

Математические основы Computer Science  
Часть 3: Коды, исправляющие ошибки.  
Лекция 9.

Дмитрий Ицыксон

ПОМИ РАН

6 декабря 2009

## Содержание лекции

- 1 Постановка задачи
- 2 Границы Хэмминга и Гилберта
- 3 Случайные коды
- 4 Линейные коды, граница Варшамова-Гилберта
- 5 Код Хэмминга
- 6 Код Рида-Соломона
- 7 Каскадные коды

### 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>

## Постановка задачи

- $\Sigma$  — конечный алфавит,  $\Sigma_n$  — множество слов длины  $n$ .
- Расстояние Хэмминга между  $x_1x_2 \dots x_n \in \Sigma^n$  и  $y_1y_2 \dots y_n \in \Sigma^n$  — это  $|\{i : x_i \neq y_i\}|$ .
- Код:  $F : \Sigma^k \rightarrow \Sigma^n, n > k$ .
- Минимальное расстояние: минимум  $d(F(A), F(A'))$
- Код с расстоянием  $d$  позволяет исправить  $e$  ошибок, если  $d \geq 2e + 1$ .
- Код лучше, чем больше  $e$  и ближе  $n$  и  $k$
- В  $\Sigma^n$  требуется
  - упаковать без пересечений как можно больше шаров радиуса  $e$ .
  - выбрать как можно больше точек, что попарные расстояния между ними  $\geq 2e + 1$
- Хочется иметь эффективные алгоритмы кодирования и декодирования.

## Граница Хэмминга

Пусть  $|\Sigma| = q$ ,  $F : \Sigma^k \rightarrow \Sigma^n$  — код, исправляющий  $e$  ошибок.

- $V_q(e, n)$  — объем шара радиуса  $e$ .
- Шары радиуса  $e$  с центром в кодовых словах ( $F(\Sigma^k)$ ) не пересекаются.
- $q^k V_q(e, n) \leq q^n$
- $\frac{k}{n} + \frac{\log_q V_q(e, n)}{n} \leq 1$

## Граница Гилберта

**Теорема.** Если  $(q^k - 1)V_q(2e, n) < q^n$ , то существует код с параметрами  $q, k, n, e$ .

**Доказательство.**

- Будем выбирать кодовые слова одно за другим, чтобы расстояния между ними были  $> 2e$ .
- Если  $\ell$ -ое слово выбрать нельзя, то  $(\ell - 1)V_q(2e, n) \geq q^n$ .

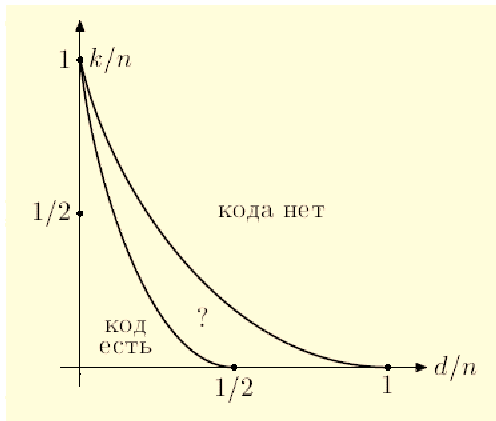
$$\frac{k}{n} + \frac{\log_q V_q(2e, n)}{n} \leq 1$$

## Размер шара

- Если  $q = 2$ , то  $V_2(s, n) = C_n^0 + C_n^1 + \dots + C_n^s$
- При  $s \leq \frac{n}{2}$ ,  $V_2(s, n) \leq sC_n^s = \text{poly}(n)2^{H(\frac{s}{n})n}$ .
- $H(p) = p \log \frac{1}{p} + (1 - p) \log \frac{1}{1-p}$
- Для произвольного  $q$ :  $V_q(s, n) = \text{poly}(n)q^{nH_q(\frac{s}{n})}$
- $H_q(p) = \left( p \log_q \frac{1}{p} + (1 - p) \log_q \frac{1}{1-p} \right) + p \log_q(q - 1)$

## Условия существования кода

- Граница Хэмминга:  $\frac{k}{n} + \frac{\log_q V_q(e, n)}{n} \leq 1$
- Граница Гилберта:  $\frac{k}{n} + \frac{\log_q V_q(2e, n)}{n} \leq 1$
- Граница Хэмминга:  $\frac{k}{n} + H\left(\frac{e}{n}\right) + O\left(\frac{\log n}{n}\right) \leq 1$
- Граница Гилберта:  $\frac{k}{n} + H\left(\frac{2e}{n}\right) + O\left(\frac{\log n}{n}\right) \leq 1$



