Some NP-Hard Problems for the Simultaneous Coprimeness of Values of Linear Polynomials

Starchak M.R[1], Kosovskii N.K.[2] and Kosovskaya T.M.[3]

[1] St. Petersburg State University

Received: 11 December 2016 Accepted: 2 January 2017 Published: 15 January 2017

Abstract

The algorithmic-time complexity of some problems connected with linear polynomials and coprimeness relation on natural numbers is under consideration in the paper.We regard two easily stated problems. The first one is on the consistency in natural numbers from the interval of a linear coprimeness system. This problem is proved to be NP-complete. The second one is on the consistency in natural numbers of a linear coprimeness and discoprimeness system for polynomials with not greater than one non-zero coefficient. This problem is proved to be NP-hard.Then the complexity of some existential theories of natural numbers with coprimeness is considered. These theories are in some sense intermediate between the existential Presburger arithmetic and the existential Presburger arithmetic with divisibility.

Index terms— NP, NP-completeness, NP-hardness, coprimeness of values of linear polynomials, simultaneous divisibility of linear polynomials, existential theories w

1 I. Introduction

he proof of NP-hardness of a certain computational problem gives us rather strong assurance of the absence of any polynomial-time algorithm for this problem. Hence, the existence of such proof gives us not only theoretical but also an important practical result for a working programmer. On the other hand, number-theoretical relations like divisibility or coprimeness of integers provides us one of the most natural languages for stating computational problems. We thus come to the study of the algorithmic-time complexity of the decision problems for various subclasses of arithmetic which are sometimes referred as weak arithmetics (see [16]). These reasons motivate the appearance of this paper.

The problem of integer linear programming (ILP) is well-known and one of the first to be proved NPcomplete (see, [2] and [6], problem MP1). It can be regarded as a problem of consistency in non-negative integers of a system of linear equations with integer coefficients. In the sense of the weak arithmetics complexity this result can be interpreted as the NP-T completeness of the decision problem for the existential Presburger Arithmetic ?Th??;+,=,0,1? (abbreviated as ?PA). The decidability of Presburger Arithmetic is a classical result [15] and the complexity of its subclasses is studied rather extensively. For example, the paper [7] completes the classification of the time-complexity results corresponding fixed number of quantifier alternations and fixed maximum number of variables in each quantifier group. The lowest level of this subproblem hierarchy is just the famous H.W.Lenstra Jr. theorem [13] on the polynomial algorithm for ILP with a fixed number of variables. As was shown in [5] this result provides us with polynomial algorithms for various practical graph problems when we fix the value of some natural parameter of a given graph. In other words, there was proved the fixed-parameter tractability of these problems by rewriting each one as an instance of ILP. In this paper, we will prove NP-hardness of some problems from the extensions of ?PA.

The time-complexity of ?PA extended with thedivisibility relation | ( ) x y z y x z â??” ? = ?

was studied in [12,14]. For this problem we will use the abbreviation ?PAD. In non-deterministic polynomial time the problem is reducible to the consistency in non-negative integers of a system of linear divisibilities of the form,0 ,**1 1 , ,0 ,1 1 , 1 (...**| ...). m i i i n n i i i n n i a a x a x b b x b x = + + + + + + ?**(1)**

L.Lipshitz in [14] proved that this problem is NPcomplete for every fixed number of divisibilities m?5, whereas the general problem, as was shown in [12] by A.Lechner, J.Ouaknine and J.Worrell, is in NEXPTIME.

The exact complexity of ?PAD remains an open problem, and the answer is of considerable interest as it will effect on the related problems of formal verification (see, for example, [3,11]). Some NP-complete problems with an arbitrary number of divisibilities but with restrictions on the values of the coefficients of linear polynomials are presented in [10].

One of the possible approaches to solve this problem is to establish complexity of some intermediate theories, that is, simultaneously extensions of ?PA and subclasses of ?PAD. This question has not been studied apparently because of the common belief that ?PAD is in NP citing the paper [14]. This inaccuracy was firstly pointed at by the authors of [12]. For example, the paper [4] The object of consideration of this paper is the complexity of linear systems with coprimeness relation of the form,0 ,**1 1 , ,0 ,1 1 , 1 (**

... ...).m i i i n n i i i n n i a a x a x b b x b x = + + + ? + + + ?**(2)**

We will further prove NP-hardness of a system of linear coprimeness and discoprimeness for linear polynomials with not greater than one non-zero coefficient in each polynomial. Formally, this system has form1 2 1 1 ( ) ( ) (( ) ( )), m m i i j j i j f x g x f x g x = = ? ? ¬ ? ? ?**(3)**

where ??=( )and each linear polynomial (??), (??) has the form for some[1,]. j n ?

