, и поэтому экзистенциальная теория этой структуры неразрешима.

Методология и методы исследования. В диссертации используется инструмент элиминации кванторов, элементарные методы теории чисел, слабых арифметик, линейной алгебры, теории алгоритмов и теории графов.

Алгоритм для $\exists\text{Th}\langle \mathbb{N}; 1, +, | \rangle$, построенный в первой главе, состоит из двух этапов, соответствующих двум вариациям алгоритма квази-ЭК. Первый такой алгоритм сводит проблему разрешимости для экзистенциальной теории структуры $\langle \mathbb{Z}; 0,1, +, -, \leqslant, \text{НОД} \rangle$ к проблеме разрешимости для позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a \in \mathbb{Z}_{>0}}, \text{НОД} \rangle$, где $a\cdot$ есть унарный функциональный символ для умножения на положительное целое число a. Второй алгоритм квази-ЭК позволяет доказать разрешимость последней теории. Преобразования формул в обоих алгоритмах основаны на обобщении китайской теоремы об остатках для систем вида $\bigwedge_{i \in [1..m]} \text{НОД}(a_i, b_i + x) = d_i$, где

a_i,b_i,d_i — целые числа, такие что $a_i \neq 0$, $d_i > 0$ для всех $i \in [1..m]$. Это утверждение является элементарным результатом из теории сравнений и будет называться НОД-леммой. На шаге отделения переменной в первом случае используется лемма И. фон цур Гаттена и М. Сифкинга [34], аналог которой также применял Л. Липшиц [51, Lemma 1]. Во втором алгоритме эта лемма не используется; по данной формуле строится ориентированный граф, в котором выделяются и устраняются циклы.

НОД-лемма является основным инструментом описания РЭ-выразимых в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$ отношений. Тот факт, что $x \not\perp y$ таковым не является, следует из основной теоремы из главы 2 и результата Д. Ришара [67] о неразрешимости элементарной теории указанной структуры. Доказательство разрешимости $\exists\mathrm{Th}\langle \mathbb{R}; 0, 1, +, -, [\,], =, <, | \rangle$ получено сведением к разрешимой $\exists$-теории структуры с той же сигнатурой, носителем которой является множество рациональных чисел $\mathbb{Q}$.

В третьей главе используются классические понятия и приёмы доказательства Def-полноты и $\exists$Def-полноты арифметических структур. Def-полнота $\langle \mathbb{N}; |, {}^{S}| \rangle$ получается из выразимости в этой структуре графика функции следования S и теоремы Дж. Робинсон [69] о Def-полноте $\langle \mathbb{N}; S, | \rangle$. Для доказательства $\exists$Def-полноты $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$ используется бесквантороная выразимость сложения с помощью S и умножения и доказывается экзистенциальная выразимость графика функции следования. Неразрешимость $\exists$-теории этой структуры следует из ДПРМ-теоремы. Из результата Д. Ришара [66] о Def-полноте структуры $\langle \mathbb{N}; S, 2^x, \perp \rangle$ и выразимости отношения взаимной простоты получаем Def-полноту $\langle \mathbb{N}; S, 2^x, {}^{S}| \rangle$. Доказательство неразрешимости $\mathrm{Th}\langle \mathbb{N}; <, {}^{S}|, P_2 \rangle$ проводится доказательством существования подструктуры, изоморфной Def-полной структуре $\langle \mathbb{N}; <, | \rangle$.

Теоретическая и практическая значимость. Отметим следующие направления, в которых могут найти приложения полученные результаты.

В недавнем препринте Г.А. Переса и Р. Рахи [61] показано, что в доказательстве одного обобщения БЛ-теоремы, полученного И. Божгой и Р. Иосифом [15], содержится ошибка, и, в действительности, разрешимым оказывается несколько более ограниченный фрагмент $\forall\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Подобного рода ошибок можно было бы избежать, если бы мы обладали доказательством БЛ-теоремы, полученным с помощью интерактивных систем доказательства теорем, таких как Isabelle, Coq или Lean. Построение такого рода доказательств является интенсивно развивающейся областью исследований на стыке функционального программирования и теории доказательств. Например, в 2018 году был инициирован процесс доказательства ДПРМ-теоремы в Isabelle [81], в том же году М. Карнейро [21] автоматизировал в системе Lean доказательство теоремы Матиясевича, а в 2020 году была анонсирована [45] полная формализация ДПРМ-теоремы в Coq. Предлагаемое в первой главе доказательство БЛ-теоремы в терминах квазиэлиминации, вероятно, более пригодно для целей автоматизации процесса доказательства, так как оно основано на идее элиминации кванторов, привычной для специалистов в таких областях теоретической информатики, как символьные вычисления и формальная верификация.

С другой стороны, само понятие квазиэлиминации может оказаться полезным при попытках дальнейшего обобщения этой теоремы, например, для решения проблемы о возмож-

ности добавить в структуру отношения P_2. Кроме того, при изучении сложности проблемы разрешимости $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ естественно было бы попытаться доказать принадлежность **NP** (или **EXPTIME**) хотя бы для более слабой $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$. Построенный во второй главе алгоритм квази-ЭК для этой теории может способствовать как решению указанного вопроса, так и для доказательства разрешимости экзистенциальной теории структуры $\langle\mathbb{Z};1,+,-,\leqslant,\perp,P_2\rangle$.

Вопросы экзистенциальной выразимости в структуре $\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ допускают различные переформулировки и часто проявляются в исследованиях по алгоритмической разрешимости проблем теоретической информатики. В то же время, мы не обладаем удовлетворительным описанием отношений, $\exists$-выразимых в этой структуре. Автору во всяком случае не известны результаты, аналогичные описанию всех отношений, P$\exists$-выразимых в $\langle\mathbb{Z};1,+,\perp\rangle$ из главы 2. Этот результат может послужить отправной точкой для поисков описания более широких классов P$\exists$-выразимых отношений.

Апробация работы. Основные результаты работы докладывались на следующих конференциях и семинарах:

1. Международная конференция «Journées sur les Arithmétiques Faibles 37 (JAF37)», Флоренция, Италия, 29.05.2018;
2. Всероссийская конференция «СПИСОК-2019», Санкт-Петербург, Россия, 25.04.2019;
3. Семинар «Городской семинар по математической логике», Санкт-Петербург, Россия, 31.05.2019;
4. Международная конференция «Polynomial Computer Algebra 2020 (PCA 2020)», Санкт-Петербург, Россия, 12.10.2020;
5. Международная конференция «International Symposium on Symbolic and Algebraic Computation 2021 (ISSAC'21)», Санкт-Петербург, Россия, 22.07.2021.
6. Международная конференция «Journées sur les Arithmétiques Faibles 40 (JAF40)», Афины, Греция, 25.10.2021;

Публикации. Основные результаты по теме диссертации изложены в 4 печатных изданиях, 1 из которых издано в журнале, рекомендованном ВАК [10], 3 — в периодических научных журналах и материалах конференций, индексируемых Web of Science / Scopus [75—77].

Объем и структура работы. Диссертация состоит из введения, 3 глав и заключения. Первая глава объединяет результаты работ [75] и [76]. Глава 2 основана на статье [77], отправленной на конференцию ISSAC'21, и дополнена результатами, доложенными на конференции PCA'20. Третья глава является расширенной версией статьи [10].Полный объём диссертации составляет 92 страницы. Список литературы содержит 85 наименований.

Автор благодарен своим научным руководителям Н.К. Косовскому и Т.М. Косовской за длительное внимание, советы и поддержку в работе. Кроме того, автор благодарен анонимным рецензентам своих статей по теме диссертации за весьма полезные замечания и советы, способствовавшие значительному улучшению качества изложения.

Глава 1. Доказательство теоремы Бельтюкова – Липшица квазиэлиминацией кванторов

> This is just the Chinese Remainder Theorem (see [M]). Of course g.c.d.(f_i,f_j) is not in our language so we have not actually eliminated x_n...
>
> L. Lipshitz [52] (1981)

В главе предлагается новое доказательство теоремы о разрешимости экзистенциальной теории натуральных чисел с единицей, сложением и делимостью. Теорема была доказана независимо А.П. Бельтюковым [1] и Л. Липшицем [51] и будет далее называться БЛ-теоремой. Чтобы доказать эту теорему способом близким элиминации кванторов, вводится понятие алгоритма квазиэлиминации кванторов, а затем строятся два таких алгоритма. В начале главы приводятся основные определения, которые будут использоваться в формулировках утверждений в этой и в последующих главах.

1.1 Экзистенциальная арифметика натуральных чисел с единицей, сложением и делимостью

1.1.1 Основные определения и примеры

Пусть σ есть некоторая сигнатура и задано некоторое непустое множество M. Назовём *интерпретацией сигнатуры* σ *на* M отображение, сопоставляющее каждому функциональному символу из σ некоторую функцию на M и предикатному символу из σ предикат на M соответствующей местности.

Структура определяется некоторой сигнатурой σ, множеством M и интерпретацией σ на M. Множество M назовём *носителем структуры*.

В диссертации будут рассматриваться различные сигнатуры, однако, в качестве носителя будет использоваться либо множество натуральных чисел $\mathbb{N} = \{0,1,2,...\}$, либо множество целых чисел $\mathbb{Z}$, либо рациональных $\mathbb{Q}$, либо вещественных $\mathbb{R}$, либо p-адических $\mathbb{Q}_p$, а всякому функциональному и предикатному символу будет сопоставляться естественным образом определяемая функция и предикат. Структуру сигнатуры σ с носителем M будем обозначать $\langle M; \sigma \rangle$.

Язык первого порядка сигнатуры σ будет обозначаться L_σ; формулу языка $L \subseteq L_\sigma$ назовём L-формулой. Пренексная L_σ-формула есть формула вида $Q_1 y_1 ... Q_m y_m \varphi(x_1,...,x_n,y_1,...,y_m)$, где $\varphi(x_1,...,x_n,y_1,...,y_m)$ — бескванторная L_σ-формула, а Q_i —

кванторы. Если объединить одинаковые кванторы в блоки, то формулы с единственным блоком определяют язык $\exists L_\sigma$, если это кванторы существования, и $\forall L_\sigma$, если это кванторы всеобщности. Аналогично определяются языки $\forall\exists L_\sigma$, $\exists\forall L_\sigma$ и т.д. $\exists L_\sigma$-формулы называются *экзистенциальными*, а $\forall L_\sigma$-формулы — *универсальными* L_σ*-формулами*.

Бескванторную формулу будем называть *позитивной*, если она построена из атомарных формул с помощью только логических связок конъюнкции и дизъюнкции. Если в приведённых выше определениях потребовать позитивность формулы $\varphi(x_1,...,x_n,y_1,...,y_m)$, то к обозначению получаемых языков добавится приставка "P", а формулы этих языков будут называться *позитивными*. Например, $\mathrm{P}\exists L_\sigma$ есть множество позитивных экзистенциальных L_σ-формул.

Пусть φ есть некоторая L_σ-формула. Мы будем говорить, что «φ *истинна в* M» вместо фразы «истинна в структуре $\langle M;\sigma\rangle$». Множество всех замкнутых L_σ-формул, истинных в M, называется *элементарной теорией структуры* $\langle M;\sigma\rangle$ и будет обозначаться $\mathrm{Th}\langle M;\sigma\rangle$. Если рассматривать только экзистенциальные L_σ-формулы, то мы определяем экзистенциальную теорию ($\exists\mathrm{Th}$), а для только универсальных L_σ-формул — универсальную теорию ($\forall\mathrm{Th}$) структуры $\langle M;\sigma\rangle$. В общем случае, для всякого языка $L\subseteq L_\sigma$ множество всех замкнутых L-формул, истинных в M, определяет L*-теорию структуры* $\langle M;\sigma\rangle$ и обозначается L-$\mathrm{Th}\langle M;\sigma\rangle$. Назовём *задачей разрешимости (проблемой разрешимости) для некоторой* L*- теории структуры* $\langle M;\sigma\rangle$ проблему распознавания формул этой теории среди всех L-формул или, иными словами, проблему распознавания L-формул, истинных в M.

В качестве иллюстрации приведённых понятий, рассмотрим подробнее различные переформулировки БЛ-теоремы, о которых шла речь во введении. Пусть дана структура $\langle\mathbb{N};1,+,|\rangle$, где отношение делимости определяется следующим образом: $x\mid y\Leftrightarrow\exists z(y=z\cdot x)$. В частности, $0\mid y\Leftrightarrow y=0$.

Ясно, что для доказательства разрешимости $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$ достаточно обладать алгоритмом проверки совместности в натуральных числах систем вида

$$\bigwedge_{i\in[1..m]} f_i(\overline{x})\mid g_i(\overline{x}), \tag{1.1}$$

где $\overline{x}$ — это список переменных $x_1,...,x_n$, $f_i(\overline{x})$,$g_i(\overline{x})$ — линейные полиномы вида $a_{i,0}+a_{i,1}x_1+...+a_{i,n}x_n$ с натуральными коэффициентами. Воспользуемся законами дистрибутивности для логических связок конъюнкции и дизъюнкции и преобразуем данную $\mathrm{P}\exists L_{\langle 1,+,|\rangle}$-формулу в дизъюнкцию систем вида (1.1).

Теперь воспользуемся определением (1) для того, чтобы рассматривать произвольные, а не только позитивные, экзистенциальные формулы. Для всякой $\exists L_{\langle 1,+,|\rangle}$-формулы пронесём отрицания до атомарных формул и снова воспользуемся законами дистрибутивности. Теперь избавимся от отношений неделимости в полученных системах введением новых переменных с помощью формулы

$$x\nmid y\Leftrightarrow(x=0\wedge 1\leqslant y)\vee\exists z(1\leqslant z\wedge z\leqslant x-1\wedge x\mid y+z), \tag{1.2}$$

где отношение $x\leqslant y$ есть по определению $\exists z(y=x+z)$, в то время как $x=y\Leftrightarrow x\mid y\wedge y\mid x$. Заметим, что отношение $x\leqslant y$ можно сразу переписать в виде $\exists z(x+z\mid y)$.

Покажем, что для структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ проблема разрешимости для Р$\exists$-теории сводится к проблеме разрешимости для $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, | \rangle$, и наоборот. Сведение в обратную сторону очевидно, так как достаточно добавить к формуле $\varphi(x_1,...,x_n)$, исследуемой на выполнимость в $\mathbb{Z}$, систему неравенств $\bigwedge\limits_{i\in[1..n]} x_i \geqslant 0$.

Чтобы перейти от целых чисел к натуральным, заменим всякую целочисленную переменную x_i на $x_i' - x_i''$, где переменные x_i', x_i'' принимают натуральные значения. Теперь избавимся от отрицательных коэффициентов в линейных полиномах. В линейных неравенствах перенесём переменные с отрицательными коэффициентами в противоположную часть. Для линейных делимостей рассмотрим конъюнкцию вида

$$\varphi(\overline{x},\overline{y}) \wedge f(\overline{x}) - g(\overline{y}) \mid h(\overline{x},\overline{y}), \tag{1.3}$$

где $\varphi(\overline{x},\overline{y})$ есть некоторая система линейных неравенств и делимостей, $h(\overline{x},\overline{y})$ — линейный полином с целыми коэффициентами, а полиномы $f(\overline{x})$ и $g(\overline{y})$ имеют неотрицательные целые коэффициенты. Формула (1.3) эквивалентна в $\mathbb{N}$ следующей экзистенциальной формуле:

$$\varphi(\overline{x},\overline{y}) \wedge \exists z \left(z \mid h(\overline{x},\overline{y}) \wedge \left(f(\overline{x}) = g(\overline{y}) + z \vee f(\overline{x}) + z = g(\overline{y})\right)\right).$$

Так поступим с каждым линейным полиномом, содержащим отрицательные коэффициенты. Осталось переписать неравенства и уравнения с помощью делимости, как это делалось выше.

Несложно увидеть как воспользоваться (1), чтобы и в случае целых чисел избавиться от ограничения позитивности. Зафиксируем полученный результат.

Утверждение 1.1.1. *Задачи разрешимости для экзистенциальных теорий структур* $\langle \mathbb{N}; 1, +, | \rangle$ *и* $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ *сводятся друг к другу.*

Перед тем, как рассматривать связь делимости с отношением НОД, формально определим понятие выразимости.

Для всякого языка $L \subseteq L_\sigma$ будем говорить, что n-местное отношение R на M *«L-выразимо в структуре* $\langle M; \sigma \rangle$*»*, если найдётся L-формула $\varphi(\overline{x})$, такая что для любого $\overline{a} \in M^n$ имеет место $R(\overline{a}) \Leftrightarrow \varphi(\overline{a})$. В том случае, когда язык L определён с помощью L_σ и приставок "Р", "$\exists$", "$\forall$", символ L можно опустить. В частности, Р$\exists L_\sigma$-выразимые в структуре $\langle M; \sigma \rangle$ отношения будут называться *позитивно экзистенциально выразимыми в структуре* $\langle M; \sigma \rangle$ или Р$\exists$-выразимыми. Если из контекста ясно, о какой структуре идёт речь, будем говорить просто о L-теории и об L-выразимости.

Через год после появления оригинальных доказательств, БЛ-теорема была доказана В. И. Мартьяновым [5]. Им был получен эквивалентный результат, так как вместо делимости рассматривался трехместный предикат НОД, такой что НОД(x,y,z) тогда и только тогда, когда $\pm z$ является наибольшим общим делителем x и y. Более естественным представляется использование функции НОД, принимающей неотрицательные значения, причём нулевое только при равенстве нулю обоих аргументов. Запишем график этой функции в виде НОД$(x,y) = z$; тогда $x \mid y \Leftrightarrow$ НОД$(x,y) = x \vee$ НОД$(x,y) = -x$. И наоборот, из алгоритма

Евклида доказываем экзистенциальную выразимость отношения НОД и его отрицания в структуре $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$:

$$\begin{aligned} \text{НОД}(x,y) = z \;&\Leftrightarrow\; 0 \leqslant z \wedge z \mid x \wedge z \mid y \wedge \exists u\,(x \mid u \wedge y \mid u + z) \\ \neg\text{НОД}(x,y) = z \;&\Leftrightarrow\; z + 1 \leqslant 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v\,(v \mid x \wedge v \mid y \wedge z + 1 \leqslant v)\,. \end{aligned} \tag{1.4}$$

В структурах, рассматриваемых в диссертации, НОД будет трёхместным предикатным символом, которому сопоставляется график соответствующей функции. Теперь можно обобщить утверждение 1.1.1.

Утверждение 1.1.2. *Задачи разрешимости для экзистенциальных теорий следующих структур:* $\langle \mathbb{N}; 1, +, | \rangle$, $\langle \mathbb{N}; 1, +, \text{НОД} \rangle$, $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ *и* $\langle \mathbb{Z}; 1, +, -, \leqslant, \text{НОД} \rangle$ *сводятся друг к другу.*

Классическим способом изучения свойств выразимости и разрешимости для арифметических структур является построение алгоритма элиминации кванторов. *Алгоритмом элиминации кванторов (ЭК) для языка* L_σ *в структуре* $\langle M; \sigma \rangle$ называется алгоритм, который по всякой L_σ-формуле вида $\exists x \varphi(x, y_1, ..., y_n)$, где $\varphi(x, y_1, ..., y_n)$ — бескванторная, строит эквивалентную ей в этой структуре бескванторную L_σ-формулу $\psi(y_1, ..., y_n)$. В качестве следствия получаем, что алгоритм ЭК позволяет построить по всякой L_σ-формуле эквивалентную в соответствующей структуре бескванторную L_σ-формулу. Отметим, что именно алгоритм из следствия обычно (например, в [38] или [83]) называется алгоритмом ЭК, однако его построение сводится к построению алгоритма ЭК в нашем смысле. „Как обычно, достаточно рассматривать формулу с единственным квантором существования [...]“, — так начинают Н.К. Верещагин и А. Шень [3] изложение алгоритма ЭК для языка первого порядка сигнатуры $\sigma = \langle 0, 1, +, \cdot, =, < \rangle$ в структуре $\langle \mathbb{R}; \sigma \rangle$.

В подразделе 1.2.3 определённое таким образом понятие алгоритма ЭК обобщается до алгоритмов квазиэлиминации кванторов. В терминах квазиэлиминации будет построено доказательство теоремы 1.

Теорема 1 (А. П. Бельтюков [1], Л. Липшиц [51], В. И. Мартьянов [5])**.** *Экзистенциальная теория структуры* $\langle \mathbb{Z}; 0, 1, +, -, \leqslant, \text{НОД} \rangle$ *разрешима.*

Заметим, что $\neg\text{НОД}(x,y) = z \Leftrightarrow \exists t\,(\text{НОД}(x,y) = t \wedge t \neq z)$ для $t \neq z \Leftrightarrow t \leqslant z - 1 \vee z + 1 \leqslant t$, причем $\neg x \leqslant y \Leftrightarrow y + 1 \leqslant x$. Удобно выделить в формулах отдельно системы уравнений и неравенств, записанные в матричном виде. Таким образом, введением (возможно) некоторых новых переменных, сводим задачу разрешимости к проблеме выполнимости в $\mathbb{Z}$ формул вида

$$\varphi(\overline{x}) \rightleftharpoons A\overline{x} = b \wedge C\overline{x} \geqslant d \wedge \bigwedge_{i \in [1..m]} \text{НОД}(f_i(\overline{x}), g_i(\overline{x})) = h_i(\overline{x}), \tag{1.5}$$

где, как и прежде, $\overline{x}$ — это список переменных $x_1, ..., x_n$; $f_i(\overline{x}), g_i(\overline{x}), h_i(\overline{x})$ — линейные полиномы с целыми коэффициентами; A и C — целочисленные матрицы; b, d — некоторые целочисленные векторы. Выражения вида $\text{НОД}(f(\overline{x}), g(\overline{x})) = h(\overline{x})$ далее будут называться *нод-выражениями.*

1.1.2 Описание разделов главы

Глава организована следующим образом. В разделе 1.2 вводится понятие алгоритма квазиэлиминации кванторов (квази-ЭК), которое в некотором смысле обобщает понятие алгоритма ЭК, и даётся план доказательства теоремы 1 с помощью алгоритмов квази-ЭК $\mathcal{R}$ и $\mathcal{D}$. Первый сводит проблему разрешимости для экзистенциальной теории структуры $\langle \mathbb{Z}; 0,1, +, -, \leqslant, \text{НОД} \rangle$ к проблеме разрешимости для позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД} \rangle$, где $a\cdot$ есть унарный функциональный символ для умножения на положительное целое число a. В разделе 1.7 алгоритм квази-ЭК $\mathcal{D}$ позволит доказать разрешимость последней теории. Описанию основного алгоритма $\mathcal{R}$, осуществляющего сведение, посвящены разделы 1.4 и 1.5, а в разделе 1.6 доказывается тот факт, что полученный алгоритм действительно является алгоритмом квази-ЭК.

Как отмечает А. П. Бельтюков [2] о теореме, доказанной в одно время с Л. Липшицем, «в сущности, наше решение было очень сложным обобщением широко известной Китайской Теоремы об Остатках...». После описания плана доказательства, в разделе 1.3 обобщается китайская теорема об остатках на системы вида $\bigwedge\limits_{i\in[1..m]} \text{НОД}(a_i, b_i + x) = d_i$, где a_i, b_i, d_i — целые числа, такие что $a_i \neq 0$, $d_i > 0$ для всех $i \in [1..m]$. Этот результат будет основным инструментом в преобразовании формул в алгоритме квази-ЭК $\mathcal{R}$. Частный случай этого обобщения будет использован в алгоритме $\mathcal{D}$.

1.2 Краткое описание алгоритма

1.2.1 Лемма о линейных системах и простые преобразования формул

Проблема совместности в $\mathbb{Z}$ системы (1.5) будет сведена к проблеме выполнимости в неотрицательных целых числах $\mathbb{N}$ дизъюнкции систем $\widetilde{\varphi}_j$. В каждой системе $\widetilde{\varphi}_j$ найдётся переменная $\widetilde{x}_j$, которая появляется только в нод-выражениях вида $\text{НОД}(f(\overline{z}), g(\overline{z}) + c\widetilde{x}_j) = h(\overline{z})$ для списка переменных $\overline{z}$, не содержащего $\widetilde{x}_j$. Эти преобразования могут быть выполнены с использованием следующей леммы о линейных системах (ЛС-леммы), которая в более сильной форме представлена в работе А. Лечнер с соавторами [50, Theorem 3]. Это утверждение было доказано Й. фон цур Гаттеном и М. Сивкингом [34]; Л. Липшиц использовал некоторый его аналог (см. [51, Lemma 1]).

Лемма 1.2.1 (Лемма о линейных системах (ЛС-лемма) [51, Lemma 1] и [34] в форме [50, Theorem 3]). *Пусть даны целочисленная матрица A размера $p \times n$ ранга r, целочисленная матрица C размера $q \times n$, целочисленные столбцы b и d размеров p и q соответственно.*

Существует алгоритм построения конечного множества целочисленных матриц $E^{(j)}$ *размера* $n \times (n-r)$ *и столбцов* $u^{(j)}$ *размера* n *для* $j \in J$ *таких, что*

$$\{\overline{x} \in \mathbb{Z}^n \,:\, A\overline{x} = b \wedge C\overline{x} \geqslant d\} = \bigcup_{j \in J} \left\{ E^{(j)}\overline{y} + u^{(j)} \,:\, \overline{y} \in \mathbb{N}^{n-r} \right\}.$$

Разделим список $\overline{x}$ на две части $\overline{s} = x_1,...,x_l$ и $\overline{t} = x_{l+1},...,x_n$. Пусть система $A\overline{x} = b \wedge C\overline{x} \geqslant d$ распадается на две подсистемы: $S(\overline{s}) \rightleftharpoons A_1\overline{s} = b_1 \wedge C_1\overline{s} \geqslant d_1$ и $T(\overline{x}) \rightleftharpoons A_2\overline{x} = b_2 \wedge C_2\overline{x} \geqslant d_2$, где матрица A_1 имеет ранг r_1. Под *«применением ЛС-леммы к подсистеме* $S(\overline{s})$ *формулы* $\varphi(\overline{x})$*»* мы будем предполагать следующее. Пусть для системы $S(\overline{s})$ построены целочисленные матрицы $E^{(j)}$ и столбцы $u^{(j)}, j \in J$. Построим множество формул $\{\psi_j\}_{j \in J}$, где

$$\psi_j(\overline{y},\overline{t}) \rightleftharpoons \widetilde{T}_j(\overline{y},\overline{t}) \wedge \overline{y} \geqslant 0 \wedge \bigwedge_{i \in [1..m]} \text{НОД}(\widetilde{f}_{i,j}(\overline{y},\overline{t}),\widetilde{g}_{i,j}(\overline{y},\overline{t})) = \widetilde{h}_{i,j}(\overline{y},\overline{t}), \tag{1.6}$$

как результат подстановки $E^{(j)}\overline{y} + u^{(j)}$ вместо $\overline{s}$ в

$$T(\overline{s},\overline{t}) \wedge \bigwedge_{i \in [1..m]} \text{НОД}(f_i(\overline{s},\overline{t}),g_i(\overline{s},\overline{t})) = h_i(\overline{s},\overline{t}).$$

Таким образом, мы преобразовали $\varphi(\overline{x})$ в равновыполнимую в целых числах дизъюнкцию $\bigvee\limits_{j \in J} \psi_j(\overline{y},\overline{t})$, в которой число переменных уменьшилось на r_1.

Применением ЛС-леммы к подсистеме $\bigwedge\limits_{i \in [1..m]} h_i(\overline{x}) \geqslant 0 \wedge A\overline{x} = b \wedge C\overline{x} \geqslant d$ формулы $\bigwedge\limits_{i \in [1..m]} h_i(\overline{x}) \geqslant 0 \wedge \varphi(\overline{x})$ (равновыполнимой с $\varphi(\overline{x})$ в $\mathbb{Z}$ ввиду того, что правые части нод-выражений могут принимать только неотрицательные значения) мы получаем следующую вспомогательную лемму.

Лемма 1.2.2. *Для всякой формулы вида (1.5) можно построить равновыполнимую в* $\mathbb{Z}$ *дизъюнкцию формул вида*

$$\overline{y} \geqslant 0 \wedge \bigwedge_{i \in [1..m]} \text{НОД}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}), \tag{1.7}$$

где $\overline{y}$ *есть список переменных* $y_1,...,y_k$, $k \leqslant n$; $f_i(\overline{y}),g_i(\overline{y}),h_i(\overline{y})$ *суть линейные полиномы с целыми коэффициентами и, кроме того, коэффициенты* $h_i(\overline{y})$ *неотрицательные.*

Аналогичный приём получения неотрицательных коэффициентов в линейных полиномах с помощью ЛС-леммы будет применяться на шаге 1 изолирования переменной (т. е. построения $\widetilde{\varphi}_j$), который описан в разделе 1.4.

1.2.2 НОД-лемма

Под китайской теоремой об остатках мы предполагаем теорему [71], утверждающую существование целочисленного решения у системы делимостей $\bigwedge\limits_{i \in [1..m]} d_i \mid b_i + x$ тогда и только

тогда, когда $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(d_i,d_j) \mid b_i - b_j$. В разделе 1.3 доказывается следующее обобщение китайской теоремы об остатках, которое будет использовано на шаге 2 квазиэлиминации для систем $\widetilde{\varphi}_j$ в разделе 1.5.

Для каждого положительного целого числа x и простого p, выражение $v_p(x)$ обозначает p-показатель x, то есть максимальное k, для которого $p^k \mid x$. Будем писать НОД(x,y,z) вместо НОД(НОД(x,y),z). Тогда для системы

$$\bigwedge_{i\in[1..m]} \text{НОД}(a_i,b_i + x) = d_i, \tag{1.8}$$

можно доказать следующую лемму.

Лемма 1.2.3 (НОД-лемма)**.** *Определим для системы (1.8), где a_i,b_i,$d_i \in \mathbb{Z}$ и $a_i \neq 0$, $d_i > 0$, $i \in [1..m]$, и всякого простого числа p целое число $M_p = \max\limits_{i\in[1..m]} v_p(d_i)$ и два множества индексов $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ и $I_p = \{i \in J_p : v_p(a_i) > M_p\}$.*

Система (1.8) имеет решение в $\mathbb{Z}$ тогда и только тогда, когда одновременно выполняются следующие условия:

(i) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$

(ii) $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(d_i,d_j) \mid b_i - b_j$

(iii) $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(a_i,d_j,b_i - b_j) \mid d_i$

(iv) Для всякого простого $p \leqslant m$ и всякого $I \subseteq I_p$ такого, что $|I| = p$ существуют такие $i, j \in I$, $i \neq j$, что $v_p(b_i - b_j) > M_p$.

Рассмотрим подсистему $\widetilde{\varphi}_j$, образованную из всех нод-выражений с изолированной переменной, причём несложно добиться того, чтобы коэффициенты при этой переменной были равны единице. Эта подсистема будет иметь вид (1.8), где на месте a_i, b_i и d_i будут некоторые линейные полиномы с целыми коэффициентами $f_i(\overline{z})$, $g_i(\overline{z})$ и $h_i(\overline{z})$ соответственно. Применение НОД-леммы потребует введения новых переменных, принимающих положительные целые значения. Эти переменные будут названы буквами греческого алфавита, в то время как латинские буквы будут использоваться для переменных, введенных с помощью ЛС-леммы. Греческие переменные будут появляться только в полиномах вида $a\zeta$.

Поясним сказанное на примере переписывания условия (ii). В этом случае для каждой пары индексов (i,j), $1 \leqslant i < j \leqslant m$ вводится новая переменная $\zeta_{i,j}$, так что соответствующая делимость переписывается в следующем виде:

$$\exists\zeta_{i,j}\,(\text{НОД}(h_i(\overline{z}),h_j(\overline{z})) = \zeta_{i,j} \wedge \text{НОД}(\zeta_{i,j},g_i(\overline{z}) - g_j(\overline{z})) = \zeta_{i,j})\,.$$

Леммы 1.2.1 и 1.2.3 образуют два шага, которые повторно выполняются для получения дизъюнкции систем нод-выражений, не содержащих латинских переменных. Таким образом, каждый линейный полином будет иметь вид $a\zeta$ либо a для некоторого положительного целого числа a. Это сведение может быть формализовано с помощью понятия «алгоритма квазиэлиминации кванторов».

1.2.3 Определение алгоритмов квазиэлиминации кванторов

Пусть имеются два непересекающихся сорта переменных S_1 и S_2. Переменные из S_1 будут обозначаться латинскими буквами (и будут называться «латинскими переменными»), а из S_2 — греческими буквами («греческие переменные»). Пусть $L_\sigma^{1,2}$ — язык первого порядка сигнатуры σ с переменными из $S_1 \cup S_2$. Обозначим L_σ^1 и L_σ^2 языки первого порядка сигнатуры σ с переменными соответственно из S_1 и S_2.

Обозначим $[\varphi]_t^x$ результат подстановки терма t вместо каждого свободного вхождения переменной x в формулу φ. Множество формул $L \subset L_\sigma$ назовём *эффективно проверяемым*, если существует алгоритм, распознающий L-формулы.

Определение 1. *Пусть дана некоторая структура $\langle M; \sigma\rangle$ с сигнатурой σ и эффективно проверяемое множество формул $L \subset L_\sigma^{1,2}$, такое, что все латинские переменные входят свободно, а все греческие связаны кванторами существования. Пусть также для некоторой переменной $x \in S_1$ определено эффективно проверяемое множество* ***L-формул элиминационного вида*** *$L^x \subseteq L$ и заданы два шага:*

Шаг 1. *Построение по всякой L-формуле $\exists\overline{\alpha}\varphi(\overline{y},\overline{\alpha})$ равновыполнимой в $\langle M; \sigma\rangle$ дизъюнкции $\bigvee\limits_{j\in J} \exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})$ для некоторого конечного множества индексов J и списков латинских переменных $\overline{y_j}$ таких, что для всякого $j \in J$:*

1. *Количество переменных в списке $\overline{y_j}$ не превосходит количества переменных в $\overline{y}$.*
2. *Если список переменных $\overline{y_j}$ не пуст, то найдётся переменная $\widetilde{x}_j \in \overline{y_j}$, что $[\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})]_x^{\widetilde{x}_j} \in L^x$.*

Шаг 2. *Построение по всякой формуле $\exists x\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$, такой что $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ является L^x-формулой, эквивалентной в структуре $\langle M; \sigma\rangle$ L-формулы $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$.*

Тогда $\mathcal{A}$ — ***алгоритм квазиэлимиации кванторов (квази-ЭК) для языка L в структуре*** *$\langle M; \sigma\rangle$, если по данной на вход L-формуле $\exists\overline{\alpha}\varphi(y_1,\ldots,y_k,\overline{\alpha})$ сначала выполняется шаг 1, а затем для каждой формулы $\exists x\,[\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})]_x^{\widetilde{x}_j}$ шаг 2. Таким образом, получается равновыполнимая дизъюнкция L-формул, в каждой из которых число латинских переменных меньше k.*

Язык L будет называться ***языком алгоритма квази-ЭК*** *$\mathcal{A}$.*

Рассмотрим некоторые свойства алгоритма квази-ЭК $\mathcal{A}$ для $L_\mathcal{A}$ в $\langle M; \sigma\rangle$.

Для подмножества L бесквантворных формул L_σ определим язык $\exists L$ как множество формул вида $\exists\overline{x}\varphi(\overline{x},\overline{y})$ для всякой (бесквантворной) L-формулы $\varphi(\overline{x},\overline{y})$. Множество замкнутых $\exists L$-формул обозначим $E(L)$.

Основное назначение $\mathcal{A}$ можно описать следующим образом. Так как $L_\mathcal{A} \cap L_\sigma^1$ содержит только бесквантворные L_σ-формулы, то определено множество формул $E(L_\mathcal{A} \cap L_\sigma^1)$, которое обозначим $L_\mathcal{A}^1$, и пусть $L_\mathcal{A}^2 \rightleftharpoons L_\mathcal{A} \cap L_\sigma^2$. Тогда алгоритм $\mathcal{A}$ выполняет сведение проблемы разрешимости для $L_\mathcal{A}^1$-теории к проблеме разрешимости для $L_\mathcal{A}^2$-теории. Действительно, по всякой (бесквантворной) $(L_\mathcal{A} \cap L_\sigma^1)$-формуле φ повторным применением алгоритма $\mathcal{A}$ к каждой

из $L_{\mathcal{A}}$-формул получаемых дизъюнкций, построим дизъюнкцию (замкнутых) $L^2_{\mathcal{A}}$-формул, истинную в $\langle M;\sigma\rangle$ тогда и только тогда, когда φ выполнима в этой структуре.

Рассмотрим три важные вариации алгоритмов квази-ЭК для случая, когда $S_2 = \varnothing$. Из определения следует, что $L_{\mathcal{A}}$ является подмножеством бескванторных L_σ-формул.

Пример 1.2.1. *Если S_2 является пустым сортом переменных и вычисление в $\langle M;\sigma\rangle$ истинностного значения L_σ-формулы без переменных является разрешимой проблемой, то алгоритм квази-ЭК $\mathcal{A}$ позволяет доказать разрешимость $E(L_{\mathcal{A}})$-теории структуры $\langle M;\sigma\rangle$ так как для исследуемой на выполнимость формулы мы построим эквивалентную в этой структуре формулу без переменных.*

Примерами такого алгоритма квази-ЭК будут алгоритм $\mathcal{D}$ из раздела 1.7, а так же два алгоритма из раздела 2.6.

