New Designs for Signal Sets with Low Cross-correlation, Balance Property and Large Linear Span: $GF(p)$ Case

Guang Gong

Center for Applied Cryptographic Research
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email. ggong@cacr.math.uwaterloo.ca

Abstract. New designs for families of sequences over $GF(p)$ with low cross correlation, balance property and large linear span are presented. The key idea of the new designs is to use short p-ary sequences of period v with the 2-level auto correlation function to construct a set of long sequences with the designed properties. The resulting sequences are of interleaved sequences of period v^2. There are v cyclically shift distinct sequences in each family. The maximal magnitude of cross/out-of-phase auto correlation of sequences in the family is $2v+3$ which is optimal with respect to the Welch bound. In particular, for binary case, cross/out-of-phase auto correlation values belong to the set $\{1, -v, v+2, 2v+3, -2v-1\}$. Each sequence in the family is balanced and has large linear span. For binary case, any sequence in such a family where the short sequences are quadratic residue sequences achieves the maximal linear span. For non-binary case, the new design gives the first type of signal sets with optimal correlation, balance property and large linear span.

Key words. Interleaved sequences, low cross correlation, 2-level auto correlation, randomness property, linear span, finite field, non-binary sequences.

1 Introduction and Preliminaries

A family of binary or non-binary sequences with low cross correlation, good randomness, and large linear span has important applications in code-division multiple access (CDMA) communications. On the other hand, the sequences with low cross correlation employed a stream cipher cryptosystems as a key stream or employed in a block cipher cryptosystems as a session key generator or employed in a public key cryptosystem as a pseudo-random number generator can be resistant to cross correlation attack. Therefore how to generate this type of sequences are important in the applications of CDMA communications and cryptology. In this paper, we will give a new design for families of p-ary sequences with low cross correlation, balance property and large linear span. The key idea of this new design is to use short p-ary periodic sequences with 2-level auto correlation function and an interleaved structure to construct a set of long p-ary sequences with the designed properties. This property also has significant meaning in the application of signal detection of high speed broad-band communication systems. The original idea of this design was proposed by the author in 1995 [13]. But it was not emphasized in the original paper. The original design given in [13] uses m-sequences as short sequences. In recent three years, a status that constructing binary sequences with the 2-level auto correlation function has been dramatically changed. A lot of new binary sequences with 2-level auto correlation that can be applied to practical applications were discovered. In the new designs that we will proposed in this paper, we are allowed to utilize all types of 2-level auto correlation sequences as “building blocks” except for a class of 2-level auto correlation sequences of period v where v is a product of twin primes.

In the following, we give some preliminaries for sequence designs. (The reader is referred to [9] for shift register sequences and [28] for the theory of finite field.)

We will use the following notation throughout the paper:

- p, a prime.
- $\mathbb{Z}_t$, an integer residue ring of modulo t.
- $\mathbb{F}_q = GF(q)$, a finite field with q elements, and $\mathbb{F}_q^*$, the multiplication group of $\mathbb{F}_q$.
- $\mathbb{F}_p^n = \{(x_0, x_1, \cdots, x_{n-1}) | x_i \in \mathbb{F}_p\}$, a vector space over $\mathbb{F}_p$ of dimension n.
- $\underline{\mathbf{a}} = \{a_i\}$, a sequence over $\mathbb{F}_p$, i.e., $a_i \in \mathbb{F}_p$, is called a *p-ary sequence*. If $\underline{\mathbf{a}}$ is a periodic sequence with period v, then we also denote $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{v-1})$, an element in $\mathbb{F}_p^n$.

1.1 Left Shift Operator and Shift Equivalent Relation

Let $\underline{\mathbf{a}} = \{a_i\}$ be a sequence over $\mathbb{F}_p$. The left shift operator L on $\underline{\mathbf{a}}$ is defined as

$$L(\underline{\mathbf{a}}) = a_1, a_2, \cdots,$$

For any $i > 0$,

$$L^i(\underline{\mathbf{a}}) = a_i, a_{i+1}, \cdots,$$

$L^i(\underline{\mathbf{a}})$ is said to be a *phase shift* of $\underline{\mathbf{a}}$. We denote $L^0(\underline{\mathbf{a}}) = \underline{\mathbf{a}}$ for convention. Two periodic sequences $\underline{\mathbf{a}} = \{a_i\}$ and $\underline{\mathbf{b}} = \{b_i\}$ are called *(cyclically) shift equivalent* if there exists an integer k such that

$$a_i = b_{i+k}, \forall i \geq 0 \tag{1}$$

and in this case we write $\underline{\mathbf{a}} = L^k(\underline{\mathbf{a}})$, or simply $\underline{\mathbf{a}} \sim \underline{\mathbf{b}}$. Otherwise, they are called *(cyclically) shift distinct.*

1.2 Balance Property

Let $\underline{\mathbf{a}}$ is a p-ary sequence with period v. In every period, the numbers of all elements in $\mathbb{F}_p$ are nearly equal. (More precisely, the disparity is not to exceed 1.) In particular, if $v = p^n - 1$, each non-zero element in $\mathbb{F}_p$ occurs p^{n-1} times and zero element occurs $p^{n-1} - 1$ times. This property, which states that elements occur as equally often as possible within one period, is referred to as the *balance property of p-ary sequences.*

1.3 Correlation

Let $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{v-1})$ and $\underline{\mathbf{b}} = (b_0, b_1, \cdots, b_{v-1})$ be two p-ary sequences with period v, their (periodic) *cross correlation* function $C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ is defined as

$$C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \sum_{i=0}^{v-1} \omega^{a_i - b_{i+\tau}}, \tau = 0, 1, \cdots$$

where $\omega = e^{2\pi i/p}$, a pth primitive root of unity. Here τ is a phase shift of the sequence $\{b_i\}$ and the indexes are computed by modulo v. If $\underline{\mathbf{b}} = \underline{\mathbf{a}}$, then $C_{\underline{\mathbf{a}},\underline{\mathbf{a}}}(\tau)$ is called an *auto correlation* function of $\underline{\mathbf{a}}$, denoted by $C_{\underline{\mathbf{a}}}(\tau)$ or simply by $C(\tau)$. If

$$C(\tau) = \begin{cases} v & \text{if } \tau \equiv 0 \bmod v \\ -1 & \text{otherwise} \end{cases}$$

then we say that the sequence $\underline{\mathbf{a}}$ has an *(ideal) 2-level auto-correlation function.*

If $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are shift distinct and

$$|C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)| \leq \delta \text{ for any } \tau$$

where δ is a constant close to $\sqrt{v}$, the square root of v, then we say that the sequences $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ have a *low cross correlation* function.

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

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

where $\tau \neq 0$ if $i = j$. Then we say that the set S has low cross-correlation. We call S a (v, r, δ) *signal set.* (A sequence in S is also called a *signal* from the point of view of engineering [36].) When we consider the cross correlation of two sequences $\underline{\mathbf{s}}_i$, $\underline{\mathbf{s}}_j$ in S, we simply write $C_{i,j}(\tau)$ for $C_{\underline{\mathbf{s}}_i,\underline{\mathbf{s}}_j}(\tau)$.

1.4 Interleaved Sequences

Gong introduced the following concept of interleaved sequences over $\mathbb{F}_p$ in 1995 [13]. Let $\underline{\mathbf{u}} = (u_0, u_1, \cdots, u_{st-1})$ be a p-ary sequence of period st where both s and t are not equal to 1. We can arrange the elements of the sequence $\underline{\mathbf{u}}$ into a s by t array as follows:

$$A = \begin{pmatrix} u_0 & u_1 & \cdots u_{t-1} \\ u_t & u_{t+1} & \cdots u_{t+t-1} \\ u_{2t} & u_{2t+1} & \cdots u_{2t+t-1} \\ \vdots & & \\ u_{(s-1)t} & u_{(s-1)t+1} & \cdots u_{(s-1)t+t-1} \end{pmatrix}$$

If each column vector of the above array is either phase shift of a p-ary sequence, say $\underline{\mathbf{a}}$, of period s, or zero sequence, then we say that $\underline{\mathbf{u}}$ is a (s, t) *interleaved sequence over* $\mathbb{F}_p$ [13]. We also say that A is the matrix form of $\underline{\mathbf{u}}$. Let A_j be jth column vector of A, then $A = (A_0, A_1, \cdots, A_{t-1})$. We call the A_j *column sequences of* $\underline{\mathbf{u}}$ (or component sequences of $\underline{\mathbf{u}}$ in [13]). According to the definition, A_j is a transpose of $L^{e_j}(\underline{\mathbf{a}})$ or $(0, 0, \cdots, 0)$. In this paper, we omit the transpose symbol because we consider it as a sequence. I.e., we write

$$A_j = L^{e_j}(\underline{\mathbf{a}}), 0 \le j < t-1$$

where we denote $e_j = \infty$ if $A_j = (0, 0, \cdots, 0)$. $(e_0, e_1, \cdots, e_{t-1})$ is called a *shift sequence* of $\underline{\mathbf{u}}$. For a given $\underline{\mathbf{e}}$ and $\underline{\mathbf{a}}$, the interleaved sequence $\underline{\mathbf{u}}$ is uniquely determined. So we also say $\underline{\mathbf{u}}$ is a (s, t) interleaved sequence associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$.

Note. For a general discussion of periods and linear spans of interleaved sequences with m-sequences as the column sequences, see [13] [21].

Example 1. Let $\underline{\mathbf{e}} = (3, 6, 5, 5, 2, 3, 5)$ and $\underline{\mathbf{a}} = (1, 1, 1, 0, 1, 0, 0)$, a binary sequence. Then a $(7, 7)$ array is as follows:

```
0 0 0 0 1 0 0
1 1 0 0 0 1 0
0 1 1 1 1 0 1
0 1 1 1 0 0 1
1 0 1 1 0 1 1
1 1 0 0 1 1 0
1 0 1 1 1 1 1
```

Then we have the following $(7, 7)$ interleaved sequence

$$\underline{\mathbf{u}} = 0000100110001001111010111001101101111001101011111$$

Note that $\underline{\mathbf{a}}$ is a binary m-sequence of period 7.

1.5 Trace Representation

We denote a trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ for $m|n$ by $Tr_m^n(x)$:

$$Tr_m^n(x) = x + x^q + \cdots + x^{q^{l-1}}, x \in \mathbb{F}_{p^n}$$

where $q = p^m$ and $n = ml$. Any sequence $\underline{\mathbf{a}}$ over $\mathbb{F}_p$ of period $v|p^n - 1$ has a trace representation. I.e., there exists a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$

$$f(x) = \sum_{i=1}^{r} Tr_1^{n_i}(\beta_i x^{t_i}), \beta \in \mathbb{F}_{p^{n_i}}$$

such that

$$a_i = f(\alpha^i), i = 0, 1, \cdots,$$

where α is a primitive element of $\mathbb{F}_{p^n}$, t_i a coset leader of a cyclotomic coset modulo $p^{n_i} - 1$, and $n_i | n$ the size of the cyclotomic coset containing t_i. ($\underline{\mathbf{a}}$ is also to be referred as a r-term sequence.) If $r = 1$, .i.e.,

$$a_i = Tr_1^n(\beta\alpha^i), i = 0, 1, \cdots, \beta \in \mathbb{F}_{p^n}^*,$$

then $\underline{\mathbf{a}}$ is an m-sequence over $\mathbb{F}_p$ of period $p^n - 1$ of degree n. (For a detailed treatment of the trace representation of sequences, see [14].) Since there is a one-to-one correspondence between the function $f(x)$ and the sequence $\underline{\mathbf{a}}$, we use both $f(x)$ and $\underline{\mathbf{a}}$ in this paper. Note that in the language of algebraic geometry codes, $\underline{\mathbf{a}}$ is called an *evaluation* of $f(x)$ at α [40].

1.6 Linear Span

Linear span of the sequence $\underline{\mathbf{a}}$ is the length of the shortest linear feedback shift register that generates $\underline{\mathbf{a}}$. Precisely, let

$$h(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0 \in \mathbb{F}_p[x]$$

and $\underline{\mathbf{a}} = \{a_i\}$ satisfies the following recursive relation

$$a_{k+n} = c_{n-1}a_{k+n-1} + \cdots + c_1 a_{k+1} + c_0 a_k, k = 0, 1, \cdots,$$

then $h(x)$ is called a *characteristic polynomial* of $\underline{\mathbf{a}}$ (over $\mathbb{F}_p$). The polynomial with the smallest degree among all characteristic polynomials of $\underline{\mathbf{a}}$ is called the *minimal polynomial* of $\underline{\mathbf{a}}$ (over $\mathbb{F}_p$). The linear span of $\underline{\mathbf{a}}$ is equal to *degree* of the minimal polynomial of $\underline{\mathbf{a}}$.

For example, $\underline{\mathbf{a}} = 1001011$ is a binary sequence of period 7 and has $h(x) = x^3 + x + 1$ is the minimal polynomial. So the linear span of $\underline{\mathbf{a}}$ is 3.

This paper is organized as follows. Since we will utilize all but one 2-level auto correlation sequences to construct signal sets with low cross correlation, we will start by a brief review for known constructions of 2-level auto or low cross correlation sequences and some remedies for these results as well. These are the content of Section 2. In Section 3, we provide a procedure to construct a signal set consisting v (v, v) interleaved sequences and discuss a representation of these sequences, the balance property and some basic properties on cross correlation when the matrix forms of the interleaved sequences are applied. In Section 4, we present constructions for $(v^2, v, 2v+3)$ signal sets over $\mathbb{F}_p$ for both $p = 2$ and $p > 2$. In Section 5, we show the linear span of sequences in the signal sets by developing some relation between interleaved sequences over the finite field $\mathbb{F}_p$ and its extension field. Section 6 provides an architecture for implementing $(v^2, v, 2v + 3)$ signal sets and some aspects in comparison with the known constructions.

Note. The result on decomposition of interleaved sequences obtained in Section 5 is a general result, and several other methods developed in this section for determining the linear span of interleaved sequences are also general. Thus they can be applied to other areas of sequence design.

2 Known Constructions of Good Correlation and Two Remedies

In this section, first, we will give a brief summary for all known constructions for 2-level auto correlation sequences and previous known designs for signal sets with low cross correlation in the Galois field configuration. Then we will show some remedies for these known results in order to clear out some confusion in the literature. At last, we will discuss the balance property of 2-level auto-correlation sequences.

2.1 Known Constructions for p-ary Sequences of Period v with 2-level Auto-correlation

The first three classic constructions:

A. For $v = p^n - 1$, all $n \geq 2$, we have m-sequences [39] [9] [43].

B. For $v = p^n - 1$, if $n \geq 6$, n composite, we have GMW [37] and generalized GMW sequences [8] [23] [10]. (Note that a general construction for the generalized GMW sequences have not been explicitly stated in the literature. We will present it later in this section.)

C. Number theory based constructions: $p = 2$

C.1. For all $v = 2^n - 1 =$ prime or $v =$ prime $\equiv 3 \bmod 4$, we have the Quadratic Residue Sequences (Legendre Sequences) [9].

C.2. For all $v = 2^n - 1 =$ prime or $v =$ prime $\equiv 3 \bmod 4$, if $v = 4a^2 + 27$, we also have the Hall's Sextic Residue Sequences [16].

C.3. If v is a product of twin primes, that is, v is of the form $p(p+2)$ where both p and $p+2$ are prime, then we have the Jacobi symbol construction [1].

After 1997, we have the following new constructions for $p = 2$:

D. No-Golomb-Gong-Lee-Gaal Conjectured Sequences [31] (1998):

- 3-Term sequences (also Gong-Gaal-Golomb [12], 1997)
- 5-Term sequences
- Welch-Gong transformation sequences

E. Hyper-oval Construction: Segre case and Glynn types I and II (Maschietti [29], 1998).

F. Kasami Power Function Construction: the special case was conjectured by No, Chung, Yun [33] in 1998 and the general case was conjectured by Dobbertin [5] in 1999.

Remark 1.

1. The sequences obtained by D are special classes of sequences obtained by F. We list them separately due to the historic reason (for example, m-sequences can be considered as a special type of GMW sequences, but we always list them separately) and the point of view of implementation in Section 6 as well.
2. All conjectured sequences with 2-level auto-correlation have been proved by John Dillon and Hans Dobbertin in their latest draft [4] in August 1999.

