S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Том 22, № 1, стр. 683–691 (2025) УДК 510.652
https://doi.org/10.33048/semi.2025.22.045 MSC 11U99

О ПРОБЛЕМЕ P=NP В НЕКОТОРЫХ КОЛЬЦАХ

А.Н. Рыбалов

Представлено С.В. Судоплатовым

Abstract: We consider a computational complexity theory over arbitrary algebraic structures based on an approach to generalized computability developed by Ashaev, Belyaev and Myasnikov. Let $\mathcal{R}$ be a ring with a nilpotent element η of nilpotency index $k > 1$ such that η is an algebraic element over $\mathbb{Z}$ of degree k. We prove that analogs of the classical computational complexity classes **P** and **NP** over $\mathcal{R}$ are different.

Keywords: computational complexity, P vs NP, ring, nilpotent element.

1 Введение

Теория сложности вычислений над произвольными алгебраическими системами берет свое начало с работы Блюм, Шуба и Смейла [2], в которой она была развита на основе теории вычислимости над кольцами и полями. В ее рамках были определены аналоги классических полиномиальных классов **P** и **NP**. Причем последний связан с так называемыми инструкциями подсказки — командами, которые могут записывать в регистры вычислительных устройств произвольное число из $\mathbb{C}$. В работе [3] был рассмотрен прямой аналог классического класса **NP** — класс **DNP**, определенный при помощи машин с недетерминированными

Rybalov, A.N., On the P=NP problem in some rings.

Работа поддержана грантом Российского Научного Фонда № 25-11-20023.
Поступила 25 мая 2025 г., опубликована 4 июля 2025 г.

ветвлениями. Инструкции недетерминированных ветвлений могут быть смоделированы при помощи подсказок, поэтому имеет место включение **DNP** $\subseteq$ **NP**. В дальнейшем этот подход был обобщен на произвольные алгебраические системы в работе [1]. На его основе в [7] была развита теория сложности вычислений в алгебраических системах.

Наибольший интерес в теории сложности вычислений над алгебраическими системами представляет аналог известной проблемы о совпадении классов **P** и **NP**. Было получено много результатов о несовпадении этих классов над различными системами. Меер [5] доказал, что **P** $\neq$ **DNP** над аддитивной группой поля вещественных чисел. Гасснер [4] доказала неравенство **P** $\neq$ **DNP** для всех бесконечных абелевых групп, а Прунеску [6] для бесконечных булевых алгебр. Рыбалов [8] доказал, что имеет место неравенство **P** $\neq$ **DNP** над кольцами вещественных матриц. Для упоредоченного поля $\mathbb{R}$ и для поля $\mathbb{C}$ проблема **P** $\neq$ **DNP** до сих пор нерешена.

Данная работа продолжает и расширяет эти исследования. Основным результатом является доказательство неравенства **P** $\neq$ **DNP** для любого кольца, в котором существует нильпотентный элемент индекса нильпотентности $k > 1$, который также является алгебраическим над $\mathbb{Z}$ степени k. Например таковыми являются различные кольца матриц (например, рассмотренные в [8]), а также некоторые ассоциативные алгебры, связанные с алгебрами Ли.

2 Предварительные сведения

Пусть дана алгебраическая система $\mathfrak{A} = \langle A, \sigma \rangle$. Следуя [1], введем списочную надстройку $HL(A)$ множества A

$$L_0 = A, \quad L_{n+1} = L(L_n) \cup L_n,$$

$$HL(A) = \bigcup_{n=0}^{\infty} L_n(A),$$

где $L(M)$ – множество всех конечных списков с элементами из M. Расширим сигнатуру σ до сигнатуры

$$\sigma^* = \sigma \cup \{=, \mathrm{cons}^{(2)}, \mathrm{tail}^{(1)}, \mathrm{head}^{(1)}, \mathrm{nil}\},$$

