Практика № 1
04.09.23

1 Порождающие матрицы кодов

Напишите порождающие и проверочные матрицы для $[n, n-1, 2]_2$ – кода проверки на четность и для $[n, 1, n]_2$ кода с повторением.

2 Минимальное расстояние кода

Покажите, что минимальное расстояние любого линейного кода C равно минимальному весу Хэмминга ненулевого слова в C, т.е.,

$$\Delta(C) = \min_{c \in C, c \neq 0} wt(c).$$

A:

$$\Delta(C) = \min_{\substack{c_1, c_2 \in C, \\ c_1 \neq c_2}} \Delta(c_1, c_2) = \min_{\substack{c_1, c_2 \in C, \\ c_1 \neq c_2}} wt(c_1 - c_2) = \min_{c \in C} wt(c) \quad \text{так как } c := c_1 - c_2 \in C.$$

3 Систематическая форма

Пусть $G = [I_k|A] \in \mathbb{F}_q^{k \times n}$ - порождающая матрица $[n, k]_q$−кода C в систематической форме, где I_k− единичная матрица $k \times k$, $A \in \mathbb{F}_q^{k \times n-k}$. Опишите проверочную матрицу для C.

A: Для любого $c \in C, c = u \cdot G, u \in \mathbb{F}_q^k$, и вида G имеем $c = [u \mid uA]$.
$Hc = 0 \forall c$. Обозначим $H = [H_1 \mid H_2], H_1 \in \mathbb{F}_q^{n-k \times k}$.
$Hc = 0 \iff H_1 \cdot u^t + H_2 \cdot (uA)^t = 0 \iff H_1 \cdot u^t + H_2 A^t u^t = 0 \iff (H_1 + H_2 A^t) u^t = 0 \iff$
$\iff H_1 + H_2 A^t = 0$, так как равенство нулю предыдущей строки должно выполнятся для любого $u \in \mathbb{F}_q^k$ (а значит, можно найти k лин. независимых u, следовательно равенство нулю только из-за $H_1 + H_2 A^t = 0$). Из $H_1 + H_2 A^t = 0$ следует $H_1 = -A^t, H_2 = I_{n-k}$.

4 Дуальный код

Луальный код для кода C был определяется как

$$C^\perp = \{x \in \mathbb{F}_q \ : \ \langle x \, , c \rangle = 0 \, \forall c \in C\}.$$

1. Пусть G - порождающая матрица C. Докажите эквивалентность второго определения:

$$C^\perp = \{x \in \mathbb{F}_q \ : \ x G^{\mathsf{t}} = 0\}.$$

   Вывод: G – проверочная матрица $C^\perp$, $C^\perp$– линейный $[n, n-k]_q$–код для C– линейного $[n, k]_q$ – кода.

A: Обозначим $C' = \{x \in \mathbb{F}_q \ : \ xG^{\mathrm{t}} = 0\}$, покажем, что $C^{\perp} = C'$.
Пусть $x \in C^{\perp} \implies \langle x \, , c \rangle = 0 \; \forall c \in C$.
$c = u \cdot G$ для какого-то $u \in \mathbb{F}_q^k$.
$\langle x \, , c \rangle = 0 \iff x \cdot (uG)^t = 0 \; \forall u \in \mathbb{F}_q^k$.
$xG^t u^t = 0 \iff xG^t = 0$, так как можно выбрать k линейно-независимых $u \in \mathbb{F}_q^k$, для которых справедливо $xG^t u^t = 0$. Следовательно, $C^{\perp} \subseteq C'$.
$\dim C' = \dim \ker G^t = n - k = \dim C^{\perp}$. Из $C^{\perp} \subseteq C'$ и равенства размерности следует $C^{\perp} = C'$.

2. Эквивалентное утверждение: любая образующая матрица H дуального кода $C^{\perp}$ является проверочной матрицей кода C. Вывод: $(C^{\perp})^{\perp} = C$.

3. Постройте код, дуальный к $[n, 1, n]_2$ коду с повторением.

5 Количество порождающих матриц

Покажите, что для $[n, k]_q$– линейного кода C (q – простое), количество различных порождающих матриц равно

$$\prod_{i=0}^{k-1} (q^k - q^i).$$

A:

- Кол-во выборов первого базисного вектора v_1: $q^k - 1$ (все за исключением нулевого)
- Кол-во выборов второго базисного вектора v_2: $q^k - q$ (все за исключением q линейно-зависимых от v_1 векторов)
- Кол-во выборов второго базисного вектора v_3: $q^k - q^2$ (все за исключением q^2 линейно-зависимых от $\{v_1, v_2\}$ векторов)

В общем,

$$(q^k - 1) \cdot (q^k - q) \cdot \ldots \cdot (q^k - q^{k-1}) = \prod) i = 1^{k-1} (q^k - q^i).$$