# Chapter 10
# Boolean Field

Logical functions (or Boolean functions) and the Boolean field are very important in many applications, including computer science and cryptography.

## 10.1 Boolean Functions in Galois Field $\mathbb{Z}_2$

Let $p$ be a prime number and denote by

$$\mathbb{Z}_p = \{0, 1, \cdots, p-1\}.$$

Then define the addition $\oplus$ and the multiplication $\odot$ over $\mathbb{Z}_p$ as

$$\begin{cases} a \oplus b := a + b \ (\mathrm{mod}\ p) \\ a \odot b := ab \ (\mathrm{mod}\ p) \end{cases} \tag{10.1}$$

Then $(\mathbb{Z}_p, \oplus, \odot)$ becomes a field, which is called a Galois field. Note that when $p = 2$ we have $\mathbb{Z}_2 = \mathscr{D}$. For statement ease, we simply call $\mathbb{Z}_p$ the Galois field. Throughout this chapter we assume $p = 2$ we call $\mathbb{Z}_2$ a Boolean field. In this case, instead of $\mathscr{D}$, we use $\mathbb{Z}_2$, which means the operators on $\mathscr{D}$ are $\oplus$ and $\odot$.

It is obvious that in $\mathbb{Z}_2$ $\oplus$ and $\odot$ are tow logical operators. In fact, we have

$$\oplus = \bar{\vee}, \quad \odot = \wedge.$$

Now a natural question is: is $\{\oplus, \odot\}$ an adequate set of logical operators? The answer is: "Yes". Because

$$\neg x = 1 \oplus x,$$

and it is well known that $\{\neg, \wedge\}$ is an adequate set. It follows that any Boolean function can be expressed via $\oplus$ and $\odot$. Throughout this chapter a logical function is always called a Boolean function. For the sake of compactness, we simply denote

$$\begin{cases} a \oplus b = a + b \\ a \odot b = ab, \quad a, b \in \mathbb{Z}_2. \end{cases}$$

Consider an element in $\mathbb{Z}_2^n$. We propose the following three ways to express it.

(i) Component-wise (C-W) Form:

$$X = (x_1, x_2, \cdots, x_n), \quad x_i \in \mathbb{Z}_2,\ i = 1, \cdots, n. \tag{10.2}$$

(ii) Scalar Form: Consider $x_1\, x_2\, \cdots\, x_n$ as a binary number. Then in decimal form we have a number as

$$\chi = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n, \tag{10.3}$$

where $0 \le \chi \le 2^n - 1$.

(iii) Vector form: Identify $1 \sim \delta_2^1$ and $0 \sim \delta_2^2$, then $x_i \in \Delta_2$ and we set

$$x := \ltimes_{i=1}^n x_i \in \Delta_{2^n}. \tag{10.4}$$

It is obvious that these three expressions are equivalent. To convert one form to another, we need the following formula.

**Proposition 10.1.** *Let $\chi$ be a scalar form of $x \in \Delta_{2^n}$. Then*

$$x = \delta_{2^n}^{2^n - \chi}. \tag{10.5}$$

*Equivalently, let $x = \delta_{2^n}^t$. Then*

$$\chi = 2^n - t. \tag{10.6}$$

Using the definitions and Proposition 10.1, it is easy to convert an element in $\mathbb{Z}_2^n$ from one form to another. We give an example for this.

*Example 10.1.* Let $n = 8$. Then

$$\begin{array}{lll} \chi = 51 & \Leftrightarrow X = (0,0,1,1,0,0,1,1) & \Leftrightarrow x = \delta_{2^8}^{205}; \\ X = (1,1,0,0,1,0,1,0) & \Leftrightarrow \chi = 2^7 + 2^6 + 2^3 + 2^1 = 202 & \Leftrightarrow x = \delta_{2^8}^{54}; \\ x = \delta_{2^8}^{120} & \Leftrightarrow \chi = 2^8 - 120 = 136 & \Leftrightarrow X = (1,0,0,0,1,0,0,0). \end{array}$$

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a logical mapping. It is well known that there exists a matrix $M_f \in \mathcal{L}_{2 \times 2^n}$, called the structure matrix of $f$, such that in vector form $f$ can be expressed as

$$y := f(x_1, \cdots, x_n) = M_f \ltimes_{i=1}^n x_i, \quad x_i \in \Delta. \tag{10.7}$$

When $(x_1, \cdots, x_n)$ are expressed into its scalar form, the mapping can be expressed into its vector form as

$$\mathbf{f} := (f(0), f(1), \cdots, f(2^n - 1)). \tag{10.8}$$

Then it follows from the definition that

**Proposition 10.2.** *Denote the first row of $M_f$ as $m^f$, i.e., $m^f = \mathrm{Row}_1(M_f)$. Then*

$$m_i^f \,(\mathrm{mod}\ 2) = \mathbf{f}_{2^n+1-i}, \quad i = 1, \cdots, 2^n. \tag{10.9}$$

*Example 10.2.* 1. Let $M_f = \delta_2[1\ 1\ 2\ 1\ 2\ 1\ 1\ 2]$. Then

$$\mathbf{f} = (0\ 1\ 1\ 0\ 1\ 0\ 1\ 1).$$

2. Let $\mathbf{f} = (1\ 1\ 0\ 1\ 1\ 0\ 1\ 0)$. Then

$$M_f = \delta_2[2\ 1\ 2\ 1\ 1\ 2\ 1\ 1].$$

As a convention in cryptography, in the following we will not distinct the three forms of $X \in \mathbb{Z}_2^n$. That is,

$$\begin{array}{l} X = (x_1, \cdots, x_n), \quad x_i \in \mathscr{D} \Leftrightarrow \\ x = \ltimes_{i=1}^n x_i, \quad x_i \in \Delta_2 = \delta_{2^n}^{2^n - \chi} \Leftrightarrow \\ \chi = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n = \chi = 2^n - t, \text{ while } x = \delta_{2^n}^t. \end{array}$$

## 10.2 Polynomial Form of Boolean Functions

To get polynomial expression of Boolean functions we need some new notations.

**Definition 10.1.** 1. Let $X, C \in \mathbb{Z}_2^n$ be $X = \{x_1, \cdots, x_n\}$ and $C = \{c_1, \cdots, c_n\}$. Define

$$x_i^1 := x_i, \quad x_i^0 = \neg x_i. \tag{10.10}$$

Then

$$x_i^{c_i} := \begin{cases} 1, & x_i = c_i \\ 0, & x_i \neq c_i. \end{cases} \tag{10.11}$$

2.

$$X^C := \prod_{i=1}^n x_i^{c^i} = \begin{cases} 1, & X = C \\ 0, & X \neq C. \end{cases} \tag{10.12}$$

According to the definition, we have the following proposition.

**Proposition 10.3.** *Let $f : \mathbb{Z}_2^n \to \mathbb{Z}^2$. $X = (x_1, \cdots, x_n) \in \mathbb{Z}_2^n$. Then*

*1.*

$$f(X)=\sum_{i=0}^{2^n-1} f(i)X^i. \tag{10.13}$$

2.

$$\begin{aligned} f(x) &= a_0+a_1x_1+\cdots a_nx_n+a_{12}x_1x_2+\cdots \\ &\quad +a_{n-1\,n}x_{n-1}x_n+\cdots+a12\cdots nx_1x_2\cdots x_n \\ &= a_0+\sum_{k=1}^{n}\sum_{1\le j_1<\cdots<j_k\le n} a_{j_1\cdots j_k}x_{j_1}\cdots x_{j_k}. \end{aligned} \tag{10.14}$$

*Proof.* (10.13) follows from definitions immediately. By definition,

$$x_i^0=\begin{cases}1, & x_i=0\\ 0, & x_i=1.\end{cases}$$

Hence

$$x_i^0=x_i+1.$$

Then (10.14) comes from (10.13) by replacing $x_i^0$ by $x_i+1$ and multiplying out. □

(10.14) is called the polynomial form of $f(x)$. $\deg(f(x))$ is defined as the degree of the polynomial form of $f(x)$. When $\deg(f(x))=1$ it is called an affine function. Set of affine functions is denoted by $L_n[x]$. An affine function with $a_0=0$ is called a linear function.

