

## Chapter 10

# Signal Sets with Low Cross-Correlation

In this chapter, we introduce constructions for signal sets with low crosscorrelation. These sequences have important applications in wireless code division multiple access (CDMA) communications. There are three classic constructions for signal sets with low correlation, namely, the Gold-pair construction, the Kasami (small) set construction and the bent function signal set construction. In Section 1, we introduce some basic concepts and properties for crosscorrelation of sequences or functions, signal sets, and one-to-one correspondences among sequences, polynomial functions, and boolean functions. After that, three classic constructions will be presented in Sections 2, 3 and 4 respectively. With the development of new technologies, the demand for constraints on other parameters, such as linear spans of sequences, and the sizes of the signal sets has increased. Here, we will provide two examples of constructions that sacrifice ideal correlation in order to improve other properties, in Sections 5 and 6, respectively. One example is the interleaved construction for large linear spans, and the other is  $\mathbb{Z}_4$  sequences to obtain large sizes of signal sets.

## 10.1 Cross-Correlation, Signal Sets, and Boolean Functions

In this section, we discuss some basic properties of crosscorrelation of sequences (some of them have been discussed in Chapter 1), refine the concept of signal sets, and introduce the one-to-one correspondence between sequences and boolean functions (note that the one-to-one correspondence between sequences and functions is discussed in Chapter 6).

We will keep the following notation in this section. Let  $p$  be any prime,  $n$  a positive integer,  $q = p^n$ , and  $\alpha$  a primitive element in  $\mathbb{F}_q$ . Let  $\mathbf{a} = \{a_i\}$  and  $\mathbf{b} = \{b_i\}$  be two periodic sequences over  $\mathbb{F}_p$  with periods  $v = p^n - 1$  and  $t$ , where  $t|v$ , respectively; let  $f(x)$  and  $g(x)$  be their respective trace representations, i.e.,  $a_i = f(\alpha^i)$  and  $b_i = g(\alpha^i)$ . The crosscorrelation between  $\mathbf{a}$  and  $\mathbf{b}$  (see Chapter 5) is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{v-1} \omega^{a_i + \tau b_i}, \tau = 0, 1, \dots \quad (10.1)$$

where  $\omega$  is a primitive  $p$ th root of unity. Since  $t|v$ , we have

$$C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{a},\mathbf{b}}(\tau + kt), k = 0, 1, \dots \quad (10.2)$$

### 10.1.1 Basic Properties of Cross-Correlation

**Property 10.1** *Let  $L$  be the left shift operator.*

(a) *If both  $\mathbf{a}$  and  $\mathbf{b}$  are shifted by  $k$ , then their crosscorrelation does not change, i.e.,*

$$C_{L^k\mathbf{a},L^k\mathbf{b}}(\tau) = C_{\mathbf{a},\mathbf{b}}(\tau), 0 \leq k < v.$$

(b) *Shift rule: the crosscorrelation of shifted versions of  $\mathbf{a}$  and  $\mathbf{b}$  is equal to the crosscorrelation of  $\mathbf{a}$  and  $\mathbf{b}$  up to some shift, i.e.,*

$$C_{L^i\mathbf{a},L^j\mathbf{b}}(\tau) = C_{\mathbf{a},\mathbf{b}}(\tau + i - j), 0 \leq i, j < v.$$

(c) *Commutative rule:*

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \overline{C_{\mathbf{b},\mathbf{a}}(-\tau)}.$$

In other words, the crosscorrelation of  $\mathbf{a}$  and  $\mathbf{b}$  at  $\tau$  is equal to the complex conjugate of the crosscorrelation of  $\mathbf{a}$  and  $\mathbf{b}$  at negative  $\tau$ . In particular, if  $p = 2$ , then

$$C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{b},\mathbf{a}}(-\tau).$$

(Here both  $\tau + j - i$  and  $-\tau$  are reduced modulo  $v$ .)

(d) If both  $\mathbf{a}$  and  $\mathbf{b}$  are constant-on-cosets, so is their crosscorrelation function, i.e.,

$$C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{a},\mathbf{b}}(p\tau), \tau = 0, 1, \dots$$

**Example 10.1** Let  $\mathbf{a}$  and  $\mathbf{b}$  be two binary sequences whose elements are given by

$$\mathbf{a} = 000100110101111 \text{ and } \mathbf{b} = 011.$$

Let  $T$  consist of different values in the set

$$\{C_{L^i(\mathbf{a}),L^j(\mathbf{b})}(\tau) \mid 0 \leq \tau < 15, 0 \leq i < 15, 0 \leq j < 3\}.$$

Note that both  $\mathbf{a}$  and  $\mathbf{b}$  are constant-on-cosets. According to Property 10.1-(b) and 10.1-(d), in order to get the set  $T$ , we only need to compute  $C_{\mathbf{a},\mathbf{b}}(\tau)$  for  $\tau = 0, 1$ . Since  $C_{\mathbf{a},\mathbf{b}}(0) = -5$  and  $C_{\mathbf{a},\mathbf{b}}(1) = 3$ , we have  $T = \{-5, 3\}$ .

Next, we look at the crosscorrelation between the trace representations of these two sequences. Let  $\alpha$  be a primitive element in  $\mathbb{F}_{2^4}$  with minimal polynomial  $x^4 + x + 1$ . Then the trace representations of  $\mathbf{a}$  and  $\mathbf{b}$  are given by  $f(x) = Tr_1^4(x) = x + x^2 + x^4 + x^8$  and  $g(x) = Tr_1^2(x^5) = x + x^2$ , respectively. Thus,  $C_{f,g}(\lambda)$ , the crosscorrelation between  $f$  and  $g$  (defined in Section 8.4 of Chapter 8), takes the two values  $\pm 4$  for  $\lambda \neq 0$ . Precisely, we have

$$\begin{aligned} C_{f,g}(\lambda) &= \sum_{x \in \mathbb{F}_{2^4}} (-1)^{Tr_1^4(\lambda x) + Tr_1^2(x^5)} \\ &= 1 + \sum_{i=0}^{14} (-1)^{a_i + \tau + b_i} \\ &= 1 + C_{\mathbf{a},\mathbf{b}}(\tau) \in \{\pm 4\}, \lambda = \alpha^\tau. \end{aligned}$$

The following assertion follows immediately from the definitions of the shift operator and the decimation operator.

**Property 10.2** *If  $f(x)$  is the trace representation of  $\mathbf{a}$ , then  $f(\alpha^j x)$  and  $f(x^r)$  are the trace representations of  $\mathbf{a}$  at shift  $j$ ,  $L^j(\mathbf{a})$ , and the  $r$ -decimation of  $\mathbf{a}$ ,  $\mathbf{a}^{(r)}$ , respectively, i.e.,*

$$L^j(\mathbf{a}) \leftrightarrow f(\alpha^j x), \quad (10.3)$$

$$\mathbf{a}^{(r)} \leftrightarrow f(x^r). \quad (10.4)$$

Recall that, in Chapter 8, we introduced the notation  $\langle \mathbf{a}, \mathbf{b} \rangle$  to denote the dot product (see Chapter 1) of  $\chi(\mathbf{a})$  and  $\chi(\mathbf{b})$  where  $\chi(\mathbf{x}) = (\omega^{x_0}, \dots, \omega^{x_{v-1}})$  where  $\mathbf{x} = (x_0, \dots, x_{v-1}) \in \mathbb{F}_p^v$ , i.e.,

$$\langle \mathbf{a}, \mathbf{b} \rangle = (\chi(\mathbf{a}) \cdot \chi(\mathbf{b})) = \sum_{i=0}^{v-1} \chi(a_i) \chi^*(b_i) = \sum_{i=0}^{v-1} \omega^{a_i - b_i}.$$

Some relationships between this dot product and the crosscorrelation function of the sequences  $\mathbf{a}$  and  $\mathbf{b}$  are listed in Table 10.1 for easy reference.

Table 10.1: Relationship of the dot product and crosscorrelation

$\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^v, \tau \geq 0.$	
(a)	$C_{\mathbf{a}, \mathbf{b}}(0) = \langle \mathbf{a}, \mathbf{b} \rangle.$
(b)	$C_{\mathbf{a}, \mathbf{b}}(\tau) = \langle L^\tau(\mathbf{a}), \mathbf{b} \rangle.$
(c)	$C_{L^i \mathbf{a}, L^j \mathbf{b}}(\tau) = \langle L^{i+\tau}(\mathbf{a}), L^j(\mathbf{b}) \rangle, i, j \geq 0.$
(d)	$\langle \mathbf{a} + c, \mathbf{b} + d \rangle = \omega^{d-c} \langle \mathbf{a}, \mathbf{b} \rangle, c, d \in \mathbb{F}_p.$

Let  $f$  and  $g$  be two functions from  $\mathbb{F}_p^n$  to  $F_p$ . The (*Hamming*) distance between  $f$  and  $g$ , denoted by  $d(f, g)$ , is defined as the number of  $x \in \mathbb{F}_p^n$  for which  $f(x) \neq g(x)$ , i.e.,

$$d(f, g) = |\{x \in \mathbb{F}_p^n \mid f(x) \neq g(x)\}|. \quad (10.5)$$

The (*Hamming*) weight of  $f$ , denoted by  $w(f)$ , is defined as the number of

$x \in \mathbb{F}_p^n$  such that  $f(x) \neq 0$ , i.e.,

$$w(f) = |\{x \in \mathbb{F}_p^n \mid f(x) \neq 0\}|. \quad (10.6)$$

Thus, we have

$$d(f, g) = w(f - g), \quad (10.7)$$

i.e., the distance between two functions  $f$  and  $g$  is equal to the weight of their difference. For the binary case, we have the following frequently used relationships between crosscorrelation and (Hamming) weight, or distance between sequences (or functions).

**Property 10.3** *Let  $\mathbf{a} \leftrightarrow f(x)$  and  $\mathbf{b} \leftrightarrow g(x)$  be two binary sequences where one of them has period  $2^n - 1$ . Then*

$$w(L^\tau(\mathbf{a}) + \mathbf{b}) = 2^{n-1} - \frac{C_{\mathbf{a},\mathbf{b}}(\tau) + 1}{2}.$$

*Conversely,*

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = 2^n - 2w(L^\tau(\mathbf{a}) + \mathbf{b}).$$

In the function version,

$$d(f(\lambda x), g(x)) = 2^{n-1} - \frac{1}{2}C_{f,g}(\lambda), \lambda = \alpha^\tau.$$

*Note.* These formulae are similar to equation (5) for autocorrelation in Section 7.3 of Chapter 8.

The next property indicates the crosscorrelation between  $\mathbf{a}$  and a  $d$ -decimation of  $\mathbf{b}$ .

**Property 10.4** *For  $\mathbf{a} \leftrightarrow f(x)$  and  $\mathbf{b} \leftrightarrow g(x)$ , recall that  $\mathbf{b}$  has period  $t$ , where  $t \mid (2^n - 1)$ . Let  $d > 1$  satisfying  $\gcd(d, t) = 1$ . Then*

$$C_{\mathbf{a},\mathbf{b}^{(d-1)}}(\tau) = C_{\mathbf{a},\mathbf{b}^{(d)}}(-d^{-1}\tau), \lambda = \alpha^\tau.$$

*Equivalently, in the function version,*

$$C_{f(x),g(x^{d-1})}(\lambda) = C_{f(x),g(x^d)}(\lambda^{-d^{-1}}), \lambda \in \mathbb{F}_{2^n}.$$

In other words, the image of the crosscorrelation between the sequence,  $\mathbf{a}$ , and the  $(d^{-1})$ -decimation of  $\mathbf{b}$ ,  $\mathbf{b}^{(d^{-1})}$ , is equal to the image of the crosscorrelation between  $\mathbf{a}$  and the  $d$ -decimation of  $\mathbf{b}$ ,  $\mathbf{b}^{(d)}$ .

*Proof.* According to the definition of crosscorrelation,

$$\begin{aligned} C_{\mathbf{a}, \mathbf{b}^{(d^{-1})}}(\tau) + 1 &= C_{f(x), g(x^{d^{-1}})}(\lambda) \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(\lambda x) + g(x^{d^{-1}})} \\ &= \sum_{y \in \mathbb{F}_2^n} (-1)^{f(\lambda^{-d^{-1}} y) + g(y^d)} \quad (\text{set } x = \lambda^{-1} y^d) \\ &= C_{f(x), g(x^d)}(\lambda^{-d^{-1}}). \end{aligned}$$

□

### 10.1.2 Signal Sets

We mentioned the concept of signal sets with low crosscorrelation toward the end of Section 5.1 of Chapter 5. Here we present it precisely.

**Definition 10.1** Let  $\mathbf{s}_j = (s_{j,0}, s_{j,1}, \dots, s_{j,v-1})$ ,  $0 \leq j < r$ , be  $r$  shift-distinct  $p$ -ary sequences of period  $v$ . Let  $S = \{\mathbf{s}_0, \mathbf{s}_1, \dots, \mathbf{s}_{r-1}\}$  and

$$\delta = \max |C_{\mathbf{s}_i, \mathbf{s}_j}(\tau)| \text{ for any } 0 \leq \tau < v, 0 \leq i, j < r \quad (10.8)$$

where  $\tau \neq 0$  if  $i = j$ . The set  $S$  is said to be a  $(v, r, \delta)$  signal set, and  $\delta$  is referred to as the maximum correlation of  $S$ . We say that the set  $S$  has low crosscorrelation if  $\delta \leq c\sqrt{v}$  where  $c$  is a constant.

A sequence in  $S$  is also called a *signal* from the point of view of engineering [157]. When we consider crosscorrelation between two sequences  $\mathbf{s}_i$  and  $\mathbf{s}_j$  in  $S$ , we simply write  $C_{i,j}(\tau)$  for  $C_{\mathbf{s}_i, \mathbf{s}_j}(\tau)$ . We also denote by  $C(S)$  the image of all the crosscorrelation functions of pairs of sequences in  $S$  and all the out-of-phase autocorrelation functions of sequences in  $S$ , i.e.,

$$\boxed{C(S) \text{ is the set consisting of all distinct values in } \{C_{\mathbf{s}_i, \mathbf{s}_j}(\tau) \mid 0 \leq \tau < v, 0 \leq i, j < r, \tau \neq 0 \text{ if } i = j\}.} \quad (10.9)$$

Thus,  $\delta = \max_{c \in C(S)} |c|$ . Sometimes, we refer to  $C(S)$  as an *image of the correlation of  $S$* .

**Remark 10.1** The maximum correlation between any pair of the sequences in  $S$  is lower-bounded, approximately, by the square root of the length of the sequences. (This was established by Welch in 1971 [184].)

**Example 10.2** Let  $\mathbf{a}$  and  $\mathbf{b}$  be shift-distinct  $m$ -sequences of period 7, say

$$\mathbf{a} = 1110100 \text{ and } \mathbf{b} = 1001011.$$

Let

$$\mathbf{s}_j = L^j(\mathbf{a}) + \mathbf{b}, 0 \leq j < 7,$$

and  $S = \{\mathbf{a}, \mathbf{b}\} \cup \{\mathbf{s}_j | 0 \leq j < 7\}$ . We may compute the sequences in  $S$  as follows.

		$S$	
		$\mathbf{b} =$	1001011
		$\mathbf{a} =$	1110100
$\mathbf{a} =$	1110100	$\mathbf{a} + \mathbf{b} =$	0111111
$L(\mathbf{a}) =$	1101001	$L(\mathbf{a}) + \mathbf{b} =$	0100010
$L^2(\mathbf{a}) =$	1010011	$L^2(\mathbf{a}) + \mathbf{b} =$	0011000
$L^3(\mathbf{a}) =$	0100111	$L^3(\mathbf{a}) + \mathbf{b} =$	1101100
$L^4(\mathbf{a}) =$	1001110	$L^4(\mathbf{a}) + \mathbf{b} =$	0000101
$L^5(\mathbf{a}) =$	0011101	$L^5(\mathbf{a}) + \mathbf{b} =$	1010110
$L^6(\mathbf{a}) =$	0111010	$L^6(\mathbf{a}) + \mathbf{b} =$	1110001

Then all the sequences in  $S$  are shift-distinct. Since both  $\mathbf{a}$  and  $\mathbf{b}$  are  $m$ -sequences with the constant-on-cosets property, the image  $C(S)$  of the correlation of  $S$  can be determined by the weight distribution of the sequences in  $\{L^j(\mathbf{a}) + \mathbf{b} | j = 0, 1, 3\} \cup \{\mathbf{a}, \mathbf{b}\}$ . There are three different values for weights of the sequences in this set, i.e., 6, 2, and 4. Thus  $C(S) = \{-1, -5, 3\}$ . Therefore, we have  $\delta = 5$  and  $S$  is a  $(7, 9, 5)$  signal set.

### 10.1.3 Signal Sets from Pairs of Sequences

Assume that  $\mathbf{a}$  and  $\mathbf{b}$  are binary sequences, where the period of  $\mathbf{a}$  is  $v = 2^n - 1$  and the period of  $\mathbf{b}$  is  $t$  with  $t|v$ . If  $S$  is constructed by

$$S = \{\mathbf{s}_j | 0 \leq j < t\} \cup \{\mathbf{a}, \mathbf{b}\}, \mathbf{s}_j = L^j(\mathbf{a}) + \mathbf{b}, \tag{10.10}$$

then  $C(S)$ , the image of the correlation of  $S$ , are determined by the following formulae:

$$C_{i,j}(\tau) = \langle L^\tau(\mathbf{s}_i), \mathbf{s}_j \rangle = \langle L^{\tau+i}(\mathbf{a}) + L^j(\mathbf{a}, \mathbf{b}) + L^\tau(\mathbf{b}) \rangle, \quad (10.11)$$

or equivalently

$$C_{i,j}(\tau) + 1 = \sum_{x \in \mathbb{F}_q} \omega^{f(\alpha^{\tau+i}x) + f(\alpha^jx) + g(\alpha^\tau x) + g(x)}, \quad (10.12)$$

and

$$C_{\mathbf{a},\mathbf{b}}(\tau), C_{\mathbf{a},\mathbf{s}_j}(\tau), C_{\mathbf{b},\mathbf{s}_j}(\tau), C_{\mathbf{a}}(\tau), \text{ and } C_{\mathbf{b}}(\tau). \quad (10.13)$$

(Here  $i$  and  $j$  may be equal.) Let  $f_j(x) = f(\alpha^jx) + g(x)$ . Then this is the trace representation of  $\mathbf{s}_j$ ,  $0 \leq j < t$ . Thus, (10.12) becomes

$$C_{i,j}(\tau) + 1 = C_{f_i, f_j}(\alpha^\tau).$$

This is just the crosscorrelation of the functions  $f_i$  and  $f_j$ . In particular, for the following two cases, we can reduce the computation of the correlation of  $S$  dramatically.

**Case 1.** One of the sequences  $\mathbf{a}$  and  $\mathbf{b}$  is an  $m$ -sequence of period  $2^n - 1$ . We may assume that  $\mathbf{a}$  is an  $m$ -sequence of period  $2^n - 1$  with the trace representation  $f(x) = \text{Tr}(x^r)$  where  $\gcd(r, 2^n - 1) = 1$ . Thus, the correlation of  $S$  reduces to computing

$$\Delta(\lambda, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x^r) + g(\beta x) + g(x)} \quad (10.14)$$

where  $\lambda = 0$  or  $\lambda = \alpha^i, \forall i \in \Gamma_2(n)$ , the set of the coset leaders modulo  $2^n - 1$ , and for all  $\beta \in \mathbb{F}_{2^n}$ .

**Case 2.** Both  $\mathbf{a}$  and  $\mathbf{b}$  are  $m$ -sequences. We may assume that  $f(x) = \text{Tr}(x)$  and  $g(x) = \text{Tr}(x^d)$ . (Note. Since the period  $t$  of  $\mathbf{b}$  could be a proper factor of  $2^n - 1$ , then  $d$  may not be coprime to  $2^n - 1$ . In other words,  $\mathbf{b}$  could be an  $m$ -sequence of degree  $m$  for which  $m|n$ .) In this case, computation of the correlation

of  $S$  can be further reduced to the computation of the crosscorrelation of the pair  $\mathbf{a}$  and  $\mathbf{b}$ , or the Hadamard transform of  $g(x)$ , since  $f(x) = Tr(x)$ . In other words, we have

$$\begin{aligned} C(S) &\subset \{C_{\mathbf{a},\mathbf{b}}(\tau) | \tau \in \Gamma_2(n)\} \cup \{-1\} \\ &= \{\widehat{g}(\lambda) - 1 | \lambda = \alpha^\tau, \tau \in \Gamma_2(n)\} \cup \{-1\}. \end{aligned} \quad (10.15)$$

We consolidate the above discussions into the following property.

