§ 1.8 Коды Хэмминга

В данном параграфе мы обобщим конструкцию двоичного кода Хэмминга H_3 из примера 1.2.3, чья проверочная матрица имеет вид

$$H = [A^T \mid I_3] = \begin{bmatrix} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{bmatrix}$$

Заметим, что столбцы матрицы H суть все ненулевые двоичные вектора длины 3. Поэтому код H_3 эквивалентен коду с порождающей матрицей

$$H' = \begin{bmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{bmatrix}$$

Столбцы матрицы H' представляют собой естественным образом упорядочение числа $1, 2, \ldots, 7$ в двоичной системе счисления.

Эту форму порождающей матрицы легко обобщить. Пусть $n = 2^r - 1$, $r \geq 2$. Тогда $r \times (2^r - 1)$ матрица H_r, чьи столбцы представляют собой естественным образом упорядочение числа $1, 2, \ldots, 2^r - 1$ в двоичной системе счисления, будет являться проверочной матрицей $[n = 2^r - 1, k = n - r]$-кода. Любая перестановка столбцов этой матрицы будет давать эквивалентный код, и любой код из этого класса эквивалентности называется **двоичным кодом Хэмминга длины $n = 2^r - 1$** и обозначается как H_r или $H_{2,r}$

Зам.: Когда именуют код, то этим именем обычно называют любой код из соответствующего класса эквивалентности.

Упр. 54.5: Доказать, что

$$H_r - [2^r - 1, 2^r - 1 - r, 3]\text{-код}.$$

Этот код является уникальным в следующем смысле:

Теорема 1.8.1: Любой двоичный $[2^r-1, 2^r-1-r, 3]$-код эквивалентен двоичному коду Хэмминга $\mathcal{H}_r$.

Упр. 55: Доказать теорему 1.8.1.

Упр. 56: Доказать, что любой двоичный $[8,4,4]$-код эквивалентен расширенному коду Хэмминга.

Похожим образом коды Хэмминга $\mathcal{H}_{q,r}$ могут быть определены и над произвольным конечным полем $\mathbb{F}_q$. Для $r \geq 2$ код $\mathcal{H}_{q,r}$ имеет проверочную матрицу, в столбцы которой выбраны представители всех 1-мерных подпространств в $\mathbb{F}_q^r$ (другими словами, эти столбцы суть точки проективной геометрии $PG(r-1, q)$). Существует всего

$(q^r-1)/(q-1)$ 1-мерных подпространств. Таким образом код $\mathcal{H}_{q,r}$ имеет длину $n=(q^r-1)/(q-1)$, размерность $n-r$ и избыточность r.

Упр. 56.5: Показать, что $\mathcal{H}_{q,r}$ является $[n=(q^r-1)/(q-1), n-r, 3]$-кодом.

При $q=2$ $\mathcal{H}_{2,r} = \mathcal{H}_r$.

Из определения кода $\mathcal{H}_{q,r}$ видно, что этот код определен с точностью до монономиальной эквивалентности. Два кода C_1 и C_2 длины n над $\mathbb{F}_q$ называются монономально эквивалентными, если существует такой набор $\vec{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ и перестановка $\sigma \in Sym_n$, что

$$C_2 = \left\{ \vec{y} \;\middle|\; \vec{y} = (\vec{x} \odot \vec{\alpha})\sigma, \; \vec{x} \in C_1 \right\},$$

где $\vec{x} \odot \vec{\alpha} = (\alpha_1 x_1, \ldots, \alpha_n x_n)$.

Теорема 1.8.2: Любой $[(q^r-1)/(q-1), (q^r-1)/(q-1) - r, 3]$-код над $\mathbb{F}_q$ монимально эквивалентен коду Хэмминга $\mathcal{H}_{q,r}$.

Упр. 57: Доказать теорему 1.8.2.

Упр. 58: Показать, что тетракод из примера 1.3.3. с порождающей матрицей

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix} \quad \text{над } \mathbb{F}_3,$$

удачным образом обозначений как $\mathcal{H}_{3,2}$ действительно является кодом Хэмминга $\mathcal{H}_{3,2}$.