*Example 10.3.* Consider

$$f(x_1,x_2,x_3)=(x_1\wedge x_2)\leftrightarrow x_3.$$

Then we have

$$\begin{array}{l} f(0)=f(0,0,0)=1,\ f(1)=f(0,0,1)=0,\ f(2)=f(0,1,0)=1,\\ f(3)=f(0,1,1)=0,\ f(4)=f(1,0,0)=1,\ f(5)=f(1,0,1)=0,\\ f(6)=f(1,1,0)=0,\ f(7)=f(1,1,1)=1. \end{array}$$

Then the C-W form of $f$ is

$$\mathbf{f}=(1\,0\,1\,0\,1\,0\,0\,1).$$

The polynomial form of $f$ is:

$$\begin{aligned} f(x) &= x_1^0x_2^0x_3^0+x_1^0x_2^1x_3^0+x_1^1x_2^0x_3^0+x_1^1x_2^1x_3^1 \\ &= (1+x_1)(1+x_2)(1+x_3)+(1+x_1)x_2(1+x_3)+x_1(1+x_2)(1+x_3)+x_1x_2x_3 \\ &= 1+x_3+x_1x_2. \end{aligned}$$

Denote by $\mathscr{BF}_n$ the set of logical functions $\mathbb{Z}_2^n\to\mathbb{Z}_2$, which is a vector space over $\mathbb{Z}_2$. Denote by $\mathscr{BA}_n$ its affine subspace and $\mathscr{BL}_n$ its linear subspace.

## 10.3 Walsh Transformation

**Definition 10.2.** Let $X=(x_1,\cdots,x_n),\Omega=(\omega_1,\cdots,\omega_n)\in\mathbb{Z}_2^n$.

1. The inner product of $X$ and $\Omega$ is defined as

$$X\cdot\Omega=x_1\omega_1+\cdots+x_n\omega_n\in\mathbb{Z}_2^n. \tag{10.15}$$

2. Define a function $\mathbb{Z}_2^n\to\mathbb{Z}_2^n$ as:

$$Q_\Omega(X)=(-1)^{\Omega\cdot X}. \tag{10.16}$$

**Lemma 10.1.** *Assume $\Omega\neq 0$. Then*

$$\sum_{x=0}^{2^n-1}(-1)^{\Omega\cdot X}=0. \tag{10.17}$$

*Proof.* Assume $\omega_i\neq 0$. For each $X=(x_1,\cdots,x_n)$ satisfying $\Omega\cdot X=0$, we construct an $X^*=(x_1,\cdots,\neg x_i,\cdots,x_n)$, which satisfies $\Omega\cdot X=1$. Since $X\leftrightarrow X^*$ is a one-to-one correspondence, it follows that

$$|\{X|\Omega\cdot X=0\}|=|\{X|\Omega\cdot X=1\}|.$$

Then (10.17) is obvious. □

**Proposition 10.4.** $\{\mathbf{Q}_\Omega(x)|\Omega=0,1,\cdots,2^n-1\}$ *is a set of orthogonal functions. Precisely,*

$$\mathbf{Q}_U\cdot\mathbf{Q}_V=\begin{cases}2^n, & U=V\\ 0, & U\neq V.\end{cases} \tag{10.18}$$

*Proof.* Assume $U=V$. Then

$$\begin{aligned}\mathbf{Q}_U\cdot\mathbf{Q}_V &= \sum_{x=0^{2^n-1}}(-1)^{U\cdot x}(-1)^{V\cdot x}\\ &= \sum_{x=0^{2^n-1}}(-1)^{2U\cdot x}\\ &= \sum_{x=0^{2^n-1}}(-1)^0=2^n.\end{aligned}$$

Assume $U\neq V$. Since $U\neq V$, $U+V\neq 0$. Using Lemma 10.1), we have

$$\mathbf{Q}_U\cdot\mathbf{Q}_V=\sum_{x=0^{2^n-1}}(-1)^{(U+V)\cdot x}=0.$$

□

Since $\{\mathbf{Q}_\Omega(x)|\Omega=0,1,\cdots,2^n-1\}$ is a set of orthogonal functions, then for any $f\in\mathscr{BF}_n$ its vector form can be expressed as

$$\mathbf{f}(x) = \sum_{\omega=0}^{2^n-1} S_f(\omega)\mathbf{Q}_\omega(x). \tag{10.19}$$

Then $S_f(\omega)$ is called the first Walsh transformation of $f$.

**Proposition 10.5.** *The first Walsh transformation is calculated as*

$$S_f(\omega) = 2^{-n} \sum_{x=0}^{2^n-1} f(x) Q_x(\omega). \tag{10.20}$$

*Proof.* For any fixed $\omega_0 \in Z_2$, we have

$$\begin{array}{l} \mathbf{f}(x) \cdot \mathbf{Q}_{\omega_0}(x) \\ = \left( \sum_{\omega=0}^{2^n-1} S_f(\omega)\mathbf{Q}_\omega(x) \right) \cdot \mathbf{Q}_{\omega_0}(x) \\ = S_f(\omega_0)\mathbf{Q}_{\omega_0}(x) \cdot \mathbf{Q}_{\omega_0}(x) \\ = 2^n S_f(\omega_0). \end{array} \tag{10.21}$$

On the other hand, we have

$$\mathbf{f}(x) \cdot \mathbf{Q}_{\omega_0}(x) = \sum_{x=0}^{2^n-1} Q_{\omega_0}(x) f(x).$$

Hence,

$$S_f(\emptyset) = 2^{-n} \sum_{x=0}^{2^n-1} Q_\emptyset(x) f(x).$$

□

Next, we consider another Walsh Transportation. Define

$$g(x) := 1 - 2f(x). \tag{10.22}$$

We have the expression of $\mathbf{g}(x)$ over the basis $\{\mathbf{Q}_\omega(x) \mid \omega = 0, 1, \cdots, 2^n - 1\}$ as

$$\mathbf{g}(x) = \sum_{\omega=0}^{2^n-1} S_{(f)}(\omega)\mathbf{Q}_\omega(x). \tag{10.23}$$

Again, for a fixed $\omega_0 \in \mathbb{Z}_2$, we have

$$\mathbf{g}(x) \cdot \mathbf{Q}_{\omega_0}(x) = \sum_{x=0}^{2^n-1} (1 - 2f(x)) Q_{\omega_0}(x). \tag{10.24}$$

It is easy to check that

$$(-1)^{f(x)} = 1 - 2f(x). \tag{10.25}$$

Hence,

$$\mathbf{g}(x)\cdot\mathbf{Q}_{\omega_0}(x)=\sum_{x=0}^{2^n-1}(-1)^{f(x)}Q_{\omega_0}(x). \tag{10.26}$$

On the other hand, we have

$$\mathbf{g}(x)\cdot\mathbf{Q}_{\omega_0}(x)=\left(\sum_{\o=0}^{2^n-1}S_{(f)}(\o)Q_{\omega_0}(x)\right)\cdot Q_{\omega_0}(x)=2^n\times S_{(f)}(\omega_0).$$

We conclude that

$$S_{(f)}(\omega)=\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}Q_\omega(x).$$

**Definition 10.3.** For a Boolean function $f(x)$,

$$S_{(f)}(\omega)=\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}Q_\omega(x) \tag{10.27}$$

is called the second Walsh Transformation of $f$.