**Property 10.5** *Let  $S$  be constructed by (10.10).*

1. *The image of the crosscorrelation of  $S$ ,  $C(S)$ , can be determined by (10.11) or (10.12) together with (10.13).*
2. *In particular, if one of  $\mathbf{a}$  and  $\mathbf{b}$  is an  $m$ -sequence of period  $2^n - 1$ , or if both of them are  $m$ -sequences, then their respective images of correlation can be computed by (10.14) or (10.15), respectively.*

For the case that both sequence are  $m$ -sequences, using Property 10.5 together with Property 10.3, the prototypes of  $C(S)$  are determined by the weight distribution of the sequences in  $S$ . Thus, to compute  $C(S)$ , it suffices to compute the weight distribution of the sequences in  $S$ . For example, the values of the weight of the sequences in  $S$  in Example 10.1 belong to  $\{2, 4, 6\}$ . Thus  $C(S)$  can be computed from these values using Property 10.3.

**Example 10.3** For  $n = 5$  and  $n = 7$ , let  $\mathbf{a} \leftrightarrow Tr(x)$  and  $\mathbf{b} \leftrightarrow f(x) = Tr(x^d)$  where  $\gcd(d, 2^n - 1) = 1$ . Since both  $\mathbf{a}$  and  $\mathbf{b}$  are  $m$ -sequences, according to Property 10.5, we only need to compute  $C_{\mathbf{a},\mathbf{b}}(\tau) = \widehat{f}(\alpha^\tau) - 1, \forall \tau \in \Gamma_2(n)$  where  $n = 5$  or  $n = 7$ , as shown in Tables 10.2 and 10.3.

**Case 1.**  $n = 5$ . We have

$$C_{\mathbf{a},\mathbf{b}}(\tau) \in \{-1, -1 \pm 8\}, \text{ for } d = 3, 5, 7, \text{ and } 11$$

and

$$C_{\mathbf{a},\mathbf{b}}(\tau) \in \{-1, -1 \pm 8, -1 \pm 4, -1 + 12\}, \text{ for } d = 15.$$

Table 10.2:  $n = 5$ ,  $\alpha^5 + \alpha^3 + 1 = 0$ , and  $f(x) = Tr(x^d)$ 

$d$	$\widehat{f}(\lambda), \lambda = \alpha^\tau$						
	0	1	3	5	7	11	15
3	-8	0	0	-8	8	8	0
5	-8	0	0	8	-8	8	0
7	-8	0	8	0	8	0	-8
11	-8	-8	0	8	0	0	8
15	12	8	-8	4	4	-4	0

**Case 2.**  $n = 7$ . We have

$$C_{\mathbf{a}, \mathbf{b}}(\tau) \in \{-1, -1 \pm 16\}, \text{ for } d \in \{3, 5, 9, 11, 13, 15, 23, 27, 29, 43\}. \quad (10.16)$$

**Example 10.4** Let  $\mathbf{a}$  and  $\mathbf{b}$  be the  $m$ -sequence and the quadratic sequence in Example 9.11 in Section 9.4, i.e.,

$$\begin{aligned} \mathbf{a} &= 1000010101110110001111100110100 \leftrightarrow f(x) = Tr(x) \\ \mathbf{b} &= 1001001000011101010001111011011 \leftrightarrow g(x) = Tr(x + x^5 + x^7) \end{aligned}$$

where  $a_i = Tr(\alpha^i)$  and  $b_i = g(\alpha^i)$  where  $\alpha^5 + \alpha^3 + 1 = 0$ . Let

$$S = \{\mathbf{s}_j = L^j(\mathbf{a}) + \mathbf{b} \mid 0 \leq j < 31\} \cup \{\mathbf{a}, \mathbf{b}\}.$$

From Property 10.5, the prototype of  $C(S)$  is determined by

$$\Delta(\lambda, \beta) = \sum_{x \in \mathbb{F}_{2^5}} (-1)^{Tr(\lambda x) + g(\beta x) + g(x)}$$

where  $\lambda = 0$  or  $\lambda = \alpha^i, \forall i \in \Gamma_2(5)$ , the set of all the coset leaders modulo 31, and  $\forall \beta \in \mathbb{F}_{2^5}$ . Since there are 7 coset leaders modulo 31, we need to compute  $8 \times 32 = 256$  inner products of vectors of length 31. Note that if  $\lambda = 0$ , then  $\Delta(0, \beta)$  is the autocorrelation of  $g(x)$ , which is equal to 0 if  $\beta \neq 1$ . Thus, we only need to compute  $\Delta(\alpha^i, \alpha^j)$ , for all  $i \in \Gamma_2(5) = \{0, 1, 3, 5, 7, 11, 15\}$  and  $j$  with  $0 \leq i < 31$ . These values are shown in Table 10.4. Thus, we obtain

$$C(S) = \{-1, -1 \pm 8, -1 \pm 16\} \implies \delta = 17.$$

Therefore,  $S$  is a  $(31, 33, 17)$  signal set.

Table 10.3:  $n = 7$ ,  $\alpha^7 + \alpha + 1 = 0$ , and  $f(x) = \text{Tr}(x^d)$

$d$	$\widehat{f}(\lambda), \lambda = \alpha^i$																		
	0	1	3	5	7	9	11	13	15	19	21	23	27	29	31	43	47	55	63
3	16	0	0	0	16	0	0	16	0	-16	-16	0	-16	0	-16	16	16	0	16
5	16	0	0	0	16	0	0	-16	0	-16	-16	0	16	0	16	16	16	0	-16
7	-40	0	-16	0	-8	16	0	-8	-16	24	8	16	-8	0	8	8	-8	0	8
9	16	0	0	0	16	0	0	-16	0	16	16	0	-16	0	-16	16	16	0	-16
11	16	0	16	16	16	-16	0	16	0	0	-16	0	0	-16	16	0	-16	0	0
13	16	0	0	16	-16	16	0	0	0	16	0	-16	0	0	-16	0	16	-16	16
15	16	16	16	-16	0	-16	-16	0	0	0	0	0	-16	16	16	16	0	0	0
19	-40	0	16	0	-8	-16	0	-8	-16	-8	8	16	24	0	8	8	-8	0	8
21	-40	0	-16	0	-8	0	0	8	0	8	8	-16	24	16	-8	-8	-8	16	8
23	16	16	0	0	0	0	0	0	16	-16	16	-16	16	0	16	0	-16	-16	0
27	16	-16	0	-16	0	0	-16	0	16	16	0	16	0	16	0	-16	0	0	16
29	16	0	0	-16	16	16	16	16	-16	16	0	0	0	0	0	-16	-16	0	0
31	-40	-16	0	0	8	24	0	16	-8	-16	8	0	8	-8	16	0	-8	8	-8
43	16	-16	16	0	0	-16	16	-16	16	0	0	-16	0	0	0	16	0	0	16
47	-40	0	-16	-8	-8	8	0	16	16	8	0	8	0	-16	-8	0	24	8	-8
55	-40	16	-8	8	8	-8	-16	-8	0	0	8	0	0	-8	24	-16	8	16	0
63	12	0	-8	16	-12	-8	16	20	-8	4	12	8	4	0	12	-20	4	-16	-4

Table 10.4: Evaluation of  $\Delta(\alpha^i, \alpha^j)$

$i$	0	1	3	5	7	11	15	$i$	0	1	3	5	7	11	15
$j$								$j$							
0	0	0	0	0	0	0	0	16	0-8	0-8	0	0	0-8		
1	0	0	0	8	0	8	0	17	8	0	0	0	0	8	8
2	0	8	0	0-8	0	0	0	18	0	0	8	8-8	0	0	0
3	8	8	8	0	0	8-8		19	8	8	8	8	0	0	8
4	0	8	0	0	16	8-8		20	0	0-8	0	8	8	0	
5	0	0	8-8	0	8	8		21	-8	0	0	0-8	8	0	
6	8	0-8	8-8	8	0	8		22	-8	0	0	8	0	8	8
7	8	0-8	8	8	0	8		23	0	8	0	0	0	0-8	
8	0	8	0	0	8	0	0	24	8	0	8	0	0	0	0
9	0	0	0	0	0	8	0	25	8-8	0	0	8	-8-8		
10	0-16	0	8	0	0	0	0	26	-8	8	0	8	0-16	0	
11	-8	8	0-8	0	0	0	0	27	0	0	16-8	8	-8	8	
12	8	8-8	0	0-8	8			28	8	0	0	8	0	0-8	
13	-8	0	8	8	0	0	0	29	0	0	0-8	0	0	0	0
14	8	0	0	0-8	0	0	0	30	0-8	8	0	8	0	8	
15	0	0	0	8	0	0	0								

### 10.1.4 One-to-one Correspondence between Sequences and Boolean Functions

In Section 6.4, we introduced the one-to-one correspondence between sequences and polynomial functions in terms of the trace representations of the sequences. Here, we revisit this relation and extend it to boolean functions. Recall that we introduced the notation:  $\mathcal{S}_2$ , the set of all binary sequences with period  $N|(2^n - 1)$ ; and  $\mathcal{F}_2$ , the set of all (polynomial) functions from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ .

A *boolean function* is a function of  $n$  variables from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ . An algebraic normal form of a boolean function of  $n$  variables is given by

$$g(x_0, \dots, x_{n-1}) = \sum a_{i_1, \dots, i_t} x_{i_1} \cdots x_{i_t}, a_{i_1, \dots, i_t} \in \mathbb{F}_2 \tag{10.17}$$

where the sum runs through all the  $t$ -subsets  $\{i_1, \dots, i_t\} \subset \{0, 1, \dots, n-1\}$ . The *degree* of the boolean function  $g$  is the largest  $t$  for which  $a_{i_1, \dots, i_t} \neq 0$ . We now denote by  $\mathcal{B}_2$  the set of all boolean functions of  $n$  variables. We will establish

that there exist one-to-one correspondences among these three sets:

$$\mathcal{S}_2 \leftrightarrow \mathcal{F}_2 \leftrightarrow \mathcal{B}_2.$$

We have seen the one-to-one correspondence between  $\mathcal{S}_2$  and  $\mathcal{F}_2$ , i.e., the sequences and the polynomial functions in Chapter 6. Applying the Lagrange interpolation formula to a given boolean function  $g(x_0, \dots, x_{n-1}) \in \mathcal{B}_2$  (see (6.3) in Sec. 6.4), we can determine its polynomial representation  $f(x)$  as follows:

$$\boxed{\begin{aligned} f(x) &= \sum_{i=0}^{2^n-1} d_i x^i, \quad \text{where} \\ d_i &= \sum_{x \in \mathbb{F}_2^n} [g(x_0, \dots, x_{n-1}) - g(0, \dots, 0)] x^{-i}, \quad x = \sum_{i=0}^{n-1} x_i \alpha_i \end{aligned}} \quad (10.18)$$

Next, we will show how to obtain a boolean representation from a polynomial representation of a function from  $\mathbb{F}_{2^n}$  to  $\mathbb{F}_2$  in terms of the linear space structure of the finite field  $\mathbb{F}_{2^n}$ . Let  $\{\alpha_0, \dots, \alpha_{n-1}\}$  be a basis of  $\mathbb{F}_{2^n}$  over  $\mathbb{F}_2$ , denoted by  $\mathbb{F}_{2^n} = \langle \alpha_0, \dots, \alpha_{n-1} \rangle$ , and let  $\alpha$  be a primitive element of  $\mathbb{F}_{2^n}$ . For any  $x \in \mathbb{F}_{2^n}$ , we can represent  $x$  as

$$\rho : x = x_0 \alpha_0 + x_1 \alpha_1 + \dots + x_{n-1} \alpha_{n-1} \leftrightarrow \mathbf{x} = (x_0, \dots, x_{n-1}), \quad x_i \in \mathbb{F}_2.$$

Thus  $\rho$  is an isomorphism between  $\mathbb{F}_{2^n}$  and  $\mathbb{F}_2^n$ . Hence, for  $f(x) \in \mathcal{F}$ , we have

$$f(x) = f \left( \sum_{i=0}^{n-1} x_i \alpha_i \right) = g(x_0, \dots, x_{n-1}),$$

i.e.,

$$\kappa_\rho : f(x) \rightarrow g(x_0, \dots, x_{n-1}) \quad (10.19)$$

which is a bijective map from  $\mathcal{F}_2$  to  $\mathcal{B}_2$  induced by  $\rho$ . Therefore, a conversion from a polynomial function to a boolean function is given by

$$\boxed{\begin{aligned} g(x_0, \dots, x_{n-1}) &= f \left( \sum_{i=0}^{n-1} x_i \alpha_i \right), \quad \text{where} \\ \mathbb{F}_{2^n} &= \langle \alpha_0, \dots, \alpha_{n-1} \rangle \end{aligned}} \quad (10.20)$$

The boolean function  $g(x_0, x_1, \dots, x_{n-1})$  has degree  $r$  where  $r$  is the maximum Hamming weight  $w(k)$  as  $k$  runs through all the exponents in the trace terms of  $f$ . This value is also called the *algebraic degree of  $f(x)$* .

Thus (10.18) gives a bijective map from  $\mathcal{B}_2$  to  $\mathcal{F}_2$  which is the inverse of (10.20). These one-to-one correspondences among those sets are shown in Figure 10.1.

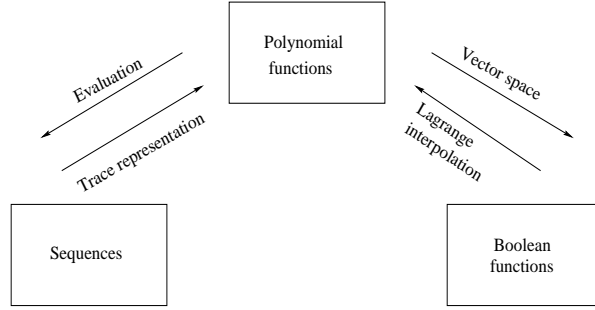


Figure 10.1: One-to-one correspondences among  $\mathcal{S}_2$ ,  $\mathcal{F}_2$  and  $\mathcal{B}_2$

**Example 10.5** Let  $n = 3$ ,  $\mathbb{F}_{2^3}$  defined by the primitive polynomial  $t(x) = x^3 + x + 1$ , and  $\alpha$  a root of  $t(x)$  in  $\mathbb{F}_{2^3}$ . Thus  $\{1, \alpha, \alpha^2\}$  is a basis for  $\mathbb{F}_{2^3}$  over  $\mathbb{F}_2$ . Let  $f(x) = Tr(x^3)$ . Then this is the trace representation of the  $m$ -sequence  $\mathbf{a} = 1110100$ . For any  $x \in \mathbb{F}_{2^3}$ , we write  $x = x_0 + x_1\alpha + x_2\alpha^2$ . From the conversion formula (10.20),

$$\begin{aligned} f(x) &= Tr(x^3) = Tr((x_0 + x_1\alpha + x_2\alpha^2)^3) \\ &= Tr(x_0 + x_1 + x_2 + x_1x_2) + Tr((x_1 + x_0x_1 + x_0x_2)\alpha) + Tr((x_0x_1 + x_2)\alpha^2) \\ &= (x_0 + x_1 + x_2 + x_1x_2) + (x_1 + x_0x_1 + x_0x_2)Tr(\alpha) + (x_0x_1 + x_2)Tr(\alpha^2) \\ &= x_0 + x_1 + x_2 + x_1x_2. \end{aligned}$$

The last identity is obtained by noting that  $Tr(\alpha) = Tr(\alpha^2) = 0$ . Therefore, we have the following one-to-one correspondences:

$$\mathbf{a} = 1110100 \leftrightarrow Tr(x^3) \leftrightarrow x_0 + x_1 + x_2 + x_1x_2.$$

### 10.1.5 Walsh Transform of Boolean Functions

**Definition 10.2** The Walsh transform of a boolean function  $f$  is defined by

$$\hat{f}(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{w} \cdot \mathbf{x} + f(\mathbf{x})}, \quad \mathbf{w} \in \mathbb{F}_2^n. \quad (10.21)$$

(Here we omit the bracket for the dot product of  $\mathbf{w}$  and  $\mathbf{x}$  for simplicity.)

In the following, we will derive a conversion between the Walsh transforms of boolean functions and the Hadamard transforms of their corresponding polynomial functions. We denote by  $a(\mathbf{x}) = \mathbf{w} \cdot \mathbf{x} = \sum_{i=0}^{n-1} w_i x_i$ , a linear boolean

function, where  $\mathbf{w} = (w_0, w_1, \dots, w_{n-1}) \in \mathbb{F}_2^n$ , a constant vector. Let  $f(x)$  and  $a(x)$  be the polynomial representations of  $f(\mathbf{x})$  and  $a(\mathbf{x})$ , respectively. (We will use the same notation for both boolean functions and their corresponding polynomial forms when the context is clear.) The following property is immediate.

**Property 10.6 (a)** *There exists some  $\lambda \in \mathbb{F}_{2^n}$  such that*

$$a(\mathbf{x}) = Tr(\lambda x). \quad (10.22)$$

**(b)** *The Hadamard transform of  $f(x)$  and the Walsh transform of  $f(\mathbf{x})$  have the following relation:*

$$\widehat{f}(\mathbf{w}) = \widehat{f}(\lambda), \mathbf{w} \in \mathbb{F}_2^n, \lambda \in \mathbb{F}_{2^n} \quad (10.23)$$

where  $\mathbf{w} \cdot \mathbf{x} = Tr(\lambda x)$ .

□

For example, with  $\alpha$  in Example 10.5, using  $Tr(\alpha^{2^i}) = 0$  and  $Tr(\alpha^{3 \cdot 2^i}) = 1$ ,  $i = 0, 1, 2$ , we have

$$\begin{aligned} Tr(x) &= Tr(x_0 + x_1\alpha + x_2\alpha^2) \\ &= x_0Tr(1) + x_1Tr(\alpha) + x_2Tr(\alpha^2) \\ &= x_0, \\ Tr(\alpha^3 x) &= Tr(x_0\alpha^3 + x_1\alpha^4 + x_2\alpha^5) \\ &= x_0Tr(\alpha^3) + x_1Tr(\alpha^4) + x_2Tr(\alpha^5) \\ &= x_0 + x_2. \end{aligned}$$

## 10.2 Odd Case: Gold-pair Signal Sets and Their Generalization

In this section, we introduce the Gold-pair construction and its generalization to binary signal sets with parameters  $(2^n - 1, 2^n + 1, 2^{(n+1)/2} + 1)$  where  $n$  is odd. We keep the notation that  $n = 2m + 1$ , an odd number, and  $\alpha$  is a primitive element in  $\mathbb{F}_{2^n}$ .

### 10.2.1 Gold-pair Construction

**Construction:** Select  $d$  from the following list:

- (a)  $d = 2^k + 1$  (the Gold decimation),  $\gcd(k, n) = 1$  and  $k \leq \frac{n-1}{2}$ .
- (b)  $d = 2^{2k} - 2^k + 1$  (the Kasami (large set) decimation),  $\gcd(k, n) = 1$  and  $k \leq \frac{n-1}{2}$ .
- (c)  $d = 2^{\frac{n-1}{2}} + 3$  (the Welch decimation).
- (d)  $d = 2^{2k} + 2^k - 1$  (the Niho decimation) where

$$k = \begin{cases} \frac{n-1}{4} & \text{if } n \equiv 1 \pmod{4} \\ \frac{3n-1}{4} & \text{if } n \equiv 3 \pmod{4} \end{cases}.$$

- (e) Inverse of  $d$ , for  $d$  in each of the above four cases.

For  $0 \leq j < 2^n - 1$ , let  $\mathbf{s}_j = \{s_{j,i}\}$  be a binary sequence whose elements are given by

$$s_{j,i} = \text{Tr}(\alpha^j \alpha^i + \alpha^{di}), i = 0, 1, \dots, 2^n - 2.$$

Then  $\mathbf{s}_j$  is called a *Gold-pair sequence*. Let  $\mathbf{s}_{2^n-1} = \mathbf{a} = \{\text{Tr}(\alpha^i)\}$  and  $\mathbf{s}_{2^n} = \mathbf{b} = \mathbf{a}^{(d)}$ . The set given by

$$S(d) = \{\mathbf{s}_j \mid 0 \leq j \leq 2^n\}$$

is said to be a *Gold-pair (signal) set*.

