S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 1, стр. 91–98 (2004) УДК 510.52, 510.57
MSC 03D60, 68Q15

РЕЛЯТИВИЗАЦИИ ВОПРОСА P=NP НАД ПОЛЕМ КОМПЛЕКСНЫХ ЧИСЕЛ

А.Н. РЫБАЛОВ

Abstract. In this article we consider the relativised polynomial complexity classes $P_{\mathbb{C}}$ and $DNP_{\mathbb{C}}$ over the complex number field $\mathbb{C}$, defined in the frames of an approach to generalized computability, considered in [1]. We prove that $P_{\mathbb{C}}^{\mathbb{Z}} \neq DNP_{\mathbb{C}}^{\mathbb{Z}}$, where the oracle $\mathbb{Z}$ is the set of integers.

1. Введение

Блюм, Смейлом и Шубом в [3] была предложена теория вычислимости и вычислительной сложности над произвольными кольцами и полями, в частности над полями комплексных и действительных чисел. 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 [5] был рассмотрен прямой аналог классического класса NP — класс DNP, определенный при помощи машин с недетерминированными 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 [7]. В статье [1] был предложен иной подход к обобщенной вычислимости, на основе которого в [2] была развита теория сложности вычислений в алгебраических системах.

С самого начала изучения вопросов сложности вычислений в полях $\mathbb{C}$ и $\mathbb{R}$, исследователей интересуют вопросы о строгости включений $P \subseteq NP$ и $P \subseteq DNP$ над этими полями. Несмотря на многочисленные исследования, эти вопросы до сих пор остаются открытыми.

Rybalov, A.N., Relativizations of the P=NP problem over the complex number field.

Поступила 15 сентября 2004 г., опубликована 22 ноября 2004 г.

В работе [4] были построены такие оракулы A и B, что $P^A = NP^A$ и $P^B \neq NP^B$. Этот результат о противоречивых релятивизациях говорит о ограниченности классических методов, связанных с диагонализацией, в попытке разделить классы P и NP. Неформально, это связано с тем, что доказательство неравенства $P \neq NP$ при помощи диагонализации можно релятивизовать по любому оракулу и оно доказывало бы гораздо большее, а именно, неравенство $P^A \neq NP^A$ для любого оракула.

В качестве оракула A, для которого $P^A_{\mathbb{C}} = NP^A_{\mathbb{C}}$ (а значит и $P^A_{\mathbb{C}} = DNP^A_{\mathbb{C}}$, т.к. для любого оракула A имеет место $P^A_{\mathbb{C}} \subseteq DNP^A_{\mathbb{C}}$) можно выбрать любое NP-полное множество, существование которых доказано в [3] и [2]. Действительно, для A имеет место $NP_{\mathbb{C}} \subseteq P^A_{\mathbb{C}}$, т.к. если $S \in NP_{\mathbb{C}}$, то полиномиальная машина с оракулом, распознающая S, действует на входе x так: сначала вычисляет $f(x)$, где f — полиномиальная сводимость S к A, а затем проверяет, верно или нет, что $f(x) \in S$. С другой стороны, имеет место $NP^A_{\mathbb{C}} \subseteq NP_{\mathbb{C}}$, т.к. если в недетерминированной машине, распознающей за полиномиальное время некоторое множество S, заменить все обращения к оракулу A на вызовы недетерминированной машины, распознающей A, мы получим недетерминированную машину без оракулов, распознающую S за полиномиальное время. Таким образом, имеет место $NP^A_{\mathbb{C}} \subseteq P^A_{\mathbb{C}}$. Обратное включение следует непосредственно из определений этих классов. Это рассуждение по сути повторяет классическую схему из [4].

Основным результатом данной статьи является доказательство неравенства $P^{\mathbb{Z}} \neq DNP^{\mathbb{Z}}$ над полем $\mathbb{C}$ в рамках модели вычислимости из работы [1], где оракул $\mathbb{Z}$ — множество целых чисел. Аналогичный результат без труда можно получить для модели Блюм-Смейла-Шуба. Заметим, что техника, которую мы будем применять для этого, существенно отличается от классической схемы из работы [4]. Заметим также, что в работе [6] был доказан аналог теоремы Бэйкера-Джилла-Соловэя для упорядоченного поля действительных чисел.

