journal of Groups, Complexity, Cryptology
Volume 18, Issue 1, 2026, pp. 2:1–2:4
https://gcc.episciences.org/

Submitted Jan. 12, 2026
Published Apr. 1, 2026

ON THE DIOPHANTINE PROBLEM RELATED TO POWER CIRCUITS

ALEXANDER RYBALOV

Sobolev Institute of Mathematics, Pevtsova 13, Omsk 644099, Russia.
e-mail address: alexander.rybalov@gmail.com

Abstract. Myasnikov, Ushakov, and Won introduced power circuits in 2012 to construct a polynomial-time algorithm for the word problem in the Baumslag group, which has a non-elementary Dehn function. Power circuits are computational structures that support addition and the operation $(x, y) \mapsto x \cdot 2^y$ on integers. They also posed the question of decidability of the Diophantine problem over the structure $\langle \mathbb{N}_{>0}; +, x \cdot 2^y, \leq, 1\rangle$, which is closely related to power circuits. In this paper, we prove that the Diophantine problem over this structure is undecidable.

Dedicated to Alexei Miasnikov
on the occasion of his birthday.

1. Introduction

Power circuits have been introduced by Myasnikov, Ushakov, and Won in [7] as computational structures supporting addition and the operation $(x, y) \mapsto x \cdot 2^y$ on integers. Using power circuits they constructed in [6] a polynomial-time algorithm for the word problem in the Baumslag group

$$G_{(1,2)} = \langle a, b \mid b^{-1}a^{-1}bab^{-1}ab = a^2\rangle,$$

which has a non-elementary Dehn function.

Myasnikov, Ushakov, and Won posed in [7, Problem 10.3] the question of decidability of the Diophantine problem over the structure

$$\widetilde{N} = \langle \mathbb{N}_{>0}; +, x \cdot 2^y, \leq, 1\rangle,$$

which is closely related to power circuits. Here $\mathbb{N}$ denotes the set of natural numbers including zero, and $\mathbb{N}_{>k}$ denotes the set of natural numbers greater than k.

Recall that the Diophantine problem $\mathcal{DP}(\widetilde{N})$ over $\widetilde{N}$ is the algorithmic problem of deciding whether a given equation or a system of equations over $\widetilde{N}$ has a solution. The classical Diophantine problem $\mathcal{DP}(\mathbb{N})$ over the structure $\langle \mathbb{N}; +, \cdot, 1\rangle$, known as Hilbert's tenth problem, is undecidable, as proved by Matiyasevich in [5], building on earlier work of Davis, Putnam, and Robinson in [2]. On the other hand, Semenov in [9] proved decidability of the first-order theory of natural numbers with addition and exponentiation $\langle \mathbb{N}; +, x \mapsto 2^x, 1\rangle$. It follows that the Diophantine problem over this structure is decidable.

Key words and phrases: Diophantine problem, power circuit.
2020 *Mathematics Subject Classification.* 11U05, 03D35.
Supported by Russian Science Foundation, grant 25-11-20023.

DOI:10.46298/jgcc.2026.18.1.17270

In this paper, we prove that the Diophantine problem over the structure $\widetilde{N}$ is undecidable. As a consequence, this resolves another question posed in [7, Problem 10.5]: "Is $\widetilde{N}$ automatic?" The answer is negative, since every automatic structure has a decidable first-order theory [3], and hence a decidable Diophantine problem.

2. Main result

Consider the following variant of the Diophantine problem, denoted by $\mathcal{DP}(\mathbb{N}_{>k})$, that asks whether a given system of equations over $\mathbb{N}$ admits a solution in $\mathbb{N}_{>k}$.

Lemma 2.1. *For every natural number k there is a Cook/Turing reduction from $\mathcal{DP}(\mathbb{N})$ to $\mathcal{DP}(\mathbb{N}_{>k})$.*

Proof. For a given system of Diophantine equations $S(x_1, \ldots, x_n)$ we enumerate all subsets Y of $X = \{x_1, \ldots, x_n\}$ and all possible assignments from $\{0, \ldots, k\}$ for the variables in Y, i.e., functions $f : Y \to \{0, \ldots, k\}$. Then for each f we define the system S_f by replacing each variable $y \in Y$ in S with the value $f(y)$. Denote the resulting finite set of systems by $A(S)$. It is straightforward to verify that the system $S(x_1, \ldots, x_n)$ has a solution in $\mathbb{N}$ if and only if at least one system $S' \in A(S)$ has a solution in $\mathbb{N}_{>k}$. □

Corollary 2.2. *For every natural number k the problem $\mathcal{DP}(\mathbb{N}_{>k})$ is undecidable.*

Consider the structure $\widetilde{N} = \langle \mathbb{N}_{>0}; +, x \cdot 2^y, \leq, 1 \rangle$. To prove undecidability of the Diophantine problem over $\widetilde{N}$ we reduce $\mathcal{DP}(\mathbb{N}_{>1})$ to $\mathcal{DP}(\widetilde{N})$. For this purpose it is sufficient to define the multiplication of numbers greater than 1 in $\widetilde{N}$.