Remark 2. For the case of $p > 2$ in the literature, we only have two constructions for 2-level auto correlation sequences of period $p^n - 1$ over $\mathbb{F}_p$. One is the m-sequences over $GF(p)$ and the other is the GMW sequences over $\mathbb{F}_p$ associated with a finite field chain of length $r > 0$ [2] [10].

2.2 Previous Known Designs for Signal Sets with Low Correlation in the Galois Field Configuration

Binary Case:

A. Gold-pair Construction and the Generalization: $(2^n - 1, 2^n + 1, 1 + 2^{\lfloor (n+1)/2 \rfloor})$ signal set,

$$\{g(x) + Tr_1^n(\beta x), \beta \in \mathbb{F}_{2^n}\} \cup \{Tr_1^n(x)\}. \tag{2}$$

A.1. $g(x) = Tr_1^n(x^r)$ where r only allows to take a few different values, see [19]. This construction was first published by Gold in 1969 [7] for the case of n odd.

A.2. $g(x)$ can be selected as some special GMW functions[6], [24], or cascaded GMW functions [25], or some decimation of 2-level auto correlation sequences constructed from D and F in Section 2.2. This is considered as a generalization of the Gold-pair Construction since such a signal set can be obtained from the results on cross correlation between an m-sequence and a 2-level auto correlation sequence with the same period.

B. Kasami Construction and the Generalized Kasami Construction: $(2^{2n} - 1, 2^n, 1 + 2^n)$ signal set,

$$\Gamma = \{g(Tr_n^{2n}(x^2) + \beta x^{2^n+1}), \beta \in \mathbb{F}_{2^n}\}. \tag{3}$$

B.1. $g(x) = Tr_1^n(x)$, which represents the Kasami original construction [22].

B.2. $g(x) = Tr_1^n(x^r), gcd(r, 2^n - 1) = 1$ or $g(x)$ is an arbitrary function whose evaluation is a 2-level auto correlation sequence of period $2^n - 1$. These are called the *generalized Kasami constructions.* The former was generalized by No and Kumar [32] in 1989, called No sequences, and the later was partially generalized by No *et al.* [34] in 1998. (We will present it as a fact in the next subsection.)

C. Bent Function Construction: $(2^n - 1, 2^{n/2}, 1 + 2^{n/2})$ $(n = 4k)$ signal set, proposed by Olsen *et al.* [35] in 1982.

D. Interleaved Construction: $((2^n-1)^2, 2^n, 1+2^{n+1})$ signal set, the column sequences are chosen as m-sequences, constructed in 1995 by the author [13].

Non-binary Case: $p > 2$

For $p > 2$, only construction A.1 and C can be generalized to construct p-ary signal sets with low cross correlation in the literature.

A.1 Gold pair construction (as it is defined for the binary case) :
- $(p^n-1, p^n+1, 1+cp^{\lfloor n/2 \rfloor})$ signal sets [41] [19] where $c = \sqrt{p}$ if n odd and $c = 2$ if n even.
- $(p^n-1, p^n+1, 1+\sqrt{p^n})$ signal sets (Kumar *et al.*[27]).

C. Bent construction: $(p^n-1, p^n+1, 1+\sqrt{p^n})$ signal sets , n even [27] [26].

Helleseth has a good survey paper [19] on construction A.1 for both cases of $p = 2$ and $p > 2$. Note that there are only few choices for r in A.1.

In this paper, we will generalize Construction D for both binary and non-binary cases by employing short sequences with 2-level auto correlation. The resulting signal sets have the following types of parameters:

$$((p^n-1)^2, p^n-1, 1+2p^n) \text{ signal sets, any } n,\ p=2 \text{ or } p>2,$$

$$(v^2, v, 2v+3) \text{ signal sets, } v \text{ is prime and } p=2.$$

Moreover, each sequence in such a new set is balanced and the linear span is increased exponentially in n.

2.3 Two Important Remedies

Proposition 1. *Let m be a proper factor of n. Let $h(x)$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ whose evaluation is a 2-level auto correlation sequence of period p^m-1. Let $\sigma(x)$ be a GMW function of length r [23] [10] related to a field chain $\mathbb{F}_{p^m} = F_0 \subset F_1 \subset \cdots \subset F_r = \mathbb{F}_{p^n}$ where r is a positive integer. I.e.,*

$$\sigma(x) = Tr_{F_1/F_0}(x^{s_1}) \circ Tr_{F_2/F_1}(x^{s_2}) \circ \cdots \circ Tr_{F_{r-1}/F_r}(x^{s_r}), x \in \mathbb{F}_r$$

where $\circ$ is a function composition operator and s_i's satisfies $gcd(s_i, |F_i|-1) = 1$. Let $g(x) = h(x) \circ \sigma(x)$, a composition of $\sigma(x)$ and $h(x)$, which is a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then an evaluation of $g(x)$ is a 2-level auto correlation sequence of period p^n-1 (Such sequences are called generalize GMW sequences over $\mathbb{F}_p$).

A proof of this result can be derived from the work of Gordon, Mill, Welch in [8] as early as in 1962, and it also explicitly follows from repeatedly using the result of Klapper, Chan and Goresky in [24] in 1993.

Proposition 2. *Let S be a set consisting of 2^n sequences obtained by the functions in (3) where $g(x)$ is an arbitrary function whose evaluation is a 2-level auto correlation sequence over $\mathbb{F}_2$. Then the cross-correlation* *of any two sequences in S and out of phase auto-correlation values of any sequence in S are three-valued and belong to the set* $\{-1, -1-2^n, 2^n-1\}$.

A proof of Proposition 2 can be obtained by applying a similar method that No *et al.* used for proving Theorem 2 in [34], so we omit it.

Note. According to Proposition 1, all other results in [34] by No *et al.* can be written into the form of (3). By applying Proposition 2, these results follows directly.

2.4 The Balance Property of 2-Level Auto Correlation Sequences

Let $\underline{\mathbf{a}} = \{a_i\}$ be a p-ary sequence of period v. For a fixed $c \in \mathbb{F}_p$, let

$$H_c(\underline{\mathbf{a}}) = |\{i | a_i = c, 0 \leq i < v\}|. \tag{4}$$

I.e., $H_c(\underline{\mathbf{a}})$ is the number of occurrences of an element $c \in F_p$ in a period of the sequence $\underline{\mathbf{a}}$.

Property 1. Let $\underline{\mathbf{a}}$ be a 2-level auto correlation sequence of period v over $\mathbb{F}_p$ constructed from Section 2.1. Then

$$H_c(\underline{\mathbf{a}}) = \begin{cases} (v+1)/p & \text{if } c \in \mathbb{F}_p^* \\ (v+1)/p - 1 & \text{if } c = 0 \end{cases}$$

I.e., any 2-level auto correlation sequence satisfies the balance property.

This property can be directly obtained from the definition of 2-level auto correlation sequences.

3 A Procedure for Constructing Signal Sets and Their Basic Properties

In this section, we will give a procedure to construct a signal set consisting of v (v, v) interleaved sequences and discuss a representation of these sequences, the balance property and some basic properties on cross correlation.

3.1 A Procedure

Procedure 1

1. Choose $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{v-1})$ and $\underline{\mathbf{b}} = (b_0, b_1, \cdots, b_{v-1})$, two sequence over $\mathbb{F}_p$ of period v with 2-level auto-correlation.
2. Choose $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$, an integer sequence whose elements taken from $\mathbf{Z}_v$.
3. Construct $\underline{\mathbf{u}} = (u_0, u_1, \cdots, u_{v^2-1})$, a (v, v) interleaved sequence whose jth column sequence is given by $L^{e_j}(\underline{\mathbf{a}})$, $j = 0, 1, \cdots, v-1$.

4. Set

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

whose elements are defined by

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

5. A signal set $S = S(\underline{\mathbf{a}}, \underline{\mathbf{b}}, \underline{\mathbf{e}})$ is defined as

$$S = \{\underline{\mathbf{s}}_j : j = 0, 1, \cdots, v-1\}.$$

We call $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ *base sequences of* S *and* $\underline{\mathbf{e}}$ *a* shift sequence of S.

For a convenience of notation, we will write $\underline{\mathbf{u}} = \underline{\mathbf{s}}_\infty$ because we can consider that $u_i = u_i + 0$ at Step 4 in Procedure 1. As a convention, we define $\infty \pm r = \infty$ and $\infty \pm \infty = \infty$ where r is an non-negative integer.

Lemma 1. *Let* $\underline{\mathbf{s}}_k$ *be a sequence in* S *and let* $A_k = (A_{k,0}, A_{k,1}, \cdots, A_{k,v-1})$ *be the matrix form of* $\underline{\mathbf{s}}_k$*. Then*

$$A_{k,j} = L^{e_j}(\underline{\mathbf{a}}) + b_{j+k}, 0 \le j < v.$$

Here for $\underline{\mathbf{x}} = (x_0, x_1, \cdots, x_{v-1}) \in F_p^v$ *and* $c \in \mathbb{F}_p$*,* $\underline{\mathbf{x}} + c$ *means that* $\underline{\mathbf{x}} + \underline{\mathbf{c}}$ *where* $\underline{\mathbf{c}} = (c, \cdots, c) \in F_p^v$*. In other words, the* j*th column sequence of* $\underline{\mathbf{s}}_k$ *is the sum of the* j*th column sequence of* $\underline{\mathbf{u}}$ *and the constant* b_{j+k}*.*

Proof. From Steps 1-4 in Procedure 1, for $k \in Z_v$, $\underline{\mathbf{s}}_k \in S$ has the following matrix form

$$\begin{pmatrix} a_{e_0} + b_k & a_{e_1} + b_{k+1} & \cdots & a_{e_{v-1}} + b_{k-1} \\ a_{e_0+1} + b_k & a_{e_1+1} + b_{k+1} & \cdots & a_{e_{v-1}+1} + b_{k-1} \\ a_{e_0+2} + b_k & a_{e_1+2} + b_{k+1} & \cdots & a_{e_{v-1}+2} + b_{k-1} \\ \vdots & & & \\ a_{e_0+v-1} + b_k & a_{e_1+v-1} + b_{k+1} & \cdots & a_{e_{v-1}+v-1} + b_{k-1} \end{pmatrix}$$

which establishes the assertion.

Example 2. Let $p = 2$ and $v = 7$.

1. Choose $\underline{\mathbf{a}} = (1110100)$ and $\underline{\mathbf{b}} = (1001011)$, m-sequences of period 7.
2. Choose $\underline{\mathbf{e}} = (3, 6, 5, 5, 2, 3, 5)$.
3. Construct the interleaved sequence $\underline{\mathbf{u}}$ which is the same as in Example 1.
4. Construct $\underline{\mathbf{s}}_j$: $j = 0, 1, \cdots, 6$.

$\underline{\mathbf{u}} =$

*	-	-	*	-	*	*
0	0	0	0	1	0	0
1	1	0	0	0	1	0
0	1	1	1	1	0	1
0	1	1	1	0	0	1
1	0	1	1	0	1	1
1	1	0	0	1	1	0
1	0	1	1	1	1	1

$\underline{\mathbf{s}}_0$:

1	0	0	1	1	1	1
0	1	0	1	0	0	1
1	1	1	0	1	1	0
1	1	1	0	0	1	0
0	0	1	0	0	0	0
0	1	0	1	1	0	1
0	0	1	0	1	0	0

Since $p = 2$, from Lemma 1, the column sequences of $\underline{\mathbf{s}}_0$ can be obtained from the column sequences of $\underline{\mathbf{u}}$ by complementing columns of $\underline{\mathbf{u}}$ whose indexes correspond to 1's in the sequence $\underline{\mathbf{b}}$. I.e., by complementing columns indicated by *'s in the above diagram we obtain the matrix form of $\underline{\mathbf{s}}_0$. Column sequences of $\underline{\mathbf{s}}_1$ can be obtained by complementing columns of $\underline{\mathbf{u}}$ whose indexes correspond to 1's in the sequence $L(\underline{\mathbf{b}})$, a phase shift 1 of $\underline{\mathbf{b}}$, and so on. In this fashion, we obtain that seven sequences in S are:

$$\underline{\mathbf{s}}_0 = 1001111010100111101101110010001000001011010010100$$

$$\underline{\mathbf{s}}_1 = 0010011111010101010100101110100110011100011001000$$

$$\underline{\mathbf{s}}_2 = 0101010100110000100110010111111010110010001110001$$

$$\underline{\mathbf{s}}_3 = 1011000011111011000011100101000011101110100000011$$

$$\underline{\mathbf{s}}_4 = 0111101101101100001000000000110001010111111100110$$

$$\underline{\mathbf{s}}_5 = 1110110001000010011111001011010100100101000101101$$

$$\underline{\mathbf{s}}_6 = 1100001000011110110001011100011111000000110111010$$

5. Set $S = \{\underline{\mathbf{s}}_0, \underline{\mathbf{s}}_1, \cdots, \underline{\mathbf{s}}_6\}$.

Example 3. Let $p = 3$ and $v = 8$.

1. Choose $\underline{\mathbf{a}} = (2, 1, 0, 1, 1, 2, 0, 1)$ and and $\underline{\mathbf{b}} = (2, 2, 0, 2, 1, 1, 0, 1)$ which are two shift distinct m-sequences over $\mathbb{F}_3$ of degree 2 with period 8.
2. Choose a shift sequence $\underline{\mathbf{e}} = (0, 5, 6, 5, 7, 7, 3, 6) \in \mathbb{Z}_8^{(8)}$.
3. Construct (8, 8) interleaved sequence $\underline{\mathbf{u}}$ which is given in the matrix form as follows:

$\underline{\mathbf{u}} =$

2	2	0	2	1	1	1	0
1	0	1	0	2	2	1	1
0	1	2	1	1	1	2	2
1	2	1	2	0	0	0	1
1	1	0	1	1	1	1	0
2	0	1	0	1	1	2	1
0	1	1	1	2	2	1	1
1	1	2	1	0	0	0	2

4. Construct $\underline{\mathbf{s}}_k, k = 0, 1, \cdots, 7$. The jth column sequence of $\underline{\mathbf{s}}_0$ is equal to the sum of jth column sequence of $\underline{\mathbf{u}}$ and b_j, the jth column sequence of $\underline{\mathbf{s}}_1$ is equal to the sum of jth column sequence of $\underline{\mathbf{u}}$ and b_{1+j}, and so on. In the following, we only list two sequences $\underline{\mathbf{s}}_0$ and $\underline{\mathbf{a}}_5$ in S. We have $A_{0,j} = L^{e_j}(\underline{\mathbf{a}}) + b_j$ and $A_{5,j} = L^{e_j}(\underline{\mathbf{a}}) + b_{5+j}$. I.e.,

$\underline{\mathbf{s}}_0 =$

1	1	0	1	2	2	1	1
0	2	1	2	0	0	1	2
2	0	2	0	2	2	2	0
0	1	1	1	1	1	0	2
0	0	0	0	2	2	1	1
1	2	1	2	2	2	2	2
2	0	1	0	0	0	1	2
0	0	2	0	1	1	0	0

$\underline{\mathbf{s}}_5 =$

0	2	1	1	0	1	0	1
2	0	2	2	1	2	0	2
1	1	0	0	0	1	1	0
2	2	2	1	2	0	2	2
2	1	1	0	0	1	0	1
0	0	2	2	0	1	1	2
1	1	2	0	1	2	0	2
2	1	0	0	2	0	2	0

3.2 The Balance Property of $S(\underline{\mathbf{a}}, \underline{\mathbf{b}}, \underline{\mathbf{e}})$

We will show that any sequence in $S = S(\underline{\mathbf{a}}, \underline{\mathbf{b}}, \underline{\mathbf{e}})$ satisfies the balance property.

