

§ 1.5 Построение новых кодов из старых

1.5.1. Викаливание кодов

Пусть C — $[n, k, d]$ -код над $\mathbb{F}_q$.

Опр.: Процедурой **викаливания кода** C наз. удаление в каждом кодовом слове одной и той же координаты с номером, скажем, i . Получившийся линейный код длины $n-1$ обозначим через C^* .

Теорема 1.5.1: Пусть C — $[n, k, d]$ -код над $\mathbb{F}_q$, и пусть C^* — код C , викаливаемый в i -ой координате. Тогда

(i) Если $d > 1$, то C^* представляет собой $[n-1, k, d^*]$ -код, где $d^* = d-1$, когда в коде C есть слово минимального веса с ненулевой i -ой координатой, и $d^* = d$ в противном случае.

(ii) Если $d = 1$, то C^* представляет собой $[n-1, k, 1]$ -код, когда в коде C нет слова веса 1 с ненулевой i -ой координатой, в противном случае при $k > 1$ код C^* является $[n-1, k-1, d^*]$ -кодом с $d^* \geq 1$.

Упр. 23: Доказать теорему 1.5.1.

Пример 1.5.2: Пусть C — двоякий $[5, 2, 2]$ -код с порождающей матрицей

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Пусть C_1^* и C_5^* — коды, полученные викаливанием кода C в 1-ой и 5-ой координатах соответственно.

Их порождающие матрицы имеют вид

$$G_1^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{и} \quad G_5^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Таким образом,

C_1^* — $[4, 2, 1]$ -код, а C_5^* — $[4, 2, 2]$ -код

Пример 1.5.3: Пусть $\mathcal{D}$ — двоякий $[4, 2, 1]$ -код с порождающей матрицей

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Пусть $\mathcal{D}_1^*$ и $\mathcal{D}_4^*$ — коды, полученные вкалыванием кода $\mathcal{D}$ в 1-ой и 4-ой координатах соответственно.

Их порождающие матрицы имеют вид

$$D_1^* = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \quad \text{и} \quad D_4^* = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Таким образом,

$\mathcal{D}_1^*$ — $[3, 1, 3]$ -код и $\mathcal{D}_4^*$ — $[3, 2, 1]$ -код.

Зам.: Код $\mathcal{D}$ из примера 1.5.3 — это код C_1^* из примера 1.5.2. При этом, очевидно, код $\mathcal{D}_4^*$ может быть получен из кода C вкалыванием сразу в двух координатах $\{1, 5\}$.

В общем случае код C может быть вкалот в координатном подмножестве Γ удалением во всех кодовых словах компонент, индексированных множеством Γ . Полученный код часто обозначается как C^Γ .

Упр. 23.5: Показать, что если $|T| = t$, то код C^T представляет собой $[n-t, k^*, d^*]$ -код с $k^* \geq k-t$ и $d^* \geq d-t$.

1.5.2 Расширение кодов

Пусть C — $[n, k, d]$ -код.

Опр.: **Расширенным кодом** $\hat{C}$ для кода C наз. код, определенной как

$$\hat{C} = \left\{ x_1 x_2 \dots x_{n+1} \in \mathbb{F}_q^{n+1} \mid x_1 x_2 \dots x_n \in C \text{ и } x_1 + x_2 + \dots + x_{n+1} = 0 \right\}$$

Упр. 24: Показать, что $\hat{C}$ является $[n+1, k, d^*]$ -кодом, где $d^* = d$ или $d^* = d+1$.

Пусть G и H — порождающая и проверочная матрица для кода C .

