Вычислительно трудные задачи и дерандомизация
Лекции 7-8: Повышение трудности функции. Коды, исправляющие ошибки.

Дмитрий Ицыксон

ПОМИ РАН

19 апреля 2009

План

$H^{\rho}_{avg}(f) = \max\{S \mid \forall C, |C| \le S \implies \Pr_{x \leftarrow U_n}[C(x) = f(x)] < \rho\}$

$H_{wrs}(f) = H^{1}_{avg}$, $H_{avg}(f) = \max\left\{S \mid H^{\frac{1}{2}+\frac{1}{S}}_{avg}(f) \ge S\right\}$

Цель: По f с большой $H_{wrs}(f)$ построить f' с большой $H^{1-\delta}_{avg}(f')$.

1. Коды, исправляющие ошибки
   - Код Рида-Соломона
   - Код Уолша-Адамара
   - Каскадный код
   - Кода Рида-Мюллера
2. Локальное декодирование
3. Итог: дерандомизация

Коды, исправляющие ошибки

Определение. Σ — конечный алфавит. $E : \Sigma^n \to \Sigma^m$ называется кодом, исправляющим ошибки с расстоянием δ, если для всех $x \neq y \in \Sigma^n$ выполняется
$\Delta(E(x), E(y)) = \frac{1}{m}|\{i \mid E(x)_i \neq E(y)_i\}| \geq \delta$.
Замечание. Обычно $\Sigma = \{0, 1\}$.

Код Рида-Соломона

- $\mathbb{F}$ — конечное поле. $|\mathbb{F}| \geq m \geq n$.
- $\mathbb{F} = \{f_1, f_2, \dots, f_m, \dots\}$
- $RS : \mathbb{F}^n \to \mathbb{F}^m$.
- $RS(a_0, a_1, \dots, a_{n-1}) = (z_1, z_2, \dots, z_m)$, где
- $z_i = a_0 + a_1 f_i + a_2 f_i^2 + \dots + a_{n-1} f_i^{n-1}$

Код Рида-Соломона

- $\mathbb{F}$ — конечное поле. $|\mathbb{F}| \geq m \geq n$.
- $\mathbb{F} = \{f_1, f_2, \ldots, f_m, \ldots\}$
- $RS : \mathbb{F}^n \to \mathbb{F}^m$.
- $RS(a_0, a_1, \ldots, a_{n-1}) = (z_1, z_2, \ldots, z_m)$, где
- $z_i = a_0 + a_1 f_i + a_2 f_i^2 + \cdots + a_{n-1} f_i^{n-1}$
- Два разных многочлена степени $n - 1$ могут совпадать не более, чем в $n - 1$ точке.
- $x \neq y \implies \Delta(x, y) = \frac{1}{m}(m - (n-1)) = 1 - \frac{n-1}{m}$.
- Итого: код Рида-Соломона код с расстоянием $1 - \frac{n-1}{m}$.

Код Рида-Соломона: декодирование

- $(a_1, b_1), (a_2, b_2), \dots, (a_m, b_m) \in \mathbb{F}^2$
- Существует такой многочлен G степени d, что $G(a_i) = b_i$ для t различных i, где $t > \frac{m}{2} + \frac{d}{2}$.
- Требуется восстановить G за полиномиальное время.

Алгоритм Берлекампа-Велча

1. $E(x)$ — многочлен, такой, что $E(a_i) = 0$, если $G(a_i) \neq b_i$.
2. $\deg E(x) < \frac{m}{2} - \frac{d}{2}$
3. Пусть $C(x) = E(x)G(x)$, тогда для всех $1 \leq i \leq m$ выполняется $C(a_i) = b_i E(a_i)$.
4. Составим систему уравнение $C(a_i) = b_i E(a_i)$, где $\deg C < \frac{m}{2} + \frac{d}{2}, \deg E < \frac{m}{2} - \frac{d}{2}$.
5. m уравнений, $< m$ неизвестных — найдем ненулевое решение.

