Записки научных
семинаров ПОМИ
Том 399, 2012 г.

А. А. Кноп

ДИОФАНТОВА ИЕРАРХИЯ

§1. Введение

Теорема Дэвиса–Путнама–Робинсон–Матиясевича (ДПРМ), закрывшая десятую проблему Гильберта, гласит, что всякое перечислимое множество является диофантовым. Из ДПРМ теоремы вытекают многие результаты в теории вычислимости [5].

Исследование ограниченной версии этого вопроса начали Адлеман и Мандерс [1]. Они определили следующий класс языков:

Определение 1.1. *Язык* L *принадлежит классу* D*, если и только если существуют такие целочисленные многочлены* P*,* q *с целыми коэффициентами, что* [1] [2]*:*

$$(x_1,\dots,x_n)\in\mathsf{L}\Leftrightarrow\exists y_1,\dots,y_m \leqslant 2^{q(|\sum_{i=1}^n x_i|)}\ [P(x_1,\dots,x_n,y_1,\dots,y_m)=0].$$

Они же поставили вопрос о равенстве классов D и **NP**. Для исследования этого вопроса они ввели следующее определение [2]:

Определение 1.2.

(1) *Пусть* R *и* S *–* n*- и* l*-местные отношения на множестве неотрицательных целых чисел. Будем говорить, что* R D*-сводимо к* S *тогда и только тогда, когда существуют такие целочисленные многочлены* P*,* q*, что:*

$$R(x_1,\dots,x_n)\Leftrightarrow\ \exists y_1,\dots,y_l,y_{l+1}\dots,y_m \leqslant 2^{q(|\sum_{i=1}^n x_i|)}[P(x_1,\dots,x_n,y_1,\dots,y_m)=0\wedge S(y_1,\dots,y_l)].$$

(2) *Отношение* R *из* **NP** *будем называть* D*-полным, если любое отношение из* **NP** D*-сводимо к* R*.*

Ключевые слова: диофантова сложность.

Исследования частично поддержаны грантом РФФИ (11-01-12135-офи-м-2011) и стипендией Computer Science клуба.

[1] Здесь и далее мы будем брать кванторы существования и всеобщности по множеству неотрицательных целых чисел.

[2] Мы будем обозначать через $|x|$ длину битовой записи x.

Также Адлеман и Мандерс нашли несколько простых D-полных языков.

Теорема 1.1 (см. [2])**.**

(1) *Пусть* $R_0(x)$ *– отношение, истинное, если и только если* x *принадлежит регулярному языку* $\{10, 00\}^*$*, тогда* R_0 D*-полно.*

(2) *Пусть* Nocarry(x, y) *– отношение, истинное, если в двоичной записи при сложении* x *и* y *нет переносов. Тогда* Nocarry D*-полно.*

Продолжили изучение этого вопроса Липма [3] и Поллет [4] в 2003 году. Первый определил класс **PD** (диофантов аналог класса **P**) и исследовал его применение в криптографии, а второй доказал достаточный признак равенства D и **NP**.

Теорема 1.2 (см. [4])**.** *Если* **co-NLOGTIME** *содержится в* D*, то* D *равно* **NP**.

К сожалению, определение класса D у Адлемана и Мандерса не слишком удобно (например, для него не удается доказать замкнутость относительно объединения и пересечения). Поэтому мы изменим определение и сделаем в нем оценки различными для разных переменных. Получившийся класс содержит класс, определенный Адлеманом и Мандерсом (новый класс будем обозначать **D**).

В разделах 2.1 и 2.2 даются основные определения и доказываются простые утверждения. В разделе 2.3 доказывается, что отношение $R(a, b, c) \Leftrightarrow a = b^c$ содержится в **D**, что дает возможность вычислять битовую длину выражений и увеличивать ограничения на длину подкванторных переменных. В разделе 2.5 будет исследован диофантов аналог полиномиальной иерархии (диофантова иерархия), продемонстрирована эквивалентность оракульного и кванторных определений иерархии, а в разделе 2.6 будет показано, что полиномиальная и диофантова иерархии послойно содержатся одна в другой, в частности, **NP** содержится во втором уровне диофантовой иерархии.

§2. Результаты

2.1. Основные определения.

Определение 2.1. *Определим следующие понятия: многочлен с оракулами и значение многочлена с оракулами. Пусть* $x_1, \ldots, x_n$ *– переменные, а* $O_1, \ldots, O_m$ *– функциональные символы;* $y_1, \ldots y_n$, $k_1, \ldots,$

k_m – целые числа; $F_1, \ldots, F_m$ – отображения из $\mathbb{Z}^{k_i}$ в $\mathbb{Z}$ для каждого i от 1 до m. Тогда будем говорить, что P – оракульный многочлен (или многочлен с оракулами) от переменных $x_1, \ldots, x_n$ с оракулами $O_1, \ldots, O_m$ со значением z при значении переменных и оракулов $y_1, \ldots, y_n, F_1, \ldots, F_m$ соответственно, если выполнено одно из условий:

(1) $P = c \wedge z = c$, *где* c – *целое число.*
(2) $P = x_i \wedge z = y_i$ *при* $1 \leqslant i \leqslant n$.
(3) $P = P_1 \# P_2 \wedge z = z_1 \# z_2$, *где* $\# \in \{\times, +, -\}$ *и* P_1, P_2 – *многочлены от переменных* $x_1, \ldots, x_n$ *с оракулами* $O_1, \ldots, O_m$ *со значениями* z_1, z_2 *при значении переменных* $y_1, \ldots, y_n$ *и оракулов* $F_1, \ldots, F_m$.
(4) $O_i(P_1, \ldots, P_{k_i}) \wedge z = F_i(z_1, \ldots, z_{k_i})$ *при* $1 \leqslant i \leqslant m$, *где* $P_1, \ldots, P_{k_i}$ – *многочлены от переменных* $x_1, \ldots, x_n$ *с оракулами* $O_1, \ldots, O_m$ *со значениями* $z_1, \ldots, z_{k_i}$ *при значении переменных* $y_1, \ldots, y_n$ *и значении оракулов* $F_1, \ldots, F_m$.

