Диофантова иерархия

А. Кноп

Математико-механический факультет
Санкт-Петербургский Государственный Университет

15 апреля 2011 г.

Содержание

Десятая проблема Гильберта
Постановка вопроса

Появление

На II Международном Конгрессе математиков в Париже, в 1900 году, Давидом Гильбертом были предложены 23 кардинальные проблемы математики.

Десятая проблема

Пусть задано диофантово уравнение с произвольными неизвестными и целыми рациональными числовыми коэффициентами. Указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах.

Десятая проблема Гильберта

Постановка вопроса

Появление

На II Международном Конгрессе математиков в Париже, в 1900 году, Давидом Гильбертом были предложены 23 кардинальные проблемы математики.

Десятая проблема

Пусть задано диофантово уравнение с произвольными неизвестными и целыми рациональными числовыми коэффициентами. Указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах.

Десятая проблема Гильберта

Решение задачи

Диофоантово множество

Подмножество M множества $\mathbb{Z}^n$ диофантово, если существует P из $\mathbb{Z}[x_1, \ldots, x_{n+m}]$, для которого верно

$$(x_1, \ldots, x_n) \in M \Leftrightarrow \exists y_1, \ldots, y_m \; P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

DPRM-теорема

Множество диофантово тогда и только тогда, когда оно перечислимо.

Десятая проблема Гильберта

Решение задачи

Диофоантово множество

Подмножество M множества $\mathbb{Z}^n$ диофантово, если существует P из $\mathbb{Z}[x_1, \ldots, x_{n+m}]$, для которого верно

$$(x_1, \ldots, x_n) \in M \Leftrightarrow \exists y_1, \ldots, y_m \; P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

DPRM-теорема

Множество диофантово тогда и только тогда, когда оно перечислимо.

Недетерменированная диофантова машина

NDDM

Недетерминированной диофантовой машиной (NDDM) мы будем называть тройку (n, m, P), где P — многочлен от $n + m$ переменных, а n, m — целые числа. Также будем говорить, что (m, P) принимает $(x_1, \ldots, x_n)$ если

$$\exists y_1, \ldots, y_m : \; P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Эквивалентность

Следствием DPRM-теоремы является то, что машина Тьюринга и диофантова машина эквивалентны.

Недетерменированная диофантова машина

NDDM

Недетерминированной диофантовой машиной (NDDM) мы будем называть тройку (n, m, P), где P — многочлен от $n + m$ переменных, а n, m — целые числа. Также будем говорить, что (m, P) принимает $(x_1, \ldots, x_n)$ если

$$\exists y_1, \ldots, y_m : \; P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Эквивалентность

Следствием DPRM-теоремы является то, что машина Тьюринга и диофантова машина эквивалентны.

Класс D

Время работы

Язык L принимается NDDM за время $f(x)$, если существует такая тройка (n, m, P), где P — многочлен от $n+m$ переменных, а n, m — целые числа, что

$$\begin{aligned}(x_1, \ldots, x_n) \in L \Leftrightarrow \exists y_1, \ldots, y_m\ & P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \\ & \wedge |y_1| < f(|x_1| + \cdots + |x_n|) \\ & \ldots \\ & \wedge |y_m| < f(|x_1| + \cdots + |x_n|).\end{aligned}$$

Класс D (Adleman, Manders 1975)

Язык L принадлежит классу D тогда и только тогда, когда существует такой многочлен $p(x)$, что L принимается NDDM за время $p(x)$.

Класс D

Время работы

Язык L принимается NDDM за время $f(x)$, если существует такая тройка (n, m, P), где P — многочлен от $n + m$ переменных, а n, m — целые числа, что

$$
\begin{aligned}
(x_1, \ldots, x_n) \in L \Leftrightarrow \exists y_1, \ldots, y_m \; & P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \\
& \wedge |y_1| < f(|x_1| + \cdots + |x_n|) \\
& \ldots \\
& \wedge |y_m| < f(|x_1| + \cdots + |x_n|).
\end{aligned}
$$

Класс D (Adleman, Manders 1975)

Язык L принадлежит классу D тогда и только тогда, когда существует такой многочлен $p(x)$, что L принимается NDDM за время $p(x)$.