Theorem 1. *Let S be constructed by Procedure 1.*

1. *$p = 2$. Each sequence in S has $(v^2+1)/2$ zeros and $(v^2-1)/2$ ones. I.e., it is balanced. In particular, for $v = 2^n - 1$, there are $2^{2n-1} - 2^n + 1$ 0's and $2^{2n-1} - 2^n$ 1's in each signal in S.*
2. *$p > 2$. For each sequence in S, each nonzero element appears $p^{2n-1} - 2p^{n-1}$ times in one period of the sequence and zero element appears $p^{2n-1} - 2p^{n-1} + 1$ times. I.e., it is balanced.*

Proof. Let $\underline{\mathbf{s}}_k \in S$. According to Lemma 1, the column sequences $A_{k,j}$ of the sequence $\underline{\mathbf{s}}_k$ can be represented by

$$A_{k,j} = L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}, 0 \le j < v. \tag{5}$$

Binary Case: $p = 2$.

Note that both $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are 2-level auto-correlation sequences. According to Property 1, there are $\frac{v+1}{2}$ 1's and $\frac{v-1}{2}$ 0's in each of them. Thus for $j : 0 \le j < v$, there are $\frac{v+1}{2}$ j's such that the $H_1(L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}) = \frac{v-1}{2}$ and $\frac{v-1}{2}$ j's such that $H_1(L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}) = \frac{v+1}{2}$. Thus the Hamming weight of $\underline{\mathbf{s}}_k \in S$ is given by

$$H_1(\underline{\mathbf{s}}_k) = \sum_{j=0}^{v-1} H_1(A_{k,j}) = \sum_{j=0}^{v-1} H_1(L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}) = \frac{v+1}{2}\frac{v-1}{2} + \frac{v-1}{2}\frac{v+1}{2} = \frac{v^2-1}{2}.$$

Therefore zero occurs $v^2 - (v^2-1)/2 = (v^2+1)/2$ in $\underline{\mathbf{s}}_k$. So the result is true.

Non-binary Case: $p > 2$

In this case, we have $v = p^n - 1$ from Section 2.1. Applying Property 1, for each $j : 0 \le j < v$, we have

$$H_c(L^{e_j}(\underline{\mathbf{a}})) = \begin{cases} p^{n-1} & \text{if } c \in \mathbb{F}_p^* \\ p^{n-1} - 1 & \text{if } c = 0 \end{cases} \tag{6}$$

where $H_c(.)$ is defined by (4). From (5), if $b_{k+j} = 0$, then

$$H_d(A_{k,j}) = H_d(L^{e_j}(\underline{\mathbf{a}})) \tag{7}$$

If $b_{k+j} \ne 0$, then there are $p-2$ non-zeros c's in $\mathbb{F}_p$ for which $c + b_{k+j} \ne 0$ and there is one nonzero $c = -b_{k+j} \ne 0$ in $\mathbb{F}_p$ for which $c + b_{k+j} = 0$. Therefore for $b_{k+j} \ne 0$ and $d = c + b_{k+j}, c \in F_p$, we have

$$H_d(L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}) = \begin{cases} p^{n-1} & d \ne 0 \text{ for } p-2\ c\text{'s in } \mathbb{F}_p^* \\ p^{n-1} & d = 0 \text{ for } c = -b_{k+j} \ne 0 \\ p^{n-1} - 1 & d \ne 0 \text{ for } c = 0. \end{cases} \tag{8}$$

First applying Lemma 1, then applying (6)-(8), for each $d \in F_p^*$, we obtain that

$$\begin{aligned}
H_d(\underline{\mathbf{s}}_k) &= \sum_{j=0}^{v-1} H_1(A_{k,j}) = \sum_{j=0}^{v-1} H_d(L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}) \\
&= \sum_{\substack{b_{k+j}=0 \\ 0 \le j < v}} H_d(L^{e_j}(\underline{\mathbf{a}})) + \sum_{\substack{b_{k+j} \ne 0 \\ 0 \le j < v}} H_d(L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}) \\
&= (p^{n-1} - 1)p^{n-1} + ((p-2)p^{n-1} + (p^{n-1} - 1))p^{n-1} \\
&= p^{2n-1} - 2p^{n-1}
\end{aligned}$$

Hence

$$H_0(\underline{\mathbf{s}}_k) = (p^n - 1)^2 - (p-1)(p^{2n-1} - 2p^{n-1}) = p^{2n-1} - 2p^{n-1} + 1$$

which completes the proof.

Procedure 1 provides a general method to construct balanced sequences. In other words, from the proof of Theorem 1, we have established the following assertion.

Corollary 1. *Let $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ be balanced sequences of period v where $v = p^n - 1$ or v is prime and $\underline{\mathbf{e}} \in \mathbb{Z}_v^v$. Let S be constructed by Procedure 1, then each sequence in S is balanced and has the distribution stated in Theorem 1.*

3.3 Cross Correlation of Interleaved Sequences

In the rest of this section, we will investigate a formula for computing correlation functions of interleaved sequences when their matrix forms are applied. Let $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{v-1})$ and $\underline{\mathbf{b}} = (b_0, b_1, \cdots, b_{v-1})$ be two vectors of $\mathbb{F}_p^v$. We define

$$< \underline{\mathbf{a}}, \underline{\mathbf{b}} >= \sum_{i=0}^{v-1} \omega^{a_i + b_i} \tag{9}$$

which is an inner product of two complex vectors $(\omega^{a_0}, \omega^{a_1}, \cdots, \omega^{a_{v-1}})$ and $(\omega^{b_0}, \omega^{b_1}, \cdots, \omega^{b_{v-1}})$.

Proposition 3. *Let $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ be two sequences over $\mathbb{F}_p$ of period v. For $\tau \ge 0$,*

(a) $< \underline{\mathbf{a}}, \underline{\mathbf{b}} >= C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(0)$.

(b) $< \underline{\mathbf{a}}, L^\tau(\underline{\mathbf{b}}) >= C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$.

(c) $< L^i(\underline{\mathbf{a}}), L^{j+\tau}(\underline{\mathbf{a}}) >= C_{L^i(\underline{\mathbf{a}}),L^j(\underline{\mathbf{a}})}(\tau) = C_{\underline{\mathbf{a}}}(j - i + \tau)$ *where* $i, j \ge 0$.

(d) For $c, d \in \mathbb{F}_p$,

$$< \underline{\mathbf{a}} + c, \underline{\mathbf{b}} + d >= \omega^{c+d} < \underline{\mathbf{a}}, \underline{\mathbf{b}} > .$$

Proof. Assertions (a)-(d) are immediate from the definition of the correlation function and (9).

For a (v,v) interleaved sequence $\underline{\mathbf{u}}$ associated with $(\underline{\mathbf{a}},\underline{\mathbf{e}})$, in order to conveniently study a cyclic shift of $\underline{\mathbf{u}}$, we extend its shift sequence $\underline{\mathbf{e}}=(e_0,e_1,\cdots,e_{v-1})\in Z_v^v$ to $(e_0,e_1,\cdots,e_{2v-1})\in Z_v^{2v}$ by defining

$$e_{v+j}=1+e_j, 0\le j<v. \tag{10}$$

We still use the symbol $\underline{\mathbf{e}}$ for that.

Proposition 4. *Let $\underline{\mathbf{u}}$ be a (v,v)-interleaved sequence associated with $(\underline{\mathbf{a}},\underline{\mathbf{e}})$. For $\tau\ge 0$, let $T=(T_0,T_1,\cdots,T_{v-1})$ be the matrix form of $L^\tau(\underline{\mathbf{u}})$. If we write $\tau=rv+s, 0\le r,s<v$, then*

$$T_j=L^{r+e_{s+j}}(\underline{\mathbf{a}}), 0\le j<v.$$

Proof. Let $A=(A_0,A_1,\cdots,A_{v-1})=(a_{i,j})$ be the matrix form of $\underline{\mathbf{u}}$. From the definition, $A_j=L^{e_j}\underline{\mathbf{a}}, 0\le j<v$. Note that the first element in the sequence $L^\tau(\underline{\mathbf{u}})$ is the entry $a_{r,s}$. From the definition of the interleaved sequences, we have $a_{r,v+j}=a_{r+1,j}$ for each j with $v-s\le j<v$. So T has the following form

$$\begin{pmatrix}
a_{r,s} & \cdots a_{r,v-1} & a_{r+1,0} \cdots a_{r+1,s-1} \\
a_{r+1,s} & \cdots a_{r+1,v-1} & a_{r+2,0} \cdots a_{r+2,s-1} \\
\vdots & & \\
a_{v-1,s} & \cdots a_{v-1,v-1} & a_{1,0} \quad \cdots a_{1,s-1} \\
\vdots & & \\
a_{r-1,s} & \cdots a_{r-1,v-1} & a_{r,0} \quad \cdots a_{r,s-1}
\end{pmatrix}.$$

Therefore for $0\le j<v-s$, we have

$$T_j=L^r(A_{s+j})=L^r(L^{e_{s+j}}(\underline{\mathbf{a}}))=L^{r+e_{s+j}}(\underline{\mathbf{a}}). \tag{11}$$

For $v-s\le j<v$, we have

$$T_j=L^{r+1}(A_{j-(v-s)})=L^{r+1}(L^{e_{j-(v-s)}}(\underline{\mathbf{a}}))=L^{r+1+e_{j-(v-s)}}(\underline{\mathbf{a}}). \tag{12}$$

Applying (10), $1+e_{j-(v-s)}=e_{j-(v-s)+v}=e_{s+j}$ for $v-s\le j<v$. Substituting it into (12), we get that $T_j=L^{r+e_{j+s}}(\underline{\mathbf{a}})$ with $v-s\le j<v$. Together with (11), the result follows.

From Proposition 4 and Lemma 1, the following result is immediate.

Lemma 2. *For $\underline{\mathbf{s}}_k\in S$ and $\tau=rv+s$ with $0\le s<v$ and $r\ge 0$, the jth column sequence of $L^\tau(\underline{\mathbf{s}}_k)$ is given by*

$$L^{r+e_{s+j}}(\underline{\mathbf{a}})+b_{k+s+j}, 0\le j<v.$$

Proposition 5. *Let $\underline{\mathbf{u}}$ and $\underline{\mathbf{w}}$ be two (v,v) interleaved sequences over $\mathbb{F}_p$. Let $A=(A_0,A_1,\cdots,A_{v-1})$ and $T=(T_0,T_1,\cdots,T_{v-1})$ be the matrix forms of $\underline{\mathbf{u}}$ and $L^\tau(\underline{\mathbf{w}})$ respectively where $\tau\ge 0$. Then the cross correlation between $\underline{\mathbf{u}}$ and $\underline{\mathbf{w}}$ can be computed by*

$$C_{\underline{\mathbf{u}},\underline{\mathbf{w}}}(\tau)=\sum_{j=0}^{v-1}<A_j,T_j>.$$

Proof. The result follows directly from Proposition 3-(b) and Proposition 4.

Lemma 3. *Let $\underline{\mathbf{s}}_h$ and $\underline{\mathbf{s}}_k$ be two sequences in S. Let τ be an nonnegative integer. We write $\tau = rv + s$ with $0 \le s < v$ and $r \ge 0$. Then $C_{h,k}(\tau)$, the cross correlation between $\underline{\mathbf{s}}_h$ and $\underline{\mathbf{s}}_k$, can be computed by*

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} \omega^{d_j} C_{\underline{\mathbf{a}}}(t_j)$$

where

$$d_j = b_{h+j} - b_{k+s+j} \tag{13}$$

$$t_j = e_{j+s} - e_j + r. \tag{14}$$

Proof. Let $D = (D_0, D_1, \cdots, D_{v-1})$ and $T = (T_0, T_1, \cdots, T_{v-1})$ are the matrix forms of $\underline{\mathbf{s}}_h$ and $L^\tau(\underline{\mathbf{s}}_k)$ respectively. According to Proposition 5,

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} < D_j, T_j > .$$

From Lemmas 1 and 2, for $0 \le j < v$, we have

$$D_j = L^{e_j}(\underline{\mathbf{a}}) + b_{k+j}$$

$$T_j = L^{r+e_{s+j}}(\underline{\mathbf{a}}) + b_{k+s+j}.$$

Applying Proposition 3-(d), then (c), we get

$$\begin{aligned} < D_j, T_j > &= < L^{e_j}(\underline{\mathbf{a}}) + b_{h+j}, L^{e_{s+j}+r}(\underline{\mathbf{a}}) + b_{k+s+j} > \\ &= \omega^{b_{h+j}+b_{k+s+j}} < L^{e_j}(\underline{\mathbf{a}}), L^{e_{s+j}+r}(\underline{\mathbf{a}}) > \\ &= \omega^{d_j} C_{\underline{\mathbf{a}}}(e_{s+j} + r - e_j) \\ &= \omega^{d_j} C_{\underline{\mathbf{a}}}(t_j) \end{aligned}$$

where d_j and t_j are defined by (13) and (14). Thus the assertion follows.

□

This lemma will be used in the next section for determining cross correlation of sequences in S.

4 Constructions for $(v^2, v, 2v+3)$ signal sets

In this section, first we will give a criterion for the shift sequence $\underline{\mathbf{e}}$ such that S, constructed by Procedure 1, is a $(v^2, v, 2v+3)$ signal set. Then we will provide two methods to construct the shift sequence $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$ satisfying the criterion.

Theorem 2. *Let S be constructed by Procedure 1. If the shift sequence $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$ satisfies the following condition,*

$$|\{e_j - e_{j+s} | 0 \leq j < v - s\}| = v - s, \text{ for all } 1 \leq s < v. \tag{15}$$

Then S is a $(v^2, v, 2v+3)$ signal set. In particular, for $p = 2$, the cross-correlation of any two sequences in S and out of phase auto-correlation values of any sequence in S belong to the set $\{1, -v, v+2, 2v+3, -2v-1\}$.

In order to prove Theorem 2, we need to show that any pair of sequences in S are shift distinct, any sequence in S has period v^2, and the maximal magnitude value of cross correlation values of any two sequences in S and out of phase auto-correlation values of any sequence in S is $2v+3$. In this following, we will separate the first two results as two lemmas.

Lemma 4. *Let S be constructed by Procedure 1. If the shift sequence $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$ satisfies (15). Then any pair of sequences in S are shift-distinct.*

Proof. Let $\underline{\mathbf{s}}_h$ and $\underline{\mathbf{s}}_k$ be two different sequences in S. If they are shift equivalent, then there exists an non-negative integer τ such that

$$\underline{\mathbf{s}}_h = L^\tau(\underline{\mathbf{s}}_k). \tag{16}$$

Let $D = (D_0, D_1, \cdots, D_{v-1})$ and $T = (T_0, T_1, \cdots, T_{v-1})$ be the matrix forms of $\underline{\mathbf{s}}_h$ and $L^\tau(\underline{\mathbf{s}}_k)$ respectively. We write $\tau = rv + s$ with $0 \leq s < v, r \geq 0$. Applying Lemmas 1 and 2, we have

$$D_j = L^{e_j}(\underline{\mathbf{a}}) + b_{h+j}, 0 \leq j < v$$
$$T_j = L^{r+e_{s+j}}(\underline{\mathbf{a}}) + b_{k+s+j}, 0 \leq j < v.$$

From (16), we have

$$D_j = T_j, 0 \leq j < v. \tag{17}$$

Next we will show that (17) implies that $h \equiv k + s \bmod v$. If not, then there exists some j for which $b_{h+j} = 0$ and $b_{k+s+j} = c \neq 0$. Since $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are 2-level auto correlation sequences, from Property 1, these two sequences $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ together with their all phase shifts are balanced. Consequently,

$$H_0(D_j) = (v+1)/p - 1 \text{ and } H_0(T_j) = (v+1)/p.$$

Therefore $D_j \neq T_j$ for such j which is a contradiction with (17). Thus from (17), we derive that

$$h \equiv k + s \bmod v. \tag{18}$$

Therefore $s \neq 0$ since $h \neq k$. Again using (17), we get

$$L^{e_j}(\underline{\mathbf{a}}) = L^{r+e_{s+j}}(\underline{\mathbf{a}}), 0 \leq j < v. \tag{19}$$

The above identities are true if and only if

$$e_j \equiv r + e_{s+j} \pmod v, 0 \leq j < v. \tag{20}$$

Since $(e_0, e_1, \cdots, e_{v-1})$ satisfies the condition (15), then there are at most two j's with $0 \leq j < v$ such that the above identities are true which is a contradiction. Therefore $\underline{\mathbf{s}}_h$ and $\underline{\mathbf{s}}_k$ are shift distinct if $h \neq k$.

