Quantifier Elimination Approach to Existential Linear Arithmetic with GCD

Mikhail R. Starchak

Saint-Petersburg State University, St. Petersburg, Russia
m.starchak@spbu.ru

Keywords: Quantifier elimination · Positive existential definability · Coprimeness · Greatest common divisor · Decidability

1 Quasi-Quantifier Elimination

In this abstract we introduce a notion of quasi-quantifier elimination algorithm and then consider two such algorithms. The first one gives us a description of all positively existentially (P$\exists$-) definable relations in the structure $\langle \mathbb{Z}; 1, +, \perp\rangle$. The second one yields a decision procedure for $\exists \mathrm{Th}\langle \mathbb{Z}; 1, +, -, \leq, \mathrm{GCD}\rangle$.

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 $L^{1,2}_\sigma$ be the first-order language with the signature σ and variables from $S_1 \cup S_2$. Denote L^1_σ and L^2_σ the first-order languages with the signature σ and variables from S_1 and S_2, respectively.

Definition 1. *Let $\langle M; \sigma\rangle$ be some structure with a signature σ, and we have some decidable set of existential formulas $L \subset L^{1,2}_\sigma$ 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 $[\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j}, \overline{\alpha})]^{\widetilde{x}_j}_x \in L^x$.*

Step 2. *Transformation of every $\exists x\exists\overline{\alpha}\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$, 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 $\exists\overline{\alpha}\varphi(\overline{y}, \overline{\alpha})$, where $\overline{y} = y_1, ..., y_k$, it first applies Step 1 and then Step 2 to every formula $\exists x\, [\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j}, \overline{\alpha})]^{\widetilde{x}_j}_x$. Thus we obtain 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*** *$\mathcal{A}$.*

2 Positive Existential Definability with Unit, Addition and Coprimeness

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 $\varphi(\overline{x},\overline{y})$.

Let $\mathcal{A}$ be a quasi-QE algorithm for $L_\mathcal{A}$ in $\langle M;\sigma\rangle$. If S_2 is the empty sort of variables and $L^x_\mathcal{A} = L_\mathcal{A}$ (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 $\langle M;\sigma\rangle$. Using such kind of quasi-QE algorithm, in [4] we obtained a characterization of all relations, which are P∃-definable in the structure $\langle\mathbb{Z};1,+,\perp\rangle$.

The main elimination tool is a generalization of the Chinese remainder theorem to systems of the form

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

The following lemma is proved in [5].

Lemma 1. *For the system (1) with $a_i, b_i, d_i \in \mathbb{Z}$, $a_i \neq 0$, $d_i > 0$ 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 (1) has a solution in $\mathbb{Z}$ iff the following conditions simultaneously hold:*

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

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

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

(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 $v_p(b_i - b_j) > M_p$.

Let $L_\mathcal{A}$ be the set of positive quantifier-free (PQF-) formulas of the first-order language of the signature $\sigma = \langle 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, ...\rangle$. Here GCD_d for every $d \geq 2$ is a binary predicate symbol such that $\mathrm{GCD}_d(x, y) \rightleftharpoons \mathrm{GCD}(x, y) = d$. Applying Lemma 1, we can construct Step 2 of quasi-QE algorithm $\mathcal{A}$ and thus prove that every relation, P∃-definable in $\langle\mathbb{Z};\sigma\rangle$ is also PQF-definable in this structure.

Since it is not difficult to prove P∃-definability in the structure $\langle\mathbb{Z};1,+,\perp\rangle$ of the relations $x = 0$, $y = -x$, $x = y$, $x \neq 0$, $x \neq y$, and $\mathrm{GCD}(x, y) = d$ for every integer $d \geq 2$, we obtain the following theorem.