From (10.22) and (10.23) we have

$$f(x)=\frac{1}{2}-\frac{1}{2}\sum_{\omega=0}^{2^n-1}S_{(f)}(\omega)Q_\omega(x). \tag{10.28}$$

Next, we consider the relationship between the two Walsh Transformations, we have

**Proposition 10.6.** *$S_{(f)}(\omega)$ and $S_f(\omega)$ have the following relationships*

$$S_{(f)}(\omega)=\begin{cases}-2S_f(\omega), & \omega\neq 0\\ 1-2S_f(\omega), & \omega=0\end{cases} \tag{10.29}$$

*Proof.* Using (10.25), we have

$$\begin{aligned} S_{(f)}(\omega) &= \tfrac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}Q_\omega(x)\\ &= \tfrac{1}{2^n}\sum_{x=0}^{2^n-1}(1-2f(x))Q_\omega(x)\\ &= \tfrac{1}{2^n}\sum_{x=0}^{2^n-1}Q_\omega(x)-\tfrac{2}{2^n}\sum_{x=0}^{2^n-1}f(x)Q_\omega(x). \end{aligned} \tag{10.30}$$

Using Lemma 10.1, we have

$$S_{(f)}(\omega)=\begin{cases}-2S_f(\omega), & \omega\neq 0\\ 1-2S_f(\omega), & \omega=0.\end{cases}$$

□

In the following we consider some interesting properties of Walsh transformations.

**Proposition 10.7.** *Let $S_f(\emptyset)$ be the Walsh Transportation of $f(x)$, then for any $a \in \mathbb{Z}_2^n$, the Walsh transformation of $f(x+a)$ is*

$$S_{f(x+a)}(\omega) = Q(\omega,a)S_f(\omega). \tag{10.31}$$

*Proof.* By definition, the Walsh Transportation of $f(x+a)$ is

$$\begin{aligned}
S_{f(x+a)}(\omega) &= 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\emptyset\cdot(x)}f(x+a)\\
&= (-1)^{2\omega\cdot a}\cdot 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\omega\cdot x}f(x+a)\\
&= (-1)^{\omega\cdot a}\cdot 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\omega\cdot(x+a)}f(x+a)\\
&= (-1)^{\omega\cdot a}\cdot 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\omega\cdot(x)}f(x)\\
&= Q(\omega,a)S_f(\omega).
\end{aligned}$$

□

**Proposition 10.8.** *Let $S_f(\omega)$ be the Walsh Transportation of $f(x)$, $S_g(\omega)$ be the Walsh Transportation of $g(x)$, then the Walsh Transportation of $af(x)+bg(x)$ is*

$$S_{af(x)+bg(x)}(\omega) = aS_f(\omega)+bS_g(\omega). \tag{10.32}$$

*Proof.* Starting from its definition, the Walsh Transportation of $af(x)+bg(x)$ is

$$\begin{aligned}
S_{af(x)+bg(x)}(\omega) &= 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\omega\cdot x}(af(x)+bg(x))\\
&= a\cdot 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\omega\cdot x}f(x)+b\cdot 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{\omega\cdot x}g(x)\\
&= aS_f(\omega)+bS_g(\omega).
\end{aligned}$$

□

**Proposition 10.9 (Plancheral Equation).**

$$\sum_{\omega=0}^{2^n-1}S_f^2(\omega) = S_f(0) \tag{10.33}$$

*Proof.* Since

$$S_f(\omega) = 2^{-n}\sum_{x=0}^{2^n-1}Q_\omega(x)f(x),$$

we have

$$\begin{aligned}
\sum_{\omega=0}^{2^n-1} S_f^2(\omega) &= 2^{-2n} \sum_{\omega=0}^{2^n-1} \Big(\sum_{x=0}^{2^n-1} Q_\omega(x) f(x)\Big)\Big(\sum_{x=0}^{2^n-1} Q_\omega(x) f(x)\Big) \\
&= 2^{-2n} \sum_{\omega=0}^{2^n-1} \Big(\sum_{x=0}^{2^n-1} Q_\omega(x)\cdot Q_\omega(x) f^2(x) + \sum_{x_1\neq x_2} (-1)^{(x_1+x_2)\cdot\omega} f(x_1) f(x_2)\Big) \\
&= 2^{-2n} \sum_{\omega=0}^{2^n-1} \Big(\sum_{x=0}^{2^n-1} f(x) + \sum_{x_1\neq x_2} (-1)^{(x_1+x_2)\cdot\omega} f(x_1) f(x_2)\Big) \\
&= 2^{-2n} \sum_{\omega=0}^{2^n-1} \sum_{x=0}^{2^n-1} f(x) + 2^{-2n} \sum_{\omega=0}^{2^n-1} \sum_{x_1\neq x_2} (-1)^{(x_1+x_2)\cdot\omega} f(x_1) f(x_2) \\
&= 2^{-n} \sum_{x=0}^{2^n-1} f(x) + 2^{-2n} \sum_{x_1\neq x_2} \sum_{\omega=0}^{2^n-1} (-1)^{(x_1+x_2)\cdot\omega} f(x_1) f(x_2).
\end{aligned}$$

Since $x_1 \neq x_2$, then $x_1 + x_2 \neq 0$. It follows from Lemma 10.1 that

$$\sum_{\omega=0}^{2^n-1} (-1)^{(x_1+x_2)\cdot\omega} = 0.$$

Hence

$$\sum_{\omega=0}^{2^n-1} S_f^2(\omega) == 2^{-n} \sum_{x=0}^{2^n-1} f(x) = S_f(0).$$

□

**Proposition 10.10 (Parseval Equation).** *For the second Walsh transformation we have*

$$\sum_{\omega=0}^{2^n-1} S_{(f)}^2(\omega) = 1. \tag{10.34}$$

*Proof.* Using Proposition 10.6, we have

$$\begin{aligned}
\sum_{\omega=0}^{2^n-1} S_{(f)}^2(\omega) &= (1-2S_f(0))^2 + \sum_{\omega=1}^{2^n-1} S_f^2(\omega) \\
&= 1 - 4S_f(0) + 4\sum_{\omega=0}^{2^n-1} S_f^2(\omega) \\
&= 1.
\end{aligned}$$

Note that the last equality comes from Proposition 10.9. □

Next, we investigate the matrix converting form between $\mathbf{f}$ and its Walsh transformation $\mathbf{S}_f$. Because of the symmetry, we denote

$$Q(\omega, x) := Q_\omega(x).$$

From (10.19), we know that

$$
\begin{aligned}
&(f(0), f(1), \cdots, f(2^n-1)) \\
&= (S_f(0), S_f(1), \cdots, S_f(2^n-1)) \begin{pmatrix} Q(0,0) & Q(0,1) & \cdots Q(0,2^n-1) & \\ Q(1,0) & Q(1,1) & \cdots & Q(1,2^n-1) \\ \cdots & \cdots\cdots & \cdots & \\ Q(2^n-1,0) & Q(2^n-1,1) & \cdots Q(2^n-1,2^n-1) & \end{pmatrix} \\
&:= (S_f(0), S_f(1), \cdots, S_f(2^n-1)) H_n.
\end{aligned} \tag{10.35}
$$