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. Релятивизованные МНР в условных переходах могут иметь обращения к оракулу $S \subseteq HL(A)$, которые проверяют принадлежность содержимого регистров множеству S.

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

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

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

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

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

$R_m := R_l$,
$R_m := \text{tail}(R_l)$,
$R_m := \text{head}(R_l)$,
`if` $R_l \in S$ `then goto` l,

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

$R_m := \text{cons}(R_l, R_r)$,
`if` $R_l = R_r$ `then goto` t,

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

$$x \in S \Leftrightarrow \text{существует вычислительный путь } \tau \text{ МНР } M \text{ на } x$$

$$\text{такой, что } M \text{ принимает } x \text{ и } t_{M,\tau}(x) < p(size_{HL}(x)).$$

Совершенно аналогично определяются релятивизованные классы $P^S_{\mathfrak{A}}$ и $DNP^S_{\mathfrak{A}}$ для любого оракула $S \subseteq HL(A)$.

В заключение этой главы рассмотрим одно полезное свойство вычислительных путей детерминированных МНР. 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

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

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 $\bar{b}$ – праэлементы списка β, выписанные слева направо.

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 $\alpha \in \Delta \Leftrightarrow \beta \in \Delta$.*

Доказательство. Пусть МНР M имеет программу $I_1, \ldots, I_f$. Пусть $\tau = I_{i_1}, \ldots, I_{i_s}$ – вычислительный путь M на α, $\lambda = I_{j_1}, \ldots, I_{j_r}$ – на β. Докажем индукцией по номеру команды в пути τ, что для любого $n = 1, \ldots, s$ $I_{i_n} = I_{j_n}$. Из этого будет следовать, что $\tau = \lambda$, а потому их последние команды совпадают и МНР принимает или отвергает α и β одновременно.

Основание индукции. При $n = 1$ и для α и для β выполняется первая команда I_1.

Шаг индукции состоит в рассмотрении типа команды I_{i_n}. Если эта не команда условного перехода, то $I_{i_{n+1}} = I_{j_{n+1}}$ – следующая после I_{i_n} команда в программе M. Если I_{i_n} – команда условного перехода, то заметим, что характеристика начального участка $I_{i_1}, \ldots, I_{i_n}$ пути τ для α является характеристикой этого же участка для β (по предположению индукции эти участки в τ и λ совпадают). А т.к. условие в I_{i_n} зависит только от истинности формул характеристики и β эквивалентен α, то $I_{i_{n+1}} = I_{j_{n+1}}$. □

3. Основной результат

Рассмотрим поле комплексных чисел

$$\mathfrak{C} = \langle \mathbb{C}, \{0, 1, +, -, \times, /\} \rangle.$$

Наша цель – доказать неравенство $P^{\mathbb{Z}}_{\mathfrak{C}} \neq DNP^{\mathbb{Z}}_{\mathfrak{C}}$. МНР с оракулом $\mathbb{Z}$ над $\mathfrak{C}$ могут иметь в своей программе инструкции типа

$$\texttt{if } R_n \in \mathbb{Z} \texttt{ then goto } q.$$

Заметим, что такие МНР можно рассматривать как МНР без оракула над системой

$$\mathfrak{C}^{\mathbb{Z}} = \langle \mathbb{C}, \{Int, 0, 1, +, -, \times, /\} \rangle,$$

где одноместный предикат Int выделяет множество $\mathbb{Z}$.

Для доказательства нужного неравенства мы покажем, что множество списков глубины 1

$$\Omega = \{\langle x_1, \ldots, x_n \rangle : \exists I \subseteq \{1, \ldots, n\} \sum_{i \in I} x_i \in \mathbb{Z}\} =$$

$$= \bigcup_{I \subseteq \{1, \ldots, n\}} \{\langle x_1, \ldots, x_n \rangle : \sum_{i \in I} x_i \in \mathbb{Z}\}$$

лежит в классе $DNP_{\mathfrak{C}^{\mathbb{Z}}}$, но не лежит в $P_{\mathfrak{C}^{\mathbb{Z}}}$.

Докажем сначала несколько алгебраических лемм о покрытии множества Ω объединениями множеств специального типа.

