Лекция 3

Ilya Yaroshevskiy

15 сентября

Содержание

1 Декодирование по ИС

Теорема 1.1. Алгоритм декодирования по ИС обеспечивает полное декодирование по минимальному расстоянию

Доказательство. Необходимо доказать, что для всякого исправимого вектора ошибки существует информационная совокупность, свободная от ошибок Пусть c – единственное решение некоторой задачи декодирования по минимальному расстоянию

- $e = y - c$ – вектор ошибки
- $E = \text{supp}(e)$ – множество позиций ненулевых элементов e. $|E| \leq n - k$

Пусть $N = \{1, 2, \ldots, n\}$. Предположим, что $N \setminus E$ не содержит информационных совокупностей $\implies$ существует различные кодовые слова, отличающиеся от принятого вектора в позициях E. Это противоречит предположению о единственности c. □

1.1 Покрытия

Определение. $M(n, m, t)$ **прокрытием** называется такой набор $F \subset 2^{N_n}$ из подмножеств мощности m множества $N_n = \{1, 2, \ldots, n\}$, что всякое t-элементное подмножество N_n содержится в одном из $f \in F$

Декодирование на ИС с исправлением не более t ошибок: необходимо покрыть все исправимые конфигурации ошибок. Элементы покрытия задают проверочные совокупности.

Пример. Пример декодирования $(7, 4, 3)$ кода, порождаемого $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

- $y = (0, 1, 1, 0, 1, 0, 0)$

- Все возможные конфигурации единичных ошибок покрываются проверочными совокупностями $M(7,3,1) = \{\{1,2,4\},\{5,6,7\},\{3,4,5\}\}$
- Им соответствуют информационные совокупности $\{\{3,5,6,7\},\{1,2,3,4\},\{1,2,6,7\}\}$
- Преобразованные порождающие матрицы

$$\begin{pmatrix}1&1&1&0&0&0&0\\1&0&0&1&1&0&0\\0&1&0&1&0&1&0\\1&1&0&1&0&0&1\end{pmatrix} \sim \begin{pmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{pmatrix} \sim \begin{pmatrix}1&0&0&1&1&0&0\\0&1&1&1&1&0&0\\0&0&1&0&1&1&0\\0&0&1&1&0&0&1\end{pmatrix}$$

- Кодовые слова, соответсвующие подвекторам принятого вектора:

$$\underline{(0,1,1,1,1,0,0)}, (0,1,1,0,0,1,1), \underline{(0,1,1,1,1,0,0)}$$

2 Дуальные коды

Определение. Пусть задан (n,k) код с проверочной матрицей H. **Дуальным** к нему называется $(n,n-k)$ код с порождающей матрицей H.

Определение. Кодовые слова дуального кода – множество всех проверок на четность исходного кода

Замечание. Скалярное произведение кодового слова из дуального кода на слово из исходного кода равно 0.

Определение. Самодуальным называется код, совпадающий со своим дуальным

Утверждение. *Код с проверочной матрицей $H = (A|I)$ самодуален ттогда, когда A – квадратичная матрица, такая что $AA^T = -I$*

$$HH^T = AA^T + I$$

3 Весовой спектр кода

Определение. Спектром линейного кода называется последовательность $A_i, i = 0 \dots n$, где A_i равно числу кодовых слов веса i

Определение. Весовая функция кода

$$W(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)}$$

Теорема 3.1 (Мак-Вильямс для двоичных линейных кодов)**.** Весовая функция кода C связана с весовой функцией дуального к нему кода $C_\perp$ соотношением

$$W_{C_\perp} = \frac{1}{|C|} W_C(x+y, x-y)$$

4 Границы

4.1 Граница Хемминга

Теорема 4.1 (Граница Хемминга)**.** Для любого q-ичного кода с минимальным расстоянием $d = 2t+1$ число кодовых слов удовлетворяет

$$A_q(n,d) \le \frac{q^n}{\sum_{i=0}^{t} C_n^i (q-1)^i}$$

Доказательство. Если код способен исправлять t ошибок, то вокруг всех кодовых слов можно описать хеммингговы шары радиуса t, не пересекающиейся друг с другом

