If the error polynomial is

$$e(X) = X^i + X^j \quad i+1 \le j \le n-1$$

then $e(X) = X^i(1 + X^{j-i})$, $j - i < n$. Therefore, $h(X)$ being of exponent $e > n$ does not divide $X^i(1 + X^{j-i}) = e(X)$. Thus, $e(X)$ is not a code polynomial and, hence, this error pattern is detected.

If

$$e(X) = X^i + X^{i+1} + X^j \quad i+1 < j$$

or

$$e(X) = X^i + X^j + X^{j+1} \quad i < j$$

or

$$e(X) = X^j$$

then $1 + X \nmid e(X)$ (Proposition 2.4) and hence $g(X) \nmid e(X)$. Therefore, the three error patterns are detected. Finally, if the error polynomial is

$$e(X) = X^i + X^{i+1} + X^j + X^{j+1} = (1 + X)(X^i + X^j) \quad i < j < n$$

then $h(X) \nmid X^i + X^j$ (as seen above) and so $g(X) \nmid e(X)$. Thus, this error pattern is also detected.

Example 2.2

Consider the binary polynomial code of length 5 generated by the polynomial

$$g(X) = X^2 + 1 = (X + 1)(X + 1)$$

Observe that in this code, the following combinations of two single or double errors go undetected:

$$X, X^3 \quad 1, X^2 \quad X^2, X^4 \quad 1 + X, X^2 + X^3 \quad X + X^2, X^3 + X^4 \quad 1, X^4$$
$$1 + X, X^3 + X^4$$

However, any combination of one single and one double error is always detected. In fact, we can make the following general observation (in view of Proposition 2.4):

Remark

In a binary polynomial code with encoding polynomial $g(X) = (1 + X)h(X)$, any combination of one single and one double error is always detected.

Proposition 2.6

In a binary polynomial (m, n)-code with encoding polynomial $g(X)$, every code word is of even weight iff $1 + X \mid g(X)$.

Proof

If $g(X) = (1 + X)h(X)$, then $1 + X$ divides any code polynomial

$$b(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$$

and it follows from Proposition 2.4 that the corresponding code word $b=(b_0, b_1, \dots, b_{n-1})$ is of even weight.

Conversely, suppose that $b(X)$ is a code polynomial corresponding to a code word b of even weight. Then, on pairing adjacent terms, we see that $b(X)$ is a sum of finite number of sums of the form $X^i + X^j, i < j$. But

$$X^i + X^j = X^i(1 + X^{j-i}) = X^i(1 + X)(1 + X + \cdots + X^{j-i-1})$$

Therefore, $b(X)$ is divisible by $1 + X$. In particular, the code polynomial $Xg(X)$ corresponding to the message polynomial

$$a(X) = a_0 + a_1 X + \cdots + a_{m-1}X^{m-1} \quad a_i = 0 \forall i \neq 1, a_1 = 1$$

is also divisible by $1 + X$. But then it follows that $1 + X \mid g(X)$.

Exercise 2.1

1. Is the result of Proposition 2.4 true if we are working over a field of odd order? Justify.
2. Compute the minimum distance of the binary polynomial code of length 5 generated by $1 + X + X^2$.
3. Is the converse of Theorem 2.2 true? If the binary polynomial code of length n generated by $g(X)$ has minimum distance at least 3, is it always true that $g(X)$ divides no polynomial of the form $X^k - 1$ for $k < n$?
4. Find the minimum distance of the binary polynomial code of length 8 generated by the polynomials:
   (i) $1 + X + X^3$
   (ii) $1 + X^2 + X^3$
5. Compute all the code words of the polynomial code of length:
   (i) 3
   (ii) 4, generated by the polynomial $X^2 + 1$ over the field of 3 elements.
6. If F is a field of 3 elements and $g(X) \in F[X]$ divides no polynomial of the form $X^k - 1$ or $X^k + 1$ for $k < n$, prove that the polynomial code of length n generated by $g(X)$ over F has minimum distance at least 3.
7. Compute the exponent of the polynomial $a(X) \in \mathbb{B}[X]$ when
   (i) $a(X) = 1 + X + X^2$
   (ii) $a(X) = 1 + X + X^3$
   (iii) $a(X) = 1 + X^2 + X^3$
   (iv) $a(X) = X + X^3$
   (v) $a(X) = 1 + X^3$
   (vi) $a(X) = 1 + X^2 + X^4$