A relation $R \subseteq \mathbb{N}_{>1}^k$ is *Diophantine definable* in $\widetilde{N}$ if there exists a system of equations (a conjunction of atomic formulas) $S(y_1, \ldots, y_k, x_1, \ldots, x_n)$ over $\widetilde{N}$ such that

$$\forall a_1 \ldots \forall a_k \; R(a_1, \ldots, a_k) \Leftrightarrow \exists x_1 \ldots \exists x_n \; S(a_1, \ldots, a_k, x_1, \ldots, x_n).$$

Also, a function $f : \mathbb{N}_{>1}^k \to \mathbb{N}_{>1}$ is *Diophantine definable* in $\widetilde{N}$ if the graph of a function f is Diophantine definable in $\widetilde{N}$.

We use notation $a \mid b$ for $a, b \in \mathbb{N}$ if a divides b.

Lemma 2.3. *For all $n, m \in \mathbb{N}$ the following holds:*

$$m \mid n \Leftrightarrow 2^m - 1 \mid 2^n - 1.$$

Proof. Suppose m divides n and $n = km$ for some $k \in \mathbb{N}$. Then

$$2^n - 1 = 2^{km} - 1 = (2^m - 1)(2^{m(k-1)} + \ldots + 2^m + 1).$$

Suppose m does not divide n and $n = km + r$ with natural k and $0 < r < m$. Then

$$2^n - 1 = 2^{km+r} - 2^r + 2^r - 1 = 2^r(2^{km} - 1) + 2^r - 1$$

is not divisible by $2^m - 1$ since $2^m - 1$ divides $2^{km} - 1$ and $2^m - 1 > 2^r - 1 > 0$. □

Lemma 2.4. *The divisibility relation $x \mid y$ is Diophantine definable in $\widetilde{N}$.*

Proof. By Lemma 2.3

$$x \mid y \Leftrightarrow \exists z \; 2^y - 1 = z(2^x - 1) \Leftrightarrow \exists z \; 2^y + z = z \cdot 2^x + 1.$$ □

Robinson proved in [8] that the first-order theory of natural numbers with addition and divisibility relation is undecidable. But Beltjukov in [1] and Lipshitz in [4] proved that the Diophantine problem over this structure is decidable. Therefore, the Diophantine definability of the divisibility relation is not sufficient to prove the undecidability of the Diophantine problem over $\widetilde{N}$ and we need further research.

Lemma 2.5. *The strict order relation $x < y$ is Diophantine definable in $\widetilde{N}$.*

Proof. Note that $x < y \Leftrightarrow \exists z\ x + z = y$. □

We use notation $\lfloor a \rfloor$ to denote the integer part of a real number a.

Lemma 2.6. *The integer binary logarithm $\lfloor \log_2 x \rfloor$ for $x > 1$ is Diophantine definable in $\widetilde{N}$.*

Proof. Note that

$$y = \lfloor \log_2 x \rfloor \Leftrightarrow (2^y \le x) \wedge (x < 2^{y+1}).$$ □

Lemma 2.7. *The function $sq(x) = x^2$ for $x > 1$ is Diophantine definable in $\widetilde{N}$.*

Proof. The set

$$S(x) = \{kx(x+1)\ :\ k \in \mathbb{N}\}$$

is Diophantine definable in $\widetilde{N}$, since

$$y \in S(x) \Leftrightarrow (x \mid y) \wedge (x+1 \mid y).$$

Now consider the following Diophantine definable set in $\widetilde{N}$:

$$S'(x) = \{y\ :\ y + x \in S(x),\ \lfloor \log_2 y \rfloor \le 2\lfloor \log_2 x \rfloor + 1\}.$$

If $k \ge 4$, then

$$\lfloor \log_2(kx(x+1) - x) \rfloor = \lfloor \log_2(kx^2 + (k-1)x) \rfloor \ge \lfloor \log_2(kx^2) \rfloor =$$
$$= \lfloor \log_2 k + 2\log_2 x \rfloor \ge \lfloor 2 + 2\log_2 x \rfloor \ge 2 + \lfloor 2\log_2 x \rfloor \ge 2 + 2\lfloor \log_2 x \rfloor.$$