Пример 1.2.2. *Если S_2 является пустым сортом переменных и $L^x_{\mathcal{A}} = L_{\mathcal{A}}$ (шаг 1 алгоритма $\mathcal{A}$ становится тривиальным), то множество всех $\exists L_{\mathcal{A}}$-выразимых в $\langle M;\sigma\rangle$ отношений совпадает с множеством отношений (бескванторно) $L_{\mathcal{A}}$-выразимых в $\langle M;\sigma\rangle$.*

Единственный шаг алгоритма позволяет последовательно проэлиминировать каждый квантор данной $\exists L_{\mathcal{A}}$-формулы и получить эквивалентную в $\langle M;\sigma\rangle$ $L_{\mathcal{A}}$-формулу, которая является бескванторной L_σ-формулой. Во второй главе этот вариант алгоритма квази-ЭК позволит описать все отношения, позитивно экзистенциально выразимые в структуре $\langle\mathbb{Z};1,+,\perp\rangle$.

Пример 1.2.3. *Если, кроме того, $L_{\mathcal{A}}$ является множеством всех бескванторных L_σ-формул, то $\mathcal{A}$ есть в точности алгоритм элиминации кванторов для L_σ в $\langle M;\sigma\rangle$.*

1.2.4 Основной алгоритм квази-ЭК

Мы построим два алгоритма квази-ЭК $\mathcal{R}$ и $\mathcal{D}$. Первый сводит проблему выполнимости в $\mathbb{Z}$ формул вида (1.5) к проблеме разрешимости для позитивной экзистенциальной теории структуры $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД}\rangle$, а второй позволит доказать разрешимость этой теории. В этом подразделе мы опишем алгоритм $\mathcal{R}$, основной алгоритм квази-ЭК, а $\mathcal{D}$ будет построен в разделе 1.7.

Определим язык $L_{\mathcal{R}}$ алгоритма квази-ЭК $\mathcal{R}$ как множество формул $\exists\overline{\alpha}\bigvee\limits_{j\in J_1}\varphi_j(\overline{y_j},\overline{\alpha})$ для некоторого конечного множества индексов J_1 и формул $\varphi_j(\overline{y},\overline{\alpha})$ вида

$$\overline{\alpha}\geqslant 1\wedge\overline{y}\geqslant 0\wedge\bigwedge_{i\in[1..m_j]}\text{НОД}(f_{i,j}(\overline{y},\overline{\alpha}),g_{i,j}(\overline{y},\overline{\alpha}))=h_{i,j}(\overline{y},\overline{\alpha}),\tag{1.9}$$

где все линейные полиномы $h_{i,j}(\overline{y},\overline{\alpha})$ имеют неотрицательные целые коэффициенты и, кроме того, каждое нод-выражение имеет одну из следующих форм:

($\mathcal{R}$-1) НОД($f(\overline{y})$,$g(\overline{y})$) = $h(\overline{y})$
($\mathcal{R}$-2) НОД($f(\overline{y})$,$g(\overline{y})$) = $a\zeta$
($\mathcal{R}$-3) НОД($a\zeta$,$g(\overline{y})$) = $b\eta$
($\mathcal{R}$-4) НОД($a\zeta$,$b\eta$) = $c\theta$,

где ζ,η,θ — греческие переменные (возможно, одинаковые), а a, b, c — положительные целые числа. Кроме того, всякая греческая переменная ζ, входящая в нод-выражения вида ($\mathcal{R}$-2), входит в правые части ($\mathcal{R}$-3) и ($\mathcal{R}$-4) только в нод-выражениях вида НОД($a\zeta$,$g(\overline{y})$) = $b\zeta$ или НОД($a\zeta$,$b\zeta$) = $c\zeta$.

Последнее ограничение на вид нод-выражений необходимо по следующей прчине. Пусть из нод-выражения ($\mathcal{R}$-2) удалось получить равенство $l(\overline{y}) = a\zeta$. Подставим в систему (1.9) всюду $\frac{l(\overline{y})}{a}$ вместо ζ и домножим соответствующие нод-выражения на a. Указанные ограничения на нод-выражения с переменной ζ гарантируют, что полученная формула останется $L_{\mathcal{R}}$-формулой.

Будем называть нод-выражения НОД($f(\overline{z},\overline{\alpha})$,$g(\overline{z},\overline{\alpha}) + cx$) = $h(\overline{z},\overline{\alpha})$ *регулярными нод-выражениями*, если линейные полиномы $f(\overline{z},\overline{\alpha})$ и $h(\overline{z},\overline{\alpha})$ имеют один из следующих видов: либо $a\zeta$ для некоторой греческой переменной ζ и положительного целого числа a, либо линейного полинома $l(\overline{z})$ с неотрицательными целыми коэффициентами и положительным свободным членом. Ввиду того, что в $L_{\mathcal{R}}$-формулах $\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0$, полиномы $f(\overline{z},\overline{\alpha})$ и $h(\overline{z},\overline{\alpha})$ могут принимать только положительные значения, поэтому к системам регулярных нод-выражений можно применять НОД-лемму.

Множество формул элиминационного вида $L^x_{\mathcal{R}} \subseteq L_{\mathcal{R}}$ состоит из формул $\exists\overline{\alpha} \bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x,\overline{z_j},\overline{\alpha})$ для некоторого конечного множества индексов J_2 и формул $\widetilde{\varphi}_j(x,\overline{z},\overline{\alpha})$ вида

$$\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}_j(\overline{z},\overline{\alpha}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} \text{НОД}(\widetilde{f}_{i,j}(\overline{z},\overline{\alpha}),\widetilde{g}_{i,j}(\overline{z}) + c_{i,j}x) = \widetilde{h}_{i,j}(\overline{z},\overline{\alpha}), \qquad (1.10)$$

где x не содержится в $\overline{z}$, $c_{i,j} > 0$, каждое нод-выражение с x является регулярным нод-выражением, а $\widetilde{\widetilde{\varphi}}_j(\overline{z},\overline{\alpha})$ есть система нод-выражений без вхождений x.

В разделе 1.6 мы покажем, что преобразования, описанные в разделах 1.4 и 1.5, определяют шаг 1 и шаг 2 алгоритма квази-ЭК для $L_{\mathcal{R}}$. Поэтому, как следует из определения $L_{\mathcal{R}}$, для доказательства теоремы 1 будет достаточно доказать разрешимость позитивной экзистенциальной теории структуры $\langle\mathbb{Z}_{>0}; 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД}\rangle$. Как мы увидим в разделе 1.7, ЛС-лемма не используется в алгоритме $\mathcal{D}$, и потребуется лишь частный случай НОД-леммы.

1.3 Доказательство НОД-леммы

Перед тем, как переходить к доказательству леммы 1.2.3, удобно переформулировать её четвёртый пункт. Определим условие

((iv)) Для всякого простого p найдётся $x_p \in \mathbb{Z}$, что $\bigwedge\limits_{i\in I_p} v_p(b_i + x_p) = M_p$

и докажем следующую лемму.

Лемма 1.3.1. *Пусть для системы вида (1.8) значения a_i,b_i,d_i,M_p, I_p определены так же как в лемме 1.2.3, и выполнено условие (ii). Тогда (iv) имеет место тогда и только тогда, когда ((iv)).*

Доказательство. Рассмотрим простое p, натуральное число M_p и множество индексов I_p. Условие (ii) подразумевает совместность системы $\bigwedge\limits_{i\in I_p} p^{M_p} \mid b_i + x$. Возьмем $x_0 \in [0,p^{M_p})$ такое, что $x_0 \equiv -b_i (\mathrm{mod}\ p^{M_p})$ для $i \in I_p$. Тогда получаем, что $x = x_0 + kp^{M_p}$ является решением для любого $k \in \mathbb{Z}$ и таким образом

$$\exists x \left(\bigwedge_{i\in I_p} v_p(b_i + x) = M_p \right) \Leftrightarrow \exists k \left(\bigwedge_{i\in I_p} p \nmid \left(\frac{x_0 + b_i}{p^{M_p}} + k\right) \right). \tag{1.11}$$

Правая часть (1.11) истинна тогда и только тогда, когда $\left\{ \frac{x_0+b_i}{p^{M_p}} \right\}_{i\in I_p}$ не содержит полной системы вычетов по модулю p. Следовательно, это верно для каждого $p > m$, а для $p \leqslant m$ это условие эквивалентно тому, что для каждого $I \subseteq I_p$ такого, что $|I| = p$, существуют i,$j \in I$, $i \neq j$, что $p \mid \frac{x_0+b_i}{p^{M_p}} - \frac{x_0+b_j}{p^{M_p}}$, или, в терминах p-показателя, $v_p(b_i - b_j) > M_p$. □

Лемму 1.2.3 докажем предполагая, что условие (iv) было заменено на ((iv)).

Доказательство леммы 1.2.3. **Необходимость**. Условие (i), очевидно, необходимо. Так как для каждого i,$j \in [1..m]$ мы имеем $d_i \mid b_i + x$ и $d_j \mid b_j + x$, следовательно НОД(d_i,d_j) $\mid b_i + x - (b_j + x)$. Таким образом, получаем (ii).

Чтобы доказать (iii), рассмотрим для каждой пары индексов i,$j \in [1..m]$ следующую цепочку равенств

$$\begin{aligned} \text{НОД}(a_i,d_j,b_i - b_j) &= \text{НОД}(a_i,\text{НОД}(a_j,b_j + x),b_i - b_j) \\ &= \text{НОД}(a_i,a_j,\text{НОД}(b_i + x,b_j + x)) = \text{НОД}(d_i,d_j). \end{aligned}$$

Для всякого простого числа p имеем $v_p(\text{НОД}(a_i,b_i+x)) = v_p(d_i)$ для любого $i \in [1..m]$. В частности, если $i \in I_p$, то $\min(v_p(a_i),v_p(b_i+x)) = v_p(\text{GCD}(a_i,b_i+x)) = M_p$, причём $v_p(a_i) > M_p$. Следовательно, $v_p(b_i + x) = M_p$, и необходимость условия ((iv)) доказана.

Достаточность. Пусть P_0 — (конечное) множество всех простых чисел p таких, что $p \mid a_i$ для некоторого $i \in [1..m]$. Условие (i) подразумевает, что $v_p(a_i) \geqslant v_p(d_i)$ для всяких $i \in [1..m]$ и $p \in P_0$. Перепишем (1.8) в виде системы делимостей и неделимостей:

$$\begin{aligned} &\bigwedge_{i\in[1..m]} \left(\bigwedge_{p\in P_0 \wedge v_p(a_i)=v_p(d_i)} p^{v_p(d_i)} \mid b_i + x \right) \\ &\quad \wedge \left(\bigwedge_{p\in P_0 \wedge v_p(a_i)>v_p(d_i)} p^{v_p(d_i)} \mid b_i + x \wedge p^{v_p(d_i)+1} \nmid b_i + x \right). \end{aligned} \tag{1.12}$$

Для каждого простого числа $p \in P_0$ выделим в (1.12) подсистему, содержащую все делимости и неделимости, в которых делителем является p в некоторой степени. Определим множество индексов $K_p = \{i \in [1..m] \setminus J_p : v_p(a_i) > v_p(d_i)\}$ и систему

$$\Phi_p(x) \rightleftharpoons \bigwedge_{i \in [1..m] \setminus J_p} p^{v_p(d_i)} \mid b_i + x \wedge \bigwedge_{i \in K_p} p^{v_p(d_i)+1} \nmid b_i + x. \tag{1.13}$$

Теперь система (1.12) переписывается следующим образом:

$$\bigwedge_{p \in P_0} \left(\Phi_p(x) \wedge \bigwedge_{i \in J_p} p^{M_p} \mid b_i + x \wedge \bigwedge_{i \in I_p} p^{M_p+1} \nmid b_i + x \right). \tag{1.14}$$

По китайской теореме об остатках достаточно найти отдельно для каждого простого числа $p \in P_0$ решение соответствующей подсистемы.

Зафиксируем некоторое $p \in P_0$. Сначала построим решение x_p подсистемы делимостей и неделимостей с индексами из J_p, а затем проверим, что имеет место $\Phi_p(x_p)$.

Если $I_p = \varnothing$, то ввиду того, что по условию (ii) $b_i \equiv b_j (\mathrm{mod}\ p^{M_p})$ для всех $i,j \in J_p$, достаточно выбрать любой индекс $j_p \in J_p$ и определить $x_p \in [0,p^{M_p})$ сравнимый с $-b_{j_p}$ по модулю p^{M_p}.

Иначе, если множество индексов I_p не пусто, по условию ((iv)) найдётся $x_p \in \mathbb{Z}$, что

$$\bigwedge_{i \in I_p} p^{M_p} \mid b_i + x_p \wedge \bigwedge_{i \in I_p} p^{M_p+1} \nmid b_i + x_p. \tag{1.15}$$

Удобно считать, что $x_p \in [0,p^{M_p+1})$. Ввиду условия (ii), в подсистеме делимостей из (1.15) множество индексов I_p можно заменить на J_p.

Осталось показать, что x_p удовлетворяет системе делимостей и неделимостей (1.13). Пусть снова j_p является произвольным индексом из J_p. Из условия (ii) следует, что $b_k \equiv b_{j_p} (\mathrm{mod}\ p^{v_p(d_k)})$ для каждого $k \in [1..m] \setminus K_p$ и, значит, $p^{v_p(d_k)} \mid b_k + x_p$ так как $v_p(d_k) < M_p$, поэтому x_p удовлетворяет подсистеме делимостей из (1.13).

Чтобы доказать, что x_p также является решением подсистемы неделимостей, предположим, что $p^{v_p(d_k)+1}$ делит $x_p + b_k$ для некоторого $k \in K_p$. Тогда получим $v_p(b_k - b_{j_p}) \geqslant \min\left\{v_p(b_k + x_p), v_p(b_{j_p} + x_p)\right\} \geqslant v_p(d_k) + 1$. Из этого следует, что

$$\min\left\{\min\left\{v_p(a_k), M_p\right\}, v_p(b_k - b_{j_p})\right\} \geqslant v_p(d_k) + 1.$$

Но это противоречит (iii), так как левая часть не должна превосходить $v_p(d_k)$.

Таким образом, получаем решение из системы вида

$$\bigwedge_{p \in P_0} x \equiv x_p (\mathrm{mod}\ p^{\beta_p}), \tag{1.16}$$

где $\beta_p = M_p + 1$, если множество индексов I_p не пусто и $\beta_p = M_p$ иначе. □

Итоговая система сравнений позволяет сделать следующее замечание.

Замечание 1.3.1. *Если x является решением системы (1.8), то $x + k \cdot \operatorname{НОК}\limits_{i \in [1..m]}(d_i) \cdot \mathrm{rad}\left(\prod\limits_{i \in [1..m]} \frac{a_i}{d_i}\right)$ также является решением для каждого $k \in \mathbb{Z}$, где $\mathrm{rad}(n)$ — радикал ненулевого целого числа n, т. е. произведение различных простых делителей n.*

1.4 Шаг 1: отделение латинской переменной

Опустим индексы j в (1.9) и рассмотрим $L_{\mathcal{R}}$-формулу $\exists\overline{\alpha}\varphi(\overline{y},\overline{\alpha})$, где

$$\varphi(\overline{y},\overline{\alpha}) \rightleftharpoons \overline{\alpha} \geqslant 1 \wedge \overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y},\overline{\alpha}),g_i(\overline{y},\overline{\alpha})) = h_i(\overline{y},\overline{\alpha}). \tag{1.17}$$

Напомним, что в $L_{\mathcal{R}}$-формулах коэффициенты $h_i(\overline{y},\overline{\alpha})$ всегда неотрицательны. Пусть, как и в подразделе 1.2.1, список $\overline{y}$ разделён на $\overline{s} = y_1,...,y_l$ и $\overline{t} = y_{l+1},...,y_n$. Сформулируем два замечания.

Замечание 1.4.1. *Результатом применения ЛС-леммы к подсистеме вида $A\overline{s} = b \wedge C\overline{s} \geqslant d \wedge \overline{s} \geqslant 0$ формулы $A\overline{s} = b \wedge C\overline{s} \geqslant d \wedge \varphi(\overline{y},\overline{\alpha})$ является дизъюнкция формул $\psi_j(\overline{z},\overline{t},\overline{\alpha})$, таких, что $\exists\overline{\alpha}\psi_j(\overline{z},\overline{t},\overline{\alpha})$ является $L_{\mathcal{R}}$-формулой, и, кроме того, всякому регулярному нод-выражению в $\varphi(\overline{y},\overline{\alpha})$ с изолированной переменной из $\overline{t}$ будет соответствовать регулярное нод-выражение в $\psi_j(\overline{z},\overline{t},\overline{\alpha})$.*

Доказательство. Действительно, ввиду того, что в систему линейных уравений и неравенств входит $\overline{s} \geqslant 0$, вместо каждой переменной из $\overline{s}$ подставляется линейное выражение $l(\overline{z})$ с неотрицательными целыми коэффициентами. Поэтому каждый линейный полином $f(\overline{y})$ с неотрицательными коэффициентами (и положительным свободным членом) сохраняет это свойство после подстановки $E^{(j)}\overline{z} + u^{(j)}$ вместо $\overline{s}$. □

Замечание 1.4.2. *Можно считать, что в системе (1.17) нет нод-выражений вида ($\mathcal{R}$-1) и ($\mathcal{R}$-2), таких что $k_1 f_i(\overline{y}) = k_2 g_i(\overline{y})$ для некоторых не равных одновременно нулю целых чисел k_1 и k_2.*

Доказательство. Предположим, что $k_1 f_i(\overline{y}) = k_2 g_i(\overline{y})$ для $k_1 \neq 0$. В таком случае можно вычислить наибольший общий делитель и перейти к дизъюнкции по $\sigma \in \{-1,1\}$, заменяя в (1.17) соответствующее нод-выражение на равенство $\sigma\text{НОД}(k_1,k_2)g_i(\overline{y}) = k_1 h_i(\overline{y},\overline{\alpha})$. Для нод-выражений вида ($\mathcal{R}$-1) это равенство либо всегда истинно, либо может быть использовано для получения дизъюнкции систем с меньшим на единицу числом переменных, как результат применения ЛС-леммы к подсистеме $\overline{y} \geqslant 0 \wedge \sigma\text{НОД}(k_1,k_2)g_i(\overline{y}) = k_1 h_i(\overline{y})$ формулы (1.17).

Если же $h_i(\overline{y},\overline{\alpha}) = a_i\zeta_i$, удалим $\sigma\text{НОД}(k_1,k_2)g_i(\overline{y}) = a_i k_1 \zeta_i$ из системы, подставим всюду $\frac{\sigma\text{НОД}(k_1,k_2)g_i(\overline{y})}{a_i k_1}$ вместо ζ_i и домножим линейные выражения на $a_i k_1$. В частности, вместо $\zeta_i \geqslant 1$ появится неравенство $\sigma\text{НОД}(k_1,k_2)g_i(\overline{y}) \geqslant a_i k_1$; по определению языка $L_{\mathcal{R}}$, все нод-выражения в результате подстановки снова будут иметь вид ($\mathcal{R}$-1)–($\mathcal{R}$-4). Осталось применить ЛС-лемму к подсистеме $\overline{y} \geqslant 0 \wedge \sigma\text{НОД}(k_1,k_2)g_i(\overline{y}) \geqslant a_i k_1$. □

Теперь покажем как получить равновыполнимую в целых числах дизъюнкцию формул вида (1.10).

В первом случае существует латинская переменная x, которая не встречается в правой части никакого нод-выражения (1.17). Используя алгоритм Евклида, каждое нод-выражение вида ($\mathcal{R}$-1) или ($\mathcal{R}$-2) $\text{НОД}(f(\overline{z}) + ax, g(\overline{z}) + bx) = h(\overline{z},\overline{\alpha})$ для $a,b \neq 0$ и линейных полиномов

$f(\overline{z})$ и $g(\overline{z})$, может быть переписано таким образом, что коэффициент при x не равен нулю только в одном из полиномов. Пусть $a > b > 0$ и $a = qb + r$ для $r \in [0,b)$. Тогда имеем

$$\text{НОД}(f(\overline{z}) + ax, g(\overline{z}) + bx) = \text{НОД}(f(\overline{z}) - qg(\overline{z}) + rx, g(\overline{z}) + bx).$$

Повторяя этот шаг, получим формулу вида $\text{НОД}(\widetilde{f}(\overline{z}),\widetilde{g}(\overline{z}) + cx) = h(\overline{z},\overline{\alpha})$. Ввиду замечания 1.4.2 полином $\widetilde{f}(\overline{z})$ не является тождественно нулевым.

В другом случае каждая латинская переменная входит в правую часть хотя бы одного нод-выражения. Выделим в (1.17) подсистему нод-выражений вида ($\mathcal{R}$-1) и перепишем (1.17) следующим образом:

$$\begin{aligned}\overline{\alpha} \geqslant 1 \wedge \overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..l]} \text{НОД}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}) \\ \wedge \bigwedge_{i\in[l+1..m]} \text{НОД}(f_i(\overline{y},\overline{\alpha}),g_i(\overline{y},\overline{\alpha})) = h_i(\overline{\alpha}).\end{aligned} \tag{1.18}$$

Для каждой переменной $x \in \overline{y}$ найдётся индекс $i_x \in [1..l]$ такой, что эта переменная входит с ненулевым коэффициентом в $h_{i_x}(\overline{y})$ (то есть $h_{i_x}(\overline{y}) = h'_{i_x}(\overline{y} \setminus x) + c_{i_x}x$ для некоторого положительного целого c_{i_x}). По замечанию 1.4.2 случай $u_1 f_{i_x}(\overline{y}) = v_1 h_{i_x}(\overline{y})$ и $u_2 g_{i_x}(\overline{y}) = v_2 h_{i_x}(\overline{y})$ для некоторых целых u_1,v_1,u_2,v_2 невозможен, поэтому можно считать, что $uf_{i_x}(\overline{y}) \neq vh_{i_x}(\overline{y})$ для всяких целых u и v. Тогда получим, что система (1.17) эквивалентна следующей дизъюнкции:

$$\bigvee_{x\in\overline{y}} \left(\bigvee_{-S_x\leqslant k\leqslant S_x} \overline{\alpha} \geqslant 1 \wedge \Psi_{x,k}(\overline{y}) \wedge \bigwedge_{i\in[1..m]\wedge i\neq i_x} \text{НОД}(f_i(\overline{y},\overline{\alpha}),g_i(\overline{y},\overline{\alpha})) = h_i(\overline{y},\overline{\alpha}) \right), \tag{1.19}$$

где

$$\Psi_{x,k}(\overline{y}) \rightleftharpoons \overline{y} \geqslant 0 \wedge \bigwedge_{x'\in\overline{y}} x \geqslant x' \wedge k(h_{i_x}(\overline{y})) = f_{i_x}(\overline{y})$$

и S_x есть сумма абсолютных значений коэффициентов $f_{i_x}(\overline{y})$. Это следует из того факта, что все коэффициенты $h_{i_x}(\overline{y})$ неотрицательны, $c_{i_x} > 0$, переменные $\overline{y}$ неотрицательны и x принимает максимальное значение среди переменных из $\overline{y}$.

Применение ЛС-леммы к подсистеме $\Psi_{x,k}(\overline{y})$ каждого дизъюнкта (1.19) даст дизъюнкцию систем вида (1.17), каждая из которых содержит на единицу меньшее число переменных и на единицу меньшее число нод-выражений. Ввиду замечания 1.4.1, если обозначить эту дизъюнкцию $\psi(\overline{z},\overline{\alpha})$, мы имеем $\exists\overline{\alpha}\psi(\overline{z},\overline{\alpha}) \in L_{\mathcal{R}}$.

На этом разбор второго случая завершается, и далее в каждой системе из $\psi(\overline{z},\overline{\alpha})$ мы снова пытаемся отделить латинскую переменную, которая не встречается в правой части никакого нод-выражения, пока не получится дизъюнкция формул вида (1.10).

Теперь предположим, что искомая дизъюнкция получена. Опустим индексы j в (1.10) и обозначим эту формулу $\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$. Преобразуем $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ в равновыполнимую в целых числах дизъюнкцию формул того же вида (1.10), но с регулярными нод-выражениями. Следовательно, получим $L^x_{\mathcal{R}}$-формулу.

Поскольку $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ является $L_{\mathcal{R}}$-формулой, нерегулярными могут быть лишь нод-выражения вида ($\mathcal{R}$-1) или ($\mathcal{R}$-2). Пусть нод-выражения из $\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ с индексами $i = 1..k$

содержат все нерегулярные нод-выражения вида ($\mathcal{R}$-1), а с индексами $i = k+1..l$ все нерегулярные нод-выражения вида ($\mathcal{R}$-2), для которых положим $\widetilde{h}_i(\overline{z},\overline{\alpha}) = a_i\zeta_i$.

Перепишем $\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ в виде $\overline{\alpha} \geqslant 1 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \Delta(x,\overline{z},\overline{\alpha})$, где

$$\begin{aligned}\Delta(x,\overline{z},\overline{\alpha}) \rightleftharpoons & \bigwedge_{i\in[1..k]} \text{НОД}(\widetilde{f}_i(\overline{z}), \quad \widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z}) \\ \wedge & \bigwedge_{i\in[k+1..l]} \text{НОД}(\widetilde{f}_i(\overline{z}), \quad \widetilde{g}_i(\overline{z}) + c_i x) = a_i\zeta_i \\ \wedge & \bigwedge_{i\in[l+1..m]} \text{НОД}(\widetilde{f}_i(\overline{z},\overline{\alpha}),\widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z},\overline{\alpha})\end{aligned}$$

и построим равновыполнимую с $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ формулу

$$\exists\overline{\alpha}\Big(\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha}) \vee \widetilde{\Phi}_1(\overline{z_1},\overline{\alpha}) \vee \widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})\Big).$$

Здесь $\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha})$ и $\widetilde{\Phi}_1(\overline{z_1},\overline{\alpha})$ являются дизъюнкциями систем вида (1.17), таких что список $\overline{z_0}$ содержит на две, а $\overline{z_1}$ на одну переменную меньше, чем $x,\overline{z}$. В полученных системах снова отделяем латинскую переменную, а затем добиваемся регулярности нод-выражений с изолированной переменной. Так как число латинских переменных постоянно уменьшается, этот процесс обязательно остановится. В то же время, $\widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})$ окажется дизъюнкцией искомого вида, то есть, $\exists\overline{\alpha}\widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})$ будет некоторой $L^x_{\mathcal{R}}$-формулой.

Дизъюнкции $\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha})$ и $\widetilde{\Phi}_1(\overline{z_1},\overline{\alpha})$ соответствуют случаям равенства нулю $\widetilde{f}_i(\overline{z})$: для индексов $i = 1..k$ и для $i = k+1..l$ соответственно. Построение дизъюнкций аналогично разбору двух случаев из замечания 1.4.2. Именно,

$$\widetilde{\Phi}_0(\overline{z_0},\overline{\alpha}) \rightleftharpoons \bigvee_{i\in[1..k]} \bigvee_{\sigma\in\{-1,1\}} \Omega_{i,\sigma}(\overline{z_0},\overline{\alpha})$$

и

$$\widetilde{\Phi}_1(\overline{z_1},\overline{\alpha}) \rightleftharpoons \bigvee_{i\in[k+1..l]} \bigvee_{\sigma\in\{-1,1\}} \Omega_{i,\sigma}(\overline{z_1},\overline{\alpha}),$$

где дизъюнкции $\Omega_{i,\sigma}(\overline{z_0},\overline{\alpha})$ и $\Omega_{i,\sigma}(\overline{z_1},\overline{\alpha})$ будут получены с помощью ЛС-леммы.

Обозначим $\Delta_i(x,\overline{z},\overline{\alpha})$ системы, полученные исключением из $\Delta(x,\overline{z},\overline{\alpha})$ нод-выражения с индексом $i \in [1..l]$. Тогда для $i = 1..k$ дизъюнкция $\Omega_{i,\sigma}(\overline{z_0},\overline{\alpha})$ есть результат применения ЛС-леммы к подсистеме

$$\Phi_{i,\sigma}(x,\overline{z}) \rightleftharpoons \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{f}_i(\overline{z}) = 0 \wedge c_i x = \sigma\widetilde{h}_i(\overline{z}) - \widetilde{g}_i(\overline{z})$$

формулы $\overline{\alpha} \geqslant 1 \wedge \Phi_{i,\sigma}(x,\overline{z}) \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \Delta_i(x,\overline{z},\overline{\alpha})$.

Для индексов $i = k+1..l$ обозначим $\widetilde{\Delta}_{i,\sigma}(x,\overline{z},\overline{\alpha})$ результат подстановки $\frac{\sigma(\widetilde{g}_i(\overline{z})+c_i x)}{a_i}$ вместо ζ_i в формулу $\overline{\alpha} \setminus \zeta_i \geqslant 1 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha}) \wedge \Delta_i(x,\overline{z},\overline{\alpha})$ и домножения полученных выражений на a_i. Применение ЛС-леммы к подсистеме

$$\Phi_{i,\sigma}(x,\overline{z}) \rightleftharpoons \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{f}_i(\overline{z}) = 0 \wedge \sigma(\widetilde{g}_i(\overline{z}) + c_i x) \geqslant a_i$$

формулы $\Phi_{i,\sigma}(x,\overline{z}) \wedge \widetilde{\Delta}_{i,\sigma}(x,\overline{z},\overline{\alpha})$ даст нам дизъюнкцию $\Omega_{i,\sigma}(\overline{z_1},\overline{\alpha})$. Осталось заметить, что уменьшение числа переменных в списках $\overline{z_0}$ и $\overline{z_1}$ следует из того, что полином $\widetilde{f}_i(\overline{z})$ не равен тождественно нулю для всякого $i = 1..l$.

Теперь разберём случай не равных нулю значений $\widetilde{f}_i(\overline{z})$:

$$\bigvee_{\overline{\sigma}\in\{-1,1\}^l}\Bigg(\overline{\alpha}\geqslant 1\wedge\overline{z}\geqslant 0\wedge x\geqslant 0\wedge\widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha})\wedge\bigwedge_{i\in[1..k]}\Big(\sigma_i\widetilde{f}_i(\overline{z})\geqslant 1\wedge\widetilde{h}_i(\overline{z})\geqslant 1\Big)$$
$$\wedge\bigwedge_{i\in[k+1..l]}\sigma_i\widetilde{f}_i(\overline{z})\geqslant 1\wedge\bigwedge_{i\in[1..m]}\text{НОД}(\widetilde{f}_i(\overline{z},\overline{\alpha}),\widetilde{g}_i(\overline{z})+c_ix)=\widetilde{h}_i(\overline{z},\overline{\alpha})\Bigg). \tag{1.20}$$

Дизъюнкция $\widetilde{\Phi}_2(x,\overline{z_2},\overline{\alpha})$ есть результат применения в каждом дизъюнкте (1.20) ЛС-леммы к подсистемам, содержащим все линейные уравнения и неравенства, зависящие от переменных $\overline{z}$. Из замечания 1.4.1 следует регулярность нод-выражений в полученных системах.

1.5 Шаг 2: применение НОД-леммы

Теперь рассмотрим подсистему (1.10) с изолированной переменной x. Без потери общности можно считать, что все $c_{i,j}$ равны 1, поскольку мы можем вычислить $C=\operatorname{НОК}\limits_{i=1..\widetilde{m}_j}(c_{i,j})$; умножить каждое нод-выражение на $\frac{C}{c_{i,j}}$; заменить все вхождения Cx на $\widetilde{x}$ и добавить в систему нод-выражение $\text{НОД}(C,\widetilde{x})=C$.

С помощью новых положительных целых греческих переменных $\overline{\beta}$ перепишем формулу $\exists x\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ для $L^x_{\mathcal{R}}$-формулы $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$, где

$$\widetilde{\varphi}(x,\overline{z},\overline{\alpha})\rightleftharpoons\overline{\alpha}\geqslant 1\wedge\overline{z}\geqslant 0\wedge x\geqslant 0\wedge\widetilde{\widetilde{\varphi}}(\overline{z},\overline{\alpha})$$
$$\wedge\bigwedge_{i\in[1..m]}\text{НОД}(f_i(\overline{z},\overline{\alpha}),g_i(\overline{z})+x)=h_i(\overline{z},\overline{\alpha}), \tag{1.21}$$

чтобы получить эквивалентную в $\mathbb{Z}$ формулу вида $\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ так, что $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ является некоторой $L_{\mathcal{R}}$-формулой. Это преобразование определит шаг 2 алгоритма квази-ЭК $\mathcal{R}$.

Обозначим $\overline{u}$ список переменных $\overline{z},\overline{\alpha}$ и рассмотрим условия (i) – (iv) НОД-леммы.

(i). В этом случае введение новых переменных не требуется. Мы получаем конъюнкцию $\bigwedge\limits_{i\in[1..m]}\text{НОД}(h_i(\overline{u}),f_i(\overline{u}))=h_i(\overline{u})$.

(ii). Для каждой упорядоченной пары (i,j), $1\leqslant i<j\leqslant m$ вводится новая переменная $\zeta_{i,j}$, так что второе условие может быть записано в виде

$$\bigwedge_{1\leqslant i<j\leqslant m}\exists\zeta_{i,j}\left(\text{НОД}(h_i(\overline{u}),h_j(\overline{u}))=\zeta_{i,j}\wedge\text{НОД}(\zeta_{i,j},g_i(\overline{z})-g_j(\overline{z}))=\zeta_{i,j}\right).$$

Эта формула может быть приведена к пренексному виду, так как соответствующие переменные появляются только в одной паре нод-выражений.

(iii). Для каждой упорядоченной пары (i,j), $i,j\in[1..m]$ вводятся две новые переменные $\eta_{i,j}$ и $\theta_{i,j}$ для того, чтобы переписать делимость $\text{НОД}(f_i(\overline{u}),h_j(\overline{u}),g_i(\overline{z})-g_j(\overline{z}))\mid h_i(\overline{u})$ в следующем виде:

$$\exists\eta_{i,j}\exists\theta_{i,j}(\text{НОД}(f_i(\overline{u}),h_j(\overline{u}))=\eta_{i,j}$$
$$\wedge\,\text{НОД}(\eta_{i,j},g_i(\overline{z})-g_j(\overline{z}))=\theta_{i,j}\wedge\text{НОД}(\theta_{i,j},h_i(\overline{u}))=\theta_{i,j}).$$

(iv). Необходимо записать тот факт, что для каждого простого числа $p \leqslant m$ и множества индексов $I \subseteq [1..m]$ таких, что $|I| = p$ или ложно условие

$$\bigwedge_{i\in I}\left(v_p(h_i(\overline{u})) = \max_{j\in[1..m]} v_p(h_j(\overline{u})) \wedge v_p(f_i(\overline{u})) > v_p(h_i(\overline{u}))\right),$$

или найдутся такие $i,j \in I, i \neq j$, что $v_p\left(g_i(\overline{z}) - g_j(\overline{z})\right) > v_p\left(h_i(\overline{u})\right)$. Построим формулу $\Omega_{p,I}(\overline{u})$, такую, что это условие переписывается в виде следующей конъюнкции:

$$\bigwedge_{p\leqslant m\wedge p\in\mathbb{P}}\left(\bigwedge_{I\subseteq[1..m]\wedge|I|=p}\Omega_{p,I}(\overline{u})\right),$$

где $\mathbb{P}$ есть множество простых чисел.

В первом случае множество индексов I не является подмножеством J_p. Либо не для всех $i \in I$ значение $v_p(h_i(\overline{u}))$ одинаково, либо не максимальное $\bigvee\limits_{i\in I\wedge j\in[1..m]} v_p(h_i(\overline{u})) < v_p(h_j(\overline{u}))$. Здесь отношение $v_p(x) < v_p(y)$ выражается формулой

$$\exists\iota\left(\text{НОД}(\iota,x) = \iota \wedge \text{НОД}(p\iota,x) = \iota \wedge \text{НОД}(\iota,y) = \iota \wedge \text{НОД}(p\iota,y) = p\iota\right). \tag{1.22}$$

Теперь исключим множества I такие, что $\bigvee\limits_{i\in I} v_p(f_i(\overline{u})) = v_p(h_i(\overline{u}))$, так как в противном случае I не является подмножеством I_p. Для отношения равенства p-показателей $v_p(x) = v_p(y)$ используем экзистенциальную формулу

$$\exists\iota\left(\text{НОД}(\iota,x) = \iota \wedge \text{НОД}(\iota,y) = \iota \wedge \text{НОД}(p\iota,x) = \iota \wedge \text{НОД}(p\iota,y) = \iota\right). \tag{1.23}$$

Если ни одна из дизъюнкций не истинна (т. е. $I \subseteq I_p$), необходимо записать условие «существуют такие $i,j \in I$, $i \neq j$, что $v_p(g_i(\overline{z}) - g_j(\overline{z})) > v_p(h_i(\overline{u}))$». Объединяя дизъюнкции, получим $\Omega_{p,I}(\overline{u})$.

$$\Omega_{p,I}(\overline{u}) \rightleftharpoons \bigvee_{i\in I\wedge j\in[1..m]} v_p(h_i(\overline{u})) < v_p(h_j(\overline{u})) \vee \bigvee_{i\in I} v_p(h_i(\overline{u})) = v_p(f_i(\overline{u})) \vee \bigvee_{i,j\in I\wedge i\neq j} v_p(g_i(\overline{z}) - g_j(\overline{z})) > v_p(h_i(\overline{u})).$$

Введём новые греческие переменные для каждого дизъюнкта с помощью (1.22) и (1.23) и перепишем эту формулу в желаемом виде. На этом завершается преобразование (1.21) с использованием НОД-леммы. Поскольку все нод-выражения с x в (1.21) являются регулярными, переменные $\overline{\beta}$ могут принимать только положительные значения. Присоединением $\overline{\beta} \geqslant 1$ к итоговой формуле, получим искомую формулу $\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$.