Алгоритм Берлекампа-Велча

1. $E(x)$ — многочлен, такой, что $E(a_i) = 0$, если $G(a_i) \neq b_i$.
2. $\deg E(x) < \frac{m}{2} - \frac{d}{2}$
3. Пусть $C(x) = E(x)G(x)$, тогда для всех $1 \leq i \leq m$ выполняется $C(a_i) = b_i E(a_i)$.
4. Составим систему уравнение $C(a_i) = b_i E(a_i)$, где $\deg C < \frac{m}{2} + \frac{d}{2}, \deg E < \frac{m}{2} - \frac{d}{2}$.
5. m уравнений, $< m$ неизвестных — найдем ненулевое решение.
6. $\widetilde{C}(x), \widetilde{E}(x)$ — найденные решения.
7. $\widetilde{C}(x) - \widetilde{E}(x)G(x)$ — многочлен степени $< \frac{m}{2} + \frac{d}{2}$, у которого $> \frac{m}{2} + \frac{d}{2}$ корней $\implies$ это нуль-многочлен.
8. $G(x) = \widetilde{C}(x)/\widetilde{E}(x)$.

Код Уолша-Адамара

- Основной недостаток кода Рида-Соломона: не бинарный алфавит.

Код Уолша-Адамара

- $x, y \in \{0,1\}^n$, определим $x \odot y = \oplus_{i=1}^n x_i y_i$.
- $WH(x) = (x \odot y)_{y \in \{0,1\}^n}$
- $WH : \{0,1\}^n \to \{0,1\}^{2^n}$
- Это линейный код: $WH(x \oplus z) = WH(x) \oplus WH(z)$
- $x, z \in \{0,1\}^n$, $x \neq z \implies x \oplus z \neq 0^n \implies \exists i (x \oplus z)_i = 1$.
- $y \in \{0,1\}^n$, $y^{(i)}$ — строка с замененым i-м битом. $(x \oplus z) \odot y \neq (x \oplus z) \odot y^{(i)}$.
- $WH(x)$ и $WH(z)$ отличаются как минимум в половине битов.
- Код Уолша-Адамара имеет расстояние $\frac{1}{2}$.

Каскадный код

- Код Рида-Соломона не для бинарного алфавита
- Код Уолша-Адамара экспоненциально удлиняет

Каскадный (concatenated) код

- Выберем поле $\mathbb{F}$, $|\mathbb{F}| = 2^k$
- $RS : \mathbb{F}^n \to \mathbb{F}^m$
- $WH : \{0,1\}^k \to \{0,1\}^{2^k}$
- Каждый элемент поля $\mathbb{F}$ стандартным образом отождествляется с $\{0,1\}^k$.
- $x \in \{0,1\}^{nk}$, $RS(x) = z_1 z_2 \dots z_m$, где $z_i \in \{0,1\}^k$
- $WH \circ RS(x) = WH(z_1)WH(z_2)\dots WH(z_m)$.

Каскадный код

- $x \in \{0,1\}^{nk}$, $RS(x) = z_1 z_2 \dots z_m$, где $z_i \in \{0,1\}^k$
- $WH \circ RS(x) = WH(z_1)WH(z_2)\dots WH(z_m)$.
- Пусть $\delta_1 = 1 - \frac{n-1}{m}$ — расстояние кода RS, $\delta_2 = \frac{1}{2}$ — расстояние кода WH.
- Расстояние каскадного кода $\delta_1 \delta_2$.
- $WH \circ RS : \{0,1\}^{nk} \to \{0,1\}^{m2^k}$
- Выберем $m = 5n \leq 2^k \leq 10n$. Тогда код $WH \circ RS : \{0,1\}^{nk} \to \{0,1\}^{5n2^k}$ с $\delta = 0.4$.

Код Рида-Мюллера

- $\mathbb{F}$ — конечное поле. ℓ, d — числа. $d < \mathbb{F}$.
- Входная строка: многочлен от ℓ переменных степени d:

$$P(x_1, x_2, \ldots, x_\ell) = \sum_{i_1+\cdots+i_\ell \leq \ell} c_{i_1 \ldots i_\ell} x_1^{i_1} x_2^{i_2} \ldots x_l^{i_\ell}$$

- Код: значение P на всех возможных значениях переменных.
- $RM : \mathbb{F}^{C_{\ell+d}^d} \longrightarrow \mathbb{F}^{|\mathbb{F}|^l}$
- При $l = 1$ получается код Рида-Соломона.
- При $d = 1, \mathbb{F} = \mathbb{Z}_2$ получается почти код Уолша-Адамара: $x \in \{0,1\}^n \mapsto z \in \{0,1\}^{2 \cdot 2^n}$, где $z_{y,a} = x \odot y \oplus a$, $y \in \{0,1\}^n, a \in \{0,1\}$
- Расстояние кода $1 - \frac{d}{|\mathbb{F}|}$.

