

26 Polynomial codes

where $c_i = a_i + b_i \forall i$ and

$$d_j = a_0 b_j + a_1 b_{j-1} + \cdots + a_j b_0$$

it being understood that $a_i = 0$ for $i > m$ and $b_i = 0$ for $i > n$, becomes a commutative ring with identity. The elements

$$a(X) = a_0 + a_1 X + \cdots + a_m X^m$$

of $F[X]$ are called **polynomials** and if $a_m \neq 0$, we say that $a(X)$ is a polynomial of degree m (expressed as $\deg a(X) = m$). Since the product of non-zero elements in F is non-zero, it follows from the definition of multiplication in $F[X]$ that for non-zero $a(X), b(X)$ in $F[X]$, $a(X)b(X) \neq 0$ and that

$$\deg(a(X)b(X)) = \deg a(X) + \deg b(X)$$

(Recall that a commutative ring R in which $ab = 0$, $a, b \in R$, implies $a = 0$ or $b = 0$ is called an **integral domain**.) Observe that a polynomial

$$a(X) = a_0 + a_1 X + \cdots + a_m X^m = 0$$

iff $a_0 = a_1 = \cdots = a_m = 0$. Thus for any $m \geq 1$, the elements $1, X, X^2, \dots, X^m$ are linearly independent over F .

We could have defined a polynomial ring $R[X]$ in the variable X over any commutative ring R with identity but $R[X]$ is not, in general, an integral domain.

2.2 POLYNOMIAL CODES

Let F be any field and $F[X]$ be the polynomial ring in the variable X over F . Let n be a given positive integer. With a polynomial

$$a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

of degree at most $n - 1$, we can associate an ordered n -tuple or a word-ordered sequence

$$a = (a_0, a_1, \dots, a_{n-1})$$

of length n and conversely, with every word

$$a = (a_0, a_1, \dots, a_{n-1}) \quad a_i \in F$$

we can associate a polynomial

$$a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

of degree at most $n - 1$. Observe that for the polynomial

$$a_0 + a_1 X + \cdots + a_m X^m$$

of degree $m \leq n - 1$, we first rewrite $a(X)$, by introducing zero coefficients, as

$$a_0 + a_1 X + \cdots + a_m X^m + a_{m+1} X^{m+1} + \cdots + a_{n-1} X^{n-1}$$

with $a_i = 0$ for $m + 1 \leq i \leq n - 1$ and then associate with it the word

$$(a_0, a_1, \dots, a_m, a_{m+1}, \dots, a_{n-1})$$

of length n .

Let, as usual, $F^{(n)}$ denote the set of all words of length n with entries in F . Recall that $F^{(n)}$ is an n -dimensional vector space over F . Let $\mathcal{P}_n(X)$ denote the set of all polynomials in $F[X]$ which are of degree at most n . It is clear that the sum of two polynomials of degree at most n is again a polynomial of degree at most n and the multiplication of a polynomial of degree at most n with an element of F is again a polynomial of degree at most n . With these compositions (addition and scalar multiplication), $\mathcal{P}_n(X)$ becomes a vector space over F . The elements $1, X, \dots, X^n$ of $\mathcal{P}_n(X)$ are such that any element of $\mathcal{P}_n(X)$ is a linear combination of these elements over F and that these elements are linearly independent over F . Thus, $\mathcal{P}_n(X)$ is a vector space of dimension $n + 1$ over F . Two vector spaces over the same field and of equal dimensions are always isomorphic. We thus have the following theorem.

Theorem 2.1

The vector spaces $\mathcal{P}_{n-1}(X)$ and $F^{(n)}$ are isomorphic with the element

$$a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1}$$

corresponding to the element

$$a = (a_0, a_1, \dots, a_{n-1})$$

under this isomorphism.

Remark

In view of the above isomorphism, we use

$$a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1}$$

and

$$a = (a_0, a_1, \dots, a_{n-1}) \quad a_i \in F$$

interchangeably.