где функции cons – добавление одного списка в конец другого, tail – отбрасывание первого элемента списка, head – взятие первого элемента списка, а константа nil – пустой список. В итоге получаем систему

$$HL(\mathfrak{A}) = \langle HL(A), \sigma^* \rangle,$$

которая называется списочной надстройкой системы $\mathfrak{A}$. За основную вычислительную модель примем машины с неограниченными регистрами (МНР) над $HL(\mathfrak{A})$. Эти вычислительные устройства имеют конечный набор регистров, в которых можно хранить элементы $HL(A)$, и программу, состоящую из набора команд, которые могут записывать в регистры значения функций и констант из σ^* и совершать условные ветвления в зависимости от истинности предикатов из σ^*. Нас будут интересовать только МНР, распознающие некоторые подмножества $HL(A)$, поэтому будем предполагать, что программы МНР могут содержать команды `accept` и `reject`, выполнение которых приводит к остановке МНР и к допусканию, либо отверганию входного списка. Будем говорить, что МНР M распознает множество $S \subseteq HL(A)$, если

- $x \in S \Leftrightarrow M$ допускает x,
- $x \notin S \Leftrightarrow M$ отвергает x.

Заметим, что МНР распознающая некоторое множество всегда останавливается. Далее будем рассматривать только такие машины. Недетерминированные МНР имеют команды недетерминированных ветвлений, после выполнения которых управление может быть передано одной из двух команд.

Определим функцию размера $size_{HL} : HL(A) \to \mathbb{N}$ следующим образом

$$size_{HL}(\alpha) = \begin{cases} 1, \text{ если } \alpha = \mathrm{nil} \text{ или } \alpha \in A, \\ \\ size_{HL}(\alpha_1) + \ldots + size_{HL}(\alpha_n) + 1, \text{ при } \alpha = \langle \alpha_1, \ldots, \alpha_n \rangle. \end{cases}$$

По МНР M над $HL(\mathfrak{A})$ определим функцию времени t_M. Если M на входе x не останавливается, полагаем $t_M(x) = \infty$. Пусть $\tau = \{I_1, \ldots, I_n\}$ — вычислительный путь M на x. Положим

$$t_{M,\tau}(x) = \sum_{k=1}^{n} time(I_k),$$

где $time(I_k) = 1$, если I_k – одна из следующих команд

$$\begin{array}{l} R_m := c, \; c \in \sigma^* - \text{константа}, \\ R_m := f(R_{i_1}, \ldots, R_{i_m}), \; \text{где } f \in \sigma - \text{функция}, \\ \texttt{if } P(R_{i_1}, \ldots, R_{i_m}) \texttt{ then goto } l, \; \text{где } P \in \sigma - \text{предикат}, \\ \texttt{if } ? \texttt{ then goto } l, \\ \texttt{accept}, \\ \texttt{reject}, \end{array}$$

и $time(I_k) = size_{HL}(\alpha_l)$, если I_k – одна из команд

$$\begin{array}{l} R_m := R_l, \\ R_m := \mathrm{tail}(R_l), \\ R_m := \mathrm{head}(R_l), \end{array}$$

где α_l – содержимое регистра R_l. Наконец

$$time(I_k) = size_{HL}(\alpha_l) + size_{HL}(\alpha_r),$$

если I_k – одна из команд

$$\begin{array}{l} R_m := \mathrm{cons}(R_l, R_r), \\ \texttt{if } R_l = R_r \texttt{ then goto } t, \end{array}$$

где α_l, α_r – содержимые R_l, R_r. Положим теперь $t_M(x) = t_{M,\tau}(x)$ для детерминированной МНР M. Для недетерминированной МНР M мы будем использовать полную запись $t_{M,\tau}(x)$.

Будем говорить, что детерминированная МНР M полиномиальна, если существует полином p такой, что

$$\forall x \in HL(A)\ M \text{ останавливается на } x \text{ и } t_M(x) < p(size_{HL}(x)).$$

В класс $\mathbf{P}_{\mathfrak{A}}$ входят все подмножества $HL(A)$, распознаваемые полиномиальными детерминированными МНР. Множество $S \subseteq HL(A)$ принадлежит классу $\mathbf{DNP}_{\mathfrak{A}}$, если существует такая недетерминированная МНР M и такой полином p, что

$$x \in S \Leftrightarrow \text{существует вычислительный путь } \tau \text{ МНР } M \text{ на } x$$
$$\text{такой, что } M \text{ принимает } x \text{ и } t_{M,\tau}(x) < p(size_{HL}(x)).$$

