2301532 : Coding Theory

Notes by

Assoc. Prof. Dr. Patanee Udomkavanich

October 30, 2006

http://pioneer.chula.ac.th/∼upattane

Chapter 1

Error detection, correction and decoding

1.1 Basic definitions and examples

Definition 1.1.1. Let $A = \{a_1, a_2, \ldots, a_q\}$ be a set of size q, which we refer to as a *code alphabet* and whose elements are called *code symbols* .

(*i*) A set A^n is defined to be $A^n = \{w_1 w_2 \ldots w_n | w_i \in A\}$, an element $w = w_1 w_2 \ldots w_n \in A^n$ is called a $q-ary\ word$ of length n over A. Equivalently, $w = w_1 w_2 \ldots w_n$ may also de regarded as the vector $(w_1, w_2, \ldots, w_n)$.

(*ii*) A $q-ary\ block\ code$ of length n over A is a nonempty set $\mathcal{C}$ of A^n.

(*iii*) An element of $\mathcal{C}$ is called a *codeword* in $\mathcal{C}$.

(*iv*) The number of codewords in $\mathcal{C}$, denoted by $|\mathcal{C}|$, is called the *size* of $\mathcal{C}$.

(*v*) The *(information) rate* of a code $\mathcal{C}$ of length n is defined to be $\frac{\log_q |\mathcal{C}|}{n}$.

(*vi*) A code of length n and size M is called an $(n, M) - code$.

Definition 1.1.2. Let $m, n \in \mathbb{N}$ be such that $m < n$, A be a code alphabet and $\mathcal{M}$ be a nonempty subset of A^m. Encoding and decoding functions are defined as follow :

1. an injective function $E : \mathcal{M} \to A^n$, called an *encoding function*,

2. a function $D : A^n \to \mathcal{M}$ such that $D(E(w)) = w$ for all $w \in M$, called a *decoding function*.

We call a set $\mathcal{M}$ and $w \in \mathcal{M}$ a *set of massages* and a *message word*, respectively. Hence $\mathcal{C} := E(\mathcal{M})$ is an $(n, |\mathcal{M}|)-$code.

Example 1.1.1 (Even parity-check code). We define

$$E : B^m \to B^{m+1} \text{ by } b_1 b_2 \dots b_m \mapsto b_1 b_2 \dots b_m b_{m+1}$$

where

$$b_{m+1} = \begin{cases} 0 \text{ if the number of } 1s' \text{ in } b_1 b_2 \dots b_m \text{ is even} \\ 1 \text{ if the number of } 1s' \text{ in } b_1 b_2 \dots b_m \text{ is odd} \end{cases}$$

and

$$D : B^{m+1} \to B^m$$

by

$$b_1 b_2 \dots b_m b_{m+1} \mapsto \begin{cases} b_1 b_2 \dots b_m & \text{if the number of } 1s' \text{ in } b_1 b_2 \dots b_{m+1} \text{ is even} \\ 00 \dots 0 & \text{if the number of } 1s' \text{ in } b_1 b_2 \dots b_{m+1} \text{ is odd} \end{cases}$$

Example 1.1.2 (Triple-repetition code). Triple-repetition code is a code such that an encoding function

$$E : B^m \to B^{3m}$$

is defined by

$$b_1 b_2 \dots b_m \mapsto b_1 b_2 \dots b_m b_1 b_2 \dots b_m b_1 b_2 \dots b_m$$

and a decoding function

$$D : B^{3m} \to B^m$$

is defined by

$$x_1 x_2 \dots x_m y_1 y_2 \dots y_m z_1 z_2 \dots z_m \mapsto b_1 b_2 \dots b_m$$

where

$$b_i \mapsto \begin{cases} 0 & \text{if 0 occurs in } x_iy_iz_i \text{ at least twice} \\ 1 & \text{if 1 occurs in } x_iy_iz_i \text{ at least twice} \end{cases}$$

Moreover, $n-$repetition code is defined similarly.

Definition 1.1.3. Let $\mathcal{C} \subseteq A^n$ be a code and c be a codeword in $\mathcal{C}$. A word $r \in A^n$ is called a *received word* (corresponding to c) if r is received (from sending c through the channel).

Definition 1.1.4. A *communication channel* consist of a finite *channel alphabet* $A = \{a_1, a_2, \ldots, a_q\}$ as well as a set of *forward channel properties* $\mathcal{P}(a_j \text{ received} \mid a_i \text{ sent})$, satisfying

$$\sum_{j=1}^{q} \mathcal{P}(a_j \text{ received} \mid a_i \text{ sent}) = 1$$

for all i. (Here, $\mathcal{P}(a_j \text{ received} \mid a_i \text{ sent})$ is the conditional probability that a_j is received, given that a_i is sent.)

Definition 1.1.5. A communication channel is said to be *memoryless* if the out come of any one transmission is independent of the out come of the previous transmissions; i.e., if $c = c_1c_2 \ldots c_n$ and $x = x_1x_2 \ldots x_n$ are word of length n, then

$$\mathcal{P}(x \text{ received} \mid c \text{ sent}) = \prod_{i=1}^{n} \mathcal{P}(x_i \text{ received} \mid c_i \text{ sent}).$$

Definition 1.1.6. A $q-$*ary symmetric channel* is a memoryless channel which has a channel alphabet of size q such that

(i) each symbol transmitted has the same probability p $(< 1/2)$ of being received in error,

(ii) if a symbol is received in error, then $q-1$ possible errors is equally likely.

In particular, the *binary symmetric channel (BSC)* is a memoryless channel which has the channel alphabet $\{0, 1\}$ and the channel probabilities

$$\mathcal{P}(1 \text{ received} \mid 0 \text{ sent}) = \mathcal{P}(0 \text{ received} \mid 1 \text{ sent}) = p$$

$$\mathcal{P}(0 \text{ received} \mid 0 \text{ sent}) = \mathcal{P}(1 \text{ received} \mid 1 \text{ sent}) = 1 - p$$

Thus, the probability of a bit error in a BSC is p. This is called the *crossover probability* of the BSC.

Suppose that codewords from a code $\mathcal{C}$ is being send over a communication channel. If a word x is received, x is called a *received word*. Then we can compute the forward channel probabilities

$$\mathcal{P}(x \text{ received} \mid c \text{ sent})$$

for all codewords $c \in \mathcal{C}$.

Definition 1.1.7 (The maximum likelihood decoding rule). If a word x is received, the *maximum likelihood decoding (MLD) rule* will conclude that c_x is the most likely codeword transmitted if c_x maximizes the forward channel probabilities; i.e.,

$$\mathcal{P}(x \text{ received} \mid c_x \text{ sent}) = \max_{c \in \mathcal{C}} \mathcal{P}(x \text{ received} \mid c \text{ sent})$$

There are two kinds of MLD :

(i) *Complete maximum likelihood decoding (CMLD)* : If more than one candidate appears, choose arbitrarily.

(ii) *Incomplete maximum likelihood decoding (IMLD)* : If more than one candidate appears, request a retransmission.

1.2 Hamming distance and Nearest neighbor decoding

Definition 1.2.1. Let A be a code alphabet and $u = u_1u_2 \dots u_n,\ v = v_1v_2 \dots v_n \in A^n$. The *(Hamming)distance* $d(u, v)$ of u and v is defined by

$$d(u, v) = |\{i \in \{1, 2, \dots, n\} | u_i \neq v_i\}|.$$

Equivalently, $d(u, v) = d(u_1, v_1) + d(u_2, v_2) + \cdots + d(u_n, v_n)$ where

$$d(u_i, v_i) = \begin{cases} 0 \text{ if } u_i = v_i \\ 1 \text{ if } u_i \neq v_i \end{cases}$$

Lemma 1.2.1. *Let $u, v, w \in A^n$. Then*

(i) $d(u, v) \geq 0$,

(ii) $d(u, v) = 0$ *if and only if* $u = v$,

(iii) $d(u, v) = d(v, u)$,

(iv) $d(u, v) \leq d(u, w) + d(w, v)$,

and hence (A^n, d) is a metric space.

Definition 1.2.2 (Nearest Neighbor Decoding). For a code $\mathcal{C}$, if a word $x \in A^n$ is received, the *Nearest Neighbor Decoding rule* decode x to the codeword in $\mathcal{C}$ closest to it, i.e, decode x to c_x if $d(r, c_x) = \min_{c \in \mathcal{C}}(x, c)$.
Complete Nearest Neighbor Decoding : If more than one candidate appears, choose arbitrarily.
Incomplete Nearest Neighbor Decoding : If more than one candidate appears, request a retransmission.

Theorem 1.2.2. *For a BSC with crossover probability $p < 1/2$, the maximum likelihood decoding rule is the Nearest Neighbor Decoding rule.*

1.3 Distance of a code

Definition 1.3.1. Let $\mathcal{C}$ be a code such that $|\mathcal{C}| \neq 1$. The *minimum distance* $d(\mathcal{C})$ of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{d(u, v) | u, v \in \mathcal{C}, u \neq v\}.$$

Definition 1.3.2. A code of length n, size M and minimum distance d is referred to as an $(n, M, d)-$code. The numbers n, M and d are called the *parameters* of the code.