Definition 2.2

Let $g(X) = g_0 + g_1X + \dots + g_kX^k \in F[X]$ be a polynomial of degree at most k . The **polynomial code** with encoding (generating) polynomial $g(X)$ encodes each message word

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

of length m into the code word

$$b = (b_0, b_1, \dots, b_{m+k-1})$$

which corresponds to the code polynomial

$$b(X) = b_0 + b_1 X + \cdots + b_{m+k-1} X^{m+k-1} = a(X)g(X)$$

where

$$a(X) = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Remark

If $g_0 = 0$ in the encoding polynomial $g(X)$, then the first entry in every code word is 0 – thus this entry gives no useful information about the code. Similarly, if $g_k = 0$ in the encoding polynomial $g(X)$, then the last entry in every code word in the code generated by $g(X)$ is 0 and thus the last code word digit is wasted. To avoid this waste, we shall assume throughout that $g_0 \neq 0$ and $g_k \neq 0$.

Proposition 2.2

The polynomial code of length $n = m + k$ generated by the polynomial $g(X) = g_0 + g_1 X + \cdots + g_k X^k$ is a subspace of $F^{(n)}$.

Proof

Let

$$a = (a_0, a_1, \dots, a_{m-1}) \quad b = (b_0, b_1, \dots, b_{m-1})$$

be two message words. Let

$$\begin{aligned} a(X) &= a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} \\ b(X) &= b_0 + b_1 X + \cdots + b_{m-1} X^{m-1} \end{aligned}$$

be the corresponding message polynomials and $\alpha, \beta \in F$. Then the code polynomial corresponding to the message polynomial $\alpha a(X) + \beta b(X)$ is

$$[\alpha a(X) + \beta b(X)]g(X) = (\alpha a(X))g(X) + (\beta b(X))g(X) = \alpha(a(X)g(X)) + \beta(b(X)g(X))$$

■

Since a vector space is first a group under addition, a polynomial code is always a group code. For a group code, we have seen earlier (Proposition 1.2) that the minimum distance equals the minimum of the weights of non-zero code words. We thus have a similar proposition for polynomial codes.

Proposition 2.3

The minimum distance of a polynomial code with encoding polynomial $g(X)$ is the minimum weight $\text{wt}(a(X)g(X))$ of the non-zero code polynomials $a(X)g(X)$.

Of course, by the weight of a code polynomial, we mean the number of non-zero terms in the polynomial. For example:

$$\text{wt}(X + X^2 + X^3 + X^6) = 4 \quad \text{wt}(1 + X + X^3) = 3$$

The following simple observation will be useful later.

Proposition 2.4

A polynomial with coefficients in \mathbb{B} is divisible by $1 + X$ iff it has an even number of terms.

Proof

Let $f(X) = a_0 + a_1X + \dots + a_nX^n$, $a_i \in \mathbb{B}$ be a polynomial which is divisible by $1 + X$. Then there exists a polynomial $b(X) \in \mathbb{B}[X]$ such that

$$f(X) \equiv (1 + X)b(X)$$

Since this is an identity, taking $X = 1$ on both sides of this identity gives

$$a_0 + a_1 + \dots + a_n = 2b(1) = 0$$

in \mathbb{B} .

The field \mathbb{B} being of characteristic 2, this is possible only if the number of non-zero a_i 's is even.

Conversely, let

$$f(X) = a_0 + a_1X + \dots + a_nX^n \quad a_i \in \mathbb{B}$$

be a polynomial having an even number of non-zero terms; say

$$f(X) = X^{i_1} + X^{i_2} + \dots + X^{i_{2k}}$$

where $i_1 < i_2 < \dots < i_{2k}$. We rewrite

$$f(X) = (X^{i_1} + X^{i_2}) + (X^{i_3} + X^{i_4}) + \dots + (X^{i_{2k-1}} + X^{i_{2k}})$$

Since for $i < j$,

$$\begin{aligned} X^i + X^j &= X^i(1 + X^{j-i}) \\ &= X^i(1 + X)(1 + X + \dots + X^{j-i-1}) \end{aligned}$$

$1 + X | X^i + X^j$. Thus $1 + X$ divides every bracketed term in $f(X)$ and, therefore, $f(X)$ is divisible by $1 + X$.