1.6 Теорема о сведении

Теперь мы можем доказать следующую теорему. Напомним, что позитивную экзистенциальную теорию некоторой структуры S мы обозначаем $\text{P}\exists\text{Th}S$. Для умножения на положительное целое число a введем унарный функциональный символ $a\cdot$.

Теорема 2. *Проблема разрешимости для* $\exists\mathrm{Th}\langle\mathbb{Z};0,1,+,-,\leqslant,\text{НОД}\rangle$ *сводится к проблеме разрешимости для* $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД}\rangle$.

Доказательство. Из леммы 1.2.2 следует, что достаточно проверить выполнимость в $\mathbb{Z}$ формул вида (1.7). Так как (1.7) является $L_{\mathcal{R}}$-формулой, докажем, что шаги 1 и 2 из разделов 1.4 и 1.5 действительно определяют алгоритм квазиэлиминации кванторов $\mathcal{R}$.

То, что шаг 1 удовлетворяет определению, следует из построения.

Для шага 2, во-первых, заметим, что условие (i) вводит нод-выражения, каждое из которых имеет вид ($\mathcal{R}$-1), ($\mathcal{R}$-3) или ($\mathcal{R}$-4); при переписывании (ii) и (iii) вводятся выражения следующих видов: ($\mathcal{R}$-2), ($\mathcal{R}$-3) или ($\mathcal{R}$-4), а для условия (iv) — нод-выражения ($\mathcal{R}$-3), либо ($\mathcal{R}$-4).

Теперь проверим, что выполняются ограничения на вид нод-выражений, содержащих греческую переменную из некоторого нод-выражения вида ($\mathcal{R}$-2). Видим, что для всех (новых) греческих переменных, введённых при переписывании условий (ii) и (iii), ограничение выполняется. В то же время, для всякой греческой переменной ζ, входившей в нод-выражение вида ($\mathcal{R}$-2) системы (1.21), появление ζ в правой части нод-выражения, полученного на шаге 2, может быть связано лишь с условием (i). Так как $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$ является $L^x_{\mathcal{R}}$-формулой, всякое нод-выражение с x, в правой части которого находится переменная ζ, имеет вид либо $\text{НОД}(f(\overline{z}),g(\overline{z})+x)=a\zeta$, либо $\text{НОД}(a\zeta,g(\overline{z})+x)=b\zeta$. Следовательно, из (i) получаем нод-выражения вида $\text{НОД}(a\zeta,f(\overline{z}))=a\zeta$, либо $\text{НОД}(b\zeta,a\zeta)=b\zeta$. Таким образом, формула $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$, полученная в результате выполнения шага 2, действительно является $L_{\mathcal{R}}$-формулой.

Для завершения доказательства достаточно заметить, что каждая $L^2_{\mathcal{R}}$-формула является формулой вида $\exists\overline{\alpha}\left(\overline{\alpha}\geqslant 1\wedge\bigvee\limits_{j\in J}\varphi_j(\overline{\alpha})\right)$ для конечного множества индексов J, где $\varphi_j(\overline{\alpha})$ есть конъюнкция атомарных формул вида $\text{НОД}(a',b')=c'$, $\text{НОД}(a',b')=c\zeta$, $\text{НОД}(a\zeta,b')=c\eta$ или $\text{НОД}(a\zeta,b\eta)=c\theta$ для некоторых положительных целых чисел a,b,c и неотрицательных целых чисел a',b',c'. Чтобы получить позитивную формулу сигнатуры $\langle 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД}\rangle$, избавимся от случаев равенства нулю чисел a',b',c'.

Истинность $\text{НОД}(a',b')=c'$ можно непосредственно проверить и либо исключить это нод-выражение из системы $\varphi_j(\overline{\alpha})$, либо заключить, что система невыполнима. Невыполнимость $\varphi_j(\overline{\alpha})$ в положительных целых числах также следует из наличия нод-выражения вида $\text{НОД}(0,0)=c\zeta$. Наконец исключим выражения вида $\text{НОД}(a,0)=c\zeta$ и $\text{НОД}(a\zeta,0)=c\eta$, подставляя всюду в первом случае $\frac{a}{c}$ вместо ζ и во втором случае $\frac{a}{c}\zeta$ вместо η, а затем умножая полученные нод-выражения на c. □

1.7 Системы нод-выражений с единственным ненулевым коэффициентом в полиномах

В этом разделе с помощью алгоритма квазиэлиминации кванторов будет доказана разрешимость позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$, что завершит доказательство теоремы 1.

Отметим, что если бы перед нами стояла оригинальная задача доказательства разрешимости $\exists$-теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leqslant, \text{НОД}\rangle$, то было бы достаточно дополнить теорему 2 ссылкой на разрешимость арифметики Сколема с константами. Напомним, что арифметика Сколема есть элементарная теория структуры $\langle \mathbb{Z}_{>0}; \cdot, =\rangle$, то есть, арифметика умножения. Т. Сколем дал неформальное доказательство разрешимости методом близким элиминации кванторов [13; 73]. Строгое доказательство было получено в 1952 году А. Мостовским [57] с помощью разработанного им инструмента прямого произведения структур. Альтернативные доказательства были позже получены П. Сигиельски [22] и Б.Р. Ходжсоном [41]. Так как в структуре $\langle \mathbb{Z}_{>0}; \cdot, =\rangle$ не выразимы отношения $x = a$ ни для какого натурального $a \geqslant 2$ (см. [13]), для наших целей потребуется несколько более общий результат. Доказательство разрешимости $\text{Th}\langle \mathbb{Z}_{>0}; \{a\}_{a\in\mathbb{Z}_{>0}}, \cdot, =\rangle$ проводится несложным сведением к арифметике Сколема [32]. Теперь, ввиду выразимости отношения НОД с помощью формулы

$$\text{НОД}(x,y) = z \Leftrightarrow z \mid x \wedge z \mid y \wedge \forall t(t \mid x \wedge t \mid y \Rightarrow t \mid z), \tag{1.24}$$

по определению делимости $x \mid y \rightleftharpoons \exists z(y = z \cdot x)$ получаем разрешимость элементарной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$.

В то же время, для завершения доказательства теоремы 1 достаточно доказать разрешимость только позитивной экзистенциальной теории указанной структуры. Продемонстрируем удобство использования алгоритмов квазиэлиминации кванторов на примере решения этой задачи. Ясно, что достаточно рассмотреть проблему выполнимости в положительных целых числах системы нод-выражений с линейными полиномами вида либо a, либо ax для некоторого положительного целого числа a. Для этой задачи будет построен алгоритм квази-ЭК $\mathcal{D}$. На шаге 2 алгоритма $\mathcal{D}$ используется следующий частный случай НОД-леммы.

Лемма 1.7.1. *Система* $\bigwedge\limits_{i\in[1..m]} \text{НОД}(a_i, x) = d_i$, *где* $a_i, d_i \in \mathbb{Z}$ *такие, что* $a_i \neq 0$, $d_i > 0$ *для каждого* $i \in [1..m]$, *имеет решение в* $\mathbb{Z}$ *тогда и только тогда, когда одновременно выполняются следующие условия:*

(a) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$

(b) $\bigwedge\limits_{1\leqslant i<j\leqslant m} \text{НОД}(a_i,d_j) = \text{НОД}(a_j,d_i) = \text{НОД}(d_i,d_j)$

Доказательство. Поскольку в данном случае все значения b_i из НОД-леммы равны нулю, достаточно рассмотреть только условия (i) и (iii). Первое из них остается неизменным, а третье имеет вид системы следующих пар делимостей:

$$\text{НОД}(a_i,d_j) \mid d_i \wedge \text{НОД}(a_j,d_i) \mid d_j$$

для всяких $1 \leqslant i < j \leqslant m$. Делимость, очевидно, вытекает из (b). Обратно, (b) получаем из следующей цепочки равенств:

$$\text{НОД}(a_i,d_j) = \text{НОД}\,(d_i,\text{НОД}(a_i,d_j)) = \text{НОД}\,(\text{НОД}(d_i,a_i),d_j)) = \text{НОД}\,(d_i,d_j)\,.$$

□

Теперь рассмотрим структуру $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$ и определим алгоритм квази-ЭК $\mathcal{D}$. В этом алгоритме S_2 будет пустым сортом переменных. Язык $L_{\mathcal{D}}$ алгоритма $\mathcal{D}$ будет представлять собой множество формул $\bigvee\limits_{j\in J_1} \varphi_j(\overline{y_j})$ для некоторого конечного множества индексов J_1 и конъюнкций нод-выражений $\varphi_j(\overline{y})$, таких что каждое нод-выражение имеет одну из следующих форм:

($\mathcal{D}$-1) $\text{НОД}(au,bv) = dw$

($\mathcal{D}$-2) $\text{НОД}(au,bv) = d$

($\mathcal{D}$-3) $\text{НОД}(a,bv) = d$

($\mathcal{D}$-4) $\text{НОД}(a,b) = d$,

где u и v — различные переменные, w может совпадать с u или v, а a,b,d — положительные целые числа. Кроме того, каждая конъюнкция $\varphi_j(\overline{y})$ для всякой пары переменных $u,v \in \overline{y}$ содержит нод-выражение с левой частью вида $\text{НОД}(au,bv)$ для некоторых положительных целых чисел a и b.

Множество формул элиминационного вида $L^x_{\mathcal{D}} \subseteq L_{\mathcal{D}}$ содержит формулы $\bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x,\overline{z_j})$ для конечного множества индексов J_2 и $\widetilde{\varphi}_j(x,\overline{z})$ вида

$$\widetilde{\widetilde{\varphi}}_j(\overline{z}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} \text{НОД}(\widetilde{f}_{i,j}(\overline{z}),c_{i,j}x) = \widetilde{h}_{i,j}(\overline{z}), \tag{1.25}$$

так что x не входит в $\overline{z}$, $c_{i,j} > 0$ и $\widetilde{\widetilde{\varphi}}_j(\overline{z})$ есть система нод-выражений с переменными из $\overline{z}$.

Прежде чем определить шаги 1 и 2 алгоритма $\mathcal{D}$, докажем следующую лемму.

Лемма 1.7.2. *Проблема разрешимости для* $\text{P}\exists\text{Th}\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$ *сводится к проблеме разрешимости для* $L^1_{\mathcal{D}}$*-теории.*

Доказательство. Рассмотрим систему нод-выражений

$$\bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}) \tag{1.26}$$

для $f_i(\overline{y})$,$g_i(\overline{y})$,$h_i(\overline{y})$ вида либо au, либо a, где a есть некоторое положительное целое число и $u \in \overline{y}$.

Для нод-выражений вида $\text{НОД}(au,bu) = h(\overline{y})$ наибольший общий делитель может быть непосредственно вычислен, и мы можем избавиться от одной из переменных. В случае $\text{НОД}(a,g(\overline{y})) = du$, где $a,d > 0$, система (1.26) эквивалентна дизъюнкции по всем положительным делителям d' числа $\frac{a}{d}$ систем, полученных из (1.26) подстановкой d' вместо каждого вхождения u.

Рассмотрим пары переменных $u,v \in \overline{y}$, для которых в (1.26) не задано значение НОД(au,bv) ни для каких положительных целых чисел a и b. Введем новую переменную $t_{\{u,v\}}$ для каждой такой пары (u,v) и добавим в систему (1.26) выражение НОД$(u,v) = t_{\{u,v\}}$. Продолжая этот процесс для новых переменных, мы вводим не более 2^n переменных t_Y для наибольших общих делителей различных подмножеств Y из $\overline{y}$ (так как для каждой пары переменных t_{Y_1} и t_{Y_2} имеем НОД(t_{Y_1},t_{Y_2}) $= t_{Y_1 \cup Y_2}$). □

Теорема 3. P∃Th$\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}$,НОД$\rangle$ *разрешима.*

Доказательство. Из леммы 1.7.2 следует, что если определить алгоритм квази-ЭК $\mathcal{D}$ для языка $L_{\mathcal{D}}$ в $\mathbb{Z}_{>0}$, то получим разрешающую процедуру для P∃Th$\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}$,НОД$\rangle$. Определим два шага $\mathcal{D}$.

Шаг 1. Пусть имеется некоторая $L_{\mathcal{D}}$-формула вида (1.26). Построим ориентированный граф, вершинами которого являются переменные системы (1.26), а каждая дуга от вершины u к вершине v соответствует нод-выражению, в котором $h_i(\overline{y})$ имеет вид du, и либо $f_i(\overline{y})$, либо $g_i(\overline{y})$ имеет вид av. В полученном графе будем искать циклы и переписывать (1.26) в виде дизъюнкции систем с меньшим числом переменных. Видим, что если граф, построенный по системе вида (1.26), не имеет циклов, то $L_{\mathcal{D}}$-формула (1.26) содержит переменные, которые не входят в правую часть ни одного из нод-выражений и, таким образом, является $L^x_{\mathcal{D}}$-формулой.

Предположим, имеется некоторый цикл $y_1 \to y_2 \to ... \to y_s \to y_1$. Он соответствует последовательности делимостей вида

$$a_1y_1 \mid b_1y_2,...,a_{s-1}y_{s-1} \mid b_{s-1}y_s,\gamma y_s \mid \delta y_1.$$

Первые $(s-1)$ делимостей дают делимость вида $\alpha y_1 \mid \beta y_s$. Таким образом, имеем $\beta y_s = k\alpha y_1$ для некоторого положительного целого числа k. Так как $\gamma y_s \mid \delta y_1$, то $\gamma\beta y_s \mid \delta\beta y_1$ и следовательно $\gamma k\alpha y_1 \mid \delta\beta y_1$. Поскольку $y_1 > 0$, существует конечное множество таких k, и мы можем исключить одну из переменных, например, y_s. Продолжая этот процесс, исключаем все переменные из этого цикла, кроме y_1.

Шаг 2. Рассмотрим подсистему (1.25) с изолированной переменной x. Как и в разделе 1.5, мы можем предположить, что все $c_{i,j}$ равны 1, и работать с $L^x_{\mathcal{D}}$-формулой вида

$$\widetilde{\widetilde{\varphi}}(\overline{z}) \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{z}),x) = h_i(\overline{z}). \tag{1.27}$$

Применяя лемму 1.7.1, рассмотрим каждый пункт отдельно.

(a). В этом случае получаем конъюнкцию $\bigwedge\limits_{i\in[1..m]}$ НОД($h_i(\overline{z})$,$f_i(\overline{z})$) $= h_i(\overline{z})$.

(b). Для каждой пары $1 \leqslant i < j \leqslant m$ необходимо переписать цепочку равенств

$$\text{НОД}(f_i(\overline{z}),h_j(\overline{z})) = \text{НОД}(f_j(\overline{z}),h_i(\overline{z})) = \text{НОД}(h_i(\overline{z}),h_j(\overline{z})).$$

Рассмотрим два случая. Если $h_i(\overline{z}) = d_i$ или $h_j(\overline{z}) = d_j$ для некоторых положительных целых чисел d_i, d_j, то получим следующую дизъюнкцию по всем положительным делителям

d_i (предполагая, что имеет место первое равенство):

$$\bigvee_{d|d_i} (\text{НОД}(f_i(\overline{z}),h_j(\overline{z})) = d \wedge \text{НОД}(f_j(\overline{z}),d_i) = d \wedge \text{НОД}(d_i,h_j(\overline{z})) = d)\,.$$

Теперь предположим, что нод-выражения с номерами i и j имеют вид ($\mathcal{D}$-1). Для $h_i(\overline{z}) = d_i z_i$ и $h_j(\overline{z}) = d_j z_j$ это условие переписывается следующим образом.

Если $z_i = z_j$, то получим конъюнкцию

$$\text{НОД}(f_i(\overline{z}),d_j z_j) = \text{НОД}(d_i,d_j)z_i \wedge \text{НОД}(f_j(\overline{z}),d_i z_i) = \text{НОД}(d_i,d_j)z_i.$$

Пусть теперь $z_i \neq z_j$, тогда система (1.27) должна содержать нод-выражение вида $\text{НОД}(az_i,bz_j) = h(\overline{z})$. Следовательно, $\text{НОД}(z_i,z_j) = \frac{h(\overline{z})}{\text{НОД}(a,b)l}$ для некоторого делителя l числа $\text{НОК}(a,b)$, а значит $\text{НОД}(h_i(\overline{z}), h_j(\overline{z}))$ должен быть равным $\frac{\text{НОД}(d_i,d_j)k}{\text{НОД}(a,b)l}h(\overline{z})$ для некоторого $k \mid \text{НОК}(d_i,d_j)$.

Обозначим $M_{k,l} = \frac{\text{НОД}(d_i,d_j)k}{\text{НОД}(a,b)l}$ и перепишем условие (b) для пары (i,j) с помощью следующей дизъюнкции:

$$\bigvee_{k|\text{НОК}(d_i,d_j)} \Bigg(\bigvee_{l|\text{НОК}(a,b)} \text{НОД}(h_i(\overline{z}),h_j(\overline{z})) = M_{k,l}h(\overline{z}) \\ \wedge \text{НОД}(f_i(\overline{z}),h_j(\overline{z})) = M_{k,l}h(\overline{z}) \wedge \text{НОД}(f_j(\overline{z}),h_i(\overline{z})) = M_{k,l}h(\overline{z}) \Bigg).$$

Полученная формула, очевидно, является $L_{\mathcal{D}}$-формулой, что завершает определение алгоритма квази-ЭК $\mathcal{D}$ и доказательство теоремы. □

Теорема 1 теперь следует из теоремы 2 и теоремы 3.

1.8 Заключение и переход к главе 2

Проблема разрешимости для экзистенциальной теории структуры $\langle \mathbb{Z}; 0,1, +, -, \leqslant, \text{НОД}\rangle$ была сведена к проблеме разрешимости для позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$. Затем была доказана разрешимость последней теории. Идеи как сведения, так и доказательства разрешимости были по существу одинаковы: изолировать переменную и затем преобразовать формулу с помощью НОД-леммы, обобщения китайской теоремы об остатках. Для формализации этой идеи было введено понятие алгоритма квазиэлиминации кванторов, и были построены алгоритмы квази-ЭК $\mathcal{R}$ и $\mathcal{D}$ для решения двух указанных задач.

Алгоритм не использует сложных аргументов и, по существу, полностью описан в разделе 1.2, в то время как остальные разделы главы раскрывают конкретные детали. Нетрудно получить из нашего алгоритма разрешающие процедуры для экзистенциальных теорий таких структур, как $\langle \mathbb{N}; 0,S, |\rangle$ или $\langle \mathbb{Z}; 0,S, \leqslant, \text{НОД}\rangle$, где S соответствует функции следования

$Sx = x + 1$. Указанные структуры интересны в том смысле, что с помощью символов их сигнатур можно записать систему (4). Следовательно, не существует полинома $poly$, такого, что всякая выполнимая в $\mathbb{N}$ формула φ языка $L_{\langle 0,S,|\rangle}$ (либо выполнимая в целых числах $L_{\langle 0,S,\leqslant,\text{НОД}\rangle}$-формула) содержит выполняющий набор, ограниченный $poly(|\varphi|)$, где $|\varphi|$ есть число символов в записи формулы φ. Любопытно ответить на вопрос о принадлежности какой-либо из указанных теорий классу **NP**. Это исследование кажется естественным подходом к изучению алгоритмической сложности $\exists\mathrm{Th}\langle\mathbb{Z}; 0,1, + , - , \leqslant ,\text{НОД}\rangle$.

Понятие квазиэлиминации может помочь при попытке доказательства разрешимости $\exists\mathrm{Th}\langle\mathbb{N}; 1, + , | ,P_2\rangle$. Как отмечает А. Сирокофских [72], на близкий вопрос пробовали найти ответ Дж. Робинсон и Л. Липшиц: „J. Robinson asked in a personal communication with L. Lipshitz whether the existential theory of $\mathbb{Z}$ in the language of addition, divisibility and the predicate for powers of 2 is decidable“. Заметим также, что эта задача и проблема разрешимости для экзистенциальной арифметики Бюхи по основанию 2 с делимостью сводятся друг к другу. Последняя теория есть $\exists\mathrm{Th}\langle\mathbb{N}; 1, + , | ,V_2\rangle$, где V_2 — это двухместный предикат, такой что $V_2(x,y)$ имеет место тогда и только тогда, когда y является наибольшей степенью двойки, делящей x. Видим, что $V_2(x,y) \Leftrightarrow P_2(y) \wedge y \mid x \wedge 2y \nmid x$, и обратно: $P_2(x) \Leftrightarrow V_2(x,x)$. Даже в случае отрицательного ответа на вопрос о разрешимости этих проблем, можно далее спросить, разрешима ли хотя бы $\exists\mathrm{Th}\langle\mathbb{N}; 1, + , \perp ,P_2\rangle$? Чтобы ответить на такой вопрос, необходимо представлять себе особенности разрешающего алгоритма для $\exists\mathrm{Th}\langle\mathbb{N}; 1, + , \perp\rangle$.

Если заменить отношение НОД в БЛ-теореме на отношение взаимной простоты, шаг 1 алгоритма $\mathcal{R}$ значительно упростится. В этом случае нод-выражения имеют вид либо $\text{НОД}(f(\overline{x}),g(\overline{x})) = d$ для выражений с отношением взаимной простоты, либо, для их отрицаний, $\text{НОД}(f(\overline{x}),g(\overline{x})) = a\zeta$, где $\zeta \geqslant 2$ и a,d — положительные целые числа, в изначальной формуле равные единице. Более того, использование греческих переменных в алгоритме $\mathcal{R}$ можно избежать, если рассматривать только позитивные экзистенциальные формулы языка первого порядка сигнатуры $\sigma_\perp = \langle 0,1, + , - , \neq ,\text{НОД}_1,\text{НОД}_2,...\rangle$, где $\text{НОД}_d(x,y) \rightleftharpoons \text{НОД}(x,y) = d$. В этом случае, как и в примере 1.2.2, алгоритм может быть легко преобразован в алгоритм построения по всякой позитивной экзистенциальной $L_{\sigma_\perp}$-формуле эквивалентной в $\mathbb{Z}$ позитивной бесквантворной $L_{\sigma_\perp}$-формулы. Таким способом в следующей главе будет получено описание всех отношений, Р$\exists$-выразимых в структуре $\langle\mathbb{Z}; 1, + , \perp\rangle$.

Глава 2. Позитивная экзистенциальная выразимость с единицей, сложением и взаимной простотой

> For instance, it is not clear whether one can define the order relation in the existential fragment of $\langle \mathbb{Z}; +, |, 0, 1\rangle$, hence we will work with $\langle \mathbb{Z}; +, |, \leqslant, 0, 1\rangle$ instead of it, whenever needed.
>
> M. Bozga and R. Iosif [15] (2005)

Глава посвящена применению алгоритмов квази-ЭК к вопросам выразимости. В частности, будет доказано, что если определить $\text{НОД}_d(x,y) \rightleftharpoons \text{НОД}(x,y) = d$, то всякое отношение является позитивно экзистенциально выразимым в структуре $\langle \mathbb{Z}; 1, +, \perp\rangle$ тогда и только тогда, когда оно позитивно бесквантorно выразимо в структуре $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \text{НОД}_4, \ldots\rangle$. Следствием этого результата является тот факт, что отрицание отношения взаимной простоты и отношение порядка не являются позитивно экзистенциально выразимыми в структуре $\langle \mathbb{Z}; 1, +, \perp\rangle$. Кроме того, будут получены три обобщения БЛ-теоремы. Глава завершается построением квази-ЭК алгоритмов для $\exists\text{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, \perp\rangle$ и для значительно более простого позитивного фрагмента этой теории.

2.1 Арифметика целых чисел с единицей, сложением и взаимной простотой

В тех случаях, когда удаётся описать свойства некоторых объектов (таких как программы со списками [15] или параметрические отднсчётчиковые автоматы [37]) с помощью формул арифметики целых чисел с единицей, сложением, порядком и делимостью, хотелось бы также иметь некоторое описание отношений, выразимых с помощью таких формул. Помимо нескольких примеров, мы не обладаем значительными общими результатами об экзистенциальной выразимости в структуре $\langle \mathbb{Z}; 1, +, -, \leqslant, |\rangle$. В первой главе была показана $\exists$-выразимость графика функции НОД и его отрицания (1.4), а значит, и отношения взаимной простоты $x \perp y$ вместе со своим отрицанием. Кроме того, мы пользовались P$\exists$-выразимостью в этой структуре отношения неделимости (1.2), и поэтому естественно спросить, является ли отрицание отношения взаимной простоты P$\exists$-выразимым в $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp\rangle$? Другой естественный вопрос задают М. Божга и Р. Иосиф [15, замечание 2 на с. 428]: является ли отношение порядка $\exists$-выразимым в структуре $\langle \mathbb{Z}; 1, +, -, |\rangle$?

Среди общих результатов о $\exists$-выразимости в $\langle \mathbb{Z}; 1, +, -, \leqslant, |\rangle$ можно отметить результат Л. Липшица [52] о том, что всякое таким образом выразимое множество $S \subseteq \mathbb{N}$ является

объединением некоторого конечного множества и (возможно пустого или бесконечного) объединения арифметических прогрессий. Некоторые свойства роста функций с $\exists$-выразимыми в $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$ графиками изучались Л. ван ден Дрисом и А. Уилки [31], однако эти результаты не помогают ответить на указанные выше вопросы о выразимости.

Классическим способом описания отношений, выразимых в некоторой структуре $\langle M; \sigma \rangle$, является построение алгоритмов элиминации кванторов. Наиболее близкими к интересующей нас структуре являются: арифметика целых чисел с единицей, сложением и порядком и арифметика p-адических чисел с единицей, сложением, равенством и отношением строгой делимости $x \parallel y \rightleftharpoons v_p(x) < v_p(y)$. В первом случае М. Пресбургером [63] (см. также [38]) было показано, что всякое отношение выразимо в структуре $\langle \mathbb{Z}; 1, +, -, \leqslant \rangle$ тогда и только тогда, когда оно бесквантворно выразимо в $\langle \mathbb{Z}; 1, +, -, \leqslant, 2 \mid, 3 \mid, 4 \mid, ... \rangle$, где $d \mid$ суть унарные отношения делимости на целые константы $d \geqslant 2$. Алгоритмы элиминации кванторов для структуры $\langle \mathbb{Q}_p; 1, +, -, =, \| \rangle$ были построены В. Виспфеннингом [83] и Т. Штурмом [78], из чего также следует описание всех выразимых в этой структуре отношений, как выразимых некоторой бесквантворной формулой.

Указанная статья Виспфеннинга [83] повлекла за собой интенсивное развитие методов элиминации кванторов с помощью так называемой виртуальной подстановки. Реализацией этих методов на практике занялись ученики Виспфеннинга, главным образом, А. Дольцман и Т. Штурм. Ими был разработан пакет RedLog [30] для системы компьютерной алгебры REDUCE, нашедший массу приложений и продолжающий развиваться по настоящее время (см. обзор Т. Штурма [80], а так же страницу пректа RedLog[1]). В частности, в RedLog реализована элиминация кванторов в линейной теории p-адических чисел, а для арифметики Пресбургера применялись алгоритмы элиминации кванторов, разработанные А. Лазаруком и Т. Штурмом [46; 47].

Аналоги элиминации кванторов в арифметике Пресбургера применяются и для иных структур, как, например, в недавней работе П. Бэкмана, Ф. Рюммера и А. Зельича [12] об элиминации кванторов в машинной арифметике (арифметике битовых векторов). Отметим, что несмотря на известную взаимосвязь операций над битовыми векторами и над 2-адическими числами [43], алгоритмы элиминации кванторов в линейных теориях 2-адических чисел, по-видимому, не привлекали значительного внимания у специалистов по формальной верификации.

Другим важным для нас примером является результат В. Виспфеннинга [84], который был получен в 1999 году. Элиминацией кванторов Виспфеннинг показал, что множества, выразимые в структуре $\langle \mathbb{Q}; 1, +, -, =, <, Int \rangle$, где Int — унарный предикатный символ для свойства «быть целым числом», суть в точности множества, бесквантворно выразимые в структуре $\langle \mathbb{Q}; 1, +, -, [\,], \{c\cdot\}_{c \in \mathbb{Q}}, =, < \rangle$. Здесь $[\,]$ есть унарный функциональный символ для функции, вычисляющей целую часть числа, а $c\cdot$ — унарные функциональные символы для умножения на рациональные константы c. Отметим, что этот результат был известен ещё в 1991 году К. Сморьинскому, однако, вероятно, он не придавал этому утверждению

[1] https://www.redlog.eu/references/

особенного значения и включил в свою книгу «Logical Number Theory I» в качестве упражнения [74, III.4, Exercise 15].

Отметим, что во всех рассмотренных структурах достаточно было построить позитивную бесквантерную формулу $\psi(\overline{y})$, эквивалентную в соответствующей структуре данной позитивной экзистенциальной формуле (P$\exists$-формуле) $\exists x \varphi(x,\overline{y})$, так как всякое отрицание атомарной формулы может быть переписано некоторой позитивной бесквантерной формулой. В каждом случае мы в качестве следствия получаем разрешимость элементарных теорий.

В той же работе В. Виспфеннинг [84] замечает: «By way of contrast, quantifier elimination definitely breaks down if one admits scalar multiplication by a real parameter or integer divisibility in the language» и в связи с БЛ-теоремой спрашивает, будет ли разрешимой P$\exists$Th$\langle \mathbb{R}; 1, +, -, [\,], | \rangle$, где $x \mid y \rightleftharpoons \exists z(Int(z) \wedge y = xz)$? Утверждение о невозможности проэлиминировать кванторы в случае добавления в сигнатуру отношения целочисленной делимости есть следствие несложного замечания Л. Липшица [52]. Им было показано, что всякое перечислимое множество является выразимым в структуре $\langle \mathbb{N}; 1, +, | \rangle$ с помощью формулы с единственным универсальным квантором, который следует за блоком экзистенциальных кванторов: $\exists ... \exists \forall$. Действительно, можно показать (аналогичное рассуждение будет использовано в доказательстве следствия 3.4.1.1), что этот факт следует из выразимости графика возведения в квадрат с помощью следующей универсальной формулы:

$$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z(x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z). \qquad (2.1)$$

Таким образом, неразрешимыми оказываются $\forall\exists$- и $\exists\forall$-теории структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Отметим, что если определить отношение делимости на два последовательных числа $x \,{}^{S}|\, y \rightleftharpoons x \mid y \wedge x + 1 \mid y$, то из формулы (2.1) практически непосредственно следует выразимость графика возведения в квадрат в структуре $\langle \mathbb{N}; 1, +, {}^{S}| \rangle$. К вопросам выразимости в структурах с отношением ${}^{S}|$ мы перейдём в главе 3.

В связи с этим отрицательным результатом важной проблемой является поиск возможно более широких разрешимых фрагментов $\forall\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Основываясь на работах М. Божги и Р. Иосифа [15], и в особенности на работах К. Хаасе, С. Крётцера, Дж. Оакнина, Дж. Уоррелла [64] и А. Лечнер [48], в недавнем препринте [61] Г.А. Перес и Р. Раха определили семейство $\forall\exists$-формул языка с единицей, сложением и делимостью; доказали его разрешимость в натуральных числах и применили полученный результат при изучении разрешимости и алгоритмической сложности проблем синтеза для параметрических односчётчиковых автоматов (P1CA). Разрешимость проблемы достижимости для P1CA была установлена в 2009 году в указанной работе К. Хаасе и соавторов [64] с помощью БЛ-теоремы. Оказывается, что свойство достижимости в P1CA можно выразить экзистенциальной $L_{\langle 1,+,-,\leqslant,| \rangle}$-формулой и, кроме того, существует и обратное сведение [37, Lemma 4.2.1].

О взаимосвязи автоматов и вопросов выразимости в арифметических теориях отметим следующее. В некоторых структурах, таких как $\langle \mathbb{N}; 0, 1, +, P_k, = \rangle$ или в k-арифметике Бюхи $\langle \mathbb{N}; 0, 1, +, V_k, = \rangle$, где $k \geqslant 2$ и $V_k(x,y) \Leftrightarrow (P_k(y) \wedge \text{НОД}(ky,x) = y)$, вопросы выразимости успешно решаются с помощью автоматных средств. По известной теореме Р.Ю. Бюхи [18;

54] всякое отношение на натуральных числах, закодированных в системе счисления по основанию $k \geqslant 2$, является распознаваемым детерминированным k-автоматом тогда и только тогда, когда это отношение выразимо в структуре $\langle \mathbb{N}; 0,1, +, V_k, = \rangle$. В то же время, как было показано А.Л. Семёновым [8], структура $\langle \mathbb{N}; 0,1, +, P_k, = \rangle$ является менее выразительной. В 1992 году Р. Вильмер [82] показал, что всякое отношение, выразимое в арифметике Бюхи, выразимо в этой структуре некоторой $\exists\forall\exists$-формулой. Как замечают К. Хаасе и Я. Ружицкий [40], несложная модификация доказательства Вильмера позволит строить $\forall\exists$-формулы, однако экзистенциальная арифметика Бюхи оказывается уже менее выразительной.

Обозначим $L_{k\text{-}BA}$ язык арифметики Бюхи по основанию k. Указанные описания всех отношений, выразимых в k-арифметике Бюхи, были получены следующим образом: для всякой $L_{k\text{-}BA}$-формулы $\varphi(x_1,...,x_n)$ по теореме Бюхи строится k-автомат $\mathcal{A}$, который распознаёт в точности те $(a_1,...,a_n) \in \mathbb{N}^n$, для которых истинна формула $\varphi(a_1,...,a_n)$. Далее по автомату $\mathcal{A}$ можно построить $\forall\exists L_{k\text{-}BA}$-формулу $\psi(x_1,...,x_n)$, кодирующую работу $\mathcal{A}$, то есть, формула ψ истинна для значений $(a_1,...,a_n)$ в том и только том случае, когда $\mathcal{A}$ принимает $(a_1,...,a_n)$. Таким образом, говоря несколько неформально, в случае арифметики Бюхи *«элиминационным видом»* данной формулы является соответствующий этой формуле автомат. Возможно, автоматный подход к арифметике натуральных чисел с единицей, сложением и делимостью [19; 37; 49; 64] даст столь же значительные результаты в вопросах выразимости, как и в случае арифметики Бюхи (см. обзоры [13; 54]). Однако, в диссертации будет использоваться арифметический способ исследования выразимости, и в дальнейшем мы не будем возвращаться к автоматному подходу.

С практической точки зрения вопрос о том, какой подход к изучению вопросов выразимости и разрешимости для арифметических структур является более удачным, с помощью элиминации кванторов или автоматный, по-видимому, следует считать мало изученным. Процитируем замечание К. Хаасе [38] в связи разрешающими процедурами для арифметикой Пресбургера: «While to the best of the author's knowledge the automata-based approach is not widely applied in practice these days, it is worth mentioning that it can empirically be more efficient compared to quantifier elimination. For instance, even on small instances of the Frobenius problem presented in the introduction, a straight-forward implementation of the automata-based decision procedure outperforms the quantifier-elimination procedure implemented in the SMT-solver Z3 [58] by orders of magnitudes». В последнем утверждении Хаасе ссылается на неформальное обсуждение вопроса с М. Блондином.

Не выглядит простой задачей понять, как можно было бы воспользоваться алгоритмом квазиэлиминации кванторов из главы 1 для описания отношений, экзистенциально выразимых (этот класс совпадает, как было отмечено выше, со всеми Р$\exists$-выразимыми) в структуре $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Однако, в случае, когда второй сорт переменных в алгоритме квазиэлиминации является пустым, как примере 1.2.2, возможно применение подхода элиминации кванторов к описанию предикатов, выразимых экзистенциальными формулами языка этого алгоритма. Поэтому естественно рассмотреть языки, промежуточные между $\exists L_{\langle 1,+,-,\leqslant \rangle}$ и $\exists L_{\langle 1,+,-,\leqslant,| \rangle}$, и попытаться построить для них алгоритмы квазиэлиминации в $\mathbb{Z}$. В этой главе будет изучаться Р$\exists$-выразимость в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$ и близкие вопросы.

Выразимость графика умножения в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$ была доказана в 1989 году Д. Ришаром [67]. Основной трудностью при доказательстве этого результата было установление выразимости отношения порядка (или, что эквивалентно, отношения «быть неотрицательным целым числом»), так как к тому моменту было известно, что в структуре $\langle \mathbb{N}; 1, +, \perp \rangle$ выразимо всякое арифметическое отношение. Последний результат был получен А. Вудсом [85] (причём двумя различными способами) и независимо Дж. Робинсон, однако это доказательство не было опубликовано.