Лемма Шварца-Зиппеля

Лемма. Если многочлен $p(x_1, x_2, \ldots, x_\ell)$ над конечным полем $\mathbb{F}$ ненулевой степени $\leq d$, тогда

$$\Pr_{a_1,\ldots,a_l \leftarrow F}[p(a_1, a_2, \ldots, a_\ell) \neq 0] \geq 1 - \frac{d}{|\mathbb{F}|}$$

Доказательство.

- $l = 1$: известное утверждение
- $p(x_1, \ldots, x_\ell) = \sum_{i=0}^{d} x_1^i p_i(x_2, \ldots, x_\ell)$
- Пусть k наибольшее число, что $p_k \neq 0$, $\deg p_k \leq d - k$.
- $\Pr_{a_1,\ldots,a_l \leftarrow F}[p_k(a_2, \ldots, a_\ell) \neq 0] \geq 1 - \frac{d-k}{|\mathbb{F}|}$
- Когда $p_k(a_2, \ldots, p_\ell) \neq 0$, то $p(x_1, a_2, \ldots, a_k)$ имеет $\leq k$ корней.
- $\Pr[p(a_1 \ldots a_m) \neq 0] \geq (1 - \frac{k}{|\mathbb{F}|})(1 - \frac{d-k}{|\mathbb{F}|}) \geq 1 - \frac{d}{|\mathbb{F}|}$

Локальный декодер

Определение. $E : \{0,1\}^n \to \{0,1\}^m$ — код. Локальным декодером для E, исправляющим ρ ошибок, называется вероятностный алгоритм D:

1. Который получает оракульный доступ к битам y, где $\Delta(y, E(x)) < \rho$
2. D работает $poly(\log m)$ шагов
3. $\Pr[D^y = x_j] \geq \frac{2}{3}$

Чем помогает локальный декодер?

- Пусть $f : \{0,1\}^n \to \{0,1\}$ — явная трудная функция $H_{wrs}(f) = S(n)$.
- Таблица истинности f — это строка из $\{0,1\}^N$, где $N = 2^n$.
- $E(f) \in \{0,1\}^{N^c}$ — это таблица истинности функции $g : \{0,1\}^{cn} \to \{0,1\}$.
- Пусть $H_{avg}^{1-\rho}(g) = S'(cn)$.
- Есть локальный декодер, который читает $E(f)$ с ρ ошибками, работает $(cn)^r$ шагов.
- По декодеру строим схему размера $(cn)^{2r} n^2 S'(cn)$, которая без ошибок вычисляет f.
- $S'(cn) \geq S(n)/poly(n)$

Локальный декодер для кода Уолша-Адамара

- Дана такая функция $g : \{0,1\}^n \to \{0,1\}$, что $\Pr_y[g(y) \neq x \odot y] \leq \rho < \frac{1}{4}$ для некоторого x.
- Требуется узнать x_j
- Пусть e^j: вектор с $e^j_j = 1, e^j_k = 0, k \neq j$.
- Выберем случайную строку $y \in \{0,1\}^n$.
- С вероятностью $1 - 2\rho > \frac{1}{2}$ выполняется $g(y) = x \odot y, g(y + e^j) = x \odot (y + e^j)$.
- $g(y) + g(y + e^j) = x \odot y + x \odot (y + e^j) = 2(x \odot y) + x \odot e^j = x \odot e^j = x_j$.
- Повторением можно понизить вероятность ошибки.

Локальный декодер для кода Рида-Мюллера

- Будем считать, что многочлен задан не списком коэффицентов, а значениями на некоторых $C_{\ell+d}^{\ell}$ точках.
- $\Pr_{y\in\mathbb{F}^\ell}[P(y) \neq g(y)] < \rho \leq (1 - \frac{d}{|\mathbb{F}|})/6$, P — многочлен степени d от ℓ переменных.
- Цель: вычислить $P(x)$ (есть оракульный доступ к g!).
- Выберем случайную прямую, проходящую через точку x. $L_x = \{x + ty \mid t \in \mathbb{F}\}$, $y \leftarrow U(\mathbb{F}^\ell)$
- Запросим g на всех $|\mathbb{F}|$ точках L_x, получим точки $\{(t, g(x + ty))\}$ для $t \in \mathbb{F}$.
- С вероятностью хотя бы $\frac{2}{3}$ на выбранной прямой будет не более $3\rho|\mathbb{F}| < (1 - d/|\mathbb{F}|)|\mathbb{F}|/2$ неправильных ответов.
- $Q(t) = P(x + ty)$ — многочлен степени d. Воспользуемся декодером для кода Рида-Соломона.
- Выдадим $Q(0)$.

