SYSTEMS OF LINEAR DIOPHANTINE EQUATIONS AND DIS-EQUATIONS COMPLEXITY

Nikolay K. Kosovskii, Nikolay N. Kosovskii

Abstract: *Series of problems concerning systems of linear Diophantine equations and dis-equations with explicitly given parameters are offered below. For every problem from a series the conditions upon the parameters under which the problem is NP-complete are proved.*

Keywords: *NP-completeness, system of linear Diophantine equations, system of linear Diophantine dis-equations*

ACM Classification Keywords: *F.2.m Analysis of Algorithms and Problem Complexity Miscellaneous*

Introduction

The importance of formulation and proof NP-completeness for theoretic-number problems is connected with the fact that a polynomial (under the number of Turing machine steps) algorithm solving any of these problem is absent at the present time and probably would not be found in the future (see, for example, [Garey & Johnson, 1979]).

The interest to NP-complete and P-SPACE-complete problems as well as to the explicit extraction of their sub-problems belonging to the class P is presented, for example, in [Kosovskaya, 2011; Kosovskaya, 2014]. One of the authors have proved P-SPACE-completeness of some problems connected with the checking of correctness for properties of Pascal total functions [Kosovskiy, 2013] and also P-SPACE-completeness of checking a predicate formula identically truth in an elementary logic theory of the signature with one modulo arithmetic operations [Kosovskii, 2014].

Note that the computation of 2n in binary notation cannot be done in a polynomial number of steps because the length of its value binary notation is n + 1 that is an exponent of the argument binary notation.

Main results

Let $L(x_1, \ldots, x_k)$ denotes a linear expression with k variables in the form $a_1x_1 + \ldots + x_ka_k + b$ where $a_1, \ldots, a_k$ are integer nonzero coefficients. An equation in the form $L(x_1, \ldots, x_k) = 0$ is called here a linear k-equation and inequality in the form $L(x_1, \ldots, x_k) \neq 0$ is called here a linear k-dis-equation.

Let integers m and m' be such that $m < m'$. The first of the presented problems is the following.

System of linear 3-equations on the segment [*m, m'*]

INSTANCE. Given a set of variables $\{x_1, \ldots, x_n\}$. Given a system of linear 3-equations in the form $L(x, y, z) = 0$ and every its variable coefficient belongs to the set $\{-1, 1\}$.

QUESTION. Whether the system is consistent in integers from the segment [*m, m'*]?

Theorem 1. *For every* distinct *integers m and m' the problem* **System of linear 3-equations on the segment [*m, m'*]** *is an NP-complete one.*

Scheme of the proof. The fact that the problem belongs to **NP** is evident.

Prove that the NP-complete problem ONE-IN-THREE 3-SAT from [Garey and Johnson, 1979] is polynomially reducible to the problem. The values *false* and *true* correspond to the constants m and $m + 1$ respectively. The variable u_j is represented by u_j and its negation $\neg u_j$ by $2m + 1 - u_j$. The disjunction $x \vee y \vee z$ is represented by $x + y + z = 3m + 1$.

Note that if x, y and t belong to [*m, m'*] then

$$\exists y\,(x + t = y) \Leftrightarrow m \le x + t \le m'. \qquad (1)$$

The equation from (1) $x + m' - m - 1 = y$ (for $t = m' - m - 1$) has an integer solution from [*m, m'*] iff $x = m$ or $x = m + 1$. Add to the system an equation of such a form for every variable. As every equation of the added system has only 2 variables let's add as an added an equal to m variable w to the left part of the equation and the constant m to the right part of the equation. Besides, the equation $w + u + v = 3m$ (providing equality of variables to m) must be added to the system. The received system of linear equations (every with 3 variables) is consistent iff the given set of disjunctions is satisfiable and only one literal in every disjunction is true. **The theorem is proved.**

Note that Theorem 1 is a corollary of NP-completeness of the problem of consistency in integers checking for a system of linear nonstrict inequalities from [Schrijver, 1986].

Theorem 1 has a geometrical interpretation.