Значительное внимание вопросам выразимости, и в частности, для структур с отношением взаимной простоты, было, по-видимому, впервые уделено в работе Дж. Робинсон [69]. Было доказано, что всякое арифметическое отношение, то есть, выразимое в структуре $\langle \mathbb{N}; +, \cdot, = \rangle$, является выразимым в $\langle \mathbb{N}; S, | \rangle$, где унарному функциональному символу S ставится в соответствие функция следования $x \mapsto x + 1$, а символ $|$, как обычно, соответствует делимости. Структуры, обладающие подобным свойством, были названы *полными по выразимости (Def-полными)* И. Корецом [44], которым был собран список наиболее примечательных Def-полных структур. Заменяя отношение делимости на отношение взаимной простоты, Дж. Робинсон спрашивает, является ли Def-полной структура $\langle \mathbb{N}; S, \perp \rangle$, либо возможно ли доказать по крайней мере неразрешимость элементарной теории этой структуры? Утвердительный ответ на второй вопрос был получен независимо Д. Ришаром [65] и А. Вудсом [85], в то время как вопрос о Def-полноте остаётся открытым. Известно, что эта проблема тесно связана с гипотезой Вудса-Эрдёша (см. обзор работ А. Вудса, написанный П. Сигиельски и Д. Ришаром [25]). Строгое определение понятия Def-полноты, близкие определения и примеры будут даны в главе 3.

Основным результатом настоящей главы является доказательство того, что всякое отношение, РЭ-выразимое в $\langle \mathbb{Z}; 1, +, \perp \rangle$, оказывается позитивно бесквантворно выразимым в структуре $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \ldots \rangle$, и наоборот. Здесь НОД_d для всякого $d \geqslant 2$ есть двухместный предикатный символ для отношения $\text{НОД}_d(x,y) \rightleftharpoons \text{НОД}(x,y) = d$. Сначала в разделе 2.2 будет показано, почему для элиминации сигнатура должна быть расширена. Затем в разделе 2.3 для всякой РЭ-формулы языка соответствующим образом расширенной сигнатуры $\exists x \varphi(x, \overline{y})$ будет построена эквивалентная в $\mathbb{Z}$ позитивная бесквантворная формула $\psi(\overline{y})$ того же языка. Это построение основано на НОД-лемме и задаёт алгоритм квазиэлиминации кванторов. Заметим, что переписывание четвёртого условия НОД-леммы для каждого простого p схоже с процессом элиминации кванторов в структуре $\langle \mathbb{Q}_p; 1, +, -, =, \| \rangle$.

В разделе 2.4 будет доказано, что отрицание отношения взаимной простоты не является РЭ-выразимым в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$, так как иначе $\text{Th}\langle \mathbb{Z}; 1, +, \perp \rangle$ оказалась бы разрешимой. Затем будут получены близкие результаты о РЭ-выразимости для структур $\langle \mathbb{N}; S, \perp \rangle$ и $\langle \mathbb{Q}; 1, +, -, \{c\cdot\}_{c \in \mathbb{Q}}, \perp \rangle$. Объединяя основную теорему главы с БЛ-теоремой, в разделе 2.5 будет построен разрешимый фрагмент $\forall\exists\text{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Также будет показано, как можно применить НОД-лемму для того, чтобы обобщить результат о разрешимости, полученный Г.А. Пересом и Р. Рахой [61]. В этом же разделе будет получено ещё одно обобщение БЛ-теоремы, именно, разрешимой оказывается экзистенциальная теория структуры $\langle \mathbb{R}; 1, +, -, [\,], <, | \rangle$, что даст утвердительный ответ на вопрос Виспфеннинга.

Глава заканчивается построением алгоритмов квази-ЭК для позитивного и общего случая экзистенциальной теории структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$. Алгоритм элиминации кванторов из основной теоремы раздела 2.3 и два эти алгоритма являются тремя последовательно обобщающими друг друга случаями, когда сигнатура дополняется отношением порядка и отрицанием отношения взаимной простоты. Эти построения демонстрируют следующее. Алгоритмы квази-ЭК оказываются удобными при построении разрешающих процедур для теорий, промежуточных между экзистенциальной арифметикой сложения и $\exists$-арифметикой со сложением и делимостью. Заметим, что для $\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant \rangle$ сильная форма ЛС-леммы практически непосредственно даёт алгоритм из класса **NP** (см. [34] и [49, Section 2.3, Corollary 2]). Кроме того, эти алгоритмы укажут на существенные отличия между этими промежуточными P$\exists$-теориями при расширении сигнатуры.

2.2 Результаты о позитивной бескванторной невыразимости

В этом разделе будет показано, что для того, чтобы было возможно применить элиминацию кванторов для структуры $\langle \mathbb{Z}; 1, +, \perp \rangle$ в случае позитивных экзистенциальных формул, необходимо сначала расширить сигнатуру некоторыми P$\exists$-выразимыми предикатами. Следующая лемма даст нам основные примеры P$\exists$-выразимых в этой структуре отношений.

Лемма 2.2.1. *Отношения $x = 0$, $y = -x$, $x = y$, $x \neq 0$, $x \neq y$ и* НОД$(x,y) = d$ *для всякого целого $d \geqslant 2$ являются позитивно экзистенциально выразимыми в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$.*

Доказательство. Для первых двух отношений имеем следующие бескванторные определения: $x = 0 \Leftrightarrow x + 1 \perp x + 1 \wedge 3 \perp x + 2$ и $y = -x \Leftrightarrow x + y = 0$.

Формула $\exists t\,(x \perp t \wedge x \perp t + 4)$ определяет свойство $x \neq 0$. Формула очевидно ложна в случае $x = 0$. Если же теперь $x \neq 0$, то множество P_x простых делителей x будет конечным. Чтобы построить необходимое t, достаточно воспользоваться китайской теоремой об остатках для решения следующей системы сравнений:

$$t \equiv 1 (\mathrm{mod}\ 2) \wedge t \equiv 1 (\mathrm{mod}\ 3) \wedge \bigwedge_{p \in P_x \setminus \{2,3\}} t \equiv 2 (\mathrm{mod}\ p).$$

Действительно, для всякого простого делителя p числа x должно выполняться $p \nmid t \wedge p \nmid t + 4$.

Наконец, для равенства и его отрицания имеем $x = y \Leftrightarrow \exists t (t = -y \wedge x + t = 0)$ и $x \neq y \Leftrightarrow \exists t (t = -y \wedge x + t \neq 0)$, а отношение НОД$(x,y) = d$ выразимо формулой $\exists u \exists v\,(x = du \wedge y = dv \wedge u \perp v)$. □

Удобно включить в сигнатуру унарный функциональный символ '$-$', и далее считать, что каждый терм является линейным полиномом с целыми коэффициентами. Отношение равенства теперь бескванторно выразимо в $\langle \mathbb{Z}; 1, +, -, \perp \rangle$, а его отрицание (дизравенство) $\neq$ оказывается бескванторно выразимым в структуре $\langle \mathbb{Z}; 1, +, -, \neq 0, \perp \rangle$. В следующих двух

утверждениях мы покажем, что для того, чтобы каждое отношение из леммы 2.2.1 можно было выразить некоторой бесквантворной формулой, сигнатура $\langle \mathbb{Z}; 1, +, -, \perp \rangle$ должна быть расширена.

Прежде чем перейти к вопросам бесквантворной невыразимости, сформулируем в виде леммы одно стандартное преобразование, которым мы пользовались в разделе 1.4. Всякое выражение вида НОД$(f(\overline{y})+ax,g(\overline{y})+bx) = d$, где $a, b \neq 0$ и $f(\overline{y})$, $g(\overline{y})$ — линейные полиномы с целыми коэффициентами, может быть переписано с помощью алгоритма Евклида так, что коэффициент при переменной x окажется не равным нулю только в одном из полиномов этого выражения. Пусть $a > b > 0$ и $a = qb + r$, где $r \in [0, b)$, тогда

$$\text{НОД}(f(\overline{y}) + ax,g(\overline{y}) + bx) = d \Leftrightarrow$$
$$\text{НОД}(f(\overline{y}) - qg(\overline{y}) + rx, g(\overline{y}) + bx) = d.$$

Повторяя этот процесс до тех пор, пока один из коэффициентов x не станет делителем другого коэффициента, а затем ещё один раз применяя указанный шаг, мы получим выражение вида НОД$(\widetilde{f}(\overline{y}),\widetilde{g}(\overline{y}) + cx) = d$.

Лемма 2.2.2. *Для любых линейных полиномов с целыми коэффициентами $f(\overline{y})+ax$, $g(\overline{y})+bx$ можно построить линейные полиномы $\widetilde{f}(\overline{y})$ и $\widetilde{g}(\overline{y})+cx$, что* НОД$(f(\overline{y})+ax, g(\overline{y})+bx) =$ НОД$(\widetilde{f}(\overline{y}), \widetilde{g}(\overline{y}) + cx)$.

Утверждение 2.2.1. *Отношение $x \neq 0$ не является позитивно бесквантворно выразимым в структуре $\langle \mathbb{Z}; 1, +, -, \perp \rangle$.*

Доказательство. Предположим, что существует формула

$$\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right),$$

где $c_i > 0$, которая определяет отношение $x \neq 0$. Тогда $\varphi(0)$ должно быть ложно; следовательно, для любого $j \in J$ существует индекс $i \in I_j$ такой, что $a_i \not\perp b_i$. Обозначим этот индекс i_j. Если для всех $j \in J$ мы имеем $a_{i_j} = 0$, то формула $\varphi(x)$ является ложной для любого $x > \max\limits_{j \in J} |b_{i_j}| + 1$. Для случая, когда хотя бы одно из чисел a_{i_j} не равно нулю, определим $A = \prod\limits_{j \in J \wedge a_{i_j} \neq 0} a_{i_j}$. Но теперь A есть положительное целое число, для которого $\neg\varphi(A)$, что противоречит определению φ. □

Теперь докажем, что расширение сигнатуры предикатным символом для дизравенства всё ещё не является достаточным.

Утверждение 2.2.2. *Отношение* НОД$(x,y) = d$ *для любого фиксированного целого $d \geqslant 2$ не является позитивно бесквантворно выразимым в структуре $\langle \mathbb{Z}; 1, +, -, \neq, \perp \rangle$.*

Доказательство. Покажем, что утверждение истинно уже для $p \parallel x \rightleftharpoons p \mid x \wedge p^2 \nmid x$ для любого простого p. Это отношение является частным случаем формулы НОД$(x,y) = d$ для значений $d = p$ и $y = p^2$.

Предположим, что для отношения $p \parallel x$ имеется следующая формула:

$$\varphi(x) \rightleftharpoons \bigvee_{j\in J}\left(\bigwedge_{i\in I_j} a_i \perp b_i + c_i x \wedge \bigwedge_{i\in K_j} x \neq d_i\right).$$

Пусть D есть максимум всех чисел d_i из дизуравнений этой формулы. Ясно, что для всякого $x > D$ имеем $\varphi(x) \Leftrightarrow \bigvee\limits_{j\in J}\bigwedge\limits_{i\in I_j} a_i \perp b_i + c_i x$. Выберем $k > 1$, так что $p^k > D$. Тогда формула $\varphi(p^k)$ должна быть ложной. Теперь построим целое число A такое, что $p \parallel A$, но в то же время $\neg\varphi(A)$.

Поскольку имеет место $\neg\varphi(p^k)$, то для каждого $j \in J$ верно, что хотя бы для одного индекса $i \in I_j$ выполняется $a_i \not\perp b_i + c_i p^k$. Обозначим соответствующий индекс i_j для каждого $j \in J$. Разделим множество индексов J на два подмножества J_1 и J_2, первое из которых будет содержать такие индексы, что $p \nmid a_{i_j} \vee p \nmid b_{i_j}$, а второе множество J_2 — оставшиеся индексы, т.е., для которых $p \mid a_{i_j} \wedge p \mid b_{i_j}$. Видим, что для любого $x > D$ если $p \mid x$, то $\varphi(x) \Leftrightarrow \bigvee\limits_{j\in J_1}\bigwedge\limits_{i\in I_j} a_i \perp b_i + c_i x$.

Пусть для любого $j \in J_1$ имеем $a_{i_j} = p^{\alpha_j}\widetilde{a_{i_j}}$, где $\widetilde{a_{i_j}} \perp p$. Если определить $A = p^k + p \cdot \prod\limits_{j\in J_1}\widetilde{a_{i_j}}$, то ясно, что $p \parallel A$, но в то же время для любого $j \in J_1$ получим следующую цепочку равенств:

$$\text{НОД}(a_{i_j}, b_{i_j} + c_{i_j}p^k) = \text{НОД}(\widetilde{a_{i_j}}, b_{i_j} + c_{i_j}p^k) = \text{НОД}(\widetilde{a_{i_j}}, b_{i_j} + c_{i_j}A).$$

Первое равенство следует из того факта, что для $j \in J_1$ если $\alpha_j \neq 0$, то $p \perp b_{i_j}$ и поэтому ввиду $k > 1$, $b_{i_j} + c_{i_j}p^k$ не делится на p. Второе равенство следует из того, что остаток от деления A на a_{i_j} есть p^k для всякого $j \in J_1$.

Так как $a_{i_j} \not\perp b_{i_j} + c_{i_j}p^k$, получаем $a_{i_j} \not\perp b_{i_j} + c_{i_j}A$, и следовательно $\neg\varphi(A)$. □

Отношение $p \parallel x$ является бесквантворно выразимым в $\langle\mathbb{Z}; 1, +, -, 2\mid, 3\mid, 4\mid, ...\rangle$ формулой $p \mid x \wedge p^2 \nmid x$. Кроме того, для каждого фиксированного целого a, такого что $a = cd$ для некоторого целого c, отношение НОД(a,x) $= d$ выразимо с помощью формулы $\bigvee\limits_{k\perp c\wedge 1\leqslant k\leqslant c} a \mid x - dk$. Действительно, необходимо и достаточно, чтобы остаток от деления x на a делился на d и был взаимно прост с c.

Может быть интересным следующий вопрос: является ли НОД(x,y) $= d$ для $d \geqslant 2$ бесквантворно выразимым в $\langle\mathbb{Z}; 1, +, -, \perp, 2\mid, 3\mid, 4\mid, ...\rangle$? Однако в дальнейшем будет удобно использовать вместе с отношением взаимной простоты отношения НОД(x,y) $= d$ для всякого $d \geqslant 2$.

2.3 Основной результат о выразимости

Чтобы показать, что после расширения сигнатуры $\langle 1, +, -, \perp\rangle$ предикатными символами для отношений из утверждений 2.2.1 и 2.2.2, аналогичные примеры бесквантворной невыразимости уже нельзя будет построить, воспользуемся НОД-леммой из раздела 1.2.2.

Сейчас удобно повторить формулировку НОД-леммы, которая является критерием разрешимости в целых числах систем вида

$$\bigwedge_{i\in[1..m]} \text{НОД}(a_i,b_i + x) = d_i. \tag{2.2}$$

Лемма 2.3.1 (НОД-лемма)**.** *Определим для системы (2.2), где $a_i,b_i,d_i \in \mathbb{Z}$ и $a_i \neq 0$, $d_i > 0$, $i \in [1..m]$, и всякого простого числа p целое число $M_p = \max\limits_{i\in[1..m]} v_p(d_i)$ и два множества индексов $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ и $I_p = \{i \in J_p : v_p(a_i) > M_p\}$.*

Система (2.2) имеет решение в $\mathbb{Z}$ тогда и только тогда, когда одновременно выполняются следующие условия:

(i) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$

(ii) $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(d_i,d_j) \mid b_i - b_j$

(iii) $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(a_i,d_j,b_i - b_j) \mid d_i$

(iv) Для всякого простого $p \leqslant m$ и всякого $I \subseteq I_p$ такого, что $|I| = p$ существуют такие $i, j \in I$, $i \neq j$, что $v_p(b_i - b_j) > M_p$.

Зафиксируем сигнатуру $\sigma = \langle 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \text{НОД}_4, ...\rangle$ и покажем, как применить лемму 2.3.1 чтобы проэлиминировать кванторы в $\text{P}\exists L_\sigma$-формуле. Следующая теорема будет активно использоваться в разделах 2.4 и 2.5.

Теорема 4. *Существует алгоритм, сопоставляющий всякой L_σ-формуле вида $\exists x \varphi(x,\overline{y})$, где $\varphi(x,\overline{y})$ — позитивная бесквантороная, позитивную бесквантороную L_σ-формулу $\psi(\overline{y})$, эквивалентную $\exists x \varphi(x,\overline{y})$ в $\mathbb{Z}$.*

Доказательство. Принимая во внимание лемму 2.2.2, нужно показать как построить по формуле вида

$$\exists x \left(\bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y}), g_i(\overline{y}) + c_i x) = d_i \wedge \bigwedge_{i\in[m+1..l]} f_i(\overline{y}) \neq c_i x \right) \tag{2.3}$$

эквивалентную ей в $\mathbb{Z}$ бесквантороную формулу $\psi(\overline{y})$. Здесь $f_i(\overline{y})$ и $g_i(\overline{y})$ — линейные полиномы с целыми коэффициентами, и $c_i > 0$ для любого $i \in [1..m]$. Обозначим $\varphi(x, \overline{y})$ матрицу формулы (2.3). Как и в первой главе, выражения вида $\text{НОД}(f(\overline{z}),g(\overline{z})) = d$ будут в дальнейшем называться нод-выражениями.

Без потери общности можно считать, что все c_i равны 1, так как можно вычислить $C = \underset{i=1..l}{\text{НОК}}(c_i)$, умножить каждое выражение с индексом $i \in [1..l]$ на $\frac{C}{c_i}$, заменить все вхождения Cx на $\widetilde{x}$ и добавить нод-выражение $\text{НОД}(C,\widetilde{x}) = C$.

Теперь построим формулу $\psi_{GCD}(\overline{y})$ такую, что

$$\exists x \varphi(x,\overline{y}) \Leftrightarrow \bigvee_{i\in[1..m]} \left(f_i(\overline{y}) = 0 \wedge \bigvee_{s\in\{-1,1\}} \varphi(s \cdot d_i - g_i(\overline{y}),\overline{y}) \right) \vee \left(\bigwedge_{i\in[1..m]} f_i(\overline{y}) \neq 0 \wedge \psi_{GCD}(\overline{y}) \right).$$

Здесь мы рассмотрели отдельно случаи равенства нулю первых аргументов нод-выражений, когда значение x можно непосредственно вычислить. Чтобы получить L_σ-формулу, достаточно переписать линейные уравнения с помощью леммы 2.2.1.

В последнем случае заметим, что поскольку $\bigwedge\limits_{i\in[1..m]} f_i(\overline{y}) \neq 0$, то ввиду замечания 1.3.1, существование решения в подсистеме нод-выражений из $\varphi(\overline{y}, x)$ влечёт существование такого решения, которое одновременно удовлетворяет подсистеме дизуравнений $\bigwedge\limits_{i\in[m+1..l]} f_i(\overline{y}) \neq c_i x$.

Рассмотрим теперь систему $\bigwedge\limits_{i\in[1..m]} \text{НОД}(f_i(\overline{y}), g_i(\overline{y}) + x) = d_i$ с ненулевыми первыми аргументами в каждом нод-выражении и покажем, что тот факт, что эта система имеет решение в $\mathbb{Z}$, может быть записан некоторой бесквантворной L_σ-формулой.

Рассмотрим последовательно условия из леммы 2.3.1. Выражения из (i) переписываются с помощью $\text{НОД}(d_i,f_i(\overline{y})) = d_i$ для всех $i \in [1..m]$. Для условия (ii) введём обозначение $D_{i,j} = \text{НОД}(d_i,d_j)$ и воспользуемся аналогичной формулой:

$$\text{НОД}(D_{i,j},g_i(\overline{y}) - g_j(\overline{y})) = D_{i,j}$$

для каждой пары индексов $i,j \in [1..m]$.

Условие (iii) есть конъюнкция по всем парам индексов $i, j \in [1..m]$ делимостей вида

$$\text{НОД}\left(\text{НОД}\left(f_i(\overline{y}), d_j\right), g_i(\overline{y}) - g_j(\overline{y})\right) \mid d_i.$$

Ясно, что эта формула эквивалентна дизъюнкции

$$\bigvee_{a|d_j} \left(\text{НОД}(f_i(\overline{y}), d_j) = a \wedge \bigvee_{d|d_i} \text{НОД}(a,g_i(\overline{y}) - g_j(\overline{y})) = d \right).$$

Переписывая условие (iv) более формально, получим выражение следующего вида:

$$\bigwedge_{p\in\mathbb{P}\wedge p\leqslant m} \left(\bigwedge_{I\subseteq J_p\wedge|I|=p} \left(\bigvee_{i\in I} v_p(f_i(\overline{y})) \leqslant M_p \right.\right.$$
$$\left.\left. \vee \bigvee_{i,j\in I\wedge i\neq j} \text{НОД}(p^{M_p+1}, g_i(\overline{y}) - g_j(\overline{y})) = p^{M_p+1} \right) \right). \qquad (2.4)$$

Здесь в каждом дизъюнкте из (2.4) записано, что либо соответствующее множество индексов I не является подмножеством I_p, либо существуют такие $i,j \in I \wedge i \neq j$, что $v_p(g_i(\overline{y}) - g_j(\overline{y})) > M_p$. Ввиду условия (i), $\text{НОД}(d_i,f_i(\overline{y})) = d_i$ для каждого индекса $i \in [1..m]$, поэтому вместо $v_p(f_i(\overline{y})) \leqslant M_p$ достаточно потребовать $v_p(f_i(\overline{y})) = M_p$. Это равенство может быть выражено формулой $\text{НОД}(p^{M_p+1},f_i(\overline{y}))= p^{M_p}$.

Таким образом, мы построили формулу $\psi_{GCD}(\overline{y})$ и, следовательно, искомую формулу $\psi(\overline{y})$. □

Предложенный алгоритм по существу является алгоритмом квазиэлиминации кванторов для случая пустого сорта переменных S_2 и совпадения языка алгоритма квази-ЭК и множества формул элиминационного вида. Языком такого алгоритма является множество позитивных бесквантворных L_σ-формул. Теперь объединим теорему 4 и лемму 2.2.1 и получим описание всех отношений, Р∃-выразимых в $\langle\mathbb{Z}; 1, + , \perp\rangle$.

Теорема 5. *Всякое отношение является позитивно экзистенциально выразимым в структуре* $\langle \mathbb{Z}; 1, +, \perp \rangle$ *тогда и только тогда, когда оно позитивно бескванторно выразимо в структуре* $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \text{НОД}_4, ... \rangle$.

Продемонстрируем алгоритм элиминации кванторов из теоремы 4 на следующем примере. В итоговой бескванторной формуле удобно использовать отношения равенства, которое по лемме 2.2.1 является бескванторно выразимым в структуре $\langle \mathbb{Z}; 1, +, -, \perp \rangle$.

Пример 2.3.1. *Рассмотрим формулу*

$$\exists x \, (2x + y \perp 3y + z \wedge x + 3z \perp 2x + 3 \wedge 5x + 3y \perp 2x + y + 2z + 1) \, . \tag{2.5}$$

Удобно дополнить наш алгоритм элиминации кванторов некоторыми упрощениями, аналогичными тем, которые применяются к формулам арифметики Пресбургера в пакете RedLog для системы компьютерной алгебры REDUCE [29]. В частности, формула, полученная в результате элиминации, будет удовлетворять следующим условиям:

(1) Всякое линейное уравнение имеет вид $l(\overline{x}) = 0$*, и наибольший общий делитель коэффициентов* $l(\overline{x})$ *равен единице.*

(2) Всякому линейному уравнению, не имеющему никаких целочисленных решений, сопоставляется значение false*. Например, применением функции* rlqe *к формуле* $\varphi := 2x + 1 = 0$ *получим* false*.*

(3) Всякое нод-выражение имеет вид $\text{НОД}(f(\overline{x}), g(\overline{x})) = d$*, где наибольший общий делитель всех коэффициентов из* $f(\overline{x})$ *и* $g(\overline{x})$ *равен единице. Таким образом, в случае, когда наибольший общий делитель коэффициентов линейных полиномов не делит* d*, этому нод-выражению сопоставляется значение* false*.*

(4) Всякому нод-выражению вида $\text{НОД}(1, g(\overline{x})) = d$ *или* $\text{НОД}(f(\overline{x}), 1) = d$ *сопоставляется значение* true *если* $d = 1$*, а иначе* false*.*

(5) Во всяком линейном выражении $l(\overline{x})$ *переменные из* $\overline{x}$ *отсортированы в лексикографическом порядке, и первый ненулевой коэффициент является положительным.*

Приведём (2.5) к виду (2.3), а затем сделаем преобразования из леммы 2.2.2:

$$\begin{aligned} \exists x \, (\, \text{НОД}(3y + z, y + 2x) = 1 \wedge \text{НОД}(-6z + 3, 3z + x) = 1 \\ \wedge \, \text{НОД}(y - 10z - 5, y - 4z - 2 + x) = 1 \,) \, . \end{aligned} \tag{2.6}$$

Теперь построим эквивалентную формулу с коэффициентом при элиминируемой переменной в линейных выражениях равным единице. Сразу заменим новую переменную на x*.*

$$\exists x \begin{cases} \text{НОД}(3y + z, & y+ & x) = 1 \\ \text{НОД}(12z - 6, & 6z+ & x) = 2 \\ \text{НОД}(2y - 20z - 10, & 2y - 8z - 4+ & x) = 2 \\ \text{НОД}(2, & & x) = 2 \end{cases} \tag{2.7}$$

Итоговую бесквантворную формулу удобно представить в виде комбинации трёх формул: $\varphi_1(y,z) \vee \varphi_2(y,z) \wedge \varphi_3(y,z)$. *Формула* $\varphi_1(y,z)$ *будет соответствовать случаю равенства нулю первого аргумента какого-либо нод-выражения из (2.7). Вторая и третья формулы описывают случай, когда никакой из первых аргументов нод-выражений не равен нулю, и для элиминации применяется НОД-лемма. Формула* $\varphi_2(y,z)$ *есть результат переписывания условий (i) – (iii), а условие (iv) записывается отдельно с помощью формулы* $\varphi_3(y,z)$.

Ввиду того, что уравнения $12z - 6 = 0$ *и* $2 = 0$ *не имеют целочисленных решений, в формуле* $\varphi_1(y,z)$ *следует рассмотреть только случаи* $3y + z = 0$ *и* $2y - 20z + 10 = 0$. *Заменой* x *либо на* $-y+1$, *либо на* $-y-1$ *в первом случае; и либо на* $-2y+8z+6$, *либо на* $-2y+8z+2$ *во втором случае, определим первую формулу:*

$$\begin{aligned}
\varphi_1(y,z) \rightleftharpoons 3y + z = 0 \wedge \Big(\big(&\text{НОД}(12z - 6, y - 6z - 1) = 2 \ \wedge \ \text{НОД}(2y - 20z - 10, y - 8z - 3) = 2 \\
&\wedge \ \text{НОД}(2, y - 1) = 2 \big) \vee \\
\vee \big(&\text{НОД}(12z - 6, y - 6z + 1) = 2 \ \wedge \ \text{НОД}(2y - 20z - 10, y - 8z - 5) = 2 \\
&\wedge \ \text{НОД}(2, y + 1) = 2 \big) \Big) \vee \\
\vee\, y - 10z - 5 = 0 \wedge \Big(\big(&\text{НОД}(3y + z, y - 8z - 6) = 1 \ \wedge \ \text{НОД}(6z - 3, y - 7z - 3) = 1 \\
\vee \big(&\text{НОД}(3y + z, y - 8z - 2) = 1 \ \wedge \ \text{НОД}(6z - 3, y - 7z - 1) = 1 \big) \Big).
\end{aligned}$$

Если же $3y + z \neq 0 \wedge y - 10z - 5 \neq 0$, *мы можем применить НОД-лемму. Так как (2.6) содержит лишь отношения взаимной простоты, формула (2.7) очевидно удовлетворяет условиям (i) и (ii). Таким образом, чтобы построить формулу* $\varphi_2(y,z)$, *необходимо переписать только (iii).*

$$\begin{aligned}
\varphi_2(y,z) \rightleftharpoons 3y + z \neq 0 \wedge y - 10z - 5 \neq 0 \wedge \big(&\text{НОД}(3y + z, 2) = 1 \vee \\
\vee\, &\text{НОД}(3y + z, 2) = 2 \ \wedge \ \text{НОД}(2, y - 6z) = 1 \big) \wedge \\
\big(&\text{НОД}(3y + z, 2) = 1 \vee \\
\vee\, &\text{НОД}(3y + z, 2) = 2 \ \wedge \ \text{НОД}(2, y - 8z - 4) = 1 \big) \wedge \\
\big(&\text{НОД}(3y + z, 2) = 1 \vee \\
\vee\, &\text{НОД}(3y + z, 2) = 2 \ \wedge \ \text{НОД}(2, y) = 1 \big).
\end{aligned}$$

Несложно увидеть, что (iii) всегда имеет место для второго и третьего, второго и четвёртого, третьего и четвёртого нод-выражений.

Осталось переписать условие (iv). В случае $p = 2$ *имеем* $M_2 = 1$, $J_2 = \{2,3,4\}$, *и множество* I_2 *может содержать лишь индексы* 2 *и* 3. *Если* $p = 3$, $M_3 = 0$, *и значит* $J_3 = \{1,2,3,4\}$, *а единственным возможным подмножеством* I_3 *из трёх элементов является* $I = \{1,2,3\}$. *Отсюда получаем следующую формулу:*

$$\begin{aligned}
\varphi_3(y,z) \rightleftharpoons \big(&\text{НОД}(2, 6z - 3) = 1 \ \vee \ \text{НОД}(2, y - 10z - 5) = 1 \ \vee \ \text{НОД}(2, y - 7z - 2) = 2 \big) \wedge \\
\big(&\text{НОД}(3, 3y + z) = 1 \ \vee \ \text{НОД}(3, 2y - 20z - 10) = 1 \vee \\
\vee\, &\text{НОД}(3, y - 6z) = 3 \ \vee \ \text{НОД}(3, 2y - 14z - 4) = 3 \ \vee \ \text{НОД}(3, y - 8z - 4) = 3 \big).
\end{aligned}$$

Таким образом заключаем, что (2.5) эквивалентна в целых числах бесквантворной формуле $\varphi_1(y,z) \vee \varphi_2(y,z) \wedge \varphi_3(y,z)$.

2.4 Следствия и близкие вопросы выразимости

Имея описание отношений, РЭ-выразимых с структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$, можно получить некоторые результаты о позитивной экзистенциальной невыразимости.

Если предположить, что отношение $x \not\perp y$ является РЭ-выразимым в $\langle \mathbb{Z}; 1, +, \perp \rangle$, то поскольку

$$\neg\text{НОД}(x,y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v \, (x = du \wedge y = dv \wedge u \not\perp v)$$

и $d \nmid x \Leftrightarrow \bigvee\limits_{k=1..d-1} d \mid x + k$, по теореме 5 отрицания отношений $x \perp y$ и $\text{НОД}(x,y) = d$ для всех $d \geqslant 2$ являются выразимыми в структуре $\langle \mathbb{Z}; 1, +, -, =, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \ldots \rangle$ некоторыми позитивными бесквантормыми формулами. Но в этом случае из теоремы 4 следует, что можно проэлиминировать все кванторы и таким образом доказать разрешимость $\text{Th}\langle \mathbb{Z}; 1, +, \perp \rangle$, что противоречит результату Д. Ришара о неразрешимости этой теории [67]. Отсюда получим первое следствие.

Следствие 5.1. *Отношение $x \not\perp y$ не является позитивно экзистенциально выразимым в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$.*

Не удивительно, что отношение порядка (или $x \geqslant 0$) также не является РЭ-выразимым в $\langle \mathbb{Z}; 1, +, \perp \rangle$. Можно доказать этот факт с помощью теоремы 5 аналогично тому, как мы доказывали бесквантормую невыразимость в разделе 2.2.

Действительно, если предположить, что некоторая бесквантормая формула $\varphi(x)$ выражает $x \geqslant 0$ в структуре $\langle \mathbb{Z}; 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \ldots \rangle$, тогда эта формула должна иметь вид

$$\bigwedge_{i \in [1..m]} \text{НОД}(a_i, b_i + cx) = d_i \wedge \bigwedge_{i \in [m+1..l]} a_i \neq cx. \tag{2.8}$$

для некоторых целых чисел a_i, b_i, d_i и положительного целого числа c. Из замечания 1.3.1 следует, что если подсистема всех нод-выражений из (2.8) имеет какое-либо решение cx, то существует бесконечно много отрицательных целых значений cx, также являющихся решениями. Таким образом, поскольку $\varphi(x)$ истинна для некоторого целого числа (а именно, для любого неотрицательного целого числа), то она истинна для бесконечного множества отрицательных целых чисел.

Следствие 5.2. *Отношение порядка $\leqslant$ не является позитивно экзистенциально выразимым в структуре $\langle \mathbb{Z}; 1, +, \perp \rangle$.*

Теперь рассмотрим вопросы РЭ-выразимости в некоторых близких структурах.

Для структуры $\langle \mathbb{N}; S, \perp \rangle$ видим, что отношение $x \neq 0$ является РЭ-выразимым формулой $\exists y \, (x \perp SSy)$, однако, по тем же причинам что и в утверждении 2.2.1, это отношение не является позитивно бесквантормо выразимым в $\langle \mathbb{N}; S, \perp \rangle$. Для этой структуры существует следующий аналог теоремы 5.

Утверждение 2.4.1. *Всякое отношение является позитивно экзистенциально выразимым в структуре* $\langle \mathbb{N}; S, \perp \rangle$ *тогда и только тогда, когда оно позитивно бескванторно выразимо в структуре* $\langle \mathbb{N}; S, \neq 0, \perp \rangle$.

Для доказательства этого утверждения достаточно использовать частный случай леммы 2.3.1, где все $d_i = 1$.

Лемма 2.4.1. *Рассмотрим систему* $\bigwedge\limits_{i\in[1..m]} a_i \perp b_i{+}x$, *где* $a_i, b_i \in \mathbb{N}$ *и* $a_i > 0$ *для всех* $i \in [1..m]$. *Определим множество индексов* $I_p = \{i \in [1..m] : p \mid a_i\}$. *Система имеет решение в* $\mathbb{Z}$ *тогда и только тогда, когда для каждого простого* $p \leqslant m$ *и всякого множества* $I \subseteq I_p$, *такого что* $|I| = p$, *существуют такие* $i,j \in I$, $i \neq j$, *что* $p \mid b_i - b_j$.

Доказательство утверждения 2.4.1. Можно предположить, что в атомарных формулах существуют термы вида $SS...S0$, так как $a \perp b + x \Leftrightarrow a + b + x \perp b + x$.

Рассмотрим формулу

$$\varphi(x, \overline{y}) \rightleftharpoons \bigwedge_{i\in[1..m]} f_i(\overline{y}) \perp b_i + x \wedge \bigwedge_{i\in[m+1..l]} a_i + x \neq 0, \tag{2.9}$$

где $f_i(\overline{y})$ являются выражениями вида либо $y_j + a$, либо a для некоторого $y_j \in \overline{y}$ и натурального числа a.

Заметим, что $f_i(\overline{y})$ в (2.9) могут быть равны нулю только если $x = 0$ или $x = 1$, так как иначе значения выражений $b_i + x$ будут равны как минимум 2 для любого $i \in [1..m]$. Ввиду замечания 1.3.1, в случае $\bigwedge\limits_{i\in[1..m]} f_i(\overline{y}) \neq 0$ можно исключить дизуравнения из системы (2.9).

Таким образом, применяя лемму 2.4.1, получим следующую эквивалентность в $\mathbb{N}$:

$$\exists x \varphi(x,\overline{y}) \Leftrightarrow \varphi(0,\overline{y}) \vee \varphi(S0,\overline{y}) \vee \bigwedge_{i\in[1..m]} f_i(\overline{y}) \neq 0 \wedge \psi(\overline{y})$$

для

$$\psi(\overline{y}) \rightleftharpoons \bigwedge_{p\in\mathbb{P}\wedge p\leqslant m} \left(\bigwedge_{System(p,I)} \left(\bigvee_{i\in I} p \perp f_i(\overline{y}) \right) \right),$$

где $System(p,I) \rightleftharpoons I \subseteq [1..m] \wedge |I| = p \wedge \bigwedge\limits_{i,j\in I\wedge i\neq j} p \nmid b_i - b_j$. Здесь для любого простого p условие $System(p,I)$ является истинным для таких множеств индексов I, что $\{b_i\}_{i\in I}$ является полной системой вычетов по модулю p. □

Пусть теперь $v_p(x)$ есть p-показатель рационального числа x (напомним, что $v_p(0) = \infty$). Определим делимость $x \mid y$ на рациональных числах как $\bigwedge\limits_{p\in\mathbb{P}} v_p(x) \leqslant v_p(y)$, и в таком случае $\text{НОД}(x,y) = \prod\limits_{p\in\mathbb{P}} p^{\min(v_p(x),v_p(y))}$. Здесь мы предполагаем, что $\text{НОД}(0,0) = 0$. Если определить $x \perp y \rightleftharpoons \text{НОД}(x,y) = 1$, тогда для пары рациональных чисел их взаимная простота означает, что они являются взаимно простыми целыми числами.

Для отношения делимости и НОД, определённых таким образом, можно доказать следующее обобщение леммы 2.3.1.

