Definition 6.2

A Hamming code of length $n = (q^m - 1)/(q - 1)$ over GF(q) is defined to be the code given by an $m \times n$ parity check matrix **H**, the columns of which are all non-zero m-tuples over GF(q) with the first non-zero entry in each column equal to 1.

There are m columns in the parity check matrix **H** a suitable permutation of which form identity matrix of order m and it follows that the Hamming code given by **H** is a vector space of dimension $n - m$ over GF(q).

As examples we construct two Hamming codes over GF(3).

Examples 6.2

Case (i) – Hamming code of length 4 over GF(3)

As $4 = (3^2 - 1)/(3 - 1)$, the parity check matrix is a 2×4 matrix given by

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$$

Applying the permutation

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

to the columns of **H**, gives

$$\mathbf{H}_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

The corresponding generator matrix is then given by

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Applying the permutation $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$ gives the generator matrix corresponding to **H** as

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$$

All the code words of the (2, 4) ternary Hamming code are then given by:

Message word	Code word
0 0	0 0 0 0
0 1	2 1 0 1
0 2	1 2 0 2
1 0	1 1 1 0
1 1	0 2 1 1
1 2	2 0 1 2
2 0	2 2 2 0
2 1	1 0 2 1
2 2	0 1 2 2

The minimum distance of the code is 3.

Case (ii) – Hamming code of length 13 over GF(3)
As $13 = (3^3 - 1)/(3 - 1)$, the parity check matrix is a 3×13 matrix and is given by

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

Applying the permutation

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 13 & 12 & 1 & 2 & 11 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

to the columns of $\mathbf{H}$, gives

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 1 & 0 \\ 1 & 2 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 1 \end{pmatrix}$$

The corresponding generator matrix is

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 \end{pmatrix}$$

Applying the permutation $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$ gives

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

which is a generator matrix of the (3, 13) ternary Hamming code. Corresponding to message word $a_1a_2\text{---}a_{10} \in V(10, q)$ is code word

$$a_1 + 2a_2 + a_3 + 2a_4 + a_6 + 2a_7 + a_9 + 2a_{10}, a_1 + a_2 + a_5 + a_6 \\ + a_7 + 2a_8 + 2a_9 + 2a_{10}, a_1, a_2, a_3 + a_4 + a_5 + a_6 + a_7 + a_8 \\ + a_9 + a_{10}, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}$$

Exercise 6.3

1. Find a parity check matrix of a Hamming code of length 6 over GF(5).
2. Find a parity check matrix and the corresponding generator matrix of a Hamming code of length 5 over GF(4).
3. Find a parity check matrix of a Hamming code of length 21 over GF(4).
4. Find a parity check matrix and the corresponding generator matrix of a Hamming code of length
   (i) 8 over GF(7);
   (ii) 12 over GF(11);
   (iii) 14 over GF(13).
5. Find a parity check matrix of a ternary Hamming code of length 4.

While working with **non-binary codes**, the syndrome decoding procedure with a parity check matrix $\mathbf{H}$ needs to be modified as follows. Let $r = r_1\text{---}r_n$ be the word received and $\mathbf{s} = \mathbf{H}\mathbf{r}^t$ be the vector associated with its syndrome.

(i) If s equals a constant multiple of a unique column of $\mathbf{H}$, say the ith, i.e.

$$\mathbf{s} = \lambda\mathbf{H}_i \quad 0 \neq \lambda \in \mathrm{GF}(q)$$

where $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_n$ are the columns of $\mathbf{H}$, we assume that an error in transmission occurred in the ith position and take

$$c = r_i\text{---}r_{i-1}(r_i - \lambda)r_{i+1}\text{---}r_n$$

as the code word transmitted.

(ii) If s is not a multiple of any column of $\mathbf{H}$ then at least two errors occurred in transmission.

(iii) If $\mathbf{s}$ equals a multiple of $\mathbf{H}_i$ and also of $\mathbf{H}_j$ with $i \neq j$, there is the case of decoding failure.

Proceeding as in the binary case, we can prove the following proposition.

Proposition 6.1
Let $\mathscr{C}$ be a linear code over GF(q) with an $(n - m) \times n$ parity check matrix $\mathbf{H}$. The code is capable of correcting all single errors iff every two columns of $\mathbf{H}$ are linearly independent.

As the first non-zero entry in every column of the parity check matrix $\mathbf{H}$ of the Hamming code over GF(q), $q \neq 2$, is 1, it follows that no column of $\mathbf{H}$ is a scalar multiple of any other column. As such we have the following corollary.