Lemma 5. *Let S be constructed by Procedure 1. If the shift sequence $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$ satisfies (15). Then each sequence in S has period v^2.*

Proof. Let $\underline{\mathbf{s}}_k \in S$ and let $per(\underline{\mathbf{s}}_k)$ represent the period of $\underline{\mathbf{s}}_k$. Then $per(\underline{\mathbf{s}}_k)$ divides v^2. From Procedure 1, $\underline{\mathbf{s}}_k = \underline{\mathbf{u}} + L^k(\underline{\mathbf{b}})$ where $\underline{\mathbf{b}}$ has period v. Therefore we only need to prove that $per(\underline{\mathbf{u}}) = v^2$. Let $per(\underline{\mathbf{u}}) = \tau$. Thus we have

$$\underline{\mathbf{u}} = L^{\tau}(\underline{\mathbf{u}}). \tag{21}$$

Applying a similar argument that used in the proof of Lemma 4, we can get (20). If $s \neq 0$, then $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$ satisfies (15). Therefore there are at most two j's with $0 \leq j < v$ satisfies (20), which is a contradiction. So $s = 0 \Longrightarrow \tau = rv$. From the equation (19) with $s = 0$, it follows that each column sequence of $\underline{\mathbf{u}}$ has period r. Note that $per(\underline{\mathbf{a}}) = v$ and all column sequences of $\underline{\mathbf{u}}$ are phase shifts of $\underline{\mathbf{a}}$. So all column sequences of $\underline{\mathbf{u}}$ have period v. Thus $r = v \Longrightarrow per(\underline{\mathbf{u}}) = v^2 \Longrightarrow per(\underline{\mathbf{s}}_k) = v^2$ which completes the proof.

The following result comes from the property of pth primitive roots of unity.

Property 2. Let $\underline{\mathbf{d}} = \{d_i\}$ be a sequence over $\mathbb{F}_p$ of period v where $v = p^n - 1$ for $p > 2$ and $v = 2^n - 1$ or $v = prime$ for $p = 2$. If $\underline{\mathbf{d}}$ is balanced, then

$$\sum_{i=0}^{v-1} \omega^{d_i} = -1.$$

Proof of Theorem 2. According to Lemma 5, each sequence in S has period v^2. From Lemma 4, each pair of sequences in S are shift distinct. Thus there are v shift distinct sequences in S. So we only need to show the cross correlation of S. We write $\tau = rv + s, 0 \leq s < v, r \geq 0$. For two different sequences $\underline{\mathbf{s}}_h, \underline{\mathbf{s}}_k$ in S, according to Lemma 3, we have

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} \omega^{d_j} C_{\underline{\mathbf{a}}}(t_j) \tag{22}$$

where the d_j and t_j are defined in Lemma 3. Since $\underline{\mathbf{a}}$ is 2-level auto correlation sequences, then

$$C_{\underline{\mathbf{a}}}(t_j) = \begin{cases} v & \text{for } t_j \equiv 0 \pmod v \\ -1 & \text{for } t_j \not\equiv 0 \pmod v \end{cases}$$

Let $\underline{\mathbf{d}} = (d_0, d_1, \cdots, d_{v-1})$. Then

$$\underline{\mathbf{d}} = L^h(\underline{\mathbf{b}}) - L^{k+s}(\underline{\mathbf{b}}). \tag{23}$$

Noticing that $\underline{\mathbf{b}}$ is also a two-level auto correlation sequence, from Property 1, $\underline{\mathbf{d}}$ is a balanced sequence if $\underline{\mathbf{d}} \neq 0$. I.e.,

$$H_0(\underline{\mathbf{d}}) = \begin{cases} v & \text{if } h \equiv k+s \bmod v \\ (v+1)/p - 1 & \text{if } h \not\equiv k+s \bmod v. \end{cases} \tag{24}$$

Case 1. $s = 0$.

In this case, $t_j = r$ from (14). Since $\underline{\mathbf{d}} \neq 0$, from (22) and Property 2, we have

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} \omega^{d_j} C_{\underline{\mathbf{a}}}(r) = C_{\underline{\mathbf{a}}}(r) \sum_{j=0}^{v-1} \omega^{d_j} = -C_{\underline{\mathbf{a}}}(r).$$

which gives that

$$C_{h,k}(rv) \in \{1, -v\}.$$

Case 2. $s \neq 0$.

Let N be the number of j with $0 \leq j < v$ such that $t_j \equiv 0 \bmod v$. I.e.,

$$N = |\{0 \leq j < v | e_j - e_{j+s} \equiv r \bmod v\}|. \tag{25}$$

Note that r is a constant. Since the shift sequence $\underline{\mathbf{e}}$ satisfies (15), then $N \in \{0, 1, 2\}$. Thus we have the following three cases:

(c1) $N = 0$. I.e., $t_j \not\equiv 0$ for all j with $0 \leq j < v$. Thus $C_{\underline{\mathbf{a}}}(t_j) = -1$ for all j with $0 \leq j < v$.

(c2) $N = 1$. Then there exists exactly one j with $0 \leq j < v$ such that $t_j \equiv 0 \pmod v$. Hence there is one j such that $C_{\underline{\mathbf{a}}}(t_j) = v$ and for all the other j, $C_{\underline{\mathbf{a}}}(t_j) = -1$. We can suppose $t_0 = 0$ without loss of generality.

(c3) $N = 2$. In this case there are two j's with $0 \leq j < v$ such that $C_{\underline{\mathbf{a}}}(t_j) = v$ and for all the other j, $C_{\underline{\mathbf{a}}}(t_j) = -1$. We can assume that $t_0 = 0$ and $t_1 = 0$ without loss of generality.

Next we will determine the value of $C_{h,k}(\tau)$ according to the following two sub-cases.

Case 2-1. $h \equiv k + s \bmod v$. In this case, we have $d_j = 0$ for all j. From (22), we have

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} C_{\underline{\mathbf{a}}}(t_j). \tag{26}$$

Consequently, $C_{h,k}(\tau)$ takes values $-v, 1$, and $v+2$ corresponding to $N = 0, 1$, and 2.

Case 2-2. $h \not\equiv k + s \bmod v$. In this case, $\underline{\mathbf{d}} \neq 0$. So

$$\sum_{i=0}^{v-1} \omega^{d_i} = -1. \tag{27}$$

For $N=0$, using (22) and (27), we have

$$C_{h,k}(\tau) = (-1)\sum_{j=0}^{v-1}\omega^{d_j} = (-1)(-1) = 1. \tag{28}$$

For $N=1$, (22) gives that

$$C_{h,k}(\tau) = \omega^{d_0}v + (-1)\sum_{j=0}^{v-1}\omega^{d_j} + \omega^{d_0} = \omega^{d_0}(v+1)+1. \tag{29}$$

Thus

$$|C_{h,k}(\tau)| = |\omega^{d_0}(v+1)+1| \leq |\omega^{d_0}(v+1)|+1 = v+2.$$

In particular, if $p=2$, from (29), we get that $C_{h,k}(\tau)=v+2$ if $d_0=0$ and $C_{h,k}(\tau)=-v$ if $d_0=1$.

For $N=2$,

$$C_{h,k}(\tau) = (\omega^{d_0}+\omega^{d_1})v + 1 + \omega^{d_0}+\omega^{d_1} = (\omega^{d_0}+\omega^{d_1})(v+1)+1.$$

Thus

$$|C_{h,k}(\tau)| = |(\omega^{d_0}+\omega^{d_1})(v+1)+1| \leq |(\omega^{d_0}(v+1)|+|(\omega^{d_1}(v+1)|+1 = 2v+3.$$

In particular, if $p=2$, then $C_{h,k}(\tau)$ takes values 1, $2v+3$, $-2v-1$ for $d_0=1+d_1, d_0=d_1=0, d_0=d_1=1$ respectively. The proof is now completed.

Example 4. We can verify that the shift sequences in Examples 2 and 3 satisfy (15). Applying Theorem 2, we have

- Example 2 is a $(49,7,17)$ binary signal set.
- Example 3 is a $(64,8,19)$ 3-ary signal set.

Corollary 2. *For $\underline{\mathbf{u}}$ be an (v,v) interleaved sequence associates with $(\underline{\mathbf{a}},\underline{\mathbf{e}})$. If the shift sequence of $\underline{\mathbf{u}}$ satisfies (15), then the out of phase auto correlation of $\underline{\mathbf{u}}$ is 3-valued. Precisely, let N be defined by (25), then*

$$C_{\underline{\mathbf{u}}}(\tau) = \begin{cases} -v & \text{if } N=0 \text{ or } s=0 \\ 1 & \text{if } N=1 \\ v+2 & \text{if } N=2 \end{cases}$$

where $\tau = rv+s$ with $0\leq s<v$ and $r\geq 0$.

Proof. Note that $d_j=0, 0\leq j<v$ in this case. From Lemma 3,

$$C_{\underline{\mathbf{u}}}(\tau) = \sum_{j=0}^{v-1} C_{\underline{\mathbf{a}}}(t_j). \tag{30}$$

If $s=0$, then $t_j=r$ where $r\neq 0$ since $\tau\neq 0$. Thus $C_{\underline{\mathbf{a}}}(t_j)=C_{\underline{\mathbf{a}}}(r)=-1$ for all j with $0\leq j<v$. Therefore $C_{\underline{\mathbf{u}}}(\tau)=-v$. If $s\neq 0$, (30) is Case 2-1 in the proof of Theorem 2. Thus the result is true.

Remark 3. The author (1995, [13]) introduced the idea of Procedure 1 for constructing $((2^n-1)^2, 2^n-1, 1+2^{n+1})$ binary signal sets where $v = 2^n - 1$, $\underline{\mathbf{a}}$ is a binary m-sequence of period $2^n - 1$ and $\underline{\mathbf{b}}$ is a binary GMW sequence of period $2^n - 1$, proved Theorem 2 for such construction, and discovered the following two constructions of shift sequences with (15).

Construction A: $((p^n-1)^2, p^n-1, 2p^n+1)$ signal set.

1. Choose $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$, two sequences over $\mathbb{F}_p$ of period $p^n - 1$ with 2-level auto-correlation (may not be different) constructed in Section 2.1.
2. Choose α and β, primitive elements of $\mathbb{F}_{p^{2n}}$ and $\mathbb{F}_{p^n}$ respectively.
3. Compute e_j's satisfying

$$\beta^{e_j} = Tr_n^{2n}(\eta\alpha^{j+1}), 0 \leq j < p^n - 1 \tag{31}$$

where $Tr_n^{2n}(x)$ is the trace function from $\mathbb{F}_{p^{2n}}$ to $\mathbb{F}_{p^n}$ and $\eta \in \mathbb{F}_{p^{2n}}$ with $Tr_n^{2n}(\eta) = 0$.

Construction B: $(v^2, v, 2v+3)$ binary signal set where v is prime.

1. Choose $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$, two 2-level auto correlation sequences over $\mathbb{F}_2$ with a prime period v constructed in Section 2.1.
2. Choose α, a primitive element of $\mathbb{F}_v$.
3. Set

$$e_j = \alpha^j, 0 \leq j < v. \tag{32}$$

Lemma 6. *The shift sequence* $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_{v-1})$*, constructed from Construction A for* $v = p^n - 1$ *or Construction B for* v *a prime, satisfies the condition (15) in Theorem 2.*

A proof of this Lemma can be found in [13].

Remark 4. Let X represent the set of 2-level auto correlation sequences over $\mathbb{F}_p$ constructed by Construction X in Section 2.1.

1. For $p > 2$, we have Construction A for constructing a shift sequence of S and $A \cup B$ as a domain for choosing two base sequences.
2. For $p = 2$ and $v = 2^n - 1$ is not prime, we have Construction A for constructing a shift sequence of S and $A \cup B \cup D \cup E \cup F$ as a domain for choosing two base sequences.
3. For $p = 2$ and v is a prime number but v can not be written as $v = 2^n - 1$, we have Construction B for constructing a shift sequence of S and $C.1 \cup C.2$ as a domain for choosing two base sequences.
4. For $p = 2$ and $v = 2^n - 1$ is a prime number, then we have both Constructions A and B for constructing a shift sequence of S and $A \cup C.1 \cup C.2 \cup D \cup E \cup F$ as a domain for choosing two base sequences.

Example 5. In the following, we will explain how to obtain the shift sequences given in Examples 2 and 3 by using Construction A.

1. Computation of the shift sequence in Example 2. Here $p = 2$, $n = 3$, and $v = 2^3 - 1 = 7$. Let α be a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $h(x) = x^6 + x + 1$.(I.e., $h(\alpha) = 0$ and $h(x)$ is the polynomial over $\mathbb{F}_2$ with a smallest degree among the set consisting of polynomials over $\mathbb{F}_2$ having α as one of their root.) Let $\beta = \alpha^9$. Then β is a primitive element of $\mathbb{F}_{2^3}$ whose minimal polynomial over $\mathbb{F}_2$ is $g(x) = x^3 + x^2 + 1$. Choose $h(x)$ and $g(x)$ as the defining polynomials of $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^3}$ respectively. We compute $\{e_j : 0 \leq j < 7\}$ in the following way

$$\beta^{e_j} = Tr_3^6(\alpha^{j+1}), j = 0, 1, \cdots, 6, \eta = 1$$

where $Tr_3^6(x)$ is the trace function from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^3}$. Then we get the shift sequence in Example 2 as follows

$$\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_6) = (3, 6, 5, 5, 2, 3, 5).$$

According to Lemma 6, $\underline{\mathbf{e}}$ satisfies (15), applying Theorem 2, S, given by Example 2, is a $(49, 7, 17)$ signal set over $\mathbb{F}_2$.

2. Computation of the shift sequence in Example 3. Here $p = 3$, $n = 2$, and $v = 3^2 - 1 = 8$. Let α be a primitive element of $\mathbb{F}_{3^4}$ whose minimal polynomial over $\mathbb{F}_3$ is $h(x) = x^4 + x + 2$. Let $\beta = \alpha^{10}$. Then β is a primitive element of $\mathbb{F}_{3^2}$ whose minimal polynomial over $\mathbb{F}_3$ is $g(x) = x^2 + x + 2$. Choose $h(x)$ and $g(x)$ as the defining polynomials of $\mathbb{F}_{3^4}$ and $\mathbb{F}_{3^2}$ respectively. We compute $\{e_j : 0 \leq j < 8\}$ in the following way

$$\beta^{e_j} = Tr_2^4(\alpha^6 \alpha^{j+1}), j = 0, 1, \cdots, 7, \eta = \alpha^6$$

where $\mathrm{T}r_2^4(x)$ is the trace function from $\mathbb{F}_{3^4}$ to $\mathbb{F}_{3^2}$. Then we get the shift sequence in Example 2 as follows

$$\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_7) = (0, 5, 6, 5, 7, 7, 3, 6).$$

According to Lemma 6, $\underline{\mathbf{e}}$ satisfies (15). Applying Theorem 2, S given by Example 3 is a $(64, 8, 19)$ signal set over $\mathbb{F}_3$.

In the following, we will give an example which is the case of Remark 4-(3).

