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

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