From this result we can derive NP-hardness of the decision problem for the existential theory of natural numbers for with coprimeness relation ?Th??;S,??.

Note that all thus defined problems on simultaneous coprimeness of values of linear polynomials can be rewritten in a form of a system of divisibilities of values of linear polynomials. One has to introduce new variables to use the following formulas:(| |1) ( ) (2 | 2 |). x y u x u y u x y v v x v y ? â??" ? ? + ¬ ? â??" ? + ? +**(4)**

II. Two NP-Hard Problems for the Simultaneous Coprimeness of Values of Linear Polynomials

By natural numbers we will further assume nonnegative integers ?= {0, 1, 2 ?}. As it was defined in the introduction, the relation x y

? on natural numbers is true iff the greatest common divisor of x and y equals , thus we have (0 0) ¬ ? and that for every x ? the formula 1 x ? is true. We can now define a series of problems, depending on the parameter . k ?

2 Simultaneous Coprimeness of values of Linear Polynomials in the interval [k, k+1] (?LP[k, k+1]). INPUT: A set of m pairs of (n+1)-dimensional vectors (( ),(

))with natural entries for[1,]. i m ? QUESTION: Is the linear system ,0 ,**1 1 , ,0 ,1 1 , 1 (**

... ...)m i i i n n i i i n n i a a x a x b b x b x = + + + ? + + + ? consistent in natural numbers from the interval [k, k+1]? Let ?03LP[k, k+1] be a subproblem of ?LP[k, k+1]

in which each pair of coprime linear polynomials contains one with exactly three non-zero coefficients and the other is a natural number.Theorem 1. For every k ? the problem ?03LP[k, k+1] is NP-complete.

Proof. That the problem is in the class NP is obvious because every variable takes it values from the given interval of natural numbers.

To prove NP-hardness of ?03LP[k, k+1] we will construct a polynomial reduction of ONE-IN-THREE 3SAT from [6] to our problem. The truth of exactly one literal in every clause can be expressed via expression,1,**2 ,3 3 (3 2)**

.i i i k k x x x + ? + +**(5)**

Logical constants true and false are encoded respectively by numbers k+1 and k. Every negated literal ¬x is substituted in the corresponding expression by a new variable x' and we add to the system three new expressions3 (3 2) ' 3 (3 2) ' 3 (3 2) , k k x x u k k x x v k k u v w + ? + + + ? + + + ? + + (6) ?? 1 , ? , ?? ?? ð ??"ð ??" ?? ð ??"ð ??" ?? ?? ??=??+1

a ??,0 +a ???? ?? ?? the successor functiona i,O, a i, 1, ? , a i,n ?? i,0 , ?? i,1 ,?, ?? i,n of ?PAD has the following sentences: "In [5] the algorithm of [4] is made into decision procedure of class NP: hence each subdivisibility set is in the class NP.

3 [?]

Here we focus on other structural properties of these sets [?]". In [8,9] it was proved NP-completeness for some kinds of systems of linear congruences ?, incongruences ? and dis-equations ?, supplemented in some cases with geometric interpretations.

Here we use the notationGCD(,) 1, x y x y ? â??" = where GCD(,)

x y is the greatest common divisor of nonnegative integers and , assuming(0 0). ¬ ?

