# Лекция 2

Ilya Yaroshevskiy

8 сентября

## Содержание

**1 Декодирование** **1**

**2 Метрики** **1**

**3 Кодирование** **2**
3.1 Блоковые коды . . . 2
3.2 Линейный код . . . 2
3.3 Простейшие коды . . . 3

**4 Декодирование** **3**
4.1 Код Хемминга . . . 3
4.2 Жесткое и мягкое декодирование . . . 4
4.3 Жесткое декодирование линейных кодов . . . 4
4.4 Код хемминга (продолжение) . . . 4
4.5 Стирание . . . 4

**5 Качество (performace) декодирования** **5**

**6 Декодирование по информационным совокупностям** **5**
6.1 Декодирование . . . 5

## 1 Декодирование

**Определение.** Критерий минимального расстояния $X = Y$. Декодер ищет кодово слово

$$c = \text{argmin}_{c \in \mathcal{C}} d(c, y)$$

**Определение.** Алгоритм называется алгоритмом полного декодирования по критерию $K$, если он способен найти решение соответствующуй оптимизационной задачи для любого возможного принятого сигнала

## 2 Метрики

**Определение.** Функция $d(x, y)$ называется метрикой, если:

- $d(x, y) \geq 0, d(x, y) = 0 \Leftrightarrow x = y$
- $d(x, y) = d(y, x)$
- Неравенстно треугольника $d(x, y) + d(y, z) \geq d(x, z)$

**Определение.** Метрическое пространство – множество $X$ с определенной на нем метрикой

*Пример.* Расстояние Хемминга $d_H(x,y) = |\{i|x_i \neq y_i\}|$. Двоичный симметричный канал ($p < 0.5, X = Y = \{0,1\}$:

$$\hat{c} = \text{argmax}_{x\in\emptyset} \prod_{i=1}^{n} P\{y_i|c_i\} = \cdots = \text{argmin}_{c\in\mathcal{C}} \sum_{i=1}^{n} a|y_i - c_i|$$

*Пример.* Расстояние Евклида $d_E(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$. Аддитивный Гауссовский канал с амплитудно-импульсной модуляцией ($Y = \mathbb{R}^n$).

*Пример.* Расстояние Ли ($A = GF(q)^n$) : $d_L(x,y) = \sum_{i=1} \min(|x_i - y_i|, q - |x_i - y_i|)$. Аддитивный Гауссовский канал с $q$-ичной фазовой модуляцией

*Пример.* Ранговое расстояние ($A = GF(q)^{n\times m}$) : $d_R(x,y) = \text{rank}(x - y)$. Сетевые коды

# 3 Кодирование

Операция канального кодирования вносит в информационную последовательность избыточность, необходимую для последующего исправления возможных ошибок

*Замечание.* Блоковые коды преобразуют блок из $k$ символов в блок из $n$ символов. Преобразование отдельных блоков выполняется независимо

*Замечание.* Сверточные коды преобразуют блок из $k$ символов в блок из $n$ символов. Преобразование зависит от предыдущих блоков.

## 3.1 Блоковые коды

*Замечание.* $n$ – длина кода $\mathcal{C}$. Для исправления ошибок требуется, чтобы не все $|X|^n$ последовательностей были кодовыми словами. Мощность кода (число различных кодовых слов) $M = |C|$.

*Замечание.* Скорость кода: $R = \frac{\log_{|X|} M}{n}$.

**Определение.** Минимальным расстоянием кода называется минимальное расстояние Хемминга между его различными кодовыми словами

*Пример.* Пример $C = \{000, 111\}, d_{m\times n}(C) = 3$

*Замечание.* Хеммингов шар радиуса $d_{\min} - 1$, описанный вокруг кодового слова $c \in C$, не содержит никаких других кодовых слов

**Утверждение.** *Код с минимальныи расстоянием Хемминга $d$ способен исправить* $\lfloor \frac{d-1}{2} \rfloor$

## 3.2 Линейный код

**Определение. Линейным** $(n,k)$ **(длины** $n$ **размерностью** $k$**) кодом** $C$ называется $k$-мерное линейное подпространство $n$-мерного линейного пространства над полем $GF(q)$.