Локальный декодер для каскадных кодов

- $E_1 : \{0,1\}^n \to \Sigma^m$, $E_2 : \Sigma \to \{0,1\}^k$, $E = E_2 \circ E_1 : \{0,1\}^n \to \{0,1\}^{mk}$. Декодер к E_i обрабатывает ρ_i ошибок и делает q_i запросов.
- Дан оракульный доступ к такой строке $y \in \{0,1\}^{mk}$, что $\Delta(y, E_2 \circ E_1(x)) < \rho_1\rho_2$
- Моделируем работу декодера E_1. Если нужен символ $E_1(x)$, то запускаем декодер для E_2, чтобы он выдал все биты этого символ с вероятностью $\geq 1 - 1/(10q_1)$. На это уйдет $O(q_2 \log|\Sigma| \log q_1)$ вопросов.
- Не более, чем в $\rho_1 m$ символах $E_1(x)$ символы искажены больше, чем на ρ_2.
- С вероятностью 0.9 удастся промоделировать корректную работу E_1.

$WH \circ RM$

Нам достаточно получить код $E : \{0,1\}^N \to \{0,1\}^{N^c}$, где $N = 2^n$:

1. Для всех $x \in \{0,1\}^N$, $E(x)$ вычислимо за время $poly(N)$
2. Есть локальный декодирующий алгоритм, которые использует $poly(\log N)$ времени и исправляет 0.01 долю ошибок.

Выберем код Рида-Мюллера с такими параметрами:

- $|\mathbb{F}| = \log^5 N$
- Число переменных $\ell = \log N / \log\log N$
- Степень $d = \log^2 N$

$WH \circ RM$

Выберем код Рида-Мюллера с такими параметрами:

- $|\mathbb{F}| = \log^5 N$
- Число переменных $\ell = \log N / \log\log N$
- Степень $d = \log^2 N$
- Вход имеет длину $C_{l+d}^{l} \geq (\frac{d}{l})^l > N$ (можно считать, что вход из $\{0,1\}^N$). Выход имеет длину $|\mathbb{F}|^l \leq poly(N)$. Расстояние кода не меньше, чем $1 - 1/\log N$.
- Код $WH : \{0,1\}^{\log|\mathbb{F}|} = \{0,1\}^{5\log\log N} \to \{0,1\}^{|\mathbb{F}|} = \{0,1\}^{\log^5 N}$.
- $WH \circ RM : \{0,1\}^N \to \{0,1\}^{poly(N)}$
- Существует локальный декодер, исправляющий $(1 - 1/\log N)\frac{1}{6} \cdot \frac{1}{2}$ ошибок.

Дерандомизация

- По $f \in DTime(2^{O(n)})$ с $H_{wrs}(f) = S(n)$ строится $g \in DTime(2^{O(n)})$ с $H_{avg}^{0.99}(g) = S(n)/poly(n)$;
- По XOR-лемме $H_{avg}^{\frac{1}{2}+\epsilon}(g^{\oplus k}) \geq \frac{\epsilon^2}{poky(N)} S'(n)$, $\epsilon < 0.99^k$, $S'(n) = S(n)/poly(n)$.
- $\frac{1}{S'} < \epsilon < 0.99^k$
- $k = O(\log S') = O(n)$, $g^{\oplus k} : \{0,1\}^{n^2} \to \{0,1\}^{S'(n)}$
- Если $H_{wrs}(f) \geq 2^{n^\epsilon}$, то $\mathbf{BPP} \subseteq \mathbf{QuasiP} = \mathbf{DTime}[2^{polylog(n)}]$.
- Если $H_{wrs}(f) \geq n^{\omega(1)}$, то $\mathbf{BPP} \subseteq \mathbf{SUBEXP} = \cap_{\epsilon>0} \mathbf{DTime}[2^{n^\epsilon}]$.