Chapter 9

Constructions of Codes

Theorem 9.1. *Let d be odd. Then a binary (n, M, d)-code exists if and only if a binary $(n+1, M, d+1)$-code exists.*

Proof (i) *Adding an overall parity-check*

Let C be an (n, M, d)-code and C' be an $(n+1, M, d')$-code. If $x \in C$, $x = x_1 x_2 \cdots x_n$, then $x' = x_1 x_2 \cdots x_n x_{n+1} \in C'$, where

$$x_{n+1} = \begin{cases} 1 & \text{if } w(x) \text{ is odd,} \\ 0 & \text{if } w(x) \text{ is even.} \end{cases}$$

Hence, $w(x')$ is even.

From Sheet 6, Exercise 6,

$$d(x, y) = w(x) + w(y) - 2w(x \cap y).$$

Since $w(x')$ is even, for all x' in C', so is $d(x', y')$, for all $x', y' \in C'$. Now,

$$d(C') \geq d.$$

Since d is odd and $d(x', y')$ is even, so $d(C')$ is even. As $d \leq d(C') \leq d+1$, so $d(C') = d+1$.

(ii) *Shortening a code*

Suppose C' is an $(n+1, M, d+1)$-code with odd d. Let $x', y' \in C$ with $d(x', y') = d+1$. If $x'_i \neq y'_i$ delete the i-th coordinate from each word in C'. The result is an (n, M, d)-code C. □

Corollary 9.2. $\mathrm{Ham}(r, 2)'$ *is a* $[2^r, 2^r - 1 - r, 4]$*-code.*

Proof By Sheet 4, Exercise 8, the code is linear. □

Theorem 9.3. (Adding an overall parity-check) *An $[n, k]_q$-code C with parity check matrix H can be extended to an $[n+1, k]_q$-code C' with parity check matrix H', where*

$$H' = \begin{bmatrix} H & \mathbf{0}^{\perp} \\ \mathbf{1} & 1 \end{bmatrix}.$$

Proof $x \in C \Rightarrow x' \in C$ with $x' = x_1 \cdots x_{n+1}$ and $x_1 + \cdots + x_n + x_{n+1} = 0$. □

Example 9.4. The ternary [2,2] code C extends to a ternary $[3,2]$ code C' as follows:

$$\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 0 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{array}$$

$$H = [\quad] \qquad H' = [1\,1\,1] \qquad G = I_2$$

$C'^{\perp}$ is a $[3,1]$ code.

Theorem 9.5. (Shortening by taking a cross-section) *If C is a q-ary $[n,k,d]$-code with no coordinate position all zero and C_i is the code obtained by taking those codewords of C with 0 in the i-th position and deleting this zero, then C_i is a q-ary $[n-1,k-1,d']$-code with $d' \geq d$.*

Proof The codewords with 0 in the i-th position form a subspace of C of codimension 1, that is, of dimension $\dim C - 1$. □

Note 9.6. A parity-check matrix H_i of C_i is obtained by deleting the i-th column of a parity-check matrix H of C.

Example 9.7. (i) $C = \text{Ham}(3,2)$ is a $[7,4,3]$ code.

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

C	0	0	0	0	0	0	0	0
C'	1	0	0	0	0	1	1	1
	0	1	0	0	1	0	1	1
	0	0	1	0	1	1	0	1
	0	0	0	1	1	1	1	0
	1	1	0	0	1	1	0	0
	1	0	1	0	1	0	1	0
	1	0	0	1	1	0	0	1
	0	1	1	0	0	1	1	0
	0	1	0	1	0	1	0	1
	0	0	1	1	0	0	1	1
	1	1	1	0	0	0	0	1
	1	1	0	1	0	0	1	0
	1	0	1	1	0	1	0	0
	0	1	1	1	1	0	0	0
	1	1	1	1	1	1	1	1

$$C_1 = \begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{array} \qquad H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

C_1 is a $[6, 3, 3]$-code.

$$(C')_8 = \begin{matrix} 0&0&0&0&0&0&0\\ 0&0&0&1&1&1&1\\ 1&1&0&0&1&1&0\\ 1&0&1&0&1&0&1\\ 0&1&1&0&0&1&1\\ 1&1&0&1&0&0&1\\ 1&0&1&1&0&1&0\\ 0&1&1&1&1&0&0 \end{matrix} \quad [7,3,4] \text{ code,} \quad \mathrm{Ham}(3,2)^\perp$$

$$(C')_{87} = \begin{matrix} 0&0&0&0&0&0\\ 1&1&0&0&1&1\\ 1&0&1&1&0&1\\ 0&1&1&1&1&0 \end{matrix} \quad [6,2,4] \text{ code}$$

$$(C')_{870} = \begin{matrix} 0&0&0&0&0\\ 1&1&1&1&0 \end{matrix} \quad [5,1,4] \text{ code}$$

$$(C')_{8705} = \begin{matrix} 0&0&0&0\\ 1&1&1&1 \end{matrix} \quad [4,1,4] \text{ code}$$

(ii)

$$C_{11} = \begin{matrix} 0&0&0&0&0\\ 1&0&1&1&0\\ 0&1&1&1&1\\ 1&1&0&0&1 \end{matrix} \qquad H_{11} = \begin{bmatrix} 1&1&1&0&0\\ 1&1&0&1&0\\ 0&1&0&0&1 \end{bmatrix}$$

C_{11} is a $[5,2,3]$ code.

$$C_{111} = \begin{matrix} 0&0&0&0\\ 1&1&1&1 \end{matrix} \qquad H_{111} = \begin{bmatrix} 1&1&0&0\\ 1&0&1&0\\ 1&0&0&1 \end{bmatrix}$$

C_{111} is a $[4,1,4]$ code.

Theorem 2.3 gives a necessary condition for the existence of an $[n,k,d]_q$ code, with $d = 2e+1$ or $2e+2$; namely,

$$1 + (q-1)\binom{n}{1} + \cdots + (q-1)^e\binom{n}{e} \leq q^{n-k}.$$

Theorem 9.8. (Gilbert-Varshamov bound) *There exists an $[n,k,d']$-code over GF(q) with d' at least d providing*

$$1 + (q-1)\binom{n-1}{1} + \cdots + (q-1)^{d-2}\binom{n-1}{d-2} < q^{n-k}. \tag{9.1}$$

Proof It suffices to construct, by Theorem 9.19, an $r \times n$ matrix, where $r = n-k$, with no $d-1$ columns linearly dependent.

Choose the first column as any vector in $V(r,q) \setminus \{0\}$. Now proceed by induction. Suppose the first i columns have been chosen so that no $d-1$ are linearly dependent.

The sum of the numbers of distinct linear combinations, taken one at a time, two at a time, ..., $d-2$ at a time, is

$$N = (q-1)\binom{i}{1} + (q-1)^2\binom{i}{2} + \cdots + (q-1)^{d-2}\binom{i}{d-2}.$$

Provided $N < q^r - 1$, another column may be added so that no $d-1$ columns of the augmented $r \times (i+1)$ are linearly dependent. Now, $i = n-1$ gives the required result. □

Example 9.9. Does a $[7,4,3]_2$ code exist? In (9.1),

$$\text{LHS} = 1 + \binom{6}{1} = 7 < 8 = 2^{7-4} = \text{RHS}.$$

So such a code exists.