Definition 1.3.3. Let t be a positive integer. A code $\mathcal{C}$ is *t-error detecting* if, whenever a codeword incurs at least one but at most t errors, the resulting word is not a codeword. A code $\mathcal{C}$ is *exactly t-error-detecting* if it is t-error-detecting but not $(t + 1)$-error-detecting.

Theorem 1.3.1. *A code $\mathcal{C}$ is t-error-detecting if and only if $d(\mathcal{C}) \geq t+1$. That is a code with minimum distance d is an exactly $(d-1)$-error-detecting code.*

Definition 1.3.4. Let t be a positive integer. A code $\mathcal{C}$ is *t-error correcting* if nearest neighbor decoding is able to correct t or fewer errors, assuming that the incomplete decoding rule is used. A code $\mathcal{C}$ is *exactly t-error-correcting* if it is t-error-correcting but not $(t+1)$-error-correcting.

Theorem 1.3.2. *A code $\mathcal{C}$ is t-error-correcting if and only if $d(\mathcal{C}) \geq 2t+1$. That is a code with minimum distance d is an exactly $\lfloor \frac{d-1}{2} \rfloor$-error-correcting code.*

1.4 Binary group codes

For a basic case, let $B = \{0, 1\}$. Then we define $B^n = \{b_1 b_2 \dots b_n | b_i \in B\}$ which is the set of *binary word* of length n. We define binary operations $+, \cdot : B \times B \to B$ as follows :

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Then $(B, +) \cong \mathbb{Z}_2$ and $(B^n, +) \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ copies}}$ is an abelian group. The additive inverse of each $b_1 b_2 \dots b_n \in B^n$ is itself.

Definition 1.4.1. Let $u = u_1 u_2 \dots u_n \in B^n$. The *weight* $\mathrm{w}(u)$ of u is defined by

$$\mathrm{w}(u) = |\{i \in \{1, 2, \dots, n\} | u_i \neq 0\}|$$

Lemma 1.4.1. *Let $u, v \in B^n$. Then $\mathrm{w}(u) = d(u, \boldsymbol{0})$ and $d(u, v) = \mathrm{w}(u + v)$.*

Definition 1.4.2. Let $\mathcal{C}$ be a code. The *minimum weight* $\mathrm{w}(\mathcal{C})$ of $\mathcal{C}$ is

$$\mathrm{w}(\mathcal{C}) = \min\{\mathrm{w}(u) | u \in \mathcal{C} \backslash \{\mathbf{0}\}\}.$$

When size of code is large, the minimum distance of code is hard to compute. Next, we introduce you a more efficiency code which is called a group code.

Definition 1.4.3. A code $\mathcal{C} \subseteq B^n$ is called a *(binary) group code* if for all $u, v \in \mathcal{C}$, $u + v \in \mathcal{C}$.

Lemma 1.4.2. *Let $\mathcal{C} \subseteq B^n$ be a code. $\mathcal{C}$ is a group code if and only if $\mathcal{C}$ is a subgroup of B^n , and hence $|\mathcal{C}| = 2^k$ for some $0 \leq k \leq n$.*

Definition 1.4.4. We call a group code $\mathcal{C} \subseteq B^n$ with $|\mathcal{C}| = 2^k$ an $[n, k]$ code . If an $[n, k]$ code $\mathcal{C}$ has the minimum distance $\mathcal{C}$, we call $\mathcal{C}$ an $[n, k, d]$ code.

Theorem 1.4.3. *Let $\mathcal{C} \subseteq B^n$ be a group code. Then $d(\mathcal{C}) = \mathrm{w}(\mathcal{C})$.*

Since an $[n, k]$ code $\mathcal{C}$ is a subgroup of B^n, for $u \in B^n$, $u + \mathcal{C} = \{u + v | v \in \mathcal{C}\}$ is called a *coset of $\mathcal{C}$ generated by u*. Clearly, the number of all (distinct) coset of $\mathcal{C}$ is $[B^n : \mathcal{C}] = \frac{2^n}{2^k} = 2^{n-k}$.

Definition 1.4.5. For a coset $u + \mathcal{C}$, we call $e \in u + \mathcal{C}$ a *coset leader* if $\mathrm{w}(e) \leq \mathrm{w}(u + \mathcal{C})$.

Note that a coset leader may not unique.

Coset Decoding: Let $\mathcal{C}$ be an $[n, k]$ code. If a word $r \in B^n$ is received and e is the coset leader for $r + \mathcal{C}$, then decode r as $r + e$.

Theorem 1.4.4. *Coset decoding is nearest neighbor decoding.*

Generator Matrix, Parity-check Matrix and Decoding.

For a convenience, we consider a word $w = w_1 w_2 \dots w_k \in B^k$ as a matrix $w = [\ w_1 \ \ w_2 \ \ \cdots \ \ w_k\ ]$. Let G be a binary $k \times n$ matrix such that $k < n$. Then $wG = [\ w_1 \ \ w_2 \ \ \cdots \ \ w_k\ ]G \in B^n$ for all $w \in B^k$.

Definition 1.4.6. Let G be a binary $k \times n$ matrix such that $k < n$ and the first k columns is an identity matrix I_k. Define $E : B^k \to B^n$ by $E(w) = wG$. Then $\mathcal{C} := \{wG | w \in B^k\}$ is called a *code generated by G* and G is called the *(standard) generator matrix* for $\mathcal{C}$.

From the above definition, we write $G = [I_k \ \ A]$ for some $(k \times (n - k)$ matrix A. Then for each message word $u \in B^k$, $uG = [uI_k \ uA] = [u \ uA]$ which is easy to retrieve.

Exercise 1.4.1. Verify the followings :

i) E is an encoding function (i.e., E is injective).

ii) $\mathcal{C}$ is a group code.

Definition 1.4.7. A binary $(n-k) \times n$ matrix H with $k < n$ is called the *(standard) parity-check matrix for a* $[n,k]$ *code* $\mathcal{C}$ if the last $n-k$ columns is an identity matrix I_{n-k} and $Hv^t = [\mathbf{0}]$ for all $v \in \mathcal{C}$.

Lemma 1.4.5. *If G and H are generator matrix and parity-check matrix for a group code $\mathcal{C}$,respectively, then each row of G is a codeword in $\mathcal{C}$ and hence $HG^t = [\boldsymbol{0}]$*

Theorem 1.4.6. *If $G = [I_k \;\; A]$ is a generator matrix for a $[n,k]$ code $\mathcal{C}$, then $H = [A^t \;\; I_{n-k}]$ is a parity check matrix for $\mathcal{C}$.*
Conversely, if $H = [B \;\; I_{n-k}]$ is a parity check for a $[n,k]$ code $\mathcal{C}$, then $G = [I_k \;\; B^t]$ is a generator matrix for $\mathcal{C}$.

Definition 1.4.8. Let H be the parity-check matrix for a $[n,k]$ code $\mathcal{C}$. For each $v \in B^n$, the syndrome $S(v)$ of v is defined by $S(v) = Hv^t$

Theorem 1.4.7. *Let H be the parity-check matrix for a $[n,k]$ code $\mathcal{C}$ and $u, v \in B^n$. Then*

i) $S(u+v) = S(u) + S(v)$,

ii) $S(v) = [\boldsymbol{0}]$ *if and only if* $v \in \mathcal{C}$,

iii) $S(u) = S(v)$ *if and only if u and v are in the same coset.*

Definition 1.4.9. A table which matches each coset leader e with its syndrome is called a *syndrome look-up table.*

Syndrome Decoding Let H be the parity-check matrix for a $[n,k]$ code $\mathcal{C}$. If $r \in B^n$ is received, compute $S(r)$ and find e (in a syndrome look-up table) such that $S(r) = S(e)$. Decode r as $r + e$.

Parity-heck Matrix Decoding

Let H be the parity-check matrix for a $[n, k]$ code $\mathcal{C}$. If $r \in B^n$ is received, compute $S(r) = Hr^t$.

1. If $S(r) = [\mathbf{0}]$, then $r \in \mathcal{C}$ and hence decode r as r.
2. If $S(r) \neq [\mathbf{0}]$ and $S(r)$ is column i of H, decode by changing its i^{th} bit.
3. If $S(r) \neq [\mathbf{0}]$ and $S(r)$ is not a column of H, request a retransmission.