Многочлены с оракулами

Многочлены с оракулами

Будем называть P многочленом от переменных $x_1, \ldots, x_n$ с оракулами $O_1, \ldots, O_m$ если P равно одному из:

1. x_i
2. $O_i(Q_1, \ldots, Q_k)$ где Q_i — многочлен от переменных $x_1, \ldots, x_n$ с оракулами $O_1, \ldots, O_m$
3. $Q_1 \# Q_2$ где $\# \in \{\times, +, -\}$, а Q_i — многочлен от переменных $x_1, \ldots, x_n$ с оракулами $O_1, \ldots, O_m$

Вычисление значения многочлена с оракулами

Вычисление значения многочлена с оракулами определим естественным индуктивным способом.

Многочлены с оракулами

Многочлены с оракулами

Будем называть P многочленом от переменных x_1, ..., x_n с оракулами O_1, ..., O_m если P равно одному из:

1. x_i
2. $O_i(Q_1, \ldots, Q_k)$ где Q_i — многочлен от переменных x_1, ..., x_n с оракулами O_1, ..., O_m
3. $Q_1 \# Q_2$ где $\# \in \{\times, +, -\}$, а Q_i — многочлен от переменных x_1, ..., x_n с оракулами O_1, ..., O_m

Вычисление значения многочлена с оракулами

Вычисление значения многочлена с оракулами определим естественным индуктивным способом.

Отношения и функции

Ограниченное диофантово отношение с оракулами

Будем называть n-местное отношение R полиномиально-ограниченным диофантовым с оракулами $O_1, \ldots, O_l$, если существуют P — многочлен от $n+m$ переменных с оракулами $O_1, \ldots O_l$ и $k_1, \ldots, k_m$ — многочлены от n переменных такие, что

$$\begin{aligned} R(x_1, \ldots, x_n) \Leftrightarrow \exists y_1, \ldots, y_m \; & P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \\ & \wedge |y_1| < k_1(|x_1|, \ldots, |x_n|) \\ & \ldots \\ & \wedge |y_m| < k_m(|x_1|, \ldots, |x_n|). \end{aligned}$$

Отношения и функции

Ограниченная диофантова функция с оракулами

Будем называть функцию F, действующую из $\mathbb{Z}^n$ в $\mathbb{Z}^m$ полиномиально-ограниченной диофантовой с оракулами O_1, …, O_c, если существуют P — многочлен от $n+m+l$ переменных с оракулами $O_1, \ldots O_c$ и k_1, …, k_{m+l} — многочлены от n переменных такие, что

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

Класс D, новое определение

Класс D

Язык L принадлежит классу D, если существует такое полиномиально-ограниченное диофантово отношение R, что $(x_1, \ldots, x_n) \in L \Leftrightarrow R(x_1, \ldots, x_n)$

Класс DF

Массовая задача M принадлежит классу DF, если существует такая полиномиально-ограниченная диофантова функция F, что $((x_1, \ldots, x_n), (y_1, \ldots, y_m)) \in L \Leftrightarrow F(x_1, \ldots, x_n) = (y_1, \ldots, y_m)$

Класс D, новое определение

Класс D

Язык L принадлежит классу D, если существует такое полиномиально-ограниченное диофантово отношение R, что $(x_1, \dots, x_n) \in L \Leftrightarrow R(x_1, \dots, x_n)$

Класс DF

Массовая задача M принадлежит классу DF, если существует такая полиномиально-ограниченная диофантова функция F, что
$((x_1, \dots, x_n), (y_1, \dots, y_m)) \in L \Leftrightarrow F(x_1, \dots, x_n) = (y_1, \dots, y_m)$

Простейшие свойства

P, NP и D

Условие, что **P** лежит в **D** равносильно тому, что **D** равно **NP**.

Пересечение и объединение

Класс **D** замкнут относительно объединения и пересечения.