Proposition 1. *Given a many-dimensional cube every vertex of which belongs to the set of integers {m, m'} and hyper-planes cutting off equal segments on some three axes and are parallel to all other axes.*

Then the problem of the checking if there exists a point with integer coordinates of intersection of all hyperplanes inside the cube is an NP-complete one.

Regard the following series of problems.

System of linear 2-equations and 1-dis-equations on the segment [*m, m'*]

INSTANCE. Given a set of variables $\{x_1, \ldots, x_n\}$ and integers $m_1, \ldots, m_n, m_1', \ldots, m_n'$. Given a system of linear 2-equations with rational coefficients in the form $L(x, y,) = 0$, of 1-dis-equations in the form $ax+b \neq 0$ with rational a and b and of non-strict inequalities in the form $m_i \leq x_i \leq m_i'$.

QUESTION. Whether the system is consistent in integers from the segment [*m, m'*]?

Theorem 2. *For every integers m and m' there exists an algorithm solving the problem* **System of linear 2-equations and 1-dis-equations on the segment [*m, m'*]** *and belonging to the class* ***P****.*

Proof. Use the following procedure of the system transformation.

1. Eliminate a variable from the 2-equations. A system with the less number of variables and linear expressions for the eliminated variables by means of the remaining ones are received;
2. Substitute the linear expressions instead of the eliminated variable into all remaining dis-equalities and inequalities. New dis-equalities and inequalities in the same form may be obtained for some of the remaining variables.

This procedure must be repeated for every variable of the system.

A system of 1-dis-equations remains as a result. Decompose the received system into sub-systems with the only one variable. The number of these sub-systems coincides with the number of variables.

If a constant term of a dis-equation is not multiply to a variable coefficient then this dis-equation may be deleted. Otherwise the dis-equation is divided by the coefficient.

If the set of all constant terms of at least one sub-system for a variable x_i includes the segment $[m_i, m_i'] \cap [m, m']$ then the initial system has no solutions. Otherwise it is consistent.

Obviously, the algorithm is a polynomial one. **The theorem is proved.**

The proved theorem states, in particular, that if **P** $\neq$ **NP** then the term "3-equation" in the theorem 1 cannot be replaced by the term "2-equation".

System of linear 3-dis-equations on the segment [*m, m'*]

INSTANCE. Given a set of variables $\{x_1, \ldots, x_n\}$. Given a system of linear 3-dis-equations in the form $L(x, y, z) \neq 0$ and every its variable coefficient belongs to the set $\{-1,1\}$.

QUESTION. Whether the system is consistent in integers from the segment [*m, m'*]?

Theorem 3. *For every distinct integers m and m' the problem* **System of linear 3-dis-equations on the segment [*m, m'*]** *is an NP-complete one.*

Scheme of the proof. The fact that the problem belongs to **NP** is evident.

The problem 3-SAT from [Garey and Johnson, 1979] polynomially reduced to the problem under consideration. The truth of the disjunction $x \vee y \vee z$ (where *x, y* and *z* are variables or their negations) may be presented by a dis-equation $x + y + z \neq 3m$. The constant *false* is represented by the integer *m* and the constant *true* is represented by the integer $m + 1$. Instead of $\neg u_j$ the constant $2m + 1 - u_j$ is substituted.

Two 1-dis-equations with the absent variable are added instead of every eliminated 2-equation. These two 1-dis-equations provide the belonging of the eliminated variable value to the segment [*m, m'*].

For every literal *x* 3-dis-equations in the form

$$x + w + w' \neq 3m + 2$$

$$x + w + w' \neq 3m + 3$$

$$\ldots$$

$$x + w + w' \neq 3m'$$

as well as the condition for every auxiliary variable $w = w' = w'' = 3m$ in the form

$$w + w' + w'' \neq 3m + 1$$

$$w + w' + w'' \neq 3m + 2$$

$$\ldots$$

$$w + w' + w'' \neq 3m'$$

are added. **The theorem is proved.**

Theorem 3 has a geometrical interpretation.