Theorem 2.2

If $g(X) \in \mathbb{B}[X]$ divides no polynomial of the form $X^k - 1$ for $k < n$, then the binary polynomial code of length n generated by $g(X)$ has minimum distance at least 3.

Proof

Let

$$g(X) = g_0 + g_1X + \dots + g_rX^r$$

with $g_i \in \mathbb{B}$ and $g_0 \neq 0$, $g_r \neq 0$. Let $m = n - r$ so that every message polynomial is of degree at most $m - 1$. From the definition of polynomial codes, it follows that every code polynomial is divisible by $g(X)$. Also polynomial codes being

group codes, we have to prove that there is no non-zero code word of weight at most 2.

Suppose that the theorem fails. Then there exists a code polynomial $b(X)$ with at most two non-zero entries. Observe that $g(X) \nmid X^k - 1$ for any $k < n$ implies in particular that $g(X)$ is not a constant polynomial.

Case (i): $b(X) = X^i + X^j, i < j$

The code being of length n , we have $j < n$. Therefore, $0 < j - i < n$. But $g(X) | b(X)$ shows that $g(X) | X^i(1 + X^{j-i})$. Also $g_0 \neq 0$ implies that $X \nmid g(X)$. Strictly speaking, we can say that X and $g(X)$ are **relatively coprime**. Therefore $g(X) | 1 + X^{j-i}$ which contradicts the hypothesis.

Case (ii): $b(X) = X^i, i < n$

But, as seen above, $g(X) \nmid X^i$ and we have a contradiction. We have thus proved that there is no code polynomial with at most two non-zero terms and this establishes the theorem.

Examples 2.1

Case (i)

Consider first the binary polynomial code of length 6 generated by the polynomial $1 + X + X^3$. Then the message polynomials are of degree at most 2. For any message word (a_0, a_1, a_2) the corresponding message polynomial is

$$a(X) = a_0 + a_1 X + a_2 X^2$$

Therefore, the corresponding code polynomial is

$$\begin{aligned} b(X) &= (a_0 + a_1 X + a_2 X^2)(1 + X + X^3) \\ &= a_0 + (a_0 + a_1)X + (a_1 + a_2)X^2 + (a_0 + a_2)X^3 + a_1 X^4 + a_2 X^5 \end{aligned}$$

Thus, the code words of this code are

$$\begin{array}{ccccccccc} (a_0, a_1, a_2) & \longrightarrow & (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2, a_1, a_2) \\ \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{matrix} & \longrightarrow & \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{matrix} \end{array}$$

The minimum distance of this code is 3.

Observe that the encoding polynomial $1 + X + X^3$ does not divide

$$X^4 + 1 = (X + 1)^4 \quad \text{and} \quad X^5 + 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$$

and our computation of minimum distance confirms the result of Theorem 2.2.

Case (ii)

Next, we consider the binary polynomial code of length 7 generated by the polynomial $1 + X^2 + X^3$. The message words here are of length 4. The code words of this code are

$$\begin{aligned}
 (a_0, a_1, a_2, a_3) &\longrightarrow (a_0, a_1, a_0 + a_2, a_0 + a_1 + a_3, a_1 + a_2, a_2 + a_3, a_3) \\
 0 \ 0 \ 0 \ 0 &\longrightarrow 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \\
 0 \ 0 \ 0 \ 1 &\longrightarrow 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \\
 0 \ 0 \ 1 \ 0 &\longrightarrow 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \\
 0 \ 1 \ 0 \ 0 &\longrightarrow 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \\
 1 \ 0 \ 0 \ 0 &\longrightarrow 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \\
 0 \ 0 \ 1 \ 1 &\longrightarrow 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \\
 0 \ 1 \ 0 \ 1 &\longrightarrow 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \\
 1 \ 0 \ 0 \ 1 &\longrightarrow 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \\
 0 \ 1 \ 1 \ 0 &\longrightarrow 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \\
 1 \ 0 \ 1 \ 0 &\longrightarrow 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \\
 1 \ 1 \ 0 \ 0 &\longrightarrow 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \\
 0 \ 1 \ 1 \ 1 &\longrightarrow 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \\
 1 \ 0 \ 1 \ 1 &\longrightarrow 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \\
 1 \ 1 \ 0 \ 1 &\longrightarrow 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \\
 1 \ 1 \ 1 \ 0 &\longrightarrow 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \\
 1 \ 1 \ 1 \ 1 &\longrightarrow 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1
 \end{aligned}$$

Observe that the minimum distance of this code is 3.

