Theoretical Computer Science 708 (2018) 91–95

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Note

A transfer method from bounded existential Diophantine equations to Tarski algebra formulas

B. Litow

Portland, OR 97206, United States

ARTICLE INFO

Article history:
Received 6 March 2017
Received in revised form 19 September 2017
Accepted 19 October 2017
Available online 6 November 2017
Communicated by L.M. Kirousis

Keywords:
Bounded existential Diophantine equations
Tarski algebra
Size bounded quadratic residue problem
Subexponential time algorithms

ABSTRACT

We identify a transfer method from bounded existentially quantified Diophantine equations to formulas of Tarski algebra, the first order theory of the real field. The method is applied to show that **NP** is contained in $\bigcup_{n=1}^{\infty} \mathrm{Dtime}(2^{a\cdot\log^{O(1)}n})$, where a depends only on the given Diophantine equation.

1. Introduction

We follow standard definitions for the complexity class **NP**, e.g., [3]. Note also that O-notation always indicates an absolute constant.

An existential Diophantine equation (EDE) A has the form

$$\exists x_1, \ldots, x_k \; P(x_1, \ldots, x_k) = 0\,,$$

where $P(x_1, \ldots, x_k)$ is an integer coefficient polynomial and all variables range over $\mathbb{N}$. It is known that the decision problem for EDE is not computable [7]. An n-EDE is an EDE whose coefficient absolute values and variables are restricted to $[0..n]$. We introduce a transfer method that converts an n-EDE A into a sentence B of Tarski algebra such that the following theorem holds.

Theorem 1. *$A \Leftrightarrow B$ and B can be decided in time*

$$2^{O(a\cdot\log^{O(1)}n)}\,,$$

where a is the total degree of $P(x_1, \ldots, x_k)$.

The proof uses the main complexity bound for deciding Tarski algebra sentences and details of the transfer method. We use Theorem 1 to prove

E-mail address: bruce.litow@gmail.com.

https://doi.org/10.1016/j.tcs.2017.10.013
0304-3975/

Theorem 2. NP *is contained in* $\bigcup_{n=1}^{\infty} Dtime(2^{a\cdot\log^{O(1)}n})$.

The proof of Theorem 2 requires an additional fact. Let $\langle x\rangle$ denote the binary representation of $x \in \mathbb{N}$. We refer to the set of triples $(\langle a\rangle, \langle b\rangle, \langle c\rangle)$ such that there exists $x \in \mathbb{N}$ for which $x^2 \equiv a \pmod b$ and $x < c$ as SBQR (size-bounded quadratic residues problem). We can W.L.O.G. impose $a, c < b$ and measure the size of a triple in terms of $\lceil \log b \rceil = |\langle b\rangle|$. We see that SBQR is a 3-adic relation over $\mathbb{N}$. SBQR is **NP** complete [6]. It is easy to check that

$$\exists x, y_1, y_2\ (x^2 - a - b\cdot y_1)^2 + (c - x - y_2)^2 = 0 \tag{1}$$

is an EDE representation of SBQR.

2. Tarski algebra

The transfer method is based on the complexity of quantifier elimination for Tarski algebra, which is the first order theory of the real field. Only elementary facts about the theory will be needed apart from the quantifier elimination result. The language of the theory is standard first order logic with equality and the nonlogical symbols $+, \times, 0, 1$ where $+$ and $\times$ are 2-adic function symbols and 0 and 1 are 0-adic function symbols. The interpretation assigns real number values to variables and the function symbols have the obvious definitions. We will write $+$ and $\times$ as infix symbols. A term can be regarded as a polynomial with integer coefficients. We leave it to the reader to verify that subtraction is definable and that numerals for elements of $\mathbb{N}$ can be expressed as terms built up in a variant of binary representation using the abbreviation $2 = 1 + 1$. Using trichotomy of the real field we can eliminate negation so that an atomic formula can be written as $P(u_1, \ldots, u_r) \diamond 0$, where $\diamond \in \{=, <, >\}$. A general prenex formula $A(x_1, \ldots, x_k)$ (free variables are displayed) has the form