Тогда порождающая матрица $\hat{G}$ для кода $\hat{C}$ может быть получена из матрицы G добавлением дополнительного столбца, так чтобы сумма элементов в каждой строке матрицы $\hat{G}$ стала равна 0:

$$\hat{G} = \left[\begin{array}{c|c} G & \begin{matrix} g_1 \\ \vdots \\ g_i \\ \vdots \\ g_k \end{matrix} \end{array} \right] \quad \forall i \quad \sum = 0$$

Проверочная матрица $\hat{H}$ для кода $\hat{C}$ выглядит следующим образом:

$$\hat{H} = \left[\begin{array}{c|c} 1 \ 1 \ \dots \ 1 & 1 \\ \hline & 0 \\ & i \\ & \vdots \\ & 0 \end{array} \right]$$

Такое расширение кода также называют *добавлением общей проверки на чётность*

Двоичный $[8, 4, 4]$ -код $\hat{H}_3$ из примера 1.3.2 получен из $[7, 4, 3]$ -кода Хэмминга H_3 добавлением общей проверки на чётность. Код $\hat{H}_3$ наз. *расширенным кодом Хэмминга*.

Упр. 25: Доказать, что матрица $\hat{H}$, имеющая вид (*), действительно является проверочной матрицей расширенного кода $\hat{C}$.

Упр. 26: Предположим, что расширение $[n, k]$ -кода C над F_q определяется как

$$\tilde{C} = \left\{ x_1 x_2 \dots x_{n+1} \in F_q^{n+1} \mid x_1 x_2 \dots x_n \in C \text{ и } x_1^2 + x_2^2 + \dots + x_{n+1}^2 = 0 \right\}.$$

При каких условиях код $\tilde{C}$ является линейным?

Если C — двоичный $[n, k, d]$ -код, тогда $\tilde{C}$ состоит из кодовых слов только чётного веса и является $[n+1, k, \hat{d}]$ -кодом, где

$$\hat{d} = \begin{cases} d, & \text{если } d - \text{чётно} \\ d+1, & \text{иначе.} \end{cases}$$

В не двоичном случае дело обстоит сложнее. Для $[n, k, d]$ -кода C над F_q минимальный вес чётно-подобных слов (нечётно-подобных слов) назовём *минимальным чётно-подобным весом* (нечётно-подобным весом) и обозначим его через d_e (d_o).

Тогда $d = \min \{d_e, d_o\}$, и

$$\hat{d} = \begin{cases} d_e, & \text{если } d_e \leq d_o \\ d_o + 1, & \text{если } d_o < d_e. \end{cases}$$

Пример 1.5.4: Напомним, что тетракод $\mathcal{H}_{3,2}$ из примера 1.3.3 является $[4,2,3]$ -кодом над $\mathbb{F}_3$ с порождающей и проверочной матрицами

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix} \quad \text{и} \quad H = \begin{bmatrix} -1 & -1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{bmatrix}.$$

Проверочная и порождающая матрицы расширенного кода $\widehat{\mathcal{H}}_{3,2}$ имеют вид

$$\widehat{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & -1 & -1 \end{bmatrix} \quad \text{и} \quad \widehat{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

При этом $d = d_e = d_o = 3$ и $\widehat{d} = 3$.

Если расширить код, а затем выколоть его в новой координате, то получим, очевидно, исходный код.

Однако если проводить операции в обратном порядке, то, вообще говоря, можно не получить исходный код.

Пример 1.5.5: Если выколоть двоичный код C с порождающей матрицей

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

в последней координате, а затем расширить полученный код, то получится код с порождающей матрицей

$$\widehat{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Упр. 27:

- (а) Пусть $C = H_{3,2} - [4, 2, 3]$ -код над $\mathbb{F}_3$ из примера 1.3.3 с порождающей матрицей

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}$$

Построить порождающую матрицу кода, полученного из C выкалыванием крайней правой координаты, а затем расширением справа. Определить минимальный вес полученного кода.

- (б) Пусть C — код над $\mathbb{F}_q$. Пусть $C_\perp$ — код, полученный из C выкалыванием в крайней правой координате, а затем расширением справа. Доказать, что $C = C_\perp$ т. и т. т., когда C — чётно-подобный код.

- (с) Пусть $C_\perp$ — код из (б). Доказать, что если C — самоортогональный и содержит слово $\vec{1} = 11\dots 1$, то $C = C_\perp$.