Лемма 2.4.2. *Лемма 2.3.1 остается верной, если заменить в её формулировке всюду* $\mathbb{Z}$ *на* $\mathbb{Q}$.

Доказательство. Рассмотрим систему (2.2), где $a_i, b_i, d_i \in \mathbb{Q}$ и $a_i \neq 0$, $d_i > 0$ для всех $i \in [1..m]$.

Умножим каждое нод-выражение $\text{НОД}(a_i, b_i + x) = d_i$ на общий знаменатель a_i, b_i, d_i (обозначим его c_i), чтобы получить систему с целыми параметрами и некоторыми целыми коэффициентами c_i при переменной x. Пусть $C = \operatorname{НОК}_{i\in[1..m]}(c_i)$, умножим каждое выражение с индексом $i \in [1..m]$ на $\frac{C}{c_i}$ и получим одинаковый коэффициент C при переменной x в каждом нод-выражении. Так как мы ищем решение $x \in \mathbb{Q}$, заменим Cx в каждом выражении на новую рациональную переменную $\widetilde{x}$.

Представим $\widetilde{x}$ в виде $\frac{y}{z}$ и умножим каждое выражение на $z \neq 0$. Таким образом получаем следующую систему

$$\bigwedge_{i\in[1..m]} \text{НОД}(a_iCz, b_iCz + y) = d_iCz. \tag{2.10}$$

По лемме 2.3.1 система (2.10) имеет решение $y \in \mathbb{Z}$ тогда и только тогда, когда условия (i) – (iv) выполняются для параметров a_iCz, b_iCz и d_iCz.

Для первых трёх условий можно вынести общий множитель $Cz \neq 0$ из каждого параметра и сократить на него. Переписывая (iv), заметим, что поскольку $Cz \neq 0$, его p-показатель является некоторым целым числом, и имеет место равенство $v_p(d_i) = v_p(d_iCz) - v_p(C) - v_p(z)$. Следовательно, для любого простого p множества индексов J_p и I_p будут такими же, и $v_p(b_iCz - b_jCz) > \max\limits_{i\in[1..m]} v_p(d_iCz)$ тогда и только тогда, когда $v_p(b_i - b_j) > \max\limits_{i\in[1..m]} v_p(d_i)$. □

Следствие 5.3. *Всякое отношение является позитивно экзистенциально выразимым в структуре* $\langle \mathbb{Q}; 1, +, -, \{c\cdot\}_{c\in\mathbb{Q}}, \perp \rangle$ *тогда и только тогда, когда оно позитивно бескванторно выразимо в структуре* $\langle \mathbb{Q}; 1, +, -, \neq, \{c\cdot\}_{c\in\mathbb{Q}}, \perp \rangle$.

Доказательство. Рассмотрим формулу вида (2.3), где коэффициенты линейных полиномов суть некоторые рациональные числа.

Так же, как и в лемме 2.4.2, добиваемся того, чтобы коэффициенты линейных полиномов стали целыми, а коэффициент при x равен C в каждом нод-выражении. Проэлиминируем экзистенциальный квантор таким же образом, как в теореме 4, применяя на этот раз лемму 2.4.2 вместо леммы 2.3.1. Из условий (i) и (ii) следует, что значения $f_i(\overline{y})$ и $(g_i(\overline{y}) - g_j(\overline{y}))$ должны быть целыми числами, следовательно, процесс переписывания (iii) и (iv) оказывается в точности тем же, что и в теореме 4.

Осталось заметить, что для всякого рационального числа d, выражение вида $\text{НОД}(x, y) = d$ переписывается с помощью формулы $\frac{x}{d} \perp \frac{y}{d}$. □

2.5 Три обобщения БЛ-теоремы

2.5.1 Разрешимость теории из замечания Виспфеннинга

Вероятно, более естественным определением целочисленной делимости над рациональными числами будет следующее: $x \in \mathbb{Q}$ делит $y \in \mathbb{Q}$ тогда и только тогда, когда существует некоторое число $z \in \mathbb{Z}$, что $y = zx$. В. Виспфеннином [84] были рассмотрены задачи смешанного вещественно-целочисленного линейного программирования с двумя различными отношениями делимости над вещественными числами. Первое из них есть обобщение определённого выше отношения целочисленной делимости на рациональных числах: $x \mid y \rightleftharpoons \exists z(z \in \mathbb{Z} \wedge y = zx)$, а второе отношение задавалось с помощью определения $x \parallel y \rightleftharpoons x \in \mathbb{Z} \wedge \exists z(z \in \mathbb{Z} \wedge y = zx)$. Далее им было показано, что элементарные теории структур $\langle \mathbb{R}; 0{,}1, +, -, [\,], =, <, \parallel \rangle$ и $\langle \mathbb{R}; 0{,}1, +, -, [\,], =, <, | \rangle$ неразрешимы, в то время как позитивная экзистенциальная теория первой структуры оказывается разрешимой. Напомним, что унарному функциональному символу $[\,]$ ставится в соответствие функция вычисления целой части вещественного числа, а график этой функции является бесквантворно выразимым в обеих структурах, например,

$$x = [y] \Leftrightarrow (x = y \vee x < y) \wedge y < x + 1 \wedge 1 \mid x. \tag{2.11}$$

Отметим, что результаты о неразрешимости были получены с помощью ДПРМ-теоремы, а БЛ-теорема послужила для доказательства разрешимости. Завершая доказательство, В. Виспфеннинг замечает: «We do not know whether a corresponding theorem holds in the analogous language L'_{div}», то есть, неизвестно, верно ли, что структура с отношением $\mid$ вместо $\parallel$ также обладает разрешимой позитивной экзистенциальной теорией.

Первым результатом этого раздела будет утвердительный ответ на вопрос Виспфеннинга. Заметим, что в полученном ниже результате мы также опускаем ограничение позитивности, то есть, доказываем разрешимость экзистенциальной теории структуры $\langle \mathbb{R}; 0{,}1, +, -, [\,], =, <, | \rangle$. Этот результат можно рассматривать как обобщение БЛ-теоремы. Идею предлагаемого ниже доказательства легко предугадать. Пусть L_{div} обозначает язык первого порядка сигнатуры $\langle 0{,}1, +, -, =, <, | \rangle$, а L'_{div} есть расширение L_{div} унарным функциональным символом для функции взятия целой части. Сначала покажем, что если носителем интерпретации является множество рациональных чисел $\mathbb{Q}$, то соответствующая проблема разрешимости сводится к целочисленному случаю, а поэтому является разрешимой ввиду БЛ-теоремы. Затем докажем, что всякая бесквантворная L_{div}-формула выполнима в вещественных числах тогда и только тогда, когда она выполнима в рациональных числах.

Лемма 2.5.1. *Позитивная экзистенциальная теория структуры* $\langle \mathbb{Q}; 0{,}1, +, -, =, <, | \rangle$ *разрешима.*

Доказательство. Как и в лемме 2.4.2, в данной бесквантормой формуле $\varphi(x_1,...,x_n)$ для всех $i \in [1..n]$ заменим переменную x_i на дробь $\frac{y_i}{z}$. Видим, что

$$\exists x_{1\in\mathbb{Q}}...\exists x_{n\in\mathbb{Q}}\varphi(x_1,...,x_n) \Leftrightarrow \exists y_{1\in\mathbb{Z}}...\exists y_{n\in\mathbb{Z}}\exists z_{\in\mathbb{Z}}\left(z>0\wedge\varphi(\frac{y_1}{z},...,\frac{y_n}{z})\right).$$

Атомарные формулы $\varphi(x_1,...,x_n)$ имеют один из следующих видов: $f(x_1,...,x_n)=c$, $f(x_1,...,x_n) < c$ или $f(x_1,...,x_n)+c \mid g(x_1,...,x_n)+d$, где $f(x_1,...,x_n)$ и $g(x_1,...,x_n)$ суть линейные формы с целочисленными коэффициентами, а c и d — некоторые целые числа. Умножением на z всякого линейного уравнения, неравенства и делимости из $\varphi(\frac{y_1}{z},...,\frac{y_n}{z})$ получим бесквантормую L_{div}-формулу $\varphi'(y_1,...,y_n,z)$ с атомарными формулами вида $f(y_1,...,y_n)=cz$, или $f(y_1,...,y_n)<cz$, или $f(y_1,...,y_n)+cz \mid g(y_1,...,y_n)+dz$. Таким образом, $\exists x_1...\exists x_n\varphi(x_1,...,x_n)$ истинна в рациональных числах тогда и только тогда, когда формула $\exists y_1...\exists y_n\exists z\,(z>0\wedge\varphi'(y_1,...,y_n,z))$ истинна в целых числах. Разрешимость теперь следует из БЛ-теоремы. □

Лемма 2.5.2. *Всякая позитивная бесквантормая L_{div}-формула выполнима в вещественных числах $\mathbb{R}$ тогда и только тогда, когда она выполнима в рациональных числах $\mathbb{Q}$.*

Доказательство. Пусть дана выполнимая в $\mathbb{R}$ формула

$$\varphi(\overline{x}) \rightleftharpoons \bigwedge_{i=1..k} g_i(\overline{x})=0 \wedge \bigwedge_{i=k+1..l} f_i(\overline{x}) \mid g_i(\overline{x}) \wedge \bigwedge_{i=l+1..m} g_i(\overline{x})<0,$$

где $\overline{x}$ — список переменных $x_1,...,x_n$; $g_i(\overline{x})$ для $i\in[1..m]$, $f_i(\overline{x})$ для $i\in[k+1..l]$ суть линейные полиномы с целыми коэффициентами. Покажем, что $\varphi(\overline{x})$ выполнима в рациональных числах.

Пусть $\alpha_1,...,\alpha_n$ является некоторым выполняющим набором. Предположим, что $g_i(\alpha_1,...,\alpha_n)=0$ для $i=k+1..k'$ и $g_i(\alpha_1,...,\alpha_n)\neq 0$ для всякого $i\in[k'+1..l]$. Тогда определим формулу

$$\varphi'(\overline{x}) \rightleftharpoons \bigwedge_{i=1..k'} g_i(\overline{x})=0 \wedge \bigwedge_{i=k'+1..l} f_i(\overline{x}) \mid g_i(\overline{x}) \wedge \bigwedge_{i=k'+1..l} \sigma_i\cdot g_i(\overline{x})<0 \wedge \bigwedge_{i=l+1..m} g_i(\overline{x})<0,$$

где $\sigma_i=1$, если $g_i(\alpha_1,...,\alpha_n)<0$, и $\sigma_i=-1$, если $g_i(\alpha_1,...,\alpha_n)>0$ для всех $i=k'+1..l$.

Рассмотрим систему линейных уравнений с целыми коэффициентами $\bigwedge\limits_{i=1..k'} g_i(\overline{x})=0$. Пусть $A\overline{y}+b$ есть пространство решений этой системы для некоторой рациональной матрицы A, рационального вектора b и новых переменных $\overline{y}=y_1,...,y_t$. Подстановкой $A\overline{y}+b$ вместо $\overline{x}$ получим равновыполнимую в вещественных числах систему линейных неравенств и делимостей с рациональными коэффициентами

$$\varphi''(\overline{y}) \rightleftharpoons \bigwedge_{i=k'+1..l} \widetilde{f}_i(\overline{y}) \mid \widetilde{g}_i(\overline{y}) \wedge \bigwedge_{i=k'+1..l} \sigma_i\cdot\widetilde{g}_i(\overline{y})<0 \wedge \bigwedge_{i=l+1..m} \widetilde{g}_i(\overline{y})<0,$$

такую, что по всякому рациональному решению $\varphi''(\overline{y})$ можно построить рациональное решение для $\varphi'(\overline{x})$, а значит, и для системы $\varphi(\overline{x})$. Кроме того, по построению $\varphi''(\overline{y})$ выполнима в $\mathbb{R}$.

Допустим $\beta_1,...,\beta_t$ является некоторым вещественным выполняющим набором для $\varphi''(\overline{y})$. Пусть вещественные числа $\{1,\gamma_1,...,\gamma_s\}$ для некоторого $s \leqslant t$ составляют базис линейного пространства над $\mathbb{Q}$, порождённого вещественными числами $\{1,\beta_1,...,\beta_t\}$. Всякое число β_i для $i = 1..t$ представимо единственным образом в виде $c_{i,0} \cdot 1 + c_{i,1} \cdot \gamma_1 + ... + c_{i,s} \cdot \gamma_s$, где все $c_{i,j} \in \mathbb{Q}$. Определим для всех $i = 1..t$ линейные полиномы $\chi_i(z_1,...,z_s) = c_{i,0} + c_{i,1}z_1 + ... + c_{i,s}z_s$ и заменим все y_i в $\varphi''(\overline{y})$ на $\chi_i(z_1,...,z_s)$. В результате получим следующую формулу:

$$\psi(\overline{z}) = \varphi''(\chi_1(\overline{z}),...,\chi_t(\overline{z})).$$

Таким образом, по всякому рациональному выполняющему набору для $\psi(\overline{z})$ можно построить рациональный выполняющий набор для $\varphi''(\overline{y})$, и, кроме того, имеет место $\psi(\gamma_1,...,\gamma_s)$ ввиду того, что $\psi(\gamma_1,...,\gamma_s) = \varphi''(\beta_1,...,\beta_t)$.

Перепишем $\psi(\overline{z})$ в виде

$$\bigwedge_{i=1..l'} \widetilde{\widetilde{f}}_i(\overline{z}) \mid \widetilde{\widetilde{g}}_i(\overline{z}) \wedge \bigwedge_{i=1..m'} \widetilde{\widetilde{g}}_i(\overline{z}) < 0,$$

где $l' \leqslant m'$ и рассмотрим отдельно каждую делимость этой системы $\widetilde{\widetilde{f}}(\overline{z}) \mid \widetilde{\widetilde{g}}(\overline{z})$. Здесь $\widetilde{\widetilde{f}}(\overline{z}) = a_0 + a_1z_1 + ... + a_sz_s$ и $\widetilde{\widetilde{g}}(\overline{z}) = b_0 + b_1z_1 + ... + b_sz_s$ — линейные полиномы с рациональными коэффициентами, причём $\widetilde{\widetilde{g}}(\overline{z})$ не равен тождественно нулю. Покажем, что в действительности $\widetilde{\widetilde{g}}(\overline{z})$ делится нацело на $\widetilde{\widetilde{f}}(\overline{z})$, и таким образом делимость имеет место для любых значений переменных $\overline{z}$.

Допустим, что $w \cdot f(\gamma_1,...,\gamma_s) = g(\gamma_1,...,\gamma_s)$ для некоторого целого числа w. Из соображений удобства будем считать, что $\gamma_0 = 1$. Если предположить, что $w \cdot a_i\gamma_i \neq b_i\gamma_i$ для некоторого $i \in [0..s]$, то имеет место равенство $\gamma_i(w \cdot a_i - b_i) = \sum\limits_{j=0..s \wedge j \neq i} \gamma_j(b_j - w \cdot a_j)$. Однако это невозможно ввиду того, что $1,\gamma_1,...,\gamma_s$ линейно независимы над $\mathbb{Q}$.

Таким образом, каждое решение подсистемы линейных неравенств с рациональными коэффициентами $\bigwedge\limits_{i=1..m'} \widetilde{\widetilde{g}}_i(\overline{z}) < 0$ также является выполняющим набором для $\psi(\overline{z})$. Так как эта подсистема имеет вещественное решение $\gamma_1,...,\gamma_s$, то найдётся некоторое рациональное решение $q_1,...,q_s$. Наконец, $\chi_1(q_1,...,q_s),...,\chi_t(q_1,...,q_s)$ есть рациональный выполняющий набор для $\varphi''(\overline{y})$, и поэтому формула $\varphi(\overline{x})$ выполнима в $\mathbb{Q}$. □

Теорема 6. *Экзистенциальная теория структуры* $\langle \mathbb{R}; 0,1, +, -, [\,], =, <, | \rangle$ *разрешима.*

Доказательство. Воспользуемся (2.11) для преобразования данной $\exists L'_{div}$-формулы в эквивалентную в вещественных числах $\exists L_{div}$-формулу. Далее, отношение неделимости позитивно экзистенциально выразимо с помощью формулы

$$x \nmid y \Leftrightarrow (x = 0 \wedge (y < 0 \vee 0 < y)) \vee \exists z\,(0 < z \wedge (z < x \vee z < -x) \wedge x \mid y + z)\,.$$

Искомый результат теперь следует из лемм 2.5.1 и 2.5.2. □

2.5.2 Два разрешимых фрагмента ∀∃-теории

Обозначим язык арифметики Пресбургера L_{PA}, который является языком первого порядка сигнатуры $\langle 1, +, -, \leqslant, 2\mid, 3\mid, 4\mid, ...\rangle$. Заменяя все унарные предикатные символы для отношений делимости на константы на единственный бинарный предикатный символ для отношения делимости, получаем язык L_{PAD}. Известно, что $\exists\forall\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leqslant, |\rangle$ неразрешима. В этом разделе будут определены два семейства замкнутых $\forall\exists L_{PAD}$-формул, а затем будет доказана разрешимость соответствующих им фрагментов $\exists\forall$-теории.

Первый результат будет обобщением теоремы Г.А. Переса и Р. Рахи [61]. В указанном препринте они показывают, что один фрагмент $\exists\forall\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leqslant, |\rangle$, который был определён М. Божгой и Р. Иосифом [15], в действительности оказывается неразрешимым. Затем было доказано, что наложением определённых ограничений на вид формул можно получить уже разрешимый фрагмент. Именно, разрешимой оказывается проблема проверки истинности в целых числах формул вида

$$\forall\overline{x}\,\exists\overline{y}\bigvee_{j\in J}\Big(\overline{y}\geqslant 0\wedge\varphi_j(\overline{x})\wedge\bigwedge_{i\in[1..m_j]}(\text{НОД}(f_i(\overline{x}),g_i(\overline{x},\overline{y}))=f_i(\overline{x})\wedge f_i(\overline{x})>0)\Big), \tag{2.12}$$

где $f_i(\overline{x})$, $g_i(\overline{x},\overline{y})$ — линейные полиномы с целыми коэффициентами, а $\varphi_j(\overline{x})$ — некоторые бескванторные L_{PAD}-формулы.

В этом случае можно легко отделить каждую из переменных, находящихся под квантором существования, в то время как в общем случае (см. Шаг 1 алгоритма $\mathcal{R}$ в разделе 1.4) для этого применялась ЛС-лемма. Кроме того, подсистема нод-выражений из (2.12) уже допускает применение китайской теоремы об остатках, так как каждый делитель является положительным целым числом. Если использовать НОД-лемму вместо китайской теоремы об остатках, можно усилить это утверждение.

Определим семейство формул, где в каждом нод-выражении полином в правой части может отличаться от первого аргумента НОД:

$$\forall\overline{x}\,\exists\overline{y}\bigvee_{j\in J}\Big(\overline{y}\geqslant 0\wedge\varphi_j(\overline{x})\wedge\bigwedge_{i\in[1..m_j]}(\text{НОД}(f_i(\overline{x}),g_i(\overline{x},\overline{y}))=h_i(\overline{x})\wedge f_i(\overline{x})>0\wedge h_i(\overline{x})>0)\Big). \tag{2.13}$$

Здесь $h_i(\overline{x})$ также являются некоторыми линейными полиномами с целыми коэффициентами. Для определённого таким образом семейства имеет место следующая теорема.

Теорема 7. *Задача проверки истинности в целых числах формул вида (2.13) разрешима.*

Перед тем как перейти к доказательству теоремы, удобно будет несколько переформулировать НОД-лемму. Определим условие

((iii)) $\displaystyle\bigwedge_{1\leqslant i<j\leqslant m}\text{НОД}(a_i,d_j,b_i-b_j)=\text{НОД}(a_j,d_i,b_i-b_j)=\text{НОД}(d_i,d_j)$

и докажем следующую вспомогательную лемму.

Лемма 2.5.3. *Пусть имеется система вида (2.2), где a_i, b_i, d_i те же, что и в лемме 2.3.1. Предположим, что выполнено условие (i), тогда условия (ii) и (iii) одновременно имеют место тогда и только тогда, когда выполнено ((iii)).*

Доказательство. Условие (ii) очевидным образом следует из ((iii)). Условие (iii) имеет вид системы, состоящей из следующих пар делимостей:

$$\text{НОД}(a_i,d_j,b_i-b_j) \mid d_i \wedge \text{НОД}(a_j,d_i,b_i-b_j) \mid d_j$$

для всяких $1 \leqslant i < j \leqslant m$. Видим, что эти делимости также имеют место ввиду ((iii)).

Обратно, рассмотрим цепочку равенств:

$$\begin{aligned}\text{НОД}(a_i,d_j,b_i-b_j) &= \text{НОД}\,(d_i,\text{НОД}(a_i,d_j,b_i-b_j)) \\ &= \text{НОД}\,(\text{НОД}(d_i,a_i),\text{НОД}(d_j,b_i-b_j)) = \text{НОД}\,(d_i,d_j)\,.\end{aligned}$$

Первое равенство есть в точности условие (iii), а последнее равенство непосредственно следует из (i) и (ii). На этом доказательство леммы окончено. □

Замечание 2.5.1. *Если допустить в условии ((iii)) возможность $i = j$, то получим НОД(d_i,a_i) = НОД(d_i,d_i), то есть, $d_i \mid a_i$. Поэтому в условии НОД-леммы можно заменить пару условий (i) и (iii) на ((iii)) с дополнительной возможностью равенства индексов i и j. Однако такого рода переформулировка может казаться несколько запутанной ввиду того, что она скрывает явно ожидаемое условие (i).*

Доказательство теоремы 7. Наша цель — построить по всякой формуле вида (2.13) эквивалентную в целых числах универсальную L_{PAD}-формулу. Затем, ввиду того, что $\exists\text{Th}\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ разрешима тогда и только тогда, когда универсальная теория соответствующей структуры разрешима, искомый алгоритм получается из БЛ-теоремы.

Для упрощения построения введём в сигнатуру бинарный функциональный символ для функции НОД и для каждого простого числа p унарный функциональный символ для функции V_p из p-арифметики Бюхи. Мы предполагаем, что НОД$(0,0) = 0$ и $V_p(0) = 0$.

Из определений (2) следует, что отношение НОД$(x,y) = z$ и его отрицание выразимы в структуре $\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ универсальными формулами. Функциональные символы V_p в итоговой $\forall L_{PAD}$-формуле будут входить в атомарные формулы вида либо $V_p(t_1(\overline{x})) \mid t_2(\overline{x})$, либо $V_p(t_1(\overline{x})) = V_p(t_2(\overline{x}))$, где $t_1(\overline{x})$ и $t_2(\overline{x})$ суть некоторые термы, построенные с помощью переменных из $\overline{x}$, единицы, сложения, вычитания и НОД. В таком случае V_p могут быть исключены из формулы при помощи, во-первых

$$V_p(x) \mid y \Leftrightarrow V_p(\text{НОД}(x,y)) = V_p(x), \tag{2.14}$$

а во-вторых, следующего определения

$$V_p(x) = V_p(y) \Leftrightarrow \text{НОД}(x,py) = \text{НОД}(x,y) \wedge \text{НОД}(px,y) = \text{НОД}(x,y). \tag{2.15}$$

Пусть X и Y — два непересекающихся множества переменных, и пусть $L^Y_{(2.16)}$ есть множество бесквантворных формул $\bigvee\limits_{j\in J}\psi_j(\overline{x},\overline{y})$ для конечных множеств индексов J и формул $\psi_j(\overline{x},\overline{y})$ вида

$$\overline{y} \geqslant 0 \wedge \varphi_j(\overline{x}) \wedge \bigwedge_{k\in[1..m_j]} f_k(\overline{x}) > 0 \wedge h_k(\overline{x}) > 0 \wedge \bigwedge_{i\in[1..l_j]} \text{НОД}(F_i(\overline{x}), g_i(\overline{x},\overline{y})) = H_i(\overline{x}), \tag{2.16}$$

где $\overline{x}$ есть конечное множество переменных из X; $\overline{y}$ — конечное множество переменных из Y; $f_k(\overline{x})$, $h_k(\overline{x})$ для $k \in [1..m_j]$ и $g_i(\overline{x},\overline{y})$ для $i \in [1..l_j]$ суть линейные полиномы с целыми коэффициентами. Выражения $F_i(\overline{x})$ и $H_i(\overline{x})$ построены с помощью только $f_1(\overline{x})$, $h_1(\overline{x})$,...,$f_{m_j}(\overline{x})$, $h_{m_j}(\overline{x})$ и функциональных символов НОД и V_p для простых чисел p, причём имеет место следующее ограничение: для всякого $i \in [1..l_j]$ в случае, если функциональный символ V_p входит в $F_i(\overline{x})$ то он входит и в $H_i(\overline{x})$. Наконец, всякая формула $\varphi_j(\overline{x})$ имеет вид

$$\widetilde{\varphi_j}(\overline{x}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} V_{p_i}\left(t_{i,1}(\overline{x})\right) \mid t_{i,2}(\overline{x}) \wedge \bigwedge_{i\in[1..\widetilde{\widetilde{m}}_j]} V_{q_i}\left(\widetilde{t}_{i,1}(\overline{x})\right) = V_{q_i}\left(\widetilde{t}_{i,2}(\overline{x})\right), \tag{2.17}$$

где $\widetilde{\varphi_j}(\overline{x})$ есть некоторая бесквантороная $L_{\langle 1,+,-,\text{НОД},\leqslant,|\rangle}$-формула и $t_{i,1}(\overline{x})$, $t_{i,2}(\overline{x})$, $\widetilde{t}_{i,1}(\overline{x})$, $\widetilde{t}_{i,2}(\overline{x})$ — некоторые термы этого же языка.

Следующая лемма завершит доказательство теоремы. □

Лемма 2.5.4. *Пусть X и Y — два непересекающихся множества переменных, список переменных $\overline{x}$ содержится в X, а список $(\overline{y},z)$ содержится в Y. Тогда для всякой формулы вида $\exists z\psi(\overline{x},\overline{y},z)$, где $\psi(\overline{x},\overline{y},z)$ есть некоторая $L^Y_{(2.16)}$-формула, можно построить $L^Y_{(2.16)}$-формулу $\theta(\overline{x},\overline{y})$, которая будет эквивалентна в $\mathbb{Z}$ формуле $\exists z\psi(\overline{x},\overline{y},z)$.*

Доказательство. Так же, как и на Шаге 2 алгоритма $\mathcal{R}$ из раздела 1.5, и в теореме 4, можно считать, что коэффициенты при элиминируемой переменной z в каждом выражении равны единице. В каждом конъюнкте $\psi(\overline{x},\overline{y},z)$ подсистема, составленная из только тех атомарных формул, в которые входит переменная z, теперь имеет вид

$$z \geqslant 0 \wedge \bigwedge_{i\in[1..l]} \text{НОД}(F_i(\overline{x}), g_i(\overline{x},\overline{y}) + z) = H_i(\overline{x}). \tag{2.18}$$

По определению языка $L^Y_{(2.16)}$, выражения $F_i(\overline{x})$ и $H_i(\overline{x})$ могут принимать только положительные значения. Поэтому теперь мы можем применить НОД-лемму для того, чтобы переписать тот факт, что существует целое число z, являющееся решением системы (2.18). Из замечания 1.3.1 следует, что если существует какое-либо решение z, то существует бесконечно много положительных решений системы (2.18), и поэтому неравенство $z \geqslant 0$ можно исключить. Рассмотрим отдельно каждое условие НОД-леммы, причём два условия (ii) и (iii) мы заменим на одно условие ((iii)). Эта замена корректна ввиду леммы 2.5.3.

Условия (i) и ((iii)) переписать совсем несложно. Для (i) получим конъюнкцию делимостей

$$\bigwedge_{i\in[1..l]} H_i(\overline{x}) \mid F_i(\overline{x}), \tag{2.19}$$

а условие ((iii)) есть в точности формула

$$\bigwedge_{1\leqslant i<j\leqslant l} \Big(\text{НОД}(\text{НОД}(F_i(\overline{x}),H_j(\overline{x})), g_i(\overline{x},\overline{y}) - g_j(\overline{x},\overline{y})) = \text{НОД}(H_i(\overline{x}),H_j(\overline{x}))\wedge$$
$$\text{НОД}(\text{НОД}(F_j(\overline{x}),H_i(\overline{x})), g_i(\overline{x},\overline{y}) - g_j(\overline{x},\overline{y})) = \text{НОД}(H_i(\overline{x}),H_j(\overline{x}))\Big). \tag{2.20}$$

Условие (iv) будем переписывать аналогично тому, как это было сделано на Шаге 2 алгоритма квазиэлиминации кванторов $\mathcal{R}$ из раздела 1.5. Единственное отличие состоит в

том, что вместо уравнений и неравенств с p-показателями будут использоваться уравнения и делимости с функциями V_p. Именно, в нашем случае получаем следующую конъюнкцию:

$$\bigwedge_{p\leqslant l\wedge p\in\mathbb{P}}\left(\bigwedge_{I\subseteq[1..l]\wedge|I|=p}\Omega_{p,I}(\overline{x},\overline{y})\right), \tag{2.21}$$

где $\mathbb{P}$ есть множество простых чисел и

$$\Omega_{p,I}(\overline{x},\overline{y})\rightleftharpoons\bigvee_{i\in I\wedge j\in[1..l]}V_p(pH_i(\overline{x}))\mid H_j(\overline{x})\vee\bigvee_{i\in I}V_p(H_i(\overline{x}))=V_p(F_i(\overline{x}))$$
$$\vee\bigvee_{i,j\in I\wedge i\neq j}V_p(H_i(\overline{x}))\mid g_i(\overline{x},\overline{y})-g_j(\overline{x},\overline{y}). \tag{2.22}$$

Отметим, что всякая делимость в (2.22) с переменными из $\overline{y}$ может быть переписана очевидным образом в виде

$$\text{НОД}(V_p(H_i(\overline{x})),g_i(\overline{x},\overline{y})-g_j(\overline{x},\overline{y}))=V_p(H_i(\overline{x})).$$

Чтобы построить формулу $\theta(\overline{x},\overline{y})$, в каждом конъюнкте $\psi(\overline{x},\overline{y},z)$ заменим подсистему вида (2.18) на соответствующую ей конъюнкцию (2.19)$\wedge$(2.20)$\wedge$(2.21). Применением закона дистрибутивности приведём формулу к ДНФ. Осталось показать, что во всяком конъюнкте подсистемы, составленные из атомарных формул, не содержащих переменных из $\overline{y}$, можно переписать в виде (2.17). Для приведения атомарных формул к требуемому виду достаточно несколько раз воспользоваться равенствами $\text{НОД}(V_p(x),y)=V_p(\text{НОД}(x,y))$ и $\text{НОД}(V_p(x),V_q(y))=1$. □

Второй разрешимый фрагмент $\forall\exists$-теории структуры $\langle\mathbb{Z};1,+,-,\leqslant,|\rangle$ получается в качестве прямого следствия теоремы 4. Именно, рассмотрим формулы следующего вида:

$$\forall\,\overline{x}\,\exists\,\overline{y}\bigvee_{j\in J}\Big(\varphi_j(\overline{x})\wedge\bigwedge_{i\in[1..m_j]}\text{НОД}(f_i(\overline{x},\overline{y}),g_i(\overline{x},\overline{y}))=d_i\Big), \tag{2.23}$$

где $f_i(\overline{x},\overline{y})$, $g_i(\overline{x},\overline{y})$ суть некоторые линейные полиномы с целыми коэффициентами, а $\varphi_j(\overline{x})$ — некоторые бескванторные L_{PAD}-формулы. Из определений (2) следует, что это действительно некоторые $\forall\exists L_{PAD}$-формулы. Здесь уже нет никаких ограничений на полиномы в левой части нод-выражений с переменными из $\overline{y}$, однако полиномы в правых частях таких нод-выражений обязательно являются некоторыми положительными целыми числами. Кроме того, переменные из $\overline{y}$ не входят ни в какое линейное неравенство. Теорема 4 даёт нам следующий результат для таким образом определённого семейства формул.

Следствие 4.1. *Задача проверки истинности в целых числах формул вида (2.23) разрешима.*

Доказательство. Применим теорему 4 для элиминации всех экзистенциальных кванторов. Затем перепишем дизуравнения с помощью отношения порядка для получения универсальной формулы языка первого порядка сигнатуры $\langle 1,+,-,\text{НОД},\leqslant,|\rangle$. Снова воспользуемся определением (2) для исключения НОД из формулы, а затем применим БЛ-теорему, чтобы получить искомый алгоритм. □

2.6 Алгоритм квази-ЭК для экзистенциальной арифметики натуральных чисел с единицей, сложением и взаимной простотой

Не известно, можно ли обобщить теорему предыдущего параграфа и допустить использование линейных неравенств $f(\overline{x},\overline{y}) \geqslant 0$ в (2.23). Тем не менее, выглядит естественным рассмотреть проблему совместности в целых числах систем вида

$$\varphi_+(\overline{z}) \rightleftharpoons A\overline{z} = B \wedge C\overline{z} \geqslant D \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{z}),g_i(\overline{z})) = d_i, \tag{2.24}$$

где A и C — целочисленные матрицы, а B, D — целочисленные векторы.

Ввиду следствия 5.1, отрицание отношения взаимной простоты не является РЭ-выразимым в структуре $\langle\mathbb{Z};1,+,-,\perp\rangle$, однако остаётся неизвестным, будет ли оно РЭ-выразимым в структуре, расширенной отношением порядка. Чтобы распознавать произвольные формулы экзистенциальной арифметики Пресбургера с отношением взаимной простоты $\exists\text{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ (обозначим L_{PAC} соответствующий язык первого порядка), достаточно рассмотреть проблему выполнимости в $\mathbb{Z}$ формул вида

$$\begin{aligned}\varphi(\overline{z}) \rightleftharpoons \overline{\delta} \geqslant 2 \wedge A\overline{z} = B \wedge C\overline{z} \geqslant D \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{z}),g_i(\overline{z})) = d_i \\ \wedge \bigwedge_{i\in[m+1..l]} \text{НОД}(f_i(\overline{z}),g_i(\overline{z})) = d_i\delta_i.\end{aligned} \tag{2.25}$$

С помощью теоремы 4 построим квази-ЭК алгоритм для проверки истинности в целых числах замкнутых РЭL_{PAC}-формул. Этот алгоритм, который будет назван $\mathcal{C}^+$, оказывается значительно проще, чем комбинация алгоритмов $\mathcal{R}$ и $\mathcal{D}$ из первой главы для доказательства БЛ-теоремы. Далее, для произвольных $\exists L_{PAC}$-формул будет построен алгоритм квази-ЭК $\mathcal{C}$, который осуществит сведение проблемы разрешимости для $\exists\text{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ к проблеме разрешимости для одного фрагмента теории $\exists\text{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД},=\rangle$, где НОД есть двухместный функциональный символ для соответствующей функции. Для завершения доказательства разрешимости достаточно будет произвести несложную модификацию алгоритма квази-ЭК $\mathcal{D}$.

2.6.1 Позитивный случай

Ввиду леммы 1.2.2, построение разрешающей процедуры для позитивной экзистенциальной теории структуры $\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ сводится к проверке выполнимости в целых числах системы вида

$$\overline{y} \geqslant 0 \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y}),g_i(\overline{y})) = d_i. \tag{2.26}$$

Определим языки алгоритма квази-ЭК $\mathcal{C}^+$ для рассматриваемой структуры.

Сорт S_2 будет пустым, и язык $L_{\mathcal{C}^+}$ определён как множество бескванторных формул $\bigvee\limits_{j\in J_1}\varphi_j(\overline{y_j})$ для некоторого конечного множества индексов J_1 и формул $\varphi_j(\overline{y_j})$ вида (2.26). Множество формул элиминационного вида $L^x_{\mathcal{C}^+}$ для латинской переменной x есть множество $L_{\mathcal{C}^+}$-формул $\bigvee\limits_{j\in J_2}\widetilde{\varphi}_j(x,\overline{z_j})$ для конечного множества индексов J_2 и формул $\widetilde{\varphi}_j(x,\overline{z})$ следующего вида:

$$\overline{z}\geqslant 0\wedge x\geqslant 0\wedge\widetilde{\widetilde{\varphi}}(\overline{z})\wedge\bigwedge_{i\in[1..\widetilde{m}]}\text{НОД}(\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z})+c_ix)=\widetilde{d}_i, \tag{2.27}$$

где x не входит в список переменных $\overline{z}$, $c_i>0$; каждый $\widetilde{f}_i(\overline{z})$ является линейным полиномом с неотрицательными целыми коэффициентами и положительными свободными членами, а формула $\widetilde{\widetilde{\varphi}}(\overline{z})$ есть система нод-выражений.

Шаг 1 алгоритма $\mathcal{C}^+$ оказывается значительно проще шага 1 алгоритма $\mathcal{R}$ из раздела 1.4 по той причине, что полиномы в правых частях нод-выражений всегда являются некоторыми положительными константами. Кроме того, в формулах отсутствуют греческие переменные. Как будет показано ниже, их введение потребуется для записи отрицания отношения взаимной простоты в алгоритме $\mathcal{C}$. Сформулируем преобразования, выполняемые на этом шаге, в виде леммы.