Дуальные к кодам Хэмминга называются **симплексными кодами**. Это $[(q^r-1)/(q-1), r]$-коды, чей спектр обладает весьма интересным свойством:

- симплексный код $\mathcal{H}_3^1$ имеет ненулевые кодовые слова только веса 4 (см. пример 1.2.3 и упр. 19)
- тетракод, будучи самодуальным кодом Хэмминга, имеет ненулевые кодовые слова только веса 3 (см. пример 1.3.3 и упр. 19)

и в общем случае:

Теорема 1.8.3: Ненулевые кодовые слова симплексного $[(q^r-1)/(q-1), r]$-кода над $\mathbb{F}_q$ все имеют вес q^{r-1}.

Док-во: Здесь без док-ва, а далее это будет частью теоремы 2.7.5.

Вместо полного док-ва теоремы 1.8.3 мы здесь построим двоичные симплексные коды с помощью немного модифицированной $(u|u+v)$ конструкции и докажем теорему 1.8.3 в этом случае.

Пусть $G_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$.

Для $r \geq 3$ определим G_r индуктивно:

$$G_r = \left[\begin{array}{c|c|c} 0 \dots 0 & 1 & 1 \dots 1 \\ \hline G_{r-1} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & G_{r-1} \end{array}\right]$$

Утверждается, что код S_r с порождающей матрицей G_r является дуальным к коду Хэмминга H_r.

Ясно, что количество строк в матрице G_r на одну больше, чем у матрицы G_{r-1}, и при этом у G_2 всего 2 строчки. Следовательно, у матрицы G_r ровно r строчек.

С другой стороны, пусть n_r — количество столбцов в матрице G_r. Тогда $n_2 = 2^2 - 1$ и $n_r = 2n_{r-1} + 1$. Следовательно, по индукции получаем, что $n_r = 2^r - 1$.

Наконец, все столбцы у G_2 ненулевые и различные. Кроме того, из конструкции видно, что у матрицы G_r будут все ненулевые и различные столбцы, если у матрицы G_{r-1} будут все ненулевые и различные столбцы. Таким образом, снова по индукции получаем, что G_r имеет $2^r - 1$ ненулевых различных столбцов длины r. Ненулевых двоичных векторов всего $2^r - 1$, и они представляют собой числа $1, 2, \dots, 2^r - 1$ в двоичной системе счисления. Именно в таком порядке и идут столбцы в матрице G_r.

Следовательно, $\mathcal{Y}_r = \mathcal{H}_r^{\perp}$.

Видно, что ненулевые слова кода $\mathcal{Y}_2$ имеют вес 2. Предположим, что ненулевые слова кода $\mathcal{Y}_{r-1}$ имеют вес 2^{r-2}. Тогда ненулевые слова подкода, порожденного последними $r-1$ строками матрицы G_r, имеют вид $(a, 0, b)$, где $a, b \in \mathcal{Y}_{r-1}$. Поэтому такие кодовые слова имеют вес $2 \cdot 2^{r-2} = 2^{r-1}$. Оставшиеся ненулевые слова кода $\mathcal{Y}_r$ имеют вид $(a, 1, b+\vec{1})$, где $a, b \in \mathcal{Y}_{r-1}$. Поскольку

$$wt(b+\vec{1}) = 2^{r-1} - 1 - 2^{r-2} = 2^{r-2} - 1, \text{ то}$$

$$wt(a, 1, b+\vec{1}) = 2^{r-2} + 1 + 2^{r-2} - 1 = 2^{r-1}.$$

Следовательно, по индукции получаем, что все ненулевые кодовые слова кода $\mathcal{Y}_r$ имеют вес 2^{r-1}.

§ 1.9. Коды Голея.

В этом параграфе будут изучаться как оригинальные двоичные и троичные коды Голея, описанные Голеем в 1949 г., так и их расширения вариант.

1.9.1. Двоичные коды Голея.

Обозначим через G_{24} — $[24, 12]$-код с порождающей матрицей $G_{24} = [I_{12} | A]$ в стандартной форме, где

$$A = \left[\begin{array}{c|cccccccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Матрица A представляет собой окаймлённую обратно циркулянтную матрицу. Пометим её столбцы слева направо символом ∞ и числами $0, 1, 2, \ldots, 10$. Первый столбец, соответствующий ∞, и первая строчка представляют собой окаймление. Во второй строчке за исключением позиции ∞ 1 стоит на позициях $0, 1, 3, 4, 5$ и 9. Эти числа представляют собой в точности все квадраты целых чисел по $\bmod 11$:

$$0^2 = 0, \quad 1^2 \equiv 10^2 \equiv 1 \bmod 11, \quad 2^2 \equiv 9^2 \equiv 4 \bmod 11,$$

$$\ldots$$

Третья строка получена установкой 1 в позицию ∞, которая затем дополняется частью второй строки на позициях $0, 1, \ldots, 10$, цикли-

чем сдвинутой на одну позицию влево. Четвертая строка получается из третьей также, как третья из второй, и т. д.