- (д) Пусть $C_\perp$ — код из (б). Доказать, что $C = C_\perp$ т. и т. т., когда $\vec{1} = 11\dots 1 \in C^\perp$.

1.5.3 Укорачивание кодов

Пусть C — $[n, k, d]$ -код над $\mathbb{F}_q$ и

T — t -элементное подмножество координат.

Рассмотрим множество $C(T)$, представляющее собой совокупность кодовых слов, у которых на позициях из мн-ва T стоят 0. Очевидно, $C(T)$ является подкодом кода C .

Опр.: Выкалывая код $C(T)$ во всех позициях из T , получим код над $\mathbb{F}_q$, который наз. **укороченным кодом** в позициях из T и обозначается через C_T .

Пример 1.5.6: Пусть C — двоичный $[6, 3, 2]$ -код с порождающей матрицей

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Код $C^\perp$ также является $[6, 3, 2]$ -кодом с порождающей матрицей

$$G^\perp = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Переименовываем координаты: $1, 2, \dots, 6$, и возьмём $T = \{5, 6\}$. Тогда порождающие матрицы укороченного кода C_T и выколотого кода C^T выглядят следующим образом:

$$G_T = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad \text{и} \quad G^T = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Укорачивание и выкалывание дуального кода приводят к кодам $(C^\perp)_T$ и $(C^\perp)^T$ с порождающими матрицами

$$(G^\perp)_T = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{и} \quad (G^\perp)^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

По порождающим матрицам G_T и G^T можно построить порождающие матрицы для кодов C_T и C^T :

$$(G_T)^\perp = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{и} \quad (G^T)^\perp = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix},$$

из которых видно, что

$$(C^\perp)^T = (C^T)^\perp \quad \text{и} \quad (C^\perp)^T = (C_T)^\perp.$$

Оказывается имеет место общий результат

Теорема 1.5.7: Пусть C — $[n, k, d]$ -код над F_q , а T — некоторое множество из t координат. Тогда

$$(i) \quad (C^\perp)_T = (C^T)^\perp \quad \text{и} \quad (C^\perp)^T = (C_T)^\perp$$

(ii) Если $t < d$, то C^T и $(C^\perp)_T$ имеют размерности k и $n-t-k$ соответственно.

(iii) Если $t = d$ и на T некоторое кодовое слово минимального веса полностью ненулевое, то C^T и $(C^\perp)_T$ имеют размерности $k-1$ и $n-d-k+1$ соответственно.

Док-во: Пусть $c \in C^\perp$, такое что все его координаты из T равны 0, а c^* — слово, полученное из c удалением всех координат из T . Следовательно, $c^* \in (C^\perp)_T$.

Если $x \in C$, то $0 = x \cdot c = x^* \cdot c^*$, где x^* — слово, выколотое в координатах из T . Таким образом,

$$(C^\perp)_T \subseteq (C^T)^\perp.$$

Любой вектор $c \in (C^T)^\perp$ может быть расширен до вектора $\hat{c}$ добавлением 0 на позиции из T . Возьмём произвольное слово $x \in C$, выколем x во всех позициях из T , получим $x^* \in C^T$. Поскольку $0 = x^* \cdot c = x \cdot \hat{c}$, то $c \in (C^\perp)_T$.

Заменяя в первом равенстве из (i) код C на $C^\perp$, получим второе равенство.

$\Rightarrow$ (i) доказано.

Предположим теперь, что $t < d$. Тогда $n-d+1 \leq n-t$. Из этого неравенства, согласно теореме 1.4.15, следует, что любые $n-t$ координат содержат информационное мн-во для кода C .

Следовательно, C^T должен быть k -мерным, а значит $(C^\perp)_T = (C^T)^\perp$ имеет размерность $n - k$, что доказывает (ii).