Proposition 2. *Given a many-dimensional cube every vertex of which belongs to the set {m, m'} and hyperplanes cutting off equal segments on some three axes and are parallel to all other axes. Then the problem of the checking if there exists a point with integer coordinates inside the cube which does not belong to any hyperplane, is an NP-complete one.*

System of linear 2-dis-equations on the segment [*m, m'*]

INSTANCE. Given a set of variables $\{x_1, \ldots, x_n\}$. Given a system of linear 2-dis-equations in the form $L(x, y) \neq 0$ and every its variable coefficient belongs to the set $\{1, 2\}$.

QUESTION. Whether the system is consistent in integers from the segment [*m, m'*]?

Lemma. *For every integers m and m' such that m' – m > 2 every binary relation on integers from* [*m, m'*] *may be set by a system of linear 2-dis-equations with variable coefficients from the set {1, 2}*.

To prove this Lemma it is sufficient to use the system of all 2-dis-equations in the form $x + 2y \neq c$ with $c = a + 2b$ for every pair *(a, b)* of integers from [*m, m'*] not satisfying the relation.

Theorem 4. *For every integers m and m' such that m' – m > 2 the problem* **System of linear 2-dis-equations on the segment [*m, m'*]** *with variable coefficients from the set {1, 2} is an NP-complete one.*

Proof. The fact that the problem belongs to **NP** is evident.

Prove that the problem 3-SAT is polynomially reducible to the problem under consideration. Every disjunction c_j is represented by two variables s_j and s'_j with values from $\{3m, \ldots, 3m + 3\}$ and a 2-dis-equation $s_j + s'_j \neq 4m$. Actually values of variables s_j and s'_j numerate pairs *(a, b)* and *(b, c)* respectively for *a, b* and *c* from *{0, 1}* by means of the expressions $3m + a + 2b$ and $3m + b + 2c$ respectively. Here *a, b* and *c* are the truth values of literals from c_j represented by integers 0 and 1.

For every pair of disjunctions c_j and c_k containing the same variable write down the set of 2-dis-equations (according to the Lemma) corresponding to the relation "The *p*-th literal of the disjunction c_j coincides with the *q*-th literal of the disjunction c_k" or "The *p*-th literal of the disjunction c_j is opposite to the *q*-th literal of the disjunction c_k".

The system containing all dis-equations in the form $s_j + s'_j \neq 4m$, $s_j + s'_j \neq 4m + 10$, $s_j + s'_j \neq 4m + 11$, ..., $s_j + s'_j \neq 4m'$ and all dis-equations corresponding to the described above relations is consistent iff the problem 3-SAT has a solution. **The theorem is proved.**

If **P** $\neq$ **NP** then the term "2-dis-equation" in the Theorem 4 cannot be replaced by the term "1-dis-equation" because in such a case this problem is transforming into the polynomial problem **System of linear 2-equations and 1-dis-equations on the segment [*m, m'*]**.

Theorem 3 may be generalized from a many-dimensional cube up to a many-dimensional domain.

System of linear 3-dis-equations on the bounded domain with parameters *n, m_1, …, m_n, m* and *m'*.

INSTANCE. Given a set of variables $\{x_1, \ldots, x_n\}$. Given a system of linear 3-dis-equations in the form $L(x, y, z) \neq 0$ and every its variable coefficient belongs to the set $\{-1, 1\}$.

Given a domain in an n-dimensional ($n \geq 3$) space defined by means of polynomial inequalities. The domain contains n-dimensional cube $[m, m']^n$ ($m < m'$) and is included into n-dimensional parallelepiped $[-m_1, m_1] \times \ldots \times [-m_n, m_n]$.

QUESTION. Whether the system is consistent in integers containing in the domain?

Theorem 5. *For every positive integers n, m_1, …, m_n, m* and *m' the problem* **System of linear 3-dis-equations on the bounded domain with parameters *n, m_1, …, m_n, m* and *m'*** *is an NP-complete one.*

Proof. The fact that the problem belongs to **NP** is evident.