## Случайные коды

- $N$  — натуральное число.
- Выберем  $N$  независимых случайных строк из  $\{0, 1\}^n$ :  
 $\xi_1, \xi_2, \dots, \xi_N \in \Sigma^n$ .
- Фиксируем  $i$ . Вероятность  $\xi_j$  попасть в шар радиуса  $2e$  с центром в  $\xi_i$  равна  $\frac{V_q(2e, n)}{q^n}$ .
- Вероятность, что хотя бы одно  $\xi_j$  попадет в этот шар  $\leq N \frac{V_q(2e, n)}{q^n}$ .
- $i$  — плохое, если в шар с центром  $\xi_i$  попадает  $\xi_j$  при  $i \neq j$ .
- Математическое ожидание числа плохих  $i$  не превосходит  $N^2 \frac{V_q(2e, n)}{q^n}$ .
- Математическое ожидание доли плохих  $i$  не превосходит  $N \frac{V_q(2e, n)}{q^n}$ .
- Пусть  $N \frac{V_q(2e, n)}{q^n} \leq \frac{1}{2}$
- Существуют такие строки  $x_1, x_2, \dots, x_N$ , что плохих индексов не больше половины. Выберем только хорошие.
- Кодовых слов в 4 раза меньше, чем в границе Гилберта.

## Линейные коды

- Пусть  $p$  — простое число,  $q = p^n$ ,  $\mathbb{F}_q$  — поле из  $q$  элементов.
- Линейный код: линейное отображение  $L : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$ .
- $d(L(x), L(y)) = d(L(x - y), 0)$
- Минимальное расстояние: минимальное число ненулевых координат кодового слова.
- Множество кодовых слов:  $k$ -мерное подпространство  $\mathbb{F}_q^n$ .
- Набираем элементы базиса:  $f_{i+1}$  должен быть на расстоянии  $> 2e$  от  $\langle f_1, f_2, \dots, f_i \rangle$
- Достаточно неравенства  $q^{k-1} V_q(2e, n) < q^n$  (оценка Варшамова-Гилберта).

## Проверочная матрица

- Подпространство размерности  $k$  в  $\mathbb{F}_q^n$  задается  $(n - k) \times n$  матрицей  $M$ .
- $x$  — кодовое слово  $\iff Mx = 0$ .
- Если любые  $d - 1$  столбцов линейно не зависимы, то расстояние кода  $\geq d$ .

## Код Хэмминга

- $q = 2, d = 2$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
M=	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

- Биты  $x_1, x_2, x_4, x_8$  — проверочные, остальные информационные.
- Эффективное кодирование/декодирование
- $Mx$  кодирует бит, в котором ошибка
- $2^{s-1} \leq n < 2^s$ , тогда  $H : \{0, 1\}^{n-s} \rightarrow \{0, 1\}^n$
- При  $n = 2^s - 1$  достигается граница Хэмминга.

## Неравенство Сингетона

**Теорема.**  $F : \Sigma^k \rightarrow \Sigma^n$  — код с расстоянием  $d$ . Тогда выполняется неравенство  $d \leq n - k + 1$ .

**Доказательство.** Среди  $q^k$  кодовых слов есть два у которых первые  $k - 1$  символ совпадают.

### Код Рида-Соломона

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

## Код Рида-Соломона

- $\mathbb{F}$  — конечное поле.  $|\mathbb{F}| \geq n \geq k$ .
- $\mathbb{F} = \{f_1, f_2, \dots, f_n, \dots\}$
- $RS : \mathbb{F}^k \rightarrow \mathbb{F}^n$ .
- $RS(a_0, a_1, \dots, a_{k-1}) = (z_1, z_2, \dots, z_n)$ , где
- $z_i = a_0 + a_1 f_i + a_2 f_i^2 + \dots + a_{k-1} f_i^{k-1}$
- Два разных многочлена степени  $k - 1$  могут совпадать не более, чем в  $k - 1$  точке.
- $d \geq n - k + 1$
- Итого: код Рида-Соломона код с расстоянием  $n - k + 1$ .

## 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  $\tilde{C}(x), \tilde{E}(x)$  — найденные решения.
- 7  $\tilde{C}(x) - \tilde{E}(x)G(x)$  — многочлен степени  $< \frac{m}{2} + \frac{d}{2}$ , у которого  $> \frac{m}{2} + \frac{d}{2}$  корней  $\implies$  это нуль-многочлен.
- 8  $G(x) = \tilde{C}(x)/\tilde{E}(x)$ .