*Замечание.* Число кодовых слов равно $q^k$

**Определение.** Порождающая $k \times n$ матрица полного ранга $G : C = \{y = xG|x \in GF(q)^k\}$

**Определение.** Проверочная матрица $r \times n$, $H : C = \{y \in GF(q)^n | yH^T = 0\}$, $r \geq n - k = \text{rank}(H)$

$$GH^T = 0$$

*Замечание.* С помощью линейных операций над строками и перестановок столбцов порождающая матрица может быть приведена к виду $G = (I|A)$.
**NB** Вообще говоря перестановкой столбцов получается порождающая матрица другого кода, поэтому перестановка столбцов в порождающей матрице должна быть согласована с перестановкой в проверочной

*Замечание.* Систематическое кодирование $xG = (x|xA)$ – информационный вектор является подвектором кодого слова. Применение систематического кодирования упрощает декодирование

$$H = (A^T| - I)$$

**Утверждение.** *Минимальное расстояние линейного блокового кода $\mathcal{C}$ равно* $d = \min\limits_{\substack{c' \neq c'' \\ c', c'' \in \mathcal{C}}} d(c', c'') = \min_{c \in \mathcal{C} \setminus \{0\}} wt(c)$*, где $wt(c)$ – вес вектора (количество единиц)*

*Доказательство.* Расстояние между двумя векторами – число позиций в которых они отличаются

$$d(c', c'') = \sum_{i=0}^{n} d(x, y) = \sum_{i=0}^{n} d(0, x - y) = d(0, c' - c'')$$

как код образует линейное подпространство, значит он группа по сложение, значит $c' - c''$ – кодовое слово. $wt(c)$ – вес Хемминга □

**Утверждение.** *Если $H$ – проверочная матица кода длины $n$, то код имеет размерность $n - r$ $\Leftrightarrow$ существуют $r$ линейно независимых столбцов матрицы $H$, а любые $r + 1$ столбцов линейно зависимы*

**Утверждение.** *Если $H$ – проверочная матрица кода длины $n$, то код имеет минимальное расстояние $d$ $\Leftrightarrow$ любые $1, 2, \ldots, d - 1$ столбцов $H$ линейно независимы, но существуют $d$ линейно зависимых столбцов матрицы $H$*

*Замечание.* Принадлежность коду $yH^T = 0$ эквивалентна ЛЗ столбцов

**Утверждение.** *Граница Синглтона (верхняя): для любого $(n, k, d)$ линейного кода $n - k \geq d - 1$*

*Следствие* 3.0.1. Ранг матрицы $H$ (максимальное число ЛНЗ столбцов) не может превосходить $n - k$

**Определение.** Граница Синглтона для произовльных кодов $A_q(n, d) \leq q^{n-d+1}$

**Определение.** Коды с $n - k = d - 1$ называются **разделимыми** кодами с максимальным достижимым расстоянием

### 3.3 Простейшие коды

*Пример.* Пусть $G$ – обратимая $n \times n$ матрица. Она порождает код $(n, n, 1)$.

*Пример.* $(n, 1, n)$ код с $n$-кратным повторением: $G' = (11 \ldots 1)$,

$$H' = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 1 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 1 \end{pmatrix}$$

*Пример.* $(n, n - 1, 2)$ код с проверкой на четность:

$$G'' = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 1 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 1 \end{pmatrix}, H'' = \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix}$$

## 4 Декодирование

### 4.1 Код Хемминга

**Определение.** Выберем в качестве столбцов матрицы $H$ все ненулевые двоичные векторы длины $r$:

- Длина кода $n = 2^r - 1$

- Размерность $k = n - r = 2^r - r - 1$
- Минимальное расстояние $d = 3$

*Пример.* Если столбцы выписаны в соответсвии с двоичным кодом:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

## 4.2 Жесткое и мягкое декодирование

В классичесической архитектуре предполагается что модулятор преобразует закодированные данные в сигнал, демодулятор оценивает символы кодовых слов, а декодер потом пытается исправить ошибки. Такой подход плох тем что теряется информация о надежности отдельных принятых символов. Сейчас как правило используют мягкое декодирование: демодулятор каким-то образом формирует информацию о надежности отдельных принятых символов, декодер при исправлении пытается учесть эту информацию.

## 4.3 Жесткое декодирование линейных кодов

*Замечание.* Рассмотрим двоичный симметричный канал с переходной вероятностью $p < 0.5$. Предположим что передатчик использует линейный блоковый код с порождающей матрицей $G$. Тогда принятый вектор $y = xG + e$, где $e$ – вектор ошибки, который содержит 1 на тех позициях где произошла ошибка.

