Математические основы Computer Science
Часть 3: Коды, исправляющие ошибки.
Лекции 10 и 11.

Дмитрий Ицыксон

ПОМИ РАН

13 декабря 2009

Содержание лекции

1. Теорема Форни
2. Оценки Плоткина
3. Код Адамара
4. Код Рида-Майлера
5. Код БЧХ

Источники

1. Madhu Sudan. Essential Coding Theory, Lecture notes, http://people.csail.mit.edu/madhu/FT02/
2. А. Румянцев, А. Ромащенко, А. Шень. Заметки по теории кодирования. http://www.mccme.ru/~anromash/courses/essential-coding-theory.pdf

В прошлый раз

- Код: $F : \Sigma^k \to \Sigma^n$, $n > k$.
- Код с расстоянием d позволяет исправить e ошибок, если $d \geq 2e + 1$.
- Граница Хэмминга: $q^k V_q(e, n) \leq q^n$.
- Граница Гилберта: $(q^k - 1)V_q(2e, n) < q^n$.
- Код Рида-Соломона:
  - $RS : \mathbb{F}^k \to \mathbb{F}^n$. $\mathbb{F} = \{f_1, f_2, \ldots, f_n, \ldots\}$.
  - $RS(a_0, a_1, \ldots, a_{k-1}) = (z_1, z_2, \ldots, z_n)$, где
  - $z_i = a_0 + a_1 f_i + a_2 f_i^2 + \cdots + a_{k-1} f_i^{k-1}$
- Каскадные коды:
  - $F_1 : \Sigma_1^{k_1} \to \Sigma_1^{n_1}$, $F_2 : \Sigma_2^{k_2} \to \Sigma_1^{n_2}$, $|\Sigma_1| = |\Sigma_2|^{k_2}$
  - Символ Σ_1 — блок из k_2 символов Σ_2
  - $F_1 \circ F_2 : \Sigma_2^{k_1 k_2} \to \Sigma_2^{n_1 n_2}$
  - Вычисляем $F_1(a) = b_1 b_2 \ldots b_{n_1}$, где $b_i \in \Sigma_1 = \Sigma_2^k$.
  - $F_1 \circ F_2(a) = F_2(b_1)F_2(b_2)\ldots F(b_{n_1})$

Теорема Форни

- $F : \{0,1\}^k \to \{0,1\}^n$. Требуется, чтобы $\frac{k}{n}$ и $\frac{e}{n}$ были отделены от нуля.
- Каскадный код, внешний код Рида-Соломона, а внутренний ищется перебором код, на котором достигается граница Варшамова-Гилберта.
- Длина кодового слова внутреннего кода $O(\log n)$
- Пусть $\mathbb{F}$ — поле из 2^k элементов.
- $RS : \mathbb{F}^{2^{k-1}} \to \mathbb{F}^{2^k}$
- Внутренний код $C : \{0,1\}^k \to \{0,1\}^{2k}$.
- $RS \circ C : \{0,1\}^{k2^{k-1}} \to \{0,1\}^{2k2^k}$.
- Расстояние внутреннего кода 10%, расстояние RS 50%. Итого: расстояние 5%.
- Можно исправить 2.5% ошибок.

Код Форни-Возенкрафта-Юстесена

- $\mathbb{F}$ — поле размера 2^k
- $\alpha \in \mathbb{F}$, $C_\alpha : \mathbb{F} \to \mathbb{F}^2$, $C_\alpha : x \to (x, \alpha x)$
- C_α не все являются кодами, например при $\alpha = 0$
- Лемма. (Лемма Возенкрафта) Для $\alpha \in \mathbb{F}$, при которых код C_α имеет кодовое расстояние не более s, не превосходит $\frac{V_2(s,k)^2}{2^k}$
- $V_2(s,k) \approx 2^{kH(s/k)}$, при малых s/k число $2^{(2H(s/k)-1)k}$ близко к нулю.
  Доказательство.
  - Пусть кодовое расстояние C_α не больше s
  - $\exists x$: в $(x, \alpha x)$ не больше s единичек.
  - $x, \alpha x$ лежат в шаре радиуса s в центре в нуле.
  - $\alpha = \frac{\alpha x}{x}$
  - Количество таких α не превосходит $V_2(s,k)^2$

Код Форни-Возенкрафта-Юстесена

- Применим код C_α как внутренний при каскадном кодировании.
- К $P(x)$ применяем код C_x: $(P(x), xP(x))$
- $RS : \mathbb{F}^{2^{k-1}} \longrightarrow \mathbb{F}^{2^k}$
- $FWU : \{0,1\}^{2^{2k-1}} \longrightarrow \{0,1\}^{2^{2k+1}}$
- $\exists \varepsilon > 0$, что доля $x \in \mathbb{F}$ для которых расстояние меньше ε не более 1%

Коды с большими расстояниями

- Существует ли код $\{0,1\}^k \to \{0,1\}^n$ с расстоянием $0.99n$?
  - В таком коде не больше 2-х кодовых слов.
- Лемма. Пусть $1 \geq \beta > \frac{1}{2}$. Количество точек в $\{0,1\}^n$, расстояния между которыми не меньше βn, не превосходит $\frac{1}{2\beta-1} + 1$.