Как и для (ii), пункт (iii) будет доказан, если мы покажем, что C^T имеет размерность $k-1$. Итак, если $S \subset C^T$, $|S| = d-1$, то по пункту (ii) код C^S имеет размерность k . Ясно, что минимальное расстояние кода C^S равно 1, а код C^T может быть получен из C^S вставляя в нулевой координате некоторого кодового слова из C^S веса 1. Тогда по теореме 1.5.1 (ii) код C^T имеет размерность $k-1$. $\square$

Упр. 28: Пусть C — двоичный код с повторениями длины n (см. пример 1.2.2). Опишите $(C^\perp)_T$ и $(C_T)^\perp$ для любого T .

Упр. 29: Пусть C — код длины 6 из примера 1.4.4. Найдите порождающие матрицы для $(C^\perp)_T$ и $(C_T)^\perp$ при $T = \{1, 2\}$ и $T = \{1, 3\}$.

1.5.4 Прямые суммы

Пусть C_i , $i=1, 2$, — $[n_i, k_i, d_i]$ -коды над $\mathbb{F}_q$.

Опр.: Прямой суммой кодов C_1 и C_2 наз. $[n_1 + n_2, k_1 + k_2, \min(d_1, d_2)]$ -код

$$C_1 \oplus C_2 = \{(\vec{c}_1, \vec{c}_2) \mid \vec{c}_1 \in C_1, \vec{c}_2 \in C_2\}.$$

Упр. 30: Пусть G_i и H_i — порождающая и проверочная матрицы для кода C_i , $i \in \{1, 2\}$.
Показать, что

$$G_1 \oplus G_2 = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \quad \text{и}$$

$$H_1 \oplus H_2 = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}$$

— порождающая и проверочная матрицы для кода $C_1 \oplus C_2$.

Упр. 31: Пусть C — двоичный код с порождающей матрицей

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Построить группу порождающих матриц кода C , которая бы показывала, что код C является прямой суммой двух двоичных кодов.

Пример 1.5.8: $[6, 3, 2]$ -код C из примера 1.4.4 с порождающей матрицей

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

является прямой суммой 3 двоичных $[2, 1, 2]$ -кодов:

$$C = \mathcal{D} \oplus \mathcal{D} \oplus \mathcal{D},$$

где $\mathcal{D} = \{00, 11\}$.

1.5.5 Конструкция $(u / u+v)$

Пусть $C_i, i=1,2$, — $[n_i, k_i, d_i]$ -коды над $\mathbb{F}_q$.

Опр.: По определению $(u / u+v)$ конструкция по двум кодам C_1 и C_2 порождает новый код следующим образом:

$$C = \{ (u, u+v) \mid u \in C_1, v \in C_2 \}.$$

Упр. 32: Пусть G_i и H_i — порождающая и проверочная матрицы для кода $C_i, i \in \{1, 2\}$. Показать, что

$$\begin{bmatrix} G_1 & G_2 \\ 0 & G_2 \end{bmatrix} \text{ и } \begin{bmatrix} H_1 & 0 \\ -H_2 & H_2 \end{bmatrix}$$

являются порождающей и проверочной матрицей для кода C .

Пример 1.5.9: Рассмотрим двоярный $[8, 4, 4]$ -код C с порождающей матрицей

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Код C может быть из $[4, 3, 2]$ -кода C_1 и $[4, 1, 4]$ -кода C_2 с порождающими матрицами

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ и } G_2 = [1 \ 1 \ 1 \ 1]$$

соответственно, используя $(u / u+v)$ конструкцию.

В свою очередь, код C_1 также может быть построен с помощью $(u | u+v)$ конструкции из $[2, 2, 1]$ -кода C_3 и $[2, 1, 2]$ код C_4 с порождающими матрицами

$$G_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{и} \quad G_4 = [1, 1] \quad \text{соответственно.}$$

Упр. 33: Показать, что в результате применения $(u | u+v)$ конструкции к двум $[n, k_i, d_i]$ -кодам $C_i, i=1, 2$, получится $[2n, k, d]$ -код, у которого

$$k = k_1 + k_2, \quad d = \min\{2d_1, d_2\}.$$