Since $Q(a,b) = Q(b,a)$, $H_n$ is symmetric. Then the above equation can also be expressed briefly as

$$
\mathbf{f} = H_n \mathbf{S}_f. \tag{10.36}
$$

**Definition 10.4.** Let $A = (a_{ij}) \in \mathscr{M}_{s\times s}$. $A$ is called a Hadamard matrix, if it satisfies

(i)

$$
a_{ij} = \pm 1, \quad 1 \le i, j \le s;
$$

(ii)

$$
A^T A = A A^T = s I_s.
$$

**Proposition 10.11.** *The transfer matrix $H_n$, defined in (10.35), satisfies*

*(i)*

$$
H_{n+1} = H_1 \otimes H_n;
$$

*(ii)*

$$
H_n H_n = 2^n I_(2^n);
$$

*(iii) $H_n$ is a Hadamard Matrix.*

*Proof.* Item (ii) follows from Proposition 10.4 immediately. Then (iii) is obvious. We prove (i) only. Consider $H_{n+1}$. It can be expressed as

$$
\begin{aligned}
H_{n+1} &= \begin{pmatrix} Q(0,0) & \cdots & Q(0,2^n-1) & Q(0,2^n) & \cdots & Q(0,2^{n+1}-1) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ Q(2^n-1,0) & \cdots & Q(2^n-1,2^n-1) & Q(2^n-1,2^n) & \cdots & Q(2^n-1,2^{n+1}-1) \\ Q(2^n,0) & \cdots & Q(2^n,2^n-1) & Q(2^n,2^n) & \cdots & Q(2^n,2^{n+1}-1) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ Q(2^{n+1}-1,0) & \cdots & Q(2^{n+1}-1,2^n-1) & Q(2^{n+1}-1,2^n) & \cdots & Q(2^{n+1}-1,2^{n+1}-1) \end{pmatrix} \\
&:= \begin{pmatrix} H_n^1 & H_n^2 \\ H_n^2 & H_n^3 \end{pmatrix},
\end{aligned}
$$

where $H_n^i$, $i = 1,2,3$ are of the same size.

Consider $H_n^1$, and denote it as

$$
H_n^1 = \left( Q^1(\omega, x) \right),
$$

where

$$
x = (0, x_1, x_2, \cdots, x_{2^n}), \quad \omega = (0, \omega_1, \omega_2, \cdots, \omega_{2^n}),
$$

and both $(x_1,x_2,\cdots,x_{2^n})$ and $(\omega_1,\omega_2,\cdots,\omega_{2^n})$ run from $(0,\cdots,0)$ to $(1,\cdots,1)$. Then it is obvious that $H_n^1 = H_n$.

Next, consider $H_n^2$, and denote it as

$$H_n^2 = \left(Q^2(\omega,x)\right),$$

where

$$x = (1,x_1,x_2,\cdots,x_{2^n}), \quad \omega = (0,\omega_1,\omega_2,\cdots,\omega_{2^n}),$$

and both $(x_1,x_2,\cdots,x_{2^n})$ and $(\omega_1,\omega_2,\cdots,\omega_{2^n})$ run from $(0,\cdots,0)$ to $(1,\cdots,1)$. Then it is obvious that $H_n^2 = H_n$.

Finally, we consider $H_n^3$, and denote it as

$$H_n^3 = \left(Q^3(\omega,x)\right),$$

where

$$x = (1,x_1,x_2,\cdots,x_{2^n}), \quad \omega = (1,\omega_1,\omega_2,\cdots,\omega_{2^n}).$$

Similar argument shows that $H_n^3 = -H_n$.

Note that

$$H(1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

then it is clear that

$$H_{n+1} = H_1 \otimes H_n.$$

□

## 10.4 Linear Structure

**Definition 10.5.** Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ ba a Boolean function.

1. $a \in \mathbb{Z}_2^n$ is called an invariant linear structure (ILS) of $f$, if

$$f(x+a) + f(x) = 0. \tag{10.37}$$

2. $a \in \mathbb{Z}_2^n$ is called a variant linear structure (VLS) of $f$, if

$$f(x+a) + f(x) = 1. \tag{10.38}$$

3. Denote by

$$\begin{aligned} E_0 &:= \{a \in \mathbb{Z}_2^n \mid f(x+a) + f(a) = 0\} \\ E_1 &:= \{a \in \mathbb{Z}_2^n \mid f(x+a) + f(a) = 1\} \\ E &:= E_0 \cup E_1. \end{aligned} \tag{10.39}$$

Then $E$ is called the linear structure subspace of $f$.

**Proposition 10.12.** *1.* $E_0 \cap E_1 = \emptyset$.
*2.* $E$ *is a vector space and* $E_0 \subset E$ *is a vector subspace.*
*3. Assume* $E_1 \neq \emptyset$. *Then* $E_1 = E_0 + a$, *where* $a \in E_1$.

*Proof.* 1. It is obvious.
2. • Let $a, b \in E_0$. Then

$$\begin{aligned} & f(x+a+b)+f(x) \\ & = f(x+a+b)+f(x+a)+f(x+a)+f(x) \\ & = 0+0=0. \end{aligned}$$

That is, $a+b \in E_0 \subset E$.
• Let $a \in E_0$ and $b \in E_1$. Then

$$\begin{aligned} & f(x+a+b)+f(x) \\ & = f(x+a+b)+f(x+a)+f(x+a)+f(x) \\ & = 1+0=1. \end{aligned}$$

That is, $a+b \in E_1 \subset E$.
• Let $a, b \in E_1$. Then

$$\begin{aligned} & f(x+a+b)+f(x) \\ & = f(x+a+b)+f(x+a)+f(x+a)+f(x) \\ & = 1+1=0. \end{aligned}$$

That is, $a+b \in E_0 \subset E$.
Hence $E$ is a vector space. Moreover, case 1 proved that $E_0$ is a vector subspace.
3. It was proved that if $a \in E_0$, $b \in E_1$, then $a+b \in E_1$. That is, $E_0 + b \subset E_1$. Now assume $\xi \in E_1$, then $\xi + b \in E_0$, and

$$\xi = (\xi + b) + b \in E_0 + b,$$

which means $E_1 \subset E_0 + b$. The conclusion follows.

□

We have the following corollary.

**Corollary 10.1.** *1.*

$$|E_0| = 2^r, \tag{10.40}$$

*where* $r$ *is the dimension of* $E_0$.
*2. Either* $E_1 = \emptyset$, *or*

$$|E_1| = |E_0|. \tag{10.41}$$

*Proof.* 1. As a vector subspace, (10.40) is trivial.

2. Assume $E_1 \neq \emptyset$, and let $b \in E_1$. Define $\pi_b : E_0 \to E_1$ as $x \mapsto x+b$, then it is easy to check that $\pi$ is one-to-one and onto.

□

**Definition 10.6.** Given a logical function $f$.

(i) Let $|E| = 2^q$. Then $q$ is called the dimension of linear structure of $f$. When $q > 0$, $f$ is called a logical function with linear structure (LFLS).
(ii) For an LFLS $f$, if $E_0 \neq \{0\}$, then $f$ is said to be of type $I$, if $E_0 = \{0\}$, it is said to be of type $II$.