Note that both  $\mathbf{a}$  and  $\mathbf{b}$  are  $m$ -sequences, and  $\mathbf{s}_j$  is a sum of  $\mathbf{a}$  at shift  $j$  and  $\mathbf{b}$  for  $0 \leq j < 2^n - 1$ , i.e.,

$$\mathbf{s}_j = L^j \mathbf{a} + \mathbf{b}, 0 \leq j < 2^n - 1.$$

Thus  $S(d)$  has  $2^n + 1$  shift-distinct sequences. Let  $f(x) = \text{Tr}(x^d)$ . According to Property 10.5, the prototype of crosscorrelation of  $S(d)$ , i.e.,  $C(S(d))$ , is determined by  $C_{\mathbf{a},\mathbf{b}}(\tau)$  where  $\tau$  runs through  $\Gamma_2(n)$ , the set of all the coset leaders modulo  $2^n - 1$ . In other words, we have

$$C(S(d)) \subset \{\widehat{f}(\lambda) - 1 \mid \lambda = \alpha^\tau, \tau \in \Gamma_2(n)\}.$$

In the following, we show how to compute  $C_{\mathbf{a},\mathbf{b}}(\tau)$ , or equivalently,  $\widehat{f}(\lambda)$ , for the original Gold case  $d = 2^k + 1$ .

**Theorem 10.1 (Gold, 1967)** *Let  $n$  be odd and  $d = 2^k + 1$  with  $\gcd(k, n) = 1$ .*

*Then*

$$\widehat{f}(\lambda) = C_{\mathbf{a}, \mathbf{b}}(\tau) + 1 = \begin{cases} 0 & \iff Tr(\lambda) = 0 \\ \pm 2^{(n+1)/2} & \iff Tr(\lambda) = 1 \end{cases}$$

where  $\lambda = \alpha^\tau \in \mathbb{F}_{2^n}$ .

*Proof.* Here we present a proof given by L. Welch instead of the original proof of Gold. Welch's proof is unpublished, but it is well-known as the squaring method. Note that

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_q} (-1)^{Tr(\lambda x) + Tr(x^d)} \quad (\text{set } q = 2^n), \quad (10.24)$$

and by squaring (10.24), we have

$$\widehat{f}^2(\lambda) = \sum_{x, w \in \mathbb{F}_q} (-1)^{Tr(\lambda x) + Tr(\lambda(x+w)) + Tr(x^d) + Tr((x+w)^d)}.$$

Substituting  $d = 2^k + 1$ , and then using the trace function identity  $Tr(wx^{2^k}) = Tr(w^{2^{-k}}x)$ , we get

$$\begin{aligned} \widehat{f}^2(\lambda) &= \sum_{x, w \in \mathbb{F}_q} (-1)^{Tr(\lambda w) + Tr(w^d) + Tr(x^{2^k} w + x w^{2^k})} \\ &= \sum_{w \in \mathbb{F}_q} (-1)^{h(w)} \sum_{x \in \mathbb{F}_q} (-1)^{Tr((w^{2^{-k}} + w^{2^k})x)} \\ &\quad (\text{set } h(w) = Tr(\lambda w) + Tr(w^d)) \\ &= 2^n \sum_{w \in L} (-1)^{h(w)} \end{aligned}$$

where

$$L = \{w \in \mathbb{F}_q \mid w^{2^{-k}} + w^{2^k} = 0\}.$$

Since  $\gcd(2k, n) = \gcd(k, n) = 1$ , we have

$$\begin{aligned} w^{2^{-k}} + w^{2^k} = 0 &\implies w^{2^{-k}} = w^{2^k} \implies w^{2^{2k}} = w \\ &\implies w \in \mathbb{F}_{2^{2k}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^{\gcd(2k, n)}} = \mathbb{F}_2 \implies L = \mathbb{F}_2. \end{aligned}$$

Notice that  $h(0) = 0$  and  $h(1) = Tr(\lambda) + 1 \in \{0, 1\}$ . Therefore

$$\widehat{f}^2(\lambda) = 2^n \sum_{w \in \mathbb{F}_2} (-1)^{h(w)} = 2^n \left(1 + (-1)^{Tr(\lambda) + 1}\right). \quad (10.25)$$

If  $Tr(\lambda) + 1 = 1 \implies Tr(\lambda) = 0, \lambda \in \mathbb{F}_q$ , then (10.25) gives  $\widehat{f}^2(\lambda) = 0$ . Hence

$$\widehat{f}(\lambda) = 0 \iff Tr(\lambda) = 0. \quad (10.26)$$

If  $Tr(\lambda) + 1 = 0, \lambda \in \mathbb{F}_1 \implies Tr(\lambda) = 1$ , then

$$\widehat{f}^2(\lambda) = 2^n(1+1) = 2^{n+1} \implies \widehat{f}(\lambda) = \pm 2^{(n+1)/2}.$$

Therefore,

$$\widehat{f}(\lambda) = \pm 2^{(n+1)/2} \iff Tr(\lambda) = 1. \quad (10.27)$$

The assertion follows from (10.26) and (10.27). □

**Corollary 10.1** *We use the same notation as in the Gold-pair construction where  $f(x) = Tr(x^d)$  ( $n = 2m + 1$ ).*

1.  $S(d)$  is a  $(2^n - 1, 2^n + 1, 2^{m+1} + 1)$  signal set.
2. The crosscorrelation of any pair of sequences in  $S(d)$  or out-of-phase autocorrelation of any sequence in  $S$  is 3-valued, and belongs to the set  $\{-1, -1 \pm 2^{m+1}\}$ .
3. In  $\{\widehat{f}(\lambda) \mid \lambda \in \mathbb{F}_q\}$ , 0 occurs  $2^{n-1}$  times and  $\pm 2^{m+1}$  (combined) occurs  $2^{n-1}$  times. Precisely, the frequencies for these values are given by

$\widehat{f}(\lambda)$	frequency
0	$2^{n-1}$
$2^{m+1}$	$2^{n-2} + 2^{m-1}$
$-2^{m+1}$	$2^{n-2} - 2^{m-1}$

*Note.* For the Kasami exponent  $d$  with  $3k \equiv 1 \pmod{n}$ , the Hadamard transform of  $f(x) = Tr(x^d)$  has a result similar to Theorem 10.1, which appeared as identity 9.11 at the beginning of Section 9.3, when we discussed the Kasami power function construction of 2-level autocorrelation sequences.

Table 10.5: Exponents for the Gold-pair constructions

$n$	$k$	Gold exp. $d = 2^k + 1$	Inverse $d^{-1}$	Kasami exp. $d = 2^{2k} - 2^k + 1$	Inverse $d^{-1}$
5	1	3	11	$13 \in C_{11}$	3
	2	5	7		
7	1	3	43	13	11
	2	5	27	$57 \in C_{23}$	29
	3	9	15		
9	1	3	171	13	59
	2	5	103	$241 \in C_{47}$	87
	4	17	31		
11	1	3	683	13	315
	2	5	411	57	413
	3	9	231	$241 \in C_{143}$	43
	4	17	365		
	5	33	63	$993 \in C_{95}$	151

Table 10.6: Exponents for the Gold-pair constructions (cont.)

$n$	Welch exp. $d$ $2^{(n-1)/2} + 3$	Inverse $d^{-1}$	$k$	Niho exp. $d$ $2^{2k} + 2^k - 1$	Inverse $d^{-1}$
5	7	5	$\frac{n-1}{4} = 1$	5	7
7	11	13	$\frac{3n-1}{4} = 5$	$39 \in C_{29}$	23
9	19	27	$\frac{n-1}{4} = 2$	19	27
11	35	117	$\frac{3n-1}{4} = 8$	$287 \in C_{249}$	107

**Example 10.6** Let  $n \in \{5, 7, 9, 11\}$ . From the Gold-pair construction, we compute decimation values  $d$  for all cases, as shown in Tables 10.5 and 10.6. In these tables,  $C_i$  represents the coset containing the leader  $i$  modulo  $2^n - 1$ , and the columns under  $d^{-1}$  list the leaders of the cosets containing  $d^{-1}$  instead of  $d^{-1}$  itself. For the Kasami exponent, the case  $k = 1$  is omitted from the list of the Kasami exponents since  $2^{2k} - 2^k + 1 = 2^k + 1 = 2 + 1 = 3$  when  $k = 1$ , which degenerates to a Gold exponent. For each  $d$  in Table 10.5,  $S(d)$  is a signal set with the features shown below.

$n$	Parameters	$C(S(d))$	$\delta$
5	(31, 33, 9)	$\{-1, -9, 7\}$	9
7	(127, 129, 17)	$\{-1, -17, 15\}$	17
9	(511, 513, 33)	$\{-1, -33, 31\}$	33
11	(2047, 2049, 65)	$\{-1, -65, 63\}$	65

**Remark 10.2** For  $n = 5$  and 7, from Example 10.3, the exponents shown in Tables 10.5 and 10.6 are all the decimation sequences having 3-valued crosscorrelation with  $Tr(x)$ . In fact, the four cases of  $d$  in the Gold-pair construction are all the known cases whose cross-correlations with  $Tr(x)$  are 3-valued and belong to  $\{-1, -1 \pm 2^{m+1}\}$ . (No other examples have been found by computer search where decimation does not belong to one of these four cases or their inverses.)

## 10.2.2 Randomness Profile and Implementation

**The randomness profile of the Gold-pair construction ( $n = 2m + 1$ ):**

1. Each sequence has period  $2^n - 1$ .
2. There are  $2^n + 1$  shift-distinct sequences in  $S(d)$ .
3. Cross-correlation of any pair of sequences in  $S(d)$  or out-of-phase autocorrelation of any sequence in  $S(d)$  is 3-valued and belongs to  $\{-1, \pm 2^{m+1}\}$ . In other words, the image of the correlation of  $S(d)$  is given by  $C(S(d)) = \{-1, \pm 2^{m+1}\}$  for all  $d$  in the list.

- 4. Together with shift-equivalent sequences, from  $S(d)$  there are  $2^{2n} - 1$  different nonzero sequences.
- 5. There are  $2^{n-1} + 1$  balanced sequences in  $S(d)$ . In particular, for all the Gold exponents and one Kasami exponent, the balanced sequences can be determined by

$$\begin{aligned}
 & \mathbf{s}_j \text{ balanced} \\
 \iff & \begin{cases} Tr(\alpha^j) = 0 & \text{for the Gold case } d = 2^k + 1 \\ Tr(\alpha^{(2^k+1)j}) = 0 & \text{for the Kasami case } d = 2^{2k} - 2^k + 1 \\ & \text{where } 3k \equiv 1 \pmod{n}. \end{cases}
 \end{aligned}$$

Together with  $\mathbf{a}$ , this constitutes a total of  $2^{n-1} + 1$  balanced sequences.

- 6. Each sequence in  $S(d)$  has linear span  $2n$  except for  $\mathbf{a}$  and  $\mathbf{b}$  which have linear span  $n$ .
- 7. For a fixed  $\alpha$ , a primitive element of  $\mathbb{F}_q$ , the numbers of the Gold-pair signal sets for each type of  $d$  are given by

$n > 9$	Gold exp.	Kasami exp.	Welch exp.	Niho exp.	All inverses
	$\phi(n)/2$	$\phi(n)/2 - 1$	1	1	$\phi(n) + 1$
Total	$2\phi(n) + 2$				

In the following, we discuss the implementation of these signal sets.

**The LFSR Implementation:**

- 1. Select odd  $n$ , and  $t(x)$ , a primitive polynomial of degree  $n$  over  $\mathbb{F}_2$ , as the characteristic polynomial of LFSR1.
- 2. Select  $d$  from the construction, and compute the minimal polynomial of  $\alpha^d$  as the characteristic polynomial of LFSR2.
- 3. We obtain all the sequences in  $S$  by employing different initial states of LFSR1, as shown in Figure 10.2.

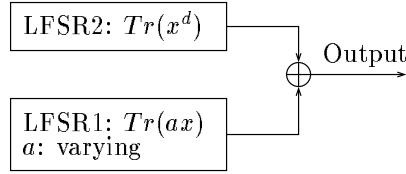


Figure 10.2: LFSR implementation of a Gold-pair generator

**Example 10.7** Design of a (31, 33, 9) Gold-pair signal set.

*Method 1. The LFSR implementation*

1. Select  $t(x) = x^5 + x^3 + 1$ , a primitive polynomial over  $\mathbb{F}_2$  of degree 5, as the characteristic polynomial of LFSR1.
2. Select  $d = 1 + 2^2 = 5$  and compute the minimal polynomial of  $\alpha^5$  where  $\mathbb{F}_{2^5}$  is defined by  $t(\alpha) = 0$ . This gives

$$v(x) = x^5 + x^4 + x^3 + x + 1.$$

Use  $v(x)$  as the characteristic polynomial of LFSR2.

3. Fixing the initial state of one of these two LFSRs and varying the other, we obtain all 33 sequences in  $S(5)$ , as shown in Figure 10.3.

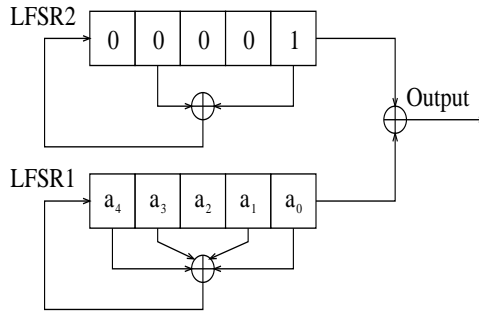


Figure 10.3: LFSR implementation of a (31, 33, 9) Gold-pair generator

*Method 2. Software implementation*

## 10.2. ODD CASE: GOLD-PAIR SIGNAL SETS AND THEIR GENERALIZATION 409

1. Select  $f(x) = x^5 + x^3 + 1$ , a primitive polynomial over  $\mathbb{F}_2$  of degree 5 to generate the sequence  $\mathbf{a}$ :

$$\mathbf{a} = 1000010101110110001111100110100.$$

2. Pick  $d = 1 + 2^2 = 5$  and perform the 5-decimation operation on  $\mathbf{a}$ . We obtain  $\mathbf{b} = \mathbf{a}^{(5)} = \{b_i\}$  where  $b_i = a_{5i}$ , as shown below

$$\mathbf{b} = 1110110011100001101010010001011.$$

3. Compute

$$\mathbf{s}_i = L^i(\mathbf{a}) + \mathbf{b}, 0 \leq i < 31.$$

Together with  $\mathbf{a}$  and  $\mathbf{b}$ , there are 33 sequences in  $S(5)$  which are presented in Table 10.7.

*Randomness profile of  $S(5)$ :*

1. Period 31.
2. There are 33 shift-distinct sequences in  $S(5)$ .
3. Cross-correlation of any two sequences in  $S$  and out-of-phase autocorrelation of any sequence in  $S$  takes the three values:  $-1, -9$ , and  $7$ .
4.  $S(5)$  is a  $(31, 33, 9)$  signal set.
5. There are 17 balanced sequences in  $S(5)$ , including  $\mathbf{a}$ ,  $\mathbf{b}$  and those framed indices in Table 10.7, i.e.,  $\mathbf{s}_i$  is balanced for  $i \in C_1 \cup C_3 \cup C_{15}$ . The other 16 sequences have their respective weights either 12 or 20.
6. Linear span 10 except for  $\mathbf{a}$  and  $\mathbf{b}$ , which have linear span 5.

### 10.2.3 Generalization of the Gold-Pair Construction

**Construction** ( $n = 2m + 1$ ): Let

$$T = \{g(x) + Tr_1^n(\beta x), \beta \in \mathbb{F}_{2^n}\} \cup \{Tr_1^n(x)\}, \quad (10.28)$$

Table 10.7:  $s_i$  in  $(31, 33, 9)$  signal set

$i$	$s_i$
0	0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 1 1 0 0 1 0 1 1 1 0 1 1 1 1 1 1
1	1 1 1 0 0 1 1 0 0 0 0 0 1 1 0 1 1 1 0 1 0 1 0 1 1 1 1 0 0 0 1 0
2	1 1 1 1 1 0 0 1 0 0 1 1 1 0 0 1 0 1 0 1 0 0 0 0 1 0 1 1 1 0 0 1
3	1 1 0 0 0 1 1 1 0 1 0 1 0 0 0 0 0 1 0 1 1 0 1 0 0 1 0 1 1 1 1
4	1 0 1 1 1 0 1 1 1 0 0 0 0 0 1 0 0 1 0 0 1 1 1 1 1 1 0 0 0 0 1 1
5	0 1 0 0 0 0 1 0 0 0 1 0 0 1 1 0 0 1 1 0 0 1 0 0 0 0 1 1 0 1 1
6	1 0 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 0 1 1 0 0 1 1 0 1 0 1 0 1 0
7	0 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 0 1 1 1 0 1 1 0 0 1 0 0 1
8	1 0 0 1 1 0 1 0 1 0 1 1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 1 0
9	0 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 1 0 1 1 1 1 0 1 1 0 0 0 0 0 0 1
10	0 0 1 1 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 1 1 0
11	0 1 0 1 1 1 0 1 0 0 0 1 0 0 1 0 1 1 1 0 0 0 0 1 0 1 0 0 0 0 0
12	1 0 0 0 1 1 1 1 0 0 0 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 1 1 1 1 0 0
13	0 0 1 0 1 0 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 0 0 0 0 1 0 0 1 0 1
14	0 1 1 0 0 0 1 1 0 1 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 0 1 1 0
15	1 1 1 1 0 0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 1 0 1 1 0 0 0 1 1 0 0 0
16	1 1 0 1 0 0 1 0 1 0 0 0 1 0 0 0 1 0 1 0 0 0 1 1 1 1 1 1 1 0 1
17	1 0 0 1 0 0 0 0 0 0 0 1 1 0 0 1 1 1 0 1 1 1 1 0 0 1 1 0 0 1 1 1
18	0 0 0 1 0 1 0 1 0 1 0 0 0 1 0 1 1 0 0 0 0 0 1 0 1 0 1 0 0 1 1
19	0 0 0 1 1 1 1 1 1 0 1 0 1 0 0 1 1 1 1 1 1 1 1 1 0 0 1 1 1 0 1 0
20	0 0 0 0 1 0 1 0 0 1 1 1 0 0 0 1 0 0 0 0 0 1 1 1 1 1 0 1 0 0 0
21	0 0 1 0 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1 1 0 1 0 0 1 0 0 1 1 0 0
22	0 1 1 1 0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0 0 0 0 1 0 0
23	1 1 0 1 1 0 0 0 0 1 1 0 0 1 0 0 1 1 0 1 1 1 1 1 0 0 1 0 1 0 0
24	1 0 0 0 0 1 0 1 1 1 1 0 1 0 1 1 0 1 0 0 0 1 0 1 0 1 1 0 1 0 1
25	0 0 1 1 1 1 1 0 1 1 1 1 0 1 0 0 0 1 1 1 0 0 0 1 1 1 1 0 1 1 1
26	0 1 0 0 1 0 0 0 1 1 0 0 1 0 1 0 0 0 0 1 1 0 0 0 1 1 1 0 0 1 0
27	1 0 1 0 0 1 0 0 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1 0 1 1 1 1 0 0 0
28	0 1 1 1 1 1 0 0 0 1 0 0 1 1 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1
29	1 1 0 0 1 1 0 1 1 0 1 1 1 1 0 0 0 0 1 0 0 1 1 0 1 0 0 0 1 1 0
30	1 0 1 0 1 1 1 0 0 1 0 1 1 1 0 1 0 1 0 1 1 0 1 1 0 0 0 1 0 0 0 1

and  $S(g)$  be the set consisting of sequences whose trace representations are functions in  $T$  (evaluated at  $\alpha$ ). If

$$g(x) = \sum_{i=1}^m \text{Tr}_1^{n_i}(x^{1+2^i})$$

where  $n_i|n$ , the size of the coset containing  $1 + 2^i$ , then  $S(g)$  is a  $(2^n - 1, 2^n + 1, 2^{m+1} + 1)$  signal set. Furthermore, crosscorrelation of any pair of the sequences in  $S(g)$  or out-of-phase autocorrelation of any sequence in  $S(g)$  is three-valued and belongs to  $\{-1, -1 \pm 2^{(n+1)/2}\}$ . (Boztas and Kumar, 1994.)

Together with the case  $g(x) = \text{Tr}(x^d)$  where  $d$  is taken from the Gold-pair construction, these are all the known constructions for  $(2^n - 1, 2^n + 1, 2^{(n+1)/2} + 1)$  signal sets for  $n$  odd.

**Example 10.8** Let  $n = 5$ , let  $\alpha$  be the primitive element in Example 10.7, and let  $g(x)$  be constructed via the above construction. Then  $g(x) = \text{Tr}(x^3 + x^5)$ . Let

$$\begin{aligned} a_i &= \text{Tr}(\alpha^i) \\ b_i &= g(\alpha^i), i = 0, 1, \dots, 30. \end{aligned}$$

Then

$$S(g) = \{L^i(\mathbf{a}) + \mathbf{b} \mid 0 \leq i < 31\} \cup \{\mathbf{a}, \mathbf{b}\}$$

forms a  $(31, 33, 9)$  signal set.

