Вероятностная проверка тождеств

Н. Н. Кузюрин С. А. Фомин

14 апреля 2016 г.

Полиномиальные и матричные тождества.

Алгоритм Фрейвалда

Первые вероятностные алгоритмы эффективнее детерминированных.

Rusins Freivalds, 1977

«Probabilistic Machines Can Use Less Running Time» IFIP Congress 1977

$$AB \stackrel{?}{=} C$$

Детерминировано $\rightarrow A \times B \stackrel{?}{=} C$.

Сложность:

- $O(n^3)$ — стандартное умножение.
- $O(n^{2.376})$ — самое асимптотически быстрое.

Алгоритм Фрейвалда

$$AB \stackrel{?}{=} C$$

- $\mathbf{x} = (x_1, \ldots, x_n)$, $x_i = random(\{0, 1\})$
- $AB \times x = A \times (B \times x)$, за $O(n^2)$.
- $C \times x$
- $AB \times x \stackrel{?}{=} C \times x$
- $AB \times x = C \times x \Rightarrow AB = C$
- $AB \times x \neq C \times x \Rightarrow AB \neq C$

Алгоритм Фрейвалда

$$AB \stackrel{?}{=} C$$

- $\mathbf{x} = (x_1, \ldots, x_n)$, $x_i = random(\{0, 1\})$
- $AB \times x = A \times (B \times x)$, за $O(n^2)$.
- $C \times x$
- $AB \times x \stackrel{?}{=} C \times x$
- $AB \times x = C \times x \Rightarrow AB = C$
- $AB \times x \neq C \times x \Rightarrow AB \neq C$

- Односторонняя ошибка. $AB \neq C$ — всегда верно.
- Сложность — $O(n^2)$

Корректность алгоритма

Теорема

Пусть A, B, и C — n × n матрицы, элементы которых принадлежат некоторому полю $\mathbf{F}$*, причем* $AB \neq C$*.*

Тогда для вектора x, выбранного случайно и равномерно из $\{0,1\}^n$*,*

$$P\{ABx = Cx\} \leq \frac{1}{2}.$$

Доказательство

Пусть $D = AB - C \neq \mathbf{0}$.

$$\mathsf{P}(D\mathbf{x} = 0) = ?$$

Пусть k ненулевых в начале первой строки D: $\mathbf{d}^{\mathbf{T}}$.

$$\mathsf{P}\{D\mathbf{x} = 0\} \leq \mathsf{P}\{\mathbf{d}^T\mathbf{x} = 0\}.$$

Но

$$\mathbf{d}^T\mathbf{x} = 0 \;\Leftrightarrow\; x_1 = \frac{-\sum_{i=2}^{k} d_i x_i}{d_1} = f(x_2, \ldots, x_k) = v \in \mathbf{F}.$$

x_1 равномерно распределено на $\{0, 1\}$.

$$\mathsf{P}\, x_1 = v \leq \frac{1}{2}$$

Доказательство

Пусть $D = AB - C \neq \mathbf{0}$.

$$\mathsf{P}(D\mathbf{x} = 0) = ?$$

Пусть k ненулевых в начале первой строки D: $\mathbf{d}^{\mathbf{T}}$.

$$\mathsf{P}\{D\mathbf{x} = 0\} \leq \mathsf{P}\{\mathbf{d}^T\mathbf{x} = 0\}.$$

Но

$$\mathbf{d}^T\mathbf{x} = 0 \quad \Leftrightarrow \quad x_1 = \frac{-\sum_{i=2}^{k} d_i x_i}{d_1} = f(x_2, \ \ldots, x_k) = v \in \mathbf{F}.$$

x_1 равномерно распределено на $\{0, 1\}$.

$$\mathsf{P}\, x_1 = v \leq \frac{1}{2}$$

$$\begin{aligned} \mathsf{P}(x_1 = 0) = \mathsf{P}(x_1 = 1) &= \frac{1}{2} \\ \mathsf{P}(x_1 > 1) &= 0 \end{aligned}$$

Полиномиальные тождества

Классическим примером задачи, где вероятностные алгоритмы традиционно успешно применяются, является задача проверки тождеств для многочлена от многих переменных.

Задача

Проверить для заданного полинома $P(x_1, \ldots, x_n)$ *выполнение тождества* $P(x_1, \ldots, x_n) \equiv 0$.