Theorem 1.4.8. *Let H be a parity check of a $[n, k]$ code $\mathcal{C}$. $\mathcal{C}$ is a 1-error-correcting code if and only if any two columns of H are distinct and nonzero.*

Exercises

1. If u, v, w are binary vectors of the same length, prove that $d(u, v) = d(u - w, v - w)$.
2. Prove that, for binary vectors u and v of the same length, we have

$$\mathrm{w}(u + v) = \mathrm{w}(u) + \mathrm{w}(v) - 2\mathrm{w}(u \star v)$$

   where $u \star v$ is defined to have a 1 only in those positions where both u and v have a 1.
3. Let $\mathcal{C}$ be a binary group code. Show that either all codewords begin with 0 or half of them begin with 0.
4. Let $\mathcal{C}$ be a binary group code. Show that either all codewords have even weight or half of them have even weight.
5. Determine the minimum distance and correction capability of followings:

   i) $\mathcal{C} = \{0111000, 0010010, 1101101, 1001000, 1100010, 0011101, 0110111, 1000111\}$

   ii) $\mathcal{C} = \{00000000, 11101011, 01011110, 10110101\}$.

   iii) $\mathcal{C} = \{000000, 001110, 010101, 011011, 100011, 101101, 110110, 111000\}$.

6. Let

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

be the a generator matrix for $[7, 4]-$code $\mathcal{C}$.

   (a) Determine the minimum distance and correction capability of $\mathcal{C}$.

   (b) Use the syndrome decoding to decode the following received words : $0001001, 1010100, 1001001, 0100101, 1110100, 1111111$.

7. Construct the parity check H and generator matrix G (corresponding to H) of a 1-error-correcting $[7, 4]-$code.

8. Is it possible to find 16 binary vectors of length 7 so that $d(u, v) \geq 3$ for any two of them ? Justify your answer.

9. Is it possible to find 17 binary vectors of length 7 so that $d(u, v) \geq 3$ for any two of them ? Justify your answer.

10. Is there a $[7, 5, 3]$ code? Justify your answer.

11. If $\mathcal{C}$ is a group code whose minimum distance d, prove that any vector of weight $\lfloor \frac{d-1}{2} \rfloor$ or less is a unique coset leader.

Chapter 2

Finite fields

2.1 Definitions and Basic Properties

Definition 2.1.1. A *field* is nonempty set $\mathbb{F}$ together with two binary operations $+$ and $\cdot$ satisfying the following conditions :

(i) $a + b = b + a$ and $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{F}$.

(ii) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{F}$.

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{F}$.

(iv) There exists unique element in $\mathbb{F}$, denoted 0, such that $a + 0 = a$ for all $a \in \mathbb{F}$. The element 0 is called the *additive identity*.

(v) For each $a \in \mathbb{F}$, there is $b \in \mathbb{F}$ such that $a + b = 0$. This b is proved to be unique and denoted by $-a$, called the *additive inverse* of a.

(vi) There exists unique element in $\mathbb{F}\backslash\{0\}$, denoted 1, such that $a \cdot 1 = a$ for all $a \in \mathbb{F}\backslash\{0\}$. The element 1 is called the *multiplicative identity*.

(vii) For each $a \in \mathbb{F}\backslash\{0\}$, there is $c \in \mathbb{F}$ such that $a \cdot c = 1$. This c is proved to be unique and denoted by a^{-1}, called the *multiplicative inverse* of a.

Example 2.1.1. Let p be a prime. Then $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is a field under addition and multiplication modulo p.

Theorem 2.1.1. *If $\mathbb{F}$ is a field, then $a \cdot b = 0$ implies $a = 0$ or $b = 0$.*

Definition 2.1.2. Let $\mathbb{E}$ and $\mathbb{F}$ be fields. If $\mathbb{F} \subseteq \mathbb{E}$ and both operations $+$ and $\cdot$ of $\mathbb{E}$ when restricted to $\mathbb{F}$ and the operations $+$ and $\cdot$ of $\mathbb{F}$ are coincide, then $\mathbb{F}$ is said to be a *subfield* of $\mathbb{E}$ and $\mathbb{E}$ is called a *field extension* of $\mathbb{F}$.

Theorem 2.1.2. *Let $\mathbb{E}$ be a field and $\mathbb{F} \subseteq \mathbb{E}$. Then $\mathbb{F}$ is a subfield of $\mathbb{E}$ if and only if $\mathbb{F}$ satisfies the following conditions*

(i) $a - b \in \mathbb{F}$ for all $a, b \in \mathbb{F}$, and

(ii) $ab^{-1} \in \mathbb{F}$ for all $a, b \in \mathbb{F}$ with $b \neq 0$.

Definition 2.1.3. Let $\mathbb{F}$ be a field. The *characteristic* of $\mathbb{F}$ is the smallest positive (if any) integer n such that $n \cdot 1 = 0$ and it is defined to be 0 if there is no such n. (Here $n \cdot 1$ means $\underbrace{1 + 1 + \cdots + 1}_{n \text{ copies}}$.)

Theorem 2.1.3. *The characteristic of a field is either 0 or a prime number.*

Proposition 2.1.4. *Any field of characteristic p, where p is a prime, can be viewed as an extension field of $\mathbb{Z}_p$.*

Theorem 2.1.5. *A finite field contains p^n elements for some prime integer p and some positive integer n.*

Proposition 2.1.6. *In a field of characteristic p, $(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}$ for all x and y in $\mathbb{F}$ and $n \in \mathbb{N}$.*

2.2 Polynomials over a Field

Definition 2.2.1. For a field $\mathbb{F}$ and a indeterminate $x \notin \mathbb{F}$,
let $\mathbb{F}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \in \mathbb{N}_0, a_i \in \mathbb{F}\}$. Then $\mathbb{F}[x]$ satisfies conditions $(i) - (vi)$, in Definition 2.1.1, of a field under the addition and multiplication defined as follows : For $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$,

with $a_n \neq 0$, $b_m \neq 0$ and $n \leq m$,

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i)x^i$$

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

$\mathbb{F}[x]$ is called the *polynomial ring* over $\mathbb{F}$. An element $f(x)$ in $\mathbb{F}[x]$ is called a *polynomial* over $\mathbb{F}$. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$. a_n is called the leading coefficient of $f(x)$. The *degree of* $f(x)$, denoted $\deg f(x)$, is defined to be n and $\deg 0$ is $-\infty$. $f(x)$ is said to be *monic* if $a_n = 1$. $f(x)$ is a *non-constant polynomial* if $\deg f(x) \geq 1$. $f(x)$ is *reducible* if there exist $g(x)$ and $h(x)$ in $\mathbb{F}[x]$ such that

(i) $1 < \deg g(x), \deg h(x) < \deg f(x)$, and

(ii) $f(x) = g(x)h(x)$.

f(x) is irreducible if it is not reducible.

Theorem 2.2.1 (Division Algorithm). *Let $f(x) \in \mathbb{F}[x]$. If $\deg f(x) \geq 1$, then for any $g(x) \in \mathbb{F}[x]$, there exists a unique pair $(q(x), r(x))$ such that*

$$g(x) = f(x)q(x) + r(x)$$

where $\deg r(x) < \deg f(x)$.

Definition 2.2.2. Let $f(x), g(x), q(x)$ and $r(x)$ be as in Theorem 2.2.1. Then $g(x)$ is called the *quotient* and $r(x)$ is called the *remainder* of $g(x)$ divided by $f(x)$. $r(x)$ will be denoted by $[g(x)]_{mod\ f(x)}$. If $r(x) = 0$, $g(x)$ is said to be *divisible* by $f(x)$, denoted $f(x) \mid g(x)$, and $f(x)$ is called a *divisor* of $g(x)$.

Definition 2.2.3. Let $f(x) \in \mathbb{F}[x]$. $\alpha \in \mathbb{F}$ is said to be a *root* of $f(x)$ if $f(\alpha) = 0$.

Corollary 2.2.2. *Let $f(x) \in \mathbb{F}[x]$. Then $\alpha \in \mathbb{F}$ is a root of $f(x)$ if and only if $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{F}[x]$.*

Theorem 2.2.3. *A polynomial of degree n over a finite field has at most n (distinct) roots.*

Definition 2.2.4. Let $f(x)$ and $g(x)$ be nonzero polynomials over a field $\mathbb{F}$. The *greatest common divisor* of $f(x)$ and $g(x)$, denoted by $\gcd(f(x), g(x))$, is the monic polynomial of the highest degree which is a divisor of $f(x)$ and $g(x)$. $f(x)$ and $g(x)$ are said to be relative prime if $\gcd(f(x), g(x)) = 1$.

