

Домашнее задание № 1

Опубликовано 08.09.19, Срок сдачи: 29.09.19 (23:59)

1 Код Адамара

Бинарный код Адамара, Had_r – это $[2^r, r]_2$ - код с порождающей матрицей $r \times 2^r$, столбцы которой представляют всевозможные битовые строки длины r . Докажите, что минимальное расстояние кода Had_r равно 2^{r-1} .

2 Линейные коды

Пусть C_1, C_2 – линейные коды длины n , заданные над \mathbb{F}_q порождающими матрицами G_1, G_2 . Определим следующие коды

- $C_3 = C_1 \cup C_2$
- $C_4 = C_1 \cap C_2$
- $C_5 = C_1 + C_2 = \{c_1 + c_2 : c_1 \in C_1, c_2 \in C_2\}$
- $C_6 = \{(c_1 | c_2) : c_1 \in C_1, c_2 \in C_2\}$, где $(\cdot | \cdot)$ обозначает конкатинацию слов.

Для $i = 1, \dots, 6$ обозначим за k_i – размерность кода $\log_q |C_i|$, а за d_i – минимальное расстояние кода C_i . Положим $k_1, k_2 > 0$.

1. Докажите, что C_3 – линейный тогда и только тогда, когда либо $C_1 \subseteq C_2$, либо $C_2 \subseteq C_1$.
2. Докажите, что коды C_4, C_5, C_6 – линейные
3. Докажите, что если $k_4 > 0$, то $d_4 \geq \max\{d_1, d_2\}$
4. Докажите, что $k_5 \leq k_1 + k_2$, и что равенство достигается тогда и только тогда, когда $k_4 = 0$
5. Докажите, что $d_5 \leq \min\{d_1, d_2\}$
6. Докажите, что

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

является порождающей матрицей для C_6 , а следовательно, $k_6 = k_1 + k_2$

7. Докажите, что $d_6 = \min\{d_1, d_2\}$.

3 Задание на программирование: расширенный код Хэмминга [15,11,3]

1. Кода Хэмминга [15,11,3] – обобщение изученного на лекции кода Хэмминга [7,4,3]. Отличное описание этого кода можно найти на
<https://www.youtube.com/watch?v=X8jsijhllIA>
https://www.youtube.com/watch?v=b3NxrZOu_CE&t=472s
2. Задача: реализовать алгоритм кодирования и декодирования для кода Хэмминга [15,11,3]. Названия функций и doctests можно найти по ссылке
https://crypto-kantiana.com/elena.kirshanova/teaching/coding_2020/PA1.txt