Review of some problems on the complexity of simultaneous divisibility of linear polynomials

Nikolay K. Kosovskii, Mikhail Starchak

Abstract: *An introduction to the problems considering complexity of simultaneous divisibilities of values of linear polynomials is presented. Some history facts, recent results and open questions that stimulate further research are discussed.*

Keywords: *NP-completeness, existential Presburger arithmetic with divisibility, systems of divisibilities of values of linear polynomials, quadratic diophantine equations*

ACM Classification Keywords*: F.1.3 Complexity Measures and Classes, Reducibility and completeness; F.2.1 Analysis of Algorithms and Problem Complexity, Numerical Algorithms and Problems, Number-theoretic computations*

Introduction

Being defined, the notion of NP-completeness has become widely known as a synonym of practical intractability of a computational problem. There were found such problems in various fields of applied mathematics. In [Garey, Johnson, 1979] there were presented the most natural ones, among those found during the first decade after the appearance of the notion. While NP-completeness of a particular problem, encountered in algorithmist's practice, is enough for him to be sure it is impossible to solve exactly this problem effectively (in time polynomial in the length of the input), the theory of computation complexity also considers questions inspired by pure mathematics fields, such as number theory and model theory. A tight relationship between computability theory and number theory was stated in Matiyasevich's theorem on equivalence of enumerablility and diophantiness of sets and consequently undecidability of Hilbert's 10th problem ([Matiyasevich, 1970] and a textbook [Matiyasevich, 1993]). Subsequent researches were partly concentrated on the lower bound for the number of variables in diophantine equation which preserved undecidability.

From the point of view of the complexity theory the intriguing question is the complexity of deciding solvability in non-negative integers of diophantine equations in two variables. S.Smale in his "Mathematical problems for the next century" [Smale, 2000] points out on the importance of these questions in his 5th problem, independently of the famous **P**?**NP** problem (number 3 in his list).

Further researches on the existential fragments of theories of non-negative integers, weaker than for addition and multiplication (Hilbert's 10th problem), resulted in decidability of the so-called "Diophantine problem for addition and divisibility". This result, obtained independently by A.P.Bel'tyukov [Bel'tyukov, 1976] and L.Lipshitz [Lipshitz, 1976], found various applications in computer science (e.g. in [Degtyarev, etc., 1996], [Bozga, Iosif, 2005]). An expressiveness of the language makes it useful in formulation of particular problems, such as reachability problem for one-counter machines and their modifications ([Haase, 2012], [Bundala, Ouaknine, 2016]), which leads their decidability.

In the following sections we will firstly represent complexity results concerning simultaneous divisibilities of linear polynomials and then consider some sub-problems and related questions.

Definitions and complexity results for simultaneous divisibility of values of linear polynomials

The decidability of the Diophantine problem for addition and divisibility means the existence of an algorithm for recognizing every satisfiable in non-negative integers quantifier-free formula of the first order language in the signature $\langle +, 1, | \rangle$, where $|$ is a predicate symbol for the relation of divisibility of integers and $x|y$ means "x is a divisor of y". The general question is reducible to the satisfiability in non-negative integers of a linear divisibilities system, i.e. formula of the form

$$\&_{j=1}^{m}(f_i(x_1, ..., x_n) \mid g_i(x_1, ...x_n)), \tag{1}$$

where $f_i(x_1, ..., x_n)$ and $g_i(x_1, ..., x_n)$ are linear polynomials with non-negative integer coefficients.

The study of the complexity of the problem was started by L.Lipshitz in [Lipshitz, 1981] and resulted in the proof of its NP-completeness for every fixed (greater than 5) number of divisibilities in a system.

Theorem 1 ([Lipshitz, 1981]) The Diophantine problem for addition and divisibility is NP-hard (and NP-complete for every fixed number of divisibilities $m \geq 5$ in 1).

It is very important that while for every arbitrarily large but fixed number of divisibilities the problem is in the class **NP**, it is only NP-hard in the general case. This situation may be illustrated, for example, with the NP-complete problem of consistency in non-negative integers of a system of linear diophantine equations, which is closer to the practical algorithms. It appears to be in the class **P** for every fixed number of variables, that is, in some extent a tractable problem (see [Schrijver, 1986]).