Значение многочлена с оракулами мы будем обозначать так: $P[x_1 = y_1, \ldots, x_n = y_n, O_1 = F_1, \ldots, O_m = F_m]$.

Определение 2.2. *Если P, Q – оракульные многочлены, а x – переменная, то $P[x = Q]$ – это такой оракульный многочлен, что выполнено одно из условий:*

(1) $P = c \wedge P[x = Q] = c$, *где* c – *целое число.*
(2) $P = x \wedge P[x = Q] = Q$.
(3) $P = y \wedge P[x = Q] = P$ *при* $x \neq y$.
(4) $P = P_1 \# P_2 \wedge P[x = Q] = P_1[x = Q] \# P_2[x = Q]$, *где* $\# \in \{\times, +, -\}$.
(5) $O_i(P_1, \ldots, P_{k_i}) \wedge P[x = Q] = O_i(P_1[x = Q], \ldots, P_{k_i}[x = Q])$ *при* $1 \leqslant i \leqslant m$.

Замечание 2.1. Мы определили оракульный многочлен как некоторую формулу, но в дальнейшем мы, как правило, будем говорить о нем как о функции, имея в виду, что мы фиксируем порядок переменных и оракулы.

Определение 2.3. *Назовем n-местное отношение $R(x_1, \ldots, x_n)$ диофантовым полиномиально ограниченным с оракулами $O_1, \ldots, O_k$, если существует P – многочлен с оракулами $O_1, \ldots, O_k$, и многочлены*

$k_1, \ldots, k_m$, такие, что

$$R(x_1,\ldots,x_n) \Leftrightarrow \exists y_1,\ldots,y_m\ [P(x_1,\ldots,x_n,y_1,\ldots,y_m)=0 \wedge |y_1|<k_1(|x_1|,\ldots,|x_n|)\wedge \ldots \wedge |y_m|<k_m(|x_1|,\ldots,|x_n|)].$$

Пару из многочлена P и последовательности $\{k_i\}_{i=1}^m$ назовем диофантовым представлением отношения $R(x_1,\ldots,x_n)$.

Определение 2.4. *Назовем n-местное отношение $R(x_1,...,x_n)$ кодиофантовым полиномиально ограниченным с оракулами O_1,...,O_k, если отношение $\neg R$ — диофантово полиномиально ограниченное с этими оракулами.*

Определение 2.5. *Назовем n-арную частичную функцию $F(x_1,\ldots,x_n)$ диофантово полиномиально ограниченной с оракулами $O_1, \ldots, O_k$, если существует многочлен P с оракулами $O_1, \ldots, O_k$ и многочлены $k_1, \ldots, k_{m+l}$, такие, что*

$$F(x_1,\ldots,x_n)=(y_1,\ldots,y_m) \Leftrightarrow \exists y_{m+1},\ldots,y_{m+l}\ [P(x_1,\ldots,x_n,y_1,\ldots,y_{m+l})=0\wedge |y_1|<k_1(|x_1|,\ldots,|x_n|)\wedge \ldots \wedge |y_{m+l}|<k_{m+l}(|x_1|,\ldots,|x_n|)].$$

Пару из многочлена P и последовательности $\{k_i\}_{i=1}^{m+l}$ назовем ограниченным диофантовым представлением функции $F(x_1,\ldots,x_n)$.

Определение 2.6. *Язык* L *принадлежит классу $\mathbf{D}^A$, если существует диофантово полиномиально ограниченное отношение $R(x_1,\ldots,x_n)$ с оракулами из A, для которого выполнено условие*

$$(x_1,\ldots,x_n)\in \mathtt{L} \Leftrightarrow R(x_1,\ldots,x_n).$$

Замечание 2.2. Пусть f – функция. Мы будем обозначать $\mathbf{D}^{\{f\}}$ как $\mathbf{D}^f$, а $\mathbf{D}^{\varnothing}$ как $\mathbf{D}$. А если L – язык, то $\mathbf{D}^L$ – это $\mathbf{D}^f$, где f — характеристическая функция языка L.

2.2. Тривиальные теоремы.

Лемма 2.1. *Если* $R_1(x_1,\dots,x_n,y_{1,1},\dots,y_{1,m_1})$ *и* $R_2(x_1,\dots,x_n,y_{2,1},\dots,y_{2,m_2})$ *– полиномиально ограниченные диофантовы отношения с оракулами* $O_1,\dots,O_l$, *то следующие отношения тоже полиномиально ограниченные отношения с оракулами* $O_1,\dots,O_l$:

$$R_1(x_1,\dots,x_n,y_{1,1},\dots,y_{1,m_1})\wedge R_2(x_1,\dots,x_n,y_{2,1},\dots,y_{2,m_2})$$
$$R_1(x_1,\dots,x_n,y_{1,1},\dots,y_{1,m_1})\vee R_2(x_1,\dots,x_n,y_{2,1},\dots,y_{2,m_2})$$

Доказательство. Пусть $(P_1,\{k_{1,i}\}_{i=1}^{p_1})$ и $(P_2,\{k_{2,i}\}_{i=1}^{p_2})$ – диофантовы представления R_1 и R_2 соответственно. Тогда нам подойдут следующие отношения (которые, очевидно, диофантовы):

$$\begin{aligned}\exists z_{1,1},\dots,z_{1,p_1},&z_{2,1},\dots,z_{2,p_2}\\ &[(P_1(x_1,\dots,x_n,y_{1,1},\dots,y_{1,m_1},z_{1,1},\dots,z_{1,p_1}))^2\\ &+(P_2(x_1,\dots,x_n,y_{2,1},\dots,y_{2,m_2},z_{2,1},\dots,z_{2,p_2}))^2=0\\ &\wedge|z_{1,1}|<k_{1,1}(|x_1|,\dots,|x_n|,|y_{1,1}|,\dots,|y_{1,m_1}|)\wedge\\ &\dots\\ &\wedge|z_{2,p_2}|<k_{2,p_2}(|x_1|,\dots,|x_n|,|y_{2,1}|,\dots,|y_{2,m_2}|)]\end{aligned}$$

и

$$\begin{aligned}\exists z_{1,1},\dots,z_{1,p_1},&z_{2,1},\dots,z_{2,p_2}\\ &[(P_1(x_1,\dots,x_n,y_{1,1},\dots,y_{1,m_1},z_{1,1},\dots,z_{1,p_1}))\\ &\cdot(P_2(x_1,\dots,x_n,y_{2,1},\dots,y_{2,m_2},z_{2,1},\dots,z_{2,p_2}))=0\\ &\wedge|z_{1,1}|<k_{1,1}(|x_1|,\dots,|x_n|,|y_{1,1}|,\dots,|y_{1,m_1}|)\wedge\\ &\dots\\ &\wedge|z_{2,p_2}|<k_{2,p_2}(|x_1|,\dots,|x_n|,|y_{2,1}|,\dots,|y_{2,m_2}|)].\end{aligned}$$

□

Лемма 2.2.