$$Q_1 y_1, \ldots, Q_s y_s\ B(A_1, \ldots, A_m)\ ,$$

where each Q_i is either $\forall$ or $\exists$ and each A_i is an atomic formula in the variables $x_1, \ldots, x_k$ and $y_1, \ldots, y_s$ and $B(z_1, \ldots, z_m)$ is a Boolean expression without negation in the Boolean variables $z_1, \ldots, z_m$. A formula without free variables is called a sentence. We say the formulas $A(x_1, \ldots, x_k)$ and $B(x_1, \ldots, x_k)$ are equivalent if $\forall x_1, \ldots, x_k\ A(x_1, \ldots, x_k) \Leftrightarrow B(x_1, \ldots, x_k)$ is a theorem of Tarski algebra. Under the interpretation two formulas are equivalent $\Leftrightarrow$ they have the same extension over the real field. For sentences this reduces to the same truth value.

From this point formula will mean a Tarski algebra prenex formula. The size $|A|$ of a formula is just the sum of the sizes of its atomic formulas and the size of an atomic formula is the sum of the sizes of its coefficients in binary. See [1] for a very detailed account of the decision procedure complexity of Tarski algebra. Tarski proposed that the first order theory of the real field (generalized to real closed fields) is decidable in [9]. He produced a fully worked out quantifier elimination algorithm in [10]. It is interesting to note that Herbrand [11] (note on p. 581) anticipated Tarski's conjecture. Considerable improvements in the complexity of quantifier elimination for Tarski algebra have followed the original algorithm but the most substantial complexity reduction is due to Grigoriev [4]. The current result (see chapter 14, p. 518 of [1]) can be summarized as

Theorem 3. *an equivalent quantifier-free formula for a formula an be computed in time*

$$a^{O(b^{O(c+1)})}\ ,$$

where a is the size of the formula, b is the number (free and bound) of variables and c is the number of quantifier alternations.

3. The transfer method

3.1. Preliminaries

Recall that an EDE has the form

$$\exists x_1, \ldots, x_k\ P(x_1, \ldots, x_k) = 0\ .$$

Some notation is needed. The binary logarithm is written as log and $[x..y]$ is the set of integers between x and y inclusive with $x < y$. Over $\mathbb{N}$ define $x = y \bmod z$ to be the least x such that $x \equiv y \pmod z$. Let $[d_1, \ldots, d_k]P(x_1, \ldots, x_k)$ be the coefficient of $x_1^{d_1}\cdots x_k^{d_k}$. The size, $|P(x_1, \ldots, x_k)|$, of the polynomial $P(x_1, \ldots, x_k)$ is just

$$\sum_{i_1,\ldots,i_k} \lceil \log |[i_1, \ldots, i_k]P(x_1, \ldots, x_k)| \rceil\ . \tag{2}$$

Summation is only over nonzero coefficients. From Eq. (2) we have

$$|P(x_1, \ldots, x_k)| \le d_* \cdot \max \lceil \log |[i_1, \ldots, i_k]P(x_1, \ldots, x_k)| \rceil\ , \tag{3}$$

where d_* is the total degree.

From this point we let $n \in \mathbb{N}$ be an upper bound on both the absolute values of coefficients and the variables. Under the size restriction the maximum absolute value P_* assumed by $P(x_1, \ldots, x_k)$ satisfies

$$P_* \leq n^{d_*} \cdot \max |[i_1, \ldots, i_k]P(x_1, \ldots, x_k)| = n^{d_*+1} . \tag{4}$$