There should be given some terminology remarks. The almost same problems have several names in different papers. In the decidability proof [Lipshitz, 1976] and in [Degtyarev, etc., 1996] we see "the Diophantine problem for addition and divisibility", in Russian literature "universal theory of natural numbers for addition and divisibility" as in [Bel'tyukov, 1976] or [Mart'yanov, 1977] (since a universal theory is decidable, the corresponding existential theory is also decidable). Furthermore, as "existential theory of $\langle \mathbb{N}; =, +, | \rangle$" in [Bes, 2002] and "existential Presburger arithmetic with divisibility" in the recent papers [Lechner, Ouaknine, Worrell, 2015] and [Bundala, Ouaknine, 2016]. In abbreviated form it is written as $\exists PAD$. Also, when we speak about the problem of consistency in non-negative integers of a system of linear diophantine equations, it is, in other words, the problem of satisfiability of a quantifier-free formula of Presburger arithmetic (abbreviated as $\exists PA$).

Detailed analysis of the decision procedure of L.Lipshitz was performed in [Lechner, Ouaknine, Worrell, 2015]. There was shown that for every satisfiable formula an upper bound for every assignment of variables would be doubly exponential in the length of the input. Thus, the problem belongs to the complexity class **NEXPTIME**, i.e. solvable on non-deterministic Turing machine using $2^{n^{O(1)}}$ number of steps, where n is the length of the input string with binary representation of the values of the input.

Theorem 2 ([Lechner, Ouaknine, Worrell, 2015]) The Diophantine problem for addition and divisibility ($\exists PAD$) is in the complexity class **NEXPTIME**.

With this result we have a complexity upper bound for those problems, which are reducible to the $\exists PAD$, in particular, those presented in the introduction. The exact complexity is not known and the problem of its determination remains open. It should also be noted that the existence of an instance of a problem with minimal solution in binary representation of size exponential in the length of the input, does not mean the problem is not in **NP**. For example, J.C.Lagarias in [Lagarias, 2006] shows that there are instances of the negative Pell equation (or anti-Pellian equation as it is named in the paper)

$$x^2 - dy^2 = -1 \tag{2}$$

with minimal non-negative integer solution of exponential length, while the problem is in **NP** since there exists a succinct certificate to establish solvability of the equation. Therefore, further progress can be quite a difficult task of significant importance for theoretical computer science.

Some sub-problems and related problems

Thus we know that $\exists PAD$ is NP-hard and we even do not know it is in **NP**. The corresponding algorithm is very impracticable. However, it could happen that for some applications it is sufficient to deal with sub-problems in order to state NP-completeness or the existence of a polynomial algorithm. In this section we will consider systems of divisibilities of a number by values of linear polynomials with non-negative coefficients and the opposite problem of systems of divisibilities of values of linear polynomials with non-negative coefficients by a number. There will not be any restrictions on the number of divisibilities, but on the number of non-zero coefficients in every polynomial. Proofs of some results, presented in the section, will be published in [Kosovskii, etc., 2017].

The first one could be considered as validity in positive integers of a formula of the form

$$\exists x_1 ... \exists x_n \, \&_{i=1}^{m} (K \mid f_i(x_1, ..., x_n)). \tag{3}$$

If there is no restriction on values of the variables, it will be a system of linear congruences

$$\exists x_1 ... \exists x_n \, \&_{i=1}^{m} (f_i(x_1, ..., x_n) \equiv 0 (\mathrm{mod}\, K)), \tag{4}$$

which could be solved in polynomial time in accordance with [Cohen, 1993] (section 2.3.4). If the variables will take their values from the interval of positive integers $[D, D']$, $0 < D \leq D' < K$, the problem is obviously in **NP**. This problem is NP-complete for every $K > 2$ (if $K = 2$ the problem is trivially in the class **P**) and exactly three non-zero coefficients of the variables in each polynomial (in [Kosovskii, etc., 2017]).