(1) *Функция* $\operatorname{rem}(x,y)$, *такая, что при* $y\neq 0$ *выполнено* $z=\operatorname{rem}(x,y)\Leftrightarrow(x\equiv z\pmod y\wedge 0\leqslant z<y)$ *– диофантово полиномиально ограниченная.*

(2) *Функция* $\operatorname{quot}(x,y)$ *равная, при* $y\neq 0$ *выражению* $\lfloor\frac{x}{y}\rfloor$ *– диофантово полиномиально ограниченная.*

(3) *Отношение* $\mathrm{equal}\,(x,y) \Leftrightarrow x = y$ *– диофантово полиномиально ограниченное.*
(4) *Отношение* $\mathrm{less}\,(x,y) \Leftrightarrow x < y$ *– диофантово полиномиально ограниченное.*
(5) *Отношение* $\mathrm{greater}\,(x,y) \Leftrightarrow x > y$ *– диофантово полиномиально ограниченное.*

Лемма 2.3. *Если класс* **P** *содержится в* $\mathbf{D}^A$*, то* **NP** *содержится в* $\mathbf{D}^A$*.*

Доказательство. Пусть язык L лежит в **NP**, тогда существует детерминированная полиномиальная по времени машина Тьюринга M, такая, что[3]

$$x \in \mathtt{L} \Leftrightarrow \exists y\ [M(x,y) = 1 \wedge |y| < p(|x|)],$$

но для M, по условию, существует диофантово отношение R, такое, что

$$R(x,y) \Leftrightarrow M(x,y) = 1.$$

А значит,

$$x \in \mathtt{L} \Leftrightarrow \exists y\ [R(x,y) \wedge |y| < p(|x|)]. \qquad \square$$

2.3. Возведение в степень. Ограниченная диофантовость возведения в степень была известна еще Адлеману и Мандерсу, но в связи с высокой важностью этого утверждения, а также в связи с тем, что в их работах доказательство не приводится, мы приведем здесь доказательство, автором которого является Ю. В. Матиясевич.

Определение 2.7. *Для произвольного целого* b *определим последовательность целых чисел:*

$$\alpha_b(0) = 0, \quad \alpha_b(1) = 1, \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n), \quad n = 0, 1, \ldots.$$

Лемма 2.4. *При* $n \geqslant 0$ *и* $b > 1$ *верно:* $\alpha_b(n+1) > \alpha_b(n)$*.*

Доказательство. Доказывать будем индукцией по n. База при n, равном нулю, очевидна. Теперь докажем переход от n к $n{+}1$. Проведем цепочку преобразований:

$$\alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) > (b-1)\alpha_b(n+1) \geqslant \alpha_b(n+1). \qquad \square$$

Следствие 2.1 (см., например, в [6])**.** Для $b \geqslant 2$ существование n, такого, что $x = \alpha_b(n+1)$ и $y = \alpha_b(n)$, эквивалентно тому, что x больше y и $x^2 - bxy + y^2 = 1$.

[3]Мы будем писать $M(x) = 1$, если M останавливается и принимает на входе x.

Лемма 2.5 (см., например, в [6]). *Если* $b_1 \equiv b_2 \pmod m$, *то для любого* $n > 0$, *верно:* $\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \pmod m$.

Лемма 2.6 (см., например, в [6]). *Для любого* $n \geqslant 0$, *верно* $\alpha_2(n) = n$.

Следствие 2.2 (см., например, в [6]). Для любого $b > 3$ и $n \geqslant 0$, верно: $\alpha_b(n) \equiv n \pmod{b-2}$.

Лемма 2.7. *Для любых* $b, x > 1$ *и* $c \geqslant 0$, *верно, что:*

$$b^c \equiv \alpha_x(c+1) - (x-b)\alpha_x(c) \pmod{bx - b^2 - 1}.$$

Доказательство. Доказывать будем индукцией по c. База индукции, очевидно, верна. Теперь докажем переход от c к $c+1$. По предположению индукции:

$$b^c \equiv \alpha_x(c+1) - (x-b)\alpha_x(c) \pmod{bx - b^2 - 1}.$$

Следовательно, если мы домножим на b, то получим:

$$b^{c+1} \equiv b\alpha_x(c+1) - (bx - b^2)\alpha_x(c) \pmod{bx - b^2 - 1}.$$

И так как $bx - b^2 \equiv 1 \pmod{bx - b^2 - 1}$, то

$$b^{c+1} \equiv b\alpha_x(c+1) - \alpha_x(c) \pmod{bx - b^2 - 1}.$$

Теперь прибавим и вычтем $x\alpha_b(c+1)$, тогда

$$\begin{aligned} b^{c+1} &\equiv -(x-b)\alpha_x(c+1) - \alpha_x(c) + x\alpha_x(c+1) \\ &\equiv \alpha_x(c+2) - (x-b)\alpha_x(c+1) \pmod{bx - b^2 - 1}. \end{aligned}$$

□

Следствие 2.3. Если $bx - b^2 - 1$ больше, чем b^c, то

$$b^c = \operatorname{rem}(\alpha_x(c+1) - (x-b)\alpha_x(c), bx - b^2 - 1).$$

Лемма 2.8. *Если* $b > 2$, *то для любого* n *верно, что* $\alpha_b(n) > \frac{1}{2}(\frac{b}{2})^{n-1}$.

