Integer divisibility on $\mathbb{Q}$, quantifier elimination and one Weispfenning's remark

Mikhail R. Starchak

Abstract. In 1999 V. Weispfenning presented a quantifier elimination procedure for the elementary theory of the structure $\left\langle \mathbb{R}; 0, 1, +, -, [\,], =, <, \{n\,|\}_{n\in\mathbb{N}} \right\rangle$, where $[\,]$ is the unary integer part operation, and therefore proved decidability of this theory. For the integer divisibility relation $x \mid y \Leftrightarrow \exists z(Int(z) \wedge y = z \cdot x)$ on $\mathbb{R}$, he proved undecidability of the elementary theory of the structure $\langle \mathbb{R}; 0, 1, +, -, [\,], =, <, | \rangle$ and that the theory does not admit quantifier elimination. As a remark, Weispfenning asked whether the positive existential theory of the same structure is decidable.

A decidability proof for this existential theory is the first result of this note. We also sketch a proof of the fact that for every positive existential formula of the first-order language with the signature $\left\langle 0, 1, +, -, \{c\cdot\}_{c\in\mathbb{Q}}, =, \neq, \perp \right\rangle$ there is an equivalent in the rationals $\mathbb{Q}$ quantifier-free formula of the same language. Here $c\cdot$ is a unary functional symbol for multiplication by a rational constant c and $x \perp y \Leftrightarrow Int(x) \wedge Int(y) \wedge GCD(x, y) = 1$.

Introduction

Let L_{PrA} be the first-order language of the signature $\langle 0, 1, +, -, =, <, 2\,|, 3\,|, 4\,|, ...\rangle$. V. Weispfenning [4] considered a natural generalization of Presburger Arithmetic (PrA) and proved that after adjoining the unary integer part operation $[\,]$ to the signature of L_{PrA} (this extended language was named L'), for every positive existential formula we can construct an equivalent in the real numbers $\mathbb{R}$ positive quantifier-free formula [4, Theorem 3.1]. As a corollary, we get decidability of the elementary theory of the structure $\langle \mathbb{R}; 0, 1, +, -, [\,], =, <, 2\,|, 3\,|, 4\,|, ...\rangle$ and also a characterization of the relations, definable in this structure.

If we introduce unary functional symbols $c\cdot$ for multiplication by rational constants c, we get a quantifier elimination procedure for the elementary theory of the structure $\left\langle \mathbb{R}; 0, 1, +, -, [\,], \{c\cdot\}_{c\in\mathbb{Q}}, =, < \right\rangle$. The corresponding language was named L'' and let σ'' be the signature of this language. Then V. Weispfenning writes: «By way of contrast, quantifier elimination definitely breaks down if one admits scalar multiplication by a real parameter or integer divisibility in the language. In the latter case the elementary theory of real is in fact undecidable». Simultaneously with the integer divisibility $x \mid y \Leftrightarrow \exists z(Int(z) \wedge y = z \cdot x)$ it was also considered the relation $x \parallel y \rightleftharpoons Int(x) \wedge Int(y) \wedge x \mid y$. For the structures $\langle \mathbb{R}; 0, 1, +, -, [\,], =, | \rangle$ and $\langle \mathbb{R}; 0, 1, +, -, [\,], =, \| \rangle$ he proved undecidablity of the elementary theories and decidability of the existential theory of the first structure (it follows from the the Bel'tyukov-Lipshitz theorem [1, 2]). After this proof there is a remark saying that «We do not know whether a corresponding theorem holds in the analogous language L'_{div}», where L'_{div} is the first-order language of the signature $\langle 0, 1, +, -, [\,], =, | \rangle$. We prove that the theory is decidable in section 1.

If we assume that $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$, then for rational numbers x and y their coprimeness means that these numbers are coprime integers. The elementary theory of the structure $\langle \mathbb{Q}; \sigma \rangle$ admits quantifier elimination (see [4, Corollary 3.5]). Extend σ'' by the coprimeness relation $\perp$ and dis-equality $\neq$; exclude the order relation and the integer part operation. Denote the resulting signature $\sigma_\perp$. In section 2 we sketch the proof of the fact that for every positive existential $L_{\sigma_\perp}$-formula there is an equivalent in $\mathbb{Q}$ quantifier-free $L_{\sigma_\perp}$-formula. Note that $\langle \mathbb{Q}; \sigma_\perp \rangle$ has undecidable elementary theory as a corollary of the undecidability result for the elementary theory of the structure $\langle \mathbb{Z}; 0, 1, +, -, =, \perp \rangle$ proved by D. Richard in [3].

1. One Weispfenning's remark

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

Proof. To prove the theorem we reduce it to the decidable positive existential theory of the structure $\langle \mathbb{Q}; 0, 1, +, -, =, <, | \rangle$. Its decidability follows from Bel'tyukov-Lipshitz theorem on decidability of $\exists \mathrm{Th} \langle \mathbb{Z}; 1, +, <, | \rangle$. In the first step of the proof we apply some syntactic transformations of a given formula. For example, using the formula $y = \left[\frac{y}{x}\right] x + \left\{\frac{y}{x}\right\} x$ we can define $x \nmid y$ by a positive existential formula in $\langle \mathbb{R}; 0, 1, +, -, =, <, | \rangle$. Then we have to prove that this formula is true in $\mathbb{R}$ iff it is true in $\mathbb{Q}$.

