Задачи к лекции 10

Пусть F — произвольный конечный алфавит, состоящий из q символов.

1. Пусть имеется код $C \subseteq F^n$ с минимальным расстоянием d. Докажите, что этот код может обнаружить $d-1$ ошибку.

2. Пусть $C \subseteq F^n$ — наибольший по мощности код, исправляющий t ошибок. Докажите, что

$$\frac{q^n}{1 + C_n^1(q-1) + C_n^2(q-1)^2 + \ldots + C_n^{2t}(q-1)^{2t}} \leqslant |C| \leqslant \frac{q^n}{1 + C_n^1(q-1) + C_n^2(q-1)^2 + \ldots + C_n^{t}(q-1)^{t}}.$$

Везде далее предполагается, что $F = \mathbb{F}_q$ — конечное поле из q элементов.

3. (Код с проверкой на чётность) Пусть $q = 2$ и функция кодирования $\mathbb{F}_2^k \to \mathbb{F}_2^{k+1}$ имеет вид $(a_1, \ldots, a_k) \mapsto (a_1, \ldots, a_k, a_1 \oplus \ldots \oplus a_k)$, где $\oplus$ обозначает сумму по модулю 2.

(а) Определите все кодовые слова и укажите проверочную матрицу для этого кода.

(б) Сколько ошибок этот код может обнаружить? А сколько исправить?

4. Пусть $k \geqslant 2$, $n = 2^k - 1$ и $C_k \subseteq \mathbb{F}_2^n$ — бинарный $(n, n-k)$-код Хэмминга.

(а) Докажите, что этот код является совершенным, то есть пространство $\mathbb{F}_2^n$ покрывается шарами радиуса 1 с центрами в кодовых словах.

(б) Предположим, что при передаче кодового слова по каналу связи произошла одна ошибка. Как узнать номер ошибочного символа?

Линейный код $C \subseteq \mathbb{F}_q^n$ называется *циклическим*, если из условия $(c_0, c_1, \ldots, c_{n-1}) \in C$ следует $(c_1, c_2, \ldots, c_{n-1}, c_0) \in C$. В этой ситуации $\mathbb{F}_q^n$ отождествляется с множеством многочленов степени не выше $n-1$, рассматриваемых как элементы факторкольца $\mathbb{F}_q[x]/(x^n - 1)$.

5. Докажите, что линейный код $C \subseteq \mathbb{F}_q^n$ является циклическим тогда и только тогда, когда он является идеалом в кольце $\mathbb{F}_q[x]/(x^n - 1)$.

6. Докажите, что всякого циклического кода $C \subseteq \mathbb{F}_q[x]/(x^n - 1)$ существует многочлен $g(x) \in \mathbb{F}_q[x]$, делящий $x^n - 1$, такой что все элементы из C кратны g.

7. Рассмотрим бинарный циклический $(7, 4)$-код, порождённый многочленом $(1 + x + x^3)$. Докажите, что кодовое расстояние этого кода равно 3.

8. При $m \geqslant 2$ рассмотрим расширение $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$. Пусть $\alpha \in \mathbb{F}_{q^m}$ — некоторый элемент.

(а) Докажите, что если α является корнем некоторого многочлена $f(x) \in \mathbb{F}_q[x]$, то α^q тоже является корнем этого многочлена.

(б) Пусть множество $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots\}$ содержит k элементов. Докажите, что минимальный многочлен элемента α над $\mathbb{F}_q$ равен $\prod\limits_{i=0}^{k-1} (x - \alpha^{q^i})$.

9. Укажите размерности всех бинарных БЧХ-кодов длины 15 и 31.