Доказательство. По формуле явного вида линейной рекуррентной последовательности

$$\alpha_b(n) = \frac{1}{\sqrt{b^2-4}}\left(\frac{b+\sqrt{b^2-4}}{2}\right)^n - \frac{1}{\sqrt{b^2-4}}\left(\frac{b-\sqrt{b^2-4}}{2}\right)^n.$$

Оценим по отдельности каждое слагаемое:

$$\frac{1}{\sqrt{b^2-4}}\left(\frac{b+\sqrt{b^2-4}}{2}\right)^n > \frac{1}{\sqrt{b^2-4}}\left(\frac{2b-1}{2}\right)^n$$

$$\frac{1}{\sqrt{b^2-4}}\left(\frac{b-\sqrt{b^2-4}}{2}\right)^n < \frac{1}{\sqrt{b^2-4}}\left(\frac{1}{2}\right)^n.$$

И, так как $\alpha_b(1) > (\frac{1}{2}(\frac{b}{2})^0)$ и $b - \frac{1}{2} \geqslant \frac{b}{2} + \frac{1}{2}$, то верно:

$$\frac{1}{\sqrt{b^2-4}}\left(\frac{b+\sqrt{b^2-4}}{2}\right)^n > \frac{1}{\sqrt{b^2-4}}\left(\left(\frac{b}{2}\right)^n + \left(\frac{1}{2}\right)^n\right),$$

а значит:

$$\alpha_b(n) > \frac{1}{\sqrt{b^2-4}}\left(\frac{b}{2}\right)^n > \frac{1}{b}\left(\frac{b}{2}\right)^n. \qquad \square$$

Лемма 2.9. *Пусть $a, b, c > 1$, тогда, если выполнены следующие условия:*

$$x^2 - (2a+2b+2c+2)xy + y^2 = 1,$$

$$x \equiv c+2 \pmod{2a+2b+2c},$$

то верно, что b^c меньше, чем $bx - b^2 - 1$. И, более того, x, равный $\alpha_{2a+2b+2c+2}(c+2)$, и y, равный $\alpha_{2a+2b+2c+2}(c+3)$, удовлетворят этим условиям.

Доказательство. По следствию 2.1 из первого условия следует, что существует d, такое, что $x = \alpha_{2a+2b+2c+2}(d)$, а по следствию 2.2 из второго условия следует, что $d \equiv c+2 \pmod{2a+2b+2c}$. Таким образом, мы получили, что d не меньше, чем $c+2$ (так как $c+2$ меньше чем $2(a+b+c)$). И из этого следует, что x больше, чем $\frac{1}{2}(b+1)^{c+1} > \frac{1}{2}(b^{c+1}+1)$. А значит

$$bx - b^2 - 1 \geqslant \frac{1}{2}b^{c+2} + b - b^2 - 1 \geqslant 2b^c - b^2 + b - 1 > b^c. \qquad \square$$

Лемма 2.10. *Пусть $b > 1$ и $n \geqslant 0$, тогда $\alpha_b(n) < 2b^n$.*

Следствие 2.4. Существует отношение $P(x,b,c)$ – диофантово полиномиально ограниченное такое, что $P(x,b,c) \Rightarrow bx - b^2 - 1 > b^c$. И более того, для любых b и c больших одного существует x, что $P(x,b,c) \wedge |x| < p(|b^c|)$, где p – некоторый целочисленный многочлен (не зависящий от b и c).

Теорема 2.1. *Отношение $P(a,b,c)$, такое, что $P(a,b,c) \Leftrightarrow a = b^c$, содержится в* **D**.

Доказательство. Рассмотрим x, такой, что $bx - b^2 - 1 > b^c$ (по следствию 2.4 если $a \geqslant b^c$ такой x можно получить в классе $\mathbf{D}$, иначе уже здесь наш предикат станет ложным), тогда нам надо проверить, что $a = \mathrm{rem}(\alpha_x(c+1) - (x-b)\alpha_x(c), bx - b^2 - 1)$. Для этого нам надо найти $\alpha_x(c)$. Рассмотрим решения системы

$$\begin{cases} k^2 - xkl + l^2 = 1 \\ k \equiv c \pmod{x-2} \end{cases},$$

все они имеют вид:

$$k = \alpha_x(c + e(x-2)).$$

При $e = 0$ верно следующее неравенство:

$$|k| = |\alpha_x(c)| < 2|a|^2(|a| + |b| + |c|),$$

а при $e > 0$ верно:

$$|k| \geqslant |\alpha_x(x-2)| > (2a + 2b + 2c + 1)^{c+1}(c+1)(|a| + |b| + |c|) > 2|a|^2(|a| + |b| + |c|).$$

□

Следствие 2.5. Функция $\mathrm{len}\,(x)$, равная $1 + \lfloor \log_2(x) \rfloor$ при x не равном нулю и равная 1 при x равном нулю, полиномиально ограниченная диофантова.

Доказательство. Для доказательства достаточно рассмотреть следующий предикат:

$$\exists a\ [(a = 2^c) \wedge (a \leqslant x < 2a) \wedge |a| < 2|x|],$$

и понять, что он истинный тогда и только тогда, когда $\mathrm{len}(x) = c$. □

Лемма 2.11. *Для любого диофантового полиномиально ограниченного отношения $R(x_1, \ldots, x_n, y_1, \ldots, y_m)$ и многочленов k_1, ..., k_m следующее отношение диофантово полиномиально ограниченное:*

$$\exists y_1, \ldots, y_m\ [R(x_1, \ldots, x_n, y_1, \ldots, y_m) \wedge |y_1| < k_1(|x_1|, \ldots, |x_n|) \wedge \ldots \wedge |y_m| < k_m(|x_1|, \ldots, |x_n|)].$$

2.4. Оракулы и простейшее представление.

Определение 2.8. *Назовем оракульный многочлен P с оракулом O O-примитивным, если P – оракульный многочлен вида:*

$$O(P_1(x_1,\dots,x_k),\dots,P_l(x_1,\dots,x_k)),$$

где $P_1,\dots,P_l$ – многочлены.