### 10.3 Even Case: Kasami (Small) Signal Sets and Their Generalization

In this section, we present constructions for binary signal sets with parameters  $(2^n, 2^{n/2}, 2^{n/2} + 1)$  where  $n$  is even. We use the following notation in this section:  $n = 2m$ ,  $q = 2^n$ ,  $\alpha$  a primitive element in  $\mathbb{F}_{2^n}$ ,  $v = 2^m - 1$ , and  $d = 2^m + 1$ .

### 10.3.1 Kasami (Small) Signal Sets

**Construction:** Let  $\mathbf{s}_\lambda = \{s_{\lambda,i}\}$  be a binary sequence whose elements are given by

$$s_{\lambda,i} = f_\lambda(\alpha^i), i = 0, 1, \dots, \text{ where} \quad (10.29)$$

$$f_\lambda(x) = \text{Tr}_1^m (\text{Tr}_m^n(x^2) + \lambda x^d), \lambda \in \mathbb{F}_{2^m}, x \in \mathbb{F}_{2^n}. \quad (10.30)$$

A signal set  $S$  consists of  $\mathbf{s}_\lambda$  for all  $\lambda \in \mathbb{F}_{2^m}$ , i.e.,

$$S = \{\mathbf{s}_\lambda \text{ such that } \lambda \in \mathbb{F}_{2^m}\}. \quad (10.31)$$

$\mathbf{s}_\lambda$  is said to be a *Kasami (small set) sequence* and  $S$  a *Kasami (small) signal set*. Note that  $f_\lambda(x)$  is the trace representation of  $\mathbf{s}_\lambda$ .

**Theorem 10.2 (Kasami, 1969)**  *$S$  is a  $(2^n, 2^m, 2^m + 1)(n = 2m)$  signal set. Moreover, the crosscorrelation of any pair of sequences in  $S$  or out-of-phase autocorrelation of any sequence in  $S$  is 3-valued and belongs to  $\{-1, -1 \pm 2^m\}$ .*

To prove Theorem 10.2, we first derive the interleaved structure for the sequences in  $S$ . This structure also gives a simple proof for the unbalanced property of the Kasami small set sequences in the next subsection. The following assertions, related to finite fields and trace functions, will be used in several places.

**Assertions:**

1.  $d^2 \equiv 2d \pmod{2^n - 1}$ .
2. Let  $\beta = \alpha^d$ . Then  $\beta$  is a primitive element in  $\mathbb{F}_{2^m}$ .
3. For any  $y \in \mathbb{F}_{2^m}, x \in \mathbb{F}_{2^n}, \text{Tr}_m^n(xy) = y\text{Tr}_m^n(x)$ .

We avoid using double subscripts by renaming the sequences in  $S$ . Thus, let  $\mathbf{u} = \{u_i\} = \mathbf{s}_\lambda \in S$ . For  $k = id + j, 0 \leq i < v, 0 \leq j < d$ ,

$$\begin{aligned} u_k = u_{id+j} &= \text{Tr}_1^m \left( \text{Tr}_m^n(\alpha^{2(id+j)}) + \lambda \alpha^{d(id+j)} \right) \\ &= \text{Tr}_1^m \left( \alpha^{2di} \text{Tr}_m^n(\alpha^{2j}) + \lambda \alpha^{2di} \alpha^{dj} \right) \quad (\text{ by Assertions 1 - 3 }) \\ \implies u_{id+j} &= \text{Tr}_1^m(\beta^{2i} t_j(\lambda)) \end{aligned}$$

where

$$t_j(\lambda) = \text{Tr}_m^n(\alpha^{2j}) + \lambda\alpha^{dj}, \lambda \in \mathbb{F}_{2^m}. \quad (10.32)$$

Thus, we have established the following result.

**Lemma 10.1** For  $\mathbf{u} = \{u_i\} = \mathbf{s}_\lambda \in S$ ,

$$u_{id+j} = \text{Tr}_1^m(\beta^{2i}t_j), 0 \leq i < v, 0 \leq j < d$$

where  $t_j = t_j(\lambda)$  is defined in (10.32). Thus  $\mathbf{s}_\lambda$  is a  $(v, d)$  interleaved sequence with the base sequence  $\mathbf{a} = \{a_i\}$  whose elements are given by

$$a_i = \text{Tr}_1^m(\beta^{2i}), i = 0, 1, \dots$$

and the shift sequence  $\mathbf{e} = (e_0, e_1, \dots, e_{d-1})$  is determined by  $t_j(\lambda)$  in (10.32). In other words, each sequence in  $S$  can be arranged into a  $v$  by  $d$  array for which the  $j$ th ( $0 \leq j < d$ ) column is given by  $L^{e_j}(\mathbf{a})$ , where  $e_j$  is determined by  $t_j = \beta^{e_j}$  if  $t_j \neq 0$ . Otherwise, the  $j$ th column is the zero sequence.

We shall also call  $(t_0, t_1, \dots, t_{d-1})$  a *phase vector* of  $\mathbf{u}$  when it is regarded as a  $(v, d)$  interleaved sequence, since it determines phase shifts of column sequences of  $\mathbf{u}$  with respect to  $\mathbf{a}$ .

*Proof of Theorem 10.2.* We will use an approach similar to the one in Section 8.1 of Chapter 8. For  $\mathbf{s}_\eta$  and  $\mathbf{s}_\lambda$  in  $S$ , considering the  $v$  by  $d$  arrays formed from  $L^\tau(\mathbf{s}_\eta)$  and  $\mathbf{s}_\lambda$ , respectively, let  $A_j$  and  $B_j$  be their  $j$ th columns. Then

$$A_j = \{\text{Tr}_1^m(\beta^{2i}t_{j+\tau}(\eta))\}_{i=1}^{v-1} \text{ and } B_j = \{\text{Tr}_1^m(\beta^{2i}t_j(\lambda))\}_{i=0}^{v-1}, 0 \leq j < d$$

where  $t_j(z)$  is defined by (10.32). Thus  $C_{\eta,\lambda}(\tau)$ , the crosscorrelation of  $\mathbf{s}_\eta$  and  $\mathbf{s}_\lambda$ , is equal to the sum of the inner products of  $A_j$  and  $B_j$ ,  $0 \leq j < d$ , i.e.,

$$C_{\eta,\lambda}(\tau) = \sum_{j=0}^{d-1} \langle A_j, B_j \rangle.$$

Thus, it suffices to prove that there are at most two identical corresponding columns in their respective matrix forms. This is equivalent to saying that there are at most two values of  $j$  among  $0 \leq j < d$  such that

$$t_{j+\tau}(\eta) = t_j(\lambda). \quad (10.33)$$

In the following, we will reduce (10.33) to a quadratic equation. Considering (10.32), let  $x = \alpha^j$ , so we can rewrite  $t_j(z)$  as:

$$\begin{aligned} t_j(z) &= Tr_m^n(x^2) + zx^d = x^2 + x^{2 \cdot 2^m} + zx^{2^m+1} \\ &= x^2(1 + x^{2(2^m-1)} + x^{2^m-1}) \\ \implies t_j(z) &= x^2(1 + y^2 + zy), \quad \text{where } y = x^{2^m-1}. \end{aligned} \quad (10.34)$$

Substituting (10.34) into (10.33),

$$t_{j+\tau}(\eta) = x^2(\alpha^{2\tau} + \alpha^{\tau 2^{m+1}} y^2 + \eta \alpha^{\tau d} y) = x^2(1 + y^2 + \lambda y) = t_j(\lambda).$$

Simplifying, we obtain a quadratic equation

$$a + by^2 + cy = 0 \quad (10.35)$$

where

$$a = 1 + \alpha^{2\tau}, b = 1 + \alpha^{\tau 2^{m+1}}, \text{ and } c = \lambda + \eta \alpha^{\tau d}$$

where  $\tau \neq 0$ . Since (10.35) is a quadratic equation over  $\mathbb{F}_{2^n}$ , it has at most two solutions  $y_i, i = 1, 2$  in  $\mathbb{F}_{2^n}$ . For each of the  $y_i$ , there exists at most one  $x = \alpha^j, 0 \leq j < d$  such that

$$y_i = x^{2^m-1}.$$

Therefore, there are at most two values of  $j$  among  $0 \leq j < d$  such that (10.33) is true. Thus

$$C_{\eta, \lambda}(\tau) = \begin{cases} -1 - 2^m & \text{if (10.33) has no solutions} \\ -1 & \text{if (10.33) has one solution} \\ -1 + 2^m & \text{if (10.33) has two solutions} \end{cases}$$

which completes the proof. □

Note that  $\mathbf{s}_0 = \{Tr_1^n(\alpha^{2^i})\} = \{Tr_1^n(\alpha^i)\}$  is an  $m$ -sequence of period  $2^n - 1$ . Thus, for  $\lambda \neq 0$ , we have

$$\mathbf{s}_\lambda = \mathbf{s}_0 + L^k \mathbf{a} \leftrightarrow Tr(x + \lambda x^d), \lambda = \beta^k, 0 \leq k < 2^m - 1.$$

Hence, the Kasami (small) signal set can be written as

$$S = \{\mathbf{s}_{\beta^k} \mid 0 \leq k < 2^m - 1\} \cup \{\mathbf{s}_0\}.$$

**Profile of the randomness of Kasami (small) signal sets ( $n = 2m$ ):**

1. The Kasami (small) signal set  $S$  is a  $(2^n - 1, 2^m, 2^m + 1)$  signal set.
2. Cross-correlation of any two sequences in  $S$  or out-of-phase autocorrelation of any sequence in  $S$  is three-valued and belongs to

$$\{-1, -1 \pm 2^m\}.$$

3. Imbalance range:  $[1, 2^m + 1]$ . (In fact, each sequence in  $S$ , except for  $\mathbf{s}_0$ , has weight either  $2^{n-1} + 2^{m-1}$  or  $2^{n-1} - 2^{m-1}$ . We will show this result in the next subsection after we introduce a construction for generalized Kasami sequences.)
4.  $\mathbf{a} = \{Tr_1^m(\beta^i)\}$  is an  $m$ -sequence of period  $2^m - 1$ . (Note that  $Tr_1^m(x) = Tr_1^m(x^2)$ .)
5. Linear span:  $3n/2$ , except for  $\mathbf{s}_0$  whose linear span is  $n$ .

The LFSR implementation of the Kasami (small) signal sets is shown in Figure 10.4, from which all the sequences in  $S$  can be generated by varying the initial state of the short LFSR.

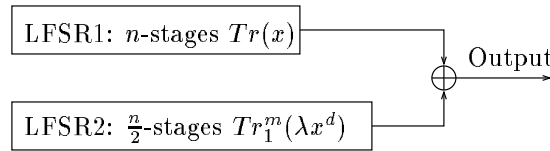


Figure 10.4: LFSR implementation of a Kasami (small) signal set generator

We will use an example to illustrate the properties of the Kasami signal sets discussed above.

**Example 10.9** Design a  $(63, 8, 9)$  Kasami signal set.

1. Pick  $n = 6$ , and  $t(x) = x^6 + x + 1$  a primitive polynomial over  $\mathbb{F}_2$ ; take  $\alpha$  a root of  $t(x)$  in  $\mathbb{F}_{2^6}$ , and  $d = 9$ . Let  $\beta = \alpha^9$ . The  $\beta$  is a primitive element of  $\mathbb{F}_{2^3}$ .

2. Compute the minimal polynomial  $v(x)$  of  $\beta$ ,  $v(x) = x^3 + x^2 + 1$  (or look-up table in Appendix C in Chapter 3).

From (10.32), we have

$$t_j(\lambda) = x^2 + x^{16} + \lambda x^9, x = \alpha^j, 0 \leq j < d,$$

whose values are shown in Table 10.8. In the  $i$ th row under the label “ $i$ ”, the  $j$ th entry,  $j = 0, \dots, 8$  is the exponent  $r$  such that  $t_j(\beta^i) = \beta^r$  where  $x = \alpha^j$ . By convention, if  $t_j(\beta^i) = 0$ , then the exponent is listed as  $\infty$ . (Note that  $t_j(\beta^i) \in \mathbb{F}_{2^3}$ .)

Table 10.8: Image of  $t_j(\lambda) = x^2 + x^{16} + \lambda x^9, \forall \lambda \in \mathbb{F}_{2^3}^*$

$\lambda = \beta^i$	$t_j(\lambda)$ for $x = \alpha^j$									
$i$	$j$	0	1	2	3	4	5	6	7	8
0		0	2	4	$\infty$	1	2	$\infty$	2	2
1		1	1	6	1	6	0	4	4	1
2		2	5	2	6	5	6	2	0	5
3		3	0	$\infty$	5	2	3	1	$\infty$	0
4		4	3	3	2	4	5	5	1	3
5		5	$\infty$	1	4	0	1	0	6	$\infty$
6		6	4	0	0	$\infty$	$\infty$	3	5	4

Table 10.8 directly determines the weight distribution of the sequences in  $S$ . In other words, for  $i \in \{0, 3, 5, 6\}$ , there are two zero columns in the 7 by 9 array from  $\mathbf{s}_{\beta^i}$ , and the other 7 columns are shifts of the  $m$ -sequence  $\mathbf{a} = 1110100$ . For  $i \in \{1, 2, 4\}$ , all columns in the array are shifts of  $\mathbf{a}$ . Therefore, we have

$$w(\mathbf{s}_{\beta^i}) = \begin{cases} 7 \cdot 2^2 = 28 & \text{for } i \in \{0, 3, 5, 6\} \\ 9 \cdot 2^2 = 36 & \text{for } i \in \{1, 2, 4\}. \end{cases}$$

Thus, no sequences in  $S$  are balanced (except for the  $m$ -sequence  $\mathbf{s}_0$ ). This is an interesting phenomenon, but was a puzzle in the literature for a long time. (We will give a proof of this result in a more general setting in the next subsection.)

All eight Kasami sequences in  $S$  are shown in Table 10.9, represented as  $(7, 9)$  interleaved sequences where the shift sequence of  $\mathbf{s}_{\beta^i}$  is given by the  $(i + 1)$ st row under the label “ $i$ ” in Table 10.8. For example, for  $\mathbf{s}_1$ , the phase vector is given by the first row under the label “ $i$ ” in Table 10.8:

$$(0, 2, 4, \infty, 1, 2, \infty, 2, 2) \leftrightarrow (1, \beta^2, \beta^4, 0, \beta, \beta^2, 0, \beta^2, \beta^2)$$

and the first two column vectors of  $\mathbf{s}_1$  are given by

$$\begin{aligned} \{Tr_1^3(\beta^{2i})\}_{i=0}^6 &= 1110100 \\ \{Tr_1^3(\beta^2\beta^{2i})\}_{i=0}^6 &= 1101001. \end{aligned}$$

Table 10.9: Sequences in the  $(63, 8, 9)$  Kasami Signal Set

$\mathbf{s}_0 =$	$\mathbf{s}_1 =$	$\mathbf{s}_{\beta} =$	$\mathbf{s}_{\beta^2} =$
0 0 0 0 0 1 0 0 0	1 1 1 0 1 1 0 1 1	1 1 0 1 0 1 1 1 1	1 0 1 0 0 0 1 1 0
0 1 1 0 0 0 1 0 1	1 1 0 0 0 1 0 1 1	0 0 1 0 1 1 0 0 0	1 1 1 1 1 1 1 1 1
0 0 1 1 1 1 0 1 0	1 0 1 0 0 0 0 0 0	0 0 0 0 0 1 1 1 0	0 1 0 0 1 0 0 1 1
0 0 1 1 1 0 0 1 0	0 1 0 0 1 1 0 1 1	1 1 0 1 0 0 0 0 1	1 1 1 0 1 0 1 0 1
0 1 0 1 1 0 1 1 1	1 0 0 0 1 0 0 0 0	1 1 1 1 1 1 0 0 1	0 0 0 1 0 1 0 1 0
0 1 1 0 0 1 1 0 1	0 0 1 0 1 0 0 0 0	1 1 1 1 1 0 1 1 1	0 1 0 1 1 1 0 0 1
0 1 0 1 1 1 1 1 1	0 1 1 0 0 1 0 1 1	0 0 1 0 1 0 1 1 0	1 0 1 1 0 1 1 0 0
$\mathbf{s}_{\beta^3} =$	$\mathbf{s}_{\beta^4} =$	$\mathbf{s}_{\beta^5} =$	$\mathbf{s}_{\beta^6} =$
0 1 0 0 1 0 1 0 1	1 0 0 1 1 0 0 1 0	0 0 1 1 1 1 1 1 0	0 1 1 1 0 0 0 0 1
0 1 0 1 1 0 0 0 1	0 0 0 1 0 1 1 0 0	1 0 0 0 1 0 1 1 0	1 0 1 1 0 0 0 1 0
1 1 0 1 0 1 0 0 1	1 1 1 0 1 1 1 0 1	1 0 0 1 1 0 1 0 0	0 1 1 1 0 0 1 1 1
1 0 0 1 1 1 1 0 0	0 1 1 1 0 1 1 1 1	1 0 1 0 0 1 0 0 0	0 0 0 0 0 0 1 1 0
1 1 0 0 0 1 1 0 1	0 1 1 0 0 0 0 1 1	0 0 1 0 1 1 1 1 0	1 0 1 1 0 0 1 0 0
0 0 0 1 0 0 1 0 0	1 0 0 0 1 1 1 1 0	1 0 1 1 0 1 0 1 0	1 1 0 0 0 0 0 1 1
1 0 0 0 1 1 0 0 0	1 1 1 1 1 0 0 0 1	0 0 0 1 0 0 0 1 0	1 1 0 0 0 0 1 0 1

The LFSR implementation of the  $(63, 8, 9)$  Kasami signal set is shown in Figure 10.5, from which all the sequences in  $S$  can be generated by varying initial states of the 3-stage LFSR.

### 10.3.2 Generalization of the Kasami (Small) Signal Sets

From the proof of Theorem 10.2, the result that  $C(S) = \{-1, -1 \pm 2^{n/2}\}$  depends only on the 2-level autocorrelation property of the column sequences,

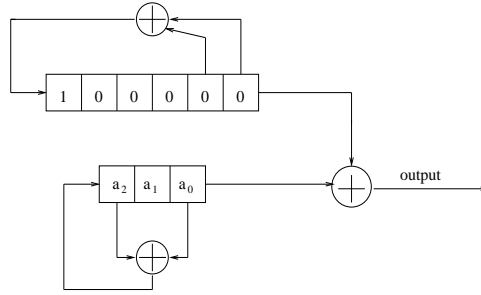


Figure 10.5: LFSR implementation of the (63, 8, 9) Kasami signal set

where the sequences in  $S$  are regarded as  $(v, d)$  interleaved sequences. Thus, the trace function  $Tr_1^m(x)$  employed in the Kasami (small) set construction can be replaced by any orthogonal function from  $\mathbb{F}_{2^m}$  to  $\mathbb{F}_2$ .

**Construction:** Let  $g(x) : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$  be an orthogonal function (i.e., the evaluation of  $g(x)$  is a 2-level autocorrelation sequence of period  $2^m - 1$ ), and let  $\mathbf{s}_\lambda = \{s_{\lambda,i}\}_{i \geq 0}$  whose elements are given by

$$s_{\lambda,i} = f_\lambda(\alpha^i), i = 0, 1, \dots, \text{ where} \tag{10.36}$$

$$f_\lambda(x) = g(Tr_m^n(x^2) + \lambda x^d), \lambda \in \mathbb{F}_{2^m}, x \in \mathbb{F}_{2^n}. \tag{10.37}$$

So,  $f_\lambda(x)$  is the trace representation of  $\mathbf{s}_\lambda$ . A signal set  $S(g)$  consists of  $\mathbf{s}_\lambda$  for all  $\lambda \in \mathbb{F}_{2^m}$ , i.e.,

$$S(g) = \{\mathbf{s}_\lambda \text{ such that } \lambda \in \mathbb{F}_{2^m}\}. \tag{10.38}$$

$S(g)$  is said to be a *generalized Kasami (small) signal set*.

**Theorem 10.3**  $S(g)$  is a  $(2^n, 2^m, 2^m + 1)$  ( $n = 2m$ ) signal set for any orthogonal function  $g$ . Furthermore,  $C(S(g)) = \{-1, -1 \pm 2^m\}$ , i.e., the crosscorrelation of any pair of sequences in  $S(g)$  or out-of-phase autocorrelation of a sequence in  $S(g)$  is 3-valued and belongs to  $C(S(g))$ .

A proof of Theorem 10.3 follows directly from the following lemma.