Next, we consider how to calculate $E_0$ and $E_1$. Let $f : \mathscr{D}^n \to \mathscr{D}$ be a logical function with its structure matrix $M_f \in \mathscr{L}_{2\times 2^n}$. Denote by $\alpha = \ltimes_{i=1}^n a_i$, $x = \ltimes_{i=1}^n x_i$. Then it is easy to see that $(a_1, \cdots, a_n) \in E_1$, iff

$$M_f M_p a_1 x_1 M_p a_2 x_2 \cdots M_p a_n x_n = M_f x_1 x_2 \cdots x_n. \tag{10.42}$$

A straightforward computation shows that (10.42) is equivalent to

$$M_f M_p \ltimes_{i=1}^{n-1} (I_{2^{2i}} \otimes M_p) \ltimes_{i=1}^{n-1} \left( I_{2^i} \otimes W_{[2,2^i]} \right) \alpha x = M_f x. \tag{10.43}$$

Define

$$\Psi_f := M_f M_p \ltimes_{i=1}^{n-1} (I_{2^{2i}} \otimes M_p) \ltimes_{i=1}^{n-1} \left( I_{2^i} \otimes W_{[2,2^i]} \right),$$

and split it into $2^n$ blocks as

$$\Psi_f = [\psi_1 \ \psi_2 \ \cdots \ \psi_{2^n}],$$

where $\psi_k = \mathrm{Blk}_k(\Psi_f)$, $k = 1, 2, \cdots, 2^n$. Then the following result is straightforward verifiable.

**Theorem 10.1.** *Let $\alpha = \ltimes_{i=1}^n a_i := \delta_{2^n}^i$. Then $(a_1, \cdots, a_n) \in E_0$, iff $\psi_i = M_f$. $(a_1, \cdots, a_n) \in E_1$, iff $\psi_i = M_n M_f$.*

*Example 10.4.* 1. Assume the structure matrix of $f$ is

$$M_f = \delta_2[2\ 2\ 2\ 1\ 2\ 1\ 1\ 1].$$

Then

$$M_n M_f = \delta_2[1\ 1\ 1\ 2\ 1\ 2\ 2\ 2].$$

It is easy to calculate that

$$\Psi_f = \begin{bmatrix} 1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 \\ 1 & 1 & 2 & 1 & 2 & 1 & 2 & 2 \\ 1 & 2 & 1 & 1 & 2 & 2 & 1 & 2 \\ 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 \\ 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 \\ 2 & 1 & 2 & 2 & 1 & 1 & 2 & 1 \\ 2 & 2 & 1 & 2 & 1 & 2 & 1 & 1 \\ 2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 \end{bmatrix}$$

Since $\psi_8 = M_f$ and $\psi_1 = M_n M_f$, we have that

$$(0,0,0,0,0,0,0,0) \in E_0,$$

and

$$(1,1,1,1,1,1,1,1) \in E_1.$$

Now $|E_0| = |E_1| = 1$, hence $|E| = 2$, $\dim(E) = 1$, and $f$ is an LFLS.

2. Assume the structure matrix of $f$ is

$$M_f = \delta_2[2\,2\,2\,2\,2\,2\,2\,1].$$

Then

$$M_n M_f = \delta_2[1\,1\,1\,1\,1\,1\,1\,2].$$

It is easy to calculate that

$$\Psi_f = \begin{bmatrix} 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \end{bmatrix}$$

Since only $\psi_8 = M_f$, we have that

$$E_0 = \{(0,0,0,0,0,0,0,0)\}$$

and

$$E_1 = \emptyset.$$

Now $|E_0| = 1$ and $|E_1| = 0$, hence $|E| = 1$ $f$ is not an LFLS.

## 10.5 Nonlinearity

**Definition 10.7.** 1. Let $X = (x_1, \cdots, x_n) \in \mathbb{Z}_2^n$. The Hamming weight of $X$ is defined as

$$w_H(X) = |\{i | x_i \neq 0\}|. \tag{10.44}$$

2. Let $f, g \in \mathscr{BF}_n$. The Hamming distance of $f$ and $g$ is defined as

$$d_H(f,g) := w_H(\mathbf{f} + \mathbf{g}). \tag{10.45}$$

Next, we consider the nonlinearity of a Boolean function.

**Definition 10.8.** Let $f \in \mathscr{BF}_n$.

1. The nonlinearity of $f$, denoted by $N_f$, is defined as

$$N_f := \min_{\ell \in L_n[x]} d_H(f, \ell). \tag{10.46}$$

2. The linearity of $f$, denoted by $C_f$, is defined as

$$C_f := \max_{\ell \in L_n[x]} d_H(f, \ell). \tag{10.47}$$

**Definition 10.9.** Assume $\ell(x) \in L_n[x]$ satisfies

$$d_H(\ell, f) = N_f. \tag{10.48}$$

Then $\ell(x)$ is called the best linear approximation of $f(x)$.

To calculate the nonlinearity of an $f \in \mathscr{BF}_n$ we consider the linear equivalence of $f$. The following theory shows the probability of linear equivalence of a Boolean function via Walsh transformation [3].

**Theorem 10.2.** *Let $\omega = (\omega_1, \omega_2 \cdots \omega_n)$, $x = (x_1, x_2 \cdots x_n) \in \mathbb{Z}_2^n$ and $x \in \mathbb{Z}_2^n$ be identically distributed. Then we have*

$$P(x | f(x) = \omega \cdot x) = \frac{1 + S_{(f)}(\omega)}{2}. \tag{10.49}$$

$$P(x | f(x) \neq \omega \cdots x) = \frac{1 - S_{(f)}(\omega)}{2} \tag{10.50}$$

To prove this theorem, we need some preparations.

**Lemma 10.2.** *Let $\emptyset \neq J = \{i_1, i_2, \cdots, i_j\} \subset \{1, 2, \cdots, n\}$. Then*

$$\left|\left\{x | f(x) = x_{i_1} + x_{i_2} \cdots + x_{i_j}\right\}\right| = 2^{n-1} - \sum_{\xi \in \mathbb{Z}_2^n} f(\xi)(-1)^{\xi_{i_1} + \cdots + \xi_{i_j}}. \tag{10.51}$$

*Proof.* It is obvious that

$$\begin{array}{l} \left|\left\{x|f(x)=x_{i_1}+x_{i_2}\cdots+x_{i_j}\right\}\right| \\ =\left|\left\{x|f(x)=x_{i_1}+x_{i_2}\cdots+x_{i_j}=1\right\}\right|+\left|\left\{x|f(x)=x_{i_1}+x_{i_2}\cdots+x_{i_j}=0\right\}\right| \\ =\sum_{\{x|x_{i_1}+\cdots+x_{i_j}=1\}} f(x)+\left|\left\{x|x_{i_1}+\cdots+x_{i_j}=0\right\}\right|-\sum_{\{x|x_{i_1}+\cdots+x_{i_j}=0\}} f(x). \end{array} \tag{10.52}$$

Similar to the proof of Lemma 10.1, we can prove that

$$\left|\left\{x|x_{i_1}+\cdots+x_{i_j}=0\right\}\right|=\left|\left\{x|x_{i_1}+\cdots+x_{i_j}=1\right\}\right|,$$

which implies that

$$\left|\left\{x|x_{i_1}+\cdots+x_{i_j}=0\right\}\right|=2^{n-1}.$$

Plugging it into (10.52), we have

$$\begin{array}{l} \left|\left\{x|f(x)=x_{i_1}+x_{i_2}\cdots+x_{i_j}\right\}\right| \\ =\sum_{\{x|x_{i_1}+\cdots+x_{i_j}=1\}} f(x)+2^{n-1}-\sum_{\{x|x_{i_1}+\cdots+x_{i_j}=0\}} f(x) \\ =2^{n-1}-\sum_{\xi\in\mathbb{Z}_2^n} f(\xi)(-1)^{\xi_{i_1}+\cdots+\xi_{i_j}}. \end{array}$$

□

*Proof.* (of Theorem 10.2) Note that

$$(-1)^{f(x)}=1-2f(x),$$

we have

$$\begin{array}{ll} \frac{1+S_{(f)}(\omega)}{2} & =\frac{1}{2}\left(1+\frac{1}{2^n}\sum_{x=0}^{2^n-1}(1-2f(x))(-1)^{\omega x}\right) \\ & =\frac{1}{2}\left(1+\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{\omega x}\right)-\frac{1}{2^n}\sum_{x=0}^{2^n-1} f(x)(-1)^{\omega x}. \end{array} \tag{10.53}$$

Case 1: $\omega=0$.