Since we are interested mainly in the number of non-zero coefficients, it will be convenient to use some abbreviations. Let $\bar{x} = (x_1, ..., x_n)$ be the list of variables of a formula and let in this case the fact that there are not greater than k non-zero coefficients in a polynomial be written down as ${}^{k}f_i(\bar{x})$. Thus, with this notation we have the following theorem.

Theorem 3 ([Kosovskii, etc., 2017]) The problem of satisfiability on the interval of positive integers $[D, D']$, $0 < D \leq D' < K$ of formulas of the form $\&_{i=1}^{m}(K \mid {}^{3}f_i(\bar{x}))$ is NP-complete for every $K \geq 3$.

From the point of view of the number of non-zero coefficients, we have the following result.

Theorem 4 ([Kosovskii, etc., 2017]) The problem of satisfiability on the interval of positive integers $[D, D']$, $0 < D \leq D' < K$ of formulas of the form $\&_{i=1}^{m}(K \mid {}^{k}f_i(\bar{x}))$ is NP-complete for every $k \geq 2$ and is in the class **P** for $k = 1$.

The case $k \geq 3$ in theorem 4 is a corollary of the Theorem 3, while for only two non-zero coefficients in each polynomial there is a polynomial reduction from GOOD SIMULTANEOUS APPROXIMATION ([Lagarias, 1982]). In his proof, J.C.Lagarias has used constructions, as he writes "inspired by Manders and Adleman" ([Manders, Adleman, 1978]). This method was introduced by K.L.Manders and L.Adleman for encoding an instance of a special case of KNAPSACK problem to an instance of solvability in non-negative integers of a quadratic diophantine equation of the form $ax^2 + by = c$ with positive integer coefficients. Possibly, the proof in [Kosovskii, etc., 2017] could be made more natural by means of polynomial reduction from 3-SAT with "conversion lemma" separately formulated in [Manders, Adleman, 1978].

For a system of divisibilities of a number on linear polynomials, the first result was achieved in [Adleman, Manders, 1977]. The problem LINEAR DIVISIBILITY (abbreviated as LD) of solvability in positive integers of one divisibility of the form $ax+1 \mid K$ was shown to be γ-complete. A problem is γ-reducible to another problem if there is a reduction procedure that can be performed in polynomial time on a non-deterministic Turing machine. Thus, a polynomial reduction is a special case of a γ-reduction. A problem is called γ-complete if it is in **NP** and every problem in **NP** is γ-reducible to it. These problems most likely are not in the class **P** nor are NP-complete; for the discussion of the notion see pages 158-160 in [Garey, Johnson, 1979].

The primary object of interest for K.L.Manders and L.Adleman was the complexity of an equivalent problem of solvability in non-negative integers of a binary quadratic equation of the form $axy + by = c$ and the study of the diophantine complexity. From this result one can conclude that simultaneous divisibility of a number by values of linear polynomials is γ-complete. By polynomial reduction from ONE-IN-THREE 3-SAT (in [Garey, Johnson, 1979]), the problem of validity in positive integers of formulas of the form

$$\exists \bar{x} \,\&_{i=1}^{m}({}^{3}f_i(\bar{x}) \mid K) \tag{5}$$

is NP-complete for every $K \geq 4$ and is in the class P for $0 < K < 4$. Though there is much more freedom for polynomial reductions for the problem

$$\exists \bar{x} \,\&_{i=1}^{m}({}^{2}f_i(\bar{x}) \mid K) \tag{6}$$

in comparison with LD, the proof of its NP-completeness does not look like obvious.

Among the references on the decidability proof of $\exists PAD$, the paper [Mart'yanov, 1977] on the decidability of the universal theory of non-negative integers for addition and D(x,y,z) predicate, true for each triplet (x,y,z) such that z=GCD(x,y), is sometimes mentioned (in [Degtyarev, etc., 1996]). As it was mentioned above, the decidability of a universal theory is equivalent to the decidability of the corresponding existential theory. This decision problem is equivalent to $\exists PAD$ because of the mutual existential definability of the predicates (see remarks in [Belyakov, Mart'yanov, 1983]). We have

$$x \mid y \;\Leftrightarrow D(x,y,x) \tag{7}$$

and in other direction

$$D(x,y,z) = \exists u(z \mid x \,\&\, z \mid y \,\&\, x \mid u \,\&\, y \mid z+u), \tag{8}$$

$$\neg D(x,y,z) = \exists u(\neg(z \mid x) \;\vee\; \neg(z \mid y) \;\vee\; (u \mid x \,\&\, u \mid y \,\&\, \neg(u \mid z)). \tag{9}$$