**Lemma 10.2** Let  $\mathbf{u} = \{u_i\} = \mathbf{s}_\lambda \in S(g)$ , defined above.

(a) The elements of  $\mathbf{u} = \{u_i\}$  are given by

$$u_{id+j} = g(\beta^{2^i} t_j), 0 \leq i < v, 0 \leq j < d,$$

where  $t_j = t_j(\lambda)$  is defined in (10.32). Thus  $\mathbf{s}_\lambda$  is a  $(v, d)$  interleaved sequence where the phase vector is  $(t_0, t_1, \dots, t_{d-1})$  (the same as the Kasami small sequences) and the elements of the base sequence  $\mathbf{a} = \{a_i\}$  are given by

$$a_i = g(\beta^{2^i}), i = 0, 1, \dots$$

(b) The sequence  $\mathbf{s}_0$  has the trace representation  $g(\text{Tr}_m^n(x^2))$ , so it is a 2-level autocorrelation sequence of period  $2^n - 1$ .

*Proof.* The assertion 1 follows directly from the same approach as used in Lemma 10.1, and the assertion 2 is a direct consequence of Construction I in Chapter 8. □

Note that  $\mathbf{a} \leftrightarrow g(x)$  is a 2-level autocorrelation sequence of period  $v = 2^m - 1$ . Thus, a generalized Kasami sequence can be constructed from the array form of the corresponding Kasami sequence by replacing the base sequence  $\{\text{Tr}_1^m(\beta^{2^j})\}_{j \geq 0}$  by  $\mathbf{a}$  while the phase vector is kept unchanged. Note that if we choose  $g(x) = \text{Tr}_1^m(x^2)$ , then  $S(g)$  is the Kasami (small) set. In the following, we will establish the weight distribution of the sequences in  $S(g)$  for a general 2-level autocorrelation function  $g(x)$ .

**Theorem 10.4** *With the above notation,*

$$w(\mathbf{s}_\lambda) = 2^{n-1} \pm 2^{m-1}, \forall \lambda \in \mathbb{F}_{2^m}^*.$$

*In other words, each generalized Kasami sequence in  $S(g)$ , except for  $\mathbf{s}_0$  (including the Kasami case) has weight either  $2^{n-1} + 2^{m-1}$  or  $2^{n-1} - 2^{m-1}$ . Thus, except for the  $m$ -sequence  $\mathbf{s}_0$ , no sequences in  $S(g)$  are balanced.*

*Proof.* For  $\lambda \neq 0$ , we consider the sequence  $\mathbf{s}_\lambda$ , regarded as a  $(v, d)$  interleaved sequence. From Lemma 10.2 -(1) and the proof of Theorem 10.3, we only need

to show that the quadratic equation

$$t_j(\lambda) = x^2(1 + y^2 + \lambda y) = 0, \quad \text{where } y = x^v, \quad (10.39)$$

has either exactly two solutions or no solutions for which

$$x = \alpha^j, 0 \leq j < d. \quad (10.40)$$

Note that (10.39) has solutions in  $\mathbb{F}_{2^n}$  if and only if  $Tr_1^n(\lambda^{-2}) = 0$ . Since  $\lambda \in \mathbb{F}_{2^m}$ , then  $Tr_1^n(\lambda^{-2}) = Tr_1^n(\lambda^{-1}) = Tr_1^m(\lambda^{-1}Tr_m^n(1)) = 0$  from  $Tr_m^n(1) = 1 + 1 = 0$ . Thus the quadratic equation (10.39) always has two solutions in  $\mathbb{F}_{2^n}$ . Let  $y_i, i = 1, 2$  be these two solutions. If there exists  $j : 0 \leq j < d$  such that  $y_1 = \alpha^{jv}$ , then  $y_1$  is a solution which satisfies (10.40). In this case,

$$y_1 y_2 = 1 \implies y_2 = y_1^{-1} = \alpha^{-jv} = \alpha^{j'v}, \quad \text{where } 0 < j' = d - j < d.$$

Thus  $y_2$  is also a solution which satisfies (10.40). Therefore, if one of these two solutions of (10.39) satisfies (10.40), so does the other. Consequently, we have

$$w(\mathbf{s}_\lambda) = \begin{cases} 2^{n-1} + 2^{m-1} & \text{if the both solutions satisfy (10.40)} \\ 2^{n-1} - 2^{m-1} & \text{if neither of the solutions satisfy (10.40)}. \end{cases}$$

□

**Example 10.10** With  $n = 6$ ,  $\alpha$ , and  $\beta = \alpha^9$  in Example 10.9, let  $g(x) = Tr_1^3(x^3)$ . Thus, for  $\mathbf{s}_{\beta^i}$ , the  $j$ th column sequence is given by

$$\{Tr_1^3((\beta^{2i}t_j)^3)\}_{i=0}^6$$

where  $(t_0, t_1, \dots, t_8)$  is given by the  $i$ th row in Table 10.8. In other words,  $\mathbf{s}_{\beta^i}$  can be obtained from Table 10.9 by replacing the base sequence  $\mathbf{a} = 1110100$  by  $\mathbf{a}^{(3)} = 1001011$  while the shifts are retained. This is the same as we did for the construction of GMW sequences using the interleaved approach. According to Theorem 10.4, no sequences in  $S(g)$  (except for  $\mathbf{s}_0$ ) are balanced. This can be verified by Table 10.8, since there are either no  $\infty$ 's in each row or there are exactly two  $\infty$ 's in each row.

### 10.3.3 Profile of the Randomness of $S(g)$ and Implementation

A profile of the randomness of the generalized Kasami signal sets is shown as follows.

Profile of  $(2^n, 2^m, 2^m + 1)$  signal set  $S(g)$

Period	$2^n - 1$
Number of sequences in $S$	$2^m$
Cross/out-of-phase autocorrelation	$\{-1, -1 \pm 2^m\}$
Distribution of 0-1	Each non- $m$ -sequence has weight $2^{n-1} \pm 2^{m-1}$ Imbalance range: $[1, 2^m + 1]$
Linear span $LS$	(a) $g(x) = Tr_1^{m^2}(x)$ , $LS = \frac{3}{2}n$ (b) $g(x) = Tr_1^m(x^r)$ , $\gcd(r, 2^m - 1) = 1$ , $LS \geq m2^{w(r)}$ (c) $g(x)$ from Chapters 8 and 9, linear span can be made large

**Example 10.11** The following examples illustrate the generalized kasami signal sets for  $n = 6, 8$  and  $10$ .

(a) Let  $n = 6$ , and let  $\alpha$  be the same as in Example 10.9. Then there are only two sequences of period 7 with 2-level autocorrelation. Thus there are only two choices for  $g(x)$ :

$$g(x) = Tr_1^3(x) \text{ or } g(x) = Tr_1^3(x^3)$$

which produce two generalized Kasami signal sets (including the Kasami case), as shown in Examples 10.9 and 10.10, respectively. In other words, we have

$$S_1 = S(Tr_1^3(x)) = \{Tr_1^3(Tr_3^6(x) + \lambda x^9) \mid \lambda \in \mathbb{F}_{2^3}\}, \text{ and}$$

$$S_2 = S(Tr_1^3(x^3)) = \{Tr_1^3((Tr_3^6(x) + \lambda x^9)^3) \mid \lambda \in \mathbb{F}_{2^3}\}.$$

Both sets produce  $(63, 8, 9)$  signal sets. The linear span of sequences in  $S_1$  is 9, or 6 for  $\lambda = 0$ ; and the linear span of sequences in  $S_2$  is 21, or 12 for  $\lambda = 0$ . The

latter follows from the expansion:

$$\text{Tr}_1^3((\text{Tr}_3^6(x) + \lambda x^9)^3) = \text{Tr}_1^6(x^3 + (1 + \lambda^2)x^5 + \lambda x^{13}) + \text{Tr}_1^3(\lambda^3 x^{27}).$$

(b)  $n = 8$ . There are two shift-distinct 2-level autocorrelation sequences of period 15. Both are  $m$ -sequences. Thus  $g(x) \in \{\text{Tr}_1^4(x), \text{Tr}_1^4(x^7)\}$ , and  $S(g)$  is a  $(255, 16, 17)$  signal set.

(c)  $n = 10$ . There are 6 shift-distinct  $m$ -sequences and 2 shift-distinct quadratic residue sequences of period 31. Thus, there are eight  $(1023, 32, 33)$  generalized Kasami signal sets in all.

A generalized Kasami (small) signal set can be implemented by the Galois configuration, as shown in Figure 10.6.

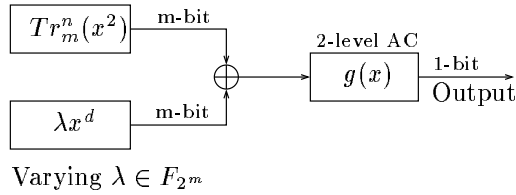


Figure 10.6: Galois configuration for implementation of generalized Kasami signal sets

## 10.4 Even Case: Bent Function Signal Sets

In this section, using bent functions, we present another construction of  $(2^n - 1, 2^m, 2^m + 1)$  signal sets for  $n = 2m$  where  $m$  is even.

### 10.4.1 Bent Functions

A bent function is a boolean function in  $n$  variables, say  $f(x_0, \dots, x_{n-1})$ , whose Walsh transform has constant magnitude, i.e.,

$$\widehat{f}(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{w} \cdot \mathbf{x} + f(\mathbf{x})} = \pm\sqrt{q}, \quad \forall \mathbf{w} \in \mathbb{F}_2^n \quad (q = 2^n). \quad (10.41)$$

From Property 10.6, a boolean function is bent if and only if the Hadamard transform of its corresponding polynomial satisfies

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + f(x)} = \pm\sqrt{q}, \forall \lambda \in \mathbb{F}_{2^n}. \quad (10.42)$$

Note that  $\widehat{f}(\lambda)$  is an integer. Thus, bent functions only exist when  $n$  is even. In the following, we will use both representations for boolean functions. There are two general constructions for bent functions, as presented below. Again take  $n = 2m$ ,  $v = 2^m - 1$ ,  $d = 2^m + 1$ , and  $\alpha$  a primitive element in  $\mathbb{F}_{2^n}$ . Let  $t(x) = x^2 + c_1x + c_0, c_i \in \mathbb{F}_{2^m}$  be the minimal polynomial of  $\alpha$  over  $\mathbb{F}_{2^m}$ . Thus, we can write  $\mathbb{F}_{2^n} = \{x + \alpha y \mid x, y \in \mathbb{F}_{2^m}\}$ .

Construction I (McFarland) for Bent Functions	
Boolean Form	Polynomial Form
$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \psi(\mathbf{y}) + g(\mathbf{y})$ where	$f(z) = x\psi(y) + g(y)$ where
$\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m,$	$z = x + \alpha y, x, y \in \mathbb{F}_{2^m}$
$g(y_0, \dots, y_{m-1}),$ a Boolean $\mathbb{F}_2^m \rightarrow \mathbb{F}_2$	$g,$ a function $\mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$
$\psi(y_0, \dots, y_{m-1}),$ a permutation of $\mathbb{F}_2^m$	$\psi(y),$ a permutation of $\mathbb{F}_{2^m}$

Construction II (Dillon) for Bent Functions
Polynomial Form $f(x) : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2, d = 2^m + 1$
$f(0) = 0, a_i = f(\alpha^i), 0 \leq i < 2^n - 1$ such that
$a_{kd+i} = a_i,$ and $w((a_0, a_1, \dots, a_{d-1})) = 2^{m-1}$

Construction II, given here, is slightly different from Dillon’s original construction. We provide a proof below.

**Property 10.7** *The trace representation of any binary sequence  $(a_0, a_1, \dots, a_{d-1})$  with weight  $2^{m-1}$  is bent. Furthermore, the least period of the sequence is equal to  $d$ .*

*Proof.* We will use the interleaved structure of  $m$ -sequences to establish this

lemma. For Construction II, let  $\mathbf{a} = \{a_i\}_{i=0}^{2^n-2}$ . We arrange  $\mathbf{a}$  into a  $(v, d)$  array:

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{d-1} \\ a_d & a_{d+1} & \cdots & a_{d+(d-1)} \\ a_{2d} & a_{2d+1} & \cdots & a_{2d+(d-1)} \\ \vdots & & & \\ a_{(v-1)d} & a_{(v-1)d+1} & \cdots & a_{(v-1)d+(d-1)} \end{bmatrix}$$

then

$$A = \begin{bmatrix} R \\ R \\ \vdots \\ R \end{bmatrix} = [A_0, A_1, \cdots, A_{d-1}]$$

where  $R = (a_0, a_1, \cdots, a_{d-1})$  is the first row vector of  $A$  where  $w(R) = 2^{m-1}$ , and the  $A_j$ 's are the column vectors of  $A$  where  $A_j$  is either the zero sequence or the constant 1 sequence. In other words, all row vectors of  $A$  are identical and the weight of the row vector is  $2^{m-1}$ . By the construction of  $R$  or  $\mathbf{a}$ ,  $f(x)$  is the trace representation of  $R$ . Next, we write  $\mathbf{b} = \{b_i\}$ , where  $b_i = \text{Tr}(\lambda\alpha^i)$ , which can be arranged into a  $(v, d)$  array:

$$B = \begin{bmatrix} b_0 & b_1 & \cdots & b_{d-1} \\ b_d & b_{d+1} & \cdots & b_{d+(d-1)} \\ b_{2d} & b_{2d+1} & \cdots & b_{2d+(d-1)} \\ \vdots & & & \\ b_{(v-1)d} & b_{(v-1)d+1} & \cdots & b_{(v-1)d+(d-1)} \end{bmatrix} = [B_0, B_1, \cdots, B_{d-1}].$$

According to Theorem 5.2 in Chapter 5, there is only one column in  $B$  which is the zero sequence, and the other  $2^m$  columns are shift-equivalent  $m$ -sequences of period  $2^m - 1$ . So, every non-zero column of  $B$  has weight  $2^{m-1}$ . Thus, the Hadamard transform of  $f(x)$  is determined by the number of 1's in entries of the sum of the matrices  $A$  and  $B$ . In the following, we will show how to count this number. Without loss of generalization, we may assume that the first column of  $B$  is the zero sequence. Thus, we have the following two cases.

**Case 1.**  $a_0 = 0$ . In the matrix  $A + B$ , there are  $2^{m-1}$  columns which have weight  $2^{m-1}$  and  $2^{m-1}$  columns have weight  $2^{m-1} - 1$  (those obtained from the complementing of  $B_j$ ). Using a similar result to Property 10.4, we have

$$\widehat{f}(\lambda) = 1 + \{2^{2m} - 1 - 2[2^{m-1} \cdot 2^{m-1} + 2^{m-1} \cdot (2^{m-1} - 1)]\} = 2^m.$$

**Case 2.**  $a_0 = 1$ . In the matrix  $A + B$ , the first column vector has weight  $2^m - 1$ . For the rest of the  $2^m$  column vectors,  $2^{m-1} + 1$  columns have weight  $2^{m-1}$ , and the other  $2^{m-1} - 1$  columns have weight  $2^{m-1} - 1$ . Thus, we have

$$\widehat{f}(\lambda) = 1 + \{2^{2m} - 1 - 2[2^{m-1} + (2^{m-1} + 1) \cdot 2^{m-1} + (2^{m-1} - 1) \cdot (2^{m-1} - 1)]\} = -2^m.$$

Therefore, for any  $\lambda \neq 0$ , we have

$$\widehat{f}(\lambda) = \begin{cases} 2^m & \text{if } B_0 = \mathbf{0} \text{ and } a_0 = 0 \\ -2^m & \text{if } B_0 = \mathbf{0} \text{ and } a_0 = 1. \end{cases}$$

If  $\lambda = 0$ , then  $\widehat{f}(0)$  is determined by the number of ones in  $A$ . In other words, we have

$$\widehat{f}(0) = 1 + [2^{2m} - 1 - 2w(a_0, a_1, \dots, a_{2^n-2})] = 1 + [2^{2m} - 1(2^m - 1) \cdot 2^{m-1}] = 2^m.$$

Thus,  $f(x)$  is bent. Since the Hamming weight of  $R$  is a power of 2, the least period of  $\mathbf{a}$  is equal to  $d$ .

□

**Example 10.12** Let  $n = 4$ , and let  $\alpha$  be a primitive element of  $\mathbb{F}_{2^4}$  with minimal polynomial  $t(x) = x^4 + x + 1$ .

*Method 1.* Using Construction I, let  $\psi(y_0, y_1) = (y_0, y_1)$ , a permutation of  $\mathbb{F}_2^2$ , and  $g(y_0, y_1) = y_0$ , a map from  $\mathbb{F}_2^2$  to  $\mathbb{F}_2$ . Then

$$f(x_0, x_1, y_0, y_1) = (x_0, x_1) \cdot \psi(y_0, y_1) + g(y_0, y_1) = x_0 y_0 + x_1 y_1 + y_0$$

is a bent function from  $\mathbb{F}_2^4$  to  $\mathbb{F}_2$ . The values of the function  $f$  and the Walsh spectrum of  $f$  are shown in Table 10.10 where  $\mathbf{z} = (x_0, x_1, y_0, y_1) \in \mathbb{F}_2^4$  and  $\mathbf{w} = (w_0, w_1, w_2, w_3) \in \mathbb{F}_2^4$ .

*Method 2.* Using Construction II, let  $\mathbf{a} = 00101$ , which is a 3-decimation from  $L(\mathbf{b})$  where  $\mathbf{b} = 000100110101111 \leftrightarrow Tr(x)$ . Thus the trace representation of  $\mathbf{a} = 00101$  is given by  $f(x) = Tr(\alpha x^3)$  where  $a_i = f(\alpha^i)$ ,  $i = 0, 1, 2, 3$ , and 4.

Table 10.10: A bent function from Construction I

$\mathbf{z}, \mathbf{w}$	$f(\mathbf{z})$	$\widehat{f}(\mathbf{w})$
0000	0	4
1000	0	-4
0100	0	4
1100	0	-4
0010	1	4
1010	0	4
0110	1	4
1110	0	4
0001	0	4
1001	0	-4
0101	1	-4
1101	1	4
0011	1	4
1011	0	4
0111	0	-4
1111	1	-4

Note that

$$A = \begin{bmatrix} 00101 \\ 00101 \\ 00101 \end{bmatrix}.$$

According to Construction II,  $f(x)$  is a bent function from  $\mathbb{F}_{2^4}$  to  $\mathbb{F}_2$ . Furthermore,

$$\{\widehat{f}(\alpha^i)\}_{i=0}^{14} = (4, -4, 4, -4, 4, 4, -4, 4, -4, 4, 4, -4, 4, -4, 4) \text{ and } \widehat{f}(0) = 4.$$

Let  $\{1, \alpha, \alpha^2, \alpha^3\}$  be a basis of  $\mathbb{F}_{2^4}$ . Then the boolean form of  $f(x)$  relative to this basis is given by

$$f(x_0, x_1, x_2, x_3) = \text{Tr}(\alpha(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3)^3).$$

Simplifying, we obtain

$$f(x_0, x_1, x_2, x_3) = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2.$$

Thus we have the following one-to-one correspondences:

$$00101 \leftrightarrow \text{Tr}(\alpha x^3) \leftrightarrow x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2.$$

**Example 10.13** Let  $f(x) = Tr_1^m(x^d)$ . For  $\eta \in \mathbb{F}_{2^n}^*$ , we have

$$\begin{aligned}\widehat{f}(\eta) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\eta x) + Tr_1^m(x^d)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(y) + Tr_1^m(\lambda y^d)}\end{aligned}$$

where  $y = \eta x$ ,  $\lambda = \eta^d \in \mathbb{F}_{2^m}^*$  and  $Tr(x) = Tr_1^n(x)$ . Thus  $\widehat{f}(\eta) = 2^n - 2w(\mathbf{s}_\lambda)$ ,  $\lambda \neq 0$ , where  $\mathbf{s}_\lambda$  is a sequence in the Kasami (small) set ( $\lambda \neq 0$ ). According to Theorem 10.4,  $w(\mathbf{s}_\lambda) = 2^{n-1} \pm 2^{m-1}$ . Therefore,

$$\widehat{f}(\eta) = \pm 2^m, \eta \in \mathbb{F}_{2^n}^*.$$

Note that for  $\eta = 0$ ,  $T = \{Tr_1^m(x^d) \mid x \in \mathbb{F}_{2^n}\}$  consists of  $d$  copies of the  $m$ -sequence  $\{Tr_1^m(\beta^j)\}_{j=0}^{2^m-2}$  where  $\beta$  is a primitive element in  $\mathbb{F}_{2^m}$ . Therefore, the number of 1's in  $T$  is given by

$$(2^m + 1)2^{m-1} = 2^{n-1} + 2^{m-1} \implies \widehat{f}(0) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(x^d)} = -2^m.$$

Thus  $f(x) = Tr_1^m(x^d)$  or  $f(x) = Tr(\eta x) + Tr_1^m(x^d), \forall \eta \in \mathbb{F}_{2^n}^*$  are bent. For example, if  $n = 4$ , then  $Tr_1^2(x^5) \leftrightarrow 011$  is a bent function from  $\mathbb{F}_{2^4}$  to  $\mathbb{F}_2$ .

