

5 Декодирование линейного кода. Коды Васильева

I. Пусть p — вероятность ошибки (искажения одного символа) в канале связи. Появление неправильного кодового слова на выходе декодера называется *ошибкой декодирования*, ее вероятность равна

$$P_{\text{ош}} \stackrel{\text{df}}{=} \frac{1}{|C|} \sum_{i=1}^{|C|} \text{prob}\{\text{выход декодера} \neq x^i \mid x^i \text{ было передано}\}.$$

• При использовании стандартного расположения

$$P_{\text{ош}} = 1 - \sum_{i=0}^n \alpha_i p^i (1-p)^{n-i}, \text{ где } \alpha_i \text{ — число лидеров веса } i \text{ смежных классов кода.}$$

• Код с расстоянием $d = 2t + 1$ называется *совершенным*, если шары радиуса t с центрами в кодовых вершинах, не пересекаясь, покрывают всё пространство E^n . Тогда

$$P_{\text{ош}} = 1 - \sum_{i=0}^t C_n^i p^i (1-p)^{n-i}.$$

• Код с расстоянием $d = 2t + 2$ называется *квазисовершенным*, если шары радиуса $t + 1$ с центрами в кодовых вершинах покрывают всё пространство E^n (при этом шары будут пересекаться). Тогда $P_{\text{ош}} = 1 - \sum_{i=0}^t C_n^i p^i (1-p)^{n-i} - \alpha_{t+1} p^{t+1} (1-p)^{n-t-1}$.

II. Пусть $C^{\frac{n-1}{2}}$ — любой совершенный код длины $\frac{n-1}{2}$ с расстоянием 3, $\lambda : C^{\frac{n-1}{2}} \rightarrow \{0, 1\}$ — произвольная функция. Множество $C^n = \{(u, u + v, |u| + \lambda(v)) \mid u \in E^{\frac{n-1}{2}}, v \in C^{\frac{n-1}{2}}\}$, где $|u| = u_1 \oplus \dots \oplus u_{\frac{n-1}{2}}$ является совершенным кодом длины n с расстоянием 3 и называется *кодом Васильева*.

5.1 Для линейного кода, заданного порождающей матрицей

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

построить таблицу стандартного расположения. Декодировать слово (110111) по таблице стандартного расположения и слово (101011) с помощью синдрома.

5.2 Вычислить вероятность ошибки декодирования для кода из задачи 5.1, если вероятность ошибки в канале связи $p = 0,01$.

5.3 Найти вероятность ошибки декодирования кода Хэмминга длины n .

5.4 Построить таблицу синдромов для расширенного кода Хэмминга длины 8. Найти вероятности правильного декодирования и ошибки декодирования для $p = 0,02$.

5.5 Вычислить нижние оценки числа различных и числа неэквивалентных кодов Васильева длины n .

5.6 Показать, что имеет место разбиение $E^n = \bigcup_{i=0}^n (C + e_i)$ для любого совершенного кода C длины n с расстоянием 3.

Теория к Семинару 6 "Поля Галуа".

I. Определение поля. Определение и свойства полей Галуа. Единственность поля Галуа каждого порядка с точностью до изоморфизма. Характеристика поля. Расширение поля. Порядок элемента поля. Примитивный элемент поля Галуа. Примитивный многочлен. Теорема Ферма.

II. Неприводимый многочлен над простым полем. Построение полей Галуа с помощью неприводимых многочленов.