NP-completeness of the problem

$$\exists \bar{x}(GCD({}^{3}f_1(\bar{x}), ..., {}^{3}f_m(\bar{x})) = K) \tag{10}$$

on every non-empty and non-trivial integer interval could be proved in the same manner as in Theorem 3 by polynomial reduction of ONE-IN-THREE 3-SAT ([Kosovskii, Starchak, 2016]). Corresponding question for only two non-zero coefficients does not look like as an evident consequence of Theorem 4.

Conclusion

One of the aims of the paper was to show the importance and actuality of problems concerning divisibilities of values of linear polynomials. Although the general problem has high complexity lower bound, some sub-problems could appear sufficient in applications for determining complexity of various problems, arising, for example, in counter automata theory.

The other purpose was to point to a number-theoretical interest in the problem and its possible relations with complexity of solvability of quadratic diophantine equations.

Bibliography

Adleman L., Manders K.L., "Reducibility, randomness and intractability" // Proceedings of the 9th Annual ACM Symposium on Theory of Computing, 1977, pp. 151-163.

Bel'tyukov A.P., "Decidability of the universal theory of the natural numbers with addition and divisibility" // Zapiski Nauchnyh Seminarov LOMI, Vol. 60, 1976, pp. 15-28. (in Russian) English translation, Journal of Soviet Mathematics, Vol. 14, No. 5, 1981, pp. 1436-1444.

Belyakov E.B., Mart'yanov V.I., "Universal theories of integers and the extended Bliznetsov hypothesis" // Algebra i Logika, Vol. 22, 1983, pp. 26-34. (in Russian) English translation, Algebra and Logik, Vol. 22, 1983, pp. 19-26.

Bes A., "A survey of arithmetical definability. A Tribute to Maurice Boffa" // Bulletin de la Societe Mathematique de Belgique, 2002, pp. 1-54.

Bozga A., Iosif R., "On decidability within the arithmetic of addition and divisibility" // Proceedings of FoSSaCS, ser. Lecture Notes in Computer Science, Springer, Vol. 3441, 2005, pp. 425-439.

Bundala D., Ouaknine J., "On parametric timed automata and one-counter machines" // Inf. Comput., 2016, http://dx.doi.org/10.1016/j.ic.2016.07.011

Cohen H., "A Course in Computational Algebraic Number Theory", ser. Graduate Texts in Mathematics. Springer-Verlag, Vol. 138, 1993.

Degtyarev A., Matiyasevich Y., Voronkov A., "Simultaneous rigid E-unification and related algorithmic problems" // Proceedings 11th Annual IEEE Symposium on Logic in Computer Science, 1996, pp. 494-502.

Garey M.R., Johnson D.S., "Computers and Intractability: A Guide to the Theory of NP-Completeness", Freeman, New York, 1979.

Haase C., "On the complexity of model checking counter automata" // Thesis, University of Oxford, 2012.

Kosovskii N.K., Starchak M.R., "NP-complete problems for greatest common divisor of values of linear polynomials" // Proceedings of the 9th conference ITU-2016, St. Petersburg, 2016, pp. 71-72. (in Russian)

Kosovskii N.K., Kosovskaya T.M., Kosovskii N.N., Starchak M.R., "NP-complete problems for systems of divisibilities of values of linear polynomials" // Vestn. St. Petersburg Univ.: Math., 2017, to be published. (in Russian)

Lagarias J.C., "The computational complexity of simultaneous diophantine approximation problems" // 23th Annual Symposium on Foundations of Computer Science, IEEE, New York, 1982, pp. 32-39.

Lagarias J.C., "Succinct certificates for the solvability of binary quadratic diophantine equations" // e-print arXiv:math/0611209v1, 2006. Extended and updated version of a 1979 FOCS paper in Proceedings of the 20th IEEE Symposium on Foundations of Computer Science , IEEE Press, 1979, pp. 47-54.