Обозначим через A_{11} обратно циркулянтную матрицу 11×11 матрицу, полученную из A удалением первой строки и столбца ∞.

Теорема 1.9.1: Код G_{24} является самодуальным $[24, 12, 8]$-кодом.

Док-во: Сначала заметим, что строки матрицы G_{24} имеют вес 8 или 12. В частности, скалярное произведение каждой строки матрицы G_{24} на себя равно 0.

Скалярное произведение первой строки матрицы G_{24} на любую другую строку также равно 0, например, потому что вес каждой строки матрицы A_1 равен 6.

При рассмотрении попарного скалярного произведения оставшихся строк матрицы G_{24} достаточно рассматривать только соответствующее скалярное произведение строк матрицы A_1. При этом, без ограничения общности, можно считать, что одна из этих строк является первой строкой матрицы A_1, в силу циркулянтности A_1. Прямой проверкой можно убедиться в том, что такие скалярные произведения равны 1, а значит соответствующие скалярные произведения строк матрицы G_{24} равны 0.

Следовательно, G_{24} является самодуальным кодом, у которого вес каждой строки порождающей матрицы $\vdots 4$. Тогда, по теореме 1.4.8(i), вес каждого кодового слова в код G_{24} $\vdots 4$.

Итак, G_{24} представляет собой самодуальный $[24, 12, d]$ – код, где $d = 4$ или 8.

Предположим, что $d = 4$. Заметим, что $A^T = A$. Тогда, поскольку G_{24} самодуальный, из теоремы 1.2.1 вытекает, что

$$[A^T \mid I_{12}] = [A \mid I_{12}]$$

также является его порождающей матрицей. Следовательно, если (a, b) – кодовое слово кода G_{24}, где $a, b \in F_2^{12}$, то и (b, a) – кодовое слово кода G_{24}. Поэтому если $c = (a, b)$ – кодовое слово кода G_{24}, то мы можем предположить, что $wt(a) \leq wt(b)$.

- Если $wt(a) = 0$, то и $wt(b) = 0$, т.к. G_{24} имеет порождающую матрицу в стандартной форме.
- Если $wt(a) = 1$, то c – это одна из строк порождающей матрицы G_{24}, чей вес > 4.
- Если $wt(a) = 2$, то c – это сумма двух строк порождающей матрицы G_{24}. Из-за циклической структуры матрицы A_{11} можно считать, что $wt(c)$ представляет собой сумму весов второй строки матрицы G_{24} и некоторой другой строки. Непосредственным перебором можно убедиться, что никакая из этих 11 сумм не даст вес 2 в последних 12 координатах.

Таким образом, $d = 8$.

□

Если выколоть код G_{24} в одной из координат, то получится двоичный $[23, 12, 7]$-код, обозначаемый как G_{23}. Оказывается, что все эти выколотые коды эквивалентны (это доказывается позднее).

Упр. 59: Доказать, что если код G_{24} выколоть в одной из координат, а затем расширить в той же позиции, то получится снова тот же самый код G_{24}.

Подсказка: см. упр. 27.

Опр.: Любой код, эквивалентный коду $\mathcal{G}_{23}$, называется *двоичным кодом Голея*; а любой код, эквивалентный коду $\mathcal{G}_{24}$, называется *расширенным двоичным кодом Голея*.

1.9.2. Троичные коды Голея

Рассмотрим код $\mathcal{G}_{12}$, представляющий собой $[12,6]$-код над F_3 с порождающей матрицей $G_{12} = [I_6 \mid A]$ в стандартной форме, где

$$A = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{array}\right].$$

Упр. 60: Доказать, что $\mathcal{G}_{12}$ является самодуальным троичным $[12,6,6]$-кодом.

Рассмотрим теперь $[12,6,5]$-код $\mathcal{G}_{11}$, получений из $\mathcal{G}_{12}$ выкалыванием в одной из координат. Снова вне зависимости от того, в какой позиции производится выкалывание, получаются эквивалентные коды. Однако расширение кода $\mathcal{G}_{11}$ в той же координате может не дать исходный код $\mathcal{G}_{12}$ — получится либо $[12,6,6]$-код, либо $[12,6,5]$-код в зависимости от выкалываемой координаты.