The problem of consistency of the linear system (2) will be denoted as SIMULTANEOUS COPRIMENESS OF LINEAR POLYNOMIALS (?LP). We will state the NPcompleteness of a series of ?LP problems with the values of the variables taken from an interval of nonnegative integers. The relation

4 [,]

x a b ? is existentially definable using equality predicate. As a corollary, we get NP-hardness of the decision problems for existential theories of natural numbers with addition, equality and coprimeness relation and also its restriction to the theory without equality. It is not known whether the equality predicate is definable even in universal theory. It was only proved in [17] (see also the survey [16]) that the definability of equality within arithmetic with addition and coprimeness is equivalent to the truth of the number-theoretic Erdös-Woods conjecture.

x y

5 = x y

We therefore can conclude that each NP-hard problem mentioned above is in NEXPTIME complexity class. The simple definition of coprimeness in terms of divisibilities suggests that ?Th??;S,?? can be proved to be in the class NP using the complexity analysis of the ?PAD decision problem from [12]. This possibility is discussed in some concluding remarks after the ?Th??;S,?? NPhardness proof. i i i i i u b u x b a ¬ ? ? ? + ?

Thus, for every SI instance we have constructed the instance of ?&Dis?LP of the form1 1 (( )) ( ). m m i i i i i i i u x b a u b = = ? + ? ? ¬ ? ? ?**(7)**

As this construction takes not greater than polynomial number of steps of a Turing machine, the problem ?&Dis?LP is NP-hard. Corollary 1 from the Theorem 2. The problem ?&Dis?LP is NP-hard.

Note that in fact we have proved a stronger theorem as every coefficient in the constructed system (7) equals to one. This provides us with one subclass of ?Th??;S,?? formulas with NP-hard decision problem. We will state some corollaries from these two theorems, concerning complexity of decision problems for existential theories in the following section.

6 III. Some Corollaries on the Time-Complexity of the Decision Problems for Existential Theories with Coprimeness Relation

The problems ?LP[k, k+1] and ?&Dis?LP can be interpreted as problems of validity in natural numbers for some classes of existentially closed formulas of the first-order language for coprimeness with addition or with successor function. We should only take care of the length of each formula that corresponds to an instance of ?LP[k, k+1] or ?&Dis?LP. Let us first prove some lemmas on the definability of certain predicates in the theories with coprimeness. Lemma 1. The relations =0 and =1 on natural numbers are existentially definable by successor and the coprimeness relation. x y ?

Proof. These definitions are: 1 x x x = â??” ? and 0 1 1 . x x x = â??” + ? + Lemma 2.n a = ? ? ? ? As the relation x 0 =1 is definable, we can define x 1 =2, x 2 =4, x 3 =8? x n =2 n by the formulas a i,O, a i, 1, ? , a i,n ?? i,0 , ?? i,1 ,?, ?? i,n {(( ),( ))}for a i,O, a i, 1, ? , a i,n ?? i,0 , ?? i,1 ,?, ?? i,n a ?? ?? ?? ?? ?? ?? ?? ??=??+1 a a

Proof. To prove the NP-hardness of the problem, we will construct a polynomial reduction of a special case of SIMULTANEOUS INCONGRUENCES problem which is named ”anti-Chinese remainder theorem” in [1]. It could be seen from the NP-completeness proof in [1], that every modulus in a system is square-free and its value is bounded polynomially in the number of the incongruences. This follows from the fact that in the polynomial reduction from 3SAT to SI, there were generated first n primes for every propositional variable from the instance of 3SAT and every modulus of the corresponding SI instance did not exceed p n p n-1 p n-2 . Thus the proof from [1] implicitly gives us the NPcompleteness of the following problem.

.n i i i k x x k = ? ? ? + ? The predicate x y

? is definable by the formula with equality: ( ). u x u y ? + = From Lemma 2 it follows that every linear term ( ) i f x and ( ) i g x can be defined by a formula of polynomial size on the length of the binary representation of the integer coefficients. Thus, introducing n new variables we construct in polynomial time a formula from ?Th??;+,=,?? which is true iff the given instance ?LP[k, k+1] is solvable.

We thus have a series of NP-complete subproblems of the decision problem of ?Th??;+,=,?? and NP-hardness of the general decision problem of this theory.

Corollary 3 from the Theorem 1. The problem ?LP is NPhard. Proof. Consider the formulas from the proof of Theorem 1 in the case of k=0. The system has form:,1 ,2 ,3 1 0 m i i i i x x x = ? + + ?**(8)**

proved by restriction to the NP-complete problem of the consistency in natural numbers of a system of the form (8).