Example 6. Let $p = 2$ and $v = 11$, a prime. Choose

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

which are shift-distinct quadratic sequences of period 11. We now use Construction B to construct a shift sequence. Since 2 is a primitive element of $\mathbb{F}_{11}$, we then compute $e_j \equiv 2^j \bmod 11$, $0 \leq j < 11$. Thus

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

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

$\underline{\mathbf{u}} =$:

*	-	*	-	-	-	*	*	*	-	*
1	0	1	0	1	0	1	0	1	0	1
0	1	1	1	0	1	0	0	1	0	0
1	1	0	0	0	1	1	1	1	0	1
1	1	0	1	0	0	1	0	0	1	1
1	0	0	1	1	1	0	1	0	0	1
0	0	1	0	0	1	1	1	0	1	0
0	0	0	1	1	1	1	0	1	1	0
0	1	1	1	1	0	1	1	0	0	0
1	0	1	1	0	0	0	1	1	1	1
0	1	0	0	1	0	0	1	1	1	0
1	1	1	0	1	1	0	0	0	1	1

According to Procedure 1, we can construct 11 sequences in S by using $\underline{\mathbf{u}}$ and $\underline{\mathbf{b}}$. For example, the elements of $\underline{\mathbf{s}}_0$ can be obtained by complement of the columns of $\underline{\mathbf{u}}$ for which correspond to *'s in the above diagram. I.e.,

$\underline{\mathbf{s}}_0 =$

0	0	0	0	1	0	0	1	0	0	0
1	1	0	1	0	1	1	1	0	0	1
0	1	1	0	0	1	0	0	0	0	0
0	1	1	1	0	0	0	1	1	1	0
0	0	1	1	1	1	1	0	1	0	0
1	0	0	0	0	1	0	0	1	1	1
1	0	1	1	1	1	0	1	0	1	1
1	1	0	1	1	0	0	0	1	0	1
0	0	0	1	0	0	1	0	0	1	0
1	1	1	0	1	0	1	0	0	1	1
0	1	0	0	1	1	1	1	1	1	0

According to Lemma 6 and Theorem 2, S is a (121, 11, 25) signal set over $\mathbb{F}_2$.

5 Linear Span of Sequences in $(v^2, v, 2v+3)$ Signal Sets

In this section, we will derive the linear span of sequences in a $(v^2, v, 2v+3)$ signal set. Precisely, we will establish the following result.

Theorem 3. *Let $S = S(\underline{\mathbf{a}}, \underline{\mathbf{b}}, \underline{\mathbf{e}})$ be a $(v^2, v, 2v+3)$ signal set constructed by Procedure 1 where $\underline{\mathbf{e}}$ is given by Construction A or Construction B in Section 4.*

1. *If $\underline{\mathbf{e}}$ is given by Construction A (here $v = p^n - 1$, we suppose that $n > 1$), then the linear span of any sequence $\underline{\mathbf{s}}_k$ in S, $0 \le k < v$, is bounded by*

$$LS(\underline{\mathbf{s}}_k) \ge \frac{p^n-1}{2} LS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}}), 0 \le k < v \text{ and } LS(\underline{\mathbf{u}}) \ge \frac{p^n-1}{2} LS(\underline{\mathbf{a}}).$$

2. *Let $f(x) = f_1(x) \cdots f_s(x)$ be the minimal polynomial of the base sequence $\underline{\mathbf{a}}$ over $\mathbb{F}_p$ where the f_i are irreducible over $\mathbb{F}_p$. If $f_i(x)$ has period v for each $i : 1 \le i \le s$, then the linear span of any sequence in S is determined by*

$$LS(\underline{\mathbf{s}}_k) = vLS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}}), 0 \le k < v \text{ and } LS(\underline{\mathbf{u}}) = vLS(\underline{\mathbf{a}}). \tag{33}$$

3. *If $\underline{\mathbf{e}}$ is given by Construction B, in this case we have $p = 2$ and v is prime, then the linear span of any sequence in S is given by (33). In particular, if both $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are quadratic sequences, then each sequence in S has linear span $(v^2-1)/2$ which is the maximal value.*

In order to prove Theorem 3, we need to develop several results on linear span of the interleaved sequence $\underline{\mathbf{u}}$ associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where the minimal polynomial of $\underline{\mathbf{a}}$ is reducible. In the following, we first investigate a decomposition of the interleaved sequence $\underline{\mathbf{u}}$ and linear span of the sum of a (v, v) interleaved sequence $\underline{\mathbf{u}}$ and an arbitrary sequence of period v. Then by using the Berlekamp-Massey algorithm, we derive a lower bound of the linear span of the interleaved sequence $\underline{\mathbf{u}}$ when the shift sequence is given by Construction A. Last we give a proof for Theorem 3.

Note. All results developed in the following are general, which can be applied to other areas in sequence design.

5.1 Decomposition of Interleaved Sequences

In this subsection, we first list some results on the minimal polynomials and periods of compositions of periodic sequences, and then discuss a decomposition of the interleaved sequences. We denote $per(s)$ a period of a sequence s which means that $per(s)$ is the smallest integer such that $s_{t+i} = s_i, i = 0, 1, \cdots,$ for $s = s_0, s_1, \cdots$ or a period of a polynomial s which means that $per(s)$ is the smallest integer such that $s(x) | x^t - 1$ for $s = s(x)$.

Fact 1 *Let $\underline{\mathbf{a}}$ be a sequence over $\mathbb{F}_p$ of period v. If there exists n such that v is a factor of $p^n - 1$, then the minimal polynomial of $\underline{\mathbf{a}}$ has no multiple roots. In particular, if v is a prime, then the minimal polynomial of $\underline{\mathbf{a}}$ has no multiple roots.*

Fact 2 *Let $\underline{\mathbf{c}} = \underline{\mathbf{c}}_1 + \underline{\mathbf{c}}_2$ where $\underline{\mathbf{c}}_1$ and $\underline{\mathbf{c}}_2$ be two nonzero periodic sequences over $\mathbb{F}_p$ of period v_1 and v_2 respectively. Let $f_1(x)$ and $f_2(x)$ be the minimal polynomials of $\underline{\mathbf{c}}_1$ and $\underline{\mathbf{c}}_2$ over $\mathbb{F}_p$ respectively. Let $f(x) = f_1(x)f_2(x)$. If $gcd(f_1(x), f_2(x)) = 1$, then*

1. *$f(x)$ is the minimal polynomial over $\mathbb{F}_p$ of $\underline{\mathbf{c}}$.*
2. *$per(\underline{\mathbf{c}}_i)|per(\underline{\mathbf{c}})$.*

   Moreover, if $f_i, i = 1, 2$ are irreducible, then
3. *$per(f_i) = per(\underline{\mathbf{c}}_i), i = 1, 2$.*
4. *$per(f) = lcm\{per(f_1), per(f_2)\}$.*
5. *$per(f) = per(\underline{\mathbf{c}})$.*

Fact 2 can be generalized to the case that $\underline{\mathbf{c}}$ is a sum of any $s \geq 1$ sequences over $\mathbb{F}_p$. (For a proof, see [18] [14].)

Fact 3 *Let $\underline{\mathbf{c}}$ be an non-sequence over $\mathbb{F}_p$ of period $t|p^n - 1$. Let $g(x) = g_1(x)\cdots g_s(x)$ be the minimal polynomial of $\underline{\mathbf{c}}$ over $\mathbb{F}_p$ where the g_j are irreducible over $\mathbb{F}_p$. Then $\underline{\mathbf{c}}$ can be decomposed into*

$$\underline{\mathbf{c}} = \underline{\mathbf{c}}_1 + \cdots + \underline{\mathbf{c}}_s$$

where $\underline{\mathbf{c}}_j \neq 0$ is periodic sequence over $\mathbb{F}_p$ and the minimal polynomial of $\underline{\mathbf{c}}_j$ is $g_j(x)$.

This result directly follows the trace representation in Section 1.5.

We are now ready to discuss a decomposition of (v, v) interleaved sequences. Note that here $v =$ prime or $v = p^n - 1$. If v is prime, from Fact 1, there exists some positive integer n such that $v|p^n - 1$. Let $f(x)$ be the minimal polynomial of $\underline{\mathbf{a}}$. If $f(x)$ is primitive, then $v = p^n - 1$, and the minimal polynomial of $\underline{\mathbf{u}}$ is equal to $f(x^v)$ which is still irreducible over $\mathbb{F}_p$ [28]. If $f(x) = f_1(x)\cdots f_s(x)$ where the $f_i(x)$'s are irreducible over $\mathbb{F}_p$. Let $n_i = deg(f_i)$, then $n_i|n$. From Fact 3, $\underline{\mathbf{a}}$ can be decomposed as

$$\underline{\mathbf{a}} = \underline{\mathbf{a}}_1 + \cdots + \underline{\mathbf{a}}_s$$

where f_i is the minimal polynomial of $\underline{\mathbf{a}}_i$. We write $A = (A_0, A_1, \cdots, A_{v-1})$ as the matrix form of $\underline{\mathbf{u}}$. By noticing that for each $i \geq 0$ the shift operator L^i is a linear transformation of the linear space consisting of all sequences over $\mathbb{F}_p$, we then have

$$A_j = L^{e_j}(\underline{\mathbf{a}}) = L^{e_j}(\sum_{k=1}^{s} \underline{\mathbf{a}}_k) = \sum_{k=1}^{s} L^{e_j}(\underline{\mathbf{a}}_k), 0 \leq j < v. \tag{34}$$

So $\underline{\mathbf{u}}$ can be decomposed as

$$\underline{\mathbf{u}} = \underline{\mathbf{u}}_1 + \cdots + \underline{\mathbf{u}}_s \tag{35}$$

where $\underline{\mathbf{u}}_i$ is a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}_i, \underline{\mathbf{e}})$. Thus we have proved that

Lemma 7. *Let $\underline{\mathbf{u}}$ be a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$. Let $f(x) = f_1(x) \cdots f_s(x)$ be the minimal polynomial of $\underline{\mathbf{a}}$ where f_i's are irreducible. Then*

1.
$$\underline{\mathbf{a}} = \underline{\mathbf{a}}_1 + \cdots + \underline{\mathbf{a}}_s$$
$$\underline{\mathbf{u}} = \underline{\mathbf{u}}_1 + \cdots + \underline{\mathbf{u}}_s$$
where the minimal polynomial of $\underline{\mathbf{a}}_i$ is $f_i(x)$ and $\underline{\mathbf{u}}_i$ is a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}_i, \underline{\mathbf{e}})$.
2. *If for some i the period of f_i is equal to v =prime or f_i is primitive for $v = p^n - 1$, then for such i the minimal polynomial of $\underline{\mathbf{u}}_i$ is $f_i(x^v)$ which is still irreducible.*
3. *The minimal polynomial of $\underline{\mathbf{u}}$ divides $f(x^v)$.*

From Lemma 7 and Fact 2-(1), the following result is immediate.

Lemma 8. *With the notation in Lemma 7. If for each $i : 1 \leq i \leq s$, f_i has the same period v, then the the minimal polynomial of $\underline{\mathbf{u}}_i$ is $f_i(x^v)$ which is irreducible over $\mathbb{F}_p$ and the minimal polynomial of $\underline{\mathbf{u}}$ is $f(x^v) = f_1(x^v) \cdots f_s(x^v)$.*

Lemma 9. *Let $\underline{\mathbf{u}}$ be a (v, v) interleaved sequence over $\mathbb{F}_p$ associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where v is prime (so that $p = 2$). Then all f_i have the same period v and the minimal polynomial of $\underline{\mathbf{u}}$ is $f(x^v)$.*

Proof. Since $\underline{\mathbf{a}}$ can be decomposed into $\underline{\mathbf{a}} = \underline{\mathbf{a}}_1 + \cdots + \underline{\mathbf{a}}_s$ where $\underline{\mathbf{a}}_i \neq 0$ has $f_i(x)$, an irreducible polynomial, as its minimal polynomial. From Fact 2-(2), we have $per(\underline{\mathbf{a}}_i) | per(\underline{\mathbf{a}})$. Since $per(\underline{\mathbf{a}}) = v$, a prime, then $per(\underline{\mathbf{a}}_i) = v$. Again using Fact 2-(3), we get $per(f_i) = v$ for each $i : 1 \leq i \leq s$ which establishes the first assertion. Therefore $\underline{\mathbf{u}}$ satisfies the condition of Lemma 8. Applying Lemma 8, we get that $f(x^v)$ is the minimal polynomial of $\underline{\mathbf{u}}$.

Let $h(x)$ and $h_i(x)$ be the minimal polynomial of $\underline{\mathbf{u}}_i$ respectively. From Lemma 8, if for each $i : 1 \leq i \leq s$, $per(f_i) = v$, then h_i's are pairwise relatively prime and $h(x) = \prod_{i=1}^{s} h_i(x)$. In the following, we will prove this result for $\underline{\mathbf{u}}$ without the imposed condition for $f_i(x)$. I.e., we want to establish the following assertion.

Theorem 4. *Let $\underline{\mathbf{u}}$ be a (v, v) interleaved sequence over $\mathbb{F}_p$ associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where v is prime or $v = p^n - 1$. Let $f(x) = f_1(x) \cdots f_s(x)$ be the minimal polynomial of $\underline{\mathbf{a}}$ where f_i is irreducible and let $\underline{\mathbf{a}}$ have a decomposition: $\underline{\mathbf{a}} = \underline{\mathbf{a}}_1 + \cdots + \underline{\mathbf{a}}_s$ where f_i is the minimal polynomial of $\underline{\mathbf{a}}_i$. Let $\underline{\mathbf{u}}$ have the following corresponding decomposition*

$$\underline{\mathbf{u}} = \underline{\mathbf{u}}_1 + \cdots + \underline{\mathbf{u}}_s$$

where $\underline{\mathbf{u}}_i$ is a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}_i, \underline{\mathbf{e}})$. Let $h(x)$ and $h_i(x)$ be the minimal polynomials of $\underline{\mathbf{u}}$ and $\underline{\mathbf{u}}_i$ respectively. Then $h_i(x), 1 \leq i \leq s$, are pairwise relatively prime and

$$h(x) = \prod_{i=1}^{s} h_i(x).$$

From Lemma 8, it suffices to consider the case that there is some i such that $per(f_i) < v$ (note that $per(f_i)|v$). We need several lemmas for this purpose. Hence after, we write $q = p^n$ sometimes.

Let $n_i = deg(f_i)$ and γ_i be a root of $f_i(x)$. Then $\gamma_i \in F_{p^n}$. So that $n_i|n$ [28]. Let $\underline{\mathbf{a}}_i = \{a_{i,t}\}$ have the following trace representation (see Section 1)

$$a_{i,t} = Tr_1^{n_i}(\eta_i \gamma_i^t), 0 \neq \eta_i \in \mathbb{F}_{p^{n_i}}, t = 0, 1, \cdots. \tag{36}$$

From Lemma 7, the elements of $\underline{\mathbf{u}}_i = \{u_{i,t}\}$ can be represented as

$$u_{i,kv+j} = Tr_1^{n_i}(\eta_i \gamma_i^{k+e_j}), 0 \leq j < v, k \geq 0. \tag{37}$$

(See [13] for detail.) Let

$$\rho_{i,kv+j} = \eta_i \gamma_i^{k+e_j}, 0 \leq j < v, k \geq 0, \tag{38}$$

and $\Pi_i = \{\rho_{i,t}\}_{t \geq 0}$, $1 \leq i \leq s$. Then we have

$$u_{i,t} = Tr_1^{n_i}(\rho_{i,t}), t = 0, 1, \cdots. \tag{39}$$

Let $g_i(x)$ be the minimal polynomial Π_i over $\mathbb{F}_q$. Before we give the relation between $h_i(x)$ and $g_i(x)$, we introduce the following notation. Let

$$\varphi(x) = t_m x^m + t_{m-1} x^{m-1} + \cdots + t_0 \in \mathbb{F}_{p^n}[x].$$

Define

$$\sigma_i(\varphi(x)) = t_m^{p^i} x^m + t_{m-1}^{p^i} x^{m-1} + \cdots + t_0^{p^i}, 0 \leq i < n.$$

($\sigma_i(\varphi(x))$ is said to be the *conjugates* of $\varphi(x)$ with respect to p.) We have the following result whose proof can be found in [21].

Proposition 6. *With the above notation. Then*

$$h_i(x) = \prod_{j=0}^{n_i-1} \sigma_j(g_i(x)), 1 \leq i \leq s.$$

Property 3. Let $\varphi_i(x) = x^v - \gamma_i$. Then

$$gcd(\varphi_i(x), \sigma^k(\varphi_j(x))) = 1 \text{ for } i \neq j, k = 0, 1, \cdots, n-1.$$

Proof. If $gcd(\varphi_{\gamma_i}(x), \sigma_k(\varphi_{\gamma_j}(x)) = d(x)$ with $deg(d(x)) \geq 1$. Let β be a root of $d(x)$ in the extension field. Then we get

$$\beta^v = \gamma_i \text{ and } \beta^v = \gamma_j^{p^k}.$$

Thus $\gamma_i = \gamma_j^{p^k}$. Therefore γ_i and γ_j are roots of the same irreducible polynomial over $\mathbb{F}_p$ which is a contradiction. So the result is true.