Упр. 61: Занумеруем последовательно столбцы матрицы A числами $\infty, 0, 1, 2, 3, 4$. Обозначим через $\mathcal{G}_{12}$ код, порождающая матрица которого G_{12} получена из матрицы A умножением столбца ∞ на -1.

(a) Показать, как получить элементы второй строки матрицы A с помощью квадратичных вычетов и невычетов по mod 5.

(b) Показать, что G_{12}' является самодуальным $[12, 6, 6]$-кодом.

(c) Показать, что викалывание кода G_{12}' в любой позиции, а затем расширение в этой позиции снова даст код G_{12}'.

(d) Показать, что если код G_{12} виколоть в координате ∞, а затем расширить его в этой координате, то получится код G_{12}'.

(e) Показать, что если код G_{12} виколоть в любой координате, отличной от ∞, а затем расширить его в той же координате, то получится $[12, 6, 5]$-код.

Согласно упр. 61, код G_{12}' является самодуальным $[12, 6, 6]$-кодом, покоординатно эквивалентным коду G_{12}. По тому же упр., если виколоть код G_{12}, а затем расширить в той же координате, то снова получится код G_{12}'. Оказывается, что все виколотые в одной координате коды G_{12}' эквивалентны коду G_{11}.

Опр.: Любой $[12, 6, 5]$-код, эквивалентный коду G_{11}, называется *троичным кодом Голея*; а любой $[12, 6, 6]$-код, эквивалентный коду G_{12}' (или G_{12}), называется *расширенным троичным кодом Голея*.

§ 1.10 Коди Рида – Маллера

В этом параграфе будут изучаться двоичные коды Рида – Маллера. Эти двоичные коды впервые были построены Маллером в 1954 г., а алгоритм мажоритарного декодирования для них был впервые описан Ридом также в 1954 г.

Определение кода Рида – Маллера может быть многими способами. Здесь приведено рекурсивное определение, основанное на $(u \mid u+v)$ конструкции.

Пусть m – положительное целое и r – неотрицательное целое, такое что $r \le m$. Двоичные коды, которые далее будут построены имеют длину 2^m. Для каждой такой длины существуют $m+1$ линейных кодов, обозначаемых как $R(r,m)$, каждый из которых называется **кодом Рида – Маллера** (или **RM – кодом**) r-ого порядка длины 2^m.

Коды $R(0,m)$ и $R(m,m)$ – тривиальные коды:

- RM – код 0-ого порядка $R(0,m)$ представляет собой двоичный код с повторениями длины 2^m,
- RM – код m-ого порядка $R(m,m)$ представляет собой все пространство $\mathbb{F}_2^{2^m}$.

Для $1 \le r < m$ определим

$$R(r,m) := \{(u \mid u+v) \mid u \in R(r,m-1), \; v \in R(r-1,m-1)\}.$$

Пусть $G(0,m) = [11\ldots1]$ и $G(m,m) = I_{2^m}$ – порождающие матрицы кодов $R(0,m)$ и $R(m,m)$ соответственно.

Для $1 \le r < m$ порождающая матрица $G(r,m)$ для кода $R(r,m)$ может быть построена как

$$G(r,m) = \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{bmatrix}.$$

Проиллюстрируем эту конструкцию, построив порождающие матрицы для кодов $R(r,m)$, $1 \le r \le m < 3$:

$$G(1,2) = \left[\begin{array}{cc|cc} 1&0&1&0 \\ 0&1&0&1 \\ \hline 0&0&1&1 \end{array}\right] \qquad G(1,3) = \left[\begin{array}{ccc|c} 1&0&1&0 & 1&0&1&0 \\ 0&1&0&1 & 0&1&0&1 \\ 0&0&1&1 & 0&0&1&1 \\ \hline 0&0&0&0 & 1&1&1&1 \end{array}\right]$$

$$G(2,3) = \left[\begin{array}{cccc|cccc} 1&0&0&0 & 1&0&0&0 \\ 0&1&0&0 & 0&1&0&0 \\ 0&0&1&0 & 0&0&1&0 \\ 0&0&0&1 & 0&0&0&1 \\ \hline 0&0&0&0 & 1&0&1&0 \\ 0&0&0&0 & 0&1&0&1 \\ 0&0&0&0 & 0&0&1&1 \end{array}\right]$$

По этим матрицам видно, что $R(1,2)$ и $R(2,3)$ представляют собой множества всех векторов чётного веса из пространств $\mathbb{F}_2^4$ и $\mathbb{F}_2^8$ соответственно.