Лемма 2.6.1. *Существует алгоритм, который по всякой $L_{\mathcal{C}^+}$-формуле $\varphi(\overline{z})$ строит равновыполнимую в целых числах дизъюнкцию $\bigvee\limits_{j\in J}\varphi_j(\overline{z_j})$ для конечного множества индексов J, так что для каждого $j\in J$ список переменных $\overline{z_j}$ содержит меньшее либо равное число переменных, чем $\overline{z}$, и $\varphi_j(\overline{z_j})$ является $L^{x_j}_{\mathcal{C}^+}$-формулой для некоторой переменной $x_j\in\overline{z_j}$.*

Доказательство. В доказательстве мы снова воспользуемся ЛС-леммой из раздела 1.2.1. В терминах раздела 1.2.1 будем также говорить, что некоторая дизъюнкция получена *«применением ЛС-леммы к формуле $\varphi(\overline{z})$»*, если в подсистему $S(\overline{s})$ вошли все линейные уравнения и неравенства из $\varphi(\overline{z})$.

Можно считать, что к каждому дизъюнкту данной $L_{\mathcal{C}^+}$-формулы была применена лемма 2.2.2, и в результате получена дизъюнкция формул вида (2.27). Для этой формулы построим равновыполнимую в целых числах формулу $\widetilde{\Phi}_1(\overline{z_1})\vee\widetilde{\Phi}_2(x,\overline{z_2})$, такую что $\widetilde{\Phi}_1(\overline{z_1})$ есть дизъюнкция формул вида (2.27) с меньшим числом переменных, а $\widetilde{\Phi}_2(x,\overline{z_2})$ является дизъюнкцией $L^x_{\mathcal{C}^+}$-формул. Повторяя этот процесс с первым дизъюнктом пока его список переменных не станет пустым, построим искомую дизъюнкцию.

Формула $\widetilde{\Phi}_1(\overline{z_1})$ получается в результате разбора случаев, для которых $\widetilde{f}_i(\overline{z})=0$. Обозначим конъюнкцию $\overline{z}\geqslant 0\wedge x\geqslant 0\wedge\widetilde{\widetilde{\varphi}}(\overline{z})$ с помощью $\Phi(x,\overline{z})$, тогда $\widetilde{\Phi}_1(\overline{z_1})$ есть результат применения ЛС-леммы к каждой системе следующей дизъюнкции:

$$\bigvee_{j\in[1..\widetilde{m}]}\bigvee_{\sigma\in\{-1,1\}}\Bigg(\Phi(x,\overline{z})\wedge\widetilde{f}_j(\overline{z})=0\wedge\widetilde{g}_j(\overline{z})+c_jx=\sigma\widetilde{d}_j$$
$$\wedge\bigwedge_{i\in[1..\widetilde{m}]\wedge i\neq j}\text{НОД}(\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z})+c_ix)=\widetilde{d}_i\Bigg).$$

Другой случай, когда первые аргументы нод-выражений ненулевые, будет описан формулой $\widetilde{\Phi}_2(x,\overline{z_2})$. Рассмотрим следующую дизъюнкцию:

$$\bigvee_{\overline{\sigma}\in\{-1,1\}^{\widetilde{m}}}\left(\Phi(x,\overline{z})\wedge\bigwedge_{i\in[1..\widetilde{m}]}\left(\sigma_i\widetilde{f}_i(\overline{z})\geqslant 1\wedge \text{НОД}(\sigma_i\widetilde{f}_i(\overline{z}),\widetilde{g}_i(\overline{z})+c_ix)=\widetilde{d}_i\right)\right). \tag{2.28}$$

Применением ЛС-леммы к подсистемам, содержащим все линейные уравнения и неравенства с переменными из $\overline{z}$ каждого дизъюнкта (2.28), получим дизъюнкцию $L^x_{\mathcal{C}^+}$-формул. Это завершает построение $\widetilde{\Phi}_2(x,\overline{z_2})$ и доказательство леммы. □

Теперь всё готово для доказательства следующего утверждения.

Утверждение 2.6.1. *Позитивная экзистенциальная теория структуры* $\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ *разрешима.*

Доказательство. Достаточно определить Шаг 2 алгоритма квази-ЭК $\mathcal{C}^+$. Пусть имеется $L^x_{\mathcal{C}^+}$-формула $\bigvee\limits_{j\in J}\varphi_j(x,\overline{z_j})$ для некоторого конечного множества индексов J и $L^x_{\mathcal{C}^+}$-формул $\varphi_j(x,\overline{z_j})$. На шаге 2 для каждого $j\in J$ к формулам $\exists x\varphi_j(x,\overline{z_j})$ применяется лемма 2.3.1 таким же образом, как и в доказательстве теоремы 4. Здесь, однако, не рассматриваются случаи равенства нулю первых аргументов нод-выражений, так как по определению языка $L^x_{\mathcal{C}^+}$ они могут принимать лишь положительные значения. Как и прежде, замечание 1.3.1 позволяет опустить ограничение неотрицательности на элиминируемую переменную.

Таким образом строим эквивалентную в целых числах дизъюнкцию $\bigvee\limits_{j\in J}\psi_j(\overline{z_j})$, где $\psi_j(\overline{z_j})$ суть некоторые $L_{\mathcal{C}^+}$-формулы. На этом завершается описание алгоритма $\mathcal{C}^+$, и мы получаем искомую разрешающую процедуру. □

Само по себе это утверждение не является новым, оно следует из БЛ-теоремы. Однако автору не известно каких-либо явных изложений алгоритма для $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$, как и для случая, когда позитивность формул не требуется. Это обобщение рассматривается в следующем подразделе.

2.6.2 Обобщение на произвольные экзистенциальные формулы

Для проверки выполнимости в $\mathbb{Z}$ бескванторных L_{PAC}-формул достаточно уметь проверять совместность в целых числах систем (2.24), в которых также допустимы выражения вида $\text{НОД}(f(\overline{x}),g(\overline{x}))\neq 1$. Эту задачу мы сразу сведём к вопросу выполнимости в $\mathbb{Z}$ формул вида

$$\overline{\delta}\geqslant 2\wedge\overline{y}\geqslant 0\wedge\bigwedge_{i\in[1..m]}\text{НОД}(f_i(\overline{y}),g_i(\overline{y}))=d_i\wedge\bigwedge_{i\in[m+1..l]}\text{НОД}(f_i(\overline{y}),g_i(\overline{y}))=d_i\delta_i. \tag{2.29}$$

Зафиксируем это преобразование в виде леммы.

Лемма 2.6.2. *Проблема разрешимости для* $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ *сводится к проблеме совместности в* $\mathbb{Z}$ *систем вида (2.29).*

Доказательство. Пусть $\varpi(\overline{z}) \rightleftharpoons \varphi_+(\overline{z}) \wedge \bigwedge\limits_{i\in[m+1..k]} \text{НОД}(f_i(\overline{z}),g_i(\overline{z})) \neq 1$, где $\varphi_+(\overline{z})$ имеет вид (2.24). Каждое нод-выражение для индексов $i \in [m+1..l]$ истинно тогда и только тогда, когда для некоторого целого числа δ_i выполняется

$$(f_i(\overline{z}) = 0 \wedge g_i(\overline{z}) = 0) \vee (\delta_i \geqslant 2 \wedge \text{НОД}(f_i(\overline{z}),g_i(\overline{z})) = \delta_i)\,.$$

Таким образом преобразуем каждое выражение указанного вида и получим для формулы $\varpi(\overline{z})$ равновыполнимую в целых числах дизъюнкцию формул вида (2.25), в которых также могут быть линейные уравнения и неравенства от переменных $\overline{z}$. Чтобы получить желаемый результат, осталось применить ЛС-лемму к подсистемам каждого дизъюнкта, состоящим из всех линейных уравнений и неравенств от переменных $\overline{z}$. □

Теперь построим алгоритм квази-ЭК $\mathcal{C}$, который сводит проблему выполнимости в целых числах формул вида (2.29) к проблеме разрешимости для фрагмента экзистенциальной теории структуры $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД},=\rangle$, где НОД является бинарным функциональным символом. Разрешимость последней теории несложно установить с помощью алгоритма $\mathcal{D}$ из раздела 1.7. Имеет место следующее обобщение теоремы 3.

Лемма 2.6.3. *Экзистенциальная теория структуры* $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД},=\rangle$ *разрешима.*

Доказательство. Эта лемма всё ещё следует из разрешимости арифметики Сколема с константами $\mathrm{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\cdot,=\rangle$. Но можно доказать её с помощью алгоритма квази-ЭК.

Данная экзистенциальная формула после введения некоторых вспомогательных переменных может быть переписана в виде дизъюнкции формул вида

$$\exists\overline{y} \bigwedge_{i\in[1..m]} f_i(\overline{y}) \neq g_i(\overline{y}) \wedge \bigwedge_{i\in[m+1..l]} \text{НОД}(f_i(\overline{y}),g_i(\overline{y})) = h_i(\overline{y}), \tag{2.30}$$

где $f_i(\overline{y})$, $g_i(\overline{y})$, $h_i(\overline{y})$ суть либо au, либо a для положительного целого числа a и переменной $u \in \overline{y}$.

Сначала преобразуем эту формулу с помощью леммы 1.7.2. В нашем случае после замены переменных в некоторой конъюнкции вида (2.30) может появиться противоречие $f(\overline{y}) \neq f(\overline{y})$, и в этом случае она всегда ложна.

Пусть теперь в формулах алгоритма $\mathcal{D}$ имеются дизуравнения. Шаг 2 очевидно остаётся без изменений, так как по замечанию 1.3.1 всегда можно выбрать решение данной системы нод-выражений, которое удовлетворяет всем дизуравнениям. Применяя преобразования шага 1, как и в только что модифицированной лемме 1.7.2, можно получить противоречие $f(\overline{y}) \neq f(\overline{y})$. В этом случае соответствующая конъюнкция может быть исключена из формулы, так как оказывается всегда ложной. На этом модификация алгоритма квази-ЭК $\mathcal{D}$ завершена, и таким образом одновременно получаем искомую разрешающую процедуру. □

Назовём термы языка $L_{\langle 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД},=\rangle}$ *примитивными нод-термами.* Если $T(\overline{\alpha})$ является примитивным нод-термом, а p — некоторым простым числом, то термы вида $V_p(T(\overline{\alpha}))$ будем называть *p-оценёнными примитивными нод-термами.* Язык $L_{\mathcal{C}}$ алгоритма квази-ЭК $\mathcal{C}$ состоит из экзистенциальных формул $\exists\overline{\delta}\bigvee\limits_{j\in J_1}\varphi_j(\overline{y_j},\overline{\delta})$ для некоторого конечного множества индексов J_1 и формул $\varphi_j(\overline{y_j},\overline{\delta})$ вида

$$\begin{aligned}\overline{\delta^{(1)}}\geqslant 2\wedge\overline{\delta^{(2)}}\geqslant 2\wedge\overline{y}\geqslant 0\wedge&\bigwedge_{i\in[1..k]}\text{НОД}(f_i(\overline{y}),g_i(\overline{y}))=d_i\\ \wedge&\bigwedge_{i\in[k+1..l]}\text{НОД}(f_i(\overline{y}),g_i(\overline{y}))=d_i\delta_i\\ \wedge&\bigwedge_{i\in[l+1..m]}\text{НОД}(\text{НОД}(f_i(\overline{y}),F_i(\overline{\delta^{(2)}})),g_i(\overline{y}))=H_i(\overline{\delta^{(2)}}),\end{aligned}\tag{2.31}$$

где $\overline{\delta^{(1)}}=\delta_{k+1},\ldots,\delta_l$ и $\overline{\delta^{(2)}}=\delta_{l+1},\ldots,\delta_m$ суть непересекающиеся множества греческих переменных; как обычно, $f_i(\overline{y})$, $g_i(\overline{y})$ — линейные полиномы с целыми коэффициентами, а $F_i(\overline{\delta^{(2)}})$, $H_i(\overline{\delta^{(2)}})$ являются либо примитивными нод-термами, либо для некоторого простого числа p одновременно p-оценёнными примитивными нод-термами. Будем в дальнейшем называть *нод-выражениям* всякое выражение вида $\text{НОД}(u,v)=w$, какими бы ни были термы u,v,w, а не только в случае линейных полиномов.

Множество формул элиминационного вида $L^x_{\mathcal{C}}$ для латинской переменной x есть множество $L_{\mathcal{C}}$-формул $\exists\overline{\delta}\bigvee\limits_{j\in J_2}\widetilde{\varphi}_j(x,\overline{z_j},\overline{\delta})$ для некоторого конечного множества индексов J_2 и $\widetilde{\varphi}_j(x,\overline{z},\overline{\delta})$ вида:

$$\overline{\delta}\geqslant 2\wedge\overline{z}\geqslant 0\wedge x\geqslant 0\wedge\widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta})\wedge\bigwedge_{i\in[1..\widetilde{m}]}\text{НОД}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{g}_i(\overline{z})+c_ix)=\widetilde{H}_i(\overline{\delta}),\tag{2.32}$$

где x не входит в список переменных $\overline{z}$, $c_i>0$; каждое выражение $\widetilde{F}_i(\overline{z},\overline{\delta})$ есть либо линейный полином с неотрицательными целыми коэффициентами и положительным свободным членом, либо $\text{НОД}(f(\overline{z}),F(\overline{\delta}))$, где $F(\overline{\delta})$ — примитивный нод-терм, либо p-оценённый примитивный нод-терм; наконец, $\widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta})$ является системой нод-выражений без вхождений переменной x.

Теперь получим основной результат этого раздела.

Утверждение 2.6.2. *Экзистенциальная теория структуры $\langle\mathbb{Z};1,+,-,\leqslant,\perp\rangle$ разрешима.*

Доказательство. Ввиду того, что из каждой $L_{\mathcal{C}}$-формулы, не содержащей латинских переменных, можно исключить p-оценённые примитивные нод-термы с помощью равенства $\text{НОД}(V_p(x),y)=V_p(\text{НОД}(x,y))$ и формулы (2.15), несложно увидеть, что алгоритм квази-ЭК $\mathcal{C}$ сводит проблему выполнимости в целых числах $\mathbb{Z}$ систем вида (2.29) к проблеме разрешимости для фрагмента экзистенциальной теории структуры $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД},=\rangle$. В лемме 2.6.3 был описан алгоритм квази-ЭК для этой теории, а из леммы 2.6.2 следует, что для завершения доказательства достаточно определить шаг 1 и шаг 2 алгоритма квази-ЭК $\mathcal{C}$.

Шаг 1. Преобразования этого шага обобщают шаг 1 алгоритма $\mathcal{C}^+$. Применяя лемму 2.2.2 к каждому нод-выражению данной системы вида (2.31), получим систему вида (2.32). Отметим, что в случае нод-выражений с примитивными нод-термами, сначала группируются линейные полиномы: НОД(НОД($f_i(\overline{y})$,$F_i(\overline{\delta^{(2)}})$),$g_i(\overline{y})$) = НОД(НОД($f_i(\overline{y})$,$g_i(\overline{y})$),$F_i(\overline{\delta^{(2)}})$), затем применяется лемма 2.2.2, и наконец выражение переписывается в стандартном виде.

Теперь рассмотрим систему $\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ вида $\overline{\delta^{(1)}} \geqslant 2 \wedge \overline{\delta^{(2)}} \geqslant 2 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta}) \wedge \Delta(x,\overline{z},\overline{\delta})$, где

$$\begin{aligned}\Delta(x,\overline{z},\overline{\delta}) \rightleftharpoons & \bigwedge_{i\in[1..k]} \text{НОД}(\widetilde{f}_i(\overline{z}), \widetilde{g}_i(\overline{z}) + c_i x) = d_i \\ \wedge & \bigwedge_{i\in[k+1..l]} \text{НОД}(\widetilde{f}_i(\overline{z}), \widetilde{g}_i(\overline{z}) + c_i x) = d_i\delta_i \\ \wedge & \bigwedge_{i\in[l+1..m]} \text{НОД}(\text{НОД}(\widetilde{f}_i(\overline{z}),\widetilde{F}_i(\overline{\delta^{(2)}})), \widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{H}_i(\overline{\delta^{(2)}}).\end{aligned}$$

Для формулы $\exists\overline{\delta}\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ таким же образом, как и на шаге 1 алгоритма $\mathcal{R}$ из раздела 1.4, построим равновыполнимую формулу

$$\exists\overline{\delta}\Big(\widetilde{\Phi}_0(\overline{z_0},\overline{\delta}) \vee \widetilde{\Phi}_1(\overline{z_1},\overline{\delta}) \vee \widetilde{\Phi}_2(x,\overline{z_2},\overline{\delta})\Big),$$

где $\widetilde{\Phi}_0(\overline{z_0},\overline{\delta})$ и $\widetilde{\Phi}_1(\overline{z_1},\overline{\delta})$ суть дизъюнкции систем вида (2.32) таких, что список переменных $\overline{z_0}$ содержит на две, а список $\overline{z_1}$ — на одну переменную меньше, чем список $(x,\overline{z})$. В то же время, $\widetilde{\Phi}_2(x,\overline{z_2},\overline{\delta})$ будет дизъюнкцией требуемого вида, то есть, $\exists\overline{\delta}\,\widetilde{\Phi}_2(x,\overline{z_2},\overline{\delta})$ окажется некоторой $L^x_{\mathcal{C}}$-формулой.

Построение этих дизъюнкций производится таким же образом, как и во второй части раздела 1.4. Отметим, что для формулы $\widetilde{\Phi}_1(\overline{z_1},\overline{\delta})$ нам не нужны ограничения на нод-выражения вида ($\mathcal{R}$-2), так как теперь имеются два непересекающихся списка греческих переменных $\overline{\delta^{(1)}}$ и $\overline{\delta^{(2)}}$. Таким образом, для всякого $i \in [k+1..l]$ замена $\frac{\sigma(\widetilde{g}_i(\overline{z})+c_i x)}{d_i}$ вместо δ_i приведёт лишь к замене неравенства $\delta_i \geqslant 2$ на $\sigma(\widetilde{g}_i(\overline{z}) + c_i x) \geqslant 2d_i$.

Шаг 2. Как обычно, не умаляя общности можно считать, что в подсистеме (2.32), содержащей изолированную переменную x, все коэффициенты c_i равны единице.

На этом шаге для данной $L^x_{\mathcal{C}}$-формулы $\exists\overline{\delta}\widetilde{\varphi}(x,\overline{z},\overline{\delta})$, где

$$\widetilde{\varphi}(x,\overline{z},\overline{\delta}) \rightleftharpoons \overline{\delta} \geqslant 2 \wedge \overline{z} \geqslant 0 \wedge x \geqslant 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z},\overline{\delta}) \wedge \bigwedge_{i\in[1..\widetilde{m}]} \text{НОД}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{g}_i(\overline{z}) + x) = \widetilde{H}_i(\overline{\delta}), \qquad (2.33)$$

формула $\exists x\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ переписывается таким образом, что в итоге мы получим эквивалентную в $\mathbb{Z}$ формулу $\psi(\overline{z},\overline{\delta})$, причём $\exists\overline{\delta}\psi(\overline{z},\overline{\delta})$ оказывается некоторой $L_{\mathcal{C}}$-формулой.

Первые аргументы нод-выражений, содержащих переменную x, могут принимать только положительные значения: это очевидно, когда $\widetilde{F}_i(\overline{z},\overline{\delta})$ суть линейные полиномы с переменными из $\overline{z}$, и также верно для выражений вида НОД($f(\overline{z})$,$F(\overline{\delta})$), так как значения $F(\overline{\delta})$ всегда положительны. Следовательно, теперь можно применять НОД-лемму, причём с технической точки зрения удобнее заменить два условия (ii) и (iii) на одно условие ((iii)). Кроме того, ввиду замечания 2.5.1, можно позволить в условии ((iii)) равенство индексов $i = j$ вместо того, чтобы переписывать отдельно условие (i).

((iii)) для всяких $i,j \in [1..\widetilde{m}]$. Для этого условия получим следующую конъюнкцию:

$$\bigwedge_{1\leqslant i,j\leqslant \widetilde{m}} \text{НОД}(\text{НОД}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{H}_j(\overline{\delta})),\widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z})) = \text{НОД}(\widetilde{H}_i(\overline{\delta}),\widetilde{H}_j(\overline{\delta})). \tag{2.34}$$

Теперь покажем, что система (2.34) может быть переписана в виде подсистемы нод-выражений из $L_{\mathcal{C}}$-формулы.

Это несложно сделать, если $\widetilde{F}_i(\overline{z},\overline{\delta})$ является линейным полиномом с переменными из $\overline{z}$. В случае $\widetilde{F}_i(\overline{z},\overline{\delta}) = \text{НОД}(f_i(\overline{z}),F_i(\overline{\delta}))$, имеем

$$\text{НОД}(\widetilde{F}_i(\overline{z},\overline{\delta}),\widetilde{H}_j(\overline{\delta})) = \text{НОД}(f_i(\overline{z}),\text{НОД}(F_i(\overline{\delta}),\widetilde{H}_j(\overline{\delta}))).$$

Для того, чтобы выполнялись ограничения на p-оценённые примитивные нод-термы, снова используем равенства $\text{НОД}(V_p(x),y) = V_p(\text{НОД}(x,y))$ и $\text{НОД}(V_p(x),V_q(y)) = V_p(1) = V_q(1) = 1$ для различных простых чисел p и q. Эти две формулы вместе с ещё одним очевидным равенством $V_p(V_q(x)) = 1$ будут использоваться неявно при переписывании условия (iv) для того, чтобы вынести V_p на внешний уровень термов языка первого порядка сигнатуры $\langle 1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\{V_p\}_{p\in\mathbb{P}},\text{НОД},=\rangle$, где $\mathbb{P}$ есть множество простых чисел.

(iv). Если рассматривать это условие аналогично тому, как это было сделано в доказательстве леммы 2.5.4, то получим следующую конъюнкцию:

$$\bigwedge_{p\leqslant\widetilde{m}\wedge p\in\mathbb{P}} \left(\bigwedge_{I\subseteq[1..\widetilde{m}]\wedge|I|=p} \Omega_{p,I}(\overline{z},\overline{\delta}) \right), \tag{2.35}$$

где

$$\Omega_{p,I}(\overline{z},\overline{\delta}) \rightleftharpoons \bigvee_{i\in I\wedge j\in[1..\widetilde{m}]} V_p(p\widetilde{H}_i(\overline{\delta})) \mid \widetilde{H}_j(\overline{\delta}) \vee \bigvee_{i\in I} V_p(\widetilde{H}_i(\overline{\delta})) = V_p(\widetilde{F}_i(\overline{z},\overline{\delta})) \vee \bigvee_{i,j\in I\wedge i\neq j} V_p(\widetilde{H}_i(\overline{\delta})) \mid \widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z}).$$

Чтобы нод-выражения имели вид, требуемый для $L_{\mathcal{C}}$-формул, сначала воспользуемся формулой (2.14) для того, чтобы переписать всякую делимость $V_p(p\widetilde{H}_i(\overline{\delta})) \mid \widetilde{H}_j(\overline{\delta})$. Имеет место следующее равенство:

$$V_p(\text{НОД}(p\widetilde{H}_i(\overline{\delta}),\widetilde{H}_j(\overline{\delta}))) = V_p(p\widetilde{H}_i(\overline{\delta})).$$

Далее, для всякого равенства $V_p(\widetilde{H}_i(\overline{\delta})) = V_p(\widetilde{F}_i(\overline{z},\overline{\delta}))$ применим (2.15) и (2.34) для случая $i = j$ и в результате получим

$$V_p(\widetilde{H}_i(\overline{\delta})) = V_p(\widetilde{F}_i(\overline{z},\overline{\delta})) \Leftrightarrow \begin{cases} \text{НОД}(\widetilde{H}_i(\overline{\delta}),p\widetilde{F}_i(\overline{z},\overline{\delta})) = \widetilde{H}_i(\overline{\delta}) \\ \text{НОД}(p\widetilde{H}_i(\overline{\delta}),\widetilde{F}_i(\overline{z},\overline{\delta})) = \widetilde{H}_i(\overline{\delta}). \end{cases}$$

Наконец, каждая делимость $V_p(\widetilde{H}_i(\overline{\delta})) \mid \widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z})$ может быть переписана по определению:

$$\text{НОД}(V_p(\widetilde{H}_i(\overline{\delta})),\widetilde{g}_i(\overline{z}) - \widetilde{g}_j(\overline{z})) = V_p(\widetilde{H}_i(\overline{\delta})).$$

Так как были введены лишь нод-выражения с примитивными нод-термами (или p-оценёнными примитивными нод-термами) в левой части, греческие переменные, которые

входили в $\widetilde{\varphi}(x,\overline{z},\overline{\delta})$ в нод-выражения вида НОД$(f_i(\overline{z}),g_i(\overline{z})+x) = d_i\delta_i$ будут исключены из списка $\overline{\delta^{(1)}}$ и войдут в список $\overline{\delta^{(2)}}$. Следовательно, переходя к ДНФ, получим искомую $L_{\mathcal{C}}$-формулу. Это завершает построение алгоритма квази-ЭК $\mathcal{C}$ и, таким образом, доказательство утверждения 2.6.2. □

2.7 Заключение и переход к главе 3

Алгоритмы квазиэлиминации кванторов $\mathcal{C}^+$ and $\mathcal{C}$ могут оказаться полезными при попытках доказательства разрешимости экзистенциальной теории структуры $\langle\mathbb{Z};1,+,-,\leqslant,\perp,P_2\rangle$ или хотя бы позитивного фрагмента этой теории. Такие вопросы выглядят естественными подходами к вопросу Дж. Робинсон о разрешимости $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,|,P_2\rangle$. Функции V_p для простых оснований p активно использовались в алгоритме $\mathcal{C}$, и нам известно, что для всякого целого числа $k\geqslant 2$ график V_k бесквантворно выразим в структуре $\langle\mathbb{Z};1,+,-,\leqslant,|,P_k\rangle$. Это наталкивает на следующий вопрос: является ли разрешимой экзистенциальная теория структуры $\langle\mathbb{Z};1,+,-,\leqslant,|,P_2,P_3,P_4,...\rangle$? В примере 3.1.3 главы 3 показано, что если заменить в этой структуре все отношения P_k на единственный двухместный предикат $Pow_x(y)\rightleftharpoons\exists z(y=x^z)$, то экзистенциальная теория полученной структуры будет неразрешимой. Заметим, что этот предикат любопытно рассмотреть вместе с умножением вместо сложения. Если бы удалось доказать разрешимость $\exists\mathrm{Th}\langle\mathbb{Z}_{>0},\{a\}_{a\in\mathbb{Z}_{>0}},\cdot,Pow,=\rangle$, то этот результат был бы аналогом БЛ-теоремы в “мире умножения”.

Вопрос М. Божги и Р. Иосифа из эпиграфа послужил мотивацией к поиску некоторых общих результатов об экзистенциальной выразимости в арифметике со сложением и делимостью. Теорема 5 предоставляет описание отношений, являющихся позитивно экзистенциально выразимыми в структуре $\langle\mathbb{Z};1,+,\perp\rangle$. В то же время, задача кажется значительно более трудной, если включить в структуру отношение порядка. Например, в случае структуры $\langle\mathbb{N};0,S,\leqslant,\perp\rangle$, простая замена взаимной простоты на $[x,y]\not\perp[u,v]\rightleftharpoons\exists u\exists v\,(u\in[x,y]\wedge v\in[z,t]\wedge u\perp v)$ не даёт желаемого описания. Отношение порядка обрабатывается в $\mathcal{C}^+$ и $\mathcal{C}$ с помощью ЛС-леммы. Эти два алгоритма показывают, что разрешающая процедура становится всё более сложной, если сначала допустить использование отношения порядка, а затем и отрицание отношения взаимной простоты. Было бы интересно выяснить, позволяют ли алгоритмы квази-ЭК для Р$\exists$-теорий некоторых структур извлечь какую-либо информацию о позитивной экзистенциальной выразимости в этих структурах.

В этой главе изучались вопросы выразимости и разрешимости, так как основная цель состояла в том, чтобы продемонстрировать различные приложения двух основных инструментов из главы 1: НОД-леммы и алгоритмов квазиэлиминации кванторов. В то же время, не рассматривались вопросы вычислительной сложности изученных проблем. Оценка алгоритмической сложности арифметических теорий почти всегда является достаточно трудной

проблемой, поэтому маловероятно, что без серьёзных модификаций алгоритмы квази-ЭК $\mathcal{R}$ или $\mathcal{C}$ могут дать что-либо сильнее результата о принадлежности проблемы распознавания истинных в целых числах $\exists L_{PAD}$-формул классу **NEXPTIME** из работы [48]. Ввиду того, что основным предметом исследования в этой главе является арифметика Пресбургера с отношением взаимной простоты, отметим сейчас следующие вопросы: верно ли, что существует полином, такой что для всякой истинной в целых числах $\exists L_{PAC}$-формулы существует выполняющий набор, размер бинарной записи которого ограничен этим полиномом от длины формулы; и верно ли, что проблема существования целочисленных решений систем вида (2.24) разрешима за полиномиальное время для всякого фиксированного числа переменных в $\overline{z}$? Известно, что ответы на аналогичные вопросы для $\exists L_{PA}$-формул [14; 34; 70] утвердительны, и оба вопроса имеют отрицательные ответы в случае $\exists L_{PAD}$-формул [48; 52]. В действительности, Л. Липшиц построил в работе [52] NP-полное семейство систем из пяти линейных делимостей от четырёх переменных. В следующей главе аналогичное утверждение будет получено для предиката делимости на два последовательных числа, а доказательство Липшица будет приведено в примере 3.4.1.

В разделе 2.5 была доказана разрешимость экзистенциальной смешанной вещественно-целочисленной линейной арифметики с целочисленной делимостью. Если пытаться найти обобщение результату В. Виспфеннинга об элиминации кванторов в смешанной вещественно-целочисленной линейной арифметике [84], то интересным направлением является изучение вопросов выразимости и разрешимости для структуры $\langle \mathbb{R}; 1, +, -, [\,], 2^{[\,]}, =, < \rangle$, где $2^{[\,]}$ есть унарный функциональный символ для функции, отображающей вещественное число x в $2^{[x]}$. В 1983 году А.Л. Семёнов [9] показал, что существует алгоритм элиминации кванторов для некоторого расширения структуры $\langle \mathbb{N}; 1, +, 2^x, = \rangle$, из чего следовала разрешимость соответствующей элементарной теории; этот алгоритм элиминации кванторов был в явном виде представлен Ф. Пуан в препринте [62]. Заметим, что если в нашей структуре использовать функциональный символ 2^x вместо $2^{[\,]}$, то совсем несложно оказывается выразить умножение. Не известно, является ли теория $\mathrm{Th}\langle \mathbb{R}; 1, +, -, [\,], 2^{[\,]}, =, < \rangle$ разрешимой, однако, пример 3.1.4 из следующей главы демонстрирует, что $\exists \mathrm{Th}\langle \mathbb{R}; 1, +, -, [\,], 2^{[\,]}, =, <, | \rangle$ уже является неразрешимой.

В том же разделе были получены два разрешимых фрагмента $\forall\exists$-теории структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$, причём известно, что в общем случае $\forall\exists$-теория этой структуры неразрешима. Последний факт есть следствие выразимости графика возведения в квадрат (посредством несложной универсальной формулы) и ДПРМ-теоремы. Это универсальное определение возведения в квадрат использует предикат делимости на два последовательных целых числа $x \,{}^S|\, y \rightleftharpoons x \mid y \wedge 1 + x \mid y$, так что можно даже доказать неразрешимость $\forall\exists$-теории структуры $\langle \mathbb{N}; +, {}^S| \rangle$. В следующей главе будут изучены различные взаимосвязи между делимостью и ${}^S|$ с точки зрения вопросов выразимости и разрешимости.

Глава 3. Вопросы выразимости и разрешимости для предиката делимости на два последовательных числа

> On the other hand, formulas of the form $\exists \mathbf{x} \forall t \psi(\mathbf{x},t)$ where $\mathbf{x}$ is several variables and t just one variable and ψ is open in the language $\langle +, -, |, 0, 1\rangle$ are undecidable.
>
> ...ψ is constructed using the following devices.
>
> $$w = z^2 \Leftrightarrow z \mid w \wedge z + 1 \mid w + z \wedge$$
> $$\forall t(z \mid t \wedge z + 1 \mid t + z \Rightarrow w + z \mid t + z).$$
>
> L. Lipshitz [52] (1981)

Предложенное Липшицем определение графика возведения в квадрат неявно использует предикат делимости на два последовательных числа $x\,{}^S|y \rightleftharpoons x \mid y \wedge 1 + x \mid y$. Отсюда несложно получить выразимость всякого арифметического отношения в структуре $\langle \mathbb{N}; +, {}^S| \rangle$. В этой главе мы покажем, что аналогичное утверждение имеет место для структур $\langle \mathbb{N}; |, {}^S| \rangle$ и $\langle \mathbb{N}; S, 2^x, {}^S| \rangle$. Также будут рассмотрены вопросы экзистенциальной выразимости с помощью ${}^S|$; в частности, графики сложения и умножения являются экзистенциально выразимыми в $\langle \mathbb{N}; \cdot, {}^S| \rangle$ и $\langle \mathbb{N}; 1, +, Sq, {}^S| \rangle$. Заканчивается глава некоторыми результатами о выразимости для структуры $\langle \mathbb{N}; <, {}^S| \rangle$.

3.1 Выразимость в арифметике, Def-полнота и ∃Def-полнота

3.1.1 Определения и примеры

Помимо определений, введённых в разделе 1.1.1, нам понадобятся следующие понятия.

И. Корец в работе [44] использует удобное для формулировки результатов понятие полноты по выразимости некоторой структуры. Именно, для любых арифметических предикатов $X_1,...,X_n$ (то есть выразимых в структуре $\langle \mathbb{N}; +, \cdot, = \rangle$) структура $\langle \mathbb{N}; X_1,...,X_n \rangle$ называется *полной по выразимости* (*Def-полной*), если в ней выразимы графики функций сложения и умножения (трёхместные предикаты $x + y = z$ и $x \cdot y = z$). Аналогично для всяких *перечислимых* предикатов $X_1,...,X_n$ будем говорить, что структура $\langle \mathbb{N}; X_1,...,X_n \rangle$ является ∃*Def-полной*, если в ней *экзистенциально* выразимы графики функций сложения и умножения. Произвольная структура $\langle \mathbb{N}; \sigma \rangle$ будет называться Def-полной (∃Def-полной), если таковой окажется структура, сигнатура которой отлична от σ лишь тем, что вместо

функциональных символов в ней находятся предикатные символы для графиков соответствующих функций.

Статья И. Кореца [44] содержит обширный список наиболее известных на тот момент (2001 год) Def-полных структур. Ясно, что элементарные теории Def-полных структур являются неразрешимыми. Наиболее яркими примерами Def-полных структур являются $\langle \mathbb{N}; S, | \rangle$ (теорема Дж. Робинсон [69]) и $\langle \mathbb{N}; < , \perp \rangle$ (теорема А. Вудса [85]). Непосредственным следствием ДПРМ-теоремы [7] является неразрешимость экзистенциальной теории всякой $\exists$Def-полной структуры. Например, из «соотношения Тарского» [69]

$$z = x + y \Leftrightarrow (x = 0 \wedge y = 0 \wedge z = 0) \vee (z \neq 0 \wedge S(zx)S(zy) = S(z^2 S(xy))) \tag{3.1}$$

видим, что $\exists$Def-полной является структура $\langle \mathbb{N}; S, \cdot \rangle$. Приведём ещё ряд примеров.

Пример 3.1.1. *Структура* $\langle \mathbb{N}; \hat{}, = \rangle$ *является* $\exists$*Def-полной.*

Доказательство. Покажем экзистенциальную выразимость графиков функций сложения и умножения с помощью возведения в степень и отношения равенства. Сначала определим бесквантормыми формулами константы: $x = 1 \Leftrightarrow x \hat{} x = x$ и далее $x = 0 \Leftrightarrow x \hat{} x = 1 \wedge \neg x = 1$. Теперь видим, что

$$\begin{aligned} z = x \cdot y \ &\Leftrightarrow \exists t(\neg t = 0 \wedge \neg t = 1 \wedge t \hat{} z = (t \hat{} x) \hat{} y) \\ z = x + y &\Leftrightarrow \exists t(\neg t = 0 \wedge \neg t = 1 \wedge t \hat{} z = (t \hat{} x) \cdot (t \hat{} y)). \end{aligned}$$

□

БЛ-теорема показывает, что структура $\langle \mathbb{N}; 1, + , | \rangle$ не является $\exists$Def-полной. Ввиду экзистенциальных формул (2) для отношения НОД$(x,y) = z$ и его отрицания, множества отношений, $\exists$-выразимых в структурах $\langle \mathbb{N}; 1, + , | \rangle$ и $\langle \mathbb{N}; 1, + ,\text{НОД} \rangle$ совпадают, следовательно, последняя структура также не является $\exists$Def-полной. В то же время, в отличие от графика функции НОД, для графика функции вычисления наименьшего общего кратного НОК имеет место следующее:

Пример 3.1.2. *Структура* $\langle \mathbb{N}; 1, + ,\text{НОК} \rangle$ *является* $\exists$*Def-полной.*

Действительно, ввиду $z = x \cdot y \Leftrightarrow (x+y)^2 = x^2 + y^2 + 2z$, достаточно выразить отношение $y = x^2$ с помощью формулы НОК$(x, x + 1) = x + y$.

