Коммуникационная сложность. Лекции в Компьютерном клубе ПОМИ.

25–26 марта 2017

Определения

$f : X \times Y \to Z$

$$CC(\pi) = \max_{x,y} (\text{количество бит, переданных } \pi \text{ на входной паре } (x, y))$$

$$D(f) = \min\{CC(\pi) \mid \pi \text{ — протокол вычисления } f\}$$

Тривиальная верхняя оценка

$$D(f) \leq \min\{\log|X| + \log|Y|, \log|X| + \log|Z|, \log|Y| + \log|Z|\}.$$

Для предикатов на двоичных словах длины n:
$D(f) \leq n + 1$.

Примеры

Pointer chasing:
$D(PC) \leq k \log n$

Медиана:
$D(MED) = O(\log^2 n)$, $D(MED) = O(\log n)$

Клика и независимое множество:
$D(CIS_G) = O(\log^2 n)$.

Равенство, порядок:
$D(EQ) \leq n + 1$, $D(GT) \leq n + 1$.

Теорема

$D(EQ) = D(GT) = n + 1$.

Вероятностные протоколы: коммуникация в среднем и в худшем случае

$$CC(\pi) = \max_{x,y,r} (\text{количество бит, переданных } \pi \text{ на входной паре } (x, y) \text{ при случайных битах } r)$$

$$CC_{\text{ave}}(\pi) = \max_{x,y} \mathrm{E}_r \, (\text{количество бит, переданных } \pi \text{ на входной паре } (x, y) \text{ при случайных битах } r)$$

Вероятностные протоколы: разные виды ошибок

Безошибочные вероятностные протоколы:

$$R_0(f) = \min\{\, CC_{ave}(\pi) \mid \pi \text{ вычисляет } f(x,y) \text{ с без ошибки на любом входе } (x,y)\}$$

Вероятностные протоколы: разные виды ошибок

С двусторонней ошибкой:

$$R_\varepsilon(f) = \min\{ CC(\pi) \mid \pi \text{ вычисляет } f(x,y) \text{ с вероятностью ошибки не более } \varepsilon \text{ на любом входе } (x,y)\}$$

Вероятностные протоколы: разные виды ошибок

С односторонней ошибкой ($f : X \times Y \to \{0,1\}$):

$$R^1_\varepsilon(f) = \min\{CC(\pi) \mid \pi \text{ вычисляет } f(x,y) \text{ с вероятностью ошибки не более } \varepsilon \text{ на любом входе с } f(x,y)=1 \text{ и без ошибки на любом входе с } f(x,y)=0.\}$$

$R^0_\varepsilon(f)$ — то же самое, что $R^1_\varepsilon(f)$, только теперь ошибаться можно, если $f(x,y) = 0$.

Amplification

Уменьшение вероятности ошибки за счет повторения:

- протоколы с односторонней ошибкой: вероятность ошибки $\varepsilon \Longrightarrow$ вероятность ошибки ε^k при k повторениях
- протоколы с односторонней ошибкой: вероятность ошибки $1/2 - \delta \Longrightarrow$ вероятность ошибки $1/(\delta^2 k)$ и $e^{-2\delta^2 k}$ при k повторениях

Теорема

Пусть события $A_1, \ldots, A_k$ независимы и вероятность каждого из них равна p. Тогда вероятность того, что произошло более $k(p+\delta)$ событий не больше $1/(\delta^2 k)$ (еравенство Чебышёва) и $e^{-2\delta^2 k}$ (неравенство Чернова).

Частные и общие случайные биты

Алиса имеет $x, r_{\text{Alice}}, r_{\text{pub}}$,
Боб имеет $y, r_{\text{Bob}}, r_{\text{pub}}$.
r_{pub} — общие случайные биты
r_{Alice} — частные случайные биты Алисы
r_{Bob} — частные случайные биты Боба

$$R_{\varepsilon}^{\text{pub}}(f) \leq R_{\varepsilon}^{\text{private}}(f)$$

Теорема Ньюмана:

Теорема (Newman)
$R_{\varepsilon+\delta}^{\text{private}}(f) \leq R_{\varepsilon}^{\text{pub}}(f) + O(\log(n/\delta))$, где $n = \log |X| \times |Y|$.

Вероятностная коммуникационная сложность предикатов равенства и порядка

$$R_\varepsilon^{0,\text{private}}(EQ) = O(\log(n/\varepsilon))$$

$$R_\varepsilon^{0,\text{pub}}(EQ) = O(\log(1/\varepsilon))$$

$$R_\varepsilon^{\text{private}}(GT) = O(\log n \log(n/\varepsilon))$$

$$R_\varepsilon^{\text{pub}}(GT) = O(\log(n/\varepsilon)) \quad \Rightarrow \quad R_\varepsilon^{\text{private}}(GT) = O(\log(n/\varepsilon))$$

[Feige, Peleg, Raghavan, Upfal]

Разбиение матрицы функции на одноцветные прямоугольники

$C^R(f) =$ минимальное количество прямоугольников в разбиении матрицы f на одноцветный прямоугольники

Теорема

$D(f) \geq \log C^R(f)$

Метод трудных множеств и размера прямоугольников

Множество $A \subset X \times Y$ называется *трудным* (fooling set) если любой одноцветный прямоугольник в $M(f)$ содержит не более одной пары из A.