Определение 2.9. *Функция f – полиномиально ограниченна, если существует многочлен $p(n)$, что $|f(x)| < p(|x|)$.*

Теорема 2.2. *Пусть $O_1,\dots,O_k$ – полиномиально ограниченные функции, тогда любое диофантово полиномиально ограниченное отношение $R(x_1,\dots,x_n)$ с оракулами O_1, …, O_k представляется в виде:*

$$\begin{aligned}
&\exists y_1,\dots,y_m,v_1,\dots,v_l\\
&\qquad [S(x_1,\dots,x_n,y_1,\dots,y_m,v_1,\dots,v_l)=0\wedge\\
&\qquad v_1=Q_1(x_1,\dots,x_n,y_1,\dots,y_m)\wedge\\
&\qquad \dots\\
&\qquad \wedge v_l=Q_l(x_1,\dots,x_n,y_1,\dots,y_m)\wedge\\
&\qquad |y_1|<k_1(|x_1|,\dots,|x_n|)\wedge\\
&\qquad \dots\\
&\qquad \wedge |y_m|<k_m(|x_1|,\dots,|x_n|)],
\end{aligned}$$

где S – многочлен, Q_i – O_{j_i} – примитивный оракульный многочлен и k_i – многочлены.

Доказательство. В этом доказательстве нам будут важны имена переменных в многочленах. Пусть P – многочлен из ограниченного диофантова представления R. Построим такие многочлен T и последовательность пар $\{(v_i,T_i)\}_{i=1}^{p}$, состоящих из переменной (причем все переменные различны) и многочлена (с оракулами), что

$$P=T[v_1=T_1]\dots[v_p=T_p],$$

T_i – O_{t_i}-примитивный и в T нет вызова оракулов. Строить будем при помощи индукции по построению P. Пусть P – многочлен от x_1, …, x_n, z_1, …, z_q. База индукции, когда P – литера или константа, очевидна. Переход:

(1) $P = A\#B$. По предположению индукции для A и B существуют соответствующие последовательности:

$$\left\{(v_i^{(1)}, T_i^{(1)})\right\}_{i=1}^{p^{(1)}}, \quad \left\{(v_i^{(2)}, T_i^{(2)})\right\}_{i=1}^{p^{(2)}}$$

и многочлены $T^{(1)}$, $T^{(2)}$. Не умаляя общности, можно считать, что $v_i^{(j)}$ различны. Тогда в качестве искомой последовательности возьмем

$$\begin{aligned} v_i &= v_i^{(1)} && \text{при } i \leqslant p^{(1)}, \\ v_i &= v_{i-p^{(1)}}^{(2)} && \text{при } i > p^{(1)}, \\ T_i &= T_i^{(1)} && \text{при } i \leqslant p^{(1)}, \\ T_i &= T_{i-p^{(1)}}^{(2)} && \text{при } i > p^{(1)}, \end{aligned}$$

а в качестве T возьмем $T^{(1)}\#T^{(2)}$.

(2) $P = O_r(P_1, \ldots, P_l)$. По предположению индукции для P_1, $\ldots$, P_l существуют соответствующие последовательности

$$\left\{(v_i^{(1)}, T_i^{(1)})\right\}_{i=1}^{p^{(1)}}, \ldots, \left\{(v_i^{(l)}, T_i^{(l)})\right\}_{i=1}^{p^{(l)}},$$

и многочлены $T^{(1)}$, $\ldots$, $T^{(l)}$. Не умаляя общности, можно считать, что $v_i^{(j)}$ различны. Пусть v – переменная, не встречающаяся в

$$T^{(l)}, \ldots, T^{(l)}, \quad T_1^{(1)}, \ldots T_{p^{(l)}}^{(l)}.$$

Тогда в качестве искомой последовательности возьмем

$$\begin{aligned} &v_1 = v, \\ &v_i = v_{i-\sum_{t=1}^{j-1} p^{(t)}}^{(j)} \text{ при } \sum_{t=1}^{j-1} p^{(t)} < i - 1 \leqslant \sum_{t=1}^{j} p^{(t)}, \\ &T_1 = O_r(T^{(1)}, \ldots, T^{(l)}), \\ &T_i = T_{i-\sum_{t=1}^{j-1} p^{(t)}}^{(j)} \text{ при } \sum_{t=1}^{j-1} p^{(t)} < i - 1 \leqslant \sum_{t=1}^{j} p^{(t)}, \end{aligned}$$

а в качестве T возьмем v.

Осталось построить S и Q_i. В качестве S возьмем построенный нами многочлен T, а в качестве Q_i возьмем T_i. □

Следствие 2.6. Если f – диофантово полиномиально ограниченная функция, то $\mathbf{D}^f$ равно $\mathbf{D}$.

Доказательство. По предыдущей теореме любой предикат из $\mathbf{D}^f$ представляется в виде:

$$\begin{aligned}
&\exists y_1, \ldots, y_m, v_1, \ldots, v_l \ [S(x_1, \ldots, x_n, y_1, \ldots, y_m, v_1, \ldots, v_l) = 0 \wedge \\
&v_1 = f(P_{1,1}(x_1, \ldots, x_n, y_1, \ldots, y_m), \ldots, P_{1,t}(x_1, \ldots, x_n, y_1, \ldots, y_m)) \wedge \\
&\ldots \\
&\wedge v_l = f(P_{l,1}(x_1, \ldots, x_n, y_1, \ldots, y_m), \ldots, P_{l,t}(x_1, \ldots, x_n, y_1, \ldots, y_m)) \wedge \\
&|y_1| < k_1(|x_1|, \ldots, |x_n|) \wedge \\
&\ldots \\
&\wedge |y_m| < k_m(|x_1|, \ldots, |x_n|)].
\end{aligned}$$

Так, как f – диофантово полиномиально ограниченная, то существует R из $\mathbf{D}$ – предикат принадлежности к графику f. А значит любой предикат из $\mathbf{D}^f$ представляется в виде:

$$\begin{aligned}
&\exists y_1, \ldots, y_m, v_1, \ldots, v_l \ [S(x_1, \ldots, x_n, y_1, \ldots, y_m, v_1, \ldots, v_l) = 0 \wedge \\
&R(v_1, P_{1,1}(x_1, \ldots, x_n, y_1, \ldots, y_m), \ldots, P_{1,t}(x_1, \ldots, x_n, y_1, \ldots, y_m)) \wedge \\
&\ldots \\
&\wedge R(v_l, P_{l,1}(x_1, \ldots, x_n, y_1, \ldots, y_m), \ldots, P_{l,t}(x_1, \ldots, x_n, y_1, \ldots, y_m)) \wedge \\
&|y_1| < k_1(|x_1|, \ldots, |x_n|) \wedge \\
&\ldots \\
&\wedge |y_m| < k_m(|x_1|, \ldots, |x_n|)],
\end{aligned}$$

а это уже предикат из $\mathbf{D}$. □

Следствие 2.7. Пусть P_1 и P_2 – многочлены, тогда отношение $R(x_1, \ldots, x_n)$, такое, что

$$R(x_1, \ldots, x_n) \Leftrightarrow P_1(|x_1|, \ldots, |x_n|) < P_2(|x_1|, \ldots, |x_n|),$$

– диофантово полиномиально ограниченное.