Следующая лемма, по сути, описывает вероятностный Монте–Карло алгоритм с односторонней ошибкой.

Лемма Шварца-Зиппеля

Лемма

Пусть $Q(x_1, \ldots, x_n)$ — многочлен от многих переменных степени d над полем F и пусть $S \subseteq F$ — произвольное подмножество. Если $r_1, \ldots, r_n$ выбраны случайно, независимо и равномерно из S, то

$$\mathsf{P}\left(Q(r_1, \ldots, r_n) = 0 \mid Q(x_1, \ldots, x_n) \not\equiv 0\right) \leq \frac{d}{|S|}.$$

Лемма Шварца-Зиппеля: доказательство

Индукция по n.
$n = 1 \Rightarrow$ полином $Q(x_1)$ степени d. $\Rightarrow Q(x_1)$ имеет не более d корней.

$$\Rightarrow \quad \mathsf{P}(Q(r_1) = 0) \leq \frac{d}{|\mathbf{S}|}.$$

Пусть ОК для всех полиномов, меньше n переменных.

Разложим $Q(x_1, \ldots, x_n)$ по x_1:

$$Q(x_1, \ldots, x_n) = \sum_{i=0}^{k} x_1^i Q_i(x_2, \ldots, x_n),$$

где $k \leq d$ — наибольшая степень x_1 в Q.

Доказательство: продолжение

Предполагая, что Q зависит от x_1, имеем $k > 0$, и коэффициент при x_1^k, $Q_k(x_2, \ldots, x_n)$ не равен тождественно нулю. Рассмотрим две возможности.

Первая — $Q_k(r_2, \ldots, r_n) = 0$. Заметим, что степень Q_k не превосходит $d - k$, и по предположению индукции вероятность этого события не превосходит $\frac{(d-k)}{|\mathbf{S}|}$.

Вторая — $Q_k(r_2, \ldots, r_n) \neq 0$. Рассмотрим следующий полином от одной переменной:

$$q(x_1) = Q(x_1, r_2, r_3, \ldots, r_n) = \sum_{i=0}^{k} Q_i(r_2, \ldots, r_n) x_1^i.$$

Полином $q(x_1)$ имеет степень k и не равен тождественно нулю, т.к. коэффициент при x_1^k есть $Q_k(r_2, \ldots, r_n)$. Базовый случай индукции дает, что вероятность события

$$q(r_1) = Q(r_1, r_2, \ldots, r_n) = 0$$

не превосходит $\frac{k}{|\mathbf{S}|}$.

Доказательство: завершение

Мы доказали два неравенства:

$$\mathsf{P}\{Q_k(r_2,\ \ldots, r_n) = 0\} \le \frac{d-k}{|\mathbf{S}|};$$

$$\mathsf{P}\{Q(r_1, r_2,\ \ldots, r_n) = 0 |\ Q_k(r_2,\ \ldots, r_n) \ne 0\} \le \frac{k}{|\mathbf{S}|}.$$

Используя результат упражнения, мы получаем, что вероятность события $Q(r_1, r_2,\ \ldots, r_n) = 0$ не превосходит суммы двух вероятностей $(d-k)/|\mathbf{S}|$ и $k/|\mathbf{S}|$, что дает в сумме желаемое $d/|\mathbf{S}|$.

Упражнение

Покажите, что для любых двух событий E_1, E_2,

$$\mathsf{P}\{E_1\} \le \mathsf{P}\{E_1 |\ \overline{E}_2\} + \mathsf{P}\{E_2\},$$

Упражнение

Имеется $n \times n$ матрица A, элементами которой являются линейные функции $f_{ij}(x) = a_{ij}x + b_{ij}$.
Придумайте Монте-Карло алгоритм с односторонней ошибкой для проверки этой матрицы на вырожденность ($\det A \equiv 0$).

Определение

*Эффективный параллельный алгоритм (или NC-**алгоритмом**) алгоритм, который*

- *на многопроцессорной RAM (PRAM)*
- *с числом процессоров, не превосходящим некоторого полинома от длины входа*
- *завершает работу за время, ограниченное полиномом от логарифма длины входа.*

Построение *NC*-алгоритма для нахождения максимального паросочетания в двудольном графе — одна из основных открытых проблем в теории параллельных алгоритмов.