New Designs for Signal Sets With Low Cross Correlation, Balance Property, and Large Linear Span: GF (p) Case

Guang Gong, *Member, IEEE*

***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 two-level autocorrelation function together with the interleaved structure to construct a set of long sequences with the desired properties. The resulting sequences are interleaved sequences of period v^2. There are v cyclically shift distinct sequences in each family. The maximal correlation value is $2v+3$ which is optimal with respect to the Welch bound. Each sequence in the family is balanced and has large linear span. In particular, for binary case, cross/out-of-phase autocorrelation values belong to the set $\{1, -v, v+2, 2v+3, -2v-1\}$, any sequence where the short sequences are quadratic residue sequences achieves the maximal linear span. It is shown that some families of these sequences can be implemented efficiently in both hardware and software.**

***Index Terms*—Finite field, interleaved sequences, linear span, low cross correlation, nonbinary sequences, two-level autocorrelation.**

I. Introduction and Preliminaries

A FAMILY of pseudorandom sequences with low cross correlation, good randomness, and large linear span has important applications in code-division multiple-access (CDMA) communications and cryptology. The pseudorandom sequences with low cross correlation employed in CDMA communications can successfully combat interference from the other users who share a common channel. On the other hand, the sequences with low cross correlation employed in either stream cipher cryptosystems as key stream generators or in digital signature algorithms as pseudorandom number generators can resist cross-correlation attacks. It is well known that the pseudorandom sequences employed in the above types of applications must have large linear spans (also called linear complexity) in order to resist attacks from the application of the Berlekamp–Massey algorithm. (The Berlekamp–Massey algorithm can reconstruct a sequence by knowing a portion of the sequence.) During the past two decades, extensive research has been done on how to generate sequences with these desired properties, see [49], [36], [46], [4], [3], [17], [32].

In this paper, we will present 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 two-level autocorrelation function and an interleaved structure to construct a set of long p-ary sequences with the desired properties. This property also has significant meaning with the application in signal detection of high-speed broad-band communication systems. The original idea of this design was proposed by the author in 1995 [17], but was not emphasized in the original paper. The original design given in [17] uses m-sequences as short sequences. In recent years, the status for constructing binary or nonbinary sequences with the two-level autocorrelation function has been dramatically changed. A lot of new binary sequences with two-level autocorrelation 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 two-level autocorrelation sequences as "building blocks" except for a class of two-level autocorrelation sequences of period v where v is a product of twin primes. Some families of the resulting sequences can be efficiently implemented in both hardware and software.

In the following, we introduce some notations and preliminaries for sequence designs which will be used throughout the paper. The reader is referred to [13] for shift-register sequences, [37] for the theory of finite field, and [27] for sequences with low cross correlation.

Notations:

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

A. Left Shift Operator and Shift Equivalent Relation

Let $\underline{\boldsymbol{a}} = \{a_i\}$ be a sequence over $\mathbb{F}_p$. The left shift operator L on $\underline{\boldsymbol{a}}$ is defined as $L(\underline{\boldsymbol{a}}) = a_1, a_2, \ldots$. For any $i > 0$, $L^i(\underline{\boldsymbol{a}}) = a_i, a_{i+1}, \ldots$. $L^i(\underline{\boldsymbol{a}})$ is said to be a *phase shift* of $\underline{\boldsymbol{a}}$. We denote $L^0(\underline{\boldsymbol{a}}) = \underline{\boldsymbol{a}}$ for convention. Two periodic sequences, $\underline{\boldsymbol{a}} = \{a_i\}$

Manuscript received April 5, 2000; revised July 8, 2002. This work was supported by NSERC under Grants RGPIN 227700-00.

The author is with the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@ece.uwaterloo.ca).

Communicated by A. M. Klapper, Associate Editor for Sequences.
Digital Object Identifier 10.1109/TIT.2002.804044.

0018-9448/02$17.00 © 2002 IEEE

and $\underline{\boldsymbol{b}} = \{b_i\}$, are called *(cyclically) shift equivalent* if there exists an integer k such that

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

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

B. Balance Property

Let $\underline{\boldsymbol{a}}$ be a p-ary sequence with period v. We say that $\underline{\boldsymbol{a}}$ is *balanced* if 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, when $v = p^n - 1$, we say that $\underline{\boldsymbol{a}}$ is *balanced* if each nonzero element in $\mathbb{F}_p$ occurs p^{n-1} times and each zero element occurs $p^{n-1} - 1$ times.