Lechner A., Ouaknine J., Worrell J., "On the Complexity of Linear Arithmetic with Divisibility" // Proceedings of the 30th Annual ACM/IEEE Symposium on Logic in Computer Science(LICS), 2015, pp. 667-676.

Lipshitz L., "The Diophantine problem for addition and divisibility" // Transactions of the American Mathematical Society, Vol. 235, 1976, pp. 271-283.

Lipshitz L., "Some remarks on the Diophantine problem for addition and divisibility" // Bull. Soc. Math. Belg. Ser. B, Vol. 33, No. 1, 1981, pp. 41-52.

Manders K.L., Adleman L., "NP-Complete decision problems for binary quadratics" // Journal of Computer and System Sciences, Vol. 16, No. 2, 1978, pp. 168-184.

Mart'yanov V.I., "Universal extended theories of integers" // Algebra i Logika, Vol. 16, No. 5, 1977, pp. 588-602. (in Russian) English translation, Algebra and Logik, Vol. 16, No. 5, 1977, pp 395-405.

Matiyasevich Y.V., "Enumerable sets are diophantine" // Doklady Akademii Nauk SSSR, Vol. 191, 1970, pp. 279-282. (in Russian) English translation, Journal of Soviet Mathematics, Doklady, Vol. 11, No. 2, 1970, pp 354-358.

Matiyasevich Y.V., "Hilbert's 10th problem", MIT Press, 1993.

Schrijver A., "Theory of Linear and Integer Programming", John Wiley and Sons, New York, 1986.

Smale S., "Mathematical problems for the next century" // Mathematics: frontiers and perspectives, Amer. Math. Soc., 2000, pp. 271-294.

Authors' Information

Nikolay K. Kosovskii *- Dr., Professor of Computer Science Chair of St. Petersburg State University, University av., 28, Stary Petergof, St. Petersburg, 198504, Russia; e-mail: kosov@NK1022.spb.edu*
Major Fields of Scientific Research: Mathematical Logic, Theory of Computational Complexity of Algorithms

Mikhail Starchak *- PhD student of Computer Science Chair of St. Petersburg State University, University av., 28, Stary Petergof, St. Petersburg, 198504, Russia; e-mail: mikhstark@gmail.com*
Major Fields of Scientific Research: Theory of Computational Complexity of Algorithms

The basic idea of the proof concerns the simultaneous metric theory of the size of integer polynomials and their derivatives. Namely, it is shown that for a given number c0 and constants c1 , c2 with c1 c2 < c0 the system of inequalities ï£± âˆ’nâˆ’1+v , ï£´ ï£²|P (w)|p < c1 Q |P 0 (w)|p < c2 Qâˆ’v , ï£´ ï£³ H(P) 6 Q has solutions P â‹ Z[t] only for a set B = {w} with ÂµB.Â As it concerns the product of the square of the distances between the roots multiplied by a2nâˆ’2 it is in n fact a polynomial of the coeï¬ƒcients of P and is therefore an integer. The discriminant D(P) can also be written as the determinant of a matrix of order 2n â€˜ 1 (for details see [12]). Therefore discriminant calculating for general polynomials with large n and H is hard to perform. For the general problem SIMULTANEOUS DIVISIBILITY OF LINEAR POLYNOMIALS, NP-hardness has been proven for its particular case, when the coefficients of the polynomials are only from the set {1, 2} and constant terms are only from the set {1, 5}. Keywords. system of linear polynomialâ€™s values divisibilities NP-hardness NP-completeness. Original Russian Text Â© N.K. Kosovskii, T.M. Kosovskaya, N.N. Kosovskii, M.R. Starchak, 2017, published in Vestnik Sankt-Peterburgskogo Universiteta: Matematika, Mekhanika, Astronomiya, 2017, Vol. 62, No. 2, pp. 52â€“60. This is a preview of subscription content, lo...Â L. Lipshitz, â€œSome remarks on the Diophantine problem for addition and divisibility,â€ Bull. Soc. Math.