In this case we have $P(f(x)=\omega x)=P(f(x)=0)$. Consider the right hand side of (10.53), we have

$$\begin{aligned} &\frac{1}{2}\left(1+\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{\omega x}\right)-\frac{1}{2^n}\sum_{x=0}^{2^n-1} f(x)(-1)^{\omega x} \\ =&\frac{1}{2}\left(1+\frac{1}{2^n}\sum_{x=0}^{2^n-1}(1)\right)-\frac{1}{2^n}\sum_{x=0}^{2^n-1} f(x) \\ =&\frac{1}{2^n}\left(2^n-\sum_{x=0}^{2^n-1} f(x)\right). \end{aligned}$$

Note that $f\in\mathbb{Z}_2$, we have

$$\sum_{x=0}^{2^n-1} f(x) = |\{x|f(x)=1\}|.$$

It follows that

$$P(x|f(x)=0) = 1 - \frac{1}{2^n}\sum_{x=0}^{2^n-1} f(x) = \frac{1+S_{(f)}(\omega)}{2}.$$

Case 2: $\omega \neq 0$.
Define a subset of indices

$$J = \{i_1, i_2, \cdots, i_j\} \subset \{1, 2, \cdots, n\},$$

such that

$$\omega_i = \begin{cases} 1, & i \in J \\ 0, & \text{otherwise.} \end{cases}$$

By assumption $|J| > 0$.
Starting from (10.53) and using Lemmas 10.1 and 10.2, we have

$$\begin{aligned}
\frac{1+S_{(f)}(\omega)}{2} &= \frac{1}{2}\left(1 + \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{\omega x}\right) - \frac{1}{2^n}\sum_{x=0}^{2^n-1} f(x)(-1)^{\omega x} \\
&= \frac{1}{2^n}\left(2^{n-1} - \sum_{\xi \in \mathbb{Z}_2^n} f(\xi)(-1)^{\xi_{i_1}+\cdots+\xi_{i_j}}\right) \\
&= \frac{1}{2^n}\left|\{x|f(x) = x_{i_1} + \cdots + x_{i_j}\}\right| \\
&= \frac{1}{2^n}|\{x|f(x) = \omega x\}| \\
&= P(x|f(x) = \omega x).
\end{aligned}$$

Summarizing the two cases, we finally have

$$P(x|f(x) = \omega x) = \frac{1+S_{(f)}(\omega)}{2}.$$

Then it follows that

$$P(x|f(x) \neq \omega x) = \frac{1-S_{(f)}(\omega)}{2}.$$

□

**Theorem 10.3.** *Let $f \in \mathscr{BF}_n$ and denote*

$$a = \max_{0 \le \omega \le 2^n-1} \left|S_{(f)}(\omega)\right|.$$

*Then*

$$N_f = 2^n \left( \frac{1-a}{2} \right); \tag{10.54}$$

*and*

$$C_f = 2^n \left( \frac{1+a}{2} \right). \tag{10.55}$$

*Proof.* For any linear function $\ell(x) = \omega x + \omega_0$ we have

$$\begin{aligned} P(x|f(x) = \ell(x)) &= P(x|f(x) = \omega x + \omega_0) \\ &= \begin{cases} P(x|f(x) = \omega x), & \omega_0 = 0 \\ P(x|f(x) = \omega x + 1) = P(x|f(x) \neq \omega x), & \omega_0 = 1. \end{cases} \end{aligned}$$

Hence

$$P(x|f(x) = \ell(x) = \begin{cases} P(x|f(x) = \omega x), & \ell(x) = \omega x \\ P(x|f(x) \neq \omega x), & \ell(x) = \omega x + 1. \end{cases}$$

According to Theorem 10.2, we have

$$P(x|f(x) = \ell(x)) = \begin{cases} \frac{1+S_{(f)}(\omega)}{2}, & \ell(x) = \omega x \\ \frac{1-S_{(f)}(\omega)}{2}, & \ell(x) = \omega x + 1. \end{cases}$$

It follows that

$$\max_{\ell \in L_n[x]} P(x|f(x) = \ell(x)) = \frac{1+a}{2}; \tag{10.56}$$

and

$$\min_{\ell \in L_n[x]} P(x|f(x) = \ell(x)) = \frac{1-a}{2}. \tag{10.57}$$

Using (10.56), we have

$$\begin{aligned} N_f &= \min_{\ell \in L_n[x]} w_H(f + \ell) \\ &= \min_{\ell \in L_n[x]} 2^n P(x|f(x) \neq \ell(x)) \\ &= \min_{\ell \in L_n[x]} 2^n \left(1 - P(x|f(x) = \ell(x))\right) \\ &= 2^n \left(1 - \max_{\ell \in L_n[x]} P(x|f(x) = \ell(x))\right) \\ &= 2^n \left(\tfrac{1-a}{2}\right). \end{aligned}$$

Using (10.57), a similar argument shows that

$$C_f = 2^n \left( \frac{1+a}{2} \right).$$

□

An immediate consequence is

**Corollary 10.2.** *For any* $f \in \mathscr{BF}_n$,

$$N_f + C_f = 2^n. \tag{10.58}$$

From Theorem 10.3 one sees that when $a$ is smallest the corresponding $N_f$ is largest. Since

$$\sum_{\omega=0}^{2^n-1} S_{(f)}^2 = 1,$$

when $\left|S_{(f)}\right| = const.$, $a$ reaches the smallest. In this case we have

$$\left|S_{(f)}\right| = 2^{-\frac{n}{2}}. \tag{10.59}$$

Hence we have

$$N_f = 2^n \left( \frac{1-2^{-\frac{n}{2}}}{2} \right) = 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{10.60}$$

Therefore, we have the following result.

**Proposition 10.13.**

$$N_f \le 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{10.61}$$

When (10.60) holds, $f$ has the highest nonlinear degree. Such a Boolean function is called a Bent function or a complete nonlinear function, which is very important in cryptography [1].

## 10.6 Expressions of Boolean Functions

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a Boolean function. It can be expressed by its structure matrix $M_f \in \mathscr{L}_{2\times 2^n}$ as

$$f(x_1, \cdots, x_n) = M_f x,$$

where $x = \ltimes_{i=1}^n x_i$. Define $a = \mathrm{Row}_1(M_f) \in \mathscr{B}_{1\times 2^n}$. It is obvious that $a$ uniquely determines $f$. In fact, $a$ is the truth table of $f$.

Moreover, $f$ can be expressed as

$$
\begin{aligned}
f(x) &= a\begin{pmatrix} x_1^1 \\ x_1^0 \end{pmatrix}\begin{pmatrix} x_2^1 \\ x_2^0 \end{pmatrix}\cdots\begin{pmatrix} x_n^1 \\ x_n^0 \end{pmatrix} \\
&= a\begin{pmatrix} x_1 \\ x_1+1 \end{pmatrix}\begin{pmatrix} x_2 \\ x_2+1 \end{pmatrix}\cdots\begin{pmatrix} x_n \\ x_n+1 \end{pmatrix} \\
&= a\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{pmatrix} 1 \\ x_1 \end{pmatrix}\cdots\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{pmatrix} 1 \\ x_n \end{pmatrix} \\
&= a\left(\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\otimes\cdots\otimes\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}}_{n}\right)\begin{pmatrix} 1 \\ x_1 \end{pmatrix}\begin{pmatrix} 1 \\ x_2 \end{pmatrix}\cdots\begin{pmatrix} 1 \\ x_n \end{pmatrix} \\
&:= aP_n\xi_n := \alpha\xi_n,
\end{aligned}
\tag{10.62}
$$

where $\alpha = aP_n$ and

$$
P_n = \left(\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\otimes\cdots\otimes\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}}_{n}\right), \tag{10.63}
$$

$$
\xi_n = \begin{pmatrix} 1 \\ x_2 \end{pmatrix}\cdots\begin{pmatrix} 1 \\ x_n \end{pmatrix} \tag{10.64}
$$

is a basis of the polynomials on $\mathbb{Z}_2^n$.