  Доказательство.
  - Перейдем от 0/1 к 1/-1.
  - Скалярное произведение в $\mathbb{R}^n$: $(<x_1, \ldots, x_n>, <y_1, \ldots, y_n>) = \frac{\sum x_i y_i}{n}$
  - $|x| = \sqrt{(x,x)} = 1$.
  - Если $d(x,y) > \beta n$, то $(x,y) < 1 - 2\beta < 0$
  - $e_1, e_2, \ldots, e_N$ — множество кодовых слов
  - $0 \leq (e_1 + e_2 + \cdots + e_N, e_1 + e_2 + \cdots + e_N) \leq N + N(N-1)(1-2\beta)$
  - $N - 1 \leq \frac{1}{2\beta-1}$
- Нет шансов исправить $> 25\%$ ошибок.

Коды с большими расстояниями

- Что происходит, если расстояние чуть-чуть больше 50%?
- Углы между кодовыми словами тупые.
- Тогда число кодовых слов не больше $n + 1$.
  - Пусть $x_0, x_1, \ldots, x_k$ образуют попарно тупые углы. Покажем, что $x_1, x_2, \ldots, x_k$ — линейно независимы.
  - Выберем минимально линейно зависимое множество.
  - $\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m = 0$
  - Если все $\lambda_i > 0$, то $0 = (x_0, \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m) < 0$.
  - $\lambda_i x_i + \cdots = \lambda_j x_j + \ldots$
  - Квадрат вектора положителен и отрицателен одновременно!

Оценка Плоткина

- Пусть расстояние $\geq 50\%$. Т.е. углы прямые или тупые. Покажем, что число векторов $\leq 2n$.
- Можно считать, что линейная оболочка векторов совпадает со всем пространством.
- $x_1, x_2, \ldots, x_n$ — базис, остальные выражаются.
- К-ты разложения остальных векторов по базису отрицательны.
  - Перенесем отрицательные к-ты в левую часть
  - $x_k + (-\lambda_s)x_s + \cdots = \lambda_t x_t + \ldots$
  - Квадрат одновременно > 0 и ≤ 0
- Если общее число векторов $> 2n$
  - $x_{n+1}, \ldots$ — линейно зависимы
  - К-ты их линейной комбинации не могут быть одного знака (так как к-ты разложения по базису каждого отрицательны)
  - $\mu_s x_s + \cdots = \mu_t x_t + \ldots$, квадрат неположительный
- Оценка Плоткина: число кодовых слов на расстоянии $n/2$ не более $2n$.

Улучшение оценки Синглетона

- $F : \{0,1\}^k \to \{0,1\}^n$ — код с расстоянием d
- Оценка Синглетона: среди 2^k кодовых слов найдутся два слова с совпадающими первыми $k-1$ символами $\Longrightarrow\ d \leq n - k + 1.$
- $t = n - 2d$
- Среди 2^k кодовых слов найдутся 2^{k-t} кодовых слов, которые совпадают в первых t битах.
- $2^{k-t} \leq 4d$
- $k - n + 2d \leq \log(4d)$
- $\frac{k}{n} + 2\frac{d}{n} \leq 1 + \frac{\log(4d)}{n}$

Код Адамара

- $x, y \in \{0,1\}^m$, определим $x \odot y = \oplus_{i=1}^{m} x_i y_i$.
- $H : \{0,1\}^{s+1} \to \{0,1\}^{2^s}$
- $H(x) = (x \odot 1y)_{y \in \{0,1\}^s}$
- Это линейный код: $H(x \oplus z) = H(x) \oplus H(z)$
- $x, z \in \{0,1\}^s$, $x \neq z \implies x \oplus z \neq 0^n \implies \exists i (x \oplus z)_i = 1$.
- Если x и z отличаются только первым битом, то $H(x)$ отличается от $H(y)$ во всех битах. Далее $i > 1$.
- $y \in \{0,1\}^s$, $y^{(i)}$ — строка с замененым i-м битом. $(x \oplus z) \odot 1y \neq (x \oplus z) \odot 1y^{(i)}$.
- $H(x)$ и $H(z)$ отличаются как минимум в половине битов.
- Код Адамара имеет расстояние $\frac{1}{2}$.
- $n = 2^s$, $2n$ кодовых слов. Достигается оценка Плоткина.