**Remark 10.3** From Proposition 6.7 in Chapter 6,  $f(x)$  is bent if and only if the additive autocorrelation of  $f(x)$ ,  $V_f(w)$ , is equal to 0 for  $w \neq 0$  and equal to  $2^n$  for  $w = 0$ . In other words,

$$\begin{aligned}f(x) \text{ bent} &\iff \\ V_f(w) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x+w) + f(x)} = \begin{cases} 2^n & \text{if } w = 0 \\ 0 & \text{if } w \neq 0 \end{cases} \quad (10.43)\end{aligned}$$

Thus, bent functions produce binary sequences with 2-level additive autocorrelation, given by (10.43), i.e., all out-of-phase autocorrelation values are equal to zero. Precisely, we have the following construction for binary sequences of period  $2^n$  with zero out-of-phase autocorrelation. Sometimes, this type of sequences is referred to as a periodic self-invertible sequence in the literature.

**Construction of binary sequences of period  $2^n$  with zero out-of-phase autocorrelation:** Let  $f(x_0, \dots, x_{n-1})$  be a boolean representation of

$f(x)$ , and let

$$k = \sum_{i=0}^{n-1} k_i 2^i.$$

Then the sequence  $\mathbf{a} = \{a_k\}$  whose elements are given by

$$a_k = f(k_0, \dots, k_{n-1}), \quad k = 0, 1, \dots, 2^n - 1$$

has additive autocorrelation with zero out-of-phase autocorrelation, i.e.,

$$C_{\mathbf{a}}(\tau) = \sum_{k=0}^{2^n-1} (-1)^{a_{k+\tau} + a_k} = \begin{cases} 2^n & \text{if } \tau \equiv 0 \pmod{2^n} \\ 0 & \text{if } \tau \not\equiv 0 \pmod{2^n} \end{cases}$$

Since bent functions exist for every even  $n$ , there exist periodic self-invertible sequences of length  $2^n$  for  $n$  even.

The 2-level autocorrelation sequences discussed in Chapters 8 and 9 arise from multiplicative autocorrelation; see Chapter 6. In general, the problem of the classification of binary 2-level autocorrelation sequences associated with the multiplicative group of a finite field is much harder than that associated with the additive group of the finite field. For example, the family of bent functions provides a large set of binary sequences of period  $2^n$  with zero out-of-phase autocorrelation for every even number  $n$ .

### 10.4.2 Bent Function Signal Sets

**Construction.** For  $n = 2m$  where  $m$  is even, let  $f(\mathbf{x})$  be a bent function in  $m$  variables and set

$$f_{\mathbf{z}}(\mathbf{x}) = f(\mathbf{x}) + \mathbf{z} \cdot \mathbf{x}, \quad \mathbf{x}, \mathbf{z} \in \mathbb{F}_2^m. \quad (10.44)$$

Let  $\mathbf{s}_{\mathbf{z}} = \{s_{\mathbf{z},i}\}$  whose elements are given by

$$s_{\mathbf{z},i} = f_{\mathbf{z}}(x_{0,i}, x_{1,i}, \dots, x_{m-1,i}) + \text{Tr}_1^n(\sigma_0 \alpha^i), \quad i = 0, 1, \dots, \quad (10.45)$$

where

$$x_{j,i} = \text{Tr}_1^n(\eta_j \alpha^i), \quad 0 \leq j < m, \quad \text{and } \sigma_0 \notin \mathbb{F}_{2^m} \quad (10.46)$$

where  $\{\eta_0, \eta_1, \dots, \eta_{m-1}\}$  is a basis of  $\mathbb{F}_{2^m}/F_2$ . In other words, we have

$$s_{\mathbf{z},i} = f(\mathbf{x}_i) + \mathbf{z} \cdot \mathbf{x}_i + \text{Tr}_1^n(\sigma_0 \alpha^i), \quad i = 0, 1, \dots \quad (10.47)$$

where  $\mathbf{x}_i = (x_{0,i}, x_{1,i}, \dots, x_{m-1,i})$ . A signal set  $S(f)$  is given by

$$S(f) = \{\mathbf{s}_z \mid \mathbf{z} \in \mathbb{F}_2^m\}. \quad (10.48)$$

Then  $S(f)$  is a  $(2^n - 1, 2^m, 2^m + 1)$  signal set. □

In the following, we will derive the trace representation of  $\mathbf{s}_z$ , i.e., the polynomial form of (10.45). Let  $\{\beta_0, \dots, \beta_{m-1}\}$  be the dual basis of  $\{\eta_0, \dots, \eta_{m-1}\}$ . From Theorem 3.13 in Chapter 3, any element  $y$  in  $\mathbb{F}_{2^m}$  can be represented as

$$y = \sum_{j=0}^{m-1} y_j \beta_j, y_j \in \mathbb{F}_2 \quad (10.49)$$

where

$$y_j = Tr_1^m(\eta_j y), 0 \leq j < m. \quad (10.50)$$

This relation aids in finding trace representations of the sequences in  $S(f)$ .

**Property 10.8** For any  $\mathbf{z} \in \mathbb{F}_2^m$ , there exists a unique  $\lambda \in \mathbb{F}_{2^m}$  such that

$$\mathbf{s}_{z,i} = f(Tr_m^n(\alpha^i)) + Tr_1^n((\lambda + \sigma_0)\alpha^i), i = 0, 1, \dots \quad (10.51)$$

*Proof.* Let  $x = \alpha^i \in \mathbb{F}_{2^n}$ . Again, we avoid using double subscripts by renaming  $\mathbf{x}_i$ . Thus, let  $\mathbf{x} = (x_0, \dots, x_{m-1}) = \mathbf{x}_i$ . According to (10.46), we have  $x_j = Tr_1^n(\eta_j x), 0 \leq j < m$ . Note that  $Tr_m^n(x) \in \mathbb{F}_{2^m}$ , denoted by  $y = Tr_m^n(x)$ . Consequently,

$$\begin{aligned} Tr_1^m(\eta_j y) &= Tr_1^m(\eta_j Tr_m^n(x)) = Tr_1^m(Tr_m^n(\eta_j x)) \text{ ( since } \eta_j \in \mathbb{F}_{2^m} \text{ )} \\ &= Tr_1^n(\eta_j x) \text{ ( by the transitivity of the trace function )} \\ \implies Tr_1^m(\eta_j y) &= Tr_1^n(\eta_j x). \end{aligned} \quad (10.52)$$

Thus, we have

$$\begin{aligned} Tr_m^n(x) &= y = \sum_{j=0}^{m-1} Tr_1^m(\eta_j y) \beta_j \\ &= \sum_{j=0}^{m-1} Tr_1^n(\eta_j x) \beta_j \text{ ( by (10.52) ).} \end{aligned}$$

Hence,

$$\mathbf{x} = (x_0, x_1, \dots, x_{m-1}) \leftrightarrow Tr_m^n(x). \quad (10.53)$$

Therefore, from the above one-to-one correspondence and Property 10.6, there exists  $\lambda \in \mathbb{F}_{2^m}$  such that

$$\mathbf{z} \cdot \mathbf{x} = Tr_1^m(\lambda Tr_m^n(x)) = Tr_1^n(\lambda x). \quad (10.54)$$

Substituting (10.53) and (10.54) into (10.45), we obtain

$$s_{\mathbf{z},i} = f(Tr_m^n(\alpha^i)) + Tr_1^n((\lambda + \sigma_0)\alpha^i), \quad i = 0, 1, \dots, \lambda \in \mathbb{F}_{2^m}.$$

□

According to Property 10.8, we have the following polynomial form construction for bent function signal sets.

Construction of Bent Function Signal Sets in Polynomial Form
Let - $f(x) : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ , bent, - $f_\lambda(x) = f(Tr_m^n(x)) + Tr_1^n((\lambda + \sigma_0)x)$ , $\lambda \in \mathbb{F}_{2^m}$ , $\sigma_0 \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ , - $\mathbf{s}_\lambda = \{\mathbf{s}_{\lambda,i}\}$ , where $\mathbf{s}_{\lambda,i} = f_\lambda(\alpha^i)$ , $i = 0, 1, \dots$ , and - $S = \{\mathbf{s}_\lambda \mid \lambda \in \mathbb{F}_{2^m}\}$ .
Then $S$ is a $(2^n - 1, 2^{n/2}, 2^{n/2} + 1)$ signal set.

**Property 10.9** *Every sequence in  $S$  is balanced.*

*Proof.* In order to prove a sequence  $\mathbf{s}_\lambda$  is balanced, it suffices to show that

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x)} = 0, \quad \forall \lambda \in \mathbb{F}_{2^m}. \quad (10.55)$$

Note that  $Tr_m^n(x)$  is the trace representation of an  $m$ -sequence over  $\mathbb{F}_{2^m}$  of degree 2. According to Definition 5.5 and Theorem 5.7 in Section 5.6 of Chapter

5,  $Tr_m^n(x)$  satisfies the 2-tuple balance property, i.e., any pair  $(\lambda, \mu) \in \mathbb{F}_{2^m}$  occurs once in the following set:

$$\{(Tr_m^n(x), Tr_m^n(\gamma x)) \mid x \in \mathbb{F}_{2^n}\}$$

when  $\gamma \notin \mathbb{F}_{2^m}$ . We now use this property to derive (10.55). Let  $\gamma = \lambda + \sigma_0$ . Then  $\sigma_0 \notin \mathbb{F}_{2^m}$  and  $\lambda \in \mathbb{F}_{2^m} \implies \gamma \notin \mathbb{F}_{2^m}$ . Using the 2-tuple balance property, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x)} &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(Tr_m^n(x)) + Tr_1^m(Tr_m^n(\gamma x))} \\ &= \sum_{\lambda, \mu \in \mathbb{F}_{2^m}} (-1)^{f(\lambda) + Tr_1^m(\mu)} \\ &= \sum_{\lambda \in \mathbb{F}_{2^m}} (-1)^{f(\lambda)} \sum_{\mu \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(\mu)} = 0. \end{aligned}$$

The last identity follows from  $\sum_{\mu \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(\mu)} = 0$ .

□

A profile of the randomness of bent function signal sets is presented in Table 10.11. Bent function signal sets can be implemented by the Galois configura-

Table 10.11:  $n = 4t$ , profile of bent function signal sets

Period	$2^n - 1$
Number of Sequences in $S$	$2^{n/2}$
Cross/out-of-phase autocorrelation	$\{-1, -1 \pm 2^{n/2}\}$
Distribution of 0-1	balanced for all sequences in $S$
Linear span	$\leq \sum_{i=1}^{n/4} \binom{n}{i}$

tion, as shown in Figure 10.7. Compared with the generalized Kasami signal sets, a 2-level autocorrelation function  $g(x)$  is replaced by a bent function  $f(x)$ . Furthermore, each sequence in a bent function signal set is a sum of two sequences. One is given by  $f(Tr_m^n(x))$  and the other by an  $m$  sequence with the trace representation  $Tr((\lambda + \sigma_0)x)$  where  $\lambda \in \mathbb{F}_{2^m}$  and  $\sigma_0 \notin \mathbb{F}_{2^m}$ . This structure results in a completely different 0-1 distribution from the Kasami or generalized Kasami signal sets.

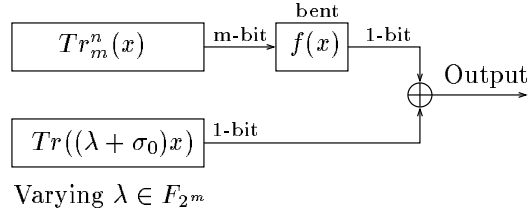


Figure 10.7: Galois configuration for implementation of bent function signal sets

**Example 10.14** Let  $n = 8$ . We will use the same parameters as in Example 8.5 of Chapter 8 in Section 8.2, i.e.,  $\mathbb{F}_{2^8}$  is defined by the primitive polynomial  $c(x) = x^8 + x^4 + x^3 + x^2 + 1$ ,  $\alpha$  a root of  $c(x)$ , and  $\beta = \alpha^d$  ( $d = 17$ ) a primitive element in  $\mathbb{F}_{2^4}$  with minimal polynomial  $t(x) = x^4 + x + 1$ .

1. Pick  $f(x)$  to be the bent function from Method 2 in Example 10.12, i.e.,

$$f(x) = Tr_1^4(\beta x^3) \leftrightarrow \{f(\beta^i)\}_{i=0}^{14} = 001010010100101$$

and denote this sequence as  $\mathbf{d}$ .

2. Set  $\sigma_0 = \alpha \notin \mathbb{F}_{2^4}$ , and

$$f_\lambda(x) = f(Tr_4^8(x)) + Tr_1^8((\lambda + \alpha)x), \lambda \in \mathbb{F}_{2^4}.$$

3. Set

$$\mathbf{s}_{\lambda,i} = f_\lambda(\alpha^i), i = 0, 1, \dots,$$

and

4.  $S = \{\mathbf{s}_\lambda \mid \lambda \in \mathbb{F}_{2^4}\}$ .

We can easily get 16 sequences in  $S$  from Example 8.5 in Chapter 8, where we constructed the GMW sequence of period 255 using the interleaved method. Let  $\mathbf{c} = \{c_i\}$  with  $c_i = Tr_1^8(\alpha^i)$  be that  $m$ -sequence of period 255, regarded as a (15, 17) interleaved sequence. We reproduce it here:

$$\mathbf{c} \leftrightarrow A = A(\mathbf{a}, \mathbf{e}) = \begin{bmatrix} 00000100011100010 \\ 01011100000011001 \\ 00100110111001000 \\ 00101011011010110 \\ 01011000011111011 \\ 01111010111010001 \\ 00001101100011110 \\ 01110011000101101 \\ 00100010100101010 \\ 01110111011001111 \\ 01111110100110011 \\ 01010001100000111 \\ 01010101111100101 \\ 00001001111111100 \\ 00101111000110100 \end{bmatrix} = \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{14} \end{bmatrix} = [B_0, B_1, \dots, B_{16}]$$

where its base sequence and shift sequence are given by

$$\mathbf{a} = \{Tr_1^4(\beta^i)\}_{i=0}^{14} = 000100110101111$$

$$\{Tr_4^8(\alpha^j)\}_{j=0}^{16} \leftrightarrow \mathbf{e} = (\infty, 2, 4, 2, 8, 12, 4, 0, 1, 9, 9, 14, 8, 5, 0, 3, 2).$$

(Note that the  $j$  entry in  $\mathbf{e}$  is the exponent  $r$  of  $\beta$  for which  $\beta^r = Tr_4^8(\alpha^j)$ , and  $A_i$  and  $B_j$  are the  $i$ th row vector and the  $j$ th column vector of  $A$ , respectively.)

Let  $\mathbf{u} = \{u_i\}$  whose elements are given by

$$u_i = f(Tr_4^8(\alpha^i)), i = 0, 1, \dots.$$

Then

$$\mathbf{s}_{\beta^j} = \mathbf{u} + L^{17j}(\mathbf{c}) + L(\mathbf{c}), 0 \leq j < 15, \text{ and } \mathbf{s}_0 = \mathbf{a} + L(\mathbf{c})$$

where  $L$  is the (left) shift operator. Note that  $\mathbf{u}$  is a (15, 17) interleaved sequence with the base sequence  $\mathbf{d} = 001010010100101 \leftrightarrow f(x)$  and the same shift

sequence  $\mathbf{e}$  as the  $m$ -sequence  $\mathbf{c}$ . Thus, we have

$$\mathbf{u} \leftrightarrow A(\mathbf{d}, \mathbf{e}) = \begin{bmatrix} 01110110011100001 \\ 00001000100010010 \\ 01010101000001101 \\ 00100010111100000 \\ 00001001000011110 \\ 01110110011100001 \\ 00001000100010010 \\ 01010101000001101 \\ 00100010111100000 \\ 00001001000011110 \\ 01110110011100001 \\ 00001000100010010 \\ 01010101000001101 \\ 00100010111100000 \\ 00001001000011110 \end{bmatrix}$$

where the  $j$ th column is the sequence  $L^{\epsilon_j}(\mathbf{d})$ . Therefore, the array form of  $\mathbf{s}_{\beta^j}$ ,  $0 \leq j < 15$ , is given by

$$A(\mathbf{d}, \mathbf{e}) + \begin{bmatrix} A_j \\ A_{j+1} \\ \vdots \\ A_{14} \\ A_0 \\ \vdots \\ A_{j-1} \end{bmatrix} + [B_1, B_2, \dots, B_{16}, B_0].$$

In other words, by shifting row vectors in the array form of the  $m$ -sequence  $\mathbf{c}$ , we obtain all sequences in  $S$  except for  $\mathbf{s}_0$ . A profile of the randomness of  $S$  is given in Table 10.12, and the implementation is shown in Figure 10.8.

## 10.5 Interleaved Construction of Signal Sets

In this section, we present a binary signal set with parameters  $(v^2, v+1, 2v+3)$  in terms of interleaved sequences. Here we have two choices, namely  $v = 2^n - 1$  or  $v$  a prime. This is an example of signal set design where the optimum correlation of the signal set is sacrificed to achieve large linear spans.

Table 10.12: Profile of  $S(f)$  with the bent function  $f(x) = Tr_1^4(\beta x^3)$  ( $n = 2 \cdot 4$ )

Period	$2^8 - 1 = 255$
Number of Sequences in $S$	16
Cross/out-of-phase autocorrelation	$\{-1, -1 \pm 16\}$
Distribution of 0-1	128 1's and 127 0's for each sequence in $S$
Linear span	24, or 16 for $\mathbf{s}_0 = \mathbf{c}$ (note: possible maximum linear span is 32)

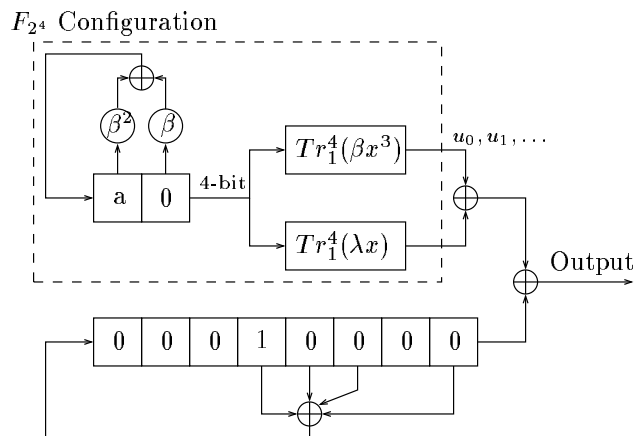


Figure 10.8: The Galois configuration for implementation of the  $(255, 16, 17)$  bent function signal set.

### 10.5.1 Constructions of $(v^2, v + 1, 2v + 3)$ Signal Sets

#### Procedure 1

1. Choose  $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$  and  $\mathbf{b} = (b_0, b_1, \dots, b_{v-1})$ , two binary sequences of period  $v$  with 2-level autocorrelation.
2. Pick  $\mathbf{e} = (e_0, e_1, \dots, e_{v-1})$ , an integer sequence whose elements are taken from  $\mathbf{Z}_v$ , the set consisting of integers modulo  $v$ .
3. Construct  $\mathbf{u} = (u_0, u_1, \dots, u_{v^2-1})$ , a  $(v, v)$  interleaved sequence whose  $j$ th column sequence is given by  $L^{e_j}(\mathbf{a})$ .
4. Set

$$\mathbf{s}_j = (s_{j,0}, s_{j,1}, \dots, s_{j,v^2-1}), 0 \leq j < v$$

whose elements are defined by

$$s_{j,i} = u_i + b_{j+i} \text{ or } \mathbf{s}_j = \mathbf{u} + L^j(\mathbf{b}), 0 \leq j < v.$$

5. A signal set  $S$  is defined as

$$S = \{\mathbf{s}_j \mid j = 0, 1, \dots, v - 1\} \cup \{\mathbf{u}\}.$$

If the shift sequence  $\mathbf{e}$  satisfies the following difference condition:

$$\boxed{\begin{array}{l} \text{for each } 1 \leq s < v, \text{ the differences} \\ e_j - e_{j+s}, 0 \leq j < v - s \text{ are all distinct} \end{array}} \quad (10.56)$$

or equivalently,

$$\boxed{|\{e_j - e_{j+s} \mid 0 \leq j < v - s\}| = v - s, \text{ for all } 1 \leq s < v} \quad (10.57)$$

then  $S$  is a  $(v^2, v + 1, 2v + 3)$  signal set. Moreover, the crosscorrelation of any two sequences in  $S$  or the out-of-phase autocorrelation of any sequence in  $S$  belongs to the set  $\{1, -v, v + 2, 2v + 3, -2v - 1\}$ .