В предыдущих главах мы отмечали, что неизвестно, является ли разрешимой экзистенциальная теория структуры $\langle \mathbb{N}; 1, + , | , P_2 \rangle$, где $P_2(y) \rightleftharpoons \exists z(y = 2^z)$. Обобщим отношение P_2 следующим образом: $Pow_x(y) \rightleftharpoons \exists z(y = x^z)$ и покажем, что неразрешимой оказывается уже экзистенциальная теория натуральных чисел со сложением и Pow.

Пример 3.1.3. *Структура* $\langle \mathbb{N}; 1, + , Pow \rangle$ *является* $\exists$*Def-полной.*

Доказательство. Как обычно, так как $x = y \Leftrightarrow Pow_x y \wedge Pow_y x$, достаточно выразить экзистенциальной формулой график возведения в квадрат. В действительности, для этого отношения имеется бесквантормая формула:

$$y = x^2 \Leftrightarrow Pow_x y \wedge Pow_{2x} 4y \wedge Pow_{3x} 9y. \tag{3.2}$$

Пусть $y = x^k$ для некоторого $k \in \mathbb{N}$, тогда $4x^k = (2x)^l$ для $l \in \mathbb{N}$. Представим x в виде $2^\alpha z$, где $z \perp 2$ и получим следующее:

$$2^{\alpha k+2} z^k = 2^{\alpha l+l} z^l.$$

Если $z = 0$, то $x = y = 0$. В случае $z > 1$ необходимо $k = l = 2$, что влечёт $y = x^2$. Для оставшегося случая $x = 2^\alpha$ предназначен последний конъюнкт (3.2), так как имеем $9 \cdot 2^{\alpha k} = (3 \cdot 2^\alpha)^m$ для некоторого неотрицательного целого m; в то же время очевидно, что $m = 2$, а значит $k = 2$ и $y = x^2$. □

Перейдём к другому примеру. Как было показано Н.К. Косовским в [4], для всякого предиката степенного роста $T(x,y)$ структура $\langle \mathbb{N}; 1, +, |, T\rangle$ уже будет $\exists$Def-полной. Двухместный предикат T, заданный на натуральных числах, называется *предикатом степенного роста*, если существуют константы $C,D,c,d \in \mathbb{Q}_{>0}$, причём $d > 1$, что одновременно выполняются условия:

1. для всяких $x,y \in \mathbb{N}$ если $T(x,y) \wedge x > 0$, то $y \leqslant Cx^D$,
2. для всякого $x \in \mathbb{N}$ найдётся $y \in \mathbb{N}$, что $y \geqslant cx^d \wedge T(x,y)$.

Воспользуемся этим результатом, чтобы получить следующее.

Пример 3.1.4. *Структура* $\langle \mathbb{N}; 1, +, |, 2^x\rangle$ *является* $\exists$*Def-полной.*

Доказательство. Докажем $\exists$-выразимость отношения $|y| \leqslant 2|x|$, где $|x|$ есть длина двоичной записи натурального числа x. Этот предикат является предикатом степенного роста так как, с одной стороны, если $|y| \leqslant 2|x|$ и $x \neq 0$, то $y \leqslant 4x^2$. С другой стороны, очевидно $|x^2| \leqslant 2|x|$, и можно выбрать константы $C = 4$, $D = 2$, $c = 1$, $d = 2$.

Ввиду определений $x = y \Leftrightarrow x \mid y \wedge y \mid x$; $x = 0 \Leftrightarrow x + x = x$; $x \leqslant y \Leftrightarrow \exists z(y = x + z)$, достаточно записать отношение $x = |y|$ с помощью формулы

$$x = |y| \Leftrightarrow (x = 1 \wedge y = 0) \vee \exists t(t + 1 = x \wedge 2^t \leqslant y \wedge y + 1 \leqslant 2^x).$$ □

3.1.2 Делимость на два последовательных числа

Во введении был определён предикат $x \,{}^S|\, y \rightleftharpoons x \mid y \wedge 1 + x \mid y$, который использовался Л. ван ден Дрисом и А. Уилки в исследовании роста функций, графики которых являются экзистенциально выразимыми в структуре $\langle \mathbb{N}; 1, +, |\rangle$. Ими было показано, что если график некоторой функции $f : S \to \mathbb{N}$ для $S \subseteq \mathbb{N}^n$ является экзистенциально выразимым в этой структуре, то найдётся $c \geqslant 1$, что для всякого ненулевого набора $(x_1,...,x_n) \in S$ имеет место $f(x_1,...,x_n) \leqslant c\,(x_1 + ... + x_n)$. Кроме того, для всякой неограниченной функции f найдётся такое вещественное $c \in (0,1)$, что для бесконечного числа наборов $(x_1,...,x_n) \in S$ выполняется $f(x_1,...,x_n) > (x_1 + ... + x_n)^c$. В заключительном примечании в [31, с. 526] приводится простой пример, показывающий, что невозможно улучшить нижнюю оценку до линейной. Достаточно рассмотреть предикат ${}^S|$ и функцию, с его помощью определяемую,

$$f(x,y) = \begin{cases} x, & x > 0 \wedge y > 0 \wedge x \,{}^{S}|y \\ 0, & \text{иначе} \end{cases}. \tag{3.3}$$

Видим, что $f(x,y)$ является неограниченной функцией, такой что для любых $(x,y) \in \mathbb{N}^2$ выполняется $f(x,y) < (x+y)^{\frac{1}{2}}$.

Неявно его использовал Л. Липшиц в [52] для выразимости графика возведения в квадрат в $\langle \mathbb{N}; 1, +, | \rangle$ с помощью только одного квантора всеобщности. Пример (4) из [50], демонстрирующий невозможность получить полиномиальную верхнюю оценку на наименьший выполняющий набор значений переменных для систем делимостей и неравенств линейных полиномов в $\mathbb{Z}$, несложно переписать с помощью только предиката ${}^{S}|$.

Таким образом, полезно было бы отдельно изучить этот предикат в смысле выразимости с его помощью арифметических предикатов и разрешимости некоторых связанных с этим предикатом теорий, таких как $\exists\mathrm{Th}\langle \mathbb{N}; \cdot, {}^{S}| \rangle$. В обзоре И. Кореца [44] сложно найти структуры с предикатами, близкими к ${}^{S}|$, и поэтому было бы любопытно рассмотреть некоторые вопросы выразимости (в том числе экзистенциальной) для этого предиката. Кроме того, определение Липшица практически немедленно даёт нам Def-полноту структуры $\langle \mathbb{N}; +, {}^{S}| \rangle$.

Заметим возможную связь ${}^{S}|$ с отношением взаимной простоты. Обобщим понятие взаимной простоты на возрастающие факториальные степени (см., например, [35]) следующим образом:

$$x \perp_k y \rightleftharpoons \text{НОД}(x^{\overline{k}}, y^{\overline{k}}) = 1^{\overline{k}}, \tag{3.4}$$

где $x^{\overline{k}} = x(x+1)...(x+k-1)$. В частности, случай $k = 1$ есть обычное отношение взаимной простоты, а при $k = 2$ получим $x \perp_2 y \rightleftharpoons \text{НОД}(x(x+1), y(y+1)) = 2$. Хотя не выглядит очевидным выразимость взаимной простоты в $\langle \mathbb{N}; <, {}^{S}| \rangle$, для случая $k = 2$ введённое отношение выразимо в структуре $\langle \mathbb{N}; S, {}^{S}| \rangle$ формулой $\exists z(x \,{}^{S}|z \wedge y \,{}^{S}|SSz)$. Действительно, по китайской теореме об остатках получаем, что указанная формула переписывается в виде

$$\exists z \begin{cases} z \equiv \ \ 0 \,(\mathrm{mod}\ x(x+1)) \\ z \equiv -2 \,(\mathrm{mod}\ y(y+1)) \end{cases} \Leftrightarrow \text{НОД}(x(x+1), y(y+1)) \mid 2, \tag{3.5}$$

причём в последнем выражении имеет место не делимость, а равенство, так как оба аргумента НОД чётные. Этим предикатом мы воспользуемся для доказательства Def-полноты структуры $\langle \mathbb{N}; S, 2^x, {}^{S}| \rangle$.

3.2 Def-полнота для ${}^{S}|$ и делимости

Определим сначала некоторые простые предикаты, выразимые только с помощью ${}^{S}|$.

Лемма 3.2.1. *Свойства $x = 0$, $x = 1$ и отношение $x = y$ выразимы в структуре $\langle \mathbb{N}; {}^{S}| \rangle$.*

Доказательство. Ясно, что $x = 0 \Leftrightarrow x \,{}^{S}|x$; $x = 1 \Leftrightarrow \forall y \forall z(z \,{}^{S}|y \Rightarrow x \,{}^{S}|y)$. Действительно, если $y = 2$ и $z = 1$, то необходимо, чтобы $x = 1$, в то время как для всяких y, для которых $z \,{}^{S}|y$ при

некотором z, формула $1\,{}^S|y$ всегда истинна. Последнее, $x = y \Leftrightarrow \forall z(x\,{}^S|z \Longleftrightarrow y\,{}^S|z)$. В случае $x = 0$ и $y > 0$ достаточно рассмотреть $z = y(y+1)$, если же оба аргумента положительны и, например, $x < y$, то возьмём $z = x(x+1)$. □

Рассмотрим вопросы выразимости и разрешимости для структур с ${}^S|$ и некоторыми арифметическими предикатами, выразимыми с помощью только умножения и равенства.

Теорема 8. *Структура* $\langle \mathbb{N}; |\,, {}^S| \rangle$ *Def-полна.*

Доказательство. По известной теореме Дж. Робинсон [69], Def-полной является структура $\langle \mathbb{N}; S, | \rangle$. Поэтому нам достаточно определить отношение $y = Sx$.

Отношение $x \perp y$ выразимо с помощью $\forall t(t \mid x \wedge t \mid y \Rightarrow t = 1)$. Тогда получаем следующее определение:

$$y = Sx \Leftrightarrow (x = 0 \wedge y = 1) \vee (\neg x = 0 \wedge x \perp y \wedge \forall z(x\,{}^S|z \Leftrightarrow x \mid z \wedge y \mid z)).$$

Импликация вправо очевидна, покажем, что импликация верна в обратную сторону. Если $x \neq 0$, то для $z = x(x+1)$ ввиду того, что $y \mid z$ и $x \perp y$, необходимо $y \neq 0$ и $y \mid Sx$, следовательно, $0 < y \leqslant Sx$. Если предположить, что $y < Sx$, то получим противоречие для $z = x \cdot y$, так как одновременно $x \cdot y < x(x+1)$ и $x(x+1) \mid z$. □

Как элементарная теория натуральных чисел с делимостью $\mathrm{Th}\langle \mathbb{N}; | \rangle$, так и элементарная теория с взаимной простотой $\mathrm{Th}\langle \mathbb{N}; \perp \rangle$ разрешимы. Это следует из выразимости этих предикатов с помощью умножения и равенства (для предиката взаимной простоты можно воспользоваться формулой из доказательства теоремы 8 и $x = 1 \Leftrightarrow \forall y(x \cdot y = y)$) и разрешимости арифметики Сколема $\mathrm{Th}\langle \mathbb{N}; \cdot, = \rangle$, доказанной А. Мостовским в [57]. Для предиката $x\,{}^S|y$ имеем следствие теоремы 8.

Следствие 8.1. *Отношение* ${}^S|$ *не является выразимым в структуре* $\langle \mathbb{N}; \cdot, = \rangle$.

3.3 Неразрешимость экзистенциальной арифметики с ${}^S|$ и умножением

Если теперь мы обратимся к только экзистенциальным теориям, то разрешимость $\exists\mathrm{Th}\langle \mathbb{N}; |\,, {}^S| \rangle$ очевидна ввиду того, что всякая формула этой теории принадлежит разрешимой $\exists\mathrm{Th}\langle \mathbb{N}; 1, +\,, | \rangle$. Исследуем вопрос о разрешимости $\exists\mathrm{Th}\langle \mathbb{N}; \cdot, {}^S| \rangle$. Покажем, что структура $\langle \mathbb{N}; \cdot, {}^S| \rangle$ является $\exists$Def-полной. В первую очередь хотелось бы получить экзистенциальные выражения для $x = 1$, $x = y$ в $\langle \mathbb{N}; \cdot, {}^S| \rangle$. Нам понадобится следующая лемма.

Лемма 3.3.1. *Для всяких целых чисел* $x \geqslant 1$ *и* $y \geqslant 0$ *делимость* $y(x+1)+1 \mid x^2$ *имеет место тогда и только тогда, когда* $y = 0$ *или* $y = x - 1$.

Доказательство. Ясно, что значения $y = 0$ и $y = x - 1$ удовлетворяют делимости. Покажем, что других решений нет.

Из делимости следует, что $y \in [0,x-1]$. Пусть $y = x - k$ для некоторого $k \in [1,x)$, тогда

$$y(x+1)+1 \mid x^2 \Leftrightarrow \exists k(y(y+k+1)+1 \mid (y+k)^2 \wedge y = x-k).$$

Делимость из подкванторного выражения перепишем, вычитая из правого аргумента левый. Вынесем сразу в получающемся выражении $(k-1)y + k^2 - 1$ множитель $k-1$ и получим следующее:

$$y(y+k+1)+1 \mid (y+k)^2 \Leftrightarrow y(y+k+1)+1 \mid (k-1)(y+k+1).$$

Так как $y > 0$, то, во-первых, $y(y+k+1)+1 \perp y+k+1$, из чего следует $y(y+k+1)+1 \mid k-1$. Во-вторых, $y(y+k+1)+1 > k+1$, поэтому $k = 1$ и $y = x-1$, что и завершает доказательство леммы. □

Заметим, что в лемме 3.2.1 мы получили бесквантороное выражение для $x = 0$. Докажем следующую вспомогательное утверждение.

Лемма 3.3.2. *Свойства $x \neq 1$, $x = 1$ и отношения $x = y$, $y = x^2 - 1$, $x \mid y$ экзистенциально выразимы в структуре $\langle \mathbb{N}; \cdot, {}^S| \rangle$.*

Доказательство. Для первого предиката можно воспользоваться отрицанием формулы для $x = 1$ из леммы 3.2.1: $x \neq 1 \Leftrightarrow \exists y \exists z(z\,{}^S|y \wedge \neg x\,{}^S|y)$. Далее, из леммы 3.3.1 следует, что

$$x > 1 \wedge y > 1 \wedge y = x^2 - 1 \Leftrightarrow x \neq 0 \wedge y \neq 0 \wedge x\,{}^S|xy \wedge y\,{}^S|yx^2). \tag{3.6}$$

Действительно, $x\,{}^S|xy \Leftrightarrow x+1 \mid y$, а $y\,{}^S|yx^2 \Leftrightarrow y+1 \mid x^2$ для положительных x и y, из чего и следует эквивалентность (3.6). Теперь, используя таким образом определённый предикат $x > 1 \wedge y > 1 \wedge y = x^2 - 1$, получим следующее:

$$x > 1 \wedge y > 1 \wedge x = y \Leftrightarrow \exists u \exists v \begin{pmatrix} x > 1 \wedge u > 1 \wedge u = x^2 - 1 \wedge u\,{}^S|y^2u \\ \wedge y > 1 \wedge v > 1 \wedge v = y^2 - 1 \wedge v\,{}^S|x^2v \end{pmatrix}.$$

С помощью такого «ограниченного» равенства мы можем выразить второй из искомых предикатов:

$$x = 1 \Leftrightarrow \exists y \exists z(y > 1 \wedge z > 1 \wedge y = z \wedge y > 1 \wedge xz > 1 \wedge y = xz).$$

Теперь мы можем, во-первых, выразить равенство $x = y \Leftrightarrow (x = 0 \wedge y = 0) \vee (x = 1 \wedge y = 1) \vee (x > 1 \wedge y > 1 \wedge x = y)$, а, во-вторых, с помощью выражения (3.6) определить аналогичным образом отношение $y = x^2 - 1$. Обладая равенством, делимость получаем по определению $x \mid y \Leftrightarrow \exists z(y = xz)$. □

Для доказательства ∃Def-полноты структуры $\langle \mathbb{N}; \cdot, {}^S| \rangle$ нам достаточно выразить экзистенциальной формулой отношение $y = Sx$, так как $\langle \mathbb{N}; S, \cdot \rangle$ является ∃Def-полной, как было уже отмечено в первом параграфе. Докажем сначала ещё одно вспомогательное утверждение.

Лемма 3.3.3. *Для всяких целых чисел $x > 1$ и $y \geqslant 0$ делимость $yx+1 \mid x^2-1$ имеет место тогда и только тогда, когда $y = 0$ или $y = 1$.*

Доказательство. Значения $y = 0$ и $y = 1$ очевидно удовлетворяют делимости. Покажем, что других таких y нет.

Пусть $y \geqslant 2$. Так как $y \leqslant x - 1$, то $y = x - k$ для некоторого $k \in [1,x - 2]$. Прибавим левый аргумент делимости к правому и вынесем общий множитель $y + k$:

$$yx + 1 \mid x^2 - 1 \Leftrightarrow y(y + k) + 1 \mid (y + k)^2 - 1 \Leftrightarrow y(y + k) + 1 \mid (y + k)(2y + k).$$

Так как $y > 0$, получаем, что $y(y+k)+1 \perp y+k$. Следовательно, необходимо $y(y+k)+1 \mid 2y+k$, где правый аргумент положителен и меньше y^2+ky+1 для всякого $y \geqslant 2$. Из этого заключаем, что при $y \geqslant 2$ делимость не имеет места. □

Теперь можно выразить «ограниченное» отношение $y = Sx$.

Лемма 3.3.4. *Отношение $x > 2 \wedge y = Sx$ экзистенциально выразимо в структуре $\langle \mathbb{N}; \cdot, {}^S| \rangle$.*

Доказательство. Мы будем пользоваться предикатами из леммы 3.3.2. Свойство $x > 1$ определяется как $x \neq 0 \wedge x \neq 1$.

Покажем, что

$$\begin{gathered} x > 2 \wedge y = Sx \Leftrightarrow \\ \exists z \exists t \left(z > 1 \wedge x > 1 \wedge x \,{}^S| xy \wedge yz = x^2 - 1 \wedge t = z^2 - 1 \wedge x \mid t \right). \end{gathered} \tag{3.7}$$

Если $y = x + 1$ для некоторого $x > 2$, то возьмём $z = x - 1$ и $t = (x - 1)^2 - 1$.

Обратно, пусть $x > 1$, тогда $x \,{}^S| xy \Leftrightarrow x + 1 \mid y$, а значит, $y = k(x + 1)$ для некоторого $k \geqslant 0$ и $k(x+1)z = (x+1)(x-1)$. Следовательно, $kz = x-1$. Получаем, что $kz+1 \mid z^2-1$ для некоторого $k \geqslant 0$, из чего по лемме 3.3.3 следует, что число k есть либо ноль, либо единица. Поскольку $k = 0$ влечёт $x = 1$, остаётся единственная возможность $k = 1$ и $z = x - 1$, а значит, $y = x + 1$. □

Теорема 9. *Отношения $x = y$ и $y = Sx$ экзистенциально выразимы в $\langle \mathbb{N}; \cdot, {}^S| \rangle$, следовательно, структура $\langle \mathbb{N}; \cdot, {}^S| \rangle$ является $\exists$Def-полной, а её экзистенциальная теория неразрешима.*

Доказательство. Нам достаточно выразить свойство $x = 2$, так как $y = 3 \Leftrightarrow \exists x(x = 2 \wedge y = x^2 - 1)$, а для случая $x > 2$ имеем определение (3.7) из леммы 3.3.4. Покажем, что

$$x = 2 \Leftrightarrow \exists y \exists z \exists t \left(zx > 2 \wedge y = Szx \wedge x \mid z \wedge t = y^2 - 1 \wedge z \,{}^S| t \right).$$

Если $x = 2$, то возьмём $z = 2$, $y = 5$ и $t = 24$.

Для доказательства в обратную сторону, перепишем выражение в скобках в следующем виде:

$$zx > 2 \wedge z(z + 1) \mid (zx + 1)^2 - 1 \wedge x \mid z.$$

Так как $z \neq 0$, избавимся от z в первой делимости: $z + 1 \mid x(zx + 2)$. Ввиду того, что $x \mid z$, получаем $z + 1 \perp x$, и поэтому $z + 1 \mid zx + 2$. Последняя делимость истинна тогда и только тогда, когда $z + 1 \mid 2 - x$, или $x \equiv 2 (\mathrm{mod}\ z + 1)$, но $0 < x < z + 1$, значит, $x = 2$.

Таким образом, $x = y$ экзистенциально выразимо в $\langle \mathbb{N}; \cdot, {}^{S}| \rangle$ по лемме 3.3.2, экзистенциальная выразимость $y = Sx$ следует из определений для $x = 0$, $x = 1$ из леммы 3.3.2, полученного выражения для $x = 2$ и $x = 3$, а также формулы для $x > 2 \wedge y = Sx$ из леммы 3.3.4. Ввиду $\exists$Def-полноты $\langle \mathbb{N}; S, \cdot \rangle$ получаем искомое. □

3.4 Вопросы Def-полноты, разрешимости и сложности для ${}^{S}|$ со сложением

3.4.1 Сложение и ${}^{S}|$

Перейдём к проблемам выразимости и разрешимости для структур и теорий натуральных чисел с ${}^{S}|$ и некоторыми, выразимыми с помощью сложения, предикатами. Начнём со следующего несложного утверждения.

Утверждение 3.4.1. *Структура $\langle \mathbb{N}; +, {}^{S}| \rangle$ Def-полна.*

Доказательство. Как обычно, достаточно выразить график функции возведения в квадрат $y = x^2$. Используя тот факт, что $x \leqslant y \Leftrightarrow \exists z(x + z = y)$, получим следующее определение:

$$y = x^2 \Leftrightarrow x \,{}^{S}|x + y \wedge \forall z(x \,{}^{S}|x + z \Rightarrow y \leqslant z). \tag{3.8}$$

Так как $x \,{}^{S}|x + y$, то x и y могут быть равны нулю только одновременно. Для ненулевых значений параметров y — наименьшее число, для которого выполняется $x(x + 1) \mid x + y$, то есть, $x^2 + x = x + y$. □

Как уже отмечалось во введении, формула (3.8) аналогична выражению, предложенному Л. Липшицем [52], для определения в структуре $\langle \mathbb{N}; 1, +, | \rangle$ графика возведения в квадрат:

$$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z(x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z). \tag{3.9}$$

Видим, что $x \mid y \wedge x + 1 \mid x + y \Leftrightarrow x \,{}^{S}|x + y$. С помощью определения (3.8), получим следствие утверждения 3.4.1. Напомним, что $\exists\forall\mathrm{Th}\langle \mathbb{N}; +, {}^{S}| \rangle$ есть множество всех истинных в $\mathbb{N}$ замкнутых формул языка $L_{\langle +, \leqslant, {}^{S}| \rangle}$ с кванторными приставками вида $\exists x_1 ... \exists x_n \forall y_1 ... \forall y_m$. Сначала докажем вспомогательную лемму.

Лемма 3.4.1. *Отношения $x = 0$ и $x = 1$ бесквантворно выразимы в структуре $\langle \mathbb{N}; +, {}^{S}| \rangle$, а отношения $x = y$ и $x \leqslant y$ — экзистенциально выразимы в этой структуре.*

Доказательство. Действительно, $x = 0 \Leftrightarrow x \,{}^{S}|x$ и $x = 1 \Leftrightarrow \neg x \,{}^{S}|x \wedge x \,{}^{S}|x + x$. Для отношения равенства воспользуемся следующей экзистенциальной формулой:

$$x = y \Leftrightarrow \exists z \left(x \,{}^{S}|z + x \wedge x \,{}^{S}|z + y \wedge y \,{}^{S}|z + x \wedge y \,{}^{S}|z + y \right). \tag{3.10}$$

Случай равенства нулю одного из аргументов влечёт равенство нулю другого. Если x,$y \neq 0$, то из первых двух выражений следует $x \equiv y (\mathrm{mod}\ x(x+1))$, а из третьего и четвёртого, что $x \equiv y (\mathrm{mod}\ y(y+1))$. Несложно увидеть, что отсюда следует равенство x и y, а следовательно и $\exists$-выразимость отношения $x \leqslant y$. □

Следствие 3.4.1.1. *Теория* $\exists\mathrm{Th}\langle\mathbb{N};+,{}^{S}|\rangle$ *разрешима, а* $\exists\forall\mathrm{Th}\langle\mathbb{N};+,{}^{S}|\rangle$ *неразрешима.*

Доказательство. Первая часть утверждения непосредственно следует из БЛ-теоремы. Вторая часть следует из ДПРМ-теоремы и формулы (3.8) аналогично тому, как было получено доказательство неразрешимости $\exists\forall\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$ Л. Липшицем [52]. Распишем это доказательство подробнее.

Покажем, что всякое множество, $\exists$-выразимое в структуре $\langle\mathbb{N};+,\cdot,=\rangle$, является $\exists\forall$-выразимым в структуре $\langle\mathbb{N};+,{}^{S}|\rangle$. Хорошо известно (см. книгу Ю.В. Матиясевича [7]), что всякое такое множество выразимо с помощью формулы $\exists\overline{y}(P(\overline{x},\overline{y})=0)$, где $P(\overline{x},\overline{y})$ есть полином с целыми коэффициентами. Ввиду известной формулы $z=xy \Leftrightarrow (x+y)^2=x^2+y^2+2z$, по этому полиномиальному уравнению можно построить $L_{\langle+,=\rangle}$-формулу $\chi(\overline{x},\overline{y},\overline{u},\overline{v})$, где $\overline{u}=u_1,...,u_m$, $\overline{v}=v_1,...,v_m$ и

$$\exists\overline{y}(P(\overline{x},\overline{y})=0) \Leftrightarrow \exists\overline{y}\exists\overline{u}\exists\overline{v}\left(\chi(\overline{x},\overline{y},\overline{u},\overline{v}) \wedge \bigwedge_{i\in[1..m]} v_i = u_i^2\right). \tag{3.11}$$

Введём новые переменные, чтобы переписать формулу $\chi(\overline{x},\overline{y},\overline{u},\overline{v})$ с помощью (3.10) в виде экзистенциальной $L_{\langle+,{}^{S}|\rangle}$-формулы.

Осталось переписать каждое выражение $v_i = u_i^2$ для $i = 1..m$ с помощью универсальных $L_{\langle+,{}^{S}|\rangle}$-формул. Для этого достаточно показать, что $x \leqslant y$ является $\forall$-выразимым в структуре $\langle\mathbb{N};+,{}^{S}|\rangle$ и затем воспользоваться формулой (3.8). Видим, что $x \leqslant y \Leftrightarrow \forall z(1+y+z \neq x)$, а универсальная выразимость $x=1$ и $x \neq y$ следует из леммы 3.4.1. □

3.4.2 NP-трудное семейство сложения и ${}^{S}|$

Предикат ${}^{S}|$ неявно появляется в работе Л. Липшица [52] в доказательстве NP-трудности проблемы совместности в натуральных числах систем из только пяти делимостей от четырёх переменных.

Будем считать, что натуральные параметры формул кодируются бинарно. Важно отметить, что Л. Липшицем было построено не NP-трудное множество, экзистенциально выразимое в структуре $\langle\mathbb{N};1,+,|\rangle$, а NP-трудное семейство. Так как доказательство Липшица совсем простое, однако опубликовано в труднодоступных материалах конференции [52], приведём его в качестве примера, а затем определим понятие семейства сложения и делимости.

Введём следующие массовые проблемы в том виде, как они сформулированы и названы в русском переводе списка NP-трудных задач книги М. Гэри и Д. Джонсона [33]:

КВАДРАТИЧНЫЕ СРАВНЕНИЯ (КС)

УСЛОВИЕ: Заданы положительные целые числа a, b и c.

ВОПРОС: Существует ли положительное целое число $x \leqslant c$, такое что $x^2 \equiv a (\mathrm{mod}\ b)$? Результат об NP-полноте этой проблемы был получен К. Мандерсом и Л. Адлеманом [56].

СОВМЕСТНАЯ ДЕЛИМОСТЬ ЛИНЕЙНЫХ ПОЛИНОМОВ (СДЛП)

УСЛОВИЕ: Заданы векторы $a_i = a_{i,0},\ldots,a_{i,n}$ и $b_i = b_{i,0},\ldots,b_{i,n}$ при $i \in [1..m]$, с неотрицательными целыми координатами.

ВОПРОС: Существуют ли такие натуральные числа $x_1, x_2, \ldots, x_n$, что при всех $i \in [1..m]$ выполняется $a_{i,0} + \sum_{j=1}^{n} a_{i,j}x_j \mid b_{i,0} + \sum_{j=1}^{n} b_{i,j}x_j$?

В работе Л. Липшица [52] доказана принадлежность **NP** задачи СДЛП при любом фиксированном числе делимостей m. NP-трудность СДЛП при $m = 5$ и $n = 4$ доказывается полиномиальным сведением к этой проблеме задачи КС. Это доказательство подскажет, как можно получить аналогичный результат для делимости на два последовательных числа.

Пример 3.4.1 (Л. Липшиц [52, Proposition 2])**.** *Проблема СДЛП, в случае когда число переменных $n = 4$, а число делимостей $m = 5$, является NP-трудной.*

Доказательство. Можно считать, что в КС $a < b$ и переменная x принимает значения из отрезка $[0..c]$. Покажем, что в $\mathbb{N}$ имеет место следующая равносильность:

$$\exists x \begin{cases} x^2 \equiv a\,(\mathrm{mod}\ b) \\ x \in [0..c] \end{cases} \Leftrightarrow \exists x \exists y \exists u \exists v \begin{cases} b \mid y + (b - a) \\ x + c \mid y + 2cx + c^2 \\ x + (c+1) \mid y + 2(c+1)x + (c+1)^2 \\ y + u \mid c^2 \\ x + v \mid c \end{cases} \tag{3.12}$$

Переменные u и v необходимы лишь для того, чтобы записать ограничения $x \in [0..c]$ и $y \in [0..c^2]$. По китайской теореме об остатках из второй и третьей делимости следует, что существует единственный y, удовлетворяющий этим двум делимостям из полуинтервала $[0,(x + c)(x + c + 1))$. Очевидно $y = x^2$ является решением этой подсистемы; в то же время, так как $(x + c)(x + c + 1) > c^2$, на отрезке $[0..c^2]$ других решений быть не может. Отсюда следует эквивалентность (3.12). □

Для формул из правой части (3.12) введём следующее понятие.

Определение 2. ***Семейство сложения и делимости*** *есть всякое множество $S \subseteq \mathbb{N}^n$, для которого существует бескванторная $L_{\langle 1,+,\cdot,|\rangle}$-формула $\varphi(\overline{x},\overline{y})$, линейная по $\overline{y}$, такая что $\overline{a} \in S \Leftrightarrow \exists \overline{y} \varphi(\overline{a},\overline{y})$.*

Таким образом, пример 3.4.1 показывает, что существует NP-трудное семейство сложения и делимости.

Очевидно, что всякое семейство сложения и делимости является экзистенциально выразимым в структуре $\langle \mathbb{N}; +, \cdot, = \rangle$. Можно попытаться обобщить определение 2 на произвольные арифметические структуры, но для данной главы в этом нет необходимости. Введём аналог определения 2 для отношения делимости на два последовательных числа.

Определение 3. ***$\langle +, {}^{S}\vert\rangle$-семейство*** *есть всякое множество $S \subseteq \mathbb{N}^n$, для которого существует бескванторная $L_{\langle +,\cdot,\, {}^{S}\vert\rangle}$-формула $\varphi(\overline{x},\overline{y})$, линейная по $\overline{y}$, такая что $\overline{a} \in S \Leftrightarrow \exists\overline{y}\varphi(\overline{a},\overline{y})$.*

Напомним, что семейство S называется NP-трудным, если NP-трудной является проблема распознавания $\overline{a} \in S$ при условии двоичного кодирования натуральных чисел вектора $\overline{a}$. Теперь докажем следующее утверждение.

Утверждение 3.4.2. *Существует NP-трудное $\langle +, {}^{S}\vert\rangle$-семейство.*

Доказательство. Построим полиномиальное сведение NP-полной проблемы разрешимости квадратичного сравнения $x^2 \equiv a(\mathrm{mod}\ b)$ на отрезке $x \in [2..c]$ для положительных параметров a, b и c, где $c \geqslant 2$, полиномиальное сведение к которой проблемы КС очевидно.

Построим экзистенциальную $L_{\langle +,\cdot,\, {}^{S}\vert\rangle}$-формулу вида $\exists\overline{y}\varphi(a,b,c,\overline{y})$, определяющую $\langle +, {}^{S}\vert\rangle$-семейство троек (a,b,c) натуральных чисел со следующим свойством. Если a, b и c — положительные целые числа и $c \geqslant 2$, то

$$\exists x \left(x^2 \equiv a(\mathrm{mod}\ b) \wedge x \in [2..c]\right) \Leftrightarrow \exists\overline{y}\varphi(a,b,c,\overline{y}).$$

Так как будет построена конкретная формула, как и в примере 3.4.1, сведение окажется полиномиальным.

Покажем, что в $\mathbb{N}$ имеет место эквивалентность, схожая с (3.12):

$$\exists x \begin{cases} x^2 \equiv a\,(\mathrm{mod}\ b) \\ x \in [2..c] \end{cases} \Leftrightarrow \exists x \exists y \begin{cases} b \mid y + (b-a) \\ cx+1 \mid c^2y + 3cx + 2 \\ cx+2 \mid c^2y + 3cx + 2 \\ x \in [2..c] \\ y \in [4..c^2] \end{cases} \tag{3.13}$$

Для того, чтобы закончить доказательство достаточно заметить следующее. С помощью формулы $b\,{}^{S}|(b+1)y+(b+1)(b-a)$ переписывается первая делимость. Подсистема, состоящая из второй и третьей делимости есть в точности $cx+1\,{}^{S}|c^2y+3cx+2$, а для двух последних выражений воспользуемся $\exists$-выразимостью отношения $\leqslant$ из леммы 3.4.1.

В формуле (3.13) очевидна импликация вправо. Докажем обратное, именно, что если правая система имеет некоторое решение x,y, то необходимо $y = x^2$.

Видим, что $cx + 1 \perp c^2$, в то время как НОД$(cx + 2, c^2) = 2$, если c чётное и $cx + 2 \perp c^2$, если c нечётное. По китайской теореме об остатках подсистема из второй и третьей делимостей имеет единственное решение в полуинтервале $\left[0, \frac{(cx+1)(cx+2)}{2}\right)$, если c чётное, а иначе — единственное в полуинтервале $[0,(cx+1)(cx+2))$. Так как $x \geqslant 2$, то $\frac{(cx+1)(cx+2)}{2} > 2c^2$, из чего следует, что при $y \in [4..c^2]$ единственным решением окажется $y = x^2$, что завершает доказательство утверждения. □

Полученное NP-трудное семейство будет принадлежать классу **NP** по теореме Л. Липшица [52] о принадлежности **NP** всякого семейства сложения и делимости. Ясно, что

множество таких семейств является более широким классом отношений, чем множество всех отношений, $\exists$-выразимых в структуре $\langle \mathbb{N}; 1, +, | \rangle$. Изучение свойств семейств сложения и делимости выглядит достаточно любопытной проблемой.

3.4.3 Множество квадратов, сложение и ${}^{S}|$

В связи с определением графика фозведения в квадрат (3.9), Л. ван ден Дрисом и А. Уилки был задан вопрос об экзистенциальной выразимости в структуре $\langle \mathbb{N}; 1, +, | \rangle$ отношения $\neg Sq(x) \rightleftharpoons \forall y(y \neq x^2)$. В то время как вопрос о $\exists$Def-полноте структуры $\langle \mathbb{N}; 1, +, Sq \rangle$ остаётся открытым (см. [53; 60], положительный ответ следовал бы из истинности гипотезы Бюхи о пяти квадратах), ван ден Дрису и Уилки, по-видимому, было известно о $\exists$Def-полноте $\langle \mathbb{N}; 1, +, Sq, | \rangle$. Так как ссылку на этот результат найти не удалось, покажем здесь, что отношение $y = x^2$ выразимо в этой структуре несложной бесквантворной формулой. Это определение позволит доказать $\exists$Def-полноту структуры $\langle \mathbb{N}; 1, +, Sq, {}^{S}| \rangle$.

Утверждение 3.4.3. *Отношение $y = x^2$ является бесквантворно выразимым в структуре $\langle \mathbb{N}; 1, +, Sq, | \rangle$, следовательно, эта структура $\exists$Def-полна, а её экзистенциальная теория неразрешима.*

Доказательство. Покажем, что

$$y = x^2 \Leftrightarrow Sq(y) \wedge Sq(y + 2x + 1) \wedge x \mid y \wedge 1 + x \mid y + 2x + 1. \tag{3.14}$$

Последнюю делимость можно переписать в виде $1 + x \mid y - 1$. Пусть $y = z^2$, тогда из того, что $x \mid y$ следует, что $z^2 = xu$ для некоторого $u > 0$ (если $u = 0$, то $y = 0$, и поэтому $1 + x \mid x$, а значит, $x = 0$).