2.3 GENERATOR AND PARITY CHECK MATRICES – GENERAL CASE

Starting with an $m \times n$ matrix $\mathbf{G} = (\mathbf{I}_m \quad \mathbf{A})$, where $\mathbf{A}$ is $m \times (n - m)$ matrix, we defined a code $\mathscr{C} = \{\mathbf{aG} \mid a \in \mathbb{B}^m\}$ of length n and called $\mathbf{G}$ a generator matrix of

$\mathscr{C}$. Also we found that $\mathbf{H} = (\mathbf{A}^t \quad \mathbf{I}_{n-m})$ has the property that $\mathbf{Hb}^t = 0$ for every $\mathbf{b} \in \mathscr{C}$ and called it the parity check matrix of the code $\mathscr{C}$. However, it is not essential that we insist on the first m columns of $\mathbf{G}$ to form the identity matrix $\mathbf{I}_m$ or that the last $(n-m)$ columns of $\mathbf{H}$ to form the identity matrix $\mathbf{I}_{n-m}$. But, in that case, a great deal of information about the code defined by $\mathbf{G}$ will be lost. Also, the relation between the generator matrix $\mathbf{G}$ and parity check matrix $\mathbf{H}$ of the same code is not as clear as in the earlier case.

All codes considered here will be over $\mathbb{B}$, the field of two elements.

Recall that the rank of an $m \times n$ matrix $\mathbf{A}$ is the maximum number of linearly independent rows or the maximum number of linearly independent columns of the matrix $\mathbf{A}$.

Definition 2.5

Let $\mathscr{C}$ be an (m,n)-code. If there exists a $m \times n$ matrix $\mathbf{G}$ of rank m such that $\mathscr{C} = \{\mathbf{aG} \mid a \in \mathbb{B}^m\}$ then $\mathbf{G}$ is called a **generator matrix** of the code $\mathscr{C}$. Also then $\mathscr{C}$ is called a **matrix code** generated by $\mathbf{G}$.

Definition 2.6

Let $\mathscr{C}$ be an (m,n)-code. If there exists an $(n-m) \times n$ matrix $\mathbf{H}$ of rank $n-m$ such that $\mathbf{Hb}^t = 0$ for all $\mathbf{b} \in \mathscr{C}$, then $\mathbf{H}$ is called a parity check matrix of $\mathscr{C}$.

With this generalized definition of a matrix code, we have the following theorem.

Theorem 2.4

A polynomial code is a matrix code.

Proof

Let $\mathscr{C}$ be a polynomial (m,n)-code with encoding polynomial

$$g(X) = g_0 + g_1 X + \cdots + g_k X^k$$

Then $n = m + k$. Let $\mathbf{G}$ be the $m \times n$ matrix

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & 0 & \cdots & 0 \\ 0 & g_1 & \cdots & g_{k-1} & g_k & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_k \end{pmatrix}$$

in which the first row has initial entries $g_0, g_1, \ldots, g_k$ and the rest of the rows are obtained by giving a cyclic shift (anticlockwise) to the entries of the previous row until we arrive at a row in which the last $k+1$ entries are $g_0, g_1, \ldots, g_k$.

The determinant of the submatrix formed by taking the first m columns is $g_0^m \neq 0$ as $g_0 \neq 0$. Therefore, the rank of $\mathbf{G}$ is m. It is straightforward to check that the code word in the code generated by the matrix $\mathbf{G}$ corresponding to the message word

$$a = (a_0, a_1, \ldots, a_{m-1})$$

equals the code word corresponding to the message word a in the polynomial code generated by $g(X)$. Thus, the two codes are identical.