Case (iii)

Finally, we consider the binary polynomial code of length 7, generated by the polynomial $1 + X + X^3$. The message words are again of length 4. The code words of this code are

$$\begin{aligned}
 (a_0, a_1, a_2, a_3) &\longrightarrow (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2 + a_3, a_1 + a_3, a_2, a_3) \\
 0 \ 0 \ 0 \ 0 &\longrightarrow 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \\
 0 \ 0 \ 0 \ 1 &\longrightarrow 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \\
 0 \ 0 \ 1 \ 0 &\longrightarrow 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \\
 0 \ 1 \ 0 \ 0 &\longrightarrow 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \\
 1 \ 0 \ 0 \ 0 &\longrightarrow 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \\
 0 \ 0 \ 1 \ 1 &\longrightarrow 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \\
 0 \ 1 \ 0 \ 1 &\longrightarrow 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \\
 1 \ 1 \ 1 \ 0 &\longrightarrow 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \quad (contd)
 \end{aligned}$$

$$\begin{array}{ccccccccc}
 1 & 0 & 0 & 1 & \longrightarrow & 1 & 1 & 0 & 0 \\
 0 & 1 & 1 & 0 & \longrightarrow & 0 & 1 & 0 & 1 \\
 1 & 0 & 1 & 0 & \longrightarrow & 1 & 1 & 1 & 1 \\
 1 & 1 & 0 & 0 & \longrightarrow & 1 & 0 & 1 & 1 \\
 0 & 1 & 1 & 1 & \longrightarrow & 0 & 1 & 0 & 0 \\
 1 & 0 & 1 & 1 & \longrightarrow & 1 & 1 & 1 & 1 \\
 1 & 1 & 0 & 1 & \longrightarrow & 1 & 0 & 0 & 0 \\
 1 & 1 & 1 & 1 & \longrightarrow & 1 & 0 & 1 & 1
 \end{array}$$

The minimum distance of this code is again 3. The encoding polynomial $1 + X + X^3$ does not divide $X^k + 1$ for $k < 7$ and the minimum distance is in conformity with Theorem 2.2.

In a group code, an error vector $\mathbf{e} = (e_0 \ e_1 \ \cdots \ e_{n-1})$ goes undetected iff it is a code word. (Note that, as before, the notation e refers to a series and \mathbf{e} refers to the vector formed using the elements in the series.) We thus have the following proposition.

Proposition 2.5

An error vector $\mathbf{e} = (e_0 \ e_1 \ \cdots \ e_{n-1})$ of a polynomial (m, n) code with generator $g(X)$ is undetected iff the associated error polynomial

$$e(X) = e_0 + e_1X + \cdots + e_{n-1}X^{n-1}$$

is a multiple of $g(X)$.

Definition 2.3

We say that the **exponent** of a polynomial $g(X) \in \mathbb{B}[X]$ is the least positive integer e such that $g(X) | X^e - 1$.

Definition 2.4

Two errors occurring at adjacent positions are called a **double error**.

Observe that $e(X) = X + X^3$ is not a double error, while $e(X) = X^2 + X^3$ or $e(X) = X + X^2$ are double errors.

Theorem 2.3

In a binary polynomial (m, n) -code, if the encoding polynomial

$$g(X) = (1 + X)h(X)$$

where $h(X)$ has exponent $e > n$, then any combination of two single or double errors will be detected.

Proof

Since the exponent of $h(X)$ is $e > n$, $h(X)$ is neither a constant polynomial nor a multiple of X .