3 Характеристики вычислительных путей

Пусть $\tau = I_1, \ldots, I_k$ – вычислительный путь МНР M на входе $\alpha \in HL(A)$. Очевидно, что на всем протяжении работы M в регистрах находятся списки, элементы которых – термы сигнатуры σ от содержащихся во входном списке α праэлементов $a_1, \ldots, a_n$ (выписанных в том порядке, в котором они встречаются в α при его просмотре слева направо). Определим структуру списка следующим образом

$$struc(\alpha) = \begin{cases} \text{nil}, \text{ если } \alpha = \text{nil или } \alpha \in A, \\ \langle struc(\alpha_1), \ldots, struc(\alpha_n) \rangle, \text{ если } \alpha = \langle \alpha_1, \ldots, \alpha_n \rangle. \end{cases}$$

Заменим все праэлементы $a_1, \ldots, a_n$ в списке α переменными $x_1, \ldots, x_n$. Содержимые регистров МНР вдоль пути τ теперь – это списки с элементами-термами сигнатуры σ от переменных x_i. Рассмотрим все условия в командах условного перехода пути τ. Все они имеют вид либо $R_i = R_j$, либо $P(R_{i_1}, \ldots, R_{i_s})$, где P – предикат из σ. Эти условия можно представить как набор атомарных формул сигнатуры σ от переменных x_i следующим образом: равенства списков представляются равенствами их соответствующих элементов-термов в случае, если их структуры равны, иначе имеем тождественно ложную формулу; любой предикат P представляется им же самим, если его аргументы – праэлементы, иначе – тождественно ложной формулой. Теперь набор $\varphi_1(\bar{x}), \ldots, \varphi_m(\bar{x})$ из всех нетождественных формул среди полученных таким образом формул назовем характеристикой пути τ. Аналогично определяется характеристика начального участка пути. Заметим, что $m \leq t_M(\alpha)$ – это непосредственно следует из определения функции времени. Назовем список β эквивалентным списку α для МНР M, если

- $struc(\alpha) = struc(\beta)$,
- $\varphi_i(\bar{a}) \leftrightarrow \varphi_i(\bar{b})\ \forall i = 1, \ldots, m$, где $\bar{a}, \bar{b}$ – праэлементы списков α и β соответственно, выписанные слева направо.

Следующая полезная лемма была доказана в [9].

Лемма 1. *Пусть M — детерминированная МНР, распознающая некоторое множество $\Delta \in HL(A)$. Если элемент $\beta \in HL(A)$ эквивалентен входу $\alpha \in HL(A)$ для МНР M, то $\alpha \in \Delta \Leftrightarrow \beta \in \Delta$.*

4 Основной результат

Пусть $\mathcal{R} = \langle R; \{+, -, \times, 0, 1\} \rangle$ – кольцо в стандартной сигнатуре. Допустим, что в этом кольце существует ненулевой нильпотентный элемент η индекса нильпотентности $k > 1$. То есть k – наименьшее натуральное такое, что $\eta^k = 0$. Очевидно, что η является алгебраическим над $\mathbb{Z}$, так как удовлетворяет уравнению $x^k = 0$. Допустим, что степень алгебраического элемента η над $\mathbb{Z}$ равна k, то есть $f(\eta) \neq 0$ для любого ненулевого целочисленного многочлена f степени меньше k.

Для любого размера n рассмотрим множество списков глубины 1 с целочисленными элементами

$$\Omega_n = \{\langle x_1, \dots, x_n \rangle : \exists I \subseteq \{1, \dots, n\},\ I \neq \varnothing,\ \sum_{i \in I} x_i = 0\} =$$

$$= \bigcup_{I \subseteq \{1,\dots,n\},\ I \neq \varnothing} \{\langle x_1, \dots, x_n \rangle : \sum_{i \in I} x_i = 0\}.$$