Лемма 2. *Пусть имеет место включение*

$$\{(x_1, \ldots, x_n) : \sum_{i=1}^{k} x_i \in \mathbb{Z}\} \subseteq \bigcup_{j=1}^{m} \{(x_1, \ldots, x_n) : f_j(x_1, \ldots, x_n) \in \mathbb{Z}\}, \tag{1}$$

где $k \leq n$ и f_j – рациональные функции с целыми коэффициентами, не равные тождественно константе. Тогда существует $i \leq m$ такое, что

$$f_i(x_1, \ldots, x_n) = f(x_1 + \ldots + x_k),$$

где f – рациональная функция от одной переменной.

Доказательство. Случай $n = 1$ очевиден. Далее предполагаем, что $n > 1$. Обозначим $t = x_1 + \ldots + x_k$ и для всех $j = 1, \ldots, m$ через $\tilde{f}_j$ обозначим функцию f_j после подстановки вместо x_1 выражения $t - x_2 - \ldots - x_k$. Некоторые из переменных $x_2, \ldots, x_n$ в $\tilde{f}_j$ после такой подстановки могут исчезнуть, сократившись. Если в некоторой $\tilde{f}_i$ осталась только одна переменная t, то f_i и есть искомая, т.к. тогда

$$\tilde{f}_i(t, x_2, \ldots, x_n) = f(t) = f(x_1 + \ldots + x_k) = f_i(x_1, \ldots, x_n).$$

Предположим, что это не так и придем к противоречию. Покажем, что существует такое целое b, что $\tilde{f}_j(b, x_2, \ldots, x_n)$ не константа для всех $j = 1, \ldots, m$. Действительно, пусть

$$\tilde{f}_j(t, x_2, \ldots, x_n) = \frac{\sum_{k=1}^{s} g_k(t) M_k + g_{s+1}(t)}{\sum_{k=1}^{r} h_k(t) N_k + h_{r+1}(t)},$$

где g_k, h_k — ненулевые полиномы с целыми коэффициентами, M_k, N_k — мономы от переменных $x_2, \ldots, x_n$ (причем M_k попарно различны и N_k попарно различны). Если $\tilde{f}_j(b, x_2, \ldots, x_n)$ — константа, то либо b — корень всех полиномов g_k, либо b — корень некоторых полиномов g_k, h_k (эти полиномы есть коэффициенты при мономах, которые есть в числителе, но отсутствуют в знаменателе и наоборот, если множества мономов в числителе и знаменателе разные), либо выполняется

$$\frac{g_1(b)}{h_j(b)} = \ldots = \frac{g_s(b)}{h_s(b)},$$

если $s = r$ и $M_k = N_k$, $k = 1, \ldots, s$. Т.к. g_k, h_k — полиномы, то последние равенства могут выполняться либо для конечного множества чисел b, либо для всех b. В последнем случае $\tilde{f}_j(t, x_2, \ldots, x_n) = f(t)$, что противоречит нашему предположению.

Итак, в любом случае получается, что $\tilde{f}_j(b, x_2, \ldots, x_n)$ может быть константой только для конечного числа b. Значит можно подобрать такое целое b, что $\tilde{f}_j(b, x_2, \ldots, x_n)$ не константа для всех $j = 1, \ldots, m$. Зафиксируем такое b.

Возьмем алгебраически независимые над $\mathbb{Z}$ комплексные числа $a_2, \ldots, a_n$. Т.к. набор $(b - a_2 - \ldots - a_k, a_2, \ldots, a_n)$ принадлежит левому множеству во включении (1), то существует $i \leq m$ такое, что

$$\tilde{f}_i(b, a_2, \ldots, a_n) = f_i(b - a_2 - \ldots - a_k, a_2, \ldots, a_n) \in \mathbb{Z}.$$

Теперь равенство $\tilde{f}_i(b, a_2, \ldots, a_n) = s \in \mathbb{Z}$ дает нетривиальное алгебраическое соотношение над $\mathbb{Z}$ между $a_2, \ldots, a_n$, что противоречит выбору чисел $a_2, \ldots, a_n$. □

Лемма 3. *Пусть имеет место включение*

$$\Omega \subseteq \bigcup_{j=1}^{m} \{(x_1, \ldots, x_n) : f_j(x_1, \ldots, x_n) \in \mathbb{Z}\},$$

где f_j – рациональные функции с целыми коэффициентами, не равные тождественно константе. Тогда $m \geq 2^n - 1$.