**Определение. Синдром** принятого вектора $S = yH^T = xGH^T + eH^T = eH^T$ зависит только от вектора ошибки

**Определение.** Пусть есть подгруппа некоторой группы $G$, $G' \subset G$. Возьмем элемент $a \in G$, то **смежным классом** подгруппы $G'$, называется $aG' = \{a \cdot x | x \in G'\} \subseteq G$

**Определение. Лидер смежного класса** – минимальный по весу вектор.

*Замечание.* Рассмотрим все возможные вектора $e$ и выпишем соответсвующие синдромы. Отсортируем по весу все возможные вектора $e$, соответствующие каждому возможному значению синдрома (*стандартная расстановка*). В качестве решения задачи декодирования выбираем самый легкий вектор $e$, соответствующий вычисленному синдрому:

## 4.4 Код хемминга (продолжение)

*Замечание.* Если произошла только одна ошибка, то $S = eH^T$ будет равно какому-то столбцу матрицы $H$. Получается синдром – двоичное представление числа, которое является номером позиции в которой произошла ошибка.

## 4.5 Стирание

*Замечание.* Некоторые символы могут просто теряться. Стирания могут происходить одновременно с ошибками. Утверждается что $(n, k, d)$ код может исправить любую комбинацию из $t$ ошибок и $v$ стираний, если $d \geq 2t + v + 1$. Стирание эквивалентно выкалыванию кода на $v$ позиций $\implies$ минимальное расстояние уменьшается не более чем на $v$.

*Замечание.* Декодирование ошибок и стираний для кодов над $GF(2)$:

- Положить все стертые позиции равными 0, исправить ошибки в полученном векторе
- Положить все стертые позиции равными 1, исправить ошибки в полученном векторе
- Выбрать результат декодирования, ближайший к принятому вектору

# 5 Качество (performace) декодирования

**Определение. Весовой спектр кода** $A_i = |\{c \in C | wt(c) = i\}|$.

*Замечание.* Рассмотрим двоичный симметричный канал с переходной вероятностью $p$. Вероятность не обнаружения ошибки:

$$P_{\text{undetect}} = P\{S = 0\} = \sum_{i=d}^{n} A_i p^i (1-p)^{n-i} \leq \sum_{i=d}^{n} C_n^i p^i (1-p)^{n-i}$$

Вероятность правильного декодирования. Вероятность того, что вектор ошибки является лидером смежного класса:

$$P_{\text{correct}} = \sum_{i=0}^{l} L_i p^i (1-p)^{n-i}$$

, где $L_i$ – число лидеров смежных классов веса $i$, $l$ – максимальный вес лидера смежного класса

# 6 Декодирование по информационным совокупностям

**Определение. Информационной совокупностью** называется множество из $k$ позиций в кодовом слове, значения которых однозначно определяют значения на остальных позициях кодового слова

**Определение.** Если $\gamma = \{j_1, \ldots, j_k\}$ – ИС, то все прочие позиции $\{1, \ldots, n\} \setminus \gamma$ образуют **проверочную совокупносить**

**Утверждение.** *Если $\gamma = \{j_1, \ldots, j_k\}$ образует ИС, то матрица, составненная из столбцов $j_1, \ldots, j_k$ порождающей матрицы, обратима*

*Доказательство.* $G = (A|B)$ – порождающая матрица. Если матрица $A$ – необратима, у нее есть линейно зависимые столбцы или строки, значит $\exists x \neq 0 : xA = 0$. Есть кодовое $c = (c'|c'')$:

$$c + xG = (c'|c'') + (xA|xB) = (c' + xA|c'' + xB) = (c'|c'' + xB)$$

$xB \neq 0$ т.к. вся линейно зависимость осталась в матрице $A$. Получилось новое кодовое слово, которые совпадает с начальным на позициях $c'$. Получается что смотря на эти позиции нельзя однозначно указать значения на остальных позициях. Значит это не информационная совокупность. Противоречие, значит $A$ – обратимая □

**Определение.** $M(\gamma) = A^{-1}$

**Утверждение.** $G(\gamma) = M(\gamma)G$ – *породжающая матрица, содержащая единичную подматрицу на столбцах $\gamma$, где $M(\gamma)$ – подходящая обратимая матрица*

*Замечание.* $G = (A|B), G(\gamma) = (\overbrace{I}^{\gamma}|M(\gamma)B)$

**Определение.** ИС **свободна от ошибок**, если соответствующие позиции вектора $e$ равны 0: $e(\gamma) = 0$

## 6.1 Декодирование

*Замечание.* Декодирование $y = xG + e$ по информационным совокупностям:

- (первоначальный кандидат) $c = 0$
- Выбрать ИС $\gamma$. Вычислить $c' = y(\gamma)G(\gamma)$
- Если $d(c', y) < d(c, y), c = c'$
- Перейти к следующей ИС. Если все ИС проверены, возвратить $c$.
- Не всякие $k$ позиций образуют информационную совокупность