Lemma 10. *With the above notation.*

$$gcd(h_i(x), h_j(x)) = 1, \text{ for } i \neq j.$$

Proof. Note that $\varphi_i(x)$ is a characteristic polynomial of Π_i over $\mathbb{F}_q$. Thus $g_i(x)|\varphi_i(x)$. Notice that σ^k restricted on $\mathbb{F}_q$ is an automorphism of $\mathbb{F}_q$. Applying Property 3, $gcd(g_i, \sigma^k(g_j)) = 1$ for $i \neq j$ and $k = 0, 1, \cdots, n-1$. From Proposition 6, $h_i(x)$ is the product of $\sigma^k(g_i)$, $k = 0, 1, \cdots, n_i - 1$. Consequently, $gcd(h_i(x), h_j(x)) = 1$ for $i \neq j$.

Proof of Theorem 4 . The assertion follows immediately from Lemma 10 and Fact 2-(1).

Corollary 3. *With the same* $\underline{\mathbf{a}}_i, \underline{\mathbf{u}}_i, f_i, h_i, h$ *and* g_i *above. Let* $LS(\underline{\mathbf{u}})$ *represent the linear span of* $\underline{\mathbf{u}}$. *Then*

$$LS(\underline{\mathbf{u}}) = \sum_{i=1}^{s} deg(f_i) deg(g_i)$$

Proof. Since $LS(\underline{\mathbf{u}}) = deg(h)$, the result follows from Theorem 4.

Lemma 11. *Let* $\underline{\mathbf{u}}$ *be a* (v, v) *interleaved sequence associated with* $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ *where* $v = p^n - 1, n > 1$ *and* $\underline{\mathbf{e}} \in \mathbb{Z}_v^v$. *Let* $h(x)$ *and* $f(x)$ *be the minimal polynomials of* $\underline{\mathbf{u}}$ *and* $\underline{\mathbf{a}}$ *respectively. If* $f(x)$ *is irreducible, then the period of each irreducible factor of* $h(x)$ *is not a divisor of* v.

Proof. Let $A = (A_0, A_1, \cdots, A_{v-1})$ be the matrix form of $\underline{\mathbf{u}}$. By the definition of the interleaved sequences, we have

$$A_j = L^{e_j}(\underline{\mathbf{a}}) \neq 0, 0 \leq j < v, e_j \in \mathbb{Z}_v. \tag{40}$$

So the minimal polynomial of each column sequence of $\underline{\mathbf{u}}$ is $f(x)$ which is irreducible. On the other hand, if there is one irreducible factor of $h(x)$ whose period divides v, then we can suppose that $h(x) = d(x)H(x)$ where $d(x)$ is irreducible and $per(d)|v$. Therefore $\underline{\mathbf{u}}$ can be decomposed as

$$\underline{\mathbf{u}} = \underline{\mathbf{c}} + \underline{\mathbf{w}} \tag{41}$$

where the minimal polynomials of $\underline{\mathbf{c}}$ and $\underline{\mathbf{w}}$ are $d(x)$ and $H(x)$ respectively. From Fact 2-(3), the period of $\underline{\mathbf{c}}$ is equal to the period of $d(x)$ which is a factor of v. Thus the jth column sequence A_j of $\underline{\mathbf{u}}$ can be written as $A_j = c_j + \underline{\mathbf{w}}_j$ where $0 \neq \underline{\mathbf{c}} = \{c_j\}$ which contradicts with (40). Therefore none of irreducible factors of $h(x)$ whose period is a divisor of v.

Theorem 5. *Let $\underline{\mathbf{u}}$ be a (v, v) interleaved sequence over $\mathbb{F}_p$ associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where v is prime or $v = p^n - 1$ and $\underline{\mathbf{e}} \in \mathbb{Z}_v^v$, $\underline{\mathbf{b}}$ a sequence over $\mathbb{F}_p$ of period v and $\underline{\mathbf{c}} = \underline{\mathbf{u}} + \underline{\mathbf{b}}$. Let $h(x)$, $t(x)$ and $g(x)$ be the minimal polynomials of $\underline{\mathbf{u}}$, $\underline{\mathbf{b}}$ and $\underline{\mathbf{c}}$ respectively. If each irreducible factor of the minimal polynomial of $\underline{\mathbf{a}}$ has degree greater than 1. Then*

1. *$gcd(h(x), t(x)) = 1$.*
2. *$g(x) = h(x)t(x)$.*
3. *The linear span of $\underline{\mathbf{c}}$ is given by $LS(\underline{\mathbf{c}}) = LS(\underline{\mathbf{u}}) + LS(\underline{\mathbf{b}})$.*

Proof. With the same $\underline{\mathbf{u}}_i$, $h_i(x)$ as Theorem 4. According to Theorem 4, $h_i(x)$'s, the minimal polynomials of $\underline{\mathbf{u}}_i$, are pairwise relatively prime and $h(x) = h_1(x) \cdots h_s(x)$. So it suffices to show that $gcd(h_i(x), t(x)) = 1$ for each i.

Case 1. v is prime.

According to Lemma 9, $h_i(x) = f_i(x^v)$ which is irreducible and $h(x) = f(x^v) = f_1(x^v) \cdots f_s(x^v)$ with $deg(f_i) > 1$. Thus each irreducible factor of $f(x^v)$ has degree greater than v. Let $t(x)$ be the minimal polynomial of $\underline{\mathbf{b}}$. Since $\underline{\mathbf{b}}$ has period v, then $deg(t(x)) \leq v$. Therefore any irreducible factor of $t(x)$ has degree less than or equal to v. So $gcd(f(x^v), t(x)) = 1$ which gives the first assertion. From Fact 2-(1), $g(x) = h(x)t(x)$. Therefore $LS(\underline{\mathbf{u}} + \underline{\mathbf{b}}) = deg(f(x^v)t(x)) = deg(f(x^v)) + deg(t(x)) = vdeg(f(x)) + deg(t(x) = vLS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}})$.

Case 2. $v = p^n - 1$.

If $f_i(x)$ is primitive, from Lemma 7-(2), $h_i(x) = f_i(x^v)$ which is irreducible. By using the similar argument used in Case 1, we get that $h_i(x)$ is coprime with $t(x)$. So, we only need to consider the case that f_i is irreducible but not primitive. From Lemma 7-(1), $\underline{\mathbf{u}}_i$ is a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}_i, \underline{\mathbf{e}})$ where the minimal polynomial of $\underline{\mathbf{a}}_i$ is irreducible. Applying Lemma 11, any irreducible factor of $h_i(x)$ has period which is not a factor of v. But $\underline{\mathbf{b}}$ is a sequence over $\mathbb{F}_p$ with period $p^n - 1$. Therefore any irreducible factor of $t(x)$ has period which divides v. Hence

$$gcd(h_i(x), t(x)) = 1, 1 \leq i \leq s.$$

Therefore $gcd(h(x), t(x)) = 1$. From Fact 2-(1), the minimal polynomial of $\underline{\mathbf{c}}$ is $h(x)t(x)$. The last assertion follows immediately from the definition of the linear span.

5.2 A Lower Bound for the Linear Span of $\underline{\mathbf{u}}$

According to Corollary 3, the computation of linear span of a (v, v) interleaved sequence where its base sequence has reducible minimal polynomial can be reduced to computation of linear span of a (v, v) interleaved sequence where its base sequence has an irreducible minimal polynomial. The later is called an *irreducible interleaved sequence* in [13] by the author. In [13], the author studied some properties on linear span of (s, t) irreducible interleaved sequences for special choices of s and t. In general, this problem is difficult. However, here we will utilize a structure of the shift sequence to establish a lower bound for linear span of (v, v) irreducible interleaved sequences when the shift sequences are obtained by Construction A in Section 4.

Now we suppose that $v = p^n - 1$ and $\underline{\mathbf{u}}$ is a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where the minimal polynomial $f(x)$ of $\underline{\mathbf{a}}$ is irreducible and $\underline{\mathbf{e}}$ is obtained from Construction A. From the discussion in Section 5.1, for $f(x)$ an irreducible polynomial over $\mathbb{F}_p$ of degree n and γ a root of $f(x)$ in $\mathbb{F}_q$, we then have

$$u_i = Tr_1^n(\rho_i), i = 0, 1, \cdots \tag{42}$$

where

$$\rho_{kv+j} = \zeta\gamma^{e_j}\gamma^k, 0 \leq j < v, k \geq 0, \zeta \in \mathbb{F}_q \tag{43}$$

and $\Pi = \{\rho_i\}$, a sequence over $\mathbb{F}_q$.

Let $g(x)$ be the minimal polynomial of Π over $\mathbb{F}_q$. Note $LS(\underline{\mathbf{a}}) = deg(f) = n$. From Corollary 3, we have

$$LS(\underline{\mathbf{u}}) = LS(\underline{\mathbf{a}})LS(\Pi) = nLS(\Pi). \tag{44}$$

Therefore, in order to establish a lower bound for the linear span of the irreducible interleaved sequence $\underline{\mathbf{u}}$, it suffices to find a lower bound for the linear span of the sequence Π over $\mathbb{F}_q$, defined by (43). In the following, we will assume that the shift sequence $\underline{\mathbf{e}}$ of $\underline{\mathbf{u}}$ is given by Construction A. Under this assumption, we have the following relation

$$\beta^{e_j} = Tr_n^{2n}(\eta\alpha^{j+1}), 0 \leq j < v, Tr_n^{2n}(\eta) = 0, \eta \in F_{q^2} \tag{45}$$

where α and β are primitive elements of $\mathbb{F}_{q^2}$ and $\mathbb{F}_q$ respectively and $Tr_n^{2n}(x)$ is the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. Note that $\gamma \in \mathbb{F}_q$. Thus exists some positive integer r such that

$$\gamma = \beta^r. \tag{46}$$

Substituting (46) into (43), we get

$$\rho_{kv+j} = \zeta\beta^{e_j}\gamma^k, 0 \leq j < v, k \geq 0, \tag{47}$$

Let

$$\theta_j = Tr_n^{2n}(\eta\alpha^{j+1}), j = 0, 1, \cdots \tag{48}$$

where η is the same as in (45). Let $\Theta = \{\theta_j\}$. Then Θ is an m-sequence over $\mathbb{F}_q$ of degree 2. Together with (45), (46) and (47), we have

$$\rho_{kv+j} = \zeta\theta_j^r\gamma^k, 0 \leq j < v, k \geq 0. \tag{49}$$

If $gcd(r,v)=1$, then $f(x)$ is primitive. Thus $h(x)=f(x^v)$. Therefore $LS(\underline{\mathbf{u}})=vn$. So we only need to consider the case $gcd(r,v)>1$. We will establish a lower bound of the linear span of Π in terms of an upper bound of the linear span of the power function sequence $\Theta^r=\{\theta_j^r\}_{j\geq 0}$ of the m-sequence Θ of degree 2. Fortunately, the linear spans of function sequences of linear feedback shift sequences have already been discussed by Herlestam in the middle of 80's [18]. From his work, we have the following result.

Proposition 7. *With the above notation. Let $r=r_0+r_1p+\cdots+r_{n-1}p^{n-1}, 0\leq r_i<p$. Then $LS(\Theta^r)$, the linear span of Θ^r, is given by*

$$LS(\Theta^r)=\prod_{i=0}^{n-1}(r_i+1)$$

Lemma 12. *With the same Θ as above. Let $0<r<p^n-1$ with $gcd(r,p^n-1)>1$. Then $LS(\Theta^r)$, the linear span of Θ^r, is bounded by*

$$LS(\Theta^r)<\frac{p^n-1}{2}.$$

Proof. Note that

$$p^n-1=2\cdot\frac{p-1}{2}(p^{n-1}+\cdots+p+1).$$

Since $r<p^n-1$ and $gcd(r,p^n-1)>1$, then

$$r\leq\frac{p^n-1}{2}. \tag{50}$$

We write $r=r_0+r_1p+\cdots+r_{n-1}p^{n-1}, 0\leq r_i<p$. If we take $r_{n-1}=p-1$, then $r>r_{n-1}p^{n-1}=(p-1)p^{n-1}>\frac{p^n-1}{2}$ which is a contradiction with (50). So, $r_{n-1}<p-1$. Applying Proposition 7, the maximal value of $LS(\Theta^r)$ can only be achieved for such r's where $r_i=p-1$, $i=0,1,\cdots,p-2$ and $r_{n-1}<p-1$. I.e., we have

$$LS(\Theta^r)=p^{n-1}(r_{n-1}+1) \tag{51}$$

for $r_i=p-1, i=0,1,\cdots,n-2$. If $r_{n-1}\geq\frac{p-1}{2}$, then

$$\begin{aligned}r&=(p-1)(p^{n-2}+\cdots+p+1)+r_{n-1}p^{n-1}\\&\geq(p-1)(p^{n-2}+\cdots+p+1)+\frac{p-1}{2}p^{n-1}\\&=p^{n-1}\frac{p+1}{2}>\frac{p^n-1}{2}.\end{aligned}$$

which is a contradiction with (50). Therefore $r_{n-1}\leq\frac{p-1}{2}-1$. Substituting it into (51), we get

$$LS(\Theta^r)\leq p^{n-1}\frac{p-1}{2}<\frac{p^n-1}{2}$$

which establishes the assertion.

We list the following properties on linear span profiles whose proof can be found in [30].

Proposition 8. *Let $\underline{\mathbf{c}} = \{c_i\}$ be a periodic sequence over $\mathbb{F}_q$, and let $d(x)$ be its minimal polynomial over $\mathbb{F}_q$ with $l = deg(d)$. Let $d_i(x)$ be a polynomial computed by applying the Berlekamp-Massey algorithm which generates $c_0, c_1, \cdots, c_i$ for $i \geq 0$ where $l_i = deg(d_i)$. Then*

1. *$d_i = d(x)$ and $l_i = l$ for all $i \geq 2l$.*
2. *$l_0 \leq l_1 \leq l_2 \cdots \leq l_i \leq \cdots$.*

In the following, we will use the Berlekamp-Massey algorithm (see [30] or [14] (Chapter 6)) to establish a lower bound of the linear span of Π.

Lemma 13. *With $q = p^n$. Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_p$ of degree n and let γ be a root of $f(x)$ in the extension $\mathbb{F}_q$. Let $\Theta = \{\theta_i\}$ be an m-sequence over $\mathbb{F}_q$ of degree 2. Let r be a positive integer with $gcd(r, q-1) > 1$. Let $\Pi = \{\rho_i\}$ be a sequence over $\mathbb{F}_q$ whose elements are given by*

$$\rho_{kv+j} = \theta_j^r \gamma^k, v = q-1, i = kv + j \text{ where } 0 \leq j < v, k \geq 0, 0 \neq \zeta \in \mathbb{F}_q.$$

Then $LS(\Pi)$, the linear span of Π, is bounded by

$$LS(\Pi) \geq \frac{p^n - 1}{2}.$$

Proof. From the assumption, we have

$$\rho_j = \theta_j^r, j = 0, 1, \cdots, v-1 = p^n - 2. \tag{52}$$

Let $d(x)$ be the minimal polynomial of $\Theta^r = \theta_0^r, \theta_1^r, \cdots$ and let $l = deg(d(x))$. Assume that $d_i(x)$ is the polynomial computed by the Berlekamp-Massey algorithm which generates the sequence $\rho_0, \rho_1, \cdots, \rho_i$ and $l_i = deg(d_i), i \geq 0$. From (52), we get that d_i is the same polynomial computed by the Berlekamp-Massey algorithm, which generates the sequence $\theta_0^r, \theta_1^r, \cdots, \theta_i^r$ for $i = 0, 1, \cdots, p^n - 2$. Note that from Lemma 12, we have $l = LS(\Theta^r) < \frac{p^n-1}{2}$. So $2l < p^n - 1$. Applying Proposition 8-(1),

$$d_i(x) = d(x) \text{ and } l_i = l \text{ for all } i : 2l \leq i \leq v - 1 = p^n - 2$$

Note that from (48) $\theta_{v+1} = 0 \Longrightarrow \theta_{v+1}^v = 0$. But from (47) $\rho_{v+1} = \zeta\theta_1\gamma \neq 0$. So $d_{v-1}(x) = d(x)$ can not generate $\rho_0, \rho_1, \cdots, \rho_{v+1}$. There are two cases that may happen.