As the relation =0 is definable by Lemma 1 in the theory ?Th??;+,??, and the coefficients of linear polynomials from (8) all equal one, we immediately get the following corollary. Corollary 4 from the Theorem 1. The decision problem of the theory ?Th??;+,?? is NP-hard.

Corollary 2 from the Theorem 2. The decision problem of the theory ?Th??;S,?? is NP-hard. Proof. To prove NP-hardness we can continue the polynomial reduction presented in the proof of Theorem 2. The relation =1 is definable in the considered theory, and therefore the unary relation ¬(?) is also definable for every positive integer a. As every natural number from the formula (7) is represented in unary, each polynomial a+x can be rewritten in the form ? ... . a times SS S x By taking existential closure of every formula of the form (7) we define some formula from ?Th??;S,??. This concludes the polynomial reduction of SI to the decision problem of ?Th??; S,??.

A natural question is whether the decision problems considered above are in fact NP-complete. As every formula of these theories can be rewritten as a ?PAD formula, one can go through the complexity analysis of the ?PAD decision procedure from [12] for some restricted class of formulas. In conclusion, we will give some remarks corresponding NP membership of the decision problem for ?Th??;S,?? formulas.

7 IV. Conclusion

Two easily formulated number-theoretic problems for coprimeness relation on natural numbers were defined in the first section. The problem of consistency of a coprimeness system of the form (2) was shown NP-complete on every interval [k, k+1] of natural numbers. The related problem of consistency in natural numbers of a coprimeness and discoprimeness system of the form (3) was proved NP-hard when the linear polynomials have not greater than one non-zero coefficient.

We then derive some corollaries from these two theorems. There was established NP-hardness of the existential theories of natural numbers for coprimeness with addition ?Th??;+,?? and for coprimeness with successor function ?Th??;S,??. These problems naturally arise in such fields of computer science as formal verification or cryptography. As it is not known whether the relation of equality is definable by addition and coprimeness, we have to independently consider the theory without equality. Let us define the problem ?LP as the problem of consistency in natural numbers of a system of coprime values of linear polynomials. That is, unlike ?LP[k, k+1], this problem does not have any restriction on the values of the variables. As the formulation of ?LP is very similar to the one of ?LP[k, k+1], we do not give it explicitly. The pairs of coprime polynomials in the proof given below will provide us with the NP-hardness proof for the decision problem of the corresponding theory without equality.

For every natural number, we have 0 1, x x ? â??” = therefore the restriction on the variables [0,1] i x ? is necessary satisfied. NP-hardness of ?LP is Note that we use in this corollary that the problem ?LP remains NP-complete even in the case of the unary representation of the coefficients of polynomials in a system from its instance. Let us now consider formulas of the theory ?Th??;S,?? with the successor function in place of addition. The formula (7) provides us with the following It could be an interesting problem i to determine whether if ?Th??;S,?? is in NP and the same question in Year 2017 [1] [2]

Year 2017

22

)

(H

which considers existentially definable subsets

Figure 1:

[1] © 2017 Global Journals Inc. (US)

[2] © 20 7 Global Journa ls Inc. (US)

Simultaneous Coprimeness and Discoprimeness of
values of Linear Polynomials(?& Dis?LP) INPUT: Two sets of (m 1 + m 2) pairs of (n+1)-dimensional vect

and {(( ),(

natural entries.
QUESTION: Is the system
1 m
1 = ? i (i a ,0 + ,1 1 a x i ... + + , i

2 m
1 = ¬ (? j a j ,0 + ,1 1 a x j ... + +

consistent in natural numbers?

Let ?&Dis?11LP be a subproblem of
?&Dis?LP such that each linear polynomial has not
greater than one non-zero coefficient and every
coefficient and constant term is represented in unary. Theorem 2. The problem ?&Dis?11LP is NP-hard.

Simultaneous Incongruences (SI) (Implicit in [1, Theorem
5.5.7]
INPUT: A set of ordered pairs (

represented in unary, with

Figure 2:

a times SS S x written on the tape of a Turing machine as the string a+x for the integer a represented in binary. Introducing new variables u i and v i while rewriting every coprimeness formula in the form of divisibility formula using the formulas (4), we get a ?PAD instance of rather convenient for the subsequent complexity analysis form. Every linear polynomial has form a+x, and the formula is already increasing (in the sense of [12]) with respect to the total ordering

variables. An attempt to apply the ?PAD decision procedure from [12] on such restricted class of divisibility formulas to get an NP upper bound could be the subject of the subsequent research.

