Коды Хэмминга и симплекс-коды

Для успешной сдачи этого листка необходимо решить шесть задач.

1. Докажите, что для совершенного кода лидеры смежного класса — в точности векторы веса, не превосходящего $[\frac{d-1}{2}]$, и в каждом смежном классе ровно один такой вектор. Приведите пример несовершенного кода, для которого это не так.

2. Пусть V — векторное пространство размерности r над полем $\mathbb{F}_q$. *Прямой* в V называется одномерное векторное подпространство в V. Определим *код Хэмминга*-(r, q) с помощью его **проверочной** матрицы H: в её **строках** будет написано по одному любому ненулевому вектору из каждой прямой. Вычислите длину и размерность кода Хэмминга.

3. Докажите, что, если вместо одной строки проверочной матрицы H кода Хэмминга взять другой вектор из той же прямой, то и в порождающей матрице G можно умножить **строку** G на число так, чтобы получить порождающую матрицу нового кода.

4. Покажите, что от перестановок строк и умножения их на ненулевые числа в порождающей матрице G минимальное расстояние кода и его свойство: быть совершенным, не меняются.

5*. Более общо, докажите, что при перестановке строк или умножения на ненулевое число множество старых кодовых слов переводится в множество новых кодовых слов с помощью линейной *изометрии* $\varphi\colon \mathbb{F}^n \to \mathbb{F}^n$, то есть линейного отображения такого, что для любых векторов $x, y \in \mathbb{F}^n$ выполнено $\mathrm{d}(x, y) = \mathrm{d}(\varphi(x), \varphi(y))$.

6. Найдите минимальное расстояние для кода Хэмминга. Докажите, что он совершенный.

7. Декодирование кода Хэмминга: докажите, что для кода Хэмминга работает следующий алгоритм декодирования: 1) вычислить вектор $H^T v$; 2) найти в H номер строки i такой, что, если её умножить на λ, то получится $H^T v$; 3) Вычесть из i-той координаты вектора v число λ.

8. *Симплекс-кодом*-(r, q) называется код, двойственный к коду Хэмминга (то есть проверочная матрица H кода Хэмминга для симплекс-кода является **порождающей**). Докажите, что любое ненулевое расстояние между его словами равно q^{r-1}.

9. *Весовой функцией* линейного кода C называется многочлен

$$W_C(x, y) = \sum_{v \in C} x^{n-w(v)} y^{w(v)};$$ напомним, что $w(v) =$ число ненулевых символов в v.

Докажите, что вероятность не заметить ошибку в информации, передаваемой по каналу $BSC(p)$, то есть бинарному каналу с вероятностью ошибки p в каждом символе, равна $W_C(1-p, p) - (1-p)^n$.

10. Вычислите вероятность не заметить ошибку для симплекс-кода-$(4, 2)$ в канале $BSC(10^{-1})$.