При $n \to \infty$ скорость q-ичного кода удовлетворяет $R \leq 1 - h_q\left(\frac{d}{2n}\right)$, где

$$h_q(x) = -x \log_q x - (1-x)\log_q(1-x)$$

Аппроксимация Стирлинга $n! \approx 2^{n \log_2 n + o(1)}$

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t} C_n^i (q-1)^i} \leq \frac{q^n}{C_n^{\lfloor (d-1)/2 \rfloor}(q-1)^{(d-1)/2}} = \frac{q^n |(d-1)/2|!(n-|(d-1)/2|)!}{n!(q-1)^{(d-1)/2}} \approx$$
$$\approx 2^{n\log_2 q + \frac{d-1}{2}\log_2\left(\frac{d-1}{2}\right) + \left(n - \frac{d-1}{2}\right)\log_2\left(n - \frac{d-1}{2}\right) - n\log_2 n - \frac{d-1}{2}\log_2(q-1)}$$
$$R = \frac{\log_q A_q(n,d)}{n} \leq \log_q 2(\log_2 q + \delta \log_2 \delta + (1-\delta)\log_2(1-\delta) + \frac{\delta}{2}\log_2(-1)), \delta = \frac{d-1}{n} \approx \frac{d}{n}$$

□

4.2 Граница Варшамова-Гильберта

Теорема 4.2 (Граница Варшамова-Гильберта)**.** Существует q-ичный код длины n с минимальными расстоянием d, число слов которого удовлетворяет

$$A_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} C_n^i (q-1)^i}$$

Доказательство. Если код C имеет максимальную мощность, для любого вектора $x \notin C$ существует кодовое слово $c : d(x,c) \leq d-1$

Итеративное построение кода:

1. $A \coloneqq GF(q)^n$ (q^n различных векоторов)
2. Выберем произвольный вектор $c \in A$ и добавим его в код
3. Удалим из A шар радиуса $d-1$ с центром в c. Число элементов в шаре $\sum_{i=0}^{d-1} C_n^i (q-1)^i$. Число удаляемых элементов может быть меньше, т.к. некоторая часть шара могла быть удалена ранее
4. Если A не пусто, перейти к п. 2

□

4.3 Граница Варшамова-Гильберта для линейных кодов

Теорема 4.3 (Граница Варшамова-Гильберта для линейных кодов)**.** Если выполняется $q^r > \sum_{i=0}^{d-2} C_{n-1}^i (q-1)^i$, то существует линейный код над $GF(q)$ длины n с минимальными расстоянием не менее d и не более чем $r = n - k$ проверочными символами

Доказательство. Построим $(n-k) \times n$ матрицу H, такую что любые ее $d-1$ столбцов ЛНЗ

- Первый столбец – произвольный ненулевой вектор
- Если уже выбраны j столбцов, в качестве $(j+1)$-го не могут использоваться никакие линейные комбинации любых $d-2$ выбранных столбцов, число которых равно $\sum_{i=0}^{d-2} C_j^i (q-1)^i$
- Если запрещены еще не все q^{n-k} векторов, можно выбрат еще один столбец

□

Замечание. Существует (n,k,d) код над $GF(q)$, где $A_q(n,d) \geq q^k$, где k – наибольшее целое, такое что $q^k < \frac{q^n}{\sum_{i=0}^{d-2} C_{n-1}^i (q-1)^i}$ Граница ВГ для произвольных кодов: $A_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} C_n^i (q-1)^i}$. Существует бесконечная последовательность двоичных линейных кодов со скоростью $R \leq 1 - g(d/n)$.

4.4 Граница Грайсмера

Определение. $N(k,d)$ – минимальная длина двоичного линейного кода размерности k с минмальными расстоянием d.

Теорема 4.4 (Граница Грайсмера)**.** $N(k,d) \geq d + N(k-1, \lceil d/w \rceil)$

Доказательство. Будем считать, что порождающая матрица (n,k,d) кода C наименьшей длины $n = N(k,d)$ имеет вид

$$G = \Big(\underbrace{\begin{matrix} 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ & & & G' & & & \end{matrix}}_{N(k,d)-d} \Big| \underbrace{\begin{matrix} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ & & & * & & & \end{matrix}}_{d} \Big)$$

G' порождает код $(n-d, k-1, d')$. Пусть $(u|v) \in C,\ wt(u) = d' \implies d' + wt(v) \geq d$