From Eq. (3) we get

$$|P(x_1, \ldots, x_k)| \leq d_* \cdot \log n . \tag{5}$$

Let $A_n = \exists x_1, \ldots, x_k \; P(x_1, \ldots, x_k) = 0$ under the size restriction of n. This is the form of an n-EDE. Let q be the least positive integer such that $q! > P_*$. From Eq. (4) and Stirling's factorial estimate,

$$q = O(\frac{d_* \cdot \log n}{\log \log n}) . \tag{6}$$

By the Chinese remainder theorem,

$$\bigwedge_{p \in [2..q]} P_p(x_1, \ldots, x_k) \equiv 0 \pmod p \Leftrightarrow P(x_1, \ldots, x_k) = 0 , \tag{7}$$

where $P_p(x_1, \ldots, x_k)$ is obtained from $P(x_1, \ldots, x_k)$ by restricting each x_i to $[0..p-1]$ and replacing each $|[i_1, \ldots, i_k]P(x_1, \ldots, x_k)|$ by $|[i_1, \ldots, i_k]P(x_1, \ldots, x_k)| \bmod p$. By Eq. (4), $P_{p,*}$ is at most p^{d_*+1} so

$$P_p(x_1, \ldots, x_k) \equiv 0 \pmod p \Leftrightarrow P_p(x_1, \ldots, x_k) = p \cdot x_0 , \tag{8}$$

where x_0 is bounded above by p^{d_*}.

The bounded EDE $A_{n,p}(x_1, \ldots, x_k)$ is defined by

$$\exists x_0 \; P_p(x_1, \ldots, x_k) - p \cdot x_0 = 0 , \tag{9}$$

where $x_0 < p^{d_*}$. From Eq. (7), Eq. (8) and Eq. (9) it is clear that

$$A_n \Leftrightarrow \exists x_1, \ldots, x_k \bigwedge_{p=2}^{q} A_{n,p}(x_1, \ldots, x_k) . \tag{10}$$

By Eq. (5), $|A_{n,p}(x_1, \ldots, x_k)|$ is at most

$$d_* \lceil \log p \rceil . \tag{11}$$

3.2. Proof of Theorem 1

We sketch a method that transfers each $A_{n,p}(x_1, \ldots, x_k)$ to a formula $B_{n,p}(x_1, \ldots, x_k)$ such that

$$A_{n,p}(x_1, \ldots, x_k) \Leftrightarrow B_{n,p}(x_1, \ldots, x_k) .$$

Using Theorem 3 each $B_{n,p}(x_1, \ldots, x_k)$ can be efficiently converted into an equivalent quantifier-free formula $B'_{n,p}(x_1, \ldots, x_k)$. It follows from Eq. (10) that the time to decide A_n is at most the time to decide

$$\exists x_1, \ldots, x_k \bigwedge_{p=2}^{q} B'_{n,p}(x_1, \ldots, x_k) .$$

We begin with a simple lemma which elaborates on numerals in Tarski algebra.

Lemma 1. *A formula $I_{2^{g+1}-1}(x) \Leftrightarrow x \in [0..2^{g+1}-1]$ can be constructed with size $O(g^2)$ and with $O(g)$ existentially bound variables.*

Proof. The term (numeral) $\overbrace{2 \times \cdots \times 2}^{k}$ defines 2^k and has size $O(k)$. Here, 2 abbreviates $1+1$. We write 2^k for this term. The formula $I_{2^{g+1}-1}(x)$ given by

$$\exists y_0, \ldots, y_g \bigwedge_{i=1}^{g} (y_i = 0 \vee y_i = 1) \wedge x = y_0 \cdot 2^0 + \cdots + y_g \cdot 2^g$$

defines $x \in [0..2^{g+1}-1]$. □

We can now prove Theorem 1.

Proof. Noting Eq. (9), $A_{n,p}(x_1,\ldots,x_k)$ can be transferred to the formula $\exists x_0\, C_{n,p}(x_0,\ldots,x_k)$ given by

$$\exists x_0\; P_p(x_1,\ldots,x_k) - p\cdot x_0 = 0 \bigwedge_{i=0}^{k} I_{m_i}(x_i)\;,$$

where for $i\in[1..k]$, m_i is the least $2^{g_i+1}-1$ larger than p and m_0 is the least $2^{g_0+1}-1$ larger than p^{d_*}. It is clear that

$$A_{n,p}(x_1,\ldots,x_k) \Leftrightarrow \exists x_0\; C_{n,p}(x_0,x_1,\ldots,x_k)\;.$$

By Theorem 3, $\exists x_0\; C_{n,p}(x_0,\ldots,x_k)$ can be converted into an equivalent quantifier-free formula $B_{n,p}(x_1,\ldots,x_k)$ in time $|P_p(x_1,\ldots,x_k)|^{O(1)}$. By this time bound, Eq. (11) and Lemma 1, $|B_{n,p}(x_1,\ldots,x_k)|$ is bounded above by $(d_*\cdot\log p)^{O(1)}$ and involves at most $O(d_*\cdot\log p)$ existentially quantified variables, all from the $I_{m_i}(x_i)$.