Theorem 2.2.4. *Let $f(x)$ and $g(x)$ be nonzero polynomials over a field $\mathbb{F}$. Then there exist $a(x)$ and $b(x)$ in $\mathbb{F}[x]$ such that*

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

2.3 Structure of Finite Fields

Theorem 2.3.1. *Let $f(x)$ be a polynomial of degree > 1 over a field $\mathbb{F}$.*

$$\mathbb{F}[x]/\langle f(x)\rangle = \{r(x) \in \mathbb{F}[x] \mid \deg r(x) < \deg f(x)\}.$$

Then $\mathbb{F}[x]/\langle f(x)\rangle$ is a ring under $\oplus$ and $\odot$ defined as follows :
For each $r_1(x), r_2(x) \in \mathbb{F}[x]/\langle f(x)\rangle$

$$r_1(x) \oplus r_2(x) = [r_1(x) + r_2(x)]_{mod\ f(x)}$$
$$r_1(x) \odot r_2(x) = [r_1(x) \cdot r_2(x)]_{mod\ f(x)}.$$

(i.e., $(\mathbb{F}[x]/\langle f(x)\rangle, \oplus, \odot)$ satisfies $(i) - (v)$ of Definition 2.1.1)

Theorem 2.3.2. *Let $f(x)$ be a nonconstant polynomial over a field $\mathbb{F}$. Then $\mathbb{F}[x]/\langle f(x)\rangle$ is a field if and only if $f(x)$ is irreducible.*

Theorem 2.3.3. *Let $\mathbb{F} \subseteq \mathbb{E}$ be finite fields and $\alpha \in \mathbb{E}/\mathbb{F}$. If $f(x)$ an irreducible polynomial of degree n. Let $\alpha \in \mathbb{E}/\mathbb{F}$ be a root of f(x). Then $\mathbb{F}[x]/\langle f(x)\rangle$ is a field of $|\mathbb{F}|^n$ elements. Moreover, $\mathbb{F}[x]/\langle f(x)\rangle$ can be viewed as $\mathbb{F}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{F}$ and $f(\alpha) = 0\}$. In this case, it is the smallest field containing $\mathbb{F}$ and α.*

Theorem 2.3.4. *Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}_{[}x]$ be irreducible. Then there is an extension filed $\mathbb{E}$ of $\mathbb{F}$ in which $f(x)$ has a root.*

Corollary 2.3.5. *Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be irreducible. Then there is an extension filed $\mathbb{E}$ of $\mathbb{F}$ containing all roots of $f(x)$.*

Theorem 2.3.6. *Let $f(x) \in \mathbb{F}[x]$ and α be a root of $f(x)$ in an extension field $\mathbb{E}$ of $\mathbb{F}$. Then*

(i) Then exists a unique monic irreducible polynomial, denoted $m_{\mathbb{F}}(\alpha)$, which has α as a root.

(ii) $g(x) \in \mathbb{F}[x]$ has α as a root if and only if $m_{\mathbb{F}}(x)$ divides $g(x)$ in $\mathbb{F}[x]$.

Definition 2.3.1. The polynomial $m_{\mathbb{F}}(\alpha)$ in Theorem 2.3.6 is called the *minimal polynomial* of α over $\mathbb{F}$.

Lemma 2.3.7. *In a field of q elements, $a^q = a$ for all $a \in \mathbb{F}$.*

Theorem 2.3.8. *Let $\mathbb{F} \subseteq \mathbb{E}$ be fields with $|\mathbb{F}| = q$ and $\alpha \in \mathbb{E}$. Then $\alpha \in \mathbb{F}$ if and only if $\alpha^q = \alpha$.*

Definition 2.3.2. The *order* of nonzero element a of a finite field $\mathbb{F}$, denoted $o(a)$ is the smallest integer n such that $a^n = 1$.

Theorem 2.3.9. *For each positive integer n and prime p, there is a unique field of order $q = p^n$, denoted $\mathbb{F}_q$.*

Theorem 2.3.10. *$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if m divides n.*

Lemma 2.3.11. *Let $\mathbb{F}$ be a finite field of q elements. Then*

(i) $o(a)$ divides $q - 1$ for every nonzero element a of $\mathbb{F}$,

(ii) if m is the least common multiple of the orders of all elements in $\mathbb{F}^*$, then there is $a \in \mathbb{F}$ such that $o(a) = m$.

Definition 2.3.3. Let $\mathbb{F}$ be a field. An element $\alpha \in \mathbb{F}$ is *primitive* if every nonzero element of $\mathbb{F}$ is a power of α.

Theorem 2.3.12. *Let $\mathbb{F}$ be the finite field of q elements. Then*

(i) A nonzero element a of $\mathbb{F}$ is a primitive element iff order of a is $q-1$.

(ii) $\mathbb{F}$ has at least one primitive element.

Theorem 2.3.13. *For each prime p and positive integer n, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

Corollary 2.3.14. *If α is a primitive element of the field $\mathbb{F}_{p^n}$, then*

$$\deg m_{\mathbb{Z}_p}(\alpha) = n.$$

Example 2.3.1. Let $f(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$. We first show that $f(x)$ is irreducible over $\mathbb{F}_2$. Suppose $f(x)$ is reducible. Then either x or $1 - x$ must be the factor of $f(x)$. Thus 0 or 1 must be a root of $f(x)$ which is impossible. Hence $f(x)$ is irreducible. Let α be a root of $f(x)$. Then $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle f(x)\rangle = \mathbb{F}_2[\alpha]$. Notice that α is also a primitive element of $\mathbb{F}_8$ because $o(\alpha) = 7$ ($\because o(\alpha) \mid 7$). Elements in $\mathbb{F}_8$ can be represented in three forms (in Table 2.1) :

I	II	III
0	0	000
1	α^7	001
α	α	010
$\alpha + 1$	α^3	011
α^2	α^2	100
$\alpha^2 + 1$	α^6	101
$\alpha^2 + \alpha$	α^4	110
$\alpha^2 + \alpha + 1$	α^5	111

Table 2.1: $\mathbb{F}_8$ where α is a root of the irreducible polynomial $f(x) = x^3 + x + 1$.

The first form is suitable for adding and the second for multiplying and finding multiplicative inverses. Thus we switch from one to another whenever it is convenient. Practically, to apply these operations, we use Zech's table, constructed as follows : Let α be a primitive element of $\mathbb{F}_q$. For each $0 \leq i \leq q-2$, let $z(i)$ be such that $1 + \alpha^i = \alpha^{z(i)}$ and set $\alpha^\infty = 0$. Then for any α^i and α^j with $1 \leq i \leq j \leq q-2$ in $\mathbb{F}$ we obtain,

$$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i}) = \alpha^{i+z(j-i)} \text{ and}$$
$$\alpha^i \cdot \alpha^j = \alpha^{i+j},$$

where the resulting power of α is computed modulo $q - 1$.

i	1	2	3	4	5	6
$z(i)$	3	6	1	5	4	2

Table 2.2: Zech's log table for $\mathbb{F}_8$.

Notice that $1 + \alpha + \alpha^3 = 0$. Thus

$$\begin{aligned} 1 + \alpha^3 &= \alpha \\ \alpha^7 + \alpha^3 &= 1 + \alpha^3 = \alpha \\ \alpha^3(\alpha^4 + 1) &= \alpha \\ \alpha^4 + 1 &= \alpha^{-2} = \alpha^5 \text{ so } 1 + \alpha^5 = \alpha^4. \end{aligned}$$

Since $1 + \alpha^2 = \alpha^6$, $1 + \alpha^6 = \alpha^2$.

Example 2.3.2. Let α be a root of the irreducible polynomial $f(x) = x^4 + x^3 + 1$ over $\mathbb{F}_2$. Then elements of $\mathbb{F}_{16}$ are displayed as follows :

I							II	III
						0	0	0000
						1	1	0001
				α			α	0010
		α^2					α^2	0100
α^3							α^3	1000
α^3					+	1	α^4	1001
α^3			+	α	+	1	α^5	1011
α^3	+	α^2	+	α	+	1	α^6	1111
		α^2	+	α	+	1	α^7	0111
α^3	+	α^2	+	α			α^8	1110
		α^2			+	1	α^9	0101
α^3			+	α			α^{10}	1010
α^3	+	α^2			+	1	α^{11}	1101
				α	+	1	α^{12}	0011
		α^2	+	α			α^{13}	0110
α^3	+	α^2					α^{14}	1100

Table 2.3: $\mathbb{F}_{16}$ where α is a root of the irreducible polynomial $f(x) = x^4 + x^3 + 1$.

2.4 Minimal polynomials and factoring $x^n - 1$

Theorem 2.4.1. *If α is root of $f(x)$, then α^{-1} is a root of $x^m f(x^{-1})$, the reciprocal polynomial of $f(x)$ where $\deg f(x) = m$. Moreover, α is primitive if and only if α^{-1} is primitive.*

Theorem 2.4.2. *Let $f(x) \in \mathbb{F}_q[x]$ and E be a field of characteristic p containing a root α of $f(x)$. Let r be the smallest positive integer such that $p^{r+1} \equiv 1 (\mathrm{mod}\ n)$ where n is the order of α. Then $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^r}$ are all distinct root of $f(x)$.*

Definition 2.4.1. Let n and q be positive integers with $\gcd(n, q) = 1$. For each $0 \leq i \leq n$, define the *cyclotomic coset of q modulo n containing i* by

$$C_i = \{[iq^i] \mod n \mid i \in \mathbb{N}_0\}.$$

A subset $i_1, i_2, \ldots, i_k$ of $\mathbb{Z}_n$ is called a *compete set of representatives of cytoclomic cosets of q modulo n* if $C_{i_1}, C_{i_2}, \ldots, C_{i_k}$ are all distinct and $\bigcup_{j=1}^{k} C_{i_j} = \mathbb{Z}_n$.