In the following, we show two methods for construction of sequences over  $\mathbb{Z}_v$  satisfying (10.56) (or equivalently, (10.57)).

**Construction A** (Shortened GMW Construction):  $(v^2, v + 1, 2v + 3)$  signal set where  $v = 2^m - 1$ . Let  $n = 2m$  and  $d = 2^m + 1$ . Select  $\alpha$  a primitive element in  $\mathbb{F}_{2^n}$ , and set  $\beta = \alpha^d$ , a primitive element in  $\mathbb{F}_{2^m}$ .

1. *Short* 2-level autocorrelation sequence **b**: Select **b** a binary 2-level autocorrelation sequence of period  $v$ .
2. *Long* 2-level autocorrelation sequence **c**: Choose  $g(x)$  an orthogonal function from  $\mathbb{F}_{2^m}$  to  $\mathbb{F}_2$ , and let  $\mathbf{c} = \{c_i\}$  whose elements are given by

$$c_i = g(\text{Tr}_m^n(\alpha^i)), i = 0, 1, \dots.$$

Then **c** is a 2-level autocorrelation sequence of period  $2^n - 1$  from the GMW construction (see Chapter 8). Thus, a  $v$  by  $d$  array from  $\{c_i\}$  has the following form:

$$\mathbf{c} = \begin{bmatrix} \begin{array}{c} \text{cut} \\ \downarrow \\ 0 \\ 0 \\ \vdots \\ 0 \end{array} & c_1 & c_2 & \cdots & c_{d-2} & \begin{array}{c} \text{cut} \\ \downarrow \\ c_{d-1} \\ a_{2d-1} \end{array} \\ c_{d+1} & c_{d+2} & \cdots & c_{d+d-2} & & \\ c_{(v-1)d+1} & c_{(v-1)d+2} & \cdots & c_{(v-1)d+d-2} & & d_{vd-1} \end{bmatrix} \quad (10.58)$$

3. Interleaved sequence **u**: Let  $U$  be a matrix obtained from **c** by deleting the first and the last columns, i.e., deleting  $(c_{id}, c_{id+d-1}), i = 0, 1, \dots$ . Then  $U$  yields a  $(v, v)$  interleaved sequence **u** of period  $v^2$  whose shift sequence satisfies (10.57). Note that  $U$  has the base sequence given by  $\{g(\beta^i)\}$ , a 2-level autocorrelation sequence of period  $v$ , and the shift sequence **e** =  $(e_0, \dots, e_{v-1})$  whose elements are given by

$$e_j = e \iff \text{Tr}_m^n(\alpha^{j+1}) = \beta^e, 0 \leq j < v. \quad (10.59)$$

Here it is not necessary to actually compute  $e_j$ .

4. Set

$$\mathbf{s}_j = \mathbf{u} + L^j(\mathbf{b}), 0 \leq j < v$$

and  $S = \{\mathbf{s}_j \mid 0 \leq j < v\}$ . Then  $S$  is a  $(v^2, v + 1, 2v + 3)$  signal set.

**Simple Case.** We may select  $g(x) = Tr_1^m(x)$  and  $\mathbf{b}$  an arbitrary binary  $m$ -sequence of period  $2^m - 1$ . In this case,  $\mathbf{c}$  is an  $m$ -sequence of period  $2^m - 1$ . The signal set given by Construction A shortens  $\mathbf{c}$  by deleting  $(c_{di}, c_{i+d-1}), i = 0, 1, \dots$  to obtain the interleaved sequence  $\mathbf{u}$  with shift sequence satisfying (10.57). This is a case similar to the Kasami (small) signal set. But here the short sequence  $\mathbf{b}$  can be any  $m$ -sequence of period  $2^m - 1$ . (Note. In the Kasami (small) set case, the short  $m$ -sequence is completely determined by  $\mathbf{c}$ , which is  $\mathbf{c}^{(d)}$ , a  $d$ -decimation of  $\mathbf{c}$  where  $d = 2^m + 1$ .)

To simplify notation, we may sometimes use the same symbol for an interleaved sequence and for its array form.

**Example 10.15** Construct a  $(49, 8, 17)$  signal set. Let  $n = 6 \implies m = 3$  and  $v = 7$ . We will use the procedure of the simple case to construct a  $(49, 8, 17)$  signal set.

1. Choose  $\mathbf{b} = 1001011$ , an  $m$ -sequence of period 7.
2. We select the same  $m$ -sequence  $\mathbf{c}$  of period 63 as in Example 10.9 for the Kasami signal set  $(63, 8, 9)$ , i.e.,

$$\mathbf{c} = \left[ \begin{array}{c|c|c} \boxed{0} & 0000100 & \boxed{0} \\ \boxed{0} & 1100010 & \boxed{1} \\ \boxed{0} & 0111101 & \boxed{0} \\ \boxed{0} & 0111001 & \boxed{0} \\ \boxed{0} & 1011011 & \boxed{1} \\ \boxed{0} & 1100110 & \boxed{1} \\ \boxed{0} & 1011111 & \boxed{1} \end{array} \right]$$

3. By deleting the first column and the last column of  $\mathbf{c}$ , which are framed in the above array, the resulting array gives a  $(7, 7)$  interleaved sequence  $\mathbf{u}$  which satisfies (10.57), i.e.,

$$\mathbf{u} = \left[ \begin{array}{c} 0000100 \\ 1100010 \\ 0111101 \\ 0111001 \\ 1011011 \\ 1100110 \\ 1011111 \end{array} \right]$$

4. Set  $\mathbf{s}_j = \mathbf{u} + L^j(\mathbf{b})$ :  $j = 0, 1, \dots, 6$  and  $S = \{\mathbf{s}_j \mid 0 \leq j < 7\} \cup \{\mathbf{u}\}$ .

Note that adding  $L^j(\mathbf{b})$ ,  $\mathbf{b}$  at shift  $j$ , to the  $(7, 7)$  interleaved sequence  $\mathbf{u}$  is equivalent to complementing those columns in  $\mathbf{u}$  for which the bits in  $L^j(\mathbf{b})$  are 1's. We illustrate this idea precisely below. Let  $B_j$  denote a  $v$  by  $v$  matrix where the top row of the matrix is  $L^j(\mathbf{b})$  and the rest of the rows are identical to the top row. For example, we have

$$B_0 = \begin{bmatrix} 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \end{bmatrix}$$

Thus,

$$\mathbf{s}_j = \mathbf{u} + B_j, 0 \leq j < 7.$$

We can easily write out the elements of  $\mathbf{s}_0$  and  $\mathbf{s}_1$  from the above arrays  $\mathbf{u}$  and  $B_0$ , i.e.,

$$\mathbf{s}_0 = \mathbf{u} + B_0 = \begin{bmatrix} 0000100 \\ 1100010 \\ 0111101 \\ 0111001 \\ 1011011 \\ 1100110 \\ 1011111 \end{bmatrix} + \begin{bmatrix} 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \\ 1001011 \end{bmatrix} = \begin{bmatrix} 1001111 \\ 0101001 \\ 1110110 \\ 1110010 \\ 0010000 \\ 0101101 \\ 0010100 \end{bmatrix}$$

$$\mathbf{s}_1 = \mathbf{u} + B_1 = \begin{bmatrix} 0000100 \\ 1100010 \\ 0111101 \\ 0111001 \\ 1011011 \\ 1100110 \\ 1011111 \end{bmatrix} + \begin{bmatrix} 0010111 \\ 0010111 \\ 0010111 \\ 0010111 \\ 0010111 \\ 0010111 \\ 0010111 \end{bmatrix} = \begin{bmatrix} 0010011 \\ 1110101 \\ 0101010 \\ 0101110 \\ 1001100 \\ 1110001 \\ 1001000 \end{bmatrix}$$

There are four 1's in  $\mathbf{b}$ , and also in the shifts of  $\mathbf{b}$ . Thus, there are  $4 \cdot 3 + 3 \cdot 4 = 24$  1's and 25 0's in  $\mathbf{s}_j$ . So, the  $\mathbf{s}_j$ 's are balanced except for  $\mathbf{u}$ .

**Profile of the  $(49, 8, 17)$  signal set:**

1. Period 49.

2. 8 shift-distinct sequences.
3. Maximum magnitude of crosscorrelation is 17.
4. Crosscorrelation takes five values:

$$\{1, -7, 9, 17, -15\}.$$

5. Balance: 25 0's and 24 1's in one period of each sequence (except  $\mathbf{u}$ ).
6. Linear span: 24, except for  $\mathbf{u}$  with linear span 21.

**Construction B:**  $(p^2, p+1, 2p+3)$  signal set ( $p$  prime).

1. Choose  $\mathbf{a}$  and  $\mathbf{b}$  from the set consisting of the quadratic residue sequences modulo  $p$  and the Hall residue sequences modulo  $p$  if those sequences exist for such  $p$ .
2. Choose  $\alpha$ , a primitive element of  $\mathbb{F}_p$ .
3. Compute

$$e_j = \alpha^j \in \mathbb{F}_p, \quad 0 \leq j < p.$$

The rest of the steps are the same as in Procedure 1.

**Example 10.16** Let  $p = 11$ , a prime. Choose

$$\mathbf{a} = \mathbf{b}^{(2)} = (11011100010) \text{ and } \mathbf{b} = (10100011101)$$

where  $\mathbf{b}$  is a quadratic residue sequence of period 11. Thus,  $\mathbf{a}$  and  $\mathbf{b}$  are two shift-distinct quadratic residue sequences of period 11. Since 2 is a primitive element of  $\mathbb{F}_{11}$ , we then compute  $e_j \equiv 2^j \pmod{11}$ ,  $0 \leq j < 11$ , as shown below:

$$\mathbf{e} = (1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1).$$

From  $\mathbf{a}$  and  $\mathbf{e}$  we can construct the interleaved sequence  $\mathbf{u}$  whose  $j$ th column sequence is  $L^{e_j}(\mathbf{a})$ :

$$\mathbf{u} = \begin{bmatrix} 10101010101 \\ 01110100100 \\ 11000111101 \\ 11010010011 \\ 10011101001 \\ 00100111010 \\ 00011110110 \\ 01111011000 \\ 10110001111 \\ 01001001110 \\ 11101100011 \end{bmatrix}.$$

Therefore

$$\mathbf{s}_j = \mathbf{u} + L^j(\mathbf{b}), \text{ and } S = \{\mathbf{s}_j \mid 0 \leq j < 11\} \cup \{\mathbf{u}\}$$

which is a  $(121, 11, 25)$  signal set. We can easily obtain any sequence in  $S$  from  $\mathbf{u}$  and  $\mathbf{b}$ . For example,  $\mathbf{s}_0$  is obtained by complementing the  $j$ th column of  $\mathbf{u}$  at those  $j$ 's such that  $b_j = 1$ , i.e., complementing columns of  $j \in \{0, 1, 6, 7, 8, 10\}$ .

Thus, we have

$$\mathbf{s}_0 = \mathbf{u} + \mathbf{b} = \begin{bmatrix} 00001001000 \\ 11010111001 \\ 01100100000 \\ 01110001110 \\ 00111110100 \\ 10000100111 \\ 10111101011 \\ 11011000101 \\ 00010010010 \\ 11101010011 \\ 01001111110 \end{bmatrix}$$

It can be verified that a profile of the randomness of  $S$  is as follows :

1. Period 121.
2. 12 shift-distinct sequences in  $S$ .
3. Maximum magnitude of crosscorrelation is equal to 25.
4. Crosscorrelation takes five values:

$$\{1, -11, 13, 25, -23\}$$

5. Each sequence in  $S$ , except for  $\mathbf{u}$ , is balanced, i.e., there are 61 0's and 60 1's in each period of the sequence.
6. The linear span is equal to 120 for  $\mathbf{s}_j$  and 110 for  $\mathbf{u}$ .

### 10.5.2 Profile of the Interleaved Constructions A and B

1.  $S$  is a  $((2^m - 1)^2, 2^m + 1, 1 + 2^{m+1})$  signal set and a  $(p^2, p + 1, 2p + 3)$  signal set, from Constructions A and B respectively.
2. Crosscorrelation of any pair of sequences in  $S$  or out-of-phase autocorrelation takes five values:

$$\{1, -v, v + 2, 2v + 3, -2v - 1\}$$

where  $v = 2^m - 1$  for Construction A and  $v = p$  for Construction B.

3. Each sequence in  $S$  except for  $\mathbf{u}$  has  $(v^2 + 1)/2$  zeros and  $(v^2 - 1)/2$  ones. In other words, all the sequences in  $S$  except for  $\mathbf{u}$  satisfy the balance property.
4. We denote the linear span of a sequence  $\mathbf{s}$  by  $LS(\mathbf{s})$ .

- (a) For  $v = 2^m - 1$  in Construction A, the linear span of any sequence in  $S$  is lower-bounded by

$$LS(\mathbf{s}_j) > (2^m - 1)LS(\mathbf{a})/2 + LS(\mathbf{b}) \text{ and } LS(\mathbf{u}) > (2^m - 1)LS(\mathbf{a})/2$$

when  $LS(\mathbf{a}) \geq n$ . Otherwise,  $LS(\mathbf{s}_j) = m2^m$  and

$$LS(\mathbf{u}) = m(2^m - 1).$$

- (b) For  $v = p$ , if both  $\mathbf{a}$  and  $\mathbf{b}$  are quadratic residue sequences, then the linear span of a sequence in  $S$  is given by

$$LS(\mathbf{s}_j) = \begin{cases} \frac{p^2-1}{2} & \text{for } p \equiv 7 \pmod{8} \\ p^2 - 1 & \text{for } p \equiv 3 \pmod{8} \end{cases}$$

and

$$L(\mathbf{u}) = \begin{cases} \frac{p(p-1)}{2} & \text{for } p \equiv 7 \pmod{8} \\ p(p-1) & \text{for } p \equiv 3 \pmod{8}. \end{cases}$$

### 10.5.3 Implementation

Construction A, which generates  $((2^m - 1)^2, 2^m + 1, 1 + 2^{m+1})$  signal sets, can be implemented, as shown in Figure 10.9, by using two binary sequence generators with 2-level autocorrelation of period  $2^n - 1$  ( $n = 2m$ , as a long sequence) and  $2^m - 1$  (as a short sequence) respectively, together with a shrinking operation: deleting two consecutive bits for each  $2^m + 1$  consecutive bits from the 2-level binary sequence of period  $2^n - 1$ , where one of these two bits corresponds to a zero column of the array form of the long sequence.

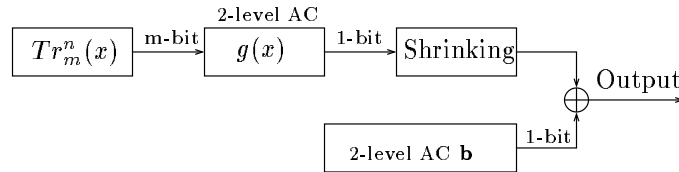


Figure 10.9: Galois configuration of  $((2^m - 1)^2, 2^m + 1, 1 + 2^{m+1})$  signal sets.

For example, the signal set given in Example 10.15 can be implemented as in Figure 10.10.

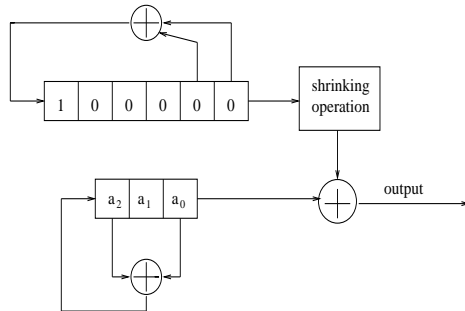


Figure 10.10: Implementation of the  $(47, 8, 17)$  signal set in Example 10.15.

Construction B can be implemented via pre-storage of both the shift sequence  $\mathbf{e}$  and the quadratic sequence  $\mathbf{a}$  (here we choose  $\mathbf{b} = \mathbf{a}$ ) for small  $p$  (for example,  $p < 2^{30}$ ).

## 10.6 $\mathbb{Z}_4$ Signal Sets

In this section, we will introduce the design of signal sets where the elements of sequences are taken from  $\mathbb{Z}_4 = \{0, 1, 2, 3\} \pmod{4}$ . This is an example of signal set design which sacrifices optimum correlation in order to obtain large sizes of the signal sets, needed in some applications of code division multiple access (CDMA) communication where the system capacity becomes a crucial consideration. For the case of  $m$ -sequences over a finite field  $\mathbb{F}_q$ , we may use primitive polynomials over  $\mathbb{F}_q$  of degree  $n$  to generate  $m$ -sequences over  $\mathbb{F}_q$  of period  $q^n - 1$ . Here we intend to generate sequences over  $\mathbb{Z}_4$  with **period**  $2^n - 1$  in terms of known results on binary  $m$ -sequences of period  $2^n - 1$ . This leads to the investigation of constructions of *basic irreducible polynomials* over  $\mathbb{Z}_4$  in terms of primitive polynomials over  $\mathbb{F}_2 = \mathbb{Z}_2$ . (In this section, we will use  $\mathbb{Z}_2$  for  $\mathbb{F}_2$  to emphasize the connection with  $\mathbb{Z}_4$ ). In the following, we first present an algorithm for construction of basic irreducible polynomials over  $\mathbb{Z}_4$ , and then show a design for  $\mathbb{Z}_4$  signal sets with parameters  $(2^n - 1, r, \delta)$ .

The crosscorrelation of two  $\mathbb{Z}_4$  sequences  $\mathbf{a}$  and  $\mathbf{b}$  of period  $v$  is defined by

$$C_{\mathbf{a}, \mathbf{b}}(\tau) = \sum_{k=0}^{v-1} \omega^{a_{k+\tau} - b_k}, \quad 0 \leq \tau < v$$

where  $\omega = -\sqrt{-1}$ , a primitive 4th root of unity ( $i = \sqrt{-1}$  by convention). We have the following map from  $\mathbb{Z}_4$  to the complex number field:

$j$	0	1	2	3
$\omega^j$	1	$-i$	$-1$	$i$

For example, with  $\mathbf{a} = (0, 2, 2, 3, 1, 1, 0)$  and  $\mathbf{b} = (3, 2, 2, 1, 2, 3, 1)$ , we have

$\tau$	$L^\tau(\mathbf{a}) - \mathbf{b}$	$C_{\mathbf{a}, \mathbf{b}}(\tau)$	$ C_{\mathbf{a}, \mathbf{b}}(\tau) $
0	1 0 0 2 3 2 3	$i$	1
1	3 0 1 0 3 1 3	$2 + i$	$\sqrt{5}$
2	3 1 3 0 2 1 1	$i$	1
3	0 3 3 3 2 3 1	$3i$	3
4	2 3 2 3 0 3 2	$-2 + 3i$	$\sqrt{13}$
5	2 2 2 1 0 0 0	$-i$	1
6	1 2 0 1 1 2 0	$-3i$	3

**Definition 10.3** Let  $g(x) \in \mathbb{Z}_4[x]$ , i.e.,  $g(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ ,  $c_i \in \mathbb{Z}_4$ , be a monic polynomial.  $g(x)$  is said to be monic basic irreducible over  $\mathbb{Z}_4$  if the modulo 2 reduction of  $g(x)$ ,

$$\bar{g}(x) = x^n + \sum_{i=0}^{n-1} (c_i \bmod 2) x^i,$$

is a monic irreducible polynomial over  $\mathbb{Z}_2$ .

**Example 10.17** Let

$$g(x) = x^5 + 2x^4 + x^3 + 3 \in \mathbb{Z}_4[x].$$

Then

$$\bar{g}(x) = x^5 + x^3 + 1$$

is primitive over  $\mathbb{Z}_2$ , and therefore it is irreducible over  $\mathbb{Z}_2$ . Thus  $g(x)$  is a basic irreducible polynomial over  $\mathbb{Z}_4$ .

### 10.6.1 Algorithm for Finding Basic Irreducible Polynomials over $\mathbb{Z}_4$

**Algorithm 10.1** ALGORITHM FOR FINDING BASIC IRREDUCIBLE POLYNOMIALS OVER  $\mathbb{Z}_4$

*Input:*  $f(x)$ , a primitive polynomial over  $\mathbb{Z}_2$  of degree  $n$ .

*Output:*  $g(x)$ , a basic irreducible polynomial over  $\mathbb{Z}_4$  of degree  $n$ .