2.5. Диофантова иерархия.

Определение 2.10. *Определим класс* $\mathbf{R}^A$ *следующим образом: язык* L *содержится в* $\mathbf{R}^A$*, если и только если существует* P *– многочлен с оракулами из* A*, такой, что*

$$(x_1, \ldots, x_n) \in \mathtt{L} \Leftrightarrow P(x_1, \ldots, x_n) = 0.$$

Замечание 2.3. Пусть f – функция. Мы будем обозначать $\mathbf{R}^{\{f\}}$ как $\mathbf{R}^f$, а $\mathbf{R}^{\varnothing}$ как $\mathbf{R}$. А если L – язык, то $\mathbf{R}^L$ – это $\mathbf{R}^f$, где f — характеристическая функция языка L.

Определение 2.11. *Определим две последовательности классов языков –* $\Sigma^i\mathbf{R}$ *и* $\Pi^i\mathbf{R}$*:*

$$\Sigma^0\mathbf{R} = \mathbf{R},$$
$$\Pi^0\mathbf{R} = \mathbf{co}\text{-}\mathbf{R},$$

язык L *содержится в* $\Sigma^{i+1}\mathbf{R}$*, если и только если существует язык* L′ *из* $\Pi^i\mathbf{R}$ *и многочлены* $k_1, \ldots, k_m$*, такие, что*

$$\begin{aligned}(x_1, \ldots, x_n) \in \mathtt{L} \Leftrightarrow \exists y_1, \ldots, y_m \\ [((x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathtt{L}') \wedge \quad |y_1| < k_1(|x_1|, \ldots, |x_n|) \wedge \\ \ldots \\ \wedge |y_m| < k_m(|x_1|, \ldots, |x_n|)].\end{aligned}$$

Положим $\Pi^{i+1}\mathbf{R} = \mathbf{co}\text{-}\Sigma^{i+1}\mathbf{R}$.

Определение 2.12. *Определим класс языков* $\mathbf{RH}$*, равный* $\bigcup\limits_{i \geqslant 0} \Sigma^i\mathbf{R}$.

Лемма 2.12. *Пусть* k *– целое неотрицательное число, а* $R_1(x_1, \ldots, x_n, y_{1,1}, \ldots, y_{1,m_1})$*,* $R_2(x_1, \ldots, x_n, y_{2,1}, \ldots, y_{2,m_2})$ *принадлежат* $\Sigma^k\mathbf{R}$*, тогда следующие отношения тоже принадлежат* $\Sigma^k\mathbf{R}$*:*

(1) $R_1(x_1, \ldots, x_n, y_{1,1}, \ldots, y_{1,m_1}) \wedge R_2(x_1, \ldots, x_n, y_{2,1}, \ldots, y_{2,m_2})$
(2) $R_1(x_1, \ldots, x_n, y_{1,1}, \ldots, y_{1,m_1}) \vee R_2(x_1, \ldots, x_n, y_{2,1}, \ldots, y_{2,m_2})$

Доказательство. Доказательство аналогично доказательству леммы 2.1. □

Теорема 2.3. *Язык* L *тогда и только тогда лежит в* $\Sigma^k\mathbf{R}$*, когда* L *лежит в* $\mathbf{D}^{\Sigma^{k-1}\mathbf{R}}$.

Доказательство.

(1) Сначала покажем, что если $\mathtt{L}$ лежит в $\Sigma^k\mathbf{R}$, то $\mathtt{L}$ лежит в $\mathbf{D}^{\Sigma^{k-1}\mathbf{R}}$. Это достаточно очевидно: для любого языка из $\Sigma^k\mathbf{R}$ существует язык $\mathtt{L}'$ из $\Pi^{k-1}\mathbf{R}$ и многочлены $k_1, \ldots, k_m$, такие, что

$$\begin{aligned}(x_1,\ldots,x_n)\in\mathtt{L}\Leftrightarrow\exists y_1,\ldots,y_m\ [&((x_1,\ldots,x_n,y_1,\ldots,y_m)\in\mathtt{L}')\wedge\\ &|y_1|<k_1(|x_1|,\ldots,|x_n|)\wedge\\ &\ldots\\ &\wedge|y_m|<k_m(|x_1|,\ldots,|x_n|)].\end{aligned}$$

Тогда если $S(x_1,\ldots,x_n,y_1,\ldots,y_m)$ характеристическая функция дополнения $\mathtt{L}'$, то L можно описать так:

$$\begin{aligned}(x_1,\ldots,x_n)\in\mathtt{L}\Leftrightarrow\exists y_1,\ldots,y_m\ [&1-S(x_1,\ldots,x_n,y_1,\ldots,y_m)=0\wedge\\ &|y_1|<k_1(|x_1|,\ldots,|x_n|)\wedge\\ &\ldots\\ &\wedge|y_m|<k_m(|x_1|,\ldots,|x_n|)],\end{aligned}$$

а это представление языка из $\mathbf{D}^{\Sigma^{k-1}\mathbf{R}}$.