From Eq. (10) we have

$$A_n \Leftrightarrow \exists x_1,\ldots,x_k) \Leftrightarrow \exists x_1,\ldots,x_k \bigwedge_{p=2}^{q} B_{n,p}(x_1,\ldots,x_k)\;. \tag{12}$$

By Theorem 3, each $B_{n,p}(x_1,\ldots,x_k)$ can be converted in time

$$(d_*\cdot\log)^{O(d_*\cdot\log p)} \tag{13}$$

into an equivalent quantifier-free formula $B'_{n,p}(x_1,\ldots,x_k)$. Thus,

$$A_n \Leftrightarrow \exists x_1,\ldots,x_k \bigwedge_{p=2}^{q} B'_{n,p}(x_1,\ldots,x_k)\;.$$

It follows from Theorem 3 and Eq. (13) that the time to produce all of the $B'_{n,p}(x_1,\ldots,x_k)$ and so also $\bigwedge_{p=2}^{q} B'_{n,p}(x_1,\ldots,x_k)$ is bounded above by

$$(d_*\cdot\log p)^{O(d_*\cdot\log p)}\;,$$

which by Eq. (6) is bounded above by

$$2^{O(d_*\cdot\log^{O(1)}n)}$$

The final elimination of the existentially bound $x_1,\ldots,x_k$ yields the same type of bound since $k=O(1)$. □

We remark that $d_*=O(1)$ but we have kept it visible.

3.3. Proof of Theorem 2

From Eq. (1) and Theorem 1, SBQR can be decided in time

$$2^{O(\log\log b)^{O(1)}}\;,$$

where total degree has been absorbed in the outer O-notation. Using the **NP** convention for problem size we write $n=\log b$. Under polynomial time reduction a size n instance of a problem in **NP** can be mapped to a size n^a instance of SBQR. This accounts for the form of the bound in Theorem 2.

4. Remarks

The complexity of residue arithmetic (Chinese remaindering) has been intensively studied in terms of parallel complexity. Two examples of these studies are [2,5]. The base case for our method is the linear n-EDE. Study of systems of linear n-EDE has a rich history. A definitive basis for a complexity analysis of these systems has been given by T. Skolem [8]. (See Theorem 5, p. 10.) It is important to compare the transfer method complexity in the linear case with the 19-th century Theorem 5.

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry, Springer, 2006.
[2] A. Chiu, G. Davida, B. Litow, Division in logspace-uniform NC^1, Theor. Inform. Appl. 35 (2001) 259–275.
[3] T. Cormen, C. Leiserson, R. Rivest, C. Stein, Introduction to Algorithms, 3rd ed., MIT Press, 2009.
[4] D.Yu. Grigoriev, Complexity of deciding Tarski algebra, J. Symbolic Comput. 5 (1988) 65–108.
[5] W. Hesse, E. Allender, D. Mix Barrington, Uniform constant-depth threshold circuits for division and iterated multiplication, J. Comput. System Sci. 65 (4) (2002) 695–716.
[6] K. Manders, L. Adleman, NP-complete decision problems for binary quadratics, J. Comput. System Sci. 16 (1978) 168–184.
[7] Y.V. Matiyasevich, Hilbert's Tenth Problem, MIT Press, 1993.
[8] T. Skolem, Diophantische Gleichungen, Chelsea Pub. Co., 1950.
[9] A. Tarski, Sur les ensembles définissables de nombres réels, Fund. Math. 17 (1931).
[10] A. Tarski, A Decision Method for Elementary Algebra and Geometry, Technical report, Rand Corp, 1948.
[11] J. van Heijenoort, From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931, Harvard Univ. Press, 1977.