Конкатенация Рида-Соломона и Уолша-Адамара

- Код Адамара: 2^{m+1} кодовых слов размера 2^m
- Макросимволы: битовые строчки размера 2^m. Нужно 2^m макросимволов.
- Код Рида-Соломона: $\varepsilon 2^m$ макросимволов переводит в 2^m.
- $\{0,1\}^{\varepsilon m 2^m} \to 2^{2m}$.
- Кодовое расстояние $\frac{1}{2}(1-\varepsilon)$

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 $d(y, E(x)) < \rho$
2. D работает $poly(\log m)$ шагов
3. $\Pr[D^y = x_j] \geq \frac{2}{3}$

Локальный декодер для кода Адамара

- Дана такая функция $g : \{0,1\}^{s+1} \to \{0,1\}$, что $\Pr_y[g(y) \neq x \odot 1y] \leq \rho < \frac{1}{4}$ для некоторого x.
- Требуется узнать x_j при $j > 1$.
- 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 $g(y) = x \odot 1y, g(y + e^j) = x \odot 1(y + e^j)$.
- $g(y) + g(y + e^j) = x \odot 1y + x \odot 1(y + e^j) = 2(x \odot 1y) + x \odot e^j = x \odot e^j = x_j$.
- Повторением можно понизить вероятность ошибки.
- Как определить x_1?
- Определим $x_2 x_3 \ldots x_n$, а затем найдем x_0 “голосованием”.

Код Рида-Маллера

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

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

- Код: значение P на всех возможных значениях переменных.
- $RM : \mathbb{F}^{C_{\ell+d}^d} \longrightarrow \mathbb{F}^{|\mathbb{F}|^l}$
- При $\ell = 1$ 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

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

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 $p_k \neq 0$, $\deg p_k \leq d - k$.
- $\Pr_{a_1,\ldots,a_\ell \leftarrow \mathbb{F}}[p_k(a_2, \ldots, a_\ell) \neq 0] \geq 1 - \frac{d-k}{|\mathbb{F}|}$
- Когда $p_k(a_2, \ldots, a_\ell) \neq 0$, 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 для кода Рида-Мюллера

- Будем считать, что многочлен задан не списком коэффицентов, а значениями на некоторых $C^{\ell}_{\ell+d}$ 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 $Q(0)$.

Коды БЧХ

- Авторы кода: Боуз (R.C. Bose), Чоудхури (D.K. Ray-Chaudhury) и Хоквингем (A. Hocquenghem)
- Код позволяет исправлять любое константное число ошибок.
- Обобщение кода Хэмминга.
- $\mathbb{F}$ — поле из $n = 2^k$ элементов.
- Многочлены степени $< n$:
  - $A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^n$
  - Определяется значениями в n точках поля
  - коэффициенты $\longleftrightarrow$ значения
- Два ограничения:
  - степень $< n - s$
  - Значения только 0 или 1

Коды БЧХ

- Два ограничения:
  - степень $< n - s$
  - Значения только 0 или 1
- Значения таких многочленов во всех точках поля — код Рида-Соломона с расстоянием $s + 1$
- $\mathbb{F}_2$ — подполе $\mathbb{F}$.
- Множество кодов — линейное пространство над $\mathbb{F}_2$.
- Без ограничений на к-ты многочлена размерность пространства кодов n
- Обращение в ноль каждого к-та: k уравнений
- $\mathbb{F}_2$-размерность $\geq n - sk = n - s \log n$
- При $s = 2$, $d = 3$, $2 \log n$ проверочных символов
- В коде Хэмминга было $\log n$ проверочных символов
- В БЧХ можно сэкономить на проверочных символах

Коды БЧХ

- $A(x)$ принимает значения только 0 или 1:
  - $A(x)^2 = A(x)$, многочлен $A(x)^2 - A(x)$ обращается в нуль для всех $x \in \mathbb{F}$.
  - $A(x) \vdots \prod_{a \in \mathbb{F}}(x - a)$
  - $\prod_{a \in \mathbb{F}}(x - a) = x^n - x$
- $A(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$
- $A^2(x) = a_{n-1}^2 x^{2n-2} + a_{n-2}^2 x^{2n-4} + \cdots + a_1^2 x^2 + a_0^2$
  - $a_{n-1}^2 = a_{n-1}$
  - $a_{n-2}^2 = a_{n-3}$
  - $a_{n-3}^2 = a_{n-5}$
  - $a_{n/2}^2 = a_1$
- Это линейные соотношения, так как $(a + b)^2 = a^2 + b^2 + 2ab = a^2 + b^2$
- Из условий $a_{n-1} = 0, a_{n-2} = 0, \ldots, a_{n-s} = 0$ можно оставить только $a_{n-1} = 0, a_{n-2} = 0, a_{n-4} = 0, \ldots$.
- $\mathbb{F}_2$-размерность $\geq n - \frac{s}{2}k = n - \frac{s \log n}{2}$

БЧХ и граница Хэмминга

- Граница Хэмминга: $2^k V_2(e, n) \leq 2^n$.
- Шар радиуса $e = s/2$ содержит примерно $C_n^e \approx \frac{n^e}{e!}$ элементов
- k примерно оценивается $n - e \log n + \log e!$
- БЧХ: $k = n - e \log n$