This page is intentionally left blank

[Mathematics. Mechanics. Astronomy ()] , *Mathematics. Mechanics. Astronomy* 2016. 49 (3) p. .

[Astronomy ()] , *Astronomy* 2017. 4 (62) p. .

[Bach and Shallit ()] *Algorithmic number theory, I: Efficient algorithms*, E Bach , J Shallit . 1996. Cambridge, MA: MIT Press.

[Borosh and Treybig ()] 'Bounds on positive integral solutions of linear diophantine equations'. I Borosh , L B Treybig . *Proceedings of the American Mathematical Society* 1976. 55 (2) p. .

[Garey and Johnson ()] *Computers and Intractability: A guide to the theory of NPcompleteness*, M R Garey , D S Johnson . 1979. New York: W. H. Freeman and co.

[Fellows et al. ()] 'Graph layout problems parameterized by vertex cover'. M R Fellows , D Lokshtanov , N Misra , F A Rosamond , S Saurabh . *Proceedings of the 19th International Symposium on Algorithms and Computation*, (the 19th International Symposium on Algorithms and Computation) 2008. p. .

[Lenstra ()] 'Integer programming with a fixed number of variables'. H W J Lenstra . *Mathematics of Operations Research* 1983. 8 (4) p. .

[Kosovskii et al.] 'NP-complete problems for systems of divisibilities of values of linear polynomials'. N K Kosovskii , T M Kosovskaya , N N Kosovskii , M R Starchak . Vestnik SPbSU. Mathematics. Mechanics

[Kosovskii et al.] *NP-completeness conditions for verifying the consistency of several kinds of systems of linear diophantine dis-equations*, N K Kosovskii , T M Kosovskaya , N N Kosovskii . Vestnik SPbSU.

[Kosovskii et al. ()] 'NP-completeness conditions for verifying the consistency of several kinds of systems of linear diophantine discongruences'. N K Kosovskii , T M Kosovskaya , N N Kosovskii . Vestnik SPbSU. Mathematics. Mechanics. Astronomy 2016. 49 (1) p. .

[Bundala and Ouaknine ()] 'On parametric timed automata and one-counter machines'. D Bundala , J Ouaknine . *Information and Computation* 2017. 253 p. .

[Lechner et al. ()] 'On the complexity of linear arithmetic with divisibility'. A Lechner , J Ouaknine , J Worrell . *Proceedings of 30th Annual IEEE Symposium on Logic in Computer Science*, (30th Annual IEEE Symposium on Logic in Computer Science) 2015. p. .

[Woods ()] *Some problems in logic and number theory, and their connections*, A Woods . 1981. University of Manchester (PhD Thesis) (the case of every term from this theory of the form ? ..)

[Lipshitz ()] 'Some remarks on the diophantine problem for addition and divisibility'. L Lipshitz . *Bulletin de la Société mathématique de Belgique. Série B* 1981. 33 (1) p. .

[Haase ()] 'Subclasses of Presburger arithmetic and the weak EXP hierarchy'. C Haase . *Proceedings of the Joint Meeting of the 23rd EACSL Annual Conference on Computer Science Logic and the 29th Annual IEEE Symposium on Logic in Computer Science*, (the Joint Meeting of the 23rd EACSL Annual Conference on Computer Science Logic and the 29th Annual IEEE Symposium on Logic in Computer Science) 2014. p. .

[Lechner ()] 'Synthesis problems for one-counter automata'. A Lechner . *Proceedings of 9th International Workshop on Reachability Problems*, (9th International Workshop on Reachability Problems) 2015. p. .

[Van Den Dries and Wilkie ()] 'The laws of integer divisibility, and solution sets of linear divisibility conditions'. L Van Den Dries , A J Wilkie . *Journal of Symbolic Logic* 2003. 68 (2) p. .

[Richard ()] 'What are weak arithmetics?'. D Richard . *Theoretical Computer Science*, 2001. 257 p. .

[Presburger ()] 'Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt'. M Presburger . *Comptes rendus du 1er Congrès des Mathématiciens des Pays Slaves*, 1929. p. .