1. $d(x)$ can generate $\rho_0, \rho_1, \cdots, \rho_v$ but not $\rho_0, \rho_1, \cdots, \rho_{v+1}$.
2. $d(x)$ can not generate $\rho_0, \rho_1, \cdots, \rho_v$.

From Lemma 12, we have

$$2l_j = 2l < p^n - 1 = v \tag{53}$$

where $j = v - 1$ if the case 1 happens and $j = v$ if the case 2 happens. According to the Berlekamp-Massey algorithm, $d_{j+1}(x)$ is given by

$$d_{j+1}(x) = x^{b-a}d(x) - d_m(x)$$

where $0 \leq m < v$, $l_m < l$, $b = j + 1 - l$ and $a < l$. Whenever $j = v - 1$ or $j = v$, we have $l_{j+1} = deg(d_{j+1}) = b - a + l = j + 1 - l - a + l = j + 1 - a > j + 1 - l > v - \frac{p^n-1}{2} = \frac{p^n-1}{2}$. Therefore $LS(\rho) \geq l_{j+1} > \frac{p^n-1}{2}$ which completes the proof.

Lemma 14. *Let $f(x) = f_1(x) \cdots f_s(x)$ where the f_i are irreducible over $\mathbb{F}_p$. Let $\underline{\mathbf{a}} = \underline{\mathbf{a}}_1 + \cdots + \underline{\mathbf{a}}_s$ be a 2-level auto correlation sequence over $\mathbb{F}_p$ of period v where the minimal polynomial of $\underline{\mathbf{a}}_i$ is $f_i(x)$. Let $\underline{\mathbf{u}}$ be a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where the shift sequence $\underline{\mathbf{e}}$ is constructed by Construction A. Let $\underline{\mathbf{u}} = \underline{\mathbf{u}}_1 + \cdots + \underline{\mathbf{u}}_s$ be the corresponding decomposition where $\underline{\mathbf{u}}_i$ is a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}_i, \underline{\mathbf{e}})$. Then*

$$LS(\underline{\mathbf{u}}_i) > deg(f_i)\frac{p^n - 1}{2} \text{ and}$$
$$LS(\underline{\mathbf{u}}) > \frac{p^n - 1}{2}LS(\underline{\mathbf{a}}).$$

Proof. With the same notation in Section 5.1. Since $\underline{\mathbf{a}}$ is a 2-level auto correlation sequence, thus $\eta_i = 1, 1 \leq i \leq s$ in (36), the trace representation of $\underline{\mathbf{a}}$. Consequenctly for each $i : 1 \leq i \leq s$, the elements of Π_i has a representation of (49) where $\zeta = 1$ and γ is replaced by γ_i which is a root of f_i. Thus Π_i satisfies the condition of Lemma 13. Therefore we have

$$deg(g_i) = LS(\Pi_i) > \frac{p^n - 1}{2}, 1 \leq i \leq s. \tag{54}$$

Applying Proposition 6, we get

$$LS(\underline{\mathbf{u}}_i) = deg(h_i(x)) = deg(f_i)deg(g_i) \overset{(54)}{>} deg(f_i)\frac{p^n - 1}{2}$$

which establishes the first assertion. Applying Corollary 3 and the above the first assertion , we have

$$LS(\underline{\mathbf{u}}) = \sum_{i=1}^{s} LS(\underline{\mathbf{u}}_i) > \sum_{i=1}^{s} deg(f_i)\frac{p^n - 1}{2} = \frac{p^n - 1}{2}\sum_{i=1}^{s} deg(f_i) = \frac{p^n - 1}{2}LS(\underline{\mathbf{a}})$$

where the last identity comes from $\sum_{i=1}^{s} deg(f_i) = deg(f) = LS(\underline{\mathbf{a}})$.

Corollary 4. *Let $v = p^n - 1$. Let $\underline{\mathbf{u}}$ be a (v, v) interleaved sequence associated with $(\underline{\mathbf{a}}, \underline{\mathbf{e}})$ where $\underline{\mathbf{a}}$ is a sequence over $\mathbb{F}_p$ of period v and $\underline{\mathbf{e}}$ is given by Construction A. Let $\underline{\mathbf{b}}$ be a sequence over $\mathbb{F}_p$ of period v. Let $\underline{\mathbf{c}} = \underline{\mathbf{u}} + \underline{\mathbf{b}}$. Then $LS(\underline{\mathbf{c}})$, the linear span of $\underline{\mathbf{c}}$, is bounded by*

$$LS(\underline{\mathbf{c}}) > \frac{p^n - 1}{2}LS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}}).$$

Proof. This follows directly from Theorem 5 and Lemma 14.

In the next subsection, we will use Corollary 4 to establish the result 1 in Theorem 3, and Lemmas 8 and 9 together with Theorem 5 to derive the results 2 and 3 in Theorem 3.

5.3 Proof of Theorem 3

For any $\underline{\mathbf{s}}_k \in S$, we have

$$\underline{\mathbf{s}}_k = \underline{\mathbf{u}} + L^k(\underline{\mathbf{b}}).$$

1. Since all shifts of $\underline{\mathbf{b}}$ have the minimal polynomial, then the result directly follows from Corollary 4.
2. If $per(f_i) = v$, according to Lemma 8, the minimal polynomial of $\underline{\mathbf{u}}$ is $f(x^v)$. Applying Theorem 5, the minimal polynomial of $\underline{\mathbf{s}}_k$ is equal to $f(x^v)t(x)$ where $t(x)$ is the minimal polynomial of $\underline{\mathbf{b}}$. Thus the result follows.
3. The first assertion follows from Lemma 9 and Theorem 5 immediately.

   For the second assertion, if $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are both quadratic sequences, according to [15], we have

   $$LS(\underline{\mathbf{a}}) = LS(\underline{\mathbf{b}}) = \frac{v-1}{2}.$$

   Applying Theorem 5,

   $$LS(s_k) = vLS(\underline{\mathbf{a}}) + \underline{\mathbf{b}} = v\frac{v-1}{2} + \frac{v-1}{2} = \frac{(v+1)(v-1)}{2} = \frac{v^2-1}{2}.$$

   Note that the result on linear spans of 2-level auto-correlation sequences of period $2^n - 1$ which were developed by the author and Golomb in [15] can be easily generalized to the sequences with period v where v is a prime. Thus a quadratic residue sequence of period v achieves maximal linear span among the sequences of period v with the 2-level auto-correlation function. Therefore if v is prime, then each sequence in a $(v^2, v, 2v+3)$ signal set achieves the maximal linear span.

6 An Architecture for Implementation and Comparisons with the Known Designs

In this section, first we provide an architecture for implementing the new designs. Then we discuss the new design in comparison with the known designs for signal sets with low cross correlation. Last, we illustrate a complete process for designing a signal set by using the new design.

6.1 Implementation

Construction A, which generates $((p^n-1)^2, p^n-1, 1+2p^n)$ signal sets, can be implemented by an linear feedback shift register (LFSR) over $\mathbb{F}_{p^n}$ of order 2 and two 2-level auto correlation sequence generators together with a *shrinking counter which cuts off two consecutive outputs of the LFSR at each v interval clock cycles*. See Figure 1.

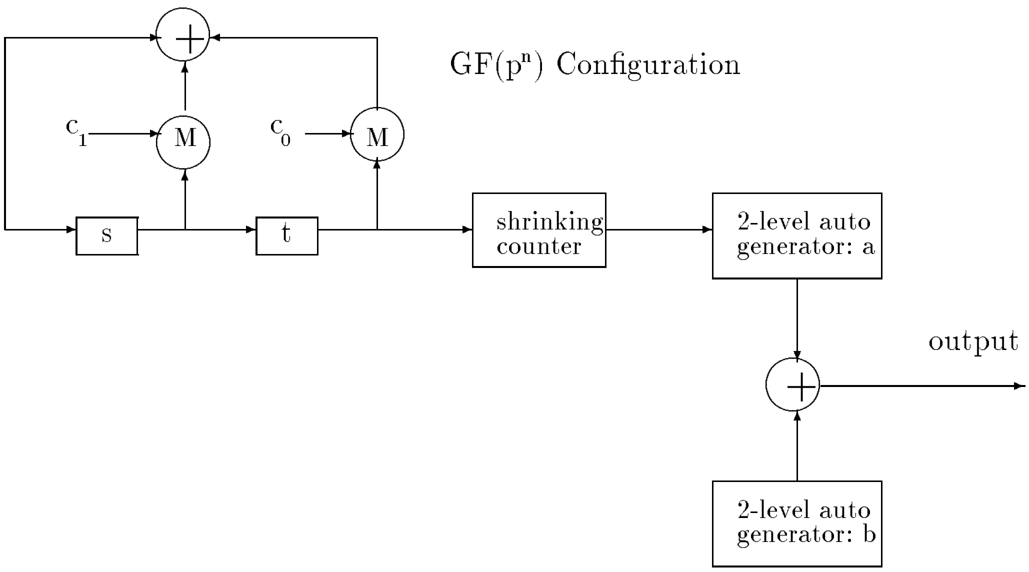

Figure 1. Galois Configuration of $((p^n-1)^2, p^n, 1+2p^n)$ Signal Sets

In figure 1, M represents the multiplication of $\mathbb{F}_{p^n}$ and $(s,t) \in \mathbb{F}_{p^n}^2$ a specific initial state of LFSR 1. Thus the complexity of implementation of a $((p^n-1)^2, p^n-1, 1+2p^n)$ signal set only depends on the complexity of these two 2-level auto correlation sequence generators. If we take two base sequences $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ from the set consisting of 2-level auto correlation sequences from Constructions A, B and D in Section 2.1, then we have an efficient implementation for such signal sets in both hardware and software.

For Construction B, which generates $(v^2, v, 2v+3)$ signal sets where v is prime, it can be implemented by means of pre-storage of the shift sequence $\underline{\mathbf{e}}$ and the 2-level auto correlation sequence $\underline{\mathbf{a}}$ (here we choose $\underline{\mathbf{b}} = \underline{\mathbf{a}}$) for small v (for example, $v < 2^{30}$). It also can be implemented by employing a division circuit, see [13].

6.2 Comparisons

In the following tables, we give profiles for the new designs in comparison with the known designs in the Galois field configuration.

We then have the following advantages for the new design.

Case 1: Binary Signal Sets with Period $(2^n-1)^2$

Table 1. Comparison with the Known Designs: Binary Case

Constr.	(v,r,δ) Signal Set	Linear Span	Range of Imbalance
Gold Gen. cases	$(2^{2n+1}-1, 1+2^{2n+1}, 1+\sqrt{2}2^n)$ n odd	$4n+2$	$[1, 1+2^{n+1}]$
Kasami	$(2^{2n}-1, 2^n, 1+2^n)$	$3n$	$[1, 1+2^n]$
Gen. Kasami (No *et al.*)	$(2^{2n}-1, 2^n, 1+2^n)$	$\geq n^2$ $\leq n(2^n-1)$	$[1, 1+2^n]$
Bent	$(2^{2n}-1, 2^n, 1+2^n)$	$\geq \binom{n}{n/2} 2^{n/2}$	1 (n even)
New Design	$((2^n-1)^2, 2^n, 1+2^{n+1})$	$\geq \frac{2^n-1}{2}n$ $\leq 2^{2n-1}$	1
(Interleave)	$(v^2, v+1, 2v+3)$	$(v^2-1)/2$	1

Table 2. Comparison with the Known Designs: Non-binary Case

Construction	(N,r,δ) Signal Set	Linear Span	Balance ?
Gold Pair	$(p^{2n+1}-1, 1+p^{2n+1}, 1+pp^n)$ (Trachtenberg [41]) $(p^{2n}-1, p^{2n}, 2p^n-1)$ (Helleseth [19]) $(p^n-1, p^n, 1+\sqrt{p^n})$ (Sidelnikov [38], Kumar, *et al.* [26])	$4n+2$ $4n$ $2n$	No No No
Bent [27] (Kumar. *et al.*)	$(p^{2n}-1, p^n, 1+p^n)$	Unclear	Unclear
New Design (interleave)	$((p^n-1)^2, p^n-1, 1+2p^n)$	$\geq \frac{p^n-1}{2}n$ $\leq p^{2n-1}(p-1)$	Yes

For the binary case, among the previous known constructions, only the generalized Kasami designs can utilize all 2-level sequences of period 2^n-1 (see Section 2.2). According to the Welch bound [42], the correlation of signal sets constructed from both the generalized Kasami design and the new design are optimal. However, from Table 1, the new design has the following better aspects in comparison with the generalized Kasami design.

1. *Linear Span*

   For the new design, the 2-level auto correlation sequence $\underline{\mathbf{a}}$ having linear span n can be only happened when $\underline{\mathbf{a}}$ is chosen as an m-sequence. For other cases, the linear span of $\underline{\mathbf{a}}$ is greater than n. So the linear span of $\underline{\mathbf{a}}$ is at least n. Therefore the lower bound of the linear span of any sequences in a $((2^n-1)^2, 2^n-1, 1+2^{n+1})$ signal set constructed from Procedure 1 is $n2^n$. On the other hand, the upper bound of a sequence in $(2^{2n}-1, 2^n, 1+2^n)$ signal sets from generalized Kasami designs is $n(2^n-1)$ which is less than the lower bound of the linear span of the sequences in the new signal sets.

2. *The Number of Different Signal Sets*

   Let N_g be the number of different 2-level auto correlation functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. According to Proposition 2 in Section 1, the number of different $(2^{2n}-1, 2^n, 1+2^n)$ signal sets, constructed from the generalized Kasami design, is equal to $N_g\frac{\phi(2^{2n}-1)}{2n}$ where $\frac{\phi(2^{2n}-1)}{2n}$ is the number of m-sequences over $\mathbb{F}_2$

of degree $2n$ and $\phi(x)$ is the Euler function. In the new design, the 2-level auto correlation sequences $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ can be selected independently. On the other hand, the shift sequence of a new set can be constructed from Construction A if $2^n - 1$ is not a prime and from Construnction A or B if $2^n - 1$ is prime. Therefore the number of different $((2^n-1)^2, 2^n-1, 1+2^{n+1})$ signal set is $N(\underline{\mathbf{e}}_B)N_g^2\frac{\phi(2^{2n}-1)}{2n}$ where $N(\underline{\mathbf{e}}_B) = 1$ if 2^n-1 is not a prime and $N(\underline{\mathbf{e}}_B) = \phi(2^n-2)$ if 2^n-1 is prime. Thus the number of different $((2^n-1)^2, 2^n-1, 1+2^{n+1})$ signal set is $N(\underline{\mathbf{e}}_B)N_q$ times as many as the number of $(2^{2n}-1, 2^n, 1+2^n)$ signal set from the generalized Kasami design.

3. *The Balance Property*

   Each sequence in a $(2^{2n}-1, 2^n, 1+2^n)$ signal set of the egeneralized Kasami design is unbalanced. But each sequence in a $((2^n-1)^2, 2^n-1, 1+2^{n+1})$ signal set of the new design is balanced.

In the following, we will give an example for $p=2$ and $n=5$ to explain these discusssions.

Example 7. Let $v = 2^5 - 1 = 31$.

Table 3. $n = 5$

Constructions	(v, r, δ) Signal Set	Linear Span	Number of Balanced Seq.	Total Number of Such Sets
Kasami	$(1023, 32, 33)$	15	0	1×60
Gen. Kasami (No *et al.*)	$(1023, 32, 33)$	$\geq 25, \leq 155$	0	8×60
New Design (Interleave)	$(961, 31, 65)$	160 or 480	31	$64 \times 8 \times 60$ $= 512 \times 60$

Since $2^5 - 1 = 31$ is a prime, then we have two constructions to construct shift sequence in a $(961, 31, 65)$ signal set. Thus the number of different binary signal sets with the parameter $(961, 31, 65)$ is $64 \times 8 \times 60$ where the numbers 60 and 8 come from the number of shift distint shift sequences by Construnctions A and B respectively. Note that 60 is the number of different primitive polynomials over $\mathbb{F}_2$ of degree 10.

