Математические модели последовательных вычислений

mk.cs.msu.ru → Лекционные курсы
→ Математические модели последовательных вычислений

Блок 7

Диофантовы уравнения

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2022/2023, весенний семестр

Обсудив основные проблемы, разрешимые для сетей Петри, перейдём к неразрешимым проблемам

Как можно догадаться по следствию из теоремы об m-сводимости, обоснование неразрешимости этих проблем будет основано на сведении к ним других известных неразрешимых проблем

В роли такой известной неразрешимой проблемы рассмотрим 10-ю проблему Гильберта: проблему разрешимости диофантовых уравнений

$\mathbb{Z}$ — так будем обозначать множество всех целых чисел

Диофантов многочлен — это многочлен $P(x_1, \ldots, x_n)$ с коэффициентами из $\mathbb{Z}$ и переменными $x_1, \ldots, x_n$, принимающими значения из $\mathbb{Z}$

Корень диофантова многочлена $P(x_1, \ldots, x_n)$ — это набор $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, такой что $P(\alpha_1, \ldots, \alpha_n) = 0$

Корни диофантова многочлена $P(x_1, \ldots, x_n)$ являются решениями соответствующего диофантова уравнения $P(x_1, \ldots, x_n) = 0$

Диофантово уравнение называется разрешимым, если оно имеет хотя бы одно решение

Проблема разрешимости диофантовых уравнений (далее — $\mathfrak{D}$) формулируется так: для произвольного заданного диофантова уравнения проверить, является ли оно разрешимым

Систематическое изучение диофантовых уравнений началось в III веке н.э., современное исследование в контексте проблем Гильберта — в 1940-е гг. с основными продвижениями силами М. Дэвиса, Х. Патнем и Дж. Робинсон и завершено в 1970 г. Ю. Матиясевичем

Здесь будем использовать только итог этих усилий, никак не затрагивая обоснование:

Теорема. Проблема разрешимости диофантовых уравнений алгоритмически неразрешима

Набор чисел будем называть неотрицательным, если все значения этого набора — неотрицательные числа

Многочлен будем называть неотрицательным, если его значение на любом неотрицательном наборе неотрицательно

Рассмотрим такой вариант $\mathfrak{D}^+$ проблемы $\mathfrak{D}$: для произвольного заданного неотрицательного многочлена проверить, существует ли у него хотя бы один неотрицательный корень

Теорема. Проблема $\mathfrak{D}$ m-сводима к проблеме $\mathfrak{D}^+$

Доказательство.

Заметим, что $(\alpha_1, \ldots, \alpha_n)$ — корень многочлена $P(x_1, \ldots, x_n) \Leftrightarrow$ $(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \ldots, \alpha_n)$ — корень многочлена $P(x_1, \ldots, x_{i-1}, -x_i, x_{i+1}, \ldots, x_n)$

Это означает, что $(\alpha_1, \ldots, \alpha_n)$ — корень многочлена $P(x_1, \ldots, x_n) \Leftrightarrow$ $(|\alpha_1|, \ldots, |\alpha_n|)$ — корень хотя бы одного из многочленов $P_1, \ldots, P_{2^n}$, получающихся из P заменой каких-либо переменных на их отрицания

Значит, многочлен P разрешим $\Leftrightarrow$ многочлен $P_1 \cdot \ldots \cdot P_{2^n}$ имеет хотя бы один неотрицательный корень

При этом $(P_1 \cdot \ldots \cdot P_{2^n})^2$ — многочлен, корни которого совпадают с корнями $P_1 \cdot \ldots \cdot P_{2^n}$

Следовательно, многочлен P разрешим $\Leftrightarrow$ неотрицательный многочлен $(P_1 \cdot \ldots \cdot P_{2^n})^2$ имеет хотя бы один неотрицательный корень ▼

Будем говорить, что многочлен P покрывается многочленом Q с тем же набором переменных $x_1, \ldots, x_n$ и записывать это как $P \leq Q$ и $Q \geq P$, если для любого набора $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ верно $P(\alpha_1, \ldots, \alpha_n) \leq Q(\alpha_1, \ldots, \alpha_n)$

Для анализа сетей Петри будет использоваться проблема включения для диофантовых многочленов специального вида ($\mathfrak{C}$): для произвольных заданных диофантовых многочленов $P(x_1, \ldots, x_n)$ и $Q(x_1, \ldots, x_n)$ с неотрицательными коэффициентами проверить соотношение $P \leq Q$

Областью покрытия многочлена $P(x_1, \ldots, x_n)$ будем называть множество наборов
$\mathcal{C}(P) = \{(\alpha_1, \ldots, \alpha_n, \beta) \mid (\alpha_1, \ldots, \alpha_n, \beta) \in \mathbb{N}_0^{n+1},\ \beta \leq P(\alpha_1, \ldots, \alpha_n)\}$

Проблему включения можно переформулировать так: для произвольных заданных диофантовых многочленов $P(x_1, \ldots, x_n)$ и $Q(x_1, \ldots, x_n)$ с неотрицательными коэффициентами проверить включение $\mathcal{C}(P) \subseteq \mathcal{C}(Q)$

Теорема. **Дополнение проблемы $\mathfrak{D}^+$ m-сводится к проблеме $\mathfrak{C}$**

Доказательство.

Рассмотрим произвольный неотрицательный диофантов многочлен $P(x_1, \ldots, x_n)$

Разделив все одночлены P на две группы: с положительными коэффициентами и с отрицательными — можно представить P в виде разности $P = Q_1(x_1, \ldots, x_n) - Q_2(x_1, \ldots, x_n)$, где Q_1 и Q_2 — многочлены с неотрицательными коэффициентами

При этом верно следующее:

$P(x_1, \ldots, x_n)$ не имеет ни одного неотрицательного корня

$\Leftrightarrow$ (многочлен P неотрицателен)

$1 \leq P(x_1, \ldots, x_n)$

$\Leftrightarrow$ $(P = Q_1 - Q_2)$

$Q_2(x_1, \ldots, x_n) + 1 \leq Q_1(x_1, \ldots, x_n)$ ▼

Следствие. **Проблема $\mathfrak{C}$ алгоритмически неразрешима**