(2) Осталось показать, что если $\mathtt{L}$ лежит в $\mathbf{D}^{\Sigma^{k-1}\mathbf{R}}$, то $\mathtt{L}$ лежит в $\Sigma^k\mathbf{R}$. Для k, равного единице, все очевидно. Поэтому будем считать, что $k\geqslant 2$. Сначала докажем это для отношений, ограниченное диофантово представление которых O-примитивно (где O – характеристическая функция произвольного языка из $\Sigma^{k-1}\mathbf{R}$). Пусть $P=O(P_1,\ldots,P_l)$ – оракульный многочлен из диофантова представления R, пусть $S=1-O$ (содержится в $\Pi^{k-1}\mathbf{R}$) и $(Q,\{k_i\}_{i=1}^m)$ — ограниченное диофантово представление O. Рассмотрим следующее отношение:

$$\begin{aligned}\exists r,y_1,\ldots,y_m\ [&((r=1\wedge Q(P_1,\ldots,P_l,y_1,\ldots,y_m)=0)\\ &\vee(r=0\wedge S(P_1,\ldots,P_l)=0))\wedge\\ &|y_1|<k_1(|P_1|,\ldots,|P_l|)\\ &\ldots\\ &|y_m|<k_m(|P_1|,\ldots,|P_l|)].\end{aligned}$$

Очевидно, что оно является характеристическим для L, но еще не ясно, что оно принадлежи $\Sigma^k\mathbf{R}$. Для этого надо написать

полиномиальные оценки на длину $y_1, \ldots, y_m$. Для того, чтобы написать оценки на длину y_i, рассмотрим k'_i, такой , что он больше (поточечно), чем $k_i(P_1, \ldots, P_l)$. Тогда мы получили, что:

$$
\begin{aligned}
&(x_1, \ldots, x_n) \in \mathtt{L} \Leftrightarrow \\
&\quad \exists r, y_1, \ldots, y_m \ [((r = 1 \wedge Q(P_1, \ldots, P_l, y_1, \ldots, y_m)) \\
&\qquad\qquad \vee (r = 0 \wedge S(P_1, \ldots, P_l)))\wedge \\
&\qquad\qquad |y_1| < k_1(|P_1|, \ldots, |P_l|)\wedge \\
&\qquad\qquad \ldots \\
&\qquad\qquad \wedge |y_m| < k_m(|P_1|, \ldots, |P_l|) \\
&\qquad\qquad |y_1| < k'_1(|x_1|, \ldots, |x_n|)\wedge \\
&\qquad\qquad \ldots \\
&\qquad\qquad \wedge |y_m| < k'_m(|x_1|, \ldots, |x_n|)],
\end{aligned}
$$

а это отношение уже диофантово по следствию 2.7. Для отношения, в котором оракулы не используются, все и так очевидно. По теореме 2.2 любое отношение $R(x_1, \ldots, x_n)$ из $\mathbf{D}^{\Sigma^{k-1}\mathbf{R}}$ представляется в виде:

$$
\begin{aligned}
&\exists y_1, \ldots, y_m, v_1, \ldots, v_l \\
&\qquad [S(x_1, \ldots, x_n, y_1, \ldots, y_m, v_1, \ldots, v_l) = 0\wedge \\
&\qquad v_1 = Q_1(x_1, \ldots, x_n, y_1, \ldots, y_m)\wedge \\
&\qquad \ldots \\
&\qquad \wedge v_l = Q_l(x_1, \ldots, x_n, y_1, \ldots, y_m)\wedge \\
&\qquad |y_1| < k_1(|x_1|, \ldots, |x_n|)\wedge \\
&\qquad \ldots \\
&\qquad \wedge |y_m| < k_m(|x_1|, \ldots, |x_n|)],
\end{aligned}
$$

где S – многочлен, Q_i – O_{j_i}-примитивный оракульный многочлен и k_i – многочлены. И по доказанному отношение

$$S(x_1,\dots,x_n,y_1,\dots,y_m,v_1,\dots,v_l)=0\wedge$$
$$v_1=Q_1(x_1,\dots,x_n,y_1,\dots,y_m)\wedge$$
$$\dots$$
$$\wedge\, v_l=Q_l(x_1,\dots,x_n,y_1,\dots,y_m)$$

лежит в $\Sigma^k\mathbf{R}$, а значит $R(x_1,\dots,x_n)$ содержится в $\Sigma^k\mathbf{R}$. □

Следствие 2.8. Если $\Sigma^k\mathbf{R}$ равно $\Pi^k\mathbf{R}$, то $\mathbf{RH}$ равно $\Sigma^k\mathbf{R}$

Доказательство. Доказательство аналогично доказательству соответствующего факта для полиномиальной иерархии. □

2.6. Диофантово кодирование. Достаточно часто нам хочется, чтобы наше диофантово отношение работало с не известным заранее количеством переменных. В этой главе мы введем необходимую для этого технику.

Определение 2.13. *Будем называть канторовым кодом чисел a и b число c, равное $((a+b)^2+3a+b)/2$, и обозначать его* $\mathrm{pair}(a,b)$.

Лемма 2.13 (см., например, в [6])**.** *Отображение* pair *– биекция из $\mathbb{N}_0^2$ в $\mathbb{N}_0$.*

Лемма 2.14.

(1) *Функция* fst, *такая, что $a=\mathrm{fst}(\mathrm{pair}(a,b))$ – полиномиально ограниченная диофантова функция.*
(2) *Функция* snd, *такая, что $b=\mathrm{snd}(\mathrm{pair}(a,b))$ – полиномиально ограниченная диофантова функция.*

Определение 2.14. *Назовем позиционным кодом последовательности $a_1,\dots,a_n$ число* $\mathrm{pair}(\mathrm{pair}(b,n),b^{n+1}+\sum_{i=1}^{n}a_i\cdot b^{i-1})$, *если для любого i от 1 до n верно, что $b>a_i$. Обозначим его* $\mathrm{pcode}(b,a_1,\dots,a_n)$.

Лемма 2.15. *Функция* pelem, *такая, что* $\mathrm{pelem}(\mathrm{pcode}(b,a_0,\dots,a_n),i,n)=a_i$ *– полиномиально ограниченная диофантова.*

Доказательство. Для доказательства этой леммы просто напишем представление предиката, проверяющего эту функцию, такое, что по

нему будет очевидна ее диофантоввость. Это представление:

$$\exists a, b, n\ [\mathrm{fst}(\mathrm{fst}(x)) = b \wedge \mathrm{fst}(\mathrm{snd}(x)) = n \wedge a = b^i \wedge y = \mathrm{quot}(\mathrm{rem}(\mathrm{snd}(x) - b^{n+1}, a \cdot b), a)].$$

Ясно что это выражение истинно если, и только если $\mathrm{pelem}(x, i){=}y$. □

Замечание 2.4. Часто вместо $\mathrm{pelem}(a, i)$ мы будем писать $a[i]$.