Case 2. Binary Signal Sets with Period v^2 where $v = prime$

The new design for $(v^2, v, 2v+3)$ signal sets where $p = 2$ and v is prime are complete new sets. In this case, the shift sequences are obtained from Construction B, and two base sequences can be choosen from the set consisting of the quadratic sequences and the Hall sixtic sequences. (Note that when v is prime, according to Section 2.1-C, there are only 3 constructions to construct a binary sequence with 2-level auto correlation. Here we can utilize two of them.)

In the following example, we list a profile of $(v^2, v, 2v+3)$ signal sets for primes less than 100 which are completely new.

Table 4. Signal Sets with the Balance Property
($\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are quadratic residue sequences)

v	$(v^2, v, 2v+3)$ Signal Set	Linear Span
7	(49, 7, 17)	24
11	(121, 11, 25)	60
19	(361, 19, 41)	180
23	(529, 23, 49)	264
31	(961, 31, 65)	480
47	(2209, 47, 97)	1104
59	(3481, 59, 121)	1740
67	(4489, 67, 137)	2244
71	(5041, 71, 145)	2520
79	(6241, 79, 161)	3120
83	(6889, 83, 169)	3444

Case 3. Non-binary Signal Sets

For nonbinary case, the new design provises a variety of $((p^n-1)^2, p^n-1, 1+2p^n)$ signal sets whose cross correlation are optimal with respect to the Welch bound. Note that for the Gold-pair construction, there are only few choices for r in $g(x) = Tr_1^n(x^r)$ defined by Construction A. 1 in Section 2.2. Also all signal sets obtained from the Gold-pair construction are unbalanced and have low linear span as well. (Here we mean that a signal set is *balanced* if each sequence in the set is balanced. Otherwise, it is said to be *unbalanced*.) Thus the new design gives the first type of nonbinary signal sets with optimal correlation, the balance property and large linear span whose value is exponentially increased in n.

The following table lists a profile of the new design for $p=3$ and $n=4$ in comparison with the signal sets with the closest length.

Table 5. Signal Sets for $p=3$ and $n=4$

Construction	(v, r, δ) Signal Set	Linear Span	Number of Balanced Seq.	Total Number of Signal Sets
Helleseth	(6560, 6562, 161)	16	3239	1×320
Kumar *et al.*	(6560, 6561, 82)	16	81	7×320
New Sets	(6400, 80, 163)	$\{164, 172, 484, 492\}$	80	256×320

where 320 is the number of primitive polynomials over $\mathbb{F}_3$ of degree 8.

6.3 A Complete Design Process

In the following we will give an example to show a complete process for design of a $((p^n-1)^2, p^n-1, 1+2p^n)$ signal set.

Example 8. Design a $(6400, 80, 163)$ balanced signal set over $\mathbb{F}_3$ where each sequence has linear span 492. (Note that from Table 5, there are $256 \times 320 = 81920$ different such signal sets.) Let $p = 3$ and $n = 4$. Then $v = 3^4 - 1 = 80 \Longrightarrow v^2 = 6400$.

1. Select two base sequences $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$:

   Since $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ can be taken from the set, say Ω, consisting of all 2-level auto correlation sequences of period $3^4 - 1 = 80$ over $\mathbb{F}_4$. From Section 2.1, we know, Ω only consists two types of sequences, one is m-equences of period 80 of degree 4 and the other is the GMW sequences of period 80. We choose $\underline{\mathbf{a}} = \{a_i\}$ and $\underline{\mathbf{b}} = \{b_i\}$ as two GMW sequences whose elements are given by

   $$a_i = Tr_1^2(Tr_2^4(\beta^i)^5), i = 0, 1, \cdots, \text{ and}$$
   $$b_i = Tr_1^2(Tr_2^4(\beta^{7i})^5), i = 0, 1, \cdots$$

   where β is a primitive element of $\mathbb{F}_{3^4}$.

   According to Figure 1, we need to compute an LFSR over the finite field $\mathbb{F}_{3^4}$ for implementing the shift sequence $\underline{\mathbf{e}}$. Since $\underline{\mathbf{b}}$ is a GMW sequence, it can be implemented by an LFSR over the finite field $\mathbb{F}_{3^2}$ together with a finite field circiut for computing $Tr_1^2(x^5)$.

2. Implementation of $\underline{\mathbf{e}}$ by an LFSR over $\mathbb{F}_{3^4}$:

   We need a 2-stage LFSR over $\mathbb{F}_{3^4}$ to implement $\underline{\mathbf{e}}$. Let $\mathbb{F}_{3^4}$ be defined by a primitive polynomial $f(x) = x^4 + 2x + x^2 + x + 2$ and let β be a root of $f(x)$ in the extension. Thus β is a primitive element of $\mathbb{F}_{3^4}$. Choose $g(x) = x^2 - \beta^{35}x - 2\beta$ which is a primitive polynomial over $\mathbb{F}_{3^4}$ of degree 2. Therefore we have an LFSR over $\mathbb{F}_{3^4}$ with $g(x)$ as its charateristic polynomial. Set an initial state (β^{67}, β^{62}) for this LFSR.

3. Implementation of $\underline{\mathbf{b}}$ by the LFSR over $\mathbb{F}_{3^2}$ together with a finite field circuit:

   Let $\mathbb{F}_{3^2}$ be defined by $h(x) = x^2 + 2x + 2$ where $h(x)$ is primitive. Let ω be a root of $h(x)$ in the extension. So ω is a primitive element of $\mathbb{F}_{3^2}$. Choose $t(x) = x^2 - 2\omega^7 - 2\omega$ which is a primitive polynomial over $\mathbb{F}_{3^2}$ of degree 2. Then we have an LFSR over $\mathbb{F}_{3^2}$ with $t(x)$ as its charateristic polynomial.

   Note that $\underline{\mathbf{a}}$ can not use an LFSR implementation, because it succeeds elements from finite field $\mathbb{F}_{3^4}$. So, it only can be implemented by the finite field circuit.

   The following figure presents this implementation. We obtain all sequences in S by varing different initial states of the LFSR2 in Figure 2.

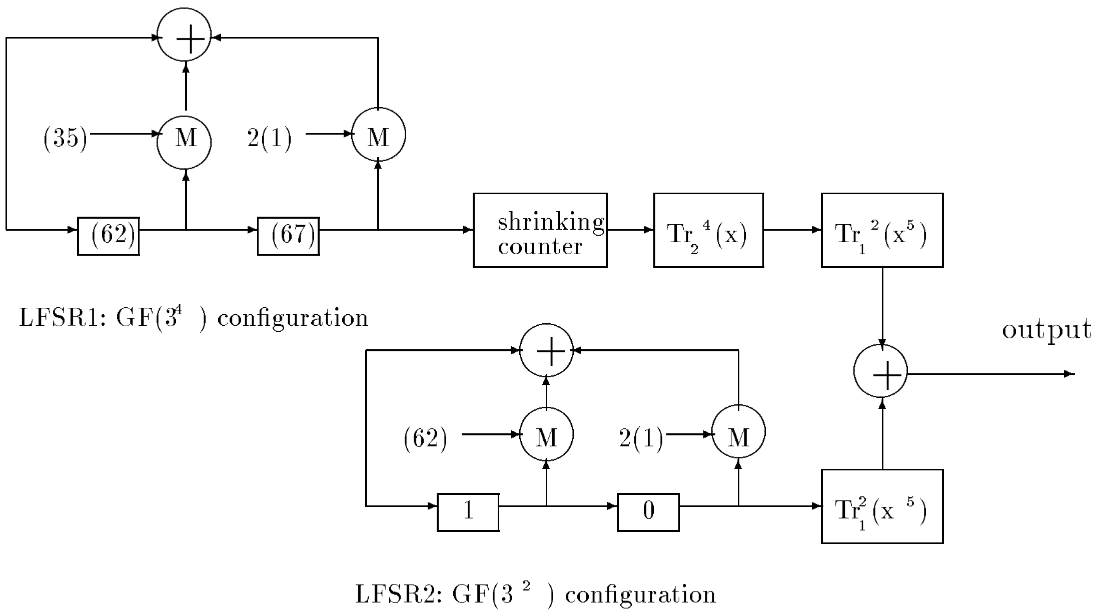

Figure 2. Galois Configuration of a $(6400, 80, 163)$ Signal Set

In Figure 2, $(i) = \beta^i$ and $(i) = \omega^i$ in LFSR1 and LFSR2 respectively.

According to Lemma 6 and Theorem 2, the signal set $S = S(\underline{\mathbf{a}}, \underline{\mathbf{b}}, \underline{\mathbf{e}})$, implemented by Figure 2, is a $(6400, 80, 163)$ signal set. From Theorems 1 and 3, we get that each sequence in S is balanced and has linear span 492. The architecture provided by Figure 2 can be efficiently implemented in both hardware and software.

References

1. L.D. Baumert, *Cyclic Difference Sets, Lecture Notes in Mathematics*, **182**, Springer-Verlag, 1971.
2. M. Antweiler and L. Bőmer, Complex sequences over $GF(p)$ with a two-level autocorrelation function and a large linear span, *IEEE Trans. on Inform. Theory*, vol. IT-38, No. 1, pp. 120-130, January 1992.
3. A.H. Chan, M. Goresky, and A. Klapper, Correlation functions of geometric sequences, *Advances in cryptology—EUROCRYPT '90 (Aarhus, 1990)*, pp. 214–221, Lecture Notes in Comput. Sci., 473, Springer, Berlin, 1991.
4. J. Dillon and H. Dobbertin, New cyclic difference sets with Spinger parameters, preprint, August 1999.
5. H. Dobbertin, Kasami power functions, permutations and cyclic difference sets, *Proc. of the NATO ASI Workshop*, Bad Windsheim, August 3-14, 1998.
6. R.A. Games, Cross corrlation of m-sequences and GMW sequences with the same primitive polynomial, *Discrete Appl. Math*, **12**(1985), pp. 139-146.
7. R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. on Inform. Theory*, January 1968, pp. 154-156.
8. B. Gordon, W.H. Mill, and L.R. Welch, Some new differnce sets, *Canadian J. Math.*, vol. 14, no. 4, pp.614-625, 1962.
9. S.W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982, pp. 39.
10. G. Gong, On $q-$ary cascaded GMW sequences, *IEEE Trans. on Inform. Theory*, vol. 42, No. 1, January 1996, pp. 263-267.

11. G. Gong, Z.T. Dai and S.W. Golomb, Criterion and Counting for Cyclically shift distinct q−ary GMW sequences of period $q^n - 1$, *IEEE Trans. on Inform. Theory*,
12. G. Gong, P. Gaal and S.W. Golomb, A suspected infinity class of cyclic Hadamard difference sets, *the Proceedings of 1997 IEEE Information Workshop*, July 6-12, 1997, Longyearbyen, Svalbard, Norway.
13. G. Gong, Theory and applications of q-ary interleaved sequences, *IEEE Trans. on Inform. Theory*, vol. 41, No. 2, March 1995, pp. 400-411.
14. Guang Gong, *Sequence Analysis*, Lecture Notes for Course CO739x, University of Waterloo, http://www.cacr.math.uwaterloo.ca/∼ggong, Chapter 5.
15. G. Gong and S.W. Golomb, Binary Sequences with Two-Level Autocorrelation, *IEEE Trans. on Inform. Theory*, vol. 45, No.2, March 1999, pp.692-693.
16. Marshall Jr. Hall, A survey of difference sets, *Proc. Amer. Math. Soc. 7*(**1956**), pp.975-986.
17. Tor Helleseth, Correlation of m-sequences and related topics, *Sequences and their Applications – Proceedings of SETA'98*, Discrete Mathematics and Theoretical Computer Science, Springer, 1999. pp. 49-66.
18. Tor Herlestam, On functions of linear shift register sequences, *Advances in Cryptology-EuroCrypt'85*, Lecture Notes in Computer Science, No. 219, Springer-Verlag, 1985, pp. 119-129.
19. Tor Helleseth, Correlation of m-sequences and related topics, *Sequences and their Applications – Proceedings of SETA'98*, Discrete Mathematics and Theoretical Computer Science, Springer, 1999. pp. 49-66.
20. Tor Helleseth, Some results about the cross-correlation functions between two maxiaml length linear sequences, *Discrete Math.*, vol. 16, pp.209-232, 1978.
21. S. Jiang, Z.D. Dai and G. Gong, Notes on q-ary inteleaved sequences, *Sequences and their Applications – Proceedings of SETA'98*, Discrete Mathematics and Theoretical Computer Science, Springer, 1999. pp. 273-283.
22. T. Kasami, Weight distribution of Bose-Chaudhuri-Hocquenghem codes, *Combinarotial Mathematics and its Applications*, Chpel Hill, NC: Univ. of North Carolina PRess, 1969.
23. A. Klapper, A.H. Chan and M. Goresky, Cascaded GMW sequences, *IEEE Trans. on Inform. Theory*, vol. 39, No. 2, Jan. 1993, pp. 177-183.
24. A. Klapper, A.H. Chan, M. Goresky, Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences, *Discrete Appl. Math.* **46**(1993), No. 1, pp. 1-20.
25. Andrew Klapper, Large families of sequences with near-optimal corrleations and large linear span, *IEEE Trans. Inform. Theory*, vol 42, No. 4, 1996, pp.1241-1248.
26. P. Vijay Kumar and Oscar Moreno, Prime-phase sequences with periodic correlstion properties better than binary sequences, *IEEE Trans. Inform. Theory*, vol 37, No. 3, May 1991, pp.603-616..
27. P. Vijay Kumar, On bent sequences and generaized bent functions, Ph. D. These, University of Southern California, Los Angeles, 1983.
28. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983, Theorem 3.35, pp. 97 -98.
29. A. Maschietti, Difference sets and hyperovals, *Designs, Codes and Cryptography*, **14**, pp. 89-98, 1998.
30. J.L. Massey, Shift-register synthesis and BCH decoding, *IEE- Trans. on Inform. Theory* vol. IT-15, January 1969.
31. J.S. No, S.W. Golomb, G. Gong, H.K. Lee, and P. Gaal, New binary pseudo-random sequences of period $2^n - 1$ with ideal autocorrelation, *IEEE Trans. on Inform. Theory*, vol. 44, No. 2, March 1998, pp.814-817.
32. J.S. No and P.V. Kumar, A new family of binary pseudo-random sequences having optimal priodic correlation properties and large linear span, *IEEE Trans. Inform. Theory*, vol 35, no. 2, March 1989, pp.371-379.
33. Jong-Seon No, Hagong Chung and Min-Seon Yin, Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$, *IEEE Trans. Inform. Theory*, vol. 44, no. 3, 1998, pp.1278-1282.
34. J.S. No, K. Yang, H.G. Chung and H.Y. Song, New constructions for families of binary sequences with optimal correlation properties, *IEEE Trans. Inform. Theory* vol. 43, no. 5, 1997, pp.1596-1602.
35. J.D. Olsen, R.A. Scholtz and L.R. Welch, Bent-function sequences. *IEEE Trans. Inform. Theory*, vol. 28, no. 6, 1982, pp. 858–864.
36. John G. Proakis, *Digital Communications*, McGraw-Hill, Inc., the third edition, 1995.
37. R.A. Scholtz and L.R. Welch, GMW sequences, *IEEE Trans. Inform. Theory*, vol. 30, no. 3, May 1984, pp.548-553.
38. V.M. Sidelnikov, On mutual correlation of sequences, *Probl.Kybern.*, vol. 24, pp.537-545, Sept. 1978.
39. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43**, pp. 377-385, 1-38.
40. Henning Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1991.
41. H.M. Trachtenberg, On the cross-correlation functions of maximal linear sequences, Ph. D. These, University of Southern California, Los Angeles, 1970.

42. L.R. Welch, Lower bounds on the manimum correlation of signals, *IEEE Trans. Inform. Theory*, vol. IT-20, no. 3, May 1974, pp.397-399.
43. N. Zierler, Linear recurring sequences, *J. Soc. Indust. Appl. Math.* **7** 31-48 (1959).