Alternatively, we can express $f$ into a natural alphabetic and power increasing form as

$$
f(x) = \beta\eta_n \tag{10.65}
$$

where $\eta_n$ is an alphabetic and power increasing basis as

$$
\eta_n = \begin{bmatrix} 1 \\ x_1 \\ \vdots \\ x_n \\ x_1x_2 \\ \vdots \\ x_{n-1}x_n \\ x_1x_2x_3 \\ \vdots \\ x_{n-1}x_{n-1}x_n \\ \vdots \\ x_1x_2\cdots x_n \end{bmatrix}. \tag{10.66}
$$

Expression (10.62) can be obtained from

We would like to find the relationship between $\eta_n$ and $\xi_n$. To achieve the goal, we may consider the position which $x_{i_1}x_{i_2}\cdots x_{i_n}$ appears in $\xi_n$

To be specific, let $\mu_{i_1,i_2,\cdots,i_r}$, $i_1 < i_2 \cdots < i_t$ be the position where $x_{i_1}x_{i_2}\cdots x_{i_t}$ appears in $\xi_n$, consider

case 1:

$$\begin{pmatrix}1\\x_{n-1}\end{pmatrix}\begin{pmatrix}1\\x_n\end{pmatrix}=\begin{pmatrix}1\\x_n\\x_{n-1}\\x_{n-1}x_n\end{pmatrix} \tag{10.67}$$

We have $\mu_n = 2^0+1$ $\mu_{n-1} = 2^1+1$ $\mu_{n-1,n} = 2^1+2^0+1$

case 2:

$$\begin{pmatrix}1\\x_{n-2}\end{pmatrix}\begin{pmatrix}1\\x_{n-1}\end{pmatrix}\begin{pmatrix}1\\x_n\end{pmatrix}=\begin{pmatrix}1\\x_{n-2}\end{pmatrix}\begin{pmatrix}1\\x_n\\x_{n-1}\\x_{n-1}x_n\end{pmatrix}=\begin{pmatrix}1\\x_n\\x_{n-1}\\x_{n-1}x_n\\x_{n-2}\\x_{n-2}x_n\\x_{n-2}x_{n-1}\\x_{n-2}x_{n-1}x_n\end{pmatrix} \tag{10.68}$$

$\vdots$

case $2^n$:

$$\begin{pmatrix}1\\x_1\end{pmatrix}\begin{pmatrix}1\\x_2\end{pmatrix}\cdots\begin{pmatrix}1\\x_n\end{pmatrix}=\xi_n \tag{10.69}$$

Then we have

**Theorem 10.4.**

$$\mu_{i_1,i_2,\cdots,i_r} := \sum_{j=1}^{r} 2^{n-i_j}+1. \tag{10.70}$$

*Proof.* For any $j$, the position where $x_{n-j}$ appears for the first time is $\mu_{n-j}$=$2^j+1$

Then for any $x_{n-i_1}x_{n-i_2}\cdots x_{n-i_t}$, we can locate $x_{n-i_1}, x_{n-i_1}x_{n-i_2}, x_{n-i_1}x_{n-i_2}\cdots x_{n-i_t}$ in sequence, and in that way the conclusion follows. □

Using Theorem 10.4, we construct $\Phi_n$ as follows

$$\Phi_n = \delta_{2^n}[1,\phi_1,\phi_2,\cdots,\phi_n], \tag{10.71}$$

where $\Phi_r = (\mu_{1,2,\cdots,r}, \mu_{1,2,\cdots,r+1},\cdots,\mu_{n-r+1,n-r+2,\cdots,n})$, $\quad r = 1,2,\cdots,n$. Then we get the conclusion that

$$\Phi_n^T \xi_n = \eta_n. \tag{10.72}$$

Finally, observing $f = \alpha\xi_n = \beta\eta_n$, we have

$$\begin{aligned} \alpha &= aP_n \\ \beta &= \alpha\Phi_n = aP_n\Phi_n. \end{aligned} \tag{10.73}$$

## 10.7 Symmetric Boolean Function

Recall that $\mathbf{S}_n$ is the $n$-th order symmetric group. Denote by $\mathbf{H}_n < \mathbf{S}_n$ a subgroup of $\mathscr{S}_n$.

**Definition 10.10.** A Boolean function $f(X) \in \mathscr{B}\mathscr{F}_n$ is said to be symmetric with respect to $\mathbf{H}_n$, if

$$f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = f(x_1, \cdots, x_n), \quad \forall \sigma \in \mathbf{H}_n. \tag{10.74}$$

Divide the row vector $\beta = aP_n\Phi_n$ into $n+1$ segments as

$$\beta = [\mu_0 \; \mu_1 \; \cdots \; \mu_n], \tag{10.75}$$

where

$$\dim(\mu_i) = \binom{n}{i}, \quad i = 0, 1, \cdots, n.$$

Using it we define the projections

$$\pi_i(f) := [0 \cdots 0 \; \mu_i \; 0 \cdots 0]\eta_n, \quad i = 0, 1, \cdots, n. \tag{10.76}$$

It is easy to see that $\pi_i(f)$ is the $i$-th degree homogeneous part of $f(x)$.

**Theorem 10.5.** *$f$ is symmetric with respect to $\mathbf{H}_n$, iff $\pi_i(f)$, $i = 0, 1, \cdots, n$ are symmetric with respect to $\mathbf{H}_n$.*

*Proof.* Sufficiency is obvious. We prove the necessity. Assume $f$ is symmetric with respect to $\mathbf{H}_n$. We prove it by contradiction. Assume there exists at least one $i$, such that $\pi_i(f)$ is not symmetric with respect to $\mathbf{H}_n$. Assume $i > 0$ be the smallest such $i$. We express $\pi_i(f)$ as

$$\pi_i(f) = \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} c_{j_1 \cdots j_i} x_{j_1} \cdots x_{j_i}. \tag{10.77}$$

Note that not all $c_{j_1 \cdots j_i} = 0$. Otherwise, $\pi_i(f) = 0$ and hence it is symmetric. For any $c_{j_1 \cdots j_i} = 1$ if $c_{\sigma(j_1) \cdots \sigma(j_i)} = 1$ for all $\sigma \in \mathscr{H}$, we are done. So we assume there exists $\sigma \in \mathscr{H}$ such that $c_{\sigma(j_1) \cdots \sigma(j_i)} = 0$. Let $X_0 = (x_1, \cdots, x_n)$ be determined by

$$x_j = \begin{cases} 1, & j \in \{j_1, \cdots, j_i\} \\ 0, & \text{otherwise.} \end{cases}$$

Then it is easy to see that

$$\begin{aligned} \pi_i(f)(x_1, \cdots, x_n) &= 1 \\ \pi_i(f)(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) &= 0. \end{aligned}$$

Note that

$$\pi_k(X_0) = 0, \quad k > i.$$

Hence

$$f(x_1, \cdots, x_n) \neq f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

This is a contradiction. □

The following corollaries are obvious.