Example 2.3

(i) The generator matrix of the $(3, 6)$ polynomial code with encoding polynomial

$$g(X) = 1 + X + X^3$$

is

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

(ii) The generator matrix of the $(4, 7)$ polynomial code with encoding polynomial

$$g(X) = 1 + X^2 + X^3$$

is

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

(iii) The generator matrix of the $(4, 7)$ polynomial code with encoding polynomial

$$g(X) = 1 + X + X^3$$

is

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

(iv) Consider the $(4, 7)$ polynomial code with encoding polynomial

$$g(X) = 1 + X + X^3$$

so that its generator matrix is as seen in (iii) above. The code word corresponding to the message word

$$a = (a_0, a_1, a_2, a_3) \text{ is } (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2 + a_3, a_1 + a_3, a_2, a_3)$$

Let $\alpha_i, 0 \le i \le 6$, be elements from $\mathbb{B}$ such that

$$\alpha_0 a_0 + \alpha_1(a_0 + a_1) + \alpha_2(a_1 + a_2) + \alpha_3(a_0 + a_2 + a_3) + \alpha_4(a_1 + a_3) + \alpha_5 a_2 + \alpha_6 a_3 = 0$$

Then

$$a_0(\alpha_0 + \alpha_1 + \alpha_3) + a_1(\alpha_1 + \alpha_2 + \alpha_4) + a_2(\alpha_2 + \alpha_3 + \alpha_5) + a_3(\alpha_3 + \alpha_4 + \alpha_6) = 0$$

Since this holds $\forall a \in \mathbb{B}^4$, we have

$$\alpha_0 + \alpha_1 + \alpha_3 = 0 \quad \alpha_1 + \alpha_2 + \alpha_4 = 0$$

$$\alpha_2 + \alpha_3 + \alpha_5 = 0 \quad \alpha_3 + \alpha_4 + \alpha_6 = 0$$

We need to find out α_i which satisfy these equations. Suppose $\alpha_0 = 0$. Then $\alpha_1 = \alpha_3, \alpha_4 = \alpha_5$ and $\alpha_2 = \alpha_6$. We may take two sets of values of α's as

$$\alpha_0 = 0 \quad \alpha_1 = \alpha_3 = 1 \quad \alpha_4 = \alpha_5 = 0 \quad \alpha_2 = \alpha_6 = 1$$

and

$$\alpha_0 = 0 \quad \alpha_1 = \alpha_3 = 1 \quad \alpha_4 = \alpha_5 = 1 \quad \alpha_2 = \alpha_6 = 0$$

In order to avoid a column of zeros, let us next suppose $\alpha_0 = 1$. Then $\alpha_1 + \alpha_3 = 1$. Suppose that $\alpha_1 = 1, \alpha_3 = 0$. Then the above equations reduce to

$$1 + \alpha_2 + \alpha_4 = 0 \quad \alpha_2 + \alpha_5 = 0 \quad \alpha_4 + \alpha_6 = 0$$

If $\alpha_2 = 0$, then $\alpha_4 = 1 = \alpha_6$ and $\alpha_5 = 0$. Thus one set of values is

$$\alpha_0 = \alpha_1 = \alpha_4 = \alpha_6 = 1$$
$$\alpha_2 = \alpha_3 = \alpha_5 = 0$$

Therefore, a parity check matrix for this code is

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

Another parity check matrix of this code is

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

There are quite a few other parity check matrices of the code.

Exercises 2.2

1. Find two parity check matrices for the code of Example 2.3(i).
2. Find two parity check matrices of the (4, 7) polynomial code of Example 2.3(ii).

Consider the 3×6 matrix

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

Then we find that

$$(000)\mathbf{G} = 000000 = (111)\mathbf{G}$$
$$(001)\mathbf{G} = 101111 = (110)\mathbf{G}$$

and

$$(100)\mathbf{G} = 110100 = (011)\mathbf{G}$$

Thus, the map $a \to \mathbf{aG}$, $a \in \mathbb{B}^3$ is not one–one. This is so because the rows of $\mathbf{G}$ are linearly dependent or that the rank $(\mathbf{G}) < 3$. To avoid this eventuality and the unnecessary extra work involved, we insist on the $m \times n$ generator matrix to be of rank m.

We shall come to generator matrices again when we discuss linear codes.