Также рассмотрим аналогичное множество списков с элементами из кольца $\mathcal{R}$

$$\Omega_n(\mathcal{R}) = \{\langle x_1, ..., x_n \rangle :\ x_1, ..., x_n \in R,\ \exists I \subseteq \{1, ..., n\},\ I \neq \varnothing,\ \sum_{i \in I} x_i = 0\}.$$

Теперь положим

$$\Omega = \bigcup_{n=1}^{\infty} \Omega_n,\ \Omega(\mathcal{R}) = \bigcup_{n=1}^{\infty} \Omega_n(\mathcal{R}).$$

Лемма 2. *Для любых целых чисел $x_1, \dots, x_n$ имеет место*

$$\langle x_1\eta, \dots, x_n\eta \rangle \in \Omega(\mathcal{R}) \Leftrightarrow \langle x_1, \dots, x_n \rangle \in \Omega.$$

Доказательство. Непосредственно следует из того, что $r\eta = 0$ для $r \in \mathbb{Z}$ тогда и только тогда, когда $r = 0$. □

Лемма 3. $\Omega(\mathcal{R}) \in \mathbf{DNP}_{\mathcal{R}}$.

Доказательство. Недетерминированная МНР для $\Omega(\mathcal{R})$ при помощи недетерминированных ветвлений решает, включать ли элемент во входном списке в тестируемую сумму или нет, а затем проверяет, равна ли эта сумма 0 или нет. Поэтому $\Omega(\mathcal{R}) \in \mathbf{DNP}_{\mathcal{R}}$. □

Следующая лемма дает полезную информацию о покрытии множеств Ω алгебраическими множествами.

Лемма 4. *Пусть*

$$\Omega_n \subseteq \bigcup_{i=1}^{m} \{\langle x_1,\dots,x_n\rangle : f_i(x_1,\dots,x_n)=0\},$$

где f_i *— непостоянные целочисленные многочлены, имеющие степень меньше* k *по любой переменной. Тогда* $m > \frac{2^{n-1}-1}{k}$.

Доказательство. Заметим, что

$$\bigcup_{i=1}^{m} \{\langle x_1,\dots,x_n\rangle : f_i(x_1,\dots,x_n)=0\} \subseteq$$

$$\subseteq \{\langle x_1,\dots,x_n\rangle : \prod_{i=1}^{m} f_i(x_1,\dots,x_n)=0\}.$$

Теперь покажем, что для любого непустого $I \subseteq \{1,\dots,n\}$ и для некоторого многочлена f если имеет место

$$\{\langle x_1,\dots,x_n\rangle : \sum_{i\in I} x_i = 0\} \subseteq$$

$$\subseteq \{\langle x_1,\dots,x_n\rangle : f(x_1,\dots,x_n)=0\},$$

то f делится на $\sum_{i\in I} x_i$.

Без ограничения общности можно полагать, что $I=\{1,\dots,s\},\ s\le n$. Представим многочлен f в виде

$$f(x_1,\dots,x_n) = g(x_1,\dots,x_n)(x_1+\ldots+x_s)+$$

$$+h(x_1,\dots,x_{s-1},x_{s+1},\dots,x_n),$$

где g,h — некоторые многочлены.

Такое представление возможно. Действительно, сделаем замену $t = x_1+\ldots+x_s$, выразим переменную $x_s = t-x_1-\ldots-x_{s-1}$. Представим многочлен f уже от переменных $x_1,\dots,x_{s-1},x_{s+1},\dots,x_n,t$ как многочлен от переменной t с коэффициентами-многочленами от остальных переменных. Теперь вынесем переменную t как множитель у всех степеней t больше нулевой. Заметим, что остаток (то есть свободный член в этом представлении) не зависит от t, а зависит от остальных переменных $x_1,\dots,x_{s-1},x_{s+1},\dots,x_n$. Затем вернемся обратно к иксам, заменив переменную t обратно на $x_1+\ldots+x_s$. Получим нужное нам представление.

Теперь если многочлен h не равен тождественно нулю, то можно выбрать целые числа $a_1,\dots,a_{s-1},a_{s+1},\dots,a_n$ так, что

$$h(a_1,\dots,a_{s-1},a_{s+1},\dots,a_n)\neq 0.$$

Теперь, взяв $a_s = -(a_1+\ldots+a_{s-1})$, мы получим, что $a_1+\ldots+a_s=0$, но $f(a_1,\dots,a_s)=0$, что противоречит исходной посылке. Таким образом, мы доказали, что f делится на $x_1+\ldots+x_s$.