2.7. Положение NP в диофантовой иерархии.

Теорема 2.4. *Класс* **NP** *содержится в* $\Sigma^2\mathbf{R}$.

Доказательство. Пусть L – язык из **P**, тогда существует детерминированная машина M (принимающая L), работающая на входе длины n ровно $p(n)$ шагов, где p – многочлен. Нам надо написать отношение из $\Sigma^2\mathbf{R}$, такое, что оно принимает тот же язык, что и M. Для этого опишем несколько отношений:

(1) $\mathrm{maxDiffLessThan}(s, n, d)$ – отношение, истинное тогда и только тогда, когда максимальная разница соседних элементов в последовательности, заданной s, меньше d. Заметим, что $P(a, i, d, s) \Leftrightarrow a = 2^{d[i]}$ – диофнатов полиномиально ограниченное отношение (в силу того, что $|s| > d[i]$). Следовательно $\mathrm{maxDiffLessThan}(s, n, d)$ можно задать так:

$$\neg(\exists i\ [(i < n - 1 \wedge \mathrm{abs}(s[i] - s[i+1]) \geqslant d) \wedge |i| < 2|n|]).$$

(2) $\mathrm{differenceIn}(s, d, n)$ – отношение, истинное, если и только если в последовательности, заданной s, изменения происходят только в битах с номерами из d. Его можно записать так:

$$\neg(\exists i\ [\neg(\mathrm{abs}(s[i] - s[i-1]) = 2^{d[i]}) \wedge \mathrm{abs}(s[i] - s[i-1]) \neq 0 \wedge i < n \wedge |i| < 2|n|]).$$

Все эти отношения являются ко-диофантово полиномиально ограниченными (отрицания диофантовых полиномиально ограниченных). Теперь напишем отношение $\mathrm{verify}(s, m, p, n)$, истинное, только если последовательности s, m, p задают последовательность состояний, последовательность состояний ленты и последовательность указателей головки машины с функцией перехода $S\colon \{1, ..., q\}\times\{0, 1\} \to \{1, ..., q\}$, правилом изменения указателя головки $P\colon \{1, \ldots, q\} \times \{0, 1\} \to \{-1, 0, 1\}$,

правилом записи на ленту $D\colon \{1,\dots,q\}\times\{0,1\}\to\{0,1\}$ и состояниями $1,\dots,q$. Его мы запишем так:

$$\begin{aligned}\operatorname{maxDiffLessThan}(p,n,2)\wedge\operatorname{differenceIn}(m,p,n)\wedge\\ \neg(\exists i\ [(\bigwedge_{\substack{c\in\{1,\dots,q\}\\ d\in\{0,1\}}}(s[i+1]\neq S(c,d)\\ \vee m[i+1][p[i]]\neq D(c,d)\vee p[i+1]-p[i]\neq P(c,d))\wedge\\ s[i]=c\wedge m[i][p[i]]=d)])\end{aligned}$$

Тогда отношение, принимающее тот же язык, что и M, это:

$$\exists s,m,p,n\ [\operatorname{verify}(s,m,p,n)\wedge m[0]=x\wedge s[0]=0\wedge s[n]=q],$$

где 0 – начальное состояние, а q – принимающее. □

Следствие 2.9. Для любого натурального i верно:

$$\Sigma^i\mathbf{R}\subseteq\Sigma^i\mathbf{P}\subseteq\Sigma^{i+1}\mathbf{R}.$$

Следствие 2.10. Класс **PH** равен **RH**.

Следствие 2.11. Диофантова иерархия коллапсирует тогда и только тогда, когда коллапсирует полиномиальная иерархия.

Благодарности

Автор выражает признательность Ю. В. Матиясевичу, подсказавшему доказательство диофантовости отношения $a=b^c$, М. А. Всемирнову, внимательно прочитавшему и нашедшему ошибки в первоначальной версии этой статьи, Э. А. Гиршу за постановку задачи и всем троим за многочисленные плодотворные разговоры.

Литература

1. L. M. Adleman, K. L. Manders, *Computational complexity of decision procedures for polynomials (extended abstract).* — In: IEEE Symposium on Foundations of Computer Science (1975), pp. 169–177.
2. L. M. Adleman, K. L. Manders, *Diophantine complexity.* — In: IEEE Symposium on Foundations of Computer Science (1976), pp. 81–88.
3. H. Lipmaa, *On Diophantine complexity and statistical zero-knowledge arguments*, — In: ASIACRYPT'03 (2003), pp. 398–415.
4. C. Pollett, *On the bounded version of Hilbert's tenth problem.* — Arch. Math. Log. **42**, No. 5 (2003), 469–488.

5. Ю. В. Матиясевич, *Диофантовость перечислимых множеств.* — Докл. АН СССР **191**, No. 2 (1970), 278–282.
6. Ю. В. Матиясевич, *Десятая проблема Гильберта* Наука, Физико-математическая литература (1993).

Knop A. A. Diophantine complexity.

Adelman and Manders (1975) defined the class D of "non-deterministic diophantine" languages. A language L is in D iff there are polynomials p and q such that $x \in L \Leftrightarrow \exists y_1, \ldots, y_n < 2^{q(|x|)}\ p(x, y_1, \ldots, y_n) = 0$ (in this formula, bit strings are treated as natural numbers). While clearly D is a subset of NP, it is unknown whether these classes are equal.

The well-known polynomial hierarchy PH consists of complexity classes constructed on the basis of the class NP. We consider a hierarchy constructed on the basis of D in a similar way. We prove that D is in the second level of the polynomial hierarchy, and hence all the classes of the two hierarchies are successively contained in each other.

Санкт-Петербургский государственный
университет, Университетский пр. 28,
Петродворец, Санкт-Петербург 198504, Россия
E-mail: aaknop@gmail.com

Поступило 12 апреля 2012 г.