Добавление квантора

Если R — $(n+m)$-местное полиномиально-ограниченное диофантово отношение, то $\exists y_1, \ldots, y_m\ R(x_1, \ldots, x_n, y_1, \ldots, y_m) \wedge |y_i| < k_i(|x_1|, \ldots, |x_n|)$ — полиномиально-ограниченное диофантово отношение.

Простейшие свойства

P, **NP** и **D**

Условие, что **P** лежит в **D** равносильно тому, что **D** равно **NP**.

Пересечение и объединение

Класс **D** замкнут относительно объединения и пересечения.

Добавление квантора

Если R — $(n+m)$-местное полиномиально-ограниченное диофантово отношение, то $\exists y_1, \ldots, y_m\ R(x_1, \ldots, x_n, y_1, \ldots, y_m) \wedge |y_i| < k_i(|x_1|, \ldots, |x_n|)$ — полиномиально-ограниченное диофантово отношение.

Простейшие свойства

P, **NP** и **D**

Условие, что **P** лежит в **D** равносильно тому, что **D** равно **NP**.

Пересечение и объединение

Класс **D** замкнут относительно объединения и пересечения.

Добавление квантора

Если R — $(n+m)$-местное полиномиально-ограниченное диофантово отношение, то $\exists y_1, \ldots, y_m\ R(x_1, \ldots, x_n, y_1, \ldots, y_m) \wedge |y_i| < k_i(|x_1|, \ldots, |x_n|)$ — полиномиально-ограниченное диофантово отношение.

Полиномиальная иерархия

Определение уровня иерархии

Определим следующие классы языков:

$$\Sigma^1\mathbf{P} = \mathbf{NP},$$
$$\Pi^1\mathbf{P} = \mathbf{co\text{-}NP},$$
$$\Pi^{i+1}\mathbf{P} = \mathbf{co\text{-}NP}^{\Sigma^i\mathbf{P}},$$
$$\Sigma^{i+1}\mathbf{P} = \mathbf{P}^{\Sigma^i\mathbf{P}}.$$

Определение иерархии

Определим класс языков $\mathbf{PH} = \bigcup\limits_{i \geqslant 1} \Sigma^i\mathbf{P}$.

Полиномиальная иерархия

Определение уровня иерархии

Определим следующие классы языков:

$$\Sigma^1\mathbf{P} = \mathbf{NP},$$
$$\Pi^1\mathbf{P} = \mathbf{co\text{-}NP},$$
$$\Pi^{i+1}\mathbf{P} = \mathbf{co\text{-}NP}^{\Sigma^i\mathbf{P}},$$
$$\Sigma^{i+1}\mathbf{P} = \mathbf{P}^{\Sigma^i\mathbf{P}}.$$

Определение иерархии

Определим класс языков $\mathbf{PH} = \bigcup\limits_{i \geqslant 1} \Sigma^i\mathbf{P}$.

Полиномиальная иерархия

Эквивалентное определение

Язык L лежит в $\Sigma^l\mathbf{P}$ тогда и только тогда, когда существует такая детерменированная машина Тьюринга (работающая полиномиальное время), что

$$(x_1, \dots, x_n) \in L \Leftrightarrow$$
$$\exists y_{1,1}, \dots, y_{1,m_1} \forall y_{2,1}, \dots, y_{2,m_2} \dots P(x_1, \dots, x_n, y_{1,1} \dots, y_{l,m_l})$$

Коллапс полиномиальной иерархии иерархии

Если $\Sigma^k\mathbf{P} = \Pi^k\mathbf{P}$, то $\mathbf{PH} = \Sigma^k\mathbf{P}$.

Полиномиальная иерархия

Эквивалентное определение

Язык L лежит в $\Sigma^l\mathbf{P}$ тогда и только тогда, когда существует такая детерменированная машина Тьюринга (работающая полиномиальное время), что

$$(x_1, \dots, x_n) \in L \Leftrightarrow$$
$$\exists y_{1,1}, \dots, y_{1,m_1} \forall y_{2,1}, \dots, y_{2,m_2} \dots P(x_1, \dots, x_n, y_{1,1} \dots, y_{l,m_l})$$

Коллапс полиномиальной иерархии иерархии

Если $\Sigma^k\mathbf{P} = \Pi^k\mathbf{P}$, то $\mathbf{PH} = \Sigma^k\mathbf{P}$.