Применяя полученное утверждение ко всем непустым подмножествам $I \subseteq \{1, \dots, n\}$, получаем, что многочлен $\prod_{i=1}^{m} f_i(x_1, \dots, x_n)$ делится на все $2^n - 1$ линейных многочлена $\sum_{i \in I} x_i$, а, значит, и на их произведение

$$\prod_{I \subseteq \{1,\dots,n\}} (\sum_{i \in I} x_i),$$

которое имеет степень $2^{n-1} - 1$ по каждой переменной. А так как все многочлены f_i имеют степени по всем переменным меньше k, то $m > \frac{2^{n-1}-1}{k}$. □

Докажем также еще одну полезную лемму о покрытии.

Лемма 5. *Пусть $f_i(x_1, \dots, x_n)$, $i = 1, \dots, m$ – конечный набор многочленов с целыми коэффициентами, среди которых нет тождественно равных нулю. Тогда*

$$\mathbb{Z}^n \neq \bigcup_{i=1}^{m} \{(x_1, \dots, x_n) \ : \ f_i(x_1, \dots, x_n) = 0\}.$$

Доказательство. Так как

$$\bigcup_{i=1}^{m} \{(x_1, \dots, x_n) \ : \ f_i(x_1, \dots, x_n) = 0\} =$$

$$= \{(x_1, \dots, x_n) \ : \ \prod_{i=1}^{m} f_i(x_1, \dots, x_n) = 0\},$$

то достаточно доказать лемму для одного многочлена $f(x_1, \dots, x_n)$.

Теперь нужное утверждение следует из известного факта коммутативной алгебры ([10], теорема 14): *Пусть $f(x_1, \dots, x_n)$ – ненулевой полином над областью целостности R и Q – бесконечное подмножество R. Тогда существуют $a_1, \dots, a_n \in Q$ такие, что $f(a_1, \dots, a_n) \neq 0$.* □

Теперь все готово, чтобы доказать основное утверждение.

Теорема 1. *Пусть в кольце $\mathcal{R}$ есть нильпотентный элемент η индекса нильпотентности $k > 1$, являющийся алгебраическим над $\mathbb{Z}$ степени k. Тогда $\mathbf{P}_{\mathcal{R}} \neq \mathbf{DNP}_{\mathcal{R}}$.*

Доказательство. По лемме 3 $\Omega(\mathcal{R}) \in \mathbf{DNP}_{\mathcal{R}}$. Докажем, что $\Omega(\mathcal{R}) \notin \mathbf{P}_{\mathcal{R}}$.

Предположим, что $\Omega(\mathcal{R}) \in \mathbf{P}_{\mathcal{A}}$ и распознается некоторой детерминированной МНР M за время, ограниченное полиномом p от размера входа. Выберем n достаточно большим, чтобы выполнялось неравенство $p(n+1) < \frac{2^{n-1}-1}{k^2}$.

Рассмотрим вход $\alpha = \langle a_1\eta, \dots, a_n\eta \rangle$ с целочисленными $(a_1, \dots, a_n)$. Характеристикой вычислительного пути M на входе α будет набор равенств от элементов $a_i\eta$

$$f_i(x_1, \dots, x_n) = 0, \ i = 1, \dots, l,$$

где f_i – непостоянные многочлены степени меньше k по каждой переменной (так как $\eta^k = 0$) с коэффициентами из $\mathbb{Z}$. Приравнивая к 0 коэффициенты при каждой степени η (так как η алгебраический над $\mathbb{Z}$ степени k), каждое такое равенство можно переписать как не более чем k равенств уже от чисел a_i

$$f_{i,j}(x_1, \ldots, x_n) = 0,\ i = 1, \ldots, m,\ j = 0, \ldots, k-1,$$

где многочлены $f_{i,j}$ опять имеют степени меньше k по каждой переменной. Перенумеруем эти многочлены для единообразия g_i, $i = 1, \ldots, m \le p(n+1)k$.