C. Correlation

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

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

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 $\underline{\boldsymbol{b}} = \underline{\boldsymbol{a}}$, then $C_{\underline{\boldsymbol{a}}, \underline{\boldsymbol{a}}}(\tau)$ is called an *autocorrelation* function of $\underline{\boldsymbol{a}}$, denoted by $C_{\underline{\boldsymbol{a}}}(\tau)$ 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 $\underline{\boldsymbol{a}}$ has an *(ideal) two-level autocorrelation function*. For a fixed $c \in \mathbb{F}_p$, let

$$H_c(\underline{\boldsymbol{a}}) = |\{i | a_i = c, 0 \leq i < v\}| \tag{2}$$

then H_c represents the number of occurrences of the element c in a period of the sequence. If $\underline{\boldsymbol{a}}$ is a two-level autocorrelation sequence over $\mathbb{F}_p$, then

$$H_c(\underline{\boldsymbol{a}}) = \begin{cases} (v+1)/p, & \text{if } c \in \mathbb{F}_p^* \\ (v+1)/p - 1, & \text{if } c = 0. \end{cases} \tag{3}$$

In other words, any two-level autocorrelation sequence satisfies the balance property.

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

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

where $\tau \neq 0$ if $i = j$. We call δ *the maximal correlation of* S and S, a (v, r, δ) *signal set*. (A sequence in S is also called a *signal* from the point of view of engineering [50].) We say that the set S has *low cross correlation* if $\delta \leq c\sqrt{v}$ where c is a constant. When we consider the cross correlation of two sequences $\underline{\boldsymbol{s}}_i, \underline{\boldsymbol{s}}_j$ in S, we simply write $C_{i,j}(\tau)$ for $C_{\underline{\boldsymbol{s}}_i, \underline{\boldsymbol{s}}_j}(\tau)$.

D. Interleaved Sequences

Gong introduced the following concept of interleaved sequences over $\mathbb{F}_p$ in 1995 [17]. Let $\underline{\boldsymbol{u}} = (u_0, u_1, \ldots, u_{st-1})$ 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 $\underline{\boldsymbol{u}}$ into a s by t matrix as follows:

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

If each column vector of the above matrix is either a phase shift of a p-ary sequence, say $\underline{\boldsymbol{a}}$, of period s, or a zero sequence, then we say that $\underline{\boldsymbol{u}}$ is an (s, t) *interleaved sequence over* $\mathbb{F}_p$. We also say that A is the matrix form of $\underline{\boldsymbol{u}}$. Let A_j be the jth column vector of A, then $A = (A_0, A_1, \ldots, A_{t-1})$. We call A_j *column sequences of* $\underline{\boldsymbol{u}}$ (or component sequences of $\underline{\boldsymbol{u}}$ in [17]). According to the definition, A_j is a transpose of $L^{e_j}(\underline{\boldsymbol{a}})$ or $(0, 0, \ldots, 0)$. In this paper, we omit the transpose symbol because we consider it as a sequence. Thus, we write

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

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

Note. For a general discussion of periods and linear spans of interleaved sequences with m-sequences as the column sequences, see [17], [28].

Example 1: Let

$$\underline{\boldsymbol{e}} = (3, 6, 5, 5, 2, 3, 5)$$

and

$$\underline{\boldsymbol{a}} = (1, 1, 1, 0, 1, 0, 0)$$

be a binary m-sequence of period 7. Then a 7 by 7 matrix A can be given as follows:

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

We read it out row by row, from left to right within a row beginning with the top row. Then we have the following $(7, 7)$ interleaved sequence of period 49:

$\underline{\boldsymbol{u}} =$

0000100110001001111010111001101101111001101011111.

E. Trace Representation

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

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

where $q = p^m$ and $n = ml$. Any sequence $\underline{\boldsymbol{a}}$ 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 $\mathbb{F}_p$

$$f(x) = \sum_{i=1}^{r} \mathrm{Tr}_1^{n_i}(\beta_i x^{t_i}), \qquad \beta \in \mathbb{F}_{p^{n_i}}$$

such that

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

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. ($\underline{\boldsymbol{a}}$ is also referred to as an r-term sequence.) Since there is a one-to-one correspondence between the function $f(x)$ and the sequence $\underline{\boldsymbol{a}}$, we use both $f(x)$ and $\underline{\boldsymbol{a}}$ in this paper. Note that in the language of algebraic-geometry codes, $\underline{\boldsymbol{a}}$ is called an *evaluation* of $f(x)$ at α [54]. Sometimes, we will also use this term for convenience.

F. Linear Span

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

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

and $\underline{\boldsymbol{a}} = \{a_i\}$ satisfy the following recursive relation:

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

so that $h(x)$ is called a *characteristic polynomial* of $\underline{\boldsymbol{a}}$ (over $\mathbb{F}_p$). The polynomial with the smallest degree among all characteristic polynomials of $\underline{\boldsymbol{a}}$ is called the *minimal polynomial* of $\underline{\boldsymbol{a}}$ (over $\mathbb{F}_p$). The linear span of $\underline{\boldsymbol{a}}$ is equal to the *degree* of minimal polynomial of $\underline{\boldsymbol{a}}$. For example, $\underline{\boldsymbol{a}} = 1001011$ is a binary sequence of period 7 and has $h(x) = x^3 + x + 1$ as minimal polynomial. Hence, the linear span of $\underline{\boldsymbol{a}}$ is 3.