Диофантова иерархия

Определение уровня иерархии

Определим следующие классы языков:

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

Определение иерархии

Определим класс языков $\mathbf{DH} = \bigcup\limits_{i\geqslant 1} \Sigma^i\mathbf{D}$.

Диофантова иерархия

Определение уровня иерархии

Определим следующие классы языков:

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

Определение иерархии

Определим класс языков $\mathbf{DH} = \bigcup_{i\geqslant 1} \Sigma^i\mathbf{D}$.

Диофантова иерархия

Эквивалентное определение

Язык L лежит в $\Sigma^l\mathbf{D}$ тогда и только тогда, когда существует такой многочлен P, что

$$(x_1, \ldots, x_n) \in L \Leftrightarrow$$
$$\exists y_{1,1}, \ldots, y_{1,m_1} \forall y_{2,1}, \ldots, y_{2,m_2} \ldots P(x_1, \ldots, x_n, y_{1,1} \ldots, y_{l,m_l})$$

Коллапс диофантовой иерархии

Если $\Sigma^k\mathbf{D} = \Pi^k\mathbf{D}$, то $\mathbf{DH} = \Sigma^k\mathbf{D}$.

Диофантова иерархия

Эквивалентное определение

Язык L лежит в $\Sigma^l \mathbf{D}$ тогда и только тогда, когда существует такой многочлен P, что

$$(x_1, \dots, x_n) \in L \Leftrightarrow$$
$$\exists y_{1,1}, \dots, y_{1,m_1} \forall y_{2,1}, \dots, y_{2,m_2} \dots P(x_1, \dots, x_n, y_{1,1} \dots, y_{l,m_l})$$

Коллапс диофантовой иерархии

Если $\Sigma^k \mathbf{D} = \Pi^k \mathbf{D}$, то $\mathbf{DH} = \Sigma^k \mathbf{D}$.

Связь диофантовой и полиномиальной иерархий

Простое наблюдение

Для любого натурального i верно, что $\Sigma^i\mathbf{D} \subseteq \Sigma^i\mathbf{P}$.

Положение NP

Класс **NP** лежит в $\Sigma^2\mathbf{D}$.

Вложенность иерархий

Для любого натурального i верно, что $\Sigma^i\mathbf{D} \subseteq \Sigma^i\mathbf{P} \subseteq \Sigma^{i+1}\mathbf{D}$.

Связь диофантовой и полиномиальной иерархий

Простое наблюдение

Для любого натурального i верно, что $\Sigma^i\mathbf{D} \subseteq \Sigma^i\mathbf{P}$.

Положение **NP**

Класс **NP** лежит в $\Sigma^2\mathbf{D}$.

Вложенность иерархий

Для любого натурального i верно, что $\Sigma^i\mathbf{D} \subseteq \Sigma^i\mathbf{P} \subseteq \Sigma^{i+1}\mathbf{D}$.

Связь диофантовой и полиномиальной иерархий

Простое наблюдение

Для любого натурального i верно, что $\Sigma^i\mathbf{D} \subseteq \Sigma^i\mathbf{P}$.

Положение NP

Класс **NP** лежит в $\Sigma^2\mathbf{D}$.

Вложенность иерархий

Для любого натурального i верно, что $\Sigma^i\mathbf{D} \subseteq \Sigma^i\mathbf{P} \subseteq \Sigma^{i+1}\mathbf{D}$.

Оракулы и класс **D**

1. $Nocarry(a, b)$ является истинным тогда только тогда, когда при сложении a и b отсутствует перенос.
2. $R_O(a)$ — тогда и только тогда, когда в битовой записи a на четных местах стоят нули.

Достаточные условия для $\mathbf{D} = \mathbf{NP}$ (Adleman, Manders 1975)

Оказывается, что если в **D** содержатся вышеперечисленные языки, то $\mathbf{D} = NP$.