Theorem 1. *A relation is P∃-definable in the structure $\langle\mathbb{Z};1,+,\perp\rangle$ if and only if it is PQF-definable in the structure $\langle\mathbb{Z};1,+,-,\neq,\perp,\mathrm{GCD}_2,\mathrm{GCD}_3,\mathrm{GCD}_4,...\rangle$.*

Having such a description, we can now reason about P∃-(un)definability in $\langle\mathbb{Z};1,+,\perp\rangle$. For example, Theorem 1 and D. Richard's undecidability result [3] for the elementary theory of this structure imply that the relation $x \not\perp y$ is not P∃-definable in $\langle\mathbb{Z};1,+,\perp\rangle$.

3 A New Proof of Bel'tyukov-Lipshitz Theorem

A.P. Bel'tyukov [1] and L. Lipshitz [2] proved decidability of $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leq,|\rangle$ by reduction to the existential linear theory of the p-adic integers with divisibility $x \text{ div } y \rightleftharpoons v_p(x) \leq v_p(y)$. It is not difficult to see that we can consider the graph of the GCD function instead of divisibility, since the decision problems for these theories are inter-reducible. We will now sketch a quasi-QE algorithm $\mathcal{R}$ from [6], which performs a reduction to a fragment of Skolem Arithmetic with constants.

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

Let $L_\mathcal{R}$ be the set of formulas $\exists\overline{\alpha} \bigvee_{j\in J} \varphi_j(\overline{y_j},\overline{\alpha})$ for some finite index set J and formulas $\varphi_j(\overline{y},\overline{\alpha})$ of the form

$$\overline{\alpha} \geq 1 \wedge \overline{y} \geq 0 \wedge \bigwedge_{i\in[1..m_j]} \mathrm{GCD}(f_{i,j}(\overline{y},\overline{\alpha}), g_{i,j}(\overline{y},\overline{\alpha})) = h_{i,j}(\overline{y},\overline{\alpha}), \tag{2}$$

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 $f(\overline{y}), g(\overline{y}), h(\overline{y})$ are linear polynomials, ζ,η,θ are Greek variables 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 language $L^x_\mathcal{R}$ can naturally be defined such that its formulas are «prepared» for application of Lemma 1. Step 1 of $\mathcal{R}$ uses analogues of two lemmas from Lipshitz's proof, and rewriting conditions (ii) – (iv) from Lemma 1 at Step 2 will require introducing new variables. Finally we obtain the following theorem.

Theorem 2. *The decision problem for $\exists\mathrm{Th}\langle\mathbb{Z};1,+,-,\leq,\mathrm{GCD}\rangle$ is reducible to the decision problem for $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\mathrm{GCD}\rangle$, where $a\cdot$ is a unary functional symbol for multiplication by a positive integer a.*

The proof of BL-theorem now follows from the decidability of Skolem Arithmetic with constants since GCD is easily definable in $\langle\mathbb{Z}_{>0};\{a\}_{a\in\mathbb{Z}_{>0}},\cdot,=\rangle$.

References

1. Beltyukov, A.P.: Decidability of the universal theory of natural numbers with addition and divisibility. Zapiski Nauchnyh Seminarov LOMI **60**, 15–28 (1976), (in Russian)
2. Lipshitz, L.: The diophantine problem for addition and divisibility. Transactions of the American Mathematical Society **235**, 271–271 (1978)
3. Richard, D.: Definability in terms of the successor function and the coprimeness predicate in the set of arbitrary integers. The Journal of Symbolic Logic **54**(4), 1253–1287 (dec 1989)
4. Starchak, M.R.: Positive existential definability with unit, addition and coprimeness. In: Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation (ISSAC '21). pp. 353–360. ACM (jul 2021)
5. Starchak, M.R.: A proof of Bel'tyukov – Lipshitz theorem by quasi-quantifier elimination. I. Definitions and GCD-Lemma. Vestnik St.Petersb. Univ. Math. **54**(3), 264–272 (Jul 2021), to appear
6. Starchak, M.R.: A proof of Bel'tyukov – Lipshitz theorem by quasi-quantifier elimination. II. The main reduction. Vestnik St.Petersb. Univ. Math. **54**(4) (Oct 2021), to appear