Также заметим, что $R(1,3)$ — это самодуальный $[8,4,4]$-код, который, согласно упр. 56, есть код $\hat{H}_3$.

Теорема 1.10.1: Пусть r — целое, $0 \le r \le m$. Тогда

(i) $R(i,m) \subseteq R(j,m)$, если $0 \le i \le j \le m$.

(ii) $\dim R(r,m) = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$

(iii) Минимальный вес кода $R(r,m)$ равен 2^{m-r}

(iv) $R(m,m)^\perp = \{0\}$, и если $0 \le r < m$, то

$$R(r,m)^\perp = R(m-1-r,m)$$

Док-во:

(i) Вложение $\mathcal{R}(i,m) \subseteq \mathcal{R}(j,m)$ будет при $m=1$ (непосредственно проверяется) и при $i=m$ (поскольку $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$)

Предположим, что $\mathcal{R}(k,m-1) \subseteq \mathcal{R}(l,m-1)$ для всех $0 \le k \le l < m$. Пусть $0 < i \le j < m$, тогда

$$\mathcal{R}(i,m) = \{(u, u+v) \mid u \in \mathcal{R}(i,m-1),\ v \in \mathcal{R}(i-1,m-1)\}$$

$$\subseteq \{(u, u+v) \mid u \in \mathcal{R}(j,m-1),\ v \in \mathcal{R}(j-1,m-1)\} =$$

$$= \mathcal{R}(j,m)$$

Откуда утверждение (i) вытекает по индукции при $0 < i$. Если $i=0$, то нужно только проверить, что вектор $\vec{1} = (1\,1 \dots 1)$ принадлежит коду $\mathcal{R}(j,m)$ при $j < m$. Это легко доказывается по индукции. В самом деле, пусть $\vec{1} \in \mathcal{R}(j,m-1)$, тогда $\vec{1}$ будет лежать и в $\mathcal{R}(j,m)$, т.к. в $(u \mid u+v)$ конструкции можно взять $u = \vec{1}$ и $v = \vec{0}$.

(ii) При $r = m$ утверждение верно, т.к. $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$ и

$$\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{m} = 2^m.$$

Очевидно, что при $m=1$ оно также верно.

Теперь предположим, что

$$\dim \mathcal{R}(i,m-1) = \binom{m-1}{0} + \binom{m-1}{1} + \dots + \binom{m-1}{i}$$

для всех $0 \le i < m$.

Согласно упр. 33, $\dim \mathcal{R}(r,m) = \dim \mathcal{R}(r,m-1) +$

$+ \dim \mathcal{R}(r-1,m-1) =$

$$= \binom{m-1}{0} + \binom{m-1}{1} + \dots + \binom{m-1}{r} + \binom{m-1}{0} + \binom{m-1}{1} + \dots + \binom{m-1}{r-1} =$$

$$= \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$$

$$\binom{m-1}{0} = \binom{m}{0} \quad \text{и} \quad \binom{m-1}{i-1} + \binom{m-1}{i} = \binom{m}{i}$$

(iii) Снова утверждение, очевидно, верно при $m = 1$, а также для $r = 0$ и $r = m$, поскольку $\mathcal{R}(0, m)$ — это двоичный код с повторениями длины 2^m, и $\mathcal{R}(m, m) = \mathbb{F}_2^{2^m}$.

Предположим, что минимальный вес кода $\mathcal{R}(i, m-1)$ равен 2^{m-1-i} для всех $0 \le i < m$. Если $0 < r < m$, то, согласно (u/u+v) конструкции кода $\mathcal{R}(r, m)$ и упр. 33, получаем, что его минимальный вес равен

$$\min\left\{2 \cdot 2^{m-1-r}, 2^{m-1-(r-1)}\right\} = 2^{m-r}.$$

(iv) Заметим сначала, что $\mathcal{R}(m, m)^\perp = \{0\}$, поскольку $\mathcal{R}(m, m) = \mathbb{F}_2^{2^m}$.

Таким образом, если положить $\mathcal{R}(-1, m) = \{0\}$, то

$$\mathcal{R}(-1, m)^\perp = \mathcal{R}(m-(-1)-1, m) \text{ для всех } m \ge 0.$$

Непосредственно проверяется, что $\mathcal{R}(r, m)^\perp = \mathcal{R}(m-1-r, m)$ при $-1 \le r \le m \ge 1$.