Hence, for every $x > 1$ we have

$$S'(x) \subseteq \{x^2, 2x^2 + x, 3x^2 + 2x\}.$$

Note that $x^2 \in S'(x)$ since

$$\lfloor \log_2(x^2) \rfloor = \lfloor 2\log_2 x \rfloor \le 2\lfloor \log_2 x \rfloor + 1.$$

To ensure that $2x^2 + x$ and $3x^2 + 2x$ do not belong to $S'(x)$, consider the following Diophantine over $\widetilde{N}$ condition:

$$P(x, y) = (x + 2 \mid y + 2x) \wedge (x + 3 \mid y + 3x).$$

Element x^2 satisfies this condition because $x + 2$ divides $x^2 + 2x$ and $x + 3$ divides $x^2 + 3x$. On the other hand, $2x^2 + x + 2x = (2x - 1)(x + 2) + 2$ does not satisfy this condition, because it is not divisible by $x + 2$ for all natural x. Similarly, $3x^2 + 2x + 2x = (3x - 2)(x + 2) + 4$ does not belong to P, because it is divisible by $x + 2$ only for $x = 2$, but for $x = 2$ we see that $3x^2 + 2x + 3x = 22$ is not divisible by $x + 3 = 5$. □

Lemma 2.8. *The multiplication operation $mul(x, y) = xy$ for $x, y > 1$ is Diophantine definable in $\widetilde{N}$.*

Proof. Note that

$$z = xy \Leftrightarrow 2z = (x + y)^2 - x^2 - y^2 \Leftrightarrow z + z + x^2 + y^2 = (x + y)^2.$$ □

Theorem 2.9. *The Diophantine problem over* $\widetilde{N} = \langle \mathbb{N}_{>0}; +, x \cdot 2^y, \leq, 1 \rangle$ *is undecidable.*

Proof. We reduce $\mathcal{DP}(\mathbb{N}_{>1})$ to the Diophantine problem over $\widetilde{N}$ in the following way. Without loss of generality any given nontrivial system S of Diophantine equations over $\mathbb{N}_{>1}$ consists of equations of the form $P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)$, where P and Q are non-zero polynomials with positive integer coefficients. Such system S can be transformed to an equivalent system in the *Skolem form*, consisting of equations of the following types:

(1) $x_i = x_j x_k$,
(2) $x_i = x_j + x_k$,
(3) $x_i = x_j + 1$,
(4) $x_i = x_j$.

By Lemma 2.8, we can replace every equation of type (1) by an equivalent system of equations over $\widetilde{N}$. Also for every variable x, which is included in equations of types (2), (3) or (4), but not included in any equation of type (1), we add the Diophantine condition $x > 1$ using Lemma 2.5. By construction, the obtained system of equations over $\widetilde{N}$ is equivalent to the original system S over $\mathbb{N}_{>1}$.

By Corollary 2.2, the problem $\mathcal{DP}(\mathbb{N}_{>1})$ is undecidable; therefore, $\mathcal{DP}(\widetilde{N})$ is also undecidable. □

Since every automatic structure has a decidable first-order theory [3], we obtain the following corollary of Theorem 2.9.

Corollary 2.10. $\widetilde{N}$ *is not automatic.*

Acknowledgment

The author thanks Alexander Ushakov for many useful suggestions and remarks.

References

[1] A. P. Beltjukov. Decidability of the universal theory of natural numbers with addition and divisibility. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 60:15–28, 1976.
[2] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Ann. Math.*, 74(3):425–436, 1961.
[3] B. Khoussainov and A. Nerode. Automatic presentations of structures. *Lect. Notes Comput. Sci.*, 960:367–392, 1995.
[4] L. Lipshitz. Undecidable existential problems for addition and divisibility in algebraic number rings. ii. *Proc. Amer. Math. Soc.*, 64(1):122–128, 1977.
[5] Yu. V. Matiyasevich. The diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191(2):279–282, 1970.
[6] A. G. Myasnikov, A. Ushakov, and D. Won. The Word Problem in the Baumslag group with a non-elementary Dehn function is polynomial time decidable. *J. Algebra*, 345:324–342, 2011.
[7] A. G. Myasnikov, A. Ushakov, and D. Won. Power circuits, exponential algebra, and time complexity. *Int. J. Algebra Comput.*, 22(6):3–53, 2012.
[8] J. Robinson. Definability and decision problems in arithmetic. *J. Symb. Log.*, 14:98–114, 1949.
[9] A. L. Semenov. Logical theories of one-place functions on the natural number series. *Izv. Akad. Nauk SSSR Ser. Mat.*, 47(3):623–658, 1983.