Доказательство. Из леммы 2 следует, что для каждого подмножества $I \subseteq \{1, \ldots, n\}$ найдется $f_j(x_1, \ldots, x_n) = g_j(\sum_{i \in I} x_i)$, где g_j рациональная функция

от одной переменной. Теперь заметим, что одна такая функция соответствует только одному подмножеству. Действительно, если имеет место

$$g_i\Big(\sum_{i\in I} x_i\Big) = g_j\Big(\sum_{j\in J} x_j\Big),$$

то любая переменная из левой части должна входить в правую и наоборот, откуда $I = J$ и $g_i = g_j$. Т.к. различных подмножеств $\{1,\dots,n\}$ существует $2^n - 1$, то существует по крайней мере $2^n - 1$ различных функций f_j. □

Теперь все готово, чтобы доказать основное утверждение.

Теорема 1. *$\Omega \in DNP_{\mathfrak{C}^{\mathbb{Z}}}$ но $\Omega \notin P_{\mathfrak{C}^{\mathbb{Z}}}$. Таким образом*

$$P^{\mathbb{Z}}_{\mathfrak{C}} \neq DNP^{\mathbb{Z}}_{\mathfrak{C}}.$$

Доказательство. Недетерминированная МНР первого рода для Ω при помощи недетерминированных ветвлений решает, включать ли число во входном списке в тестируемую сумму или нет, а затем проверяет, принадлежит ли эта сумма $\mathbb{Z}$ или нет. Поэтому $\Omega \in DNP^{\mathbb{Z}}_{\mathfrak{C}}$.

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

Рассмотрим вход $\alpha = \langle a_1,\dots,a_n\rangle$ с алгебраически независимыми над $\mathbb{Z}$ числами $a_1,\dots,a_n$. Очевидно, что $\alpha \notin \Omega$ и $size_{HL}(\alpha) = n+1$. Характеристикой вычислительного пути M на входе α будет набор равенств

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

и предикатов

$$Int(f_j(x_1,\dots,x_n)),\ j = k+1,\dots,k+m,$$

где f_i, f_j – непостоянные рациональные функции с коэффициентами из $\mathbb{Z}$. Причем $k + m \le p(n+1)$. Т.к. $a_1,\dots,a_n$ алгебраически независимые над $\mathbb{Z}$, то $f_i(\alpha) \neq 0$ и $f_j(\alpha) \notin Z$ для всех $i = 1,\dots,k$ и для всех $j = k+1,\dots,k+m$.

Т.к. $k + m \le p(n+1) < 2^n - 1$, то из леммы 3 следует, что

$$\Omega \not\subseteq \bigcup_{j=1}^{k+m} \{(x_1,\dots,x_n) : f_j(x_1,\dots,x_n) \in \mathbb{Z}\}.$$

Поэтому существует такой список $\beta = \langle b_1,\dots,b_n\rangle$, что $\beta \in \Omega$, но, в то же время, $f_j(b_1,\dots,b_n) \notin \mathbb{Z}$ для всех $j = 1,\dots,k+m$, а значит и $f_i(b_1,\dots,b_n) \neq 0$ для $i = 1,\dots,k$. Но теперь список β эквивалентен списку α и, по лемме 1, $\beta \notin \Omega$, что противоречит выбору β. □

Список литературы

[1] И.В. Ашаев, В.Я.Беляев, А.Г. Мясников, *Подходы к теории обобщенной вычислимости*, Алгебра и логика, **32**:4 (1993), 349–386.

[2] А.Н. Рыбалов, *Сложность вычислений в алгебраических системах*, Сибирский математический журнал, **45**:6 (2004), 1365–1377.

[3] 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., **21** (1989), 1–46.

[4] T. Baker, J. Gill, R. Solovay, *Relativizations of the P=?NP question*, SIAM Journal on Computing, **4** (1975), 431–442.

[5] F. Cucker, M. Matamala, *On digital nondeterminism*, Math. Syst. Theory, **29** (1996), 635–647.
[6] T. Emerson, *Relativization of the P=?NP question over the reals (and other ordered rings)*, Theoretical Computer Science, **133** (1994), 15–22.
[7] A. Hemmerling, *Computability and complexity over structures*, Math. Logic Quarterly, **44**:1 (1998), 1–44.

Александр Николаевич Рыбалов
Омский государственный университет,
пр. Мира 55а,
644077, Омск, Россия
E-mail address: rybalov@omskreg.ru