Теорема

A трудное $\Rightarrow D(f) \geq \log C^R(f) \geq \log |A|$

Теорема

Пусть w — функция, сопоставляющая каждой паре x, y её *вес* $w(x, y)$ причем любой вес любого одноцветного прямоугольника в $M(f)$ не больше ε. Тогда $C^R(f) \geq w(X \times Y)/\varepsilon$.

Метод ранга матрицы

Теорема

$C^R(f) \geq \operatorname{rk} M(f)$.

Примеры

Трудные множества:
$A = \{(x, x) \mid x \in \{0,1\}^n\}$ для EQ и GT, $|A| = 2^n$.
$A = \{(x, \bar{x}) \mid x \in \{0,1\}^n\}$ для DISJ, $|A| = 2^n$.
$\mathrm{DISJ}(x, y) = \bigvee_{i=1}^{n}(x_i \wedge y_i)$.

Размеры прямоугольников: $\mathrm{IP}(x, y) = \bigoplus_{i=1}^{n}(x_i \wedge y_i)$.

Теорема

Любой одноцветный прямоугольник в $M(IP)$ содержит не более 2^n пар $\Rightarrow D(IP) \geq \log(2^{2n}/2^n) = n$.

Ранг матрицы:
$\mathrm{rk}M(EQ) = M(GT) = M(DISJ) = M(IP) = n$.

Соотношение вероятностной и детерминированной сложностей

Пусть $R^{\text{private}}_{1/2-\varepsilon}(f) = k$. Тогда $D(f) \leq 2^k(k + \log(1/\varepsilon))$.

Следствие. $R^{\text{private}}_{1/2-\varepsilon}(EQ) \geq \log n - \log\log n - \log\log(1/\varepsilon)$.

Трудные распределения вероятностей на входах

Лемма (Yao)

$R_\varepsilon^{\text{public}}(f) > k \iff$ существует распределение вероятностей μ на $X \times Y$ такое, что любой детерминированный протокол, ошибающийся не более чем на доле ε входов относительно μ, имеет высоту больше k.

Теорема (Chor–Goldreich)

Равномерное распределение на входах является трудным для IP: не существует детерминированного протокола высоты $n/2 + \log \varepsilon$, вычисляющего IP на доле $1/2 + \varepsilon$ всех входных пар.

Пестрота: доказательство теоремы Chor–Goldreich

Определение

Функция $f : \{0,1\}^n \times \{0,1\}^n \to Z$ называется α, β-пестрым относительно μ, если для любого прямоугольника $R \subset \{0,1\}^n \times \{0,1\}^n$ и любого $z \in Z$:

$$\sum_{(x,y) \in R : f(x,y) = z} \mu(x,y) \leq \alpha \mu(R) + \beta.$$

Лемма

Детерминированный протокол с L листьями может правильно вычислить α, β-пестрый предикат на доле не более $\alpha + \beta L$ входных пар относительно μ.

Лемма

Предикат IP является $1/2, 2^{-n/2}$-пестрым относительно равномерного распределения.

Недетерминированная сложность

Определение

Недетерминированным протоколом называется вероятностный протокол с частными случайными битами.
Недетерминированный протокол π вычисляет предикат $f : X \times Y \to \{0, 1\}$, если $f(x, y) = 1 \Leftrightarrow \mathrm{P}[\pi(x, y) = 1] > 0$.
Через $N^1(f)$ обозначается минимальная коммуникационная сложность недетерминированного протокола вычисления f, а через $N^0(f)$ — минимальная коммуникационная сложность недетерминированного протокола вычисления $\neg f$.

Недетерминированная сложность

Определение

$C^1(f)$ — минимальное количество прямоугольников цвета 1, которыми пожно покрыть (возможно с пересечениями) все единицы в матрице f. $C^0(f)$ — минимальное количество прямоугольников цвета 1, которыми пожно покрыть (возможно с пересечениями) все единицы в матрице f.

Теорема

$\log C^1(f) \leq N^1(f) \leq \log C^1(f) + 2$,
$\log C^0(f) \leq N^0(f) \leq \log C^0(f) + 2$.

Теорема

$D(f) \leq C^1(f) + 1$, $D(f) \leq C^0(f) + 1$.

Теоремы Aho-Ullman-Yannakakis, Halstenberg-Reischuk и Разборова

Теорема (Aho-Ullman-Yannakakis, Halstenberg-Reischuk)

$D(f) \leq (\log C^1(f) + 1)(\log C^0(f) + 2)$.

Определение

DISJ_{nk} обозначает сужение предиката DISJ на k-элементные подмножества n-элементного множества.

Теорема (Разборов)

$D(DISJ_{nk}) \geq \log \binom{n}{k} \approx k \log n$,
$N^0(DISJ_{nk}) \leq \log n$,
$N^1(DISJ_{nk}) \leq O(k + \log \log n)$.