Consider its narrowing up to the systems containing dis-equations

$$x_i + v + w \neq m_i + 2m$$

$$x_i + v + w \neq m_i - 1 + 2m$$

$$\ldots$$

$$x_i + v + w \neq m' + 1 + 2m$$

$$x_i + v + w \neq -m_i + 2m$$

$$x_i + v + w \neq -m_i + 1 + 2m$$

$$\ldots$$

$$x_i + v + w \neq m - 1 + 2m$$

for every variable $x_1, \ldots, x_n$ and dis-equations

$$u + v + w \neq 3m + 1$$

$$u + v + w \neq 3m + 2$$

$$\ldots$$

$$u + v + w \neq 3m'$$

This restriction transforms it into the NP-complete problem **System of linear 3-dis-equations on the segment [*m, m'*]**. **The theorem is proved.**

Conclusion

Traditionally the initial problem for the proof of NP-completeness for the almost all problems is the problem of satisfiability of a propositional formula in a conjunctive normal form SAT [Garey & Johnson, 1979]. Such its restriction that every elementary conjunction contains only three variables (3-SAT [Garey & Johnson, 1979]) is more convenient for such a proof. The problem ONE-IN-THREE 3-SAT [Garey & Johnson, 1979] is yet more convenient problem for such a proof. In this problem the truth of an elementary conjunction is changed by the equality to 1 of the sum of characteristic functions for three different conjunctive terms.

The presented paper describes and proves NP-completeness of some series of problems concerning not mathematical logic but the fact of consistency for systems of linear equations and dis-equations. Such problems are more natural for mathematicians.

The proved theorems illustrate that if **P** $\neq$ **NP** then the solving of a system of linear Diophantine equations as well as of a system of linear Diophantine dis-equations with a solution from a bounded set cannot be implemented by a Turing machine in a polynomial number of steps.

NP-completeness of the problem **System of linear 3-dis-equations on the segment [m, m']** for integer m and m' has a practical significance while computer implementation. Theorem 1 shows that the use of variables of the computer type integer in the systems of linear equations cannot be solved by a polynomial in time algorithm if **P** $\neq$**NP**. This is not so if one uses a program tool with the built-in operations for arbitrary long integers. Such built-in operations are included into all dialects of the programming language Refal.

Acknowledgements

The paper is published with financial support of the project ITHEA XXI of the Institute of Information Theories and Applications FOI ITHEA (www.ithea.org) and the Association of Developers and Users of Intelligent Systems ADUIS Ukraine (www.aduis.com.ua).

Bibliography

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

[Kosovskaya, 2011] T. Kosovskaya, "Discrete Artificial Intelligence Problems and Number of Steps of their Solution" // International Journal "Information Theories and Applications", Vol. 18, Number 1, 2011, pp. 93 – 99.

[Kosovskaya, 2014] T. Kosovskaya, "Construction of Class Level Description for Efficient Recognition of a Complex Object" // International Journal "Information Content and Processing", Vol. 1, No 1, 2014, pp. 92 – 99.

[Kosovskii, 2014] N. Kosovskii, "A Language Using Quantifiers for Description of Assertions about Some Number Total Functions" // International Journal "Information Theories and Applications", Vol. 21, Number 2, 2014, pp. 120 – 125.

[Kosovskiy, 2013] N. Kosovskiy, "Algorithmic Decidability of Computer Program-Function Language Properties" // International Journal "Information Theories and Applications", Vol. 20, Number 2, 2013, pp. 131 – 136.

[Schrijver, 1986] A. Schrijver, "Theory of Linear and Integer Programming", A Wiley-Interscience Publication, John Wiley & Sons, New York, 1986.

Authors' Information

Nikolay K. Kosovskiy *– Dr., Professor, Head 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

Nikolay N. Kosovskiy *– PhD, Docent of Geometry Chair of St. Petersburg State University, University av., 28, Stary Petergof, St .Petersburg, 198504, Russia, e-mail: kosovnn@pdmi.ras.ru*

Major Fields of Scientific Research: Geometry