Remark 2.4.1.

1. The cyclotomic cosets partition $\mathbb{Z}_n$.
2. Each cyclotomic cosets C_i of p modulo $p^n - 1$ contains at most n element ($\because p^n \equiv 1 \mod (p^n - 1)$) and the equality holds when $\gcd(i, p^n - 1) = 1$.

Theorem 2.4.3. *Let α be a primitive element of $\mathbb{F}_{p^n}$. Then*

$$m_{\mathbb{Z}_p}(\alpha^i) = \prod_{j \in C_i} (x - \alpha^j)$$

where C_i is the cyclotomic coset of p modulo $p^m - 1$ containing i.

Remark 2.4.2. It follows directly from Theorem 2.4.3 that, for a primitive element ω,

$$m_{\mathbb{F}_q}(\omega^i) = m_{\mathbb{F}_q}(\omega^j) \Leftrightarrow C_i = C_j.$$

Theorem 2.4.4. *Let $n \in \mathbb{N}$ be such that $\gcd(n, p) = 1$. Let $\{s_1, s_2, \ldots, s_k\}$ be a set of representative of cyclotomic cosets of q modulo n. Let $m \in \mathbb{N}$ satisfying $n \mid (p^m - 1)$ and α a primitive element of $\mathbb{F}_{p^m}$. Then*

$$x^n - 1 = \prod_{i=1}^{k} m_{\mathbb{Z}_p}(\alpha^{\frac{p^m - 1}{n} s_i}).$$

Exercises

1. Determine the irreducibility of the following polynomial :

   (a) $1 + x + x^2 + x^3 + x^4$, $1 + x + x^4$ and $1 + x + x^3 + x^5$ over $\mathbb{F}_2$.

   (b) $1 + x^2$, $2 + x + x^2$ and $1 + 2x + x^4$ over $\mathbb{F}_3$.

2. Construct both the addition and multiplication tables for $\mathbb{F}_3[x]/ < x^2 + 2 >$

3. Find the order of elements $\alpha, \alpha^3, \alpha + 1$ and $\alpha^3 + 1$ in $\mathbb{F}_{16}$ where α is a root of $x^4 + x + 1$.

4. Let α be a primitive element of $\mathbb{F}_q$. Show that α^i is also a primitive element if and only if $\gcd(i, q - 1) = 1$.

5. Determine the number of primitive elements in the following fields : $\mathbb{F}_9, \mathbb{F}_{19}$, $\mathbb{F}_{25}, \mathbb{F}_{27}$ and $\mathbb{F}_{32}$.

6. Construct the field $\mathbb{F}_9$, and determine addition and multiplication tables.

7. Find a primitive element and construct a Zech's log table for the fields $\mathbb{F}_{5^2}, \mathbb{F}_{3^3}$ and $\mathbb{F}_{2^5}$.

8. Factor the followings :

   (a) $x^7 - 1$ over $\mathbb{F}_3$.

   (b) $x^{10} - 1$ over $\mathbb{F}_3$.

   (c) $x^9 - 1$ over $\mathbb{F}_2$.

Chapter 3

Linear codes

3.1 Vector spaces over finite fields

Definition 3.1.1. Let $\mathbb{F}_q$ be the finite field of order q. A nonempty set V, together with some (vector) addition $+$ and scalar multiplication by elements of $\mathbb{F}_q$, is a *vector space over* $\mathbb{F}_q$ if it satisfy the following conditions :

(i) $(V, +)$ is an abelian group,

(ii) $\lambda v \in V$ for all $v \in V$ and $\lambda \in \mathbb{F}_q$,

(iii) $\lambda(u + v) = \lambda u + \lambda v$ for all $u, v \in V$ and $\lambda \in \mathbb{F}_q$,

(iv) $(\lambda + \alpha)v = \lambda v + \alpha v$ for all $v \in V$ and $\lambda, \alpha \in \mathbb{F}_q$,

(v) $(\lambda\alpha)v = \lambda(\alpha v)$ for all $v \in V$ and $\lambda, \alpha \in \mathbb{F}_q$,

(vi) If 1 is the multiplicative identity of $\mathbb{F}_q$, $1v = v$ for all $v \in V$.

Example 3.1.1. For the field $\mathbb{F}_q$, let $\mathbb{F}_q^n = \{(v_1, v_2, \ldots, v_n) \mid v_i \in \mathbb{F}\}$ the set of vector of length n. Then $\mathbb{F}_q^n$ satisfies conditions in Definition 3.1.1, of a vector space under the (vector) addition and scalar multiplication defined as follows : For $v = (v_1, v_2, \ldots, v_n)$ and $u = (u_1, u_2, \ldots, u_n)$in $\mathbb{F}_q^n$ and $\lambda \in \mathbb{F}_q$,

$$v + u = (v_1 + u_1, v_2 + u_2, \ldots, v_n + u_n)$$
$$\lambda v = (\lambda v_1, \lambda v_2, \ldots, \lambda v_n).$$

Remark 3.1.1. When there is no ambiguity, it is sometime convenient to write a vector $(v_1, v_2, \ldots, v_n)$ simply as $v_1 v_2 \ldots v_n$.

Definition 3.1.2. A nonempty subset $\mathcal{C}$ of a vector space V is a *subspace* of V if it is itself a vector space with the same (vector) addition and scalar multiplication as V.

Proposition 3.1.1. *A nonempty subset $\mathcal{C}$ of a vector space V is a subspace of V over $\mathbb{F}_q$ if and only if $\lambda u + \beta v \in V$ for all $u, v \in \mathcal{C}$ and $\lambda, \beta \in \mathbb{F}_q$.*

Definition 3.1.3. Let V be a vector space over $\mathbb{F}_q$. A *linear combination*of $v_1, v_2, \ldots, v_r \in V$ is a vector of the form $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$, where $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$ are some scalars.

Definition 3.1.4. Let V be a vector space over $\mathbb{F}_q$. A set of vector $\{v_1, v_2, \ldots, v_r\}$ in V is *linearly independent* if

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0 \Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_r = 0$$

The set is *linearly dependent* if it is not linearly independent; i.e., if there are $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$, not all zero, such that $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$.

Definition 3.1.5. Let V be a vector space over $\mathbb{F}_q$ and let $S = \{s_1, s_2, \ldots, s_k\}$ be a nonempty subset of V. The *(linear) span* of S is defined as

$$< S >= \{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k \mid \lambda_i \in \mathbb{F}_q\}.$$

If $S = \emptyset$, we define $< S >= \{0\}$. It is easy to verify that $< S >$ is a subspace of V; i.e., $< S >= \mathcal{C}$ for some sub space $\mathcal{C}$ of V. In this case we say that $\mathcal{C}$ is *spanned (or generated)* by S or S span $\mathcal{C}$.

Definition 3.1.6. Let V be a vector space over $\mathbb{F}_q$. A nonempty subset

$$B = \{s_1, s_2, \ldots, s_k\}$$

of V is called a *basis* for V if $< B >= V$ and B is linearly independent.

Definition 3.1.7. Let V be a vector space over $\mathbb{F}_q$ and B a basis for V. The *dimension* of V over $\mathbb{F}_q$, denoted $\dim V$, is defined to be the cardinality of B. and B is linearly independent.

Definition 3.1.8. Let $u = u_1u_2 \dots u_n$ and $v = v_1v_2 \dots v_n$ be vectors in $\mathbb{F}_q^n$.

(i) The *scalar product* of u and v is defined as

$$u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n \in \mathbb{F}_q.$$

(ii) The two vectors u and v are said to be *orthogonal* if $u \cdot v = 0$.

(iii) Let S be a nonempty subset of $\mathbb{F}_q^n$. The *orthogonal complement* $S^\perp$ of S is defined to be

$$S^\perp = \{v \in \mathbb{F}_q^n \mid v \cdot s = 0 \text{ for all } s \in S\}.$$

If $S = \emptyset$, then we define $S^\perp = \mathbb{F}_q^n$.

Remark 3.1.2. It is easy to verify that :

(i) The above $\cdot$ is an *inner product* on $\mathbb{F}_q^n$.

(ii) $< S >$ is always a subspace of $\mathbb{F}_q^n$.

(iii) $< S >^\perp = S^\perp$.

3.2 Linear codes

Definition 3.2.1. A *linear code* $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$.

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. We denote by $[n, k]$ the linear code $\mathcal{C}$ of length n whose dimension is k, and we call an $[n, k]$ code whose minimum distance is d an $[n, k, d]$ code. To specify the field, we may write $[n, k, d]_q$ for an $[n, k, d]$ code over $\mathbb{F}_q$.

Remark 3.2.1. A linear code over $\mathbb{F}_2$ is the same as a binary group code.