**Corollary 10.3.** *$f$ is symmetric with respect to $\mathbf{S}_n$, if and only if for each $1 \leq i \leq n-1$, the coefficients of $i$-th homogeneous terms are the same. Precisely,*

$$c_{j_1 \cdots j_i}, \quad 1 \leq j_1 < j_2 < \cdots < j_i \leq n$$

*are identically 1 or 0.*

Symmetry with respect to $\mathbf{S}_n$ is also called the complete symmetry.

**Corollary 10.4.** *There are $2^{n+1}$ completely symmetric Boolean functions in $\mathscr{BF}_n$.*

*Proof.* According to Corollary 10.3, if $f$ is symmetric with respect to $\mathbf{S}_n$ we have either $\pi_i(f) \equiv 0$ or $\pi_i(f) \not\equiv 0$. Moreover, in the later case all the coefficients must be 1. The conclusion follows. □

We may name the $2^{n+1}$ completely symmetric Boolean functions as $f_0, f_1, \cdots, f_{2^n-1}$, where $f_i$ is decided in the following way: Converting $i$ into binary form as

$$i \sim i_n i_{n-1} \cdots i_0.$$

Then

$$f_i = \sum_{j=0}^{n} i_j P_j, \quad i = 0, 1, \cdots, 2^{n+1} - 1, \tag{10.78}$$

where

$$P_j = \sum_{1 \leq k_1 < \cdots < k_j \leq n} \prod_{s=1}^{j} x_{k_s}.$$

Then the following is clear.

**Proposition 10.14.** *Let $\{f_i | i = 0, 1, \cdots, 2^{n+1} - 1\}$ be the set of set of completely symmetric Boolean functions, with the indices being determined as in the above. Then the Hamming weight of $f_i$ is*

$$w_H(f_i) = \sum_{j=0}^{n} i_j \binom{n}{j}, \quad i = 0, 1, \cdots, 2^{n+1} - 1. \tag{10.79}$$

*Proof.* Since

$$w_H(P_j) = \binom{n}{j}, \quad j = 0, 1, \cdots, n,$$

the conclusion follows from (10.78) immediately. □

To consider the symmetry with respect to $\mathscr{H}$, we need some additional concepts.

**Definition 10.11.** Let $G$ be a group, and $S$ a non-empty set. A mapping $G \times S \to S$ is called the group action of $G$ on $S$, if it satisfies

(i)

$$e(s) = s, \quad \forall s \in S,$$

where $e$ is the identity of $G$.

(ii)

$$g_1(g_2(s)) = (g_1 g_2)(s), \quad \forall s \in S.$$

**Definition 10.12.** Assume $G$ acts on $S$ and $s \in S$.

1. The trajectory of $s$ under the action of $G$ is defined as

$$Gs := \{gs | g \in G\}. \tag{10.80}$$

2. The stability subgroup of $s$ is defined as

$$G_s := \{g \in G | g(s) = s\}. \tag{10.81}$$

It is obvious that the trajectories $\{G_s | s \in S\}$ form a partition of $S$. Because for $s_1, s_2 \in S$, either $Gs_1 = Gs_2$ or $Gs_1 \cap Gs_2 = \emptyset$.

For group action we have the following properties. [2]

**Proposition 10.15.** *The length of trajectory $Gs$ is*

$$|Gs| = \frac{|G|}{|G_s|}. \tag{10.82}$$

The number of the trajectories can be obtained via the following theorem.

**Theorem 10.6.** *(Burnside Lemma) Assume $G$, acting on $S$, forms $m$ trajectories. Then*

$$m|G| = \sum_{g \in G} |fix(g)|. \tag{10.83}$$

*Here*

$$fix(g) = \{s | g(s) = s\}.$$

Construct a sequence of sets as:

$$S_i = \left\{ \{j_1, \cdots, j_i\} \subset \mathbb{Z} | 1 \le j_t \le n, t = 1, \cdots, i; j_p \ne j_q, p \ne q \right\}, \quad i = 1, \cdots, n-1.$$

Let $\mathscr{H}_n < \mathscr{S}_n$. The action of $\mathscr{H}_n$ on $S_i$ is defined as:

$$\sigma(\{j_1, \cdots, j_i\}) := \{\sigma(j_1), \cdots, \sigma(j_i)\}. \tag{10.84}$$

Using Theorem 10.5 and arguing as for Corollary 10.3, we can prove the following

**Theorem 10.7.** *Assume the number of trajectories of $\mathscr{H}_n$ acting on $S_i$ is $m_i$, $i = 1, \cdots, n-1$. Then the number of symmetric Boolean functions symmetric with respect to $\mathbf{H}_n$ is*

$$m = 2^{2 + \sum_{i=1}^{n-1} m_i}. \tag{10.85}$$

Assume a subgroup $\mathbf{C}_n < \mathbf{S}_n$ is generated by $(1, 2, \cdots, n)$, that is, $\mathbf{C}_n = \langle (1, 2, \cdots, n) \rangle$, which is called a cyclic subgroup. A Boolean function $f \in \mathscr{BF}$ is said to be rotation symmetric, if it is symmetric with respect to the cyclic subgroup.

*Example 10.5.* Let $n = 4$, and $\mathbf{C}_4 = \langle (1, 2, 3, 4) \rangle$ be the cyclic subgroup generated by $(1, 2, 3, 4)$. Then

$$\begin{aligned} S_1 &= \{1, 2, 3, 4\}; \\ S_2 &= \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}; \\ S_3 &= \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}. \end{aligned}$$

It is easy to check that each $S_1$ or $S_3$ has only one trajectory. $S_2$ has two trajectories, which are

$$\begin{aligned} &\{1, 2\} \to \{2, 3\} \to \{3, 4\} \to \{4, 1\} \to; \\ &\{1, 3\} \to \{2, 4\} \to . \end{aligned}$$

We conclude that all the $f \in \mathscr{BF}_4$, which are symmetric with respect to $\mathbf{C}_4 = G\{(1, 2, 3, 4)\}$, can be expressed as

$$\begin{aligned} f(x) = &\, a_0 + a_1(x_1 + x_2 + x_3 + x_4) + a_2(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1) \\ &+ a_3(x_1x_3 + x_2x_4) + a_4(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4), \end{aligned} \tag{10.86}$$

where $a_i = 0$ or $1$, $i = 0, 1, 2, 3, 4, 5$.

## Exercise 7

1. Assume $p$ is a primer number. Show that $(\mathbb{Z}_p, \oplus, \odot)$ is a field.

2. Let $X = (1,1,0,1,0,1,0,1)$. Find its scalar form $\chi(X)$ and vector form $x(X)$.
3. Prove the Hamming distance defined in Definition 10.7 is a distance.
   hint: A distance should satisfy:
   (i) $d(x,y) \geq 0$, and $d(x,y) = 0$ iff $x = y$ ;
   (ii) $d(x,y) = d(y,x)$;
   (iii) $d(x,y) + d(y,z) \geq d(x,z)$.
4. Show that

$$S_f(0) = 2^{-n} w_H(f). \tag{10.87}$$

5. Assume $G$ acts on $S$ and $s \in S$. Prove that $G_s < G$, i.e., $G_s$ is a subgroup of $G$.
6. Prove that the action of $\mathscr{H}_n$ on $S_i$, defined by (10.84), is a group action.
7. Conclude that all the $f \in \mathscr{BF}_5$, which are symmetric with respect to $\mathbf{C}_5 = G\{(1,2,3,4,5)\}$. Give a general form of this set of Boolean functions.

## References

1. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes. Cambridge University Press, Cambridge (2010). Prelimenary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html
2. Dixon, J., Mortimer, B.: Permutation Groups. Springer-Verlag, London (1996)
3. Wen, Q., Niu, X., Yang, Y.: Boolean Functions in Modern Cryptography. Science Press, Beijing (2000). In Chinese