Перепишем делимость $1 + x \mid y - 1$ в виде $1 + x \mid xu - 1$, что равносильно $1 + x \mid u + 1$. Пусть теперь $u + 1 = (x + 1)v$ для некоторого $v > 0$. Тогда получим цепочку равенств

$$\begin{aligned} y + 2x + 1 = xu + 2x + 1 &= x((x + 1)v - 1) + 2x + 1 \\ &= x(x + 1)v + (x + 1) = (x + 1)(xv + 1). \end{aligned}$$

Осталось показать, что v может только быть равным единице.

Предположим, что $v > 1$ и выполняется

$$Sq((x + 1)(xv + 1) - 2x - 1) \wedge Sq((x + 1)(xv + 1)).$$

Пусть $t^2 = (x+1)(xv+1)$. Так как $v > 1$, то $t > x+1$, но в этом случае наибольший квадрат, меньший t^2, есть $(t - 1)^2$ и $t^2 - (t - 1)^2 > 2(x + 1) - 1 = 2x + 1$, поэтому $\neg Sq(t^2 - 2x - 1)$. Следовательно предположение неверно, а значит $v = 1$ и $y = x^2$. □

Очевидным следствием из полученного результата является тот факт, что отношение Sq не является экзистенциально выразимым в структуре $\langle \mathbb{N}; 1, +, | \rangle$. Из формулы (3.14) и равносильности $x \mid y \wedge 1 + x \mid y + 2x + 1 \Leftrightarrow x \, {}^{S}| x + y$ получим следующее утверждение.

Следствие 3.4.3.1. *Структура* $\langle \mathbb{N}; 1, +, Sq, {}^S| \rangle$ *является* $\exists$*Def-полной.*

3.5 Некоторые результаты о выразимости для ${}^S|$ с отношением порядка и функцией следования

Естественным усилением утверждения 3.4.1 могло бы служить доказательство Def-полноты структуры $\langle \mathbb{N}; <, {}^S| \rangle$. Эта проблема выглядит труднее; укажем только некоторое достаточное условие Def-полноты и докажем выразимость в $\langle \mathbb{N}; <, {}^S| \rangle$ отношений $y = 2x$ и $y = x^2$.

Для доказательства теоремы 10 достаточно более слабого результата, чем теорема Робинсон о Def-полноте структуры $\langle \mathbb{N}; S, | \rangle$. Так как график функции следования $y = Sx$ выразим формулой $x < y \wedge \forall z(x < z \Rightarrow y = z \vee y < z)$, структура $\langle \mathbb{N}; <, | \rangle$ также Def-полна. Выразимостью $y = Sx$ будем пользоваться во всех последующих утверждениях.

Теорема 10. *Если свойство* $P_2(x) \rightleftharpoons \exists y(x = 2^y)$ *выразимо в структуре* $\langle \mathbb{N}; <, {}^S| \rangle$, *то теория* $\mathrm{Th}\langle \mathbb{N}; <, {}^S| \rangle$ *неразрешима. Если же в этой структуре выразимо отношение* $x = 2^y$, *то* $\langle \mathbb{N}; <, {}^S| \rangle$ *Def-полна.*

Доказательство. Мы воспользуемся тем фактом [20], что для всяких $\alpha > \beta \geqslant 0$, таких что $\alpha \perp \beta$ и $x > y \geqslant 0$, имеет место равенство $\mathrm{НОД}(\alpha^x - \beta^x, \alpha^y - \beta^y) = \alpha^{\mathrm{НОД}(x,y)} - \beta^{\mathrm{НОД}(x,y)}$. Получаем, что $\mathrm{НОД}(2^x - 1, 2^y - 1) = 2^{\mathrm{НОД}(x,y)} - 1$, из чего следует $\mathrm{НОД}(x,y) = x \Leftrightarrow \mathrm{НОД}(2^x - 1, 2^y - 1) = 2^x - 1$ и, таким образом

$$(2^x - 1)2^x \mid (2^y - 1)2^y \Leftrightarrow 2^x - 1 \mid 2^y - 1 \wedge 2^x \mid 2^y \Leftrightarrow x \mid y. \tag{3.15}$$

Отношение $L_1(x,y) \rightleftharpoons y = x^2 + x$ выражается формулой

$$(x = 0 \wedge y = 0) \vee \neg y = 0 \wedge x \,{}^S|y \wedge \forall z(\neg z = 0 \wedge x \,{}^S|z \Rightarrow y = z \vee y < z).$$

Делимость $x(x+1) \mid y(y+1)$ выразима с помощью формулы $\exists z(L_1(y,z) \wedge x \,{}^S|z)$. Если в структуре $\langle \mathbb{N}; <, {}^S| \rangle$ выразим предикат $x = 2^y$, то из (3.15) получаем, что $x \mid y \Leftrightarrow \exists u \exists v\,(Su = 2^x \wedge Sv = 2^y \wedge u(u+1) \mid v(v+1))$. Вторая часть теоремы теперь следует из Def-полноты $\langle \mathbb{N}; <, | \rangle$.

Теперь докажем первую часть. Для этого укажем подструктуру $\langle \mathbb{N}; <, {}^S| \rangle$, изоморфную $\langle \mathbb{N}; <, | \rangle$. Определим $A \subseteq \mathbb{N}$, отношения $y \widetilde{<} x$ и $x \widetilde{|} y$ на A, так что имеется биекция $f : \mathbb{N} \to A$, что $x < y \Leftrightarrow f(x) \widetilde{<} f(y)$ и $x \mid y \Leftrightarrow f(y) \widetilde{|} f(x)$. Из выразимости в $\langle \mathbb{N}; <, | \rangle$ отношений $x \in A$, $y \widetilde{<} x$ и $x \widetilde{|} y$ затем получим неразрешимость $\mathrm{Th}\langle \mathbb{N}; <, {}^S| \rangle$.

Пусть $A = \{2^x - 1 : x \geqslant 0\}$ и $f : x \mapsto 2^x - 1$. Тогда с помощью P_2 отношение $x \in A$ определяется формулой $\exists y(P_2(y) \wedge Sx = y)$. Видим, что $x < y \Leftrightarrow 2^x - 1 < 2^y - 1$, поэтому, если определить $x \widetilde{|} y \rightleftharpoons x(x+1) \mid y(y+1)$, то из (3.15) получим изоморфность $\langle \mathbb{N}; <, | \rangle$ и $\langle A; <, \widetilde{|} \rangle$. $\square$

Способ, с помощью которого была доказана неразрешимость элементарной теории структуры $\langle \mathbb{N}; <, P_2, {}^S | \rangle$, применяется довольно широко в тех случаях, когда затруднительно доказать Def-полноту соответствующей структуры. Например, для структуры $\langle \mathbb{N}; S, \perp \rangle$, вопрос о Def-полноте которой пока остаётся открытым, А. Вудсом [85] и Д. Ришаром [65] были независимо построены различные подструктуры, изоморфные $\langle \mathbb{N}; +, \cdot, = \rangle$. В работе П. Сигиельски, Ю.В. Матиясевича и Д. Ришара [24] вводится специальное понятие *структуры с изоморфной переинтерпретацией* (*structure with isomorphic reinterpretation property*) и предлагается пример структуры, обладающей свойством изоморфной переинтерпретации, но не являющейся Def-полной.

Если теперь обратиться к структуре $\langle \mathbb{N}; S, {}^S | \rangle$, то с помощью отношения $x \perp_2 y$, определённого в разделе 3.1, можно показать, что выразимость $y = 2^x$ в $\langle \mathbb{N}; S, {}^S | \rangle$ также влечёт Def-полноту. Так как по лемме 3.2.1 равенство выразимо в $\langle \mathbb{N}; {}^S | \rangle$, то вместо графика функции включим в структуру саму функцию возведения двойки в степень, которая будет обозначаться 2^x.

Утверждение 3.5.1. *Структура* $\langle \mathbb{N}; S, 2^x, {}^S | \rangle$ *Def-полна.*

Доказательство. Воспользуемся ещё одним результатом Д. Ришара [66] о Def-полноте $\langle \mathbb{N}; S, 2^x, \perp \rangle$. Для доказательства утверждения достаточно выразить в структуре $\langle \mathbb{N}; S, 2^x, {}^S | \rangle$ отношение взаимной простоты.

Снова используем тот факт, что $\text{НОД}(2^x - 1, 2^y - 1) = 2^{\text{НОД}(x,y)} - 1$, следствием чего является $x \perp y \Leftrightarrow 2^x - 1 \perp 2^y - 1$. Покажем, что для предиката $\perp_2$ имеет место

$$x \perp y \Leftrightarrow (x = 0 \wedge y = 1) \vee 2^{2^x - 1} - 1 \perp_2 2^{2^y} - 2 \tag{3.16}$$

для всяких неотрицательных целых чисел x и y. Тогда ввиду $y = x - 1 \Leftrightarrow \exists z(x = Sy)$ и выразимости $x \perp_2 y$ в $\langle \mathbb{N}; S, {}^S | \rangle$, получим искомое.

Пусть далее $x \neq 0$. Опустим в правой части (3.16) первый дизъюнкт и перепишем $\perp_2$ согласно определению:

$$2^{2^x - 1} - 1 \perp_2 2(2^{2^y - 1} - 1) \Leftrightarrow \text{НОД}((2^{2^x - 1} - 1)2^{2^x - 1}, 2(2^{2^y - 1} - 1)(2^{2^y} - 1)) = 2. \tag{3.17}$$

Вынесем двойку и сократим; кроме того, можно сразу избавиться от степени 2 в первом аргументе НОД, а равенство единице НОД записать в виде $(2^{2^x - 1} - 1) \perp (2^{2^y - 1} - 1)(2^{2^y} - 1)$, что очевидно равносильно конъюнкции

$$2^{2^x - 1} - 1 \perp 2^{2^y - 1} - 1 \wedge 2^{2^x - 1} - 1 \perp 2^{2^y} - 1.$$

Дважды воспользуемся упомянутым выше фактом и получим $x \perp y \wedge 2^x - 1 \perp 2^y$, из чего следует истинность утверждения. □

Не известно, выразимо ли отношение $y = 2^x$ в структуре $\langle \mathbb{N}; S, {}^S | \rangle$ или хотя бы P_2 в $\langle \mathbb{N}; <, {}^S | \rangle$. Утверждения 3.5.2 и 3.5.3 могут оказаться полезными при построении формул, выражающих эти отношения в последней структуре.

Утверждение 3.5.2. *Отношение $y = 2x$ выразимо в структуре $\langle \mathbb{N}; <, {}^{S}| \rangle$.*

Доказательство. Если в определении L_1 из теоремы 10 обозначить $M_0(x,y) \rightleftharpoons \neg y = 0$, то

$$L_1(x,y) \Leftrightarrow (x = 0 \wedge y = 0) \vee M_0(x,y) \wedge \forall z(M_0(x,z) \wedge x\,{}^{S}|z \Rightarrow y = z \vee y < z).$$

Теперь можем определить $L_k(x,y) \rightleftharpoons y = kx^2 + kx$ последовательно для индексов $k = 2,3,4$ с помощью формул

$$L_k(x,y) \Leftrightarrow (x = 0 \wedge y = 0) \vee M_{k-1}(x,y) \wedge \forall z(M_{k-1}(x,z) \wedge x\,{}^{S}|z \Rightarrow y = z \vee y < z),$$

где $M_{k-1}(x,y) \rightleftharpoons M_{k-2}(x,y) \wedge \neg L_{k-1}(x,y)$. Отсюда очевидным образом выразимо $y = (2x+1)^2$, а отношение $x > 0 \wedge y = (2x-1)^2$ задаётся экзистенциальной формулой $\exists z \exists t(Sz = x \wedge L_4(z,t) \wedge y = St)$.

Следующая формула определяет искомый предикат:

$$\begin{aligned} y = 2x \Leftrightarrow (x = 0 \wedge y = 0) \vee \exists z_1 \exists z_2 \exists z_3 \exists z_4 \big(& x > 0 \\ & \wedge z_1 = (2x-1)^2 \wedge z_2 = y(y-1) \\ & \wedge z_3 = y(y+1) \wedge z_4 = (2x+1)^2 \\ & \wedge z_1 < z_2 \wedge z_3 < z_4 \big). \end{aligned}$$

Выражение в правой части требует $y \geqslant 2x \wedge y \leqslant 2x$. □

Следующая лемма послужит при доказательстве выразимости графика возведения в квадрат в структуре $\langle \mathbb{N}; <, {}^{S}| \rangle$.

Лемма 3.5.1. *Отношение $y = x(x+1)(x+2)(x+3)$ выразимо в структуре $\langle \mathbb{N}; <, {}^{S}| \rangle$.*

Доказательство. Если $y \neq 0$ удовлетворяет $x\,{}^{S}|y \wedge SSx\,{}^{S}|y$, то несложно заметить, что при условии $3 \mid x$, $y = \frac{k}{6}x(x+1)(x+2)(x+3)$, а при $3 \nmid x$, получаем $y = \frac{k}{2}x(x+1)(x+2)(x+3)$ для некоторого $k \in \mathbb{N}$.

Выразим сначала свойство $3 \mid x$. С помощью $x = 0$ и S, мы можем определить $6 \mid x \Leftrightarrow \exists y(y = 0 \wedge SSy\,{}^{S}|x)$. Тогда $3 \mid x \Leftrightarrow 6 \mid x \vee 6 \mid SSSx$.

Следуя той же схеме, что и в утверждении 3.5.2, определяем

$$S_1(x,y) \Leftrightarrow \neg y = 0 \wedge x\,{}^{S}|y \wedge SSx\,{}^{S}|y \wedge \forall z(\neg z = 0 \wedge x\,{}^{S}|z \wedge SSx\,{}^{S}|z \Rightarrow y \leqslant z),$$

и далее, для $i = 2,...,6$ последовательно конъюнктивно добавляем в формулу и в посылку импликации в подкванторном выражении $\neg S_{i-1}(x,y)$ и $\neg S_{i-1}(x,z)$ соответственно. Таким образом выражаем отношения «y является i-ым положительным целым числом, которое делится на $x(x+1)(x+2)(x+3)$». В итоге получаем

$$y = x(x+1)(x+2)(x+3) \Leftrightarrow (x = 0 \wedge y = 0) \vee (3 \mid x \wedge S_6(x,y)) \vee (3 \nmid x \wedge S_2(x,y)).$$

□

Утверждение 3.5.3. *Отношение $y = x^2$ выразимо в структуре $\langle \mathbb{N}; <, {}^{S}| \rangle$.*

Доказательство. Покажем, что имеет место следующее определение:

$$\begin{aligned} y = x^2 \Leftrightarrow\ & (x = 0 \wedge y = 0) \vee (x = 1 \wedge y = 1) \vee (x = 2 \wedge y = 4) \\ & \vee\Big(x > 2 \wedge y > 2 \wedge \forall z\big(z = y(y-1) \Rightarrow x\,{}^{S}|z \wedge x - 1\,{}^{S}|z \wedge \\ & \wedge (x-2)(x-1)x(x+1) < z \wedge z < (x-1)x(x+1)(x+2)\big)\Big). \end{aligned} \tag{3.18}$$

Заключение импликации в подкванторном выражении должно быть верно тогда и только тогда, когда $z = x^2(x^2-1)$. Для этого требуем делимость z на $x-1$,x,$x+1$ и заключаем z в интервал от $x^2(x^2-1) - 2x(x^2-1)$ до $x^2(x^2-1) + 2x(x^2-1)$.

Ясно, что $y = x^2$ удовлетворяет формуле, покажем, что иные значения x и y принимать не могут.

Пусть x,$y \geqslant 3$. Если $x\,{}^{S}|z \wedge x-1\,{}^{S}|z$, то $z = \frac{k}{2}(x-1)x(x+1)$, поэтому получаем $(x-2) < \frac{k}{2} < x+2$. Следовательно, имеются три возможности: $z = (x-1)^2x(x+1)$, $z = (x-1)x^2(x+1)$ и $z = (x-1)x(x+1)^2$.

Предположим, что $y > x^2$. Если $z = y(y-1)$, то $z > x^2(x^2-1)$, и остаётся только возможность $y(y-1) = (x-1)x(x+1)^2 = (x^2-1)(x^2+x)$. Так как ясно, что $y < x^2 + x$, положим $y = x^2 + k$ для некоторого $k \in [1,x-1]$. Следовательно, имеет место делимость $x^2 - 1 \mid (x^2+k)(x^2+k-1)$, которую можно переписать следующим образом:

$$(x^2+k)(x^2+k-1) \equiv (k+1)k \equiv 0 \,(\mathrm{mod}\ x^2-1).$$

Теперь видим, что такое число k не существует, так как из определения k и ограничения $x \geqslant 3$ получаем цепочку неравенств $0 < k(k+1) \leqslant x(x-1) < x^2 - 1$.

Если теперь $y < x^2$, то для $z = y(y-1)$ имеется единственная возможность $y(y-1) = (x-1)^2x(x+1) = (x^2-x)(x^2-1)$, из чего следует $y > x^2 - x$. Снова положим $y = x^2 - k$ для некоторого $k \in [1,x-1]$ и получим

$$(x^2-k)(x^2-k-1) \equiv (k-1)k \equiv 0 \,(\mathrm{mod}\ x^2-1).$$

Если $k = 1$, то исходное равенство имеет вид $(x^2-1)(x^2-2) = (x^2-1)(x^2-x)$, поэтому либо $x = 1$, либо $x = 2$, но эти случаи нами исключены. Если же $k > 1$, то $0 < k(k-1) < x^2 - 1$, из чего следует отсутствие таковых k и y, что и завершает доказательство утверждения. $\square$

Заключение

По существу, самыми ценными результатами диссертации являются НОД-лемма и понятие алгоритма квазиэлиминации кванторов из первой главы, а основные результаты из глав 1 и 2 получены с использованием этих инструментов. В то время как глава 3 раскрывает с точки зрения вопросов выразимости и разрешимости некоторые связи между целочисленной делимостью и делимостью на два последовательных целых числа, в главе 3 используются стандартные методы, и все результаты выглядят вполне предсказуемыми.

Определённую трудность составляло нахождение удобной формулировки для четвертого условия НОД-леммы, так как эту лемму было легче доказать, используя ((iv)), тогда как в приложениях мы всегда используем (iv). Помимо этого, условия (i) и (ii) являются отголоском китайской теоремы об остатках, хотя иногда удобнее (как, например, в алгоритме квази-ЭК $\mathcal{C}$ из утверждения 2.6.2) заменить три условия (i), (ii) и (iii) на единственное условие ((iii)) для каждого $i,j \in [1..m]$. В целом, кажется неожиданным, что такое обобщение китайской теоремы об остатках существует и, кроме того, что его можно применять для решения различных задач выразимости и разрешимости. Результаты раздела 2.6 были получены, когда глава 1 была закончена. Аналогично алгоритму квази-ЭК $\mathcal{C}$, шаг 2 алгоритма $\mathcal{R}$ может быть преобразован таким образом, что он будет ещё "ближе" к элиминации кванторов. То есть, используя бинарный функциональный символ НОД, можно добиться введения меньшего числа греческих переменных (или даже не вводить их вообще). В то же время вспомогательные греческие переменные значительно упрощают вид нод-выражений, что позволяет в свою очередь упростить рассуждения о формулах с нод-выражений такого вида.

Доказательство БЛ-теоремы из Книги [11, Preface], по-видимому, также должно предоставлять описание всех P∃-выразимых отношений. В теореме 5 эта проблема решается для случая, когда отношение порядка исключено из структуры, а делимость заменена взаимной простотой. Среди промежуточных структур наиболее важными видятся следующие: $\langle \mathbb{Z}; 1, +, -, \leqslant, \perp \rangle$ и $\langle \mathbb{Z}; 1, +, -, | \rangle$. Для второй структуры может оказаться полезным результат П. Сигиельски [23], который применил теоретико-модельные методы, чтобы доказать существование алгоритма элиминации кванторов для некоторого расширения структуры $\langle \mathbb{Z}_{>0}; | \rangle$ предикатами, выразимыми в этой структуре. Заметим, что в нашем случае достаточно рассмотреть только P∃-выразимые отношения. Решение любой из этих задач о P∃-выразимости дало бы нам новый разрешимый фрагмент ∀∃-теории структуры $\langle \mathbb{Z}; 1, +, -, \leqslant, | \rangle$. Таким образом, результаты из теоремы 7 и следствия 4.1 могут оказаться двумя частными случаями одного разрешимого фрагмента.

Вопрос Дж. Робинсон о разрешимости $\exists\mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leqslant, |, P_2 \rangle$ задаёт основное направление дальнейших исследований. Л. ван ден Дрисом (см. [62]) было предложено теоретико-модельное доказательство факта существования алгоритма элиминации кванторов в некотором расширении структуры $\langle \mathbb{N}; 1, +, \leqslant, P_2 \rangle$ функциями, графики которых выразимы в этой структуре. Для наших целей важно построить такой алгоритм в явном виде или, по крайней мере, построить алгоритм квази-ЭК для экзистенциальной теории

этой структуры. Далее, если надеяться получить утвердительный ответ на обобщение проблемы Робинсон, сформулированное в разделе 2.7, следует сначала рассмотреть проблему разрешимости для теории $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leqslant,P_2,P_3,P_4,...\rangle$ (отметим, что вопрос о разрешимости $\mathrm{Th}\langle\mathbb{N};1,+,\leqslant,P_2,P_3\rangle$ всё ещё является открытым [13]). Впрочем, эти вопросы уже далеко уходят от основной темы диссертации, и о возможных направлениях дальнейших исследований теперь сказано достаточно.

Список литературы

1. *Бельтюков, А. П.* Разрешимость универсальной теории натуральных чисел со сложением и делимостью // Записки научных семинаров ЛОМИ. — 1976. — Т. 60. — С. 15—28.
2. *Бельтюков, А. П.* К юбилею Юрия Владимировича Матиясевича // Компьютерные инструменты в образовании. — 2017. — № 6. — С. 5—11.
3. *Верещагин, Н. К., Шень, А.* Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. — Москва : МЦНМО, 2012. — 240 с. — 4-е изд., испр.
4. *Косовский, Н. К.* О решении систем, состоящих одновременно из уравнений в словах и неравенств в длинах слов // Записки научных семинаров ЛОМИ. — 1974. — Т. 40. — С. 24—29.
5. *Мартьянов, В. И.* Универсальные расширенные теории целых чисел // Алгебра и логика. — 1977. — Т. 16, № 5. — С. 588—602.
6. *Матиясевич, Ю. В.* Диофантовость перечислимых множеств // Доклады АН СССР. — 1970. — Т. 191, № 2. — С. 278—282.
7. *Матиясевич, Ю. В.* Десятая проблема Гильберта. — Москва : Физматлит, 1993.
8. *Семёнов, А. Л.* О некоторых расширениях арифметики сложения натуральных чисел // Изв. АН СССР. Сер. матем. — 1979. — Т. 43, № 5. — С. 1175—1195.
9. *Семёнов, А. Л.* Логические теории одноместных функций на натуральном ряде // Изв. АН СССР. Сер. матем. — 1983. — Т. 47, № 3. — С. 623—658.
10. *Старчак, М. Р.* Некоторые проблемы разрешимости и выразимости для предиката делимости на два последовательных числа // Компьютерные инструменты в образовании. — 2018. — Дек. — № 6. — С. 5—15.
11. *Aigner, M., Ziegler, G. M.* Proofs from THE BOOK. — Springer Berlin Heidelberg, 2010.
12. *Backeman, P., Rümmer, P., Zeljić, A.* Interpolating bit-vector formulas using uninterpreted predicates and Presburger arithmetic // Formal Methods in System Design. — 2021. — May.
13. *Bès, A.* A survey of arithmetical definability // Société mathématique de Belgique. — 2002. — P. 1—54.
14. *Borosh, I., Treybig, L. B.* Bounds on positive integral solutions of linear diophantine equations // Proceedings of the American Mathematical Society. — 1976. — Vol. 55. — P. 299—304.
15. *Bozga, M., Iosif, R.* On decidability within the arithmetic of addition and divisibility // Proceedings of FoSSaCS, ser. Lecture Notes in Computer Science. Vol. 3441. — 2005. — P. 425—439.

16. *Bozga, M., Iosif, R.* On flat programs with lists // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2007. — P. 122—136.

17. *Bozga, M., Iosif, R., Lakhnech, Y.* Flat parametric counter automata // Fundamenta Informaticae. — 2009. — Vol. 91. — P. 275—303.

18. *Büchi, J. R.* Weak second-order arithmetic and finite automata // Zeitschrift für Mathematische Logik und Grundlagen der Mathematik. — 1960. — Vol. 6, no. 1—6. — P. 66—92.

19. *Bundala, D., Ouaknine, J.* On parametric timed automata and one-counter machines // Information and Computation. — 2017. — Vol. 253. — P. 272—303.

20. *Carmichael, L.* On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$ // Ann. Math. — 1913. — Vol. 15, no. 2. — P. 30—69.

21. *Carneiro, M.* A Lean formalization of Matiyasevič's theorem // arXiv:1802.01795v1. — 2018. — Feb. — arXiv: 1802.01795v1 [math.LO].

22. *Cégielski, P.* Théorie élémentaire de la multiplication des entiers naturels // Lecture Notes in Mathematics. — Springer Berlin Heidelberg, 1981. — P. 44—89.

23. *Cégielski, P.* La théorie élémentaire de la divisibilité est finiment axiomatisable // Comptes rendus de l'Académie des sciences. Série I, Mathématique. — 1984. — Vol. 299. — P. 367—369.

24. *Cégielski, P., Matiyasevich, Y., Richard, D.* Definability and decidability issues in extensions of the integers with the divisibility predicate // The Journal of Symbolic Logic. — 1996. — Vol. 61, no. 2. — P. 515—540.

25. *Cégielski, P., Richard, D.* In memoriam of Alan Robert Woods // New Studies in Weak Arithmetics, Lecture Notes 211 / ed. by P. Cégielski, C. Cornaros, C. Dimitracopoulos. — CSLI Publications, Stanford, 2013. — P. 15—31.

26. *Cooper, D. C.* Theorem proving in arithmetic without multiplication // Machine intelligence. — 1972. — Vol. 7, no. 91—99. — P. 300.

27. *Degtyarev, A., Matiyasevich, Y., Voronkov, A.* Simultaneous rigid E-unification and related algorithmic problems // Proceedings 11th Annual IEEE Symposium on Logic in Computer Science. — IEEE Comput. Soc. Press, 1996.

28. *Degtyarev, A., Voronkov, A.* Simultaneous rigid E-unification is undecidable // Computer Science Logic. — Springer Berlin Heidelberg, 1996. — P. 178—190.

29. *Dolzmann, A., Seidl, A., Sturm, T.* Redlog user manual, edition 3.0 // Tech. Rep., University of Passau. — 2004. — URL: http://andreasseidl.com/publications/DSS04b.pdf.

30. *Dolzmann, A., Sturm, T.* REDLOG: computer algebra meets computer logic // ACM SIGSAM Bulletin. — 1997. — June. — Vol. 31, no. 2. — P. 2—9.

31. *Dries, L. van den, Wilkie, A.* The laws of integer divisibility, and solution sets of linear divisibility conditions // The Journal of Symbolic Logic. — 2003. — Vol. 68, no. 2. — P. 503—526.

32. Emptiness problems for integer circuits / D. Barth [et al.] // Electronic Colloquium on Computational Complexity. — 2017. — No. 12. — URL: https://eccc.weizmann.ac.il/report/2017/012/ ; Article Number: TR17-012.

33. *Garey, M. R.*, *Johnson, D. S.* Computers and intractability. A guide to the theory of NP-completeness. — NY, USA : W. H. Freeman, Co., 1979.

34. *Gathen, J. von zur*, *Sieveking, M.* Bounds on positive integral solutions of linear diophantine equations // Proceedings of the American Mathematical Society. — 1978. — Vol. 72. — P. 155—158.

35. *Graham, R.*, *Knuth, D.*, *Patashnik, O.* Concrete mathematics. A foundation for computer science. — Reading : Addison-Wesley, 1989.

36. *Guépin, F.*, *Haase, C.*, *Worrell, J.* On the exitential theories of Büchi arithmetic and linear p-adic fields // Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). — 2019. — P. 1—10. — (LICS '19).

37. *Haase, C.* On the complexity of model checking counter automata : Ph.D. Thesis. — University of Oxford, 2012.

38. *Haase, C.* A survival guide to Presburger arithmetic // ACM SIGLOG News. — 2018. — July. — Vol. 5, no. 3. — P. 67—82.

39. *Haase, C.*, *Mansutti, A.* On deciding linear arithmetic constraints over p-adic integers for all primes //. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

40. *Haase, C.*, *Różycki, J.* On the expressiveness of Büchi arithmetic // Lecture Notes in Computer Science. — Springer International Publishing, 2021. — P. 310—323.

41. *Hodgson, B. R.* On direct products of automaton decidable theories // Theoretical Computer Science. — 1982. — Sept. — Vol. 19, no. 3. — P. 331—335.

42. *Iwane, H.*, *Yanami, H.*, *Anai, H.* SyNRAC: A toolbox for solving real algebraic constraints // Mathematical Software – ICMS 2014. — Springer Berlin Heidelberg, 2014. — P. 518—522.

43. *Knuth, D. E.* The art of computer programming, Volume 4A, The: Combinatorial Algorithms, Part 1. — 1st. — Boston, MA : Addison-Wesley Professional, 2011.

44. *Korec, I.* A list of arithmetical structures complete with respect to the first-order definability // Theoretical Computer Science. — 2001. — Vol. 257, no. 1/2. — P. 115—151.

45. *Larchey-Wendling, D.*, *Forster, Y.* Hilbert's tenth problem in Coq // arXiv:2003.04604. — 2020. — Mar. — arXiv: 2003.04604 [cs.LO].

46. *Lasaruk, A.*, *Sturm, T.* Weak quantifier elimination for the full linear theory of the integers // Applicable Algebra in Engineering, Communication and Computing. — 2007. — Oct. — Vol. 18, no. 6. — P. 545—574.

47. *Lasaruk, A.*, *Sturm, T.* Effective quantifier elimination for Presburger arithmetic with infinity // Computer Algebra in Scientific Computing. — Springer Berlin Heidelberg, 2009. — P. 195—212.

48. *Lechner*, *A.* Synthesis problems for one-counter automata // Lecture Notes in Computer Science. — Springer International Publishing, 2015. — P. 89—100.

49. *Lechner*, *A.* Extensions of Presburger arithmetic and model checking one-counter automata : Ph.D. Thesis. — Oriel College University of Oxford, 2016.

50. *Lechner*, *A.*, *Ouaknine*, *J.*, *Worrell*, *J.* On the complexity of linear arithmetic with divisibility // 30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2015, Kyoto, Japan, July 6-10, 2015. — IEEE Computer Society, 2015. — P. 667—676. — URL: http://dx.doi.org/10.1109/LICS.2015.67.

51. *Lipshitz*, *L.* The diophantine problem for addition and divisibility // Trans. Amer. Math. Soc. — 1978. — Vol. 235. — P. 271—283.

52. *Lipshitz*, *L.* Some remarks on the diophantine problem for addition and divisibility // Bulletin de la Société mathématique de Belgique. Série B. — 1981. — Vol. 33, no. 1. — P. 41—52.

53. *Lipshitz*, *L.* Quadratic forms, the five square problem, and diophantine equations // The collected works of J. Richard Büchi / ed. by S. MacLane, D. Siefkes. — Springer, 1990. — P. 677—680.

54. Logic and p-recognizable sets of integers / V. Bruyère [et al.] // Bulletin of the Belgian Mathematical Society - Simon Stevin. — 1994. — Jan. — Vol. 1, no. 2.

55. *Loos*, *R.*, *Weispfenning*, *V.* Applying linear quantifier elimination // The Computer Journal. — 1993. — May. — Vol. 36, no. 5. — P. 450—462.

56. *Manders*, *K.*, *Adleman*, *L.* NP-Complete decision problems for binary quadratics // Journal of Computer and System Sciences. — 1978. — Vol. 16, no. 2. — P. 168—184.

57. *Mostowski*, *A.* On direct products of theories // The Journal of Symbolic Logic. — 1952. — Vol. 17, no. 1. — P. 1—31.

58. *Moura*, *L. de*, *Bjørner*, *N.* Z3: An efficient SMT solver // Tools and Algorithms for the Construction and Analysis of Systems. — Springer Berlin Heidelberg, 2008. — P. 337—340.

59. *Nipkow*, *T.* Linear quantifier elimination // Journal of Automated Reasoning. — 2010. — July. — Vol. 45, no. 2. — P. 189—212.

60. *Pasten*, *H.*, *Pheidas*, *T.*, *Vidaux*, *X.* A survey on Büchi's problem: new presentations and open problems // Zap. Nauchn. Sem. POMI. — 2010. — Vol. 377. — P. 111—140.

61. *Pérez*, *G. A.*, *Raha*, *R.* Revisiting parameter synthesis for one-counter automata. — 2021. — arXiv: 2005.01071 [cs.LO].

62. *Point*, *F.* On the expansion $(\mathbb{N}, +, 2^x)$ of Presburger arithmetic // preprint. — 2007. — URL: http://www.logique.jussieu.fr/~point/papiers/Pres.pdf.

63. *Presburger*, *M.* Über die vollständigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchem die addition als einzige operation hervortritt // Comptes Rendus du I congrès de Mathématiciens des Pays Slaves. — 1929. — P. 92—101.

64. Reachability in succinct and parametric one-counter automata / C. Haase [et al.] // CONCUR 2009 - Concurrency Theory. — Springer Berlin Heidelberg, 2009. — P. 369—383.

65. *Richard*, *D.* La théorie sans égalité du successeur et de la coprimarité des entiers naturels est indécidable. Le prédicat de primarité est définissable dans le langage de cette théorie // Comptes Rendus de l'Académie des Sciences. Série I: Mathématique. — 1982. — Vol. 294. — P. 143—146.

66. *Richard*, *D.* All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate // Discrete Mathematics. — 1985. — Vol. 53. — P. 221—247.

67. *Richard*, *D.* Definability in terms of the successor function and the coprimeness predicate in the set of arbitrary integers // The Journal of Symbolic Logic. — 1989. — Vol. 54, no. 4. — P. 1253—1287.

68. *Richard*, *D.* What are weak arithmetics? // Theoretical Computer Science. — 2001. — Vol. 257. — P. 17—29.

69. *Robinson*, *J.* Definability and decision problems in arithmetic // The Journal of Symbolic Logic. — 1949. — Vol. 14. — P. 98—114.

70. *Scarpellini*, *B.* Complexity of subcases of Presburger arithmetic // Transactions of the American Mathematical Society. — 1984. — Vol. 284, no. 1. — P. 203—218.

71. *Schmid*, *H. L.*, *Mahler*, *K.* On the Chinese remainder theorem // Mathematische Nachrichten. — 1958. — Vol. 18, no. 1—6. — P. 120—122.

72. *Sirokofskich*, *A.* On a weak form of divisibility // Definability and Decidability Problems in Number Theory. — 2016. — P. 2827—2829.

73. *Skolem*, *T.* Über gewisse satzfunktionen in der arithmetik // Skrifter utgit av Videnskapsselskapet i Kristiania. — 1930. — Vol. I. klasse, no. 7.

74. *Smoryński*, *C.* Logical number theory I. — Springer Berlin Heidelberg, 1991.

75. *Starchak*, *M. R.* A proof of Bel'tyukov–Lipshitz theorem by quasi-quantifier elimination. I. Definitions and GCD-Lemma // Vestnik St.Petersb. Univ. Math. — 2021. — Vol. 54, no. 3. — P. 264—272.

76. *Starchak*, *M. R.* A proof of Bel'tyukov–Lipshitz theorem by quasi-quantifier elimination. II. The main reduction // Vestnik St.Petersb. Univ. Math. — 2021. — Vol. 54, no. 4. — P. 372—380.

77. *Starchak*, *M. R.* Positive existential definability with unit, addition and coprimeness // Proceedings of the International Symposium on Symbolic and Algebraic Computation 2021 (ISSAC '21). — ACM, 07/2021. — P. 353—360.

78. *Sturm*, *T.* Linear problems in valued fields // Journal of Symbolic Computation. — 2000. — Aug. — Vol. 30, no. 2. — P. 207—219.

79. *Sturm, T.* A survey of some methods for real quantifier elimination, decision, and satisfiability and their applications // Mathematics in Computer Science. — 2017. — Apr. — Vol. 11, no. 3/4. — P. 483—502.

80. *Sturm, T.* Thirty years of virtual substitution // Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC '18). — ACM, 07/2018.

81. The DPRM theorem in Isabelle (short paper) / J. Bayer [et al.] // 10th International Conference on Interactive Theorem Proving (ITP 2019). — Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik GmbH, Wadern/Saarbruecken, Germany, 2019.

82. *Villemaire, R.* The theory of $(\mathbb{N}; +, V_k, V_l)$ is undecidable // Theoretical Computer Science. — 1992. — Dec. — Vol. 106, no. 2. — P. 337—349.

83. *Weispfenning, V.* The complexity of linear problems in fields // Journal of Symbolic Computation. — 1988. — Vol. 5, no. 1/2. — P. 3—27.

84. *Weispfenning, V.* Mixed real-integer linear quantifier elimination // International Symposium on Symbolic and Algebraic Computation 1999 (ISSAC '99). — ACM Press, 1999. — P. 129—136.

85. *Woods, A.* Some problems in logic and number theory : Ph.D. Thesis. — University of Manchester, 1981.