Definition 3.2.2. The *dual code* of a linear code $\mathcal{C}$ is $\mathcal{C}^{\perp}$, the orthogonal complement of the subspace $\mathcal{C}$.

Theorem 3.2.1. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$. Then ;*

(i) $|\mathcal{C}| = q^{\dim \mathcal{C}}$*; i.e.,* $\dim \mathcal{C} = \log_q |\mathcal{C}|$.

(ii) $\mathcal{C}^{\perp}$ *is a liner code and* $n = \dim \mathcal{C} + \dim \mathcal{C}^{\perp}$

(iii) $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

The followings are definitions and properties of linear codes which are directly extended from binary group code (Section 1.4)

Definition 3.2.3. Let $v, u \in \mathbb{F}_q^n$. The Hamming weight of u, denote $\mathrm{w}(u)$, is defined to be the number of nonzero coordinates in u; i.e.,

$$\mathrm{w}(u) = d(u, o).$$

Equivalently,

$$\mathrm{w}(u) = \mathrm{w}(u_1) + \mathrm{w}(u_2) + \cdots + \mathrm{w}(u_n),$$

where $u = u_1 u_2 \dots u_n$ and

$$\mathrm{w}(u_i) = \begin{cases} 0 \text{ if } u_i = 0 \\ 1 \text{ if } u_i \neq 0. \end{cases}$$

Lemma 3.2.2. *If $u, v \in \mathbb{F}_q^n$, then $d(u, v) = \mathrm{w}(u - v)$.*

Definition 3.2.4. Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. The minimum weight of $\mathcal{C}$, denoted $\mathrm{w}(\mathcal{C})$, is the smallest of the weights of nonzero codewords in $\mathcal{C}$.

Theorem 3.2.3. *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. Then $d(\mathcal{C}) = \mathrm{w}(\mathcal{C})$.*

3.3 Generator matrix and parity-check matrix

Now, we give the definitions of generator matrix and parity-check matrix of a linear code (which are little distinct from Section 1.4.)

Definition 3.3.1.

(i) A *generator matrix* for a linear code $\mathcal{C}$ is a matrix G whose rows form a basis for $\mathcal{C}$.

(ii) A *parity-check matrix* H for a linear code $\mathcal{C}$ is a generator matrix for the dual code $\mathcal{C}^{\perp}$.

Remark 3.3.1.

(i) If $\mathcal{C}$ is an $[n, k]$ code, then a generator matrix G for $\mathcal{C}$ must be a $k \times n$ matrix and a parity-check matrix H for $\mathcal{C}$ must be an $(n-k) \times n$ matrix.

(ii) Rows of G are linearly independent and rows of H are linearly independent.

Definition 3.3.2.

(i) A generator matrix of the form $[I_k \mid A]$ is said to be the *standard form.*

(ii) A parity-check matrix of the form $[B \mid I_{n-k}]$ is said to be the *standard form.*

Theorem 3.3.1. *Let $\mathcal{C}$ be an $[n, k]$ code over $\mathbb{F}_q$, with generator matrix G, and H a $q-$ary $(n-k) \times n$ matrix. Then H is a parity-check matrix for $\mathcal{C}$ if and only if the rows of H are linearly independent and $HG^T = 0$.*

Theorem 3.3.2. *Let $\mathcal{C}$ be an $[n, k]$ code over $\mathbb{F}_q$, with parity-check matrix H, and G a $q-$ary $k \times n$ matrix. Then G is a generator matrix for $\mathcal{C}$ if and only if the rows of G are linearly independent and $GH^T = 0$.*

Theorem 3.3.3. *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$, with parity-check matrix H. Then :*

(i) $\mathcal{C}$ has the minimum distance at least d if and only if any $d-1$ columns of H are linearly independent.

(ii) $\mathcal{C}$ has the minimum distance at most d if and only if H has d columns that are linearly dependent.

(*iii*) $\mathcal{C}$ *has the minimum distance* d *if and only if any* $d-1$ *columns of* H *are linearly independent and* H *has* d *columns that are linearly dependent.*

Theorem 3.3.4. *If* $G = [I_k \mid A]$ *is the standard form generator matrix for an* $[n, k]$ *code* $\mathcal{C}$*, then a parity-check matrix for* $\mathcal{C}$ *is* $H = [-A^T \mid I_{n-k}]$*, and conversely.*

Definition 3.3.3. Two codes of length n over $\mathbb{F}_q$ are *equivalent* if one can be obtained from the other by a combinations of the following operations :

1. permutation of the n digits of the codewords.
2. multiplication of the symbols appearing in the fixed position by nonzero scalar.

Theorem 3.3.5. *Any linear code* $\mathcal{C}$ *is equivalent to a linear code* $\mathcal{C}'$ *with a generator matrix in standard form.*

3.4 Encoding and decoding of linear codes

Let $\mathcal{C}$ be an $[n, k, d]$ code over $\mathbb{F}_q$ and $\{r_1, r_2, \ldots, r_k\}$ the fixed basis for $\mathcal{C}$. For each $v \in \mathcal{C}$, can be uniquely expressed as a linear combination,

$$v = u_1 r_1 + u_2 r_2 + \cdots + u_k r_k$$

where $u_1, u_2, \ldots, u_k \in \mathbb{F}_q$. Note that each r_i is a vector of length n.

Equivalently, we may set G to be a generator matric of $\mathcal{C}$ whose i^{th} row is the vector r_i in the chosen basis. Given a word $u = u_i u_2 \ldots u_k \in \mathbb{F} - q^k$, it is clear that

$$v = u_1 r_1 + u_2 r_2 + \cdots + u_k r_k$$

is a codeword in $\mathcal{C}$. Conversely, any $v \in \mathcal{C}$ can be uniquely written as $v = uG$ where $u = u_i u_2 \ldots u_k \in \mathbb{F} - q^k$. Hence, every word $u \in \mathbb{F}_q^k$ can be *encoded* as $v = uG$.

Remark 3.4.1. Advantage of having G in the standard form :

1. If a linear code $\mathcal{C}$ has a generator G in standard form, $G = [I_k \mid A]$, then $H = [-A^T \mid I_{n-k}]$ is a parity-check matrix for $\mathcal{C}$.

2. If an $[n, k, d]$ code $\mathcal{C}$ has a generator G in standard form, $G = [I_k \mid A]$, then it is trivial to recover the message u from the codeword $v = uG$ since

$$v = uG = u[I_k \mid A] = u \; uA;$$

i.e., the first k digits in the codeword $v = uG$ is the message u- they are called the *message digits* . The remaining $n-k$ digits are called *check digits* which has been added to the message for protection against noise.

The coset decoding and the syndrome decoding for a linear code over $\mathbb{F}_q$ are same idea as the binary case but if r is received and e is a coset leader for $r + \mathcal{C}$, we decode r as $v := r - e$ in stead of $r + e$ (unless $q = 2$).

3.5 Hamming codes

Definition 3.5.1. Let $r \geq 2$. A binary linear code of length $n = 2^r - 1$, with parity-check matrix H whose columns consist of all nonzero vectors in $\mathbb{F}_2^r$, is called a *binary Hamming code* of length $2^r - 1$. It is denoted by $Ham(r, 2)$.

Example 3.5.1 (Original parity-check matrix for $Ham(3, 2)$). A parity-check matrix for Original $Ham(3, 2)$ is

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

which is not the standard form.

Proposition 3.5.1 (Properties of binary Hamming codes).

(i) All the binary hamming codes of a given length are equivalent.

(ii) The dimension of $Ham(r, 2)$ is $k = 2^r - 1 - r$.

(iii) The minimum distance of $Ham(r,2)$ *is* $d = 3$*, hence* $Ham(r,2)$ *is exactly single-error correcting code.*

Definition 3.5.2. The dual of binary Hamming code $Ham(r,2)$ is called a *binary simplex code*, denoted $S(r,2)$.

Let ≥ 2 be any prime power. Note that any nonzero vector $v \in \mathbb{F}_q^r$ generates a subspace $< v >$ of dimension 1. Furthermore, for $v, w \in \mathbb{F}_q^r \setminus \{0\}$, $< v >=< w >$ if and only if there is a nonzero scalar $\lambda \in \mathbb{F}_q \setminus \{0\}$ such that $v = \lambda w$. Therefore, there are exactly $(q^r - 1)/(q - 1)$ distinct subspaces of dimension 1 in $\mathbb{F}_q^r$

Definition 3.5.3. Let $r \geq 2$. A q-ary linear code whose parity-check matrix H has the property that the columns of H are made up of precisely one nonzero vector from each subspace of dimension 1 of $\mathbb{F}_q^r$, is called a *q-ary Hamming code*. It is denoted by $Ham(r,q)$.

Proposition 3.5.2 (Properties of q-ary Hamming codes). $Ham(r,q)$ *is a* $[(q^r-1)/(q-1), (q^r-1)/(q-1)-r, 3]$ *code, hence* $Ham(r,q)$ *is exactly single-error correcting code.*

Definition 3.5.4. The dual of $q-$ary Hamming code $Ham(r,q)$ is called a *q-ary simplex code*, denoted $S(r,q)$.