Снова сделаем индукционное предположение: при $-1 \le i \le m-1$ выполняется равенство

$$\mathcal{R}(i, m-1)^\perp = \mathcal{R}((m-1)-i-1, m-1).$$

Также заметим, что для док-ва равенства

$$\mathcal{R}(r, m)^\perp = \mathcal{R}(m-1-r, m)$$

достаточно показать лишь включение

$$\mathcal{R}(m-1-r, m) \subseteq \mathcal{R}(r, m)^\perp,$$

поскольку $\dim \mathcal{R}(r, m) + \dim \mathcal{R}(m-1-r, m) = 2^m$ в силу (ii).

Пусть $x = (a, a+b) \in \mathcal{R}(m-1-r, m)$, где $a \in \mathcal{R}(m-1-r, m-1)$ и $b \in \mathcal{R}(m-1-r-1, m-1)$,

и пусть $y = (u, u+v) \in \mathcal{R}(r, m)$, где $u \in \mathcal{R}(r, m-1)$ и $v \in \mathcal{R}(r-1, m-1)$.

Тогда $x \cdot y = 2a \cdot u + a \cdot v + b \cdot u + b \cdot v = a \cdot v + b \cdot u + b \cdot v$. Каждое слагаемое в этой сумме равно 0 по следующим причинам:

- $a \in \mathcal{R}(m-1-r, m-1) = \mathcal{R}(r-1, m-1)^{\perp} \Rightarrow a \cdot v = 0$.
  $(m-1) - 1 - (r-1)$
- $b \in \mathcal{R}(m-2-r, m-1) = \mathcal{R}(r, m-1)^{\perp} \Rightarrow b \cdot u = 0$,
- в силу (i) $\mathcal{R}(r-1, m-1) \subset \mathcal{R}(r, m-1) \Rightarrow b \cdot v = 0$.

Таким образом, $\mathcal{R}(r, m)^{\perp} = \mathcal{R}(m-1-r, m)$. □

Сделаем несколько выводов из теоремы 1.10.1:

1) Поскольку $\mathcal{R}(0, m)$ — это код с повторениями длины 2^m, то $\mathcal{R}(m-1, m) = \mathcal{R}(0, m)^{\perp}$ — это код, состоящий из всех слов чётного веса пространства $\mathbb{F}_2^{2^m}$, что мы ранее видели на примерах $\mathcal{R}(1,2)$ и $\mathcal{R}(2,3)$.

2) Если m — нечётное и $r = \frac{m-1}{2}$, то из пп. (iii) и (iv) теоремы следует, что

   $\mathcal{R}(r, m) = \mathcal{R}\left(\frac{m-1}{2}, m\right)$ — самодуальный код с минимальным весом $2^{(m+1)/2}$, что мы также ранее видели на примере $\mathcal{R}(1, 3)$.

Упр. 62: Построим другую порождающую матрицу $G''(1,m)$ для кода $R(1,m)$. Положим

$$G''(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

и рекурсивно определим при $m \geq 2$

$$G'(1,m) = \left[\begin{array}{c|c} G''(1,m-1) & G''(1,m-1) \\ \hline 00\ldots0 & 11\ldots1 \end{array}\right],$$

где $G''(1,m)$ получается из $G'(1,m)$ перестановкой её последней строки на вторую позицию и сдвигом вниз всех строк со второй по предпоследнюю.

(a) Показать, что $G''(1,1)$ — порождающая матрица для кода $R(1,1)$.

(b) Построить матрицы $G'(1,2)$, $G''(1,2)$, $G'(1,3)$ и $G''(1,3)$.

(c) Что можно сказать о столбцах матриц, полученных из $G''(1,2)$ и $G''(1,3)$ удалением первой строчки и первого столбца?

(d) Показать по индукции, используя (a) и определение кода $R(1,m)$, что $G''(1,m)$ — порождающая матрица кода $R(1,m)$.

(e) Сформулируйте и докажите обобщение (c) на случай матриц, полученных из $G''(1,m)$ удалением первой строчки и первого столбца.

(f) Покажите, что код, порождённый матрицей, полученной из $G''(1,m)$ удалением первой строчки и первого столбца, представляет собой симплексный код S_m.

(g) Покажите, что код $R(m-2,m)$ является расширением двоичного кода Хэмминга $\hat{H}_m$.

Таким образом, упр. 62 показывает, что расширенные коды Хэмминга и их дуальные — суть коды Рида-Маллера.