$(u|1-v) \in C \implies d' + d - wt(v) \geq d \implies 2d' \geq d \implies d' \geq \lceil d/w \rceil \implies N(k-1, \lceil d/w \rceil) \leq N(k,d) - d$

□

Замечание.

$$N(k,d) \geq d + N(k-1, \lceil d/2 \rceil) \geq d + \lceil d/2 \rceil + N(k-2, \lceil d/4 \rceil) \geq \dots \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$$

Теорема 4.5 (Граница Мак-Элиса-Родемича-Рамсея-Велча)**.**

$$R \leq h\left(\frac{1}{2} - \sqrt{\frac{d}{n}\left(1 - \frac{d}{n}\right)} \right)$$

5 Другие формулировки задачи мягкого декодирования

5.1 Критерии мягкого декодирования

Утверждение. *Декодирования кода C по критерию максимуму правдоподобия в канале с АБГШ эквивалентно декодированию по критерию минимального расстояния Евклида*

Замечание. Рассмотрим передачу по каналу с АБГШ символов $(-1)^{c_i}, c_i \in \{0,1\}$, т.е. $y_i = (-1)^{c_i} + \eta_i$

$$\operatorname{argmin}_{c \in C} \sum_{i=0}^{n-1} (y_i - (-1)^{c_i})^2 = \operatorname{argmin}_{c \in C} \sum_{i=0}^{n-1} (y_i^2 - 2(-1)^{c_i} y_i + (-1)^{2c_i}) = \operatorname{argmax}_{c \in C} \sum_{i=0}^{n-1} (-1)^{c_i} y_i$$

Пусть $\hat{c}_i = \begin{cases} 0 & , y_i > 0 \\ 1 & , y_i \leq 0 \end{cases}$ – жесткие решения

$$\operatorname{argmax}_{c \in C} \sum_{i=0}^{n-1} (-1)^{c_i} y_i = \operatorname{argmax}_{c \in C} \sum_{i=0}^{n-1} ((-1)^{c_i} y_i - (-1)^{\hat{c}_i} y_i) = \operatorname{argmax}_{c \in C} \sum_{i: c_i \neq \hat{c}_i} -|y_i| = \operatorname{argmin}_{c \in C} E(c,y)$$

, где $E(c,y) = \sum_{i: c_i \neq \hat{c}_i} |y_i|$ – *корреляционная невязка*. y_i может быть заменено на логарифмические отношения правдоподобия $L_i = \log \frac{P\{c_i=0|y_i\}}{P\{c_i=1|y_i\}}$

Замечание. Задача минимизации евклидового расстояния эквивалентна задаче максимизации корреляция и эквивалентная задаче минимизации корреляционной невязки

5.2 Метод порядковых статистик

Замечание. Рассмотрим передачу кодовых слов $(c_0, \dots, c_{n-1})$ двоичного (n,k) кода с помощью символов 2-АМ по каналу без памяти. Пусть $(y_0, \dots, y_{n-1})$ – соответствующие принятые символы.

Пример. $y_i = (-1)^{c_i} + \eta_i,\ \eta_i \sim N(0, \sigma^2)$

- Пусть $L_i = \log \frac{P\{c_i=0|y_i\}}{P\{c_i=1|y_i\}}$ – логарифмические отношения правдоподобия

- Пусть $\hat{c}_i = \begin{cases} 0 & , L_i > 0 \\ 1 & , L_i < 0 \end{cases}$ – жесткие решения

Вероятность ошибки в $\hat{c}_i$ убывает с увеличением $|L_i|$. Выберем информационную совокупность J кода, соответствующую наибольшим значениям $|L_i|$. Приведем порождающую матрицу кода к виду G_J с единичной подматрицей в столбцах J. С большой вероятностью число неверных жестких решений $\hat{c}_i, i \in J$, мало. Переберем все конфигурации ошибок e веса не более t на J и построим кодовые слова $c_e = (\hat{c}_J + e)G_J$. Выберем наиболее правдоподобное из полученных кодовых слов. Сложность $O(k^2 n + \sum_{i=0}^{t} inC_k^i)$. При $t = d/4$ достигается вероятность ошибки, близкая к вероятности ошибки декодирования по максимуму правдоподобия