Procedure( $f, g$ ):

1. Set  $h(x) = f(x)$  and regard  $h(x)$  as a polynomial over  $\mathbb{Z}_4$ .
2. Compute  $(-1)^n h(x)h(-x)$ , which will be found to be a polynomial of degree  $n$  in  $x^2$  over  $\mathbb{Z}_4$ :

$$g(x^2) = (-1)^n h(x)h(-x).$$

3. Return  $g(x)$

4. Quit.

**Example 10.18** Select  $f(x) = x^5 + x^3 + 1$ , a primitive polynomial over  $\mathbb{Z}_2$ .

*Procedure*( $f, g$ ):

1. Set  $h(x) = f(x)$  and regard  $h(x)$  as a polynomial over  $\mathbb{Z}_4$ .
2. Compute

$$\begin{aligned} (-1)^5 h(x)h(-x) &= -(x^5 + x^3 + 1)(-x^5 - x^3 + 1) \\ &= x^{10} + 2x^8 + x^6 + 3 \\ &= (x^2)^5 + 2(x^2)^4 + (x^2)^3 + 3. \end{aligned}$$

3. Return  $g(x) = x^5 + 2x^4 + x^3 + 3$ , a basic irreducible polynomial over  $\mathbb{Z}_4$ .
4. Quit.

This is in fact the basic irreducible polynomial in Example 10.17.

### 10.6.2 $\mathbb{Z}_4$ Signal Sets of $S(t), t = 0, 1, \text{ and } 2$

**Algorithm 10.2** ALGORITHM FOR GENERATING  $\mathbb{Z}_4$  FAMILIES  $S(0), S(1)$  AND  $S(2)$

*Input:*  $f(x)$ , a primitive polynomial over  $\mathbb{Z}_2$  of degree  $n$ .  
*Output:*  $S(t)$ ,  $\mathbb{Z}_4$  families,  $t = 0, 1, 2$ .

*Procedure*( $f, S(0), S(1), S(2)$ ):

1. Apply Algorithm 10.1 to  $f(x)$  for computing a basic irreducible polynomial  $g(x) = x^n - \sum_{i=0}^{n-1} g_i x^i, g_i \in \mathbb{Z}_4$ .
2. Generate  $\mathbb{F}_{2^n}$  by  $f(\alpha) = 0$ , and compute the minimal polynomials of  $\alpha^3$  and  $\alpha^5$  over  $\mathbb{Z}_2$ :

$$\begin{aligned} f_{\alpha^3}(x) &= x^n + \sum_{i=0}^{n-1} l_i x^i, l_i \in \mathbb{Z}_2, \\ f_{\alpha^5}(x) &= x^n + \sum_{i=0}^{n-1} k_i x^i, k_i \in \mathbb{Z}_2. \end{aligned}$$

3. Randomly select initial states:

$$(a_0, a_1, \dots, a_{n-1}), a_i \in \mathbb{Z}_4,$$

$$(b_0, b_1, \dots, b_{n-1}), b_i \in \mathbb{Z}_2,$$

$$(c_0, c_1, \dots, c_{n-1}), c_i \in \mathbb{Z}_2.$$

4. Generate a quaternary sequence  $\mathbf{a} = \{a_i\}$  by  $g(x)$ :

$$a_{k+n} = \sum_{i=0}^{n-1} g_i a_{i+k}, k = 0, 1, \dots, \text{ in } \mathbb{Z}_4,$$

and two binary sequences  $\mathbf{b} = \{b_i\}$  and  $\mathbf{c} = \{c_i\}$  by  $f_{\alpha^3}(x)$  and  $f_{\alpha^5}(x)$  respectively:

$$b_{k+n} = \sum_{i=0}^{n-1} l_i b_{i+k}, k = 0, 1, \dots, \text{ in } \mathbb{Z}_2,$$

$$c_{k+n} = \sum_{i=0}^{n-1} k_i c_{i+k}, k = 0, 1, \dots, \text{ in } \mathbb{Z}_2.$$

5. Compute a quaternary sequence  $\mathbf{s} = \{s_i\}$ :

$$s_i = a_i + 2ub_i + 2vc_i, i = 0, 1, \dots, \text{ in } \mathbb{Z}_4$$

where  $u$  and  $v$  belong to  $\mathbb{Z}_2$ .

6. Return

$$S(0) = \{\mathbf{s} | u = 0, v = 0, \text{ for all initial states of } \mathbf{a}\};$$

$$S(1) = \{\mathbf{s} | u = 1, v = 0, \text{ for all initial states of } \mathbf{a} \text{ and } \mathbf{b}\};$$

$$S(2) = \{\mathbf{s} | u = 1, v = 1, \text{ for all initial states of } \mathbf{a}, \mathbf{b} \text{ and } \mathbf{c}\}.$$

7. Quit

We present the sizes of these signal sets and their maximum correlation in Table 10.13.

**Example 10.19** Compute  $\mathbb{Z}_4$  families,  $S(i)$ ,  $i = 0, 1, 2$  for  $n = 5$ .

Input:  $f(x) = x^5 + x^3 + 1$ , a primitive polynomial over  $\mathbb{Z}_2$  of degree  $n = 5$ .

Output:  $S(t)$ ,  $\mathbb{Z}_4$  families,  $t = 0, 1, 2$ .

*Procedure*( $f, S(0), S(1), S(2)$ )

Table 10.13: Parameters of  $\mathbb{Z}_4$  Families

Family	Period $v$ (or length)	Size $r$	$\delta$
$S(0)$	$2^n - 1$	$v + 2$	$\sqrt{v + 1} + 1$
$S(1)$	$2^n - 1$	$\geq v^2 + 3v + 2$	$2\sqrt{v + 1} + 1$
$S(2)$	$2^n - 1$	$\geq v^3 + 4v^2 + 5v + 2$	$4\sqrt{v + 1} + 1$

1. Apply Algorithm 10.1 to  $f(x)$ , to get the basic irreducible polynomial  $g(x) = x^5 + 2x^4 + x^3 + 3 = x^5 - (2x^4 + 3x^3 + 1)$ .
2. Generate  $\mathbb{F}_{2^5}$  by  $\alpha^5 + \alpha^3 + 1 = 0$ , and compute the minimal polynomials of  $\alpha^3$  and  $\alpha^5$  over  $\mathbb{Z}_2$ :

$$\begin{aligned} f_{\alpha^3}(x) &= x^5 + x^3 + x^2 + x + 1, \\ f_{\alpha^5}(x) &= x^5 + x^4 + x^3 + x + 1. \end{aligned}$$

3. Arbitrarily select initial states:

$$\begin{aligned} (a_0, a_1, a_2, a_3, a_4) &= (1, 3, 0, 0, 0), a_i \in \mathbb{Z}_4, \\ (b_0, b_1, b_2, b_3, b_4) &= (1, 0, 0, 0, 0), b_i \in \mathbb{Z}_2, \\ (c_0, c_1, c_2, c_3, c_4) &= (1, 0, 0, 0, 0), c_i \in \mathbb{Z}_2. \end{aligned}$$

4. Generate a quaternary sequence  $\mathbf{a} = \{a_i\}$  by  $g(x)$ :

$$\mathbf{a} = 1300011111203303201220212101330$$

where

$$a_{k+5} = 2a_{k+4} + 3a_{k+3} + a_k, k = 0, 1, \dots, \text{ in } \mathbb{Z}_4,$$

and two binary sequences  $\mathbf{b} = \{b_i\}$  and  $\mathbf{c} = \{c_i\}$  by  $f_{\alpha^3}(x)$  and  $f_{\alpha^5}(x)$ :

$$\mathbf{b} = 1000010110101000111011111001001 \text{ where}$$

$$b_{k+5} = b_{k+3} + b_{k+2} + b_{k+1} + b_k, k = 0, 1, \dots, \text{ in } \mathbb{Z}_2, \text{ and}$$

$$\mathbf{c} = 0000110101001000101111101100111 \text{ where}$$

$$c_{k+n} = c_{k+4} + c_{k+3} + c_{k+1} + c_k, k = 0, 1, \dots, \text{ in } \mathbb{Z}_2.$$

5. Compute quaternary sequences:

$$\begin{aligned} \mathbf{a} &= 1300011111203303201220212101330 \in S(0); \\ \mathbf{a} + 2\mathbf{b} &= 3300031331001303023202030103330 \in S(1); \\ \mathbf{a} + 2\mathbf{b} + 2\mathbf{c} &= 3300211133003303221020232303112 \in S(2). \end{aligned}$$

Now  $s_i = a_i + 2b_i + 2c_i, i = 0, 1, \dots, \{s_i\}$  is a  $\mathbb{Z}_4$  sequence, whose LFSR implementation is shown in Figure 10.11.

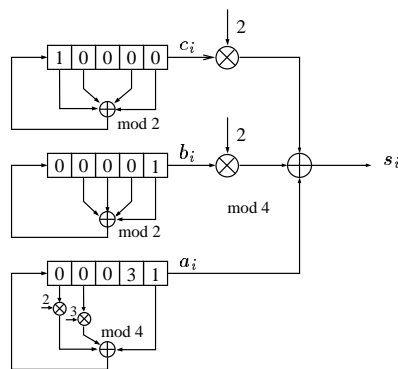


Figure 10.11: LFSR implementation of  $\mathbb{Z}_4$  Sequence  $\{s_i\}$  for  $n = 5$

The parameters of these signal sets for  $n = 5$  is shown below.

Parameters for  $n = 5$

Family	Period $v$ (or length)	Size $r$	$\delta$
$S(0)$	31	33	$4\sqrt{2} + 1$
$S(1)$	31	1057	$8\sqrt{2} + 1$
$S(2)$	31	$\geq 33792$	$16\sqrt{2} + 1$

Next we will give an example of a  $\mathbb{Z}_4$  signal set  $S(2)$  whose parameters are taken from the specification of the scrambling sequences in the 3G standard (the third generation of mobile communications).

**Example 10.20  $S(2)$  Design for  $n = 8$**

1. Select  $n = 8$  and  $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ , primitive over  $\mathbb{Z}_2$ .
2. Apply Algorithm 10.1 to  $f(x)$ , to obtain a basic irreducible polynomial over  $\mathbb{Z}_4$  as follows:

$$g(x) = x^8 - (3x^5 + x^3 + 3x^2 + 2x + 3).$$

3. Generate  $\mathbb{F}_{2^8}$  by  $f(\alpha) = 0$ , and compute the minimal polynomials of  $\alpha^3$  and  $\alpha^5$  over  $\mathbb{Z}_2$  (or use the look-up table in Appendix C in Chapter 3):

$$\begin{aligned} f_{\alpha^3}(x) &= x^8 + x^7 + x^5 + x + 1, \\ f_{\alpha^5}(x) &= x^8 + x^7 + x^5 + x^4 + 1. \end{aligned}$$

4. Randomly select initial states:

$$\begin{aligned} (a_0, a_1, \dots, a_7), a_i &\in \mathbb{Z}_4, \\ (b_0, b_1, \dots, b_7), b_i &\in \mathbb{Z}_2, \\ (c_0, c_1, \dots, c_7), c_i &\in \mathbb{Z}_2. \end{aligned}$$

5. Generate a quaternary sequence  $\mathbf{a} = \{a_i\}$  using  $g(x)$ :

$$a_{k+8} = 3a_{k+5} + a_{k+3} + 3a_{k+2} + 2a_{k+1} + 3a_k, k = 0, 1, \dots, \text{ in } \mathbb{Z}_4,$$

and two binary sequences  $\mathbf{b} = \{b_i\}$  and  $\mathbf{c} = \{c_i\}$  by  $f_{\alpha^3}(x)$  and  $f_{\alpha^5}(x)$  respectively:

$$\begin{aligned} b_{k+8} &= b_{k+7} + b_{k+5} + b_{k+1} + b_k, k = 0, 1, \dots, \text{ in } \mathbb{Z}_2, \\ c_{k+8} &= c_{k+7} + c_{k+7} + c_{k+4} + c_k, k = 0, 1, \dots, \text{ in } \mathbb{Z}_2. \end{aligned}$$

6. Compute quaternary sequences  $\mathbf{s} = \{s_i\}$ :

$$\mathbf{s} = \mathbf{a} + 2\mathbf{b} + 2\mathbf{c} \text{ in } \mathbb{Z}_4$$

for all initial states of  $\mathbf{a}$ ,  $\mathbf{b}$  and  $\mathbf{c}$ . This gives the family  $S(2)$ , whose parameters are given by

Parameters for an  $S(2)$  Design,  $n = 8$

$\mathbb{Z}_4$ Family	Period $v$	Size $r$	$\delta$
$S(2)$	255	$\geq 16842752$	65

The LFSR implementation of  $\mathbb{Z}_4$  sequence  $\{s_i\}$  for  $n = 8$  is shown in Figure 10.12.

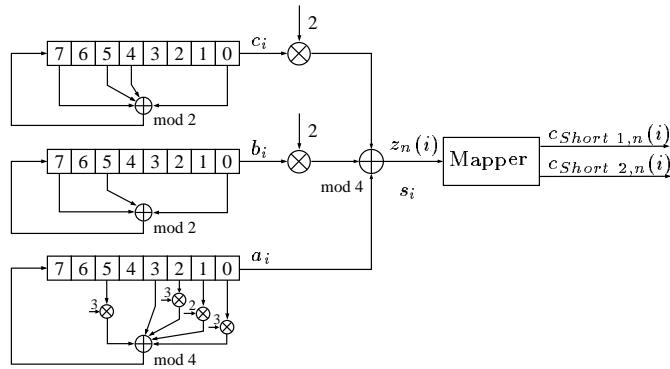


Figure 10.12: LFSR implementation of  $\mathbb{Z}_4$  Signal Sets for  $n = 8$

**Note.**

For sequences with low correlation, Kumar and Helleseth have an excellent chapter in the Handbook of Coding Theory [102]. For the lower bound on correlation, see Welch's work [184], and also Sidelnikov [170]. For the Gold-pair construction, the Gold case was discovered by Gold [60] in 1969, and a proof for Corollary 10.1 for the Kasami (large set) case was given by Kasami [110] (1971). Short proofs for the Kasami decimation  $d = 2^{2k} - 2^k + 1$  were given by Dillon (see the note for Chapter 9) and Dobbertin [39]. Welch's and Niho's cases were two old, long-standing conjectures in [176] (1970) and [141] (1972), and were recently proved by Canteaut, Charpin, and Dobbertin [18] and Hollmann and Xiang [106]. The generalization of the Gold-pair construction was discovered by Boztas and Kumar [13] in 1992. (A result similar to Theorem 10.1 for the Kasami exponent with  $3k \equiv 1 \pmod n$  was stated in Chapter 9.)

For  $n$  even, the Kasami (small) set construction was found by Kasami [110]. For the generalized Kasami construction, the case where  $g(x) = \text{Tr}_1^n(x^r)$  was generalized by No and Kumar [144] in 1989, and are called No sequences; the case where  $g(x)$  is an arbitrary orthogonal function was partially generalized by No, Yang, Chung, and Song [147] in 1997; and this general form appeared in [77]. Bent function signal sets were constructed by Olsen, Scholtz and Welch [150] in 1982, and the linear spans of these sequences were studied by Kumar [121] [120]. The proofs for correlation and linear span of the bent functions signal sets can be found in these papers. For various constructions of bent functions, see [159] [135] [35] [107] [20].

For the even case  $n = 2m$ , there are two more constructions. One is the Kerdock code construction with parameters  $(2^n - 1, 2^{n-1}, 1 + 2^{n/2})$ , see [137] [102]. The other chooses the decimation  $d = 2^m + 2^{(m+1)/2} + 1$  or  $d = 2^{m+1} + 3$  where  $m$  is odd. For  $f(x) = \text{Tr}(x^d)$ , the Hadamard transform of  $f$  has exactly three values:  $0, \pm 2^{m+1}$ . Furthermore,  $0$  occurs  $3 \cdot 2^{n-2}$  times,  $2^{m+1}$  occurs  $2^{n-3} + 2^{m-2}$  times and  $-2^{m+1}$  occurs  $2^{n-3} - 2^{m-2}$  times. This gives signal sets with parameters  $(2^n - 1, 2^n + 1, 1 + 2^{m+1})$ , which is not as good as the (generalized) Kasami case or the bent case. These two decimations were conjectured in Niho's thesis [141] and proved by Cusick and Dobbertin [30] in 1996.

For the interleaved construction of signal sets with parameters  $(v^2, v+1, 2v+3)$ , the case where  $v = 2^n - 1$  and the column sequences are  $m$ -sequences was constructed in 1995 by Gong [87]. Paterson ([154], 1998) extended this to  $v = p$  (binary case) where the two short sequences  $\mathbf{a}$  and  $\mathbf{b}$  are identical, and found another construction for the shift sequences satisfying the difference condition (10.57) using a special class of MDS codes. This investigation was further extended to  $v = p^n - 1$  ( $p$ -ary case) and  $v = p$  (binary case) where the two short sequences can be different by Gong ([77], 2002). The results using interleaved constructions A and B and the results on the linear spans of interleaved sequences for both binary and nonbinary cases, presented here, can be found in [77]. (For the linear spans of quadratic residue sequences, see [37].)  $\mathbb{Z}_4$  signal sets were constructed by Kumar, Helleseth, Calderbank, and Hammons in their

IEEE best research paper of 1996 [122]. The results introduced here are from that paper. The construction of linear recursive sequences over rings was investigated as early as the 1930's by Ward [183]. Research along this line has flourished since the end of the 1980's.

For the  $p$ -ary case where  $p > 2$ , the status of the generalization from binary cases to  $p$ -ary cases is as follows. The Gold-pair construction has been extended to the Gold type decimation  $d = \frac{1}{2}(p^k + 1)$ , and the Kasami-Welch-Trachtenberg type decimation to  $d = p^{2k} - p^k + 1$  ( $\gcd(k, n) = 1$ ) by Helleseth [100], [99] and Trachtenberg [176]. Unlike the binary case, here  $n$  can be even. For the Welch and Niho decimations, the Welch decimation was extended to the ternary case by Dobbertin, Helleseth, Kumar and Martinsen [41], but not to the general  $p$ -ary case. The ternary Niho case was also conjectured by the same authors of [41]. Bent function signal sets for the  $p$ -ary case,  $p > 2$ , were found by Kumar and Moreno [123]. For the generalized Kasami (small) set, generalizing the binary case to the  $p$ -ary case with  $p > 2$  still remains open.

## Exercises for Chapter 10

1. Compute all sequences in a  $(31, 33, 9)$  Gold-pair signal set by choosing different  $\mathbf{a}$ . Give the LFSR implementation for your design.
2. There are 50 users in an indoor wireless mobile communication network system. The system requires that
  - (a) the scrambling sequence (binary) used by each user is shift distinct from the other users;
  - (b) each sequence is balanced with length 127;
  - (c) the maximal crosscorrelation between any two of these sequence is 17.

Design a signal set which satisfies these requirements.

3. Design a Kasami set with parameters  $(63, 8, 9)$  by using a different design from the example shown in the text.
  - (a) Give the LFSR implementation.
  - (b) How many shift sequences are in this Kasami set?
  - (c) Compute the 0-1 distribution for each signal in the Kasami set and cross correlation for one pair of the signals.
4. A CDMA system needs to employ a signal set with a period of at least 1024, and the maximal value of the crosscorrelation of the signal set is less than 80. How many such designs are there? Give the parameters for each of these design.
5. Randomly choose four binary  $m$ -sequences of period 31, and compute the crosscorrelation of each pair of these  $m$ -sequences. What is the smallest maximal crosscorrelation value for all pairs?

6. Can you give a non-trivial bound for the maximal crosscorrelation of any pair of binary  $m$ -sequences of degree  $n$ ?
7. Let

$$\mathbf{e} = (2, 4, 2, 8, 12, 4, 0, 1, 9, 9, 14, 8, 5, 0, 3).$$

Then  $\mathbf{e}$  satisfies the difference condition (10.56). Using  $\mathbf{e}$  as the exponent sequence, construct an interleaved signal set with parameters  $(225, 16, 33)$ . Give the sequence  $\mathbf{u}$  and one of the sequences in this signal set (not  $\mathbf{u}$ ) in their matrix forms.

8. Design an interleaved signal set with parameters  $(49, 9, 17)$ .
- Give an LFSR implementation for your design.
  - Compare your design to a Kasami signal set having a similar parameters.
  - For any pair of sequences in your interleaved signal set, find out the shifts which yield the maximal crosscorrelation value 17.
9. Research Problem: For an interleaved signal set with parameters  $(v^2, v + 1, 2v + 3)$ , the crosscorrelation of any pair of the sequences in the signal set or the out-of-phase autocorrelation of any sequence in the signal set will be reduced to the set  $\{1, -v, v + 2\}$ , if the shift sequence  $\mathbf{e} = (e_0, e_1, \dots, e_{v-1})$  satisfies the following condition: for all  $1 \leq s < v$ ,

$$|\{e_j - e_{j+s} \mid 0 \leq j < v - s\} \cup \{e_{v-s+j} - e_j - 1 \mid v - s \leq j < v\}| = v.$$

Does such a vector  $\mathbf{e}$  exist? For small values of  $v$ , exhaustively search for such vectors  $\mathbf{e}$ .