3.6 Some bounds on linear codes

The fundamental parameters of a linear code are n, k and d. In practice, we are interested in increase the information rate k/n, and enlarge the minimum distance d. We may think of this as a typical *packing problem* of combinatorics : Is it possible to pack a large number of codeword in the space $\mathbb{F}_q^n$ such that no two codewords are closed ? This leads to study of some bounds for the parameters of linear codes.

Theorem 3.6.1 (The Singleton Bound). *The parameters of each* $[n,k,d]$ *code over* $\mathbb{F}_q$ *satisfying the inequality*

$$d - 1 \leq n - k.$$

Definition 3.6.1. A linear code whose parameters attain the singleton bound is called a *Maximum Distance Separable (MDS) code.*

Definition 3.6.2. Let A be an alphabet of size $q > 1$. For each vector $u \in A^n$ and $r \geq 0$, the *sphere of radius r and center u*, denote $S_q(u, r)$, is the set $\{v \in A^n \mid d(u, v) \leq r\}$.

Lemma 3.6.2. *For all integer $r \geq 0$, a sphere of radius r in A^n contains exactly*

$$\sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

vectors.

Theorem 3.6.3 (The Hamming bound). *The parameters of each $[n, k, d]$ code over $\mathbb{F}_q$ satisfying the inequality*

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

Equality holds if and only if the spheres of radius $\lfloor \frac{d-1}{2} \rfloor$ around codewords cover the whole space $\mathbb{F}_q^n$.

Definition 3.6.3. A linear code whose parameters attain the Hamming bound is called the a *perfect code.*

Proposition 3.6.4. *Hamming code $Ham(r, q)$ is perfect.*

Theorem 3.6.5 (The Gilbert -Varshamov bound). *Let q be a power of prime, $n, k, d \in \mathbb{N}$ with $1 \leq k \leq n$ and $2 \leq d \leq n$. If*

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k},$$

then there exists an $[n, k]$ code over $\mathbb{F}_q$ with the minimum distance at least d.

3.7 Modifying and combining codes

In this section, we study several constructions of new linear codes based on old codes.

Theorem 3.7.1. *Suppose there exist an $[n, k, d]$ code over $\mathbb{F}_q$. Then*

(i) there exist an $[n + r, k, d]$ code over $\mathbb{F}_q$ for any $r \geq 1$;

(ii) there exist an $[n, k - r, d]$ code over $\mathbb{F}_q$ for any $1 \leq r \leq k - 1$;

(iii) there exist an $[n - r, k, d - r]$ code over $\mathbb{F}_q$ for any $1 \leq r \leq d - 1$;

(iv) there exist an $[n, k, d - r]$ code over $\mathbb{F}_q$ for any $1 \leq r \leq d - 1$;

(v) there exist an $[n - r, k - r, d]$ code over $\mathbb{F}_q$ for any $1 \leq r \leq k - 1$.

Theorem 3.7.2 (Direct sum). *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ code over $\mathbb{F}_q$, respectively. Then the direct sum of $\mathcal{C}_1$ and $\mathcal{C}_2$ is defined by*

$$\mathcal{C}_1 \oplus \mathcal{C}_2 = \{uv \mid u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$$

is an $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ code over $\mathbb{F}_q$.

Theorem 3.7.3 ($u|u + v$-construction). *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be $[n, k_1, d_1]$ code over $\mathbb{F}_q$ and $[n, k_2, d_2]$ code over $\mathbb{F}_q$, respectively. Then the code*

$$\mathcal{C} := \{u|u + v \mid u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$$

is an $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ code over $\mathbb{F}_q$.

Theorem 3.7.4. *Let A be an $[N, K, D]$ code over $\mathbb{F}_{q^m}$. Then there exists an $[nN, mK, \geq dD]$ code over $\mathbb{F}_q$, provided that there is an $[n, m, d]$ code over $\mathbb{F}_q$. Moreover, an $[nN, mK, dD]$ code over $\mathbb{F}_q$can be obtained.*

Exercises

1. If $u, v \in \mathbb{F}_q^n$, then $\mathrm{w}(u) + \mathrm{w}(v) \geq \mathrm{w}(u+v) \geq \mathrm{w}(u) - \mathrm{w}(v)$.

2. Let α be a root of an irreducible polynomial of degree m over $\mathbb{F}_q$. Show that $\{1, \alpha, \ldots, \alpha^{m-1}\}$is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

3. For each of the following sets S and corresponding finite field $\mathbb{F}_q$, find the $\mathbb{F}_q-$linear span $< S >$ and its orthogonal complement $S^{\perp}$:

   (a) $S = \{101, 111, 010\}, q = 2$

   (b) $S = \{1020, 0201, 2001\}, q = 3$

   (c) $S = \{00101, 10001, 11011, 01010\}, q = 2$

   (d) $S = \{1031, 4111, 0210\}, q = 5$.

4. Let $\mathcal{C}$ and D be linear code over $\mathbb{F}_q$ of the same length. Define

$$\mathcal{C} + D = \{c + d \mid c \in \mathcal{C}, d \in D\}.$$

   Show that $\mathcal{C} + D$ is a linear code and that $(\mathcal{C} + D)^{\perp} = \mathcal{C}^{\perp} \cap D^{\perp}$.

5. Determine whether each of the following statements is true or false. Justify your answer.

   (a) If C and D are linear codes over $\mathbb{F}_q$ of the same length, then $C \cap D$ is also a linear code over $\mathbb{F}_q$.

   (b) If C and D are linear codes over $\mathbb{F}_q$ of the same length, then $C \cup D$ is also a linear code over $\mathbb{F}_q$.

   (c) If $C =< S >$, where $S = \{v_1, v_2, v_3\} \subseteq \mathbb{F}_q^n$, then $\dim C = 3$.

   (d) If $C =< S >$, where $S = \{v_1, v_2, v_3\} \subseteq \mathbb{F}_q^n$, then $d(C) = \min\{\mathrm{w}(v_1), \mathrm{w}(v_2), \mathrm{w}(v_3)\}$.

   (e) If C and D are linear codes over $\mathbb{F}_q$ with $C \subseteq D$, then $D^{\perp} \subseteq C^{\perp}$.

6. Find a generator matrix and parity-check matrix for the linear code spanned by the following sets, and give the parameter n, k and d for each of these codes:

(a) q=2, S={1000,0110,0010,0001,1001}.

(b) q=3, S={110000,011000,001100,000110,000011}.

(c) q=2, S={10101010,11001100,11110000,01100110,00111100}.

7. Find a parity check matrix H corresponding to the given generator matrix G:

(a)
$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(b)
$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

8. Find a generator matrix G of the binary linear code C corresponding to the given parity-check matrix H:

(a)
$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

(b)
$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

9. Construct a binary linear code of length 6 as follows : for every $x_1x_2x_3 \in \mathbb{F}_3^3$,

construct a 6-bits word $x_1x_2x_3x_4x_5x_6 \in \mathcal{C}$, where

$$x_4 = x_1 + x_2 + x_3,$$
$$x_5 = x_1 + x_3,$$
$$x_6 = x_2 + x_3.$$

(a) Show that $\mathcal{C}$ is a linear code.

(b) Find a generator matrix and a parity-check matrix for $\mathcal{C}$.

(c) Find the parameters n, k and d for $\mathcal{C}$.

10. Let $\mathcal{C}$ be a linear code of minimum distance d, where d is even. Show that some coset of $\mathcal{C}$ contains two vectors of weight $\lfloor \frac{d-1}{2} \rfloor + 1$.

11. (a) Given an $[n, k, d]$ code over $\mathbb{F}_q$, can one always construct an $[n+1, k+1, d]$ code over $\mathbb{F}_q$? Justify your answer.

    (b) Given an $[n, k, d]$ code over $\mathbb{F}_q$, can one always construct an $[n+1, k, d+1]$ code over $\mathbb{F}_q$? Justify your answer.

12. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be $[n_1, k, d_1]$ code over $\mathbb{F}_q$ and $[n_2, k, d_2]$ code over $\mathbb{F}_q$, respectively. Let G_1 and G_2 be generator matrices for $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Prove that there exist a linear code

$$\mathcal{C} := \{u[G_1|G_2] \mid u \in \mathbb{F}_q^k\}$$

which is an $[n_1 + n_2, k, \geq \{d_1 + d_2\}]$ code over $\mathbb{F}_q$.

13. Find the minimum distance of $[10, 9]$ code over $\mathbb{F}_{11}$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

14. Find the minimum distance of $[10, 9]$ code over $\mathbb{F}_{11}$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

Chapter 4

Cyclic codes

4.1 Definitions

Definition 4.1.1. A linear code $\mathcal{C}$ is called a *cyclic code* if $v_{n-1}v_0v_1\ldots v_{n-2} \in \mathcal{C}$ whenever $v_0v_1\ldots v_{n-2}v_{n-1} \in \mathcal{C}$.