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 in $\mathbb{R}$, where $\overline{x}$ is a list of variables $x_1, ..., x_n$; $g_i(\overline{x})$ for $i \in [1..m]$ and $f_j(\overline{x})$ for $j \in [k+1..l]$ are linear polynomials with integer coefficients.

Suppose this formula is true for some real values $\alpha_1, ..., \alpha_n$. Then let for $i = k{+}1..k'$ we have $g_i(\alpha_1, ..., \alpha_n) = 0$ and $g_j(\alpha_1, ..., \alpha_n) \neq 0$ for every $j \in [k'{+}1..l]$.

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 equations with integer coefficients $\bigwedge_{i=1..k'} g_i(\overline{x}) = 0$. Let $A\overline{y} + b$ be a solution set of the system for some rational matrix A, rational vector b and fresh variables $\overline{y} = y_1, ..., y_t$. Substitute $A\overline{y} + b$ for $\overline{x}$ and get an equisatisfiable 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 get a rational solution of $\varphi'(\overline{x})$ and thus of $\varphi(\overline{x})$.

Let $\beta_1, ..., \beta_t$ be some real satisfying assignment of $\varphi''(\overline{y})$ Let also the real numbers $\{1, \gamma_1, ..., \gamma_s\}$ for some $s \leq t$ 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 $i = 1..t$, substitute $\chi_i(z_1, ..., z_s)$ for y_i in $\varphi''(\overline{y})$ and get a new formula

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

Thus for every rational satisfying assignment of the formula $\psi(\overline{z})$ one can get a rational satisfying assignment of $\varphi''(\overline{y})$, and moreover $\psi(\gamma_1, ..., \gamma_s)$ holds.

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

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

Thus every solution of the subsystem of linear inequalities $\bigwedge_{i=1..m'} \widetilde{\widetilde{g}}_i(\overline{z}) < 0$ with rational coefficients is also a solution of $\psi(\overline{z})$, and since the system is consistent in $\mathbb{R}$, there is some rational solution. □

2. Integer divisibility on $\mathbb{Q}$ and quantifier elimination

Theorem 2. *For every positive existential $L_{\sigma_\perp}$-formula one can construct an equivalent in $\mathbb{Q}$ quantifier-free $L_{\sigma_\perp}$-formula.*

As $\mathrm{GCD}(x,y)=d \Leftrightarrow \frac{x}{d} \perp \frac{y}{d}$, we can consider linear polynomials with rational coefficients in expressions of the form $\mathrm{GCD}(f(\overline{x}), g(\overline{x}))=d$, $f(\overline{x})=0$ and $f(\overline{x})\neq 0$. Elimination of an existential quantifier is based on the following lemma.

Lemma 1. *For the system $\bigwedge_{i\in[1..m]} GCD(a_i, b_i+x)=d_i$ with $a_i, b_i, d_i \in \mathbb{Q}$ and $a_i \neq 0$, $d_i > 0$ for every $i \in [1..m]$, we define for every prime p the integer $M_p = \max_{i\in[1..m]} v_p(d_i)$ 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 the system has a solution in $\mathbb{Q}$ iff the following conditions simultaneously hold:*

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

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

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

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

In our case in place of a_i and b_i there will be some linear polynomials with rational coefficients.

As a corollary, we get that the relation $x \not\perp y$ is not positively existentially definable in this structure as otherwise the theory $\mathrm{Th}\langle\mathbb{Q}; 0, 1, +, -, =, \perp\rangle$ is decidable.

Conclusion

It is natural to ask for the following generalization of both Weispfenning's main theorem and Theorem 2. How the signature $\sigma = \left\langle 0, 1, +, -, [\,], \{c\cdot\}_{c\in\mathbb{Q}}, =, <, \perp \right\rangle$ can be extended with some predicates, positively existentially definable in $\langle\mathbb{Q}; \sigma\rangle$, such that for every positive existential formula there is some equivalent in this structure quantifier-free formula?

References

[1] A. Bel'tyukov, *Decidability of the universal theory of natural numbers with addition and divisibility (in Russian)*, Zapiski Nauchnyh Seminarov LOMI, vol. 60, 1976, pp. 15-28.

[2] L. Lipshitz, *The Diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc., vol. 235, 1978, pp. 271-283.

[3] D. Richard, *Definability in Terms of the Successor Function and the Coprimeness Predicate in the Set of Arbitrary Integers*, The Journal of Symbolic Logic, vol. 54, no. 4, 1989, pp. 1253-1287.

[4] V. Weispfenning, *Mixed real-integer linear quantifier elimination*, International Symposium on Symbolic and Algebraic Computation (ISSAC), ACM Press, 1999, pp. 129-136.

Mikhail R. Starchak
Dept. of Informatics
Saint-Petersburg State University
St. Petersburg, Russia
e-mail: `mikhstark@gmail.com`