## Каскадные коды

- $F_1 : \Sigma_1^{k_1} \rightarrow \Sigma_1^{n_1}$ ,  $F_2 : \Sigma_2^{k_2} \rightarrow \Sigma_1^{n_2}$ ,  $|\Sigma_1| = |\Sigma_2|^{k_2}$
- Символ  $\Sigma_1$  — блок из  $k_2$  символов  $\Sigma_2$
- $F_1 \circ F_2 : \Sigma_2^{k_1 k_2} \rightarrow \Sigma_2^{n_1 n_2}$
- Вычисляем  $F_1(a) = b_1 b_2 \dots b_{n_1}$ , где  $b_i \in \Sigma_1 = \Sigma_2^k$ .
- $F_1 \circ F_2(a) = F_2(b_1) F_2(b_2) \dots F_2(b_{n_1})$
- Пусть  $d_1$  расстояние кода  $F_1$ , а  $d_2$  — расстояние кода  $F_2$ .
- Два кодовых  $F_1$  слова различаются как минимум в  $d_1$  блоках, коды каждого блока различаются как минимум в  $d_2$  символах. Итого, расстояние  $\geq d_1 d_2$ .

## Декодирование каскадных кодов

- Пусть декодер для  $F_1$  исправляет  $e_1$  ошибок, а декодер для  $F_2$  исправляет  $e_2$  ошибок.
- $F_1 \circ F_2(a) = F_2(b_1)F_2(b_2) \dots F(b_{n_1})$
- Можно декодировать, если не более  $e_1$  блоков, в которых более  $e_2$  ошибок. Значит, можно исправить  $e_1 e_2$  ошибок.
- $e_1 e_2 \approx \frac{d_1 d_2}{4}$
- Если декодер для  $F_1$  позволяет бороться с пропусками (как с половиной ошибки), то можно добиться расстояния  $e_1 d_1$ .

## Декодирование каскадных кодов

- Пусть  $F_1$  исправляет  $u$  пропусков и  $v$  ошибок, если  $u + 2v < d_1$ .  $F_2$  исправляет  $e_2 \approx \frac{d_2}{2}$  ошибок.
- $t \in \{0, 1, \dots, e_2\}$
- Дано:  $n_1$  блок по  $n_2$  символов.
- Каждый блок декодируем, затем проверяем. Если ошибок  $> t$ , то блок называем неизвестным.
- **Лемма.** Если число ошибочных позиций  $\leq e_2 d_1$ , то как минимум при одном  $t$  можно правильно декодировать.
- Все  $t$  можно перебрать и проверить, что отличий меньше  $e_2 d_1$ .

## Декодирование каскадных кодов

**Лемма.** Если число ошибочных позиций  $\leq e_2 d_1$ , то как минимум при одном  $t$  можно правильно декодировать.

- Пусть  $\varepsilon_i$  — это число ошибок в  $i$ -м блоке
  - 1 Если  $\varepsilon_i \leq t$ , то  $i$ -й блок правильно декодирован.
  - 2 Если  $t < \varepsilon_i < d_2 - t$ , то  $i$ -й блок объявлен неизвестным
  - 3 Если  $d_2 - t \leq \varepsilon_i$ , то  $i$ -й блок неизвестен или неверно декодирован.
- $\alpha(t), \beta(t), \gamma(t)$  — количество блоков указанного вида.
- Достаточно доказать, что  $\beta(t) + 2\gamma(t) < d_1$  для некоторого  $t$ .
- Выберем случайное  $t$ . Посчитаем средний вклад в  $\beta(t) + 2\gamma(t)$  для  $i$  — блока.
  - Если  $\varepsilon_i \leq e_2$ , то в 3-ю группу вклада не будет. Средний вклад во 2-ю группу:  $\frac{\varepsilon_i}{e_2+1}$
  - Если  $\varepsilon_i > e_2$ , то вклад либо во 2-ю группу, либо в 3-ю. Вклад в 3-ю, если  $t \geq d_2 - \varepsilon_i$ . Средний вклад  $\frac{(e_2+1)-(d_2-\varepsilon_i)}{e_2+1} + 1 = \frac{2e_2+2-d_2+\varepsilon_i}{e_2+1} \leq \frac{\varepsilon_i+1}{e_2+1} < \frac{\varepsilon_i}{e_2}$
  - Итого средний вклад  $\leq (\sum_i \varepsilon_i)/e_2 < d_1$ .