Consider $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/\langle x^n-1\rangle$ as vector spaces over $\mathbb{F}_q$. Define

$$\Phi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n-1\rangle, \text{ by}$$

$$a_0a_1\ldots a_{n-1} \mapsto a_0 + a_1x + \ldots a_{n-1}x^{n-1} \tag{4.1}$$

Then Φ is a bijective linear transformation.

Definition 4.1.2. Let R be a commutative ring with identity (cf. Definition 2.1.1). A nonempty subset I of R is called an *ideal* if

i) $a+b,\ a-b \in I$, for all $a, b \in I$.

ii) $r \cdot a \in I$, for all $r \in R$ and $a \in I$.

Definition 4.1.3. An ideal of a ring R is is called a *principle ideal* if there exists an element $g \in I$ such that $I = \langle g\rangle := \{g \cdot r \mid r \in R\}$. The element g (may not unique) is called a *generator* of I and I is said to be generated by g.

Theorem 4.1.1. *Every ideal of a ring $\mathbb{F}_q[x]/\langle x^n-1\rangle$ is principle.*

4.2 Generator polynomials and generator matrices

Theorem 4.2.1. *Let Φ be the map defined in (4.1). Then a nonempty subset $\mathcal{C}$ of $\mathbb{F}_q^n$ is a cyclic code if and only if $\Phi(\mathcal{C})$ is an ideal of $\mathbb{F}_q[x]/\langle x^n-1\rangle$.*

Theorem 4.2.2. *Let I be a nonzero ideal in $\mathbb{F}_q[x]/\langle x^n-1\rangle$ and let $g(x)$ be a nonzero monic polynomial of the least degree in I. Then $g(x)$ is a generator of I and divides x^n-1.*

Theorem 4.2.3. *There is a unique monic polynomial of the least degree in every nonzero ideal I of $\mathbb{F}_q[x]/\langle x^n-1\rangle$. (By Theorem 4.2.2, it is a generator of I.)*

Definition 4.2.1. The unique monic polynomial of the least degree of a nonzero ideal I of $\mathbb{F}_q[x]/\langle x^n-1\rangle$ is called the *generator polynomial* of I. For a cyclic code $\mathcal{C}$, the generator polynomial of $\Phi(\mathcal{C})$ is also called the *generator polynomial* of $\mathcal{C}$.

Theorem 4.2.4. *Each monic divisor of x^n-1 is the generator of some cyclic code in $\mathbb{F}_q^n$.*

Corollary 4.2.5. *There is a one-to-one correspondence between the cyclic codes in $\mathbb{F}_q^n$ and the monic divisors of $x^n-1 \in \mathbb{F}_q[x]$.*

Theorem 4.2.6. *Let $g(x)$ be the generator polynomial of an ideal of $\mathbb{F}_q[x]/\langle x^n-1\rangle$. Then the corresponding cyclic code has dimension k if the degree of $g(x)$ is $n-k$.*

Theorem 4.2.7. *Let $g(x) = g_0 + g_1x + \cdots + g_{n-k}$ be the generator polynomial of a cyclic code $\mathcal{C}$ in $\mathbb{F}_q^n$ with $\deg g(x) = n-k$. Then the matrix*

$$G := \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & . & . & . & g_{n-k} & 0 & 0 & 0 & . & . & 0 \\ 0 & g_0 & g_1 & . & . & . & g_{n-k} & 0 & 0 & . & . & 0 \\ \vdots & & & & & & & & & & & \vdots \\ 0 & 0 & . & . & . & 0 & g_0 & g_1 & . & . & . & g_{n-k} \end{bmatrix}$$

is a generator matrix of $\mathcal{C}$.

We leave concepts of parity-check polynomials, parity-check matrices and decoding cyclic codes as your future study.

4.3 Bose-Chaudhuri-Hocquenghem (B.C.H.) codes [V.Pless, pp. 44-47]

In this section, we mention about a double-error-correcting B.C.H-code of length 15 that we can decode efficiently. For a t-error-correcting B.C.H-code with $t > 2$, we leave as your future study.

Recall

Let α be a root of the irreducible polynomial $f(x) = x^4 + x^3 + 1$ (may be other irreducible polynomials) over $\mathbb{F}_2$. Then elements of $\mathbb{F}_{16}$ are displayed as follows :

I							II	III
						0	0	0000
						1	1	0001
				α			α	0010
		α^2					α^2	0100
α^3							α^3	1000
α^3					+	1	α^4	1001
α^3			+	α	+	1	α^5	1011
α^3	+	α^2	+	α	+	1	α^6	1111
		α^2	+	α	+	1	α^7	0111
α^3	+	α^2	+	α			α^8	1110
		α^2			+	1	α^9	0101
α^3			+	α			α^{10}	1010
α^3	+	α^2			+	1	α^{11}	1101
				α	+	1	α^{12}	0011
		α^2	+	α			α^{13}	0110
α^3	+	α^2					α^{14}	1100

Table 4.1: $\mathbb{F}_{16}$ where α is a root of the irreducible polynomial $f(x) = x^4 + x^3 + 1$.

Let

$$H := \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^i & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3i} & \dots & \alpha^{12} \end{bmatrix}$$

be a parity-check matrix of a $[15, 7]$ code. A decoding algorithm are state as follows. If y is received, compute $S(y) = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$.

i) If $S(y) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, we say no errors have occurred.

ii) If $S(y) = \begin{bmatrix} \alpha^i \\ \alpha^{3i} \end{bmatrix}$, $\alpha \neq 0$, we say that there is a single error in the $(i+1)^{th}$ position.

iii) If $S(y) = \begin{bmatrix} y_1 \\ y_3 \end{bmatrix}$, $y_3 \neq y_1^3$, we consider the equation $x^2 + y_1 x + (y_3/y_1 + y_1^2)$. If it has roots α^i and α^j, we say that there are two errors in the $(i+1)^{th}$ and $(j+1)^{th}$ positions.

iv) If $S(y)$ does not fall under cases $i)$, $ii)$, or $iii)$ above (it is possible since $\mathbb{F}_{16}$ is not algebraically closed.), we say we have detected more than two errors.

To calculate syndromes, we rewrite H as a binary form

$$H = \left[\begin{array}{cccccccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right].$$

Exercises

1. Factor the followings :
   a) $x^7 - 1$ over $\mathbb{F}_3$ b) $x^{10} - 1$ over $\mathbb{F}_3$ c) $x^9 - 1$ over $\mathbb{F}_2$.

2. Determine whether the following polynomial are generator polynomials of cyclic codes of given lengths.

   (a) $g(x) = 1 + x + x^2 + x^3 + x^4$ for a binary cyclic code of length 7.

   (b) $g(x) = 2 + 2x^2 + x^3$ for a ternary cyclic code of length 8.

   (c) $g(x) = 2 + 2x + x^3$ for a ternary cyclic code of length 13.

3. Is there a $[7, 2]$-cyclic code over $\mathbb{F}_3$? Justify your answer.

4. Find the generator polynomial of $\{0000, 1010, 0101, 1111\} \subset \mathbb{F}_2^4$.

5. determine the smallest length for a binary cyclic code for which each of the following polynomial is the generator polynomial:
   a) $g(x) = 1 + x^4 + x^5$. b) $g(x) = 1 + x + x^2 + x^4 + x^6$.

6. Construct a binary $[15, 7]$ cyclic code.

7. Show that the BCH-code defined in Section 4.3 is a $[15, 7, 5]$ code.

8. Using BCH-code in Section 4.3, find the position(s) in error of words x and y of which syndromes are $S(x) = \begin{bmatrix} \alpha^{11} \\ \alpha^{14} \end{bmatrix}$ and $S(y) = \begin{bmatrix} \alpha^{6} \\ \alpha^{3} \end{bmatrix}$.

9. Using BCH-code in Section 4.3, decode the following received words:
   a) 010000010000000 b) 111011111111111
   c) 110111101011001 d) 110011001100000.

10. Give an example of quadratic equation over $\mathbb{F}_{16}$ that cannot be factor.

Bibliography

[1] F.J. MacWilliams and N.J.A. Sloan, *The Theory of Error-Correcting Codes.*, New York:Elsevier/North Halland, 1977.

[2] S. Ling and C. Xing, *Coding Theory : A First Course.*, Cambridge University Press, 2004.

[3] V. Pless, *Introduction to the Theory of Error-Correcting Codes.*, John Wiley and Son, 1990.

[4] J.H. Van Lint, *Graduate Texts in Matematics : Introduction to Coding Theory.*, Spriger-Verlag,1982.

[5] D.G. Hoffman et al, *Algebraic Coding Theory.*, Winnipeg/Canada, 1987.

[6] W.K.Nicholson, *Introduction to Abstract Algebra Algebra.*, John Wiley & Sons, 1999.