Целочисленные коэффициенты этих многочленов ограничены по модулю $2^{2^{p(n+1)}}$. Это следует из того, что на каждом шаге работы машины коэффициенты с прошлого шага могут самое большее перемножаться, а шагов не больше $p(n+1)$. Теперь рассмотрим множество всех целочисленных многочленов от n переменных степени меньше k по каждой переменной, у которых коэффициенты не превосходят $2^{2^{p(n+1)}}$, и которые не тождественно равны нулю. Их конечное число, поэтому по лемме 5 существует набор целых чисел $(a_1, \ldots, a_n)$, на которых любой из этих многочленов не равен нулю. Зафиксируем этот выбор $(a_1, \ldots, a_n)$.

По выбору чисел $a_1, \ldots, a_n$ имеет место $g_i(a_1, \ldots, a_n) \ne 0$ для всех $i = 1, \ldots, m$. Так как $m \le p(n+1)k < \frac{2^{n-1}-1}{k}$, то из леммы 4 следует, что

$$\Omega_n \not\subseteq \bigcup_{i=1}^{m} \{(x_1, \ldots, x_n) : g_i(x_1, \ldots, x_n) = 0\}.$$

Поэтому существуют такие целые числа $b_1, \ldots, b_n$, что $\langle b_1, \ldots, b_n \rangle \in \Omega$, но, в то же время, $g_i(b_1, \ldots, b_n) \ne 0$ для всех $i = 1, \ldots, m$. А значит и $\langle b_1\eta, \ldots, b_n\eta \rangle \in \Omega(\mathcal{R})$, но $f_i(b_1\eta, \ldots, b_n\eta) \ne 0$ для всех $i = 1, \ldots, l$. Но это означает, что список $\beta = \langle b_1\eta, \ldots, b_n\eta \rangle$ эквивалентен списку α и, по лемме 1, $\beta \notin \Omega(\mathcal{R})$, в то время, как, по лемме 2, $\beta \in \Omega(\mathcal{R})$. Полученное противоречие завершает доказательство теоремы. □

Автор выражает благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

References

[1] I.V. Ashaev, V.Ya. Belyaev, A.G. Myasnikov, *Toward a generalized computability theory*, Algebra Logic, **32**:4 (1993), 183–205. Zbl 0829.03023

[2] L. Blum, M. Shub, S. Smale, *On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines*, Bull. Amer. Math. Soc. (N.S.), **21**:1 (1989), 1–46. Zbl 0681.03020

[3] F. Cucker, M. Matamala, *On digital nondeterminism*, Math. Syst. Theory, **29**:6 (1996), 635–647. Zbl 0868.68058

[4] C. Gaßner, *The P-DNP problem for infinite Abelian groups*, J. Complexity, **17**:3 (2001), 574–583. Zbl 0988.68074

[5] K. Meer, *A note on a $P \neq NP$ result for a restricted class of real machines*, J. Complexity, **8**:4 (1992), 451–453. Zbl 0758.68030

[6] M. Prunescu, *$P \neq NP$ for all infinite Boolean algebras*, Math. Log. Q., **49**:2 (2003), 210–213. Zbl 1029.68070

[7] A. Rybalov, *Computational complexity in algebraic systems*, Sib. Math. J., **45**:6 (2004), 1113–1123. Zbl 1096.03046

[8] A. Rybalov, *On the P-NP problem over real matrix rings*, Theor. Comput. Sci., **314**:1-2 (2004), 281–285. Zbl 1070.68045

[9] A. Rybalov, *Relativizations of the $P = NP$ problem over the complex number field*, Sib. Èlectron. Mat. Izv., **1** (2004), 91–98. Zbl 1079.03033

[10] O. Zariski, P. Samuel, *Commutative algebra. I*, Graduate Texts in Mathematics, **28**, Springer-Verlag, New York etc., 1975. Zbl 0313.13001

Alexander Nikolaevich Rybalov
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia,
Pevtsova 13,
Omsk, 644099, Russia
Email address: alexander.rybalov@gmail.com