This paper is organized as follows. Since we will utilize all but one two-level autocorrelation sequences to construct signal sets with low cross correlation, we will start by a brief review for known constructions of two-level autocorrelation or low cross-correlation sequences and some extensions for these results as well. These are the contents of Section II. In Section III, we provide 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 when the matrix forms of the interleaved sequences are applied. In Section IV, we present constructions for $(v^2, v, 2v+3)$ signal sets over $\mathbb{F}_p$ for both $p = 2$ and $p > 2$. In Section V, 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. In Section VI, we provide an architecture for implementing $(v^2, v, 2v+3)$ signal sets, show that some families of the resulting sequences can be efficiently implemented in both hardware and software, and discuss some aspects in comparison with the known constructions.

Note. The result on decomposition of interleaved sequences obtained in Section V 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.

II. Known Constructions of Good Correlation and Two Extensions

In this section, we will first give a brief summary for all known constructions for two-level autocorrelation sequences and previous known designs for signal sets with low cross correlation in the Galois field configuration. Then we will show two extensions for these known results in order to clear up some confusion in the literature.

A. Known Constructions for p-ary Sequences of Period v With Two-Level Autocorrelation

The first three classic constructions:

A. For $v = p^n - 1$, all $n \geq 2$ and p, we have m-sequences [53], [13], [57].

B. For $v = p^n - 1$ and all p, if $n \geq 6$, n composite, we have GMW [51], generalized GMW sequences [12], [42], [4], [30], [14], [43]. Note that a general construction for the generalized GMW sequences has not been explicitly stated in the literature. We will present it later in Section II-C.

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) [13]. If $v = 4a^2 + 27$, we also have Hall's Sextic Residue Sequences [20].

C.2. 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 [2].

After 1997, we have the following new constructions D, E, and F for $p = 2$:

D. Conjectured trace sequences [45] (No *et al.*, 1998): three-term sequences (also Gong–Gaal–Golomb [16], 1997), five-term sequences and Welch–Gong transfor mation sequences.

E. Hyper-oval construction: Segre case and Glynn types I and II (Maschietti [39], 1998).

F. Kasami power function construction: the special case was conjectured by No, Chung, Yun [47] in 1998, and the general case was conjectured by Dobbertin [9] in 1999.

G. Miscellaneous constructions: for the case of $p > 2$, before 1999 we only had two constructions for two-level autocorrelation sequences of period $p^n - 1$ over $\mathbb{F}_p$. One is the m-sequences over GF (p), and the other is the Gordon–Mills–Welch (GMW) or generalized GMW sequences over $\mathbb{F}_p$. During the past two years, several new constructions have appeared, see [26], [38], [1], [44], [7], [21].

Remark 1:

a) The three- and five-term sequences obtained by D are special classes of sequences obtained by F. We list them separately due to their special properties [45] and for the point of view of implementation in Section VI as well.

b) All conjectured sequences with two-level autocorrelation have been proved by Dillon and Dobbertin in their latest draft [8] in August 1999.

B. Previous Known Designs for Signal Sets With Low Correlation in the Galois Field Configuration

Binary Case.

n Odd Case:

A. Gold-pair construction and the generalization:

$$(2^n-1,\, 2^n+1,\, 1+2^{\lfloor (n+1)/2 \rfloor})$$

signal set

$$\{g(x)+\mathrm{Tr}_1^n(\beta x),\, \beta \in \mathbb{F}_{2^n}\} \cup \{\mathrm{Tr}_1^n(x)\}. \tag{4}$$

A.1. $g(x) = \mathrm{Tr}_1^n(x^r)$ where r only allows a few different values to be taken, see [24]. This construction was first published by Gold in 1969 [11] for the case of n odd.

A.2. $g(x)$ can be selected as some special GMW functions [10], [31], or cascaded GMW functions [32], or some decimation of two-level autocorrelation sequences constructed from D and F in Section II-B (Dillon and Dobbertin, in their milestone work [8], showed that the conjectured sequences have two-level autocorrelation in terms to show that they have the same correlation as the Gold sequences). This is considered 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 two-level autocorrelation sequence or its certain decimation.

A.3.

$$g(x) = \sum_{i=1}^{(n-1)/2} \mathrm{Tr}_1^{n_i}(x^{1+2^i})$$

where $n_i | n$, discussed by Boztas and Kumar in [3].

Even Case:

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

$$\Gamma = \left\{ g\left(\mathrm{Tr}_n^{2n}(x^2)+\beta x^{2^n+1}\right),\, \beta \in \mathbb{F}_{2^n} \right\}. \tag{5}$$

B.1. $g(x) = \mathrm{Tr}_1^n(x)$, which represents the Kasami original construction [29].

B.2. $g(x) = \mathrm{Tr}_1^n(x^r)$, $\gcd(r,\, 2^n-1)=1$, or $g(x)$ is an arbitrary function whose evaluation is a two-level autocorrelation sequence of period 2^n-1. These are called the *generalized Kasami constructions*. The former was generalized by No and Kumar [46] in 1989, called No sequences, and the latter was partially generalized by No *et al.* [48] in 1998. We will present it in the next subsection.

C. Bent function construction: $(2^{2n}-1,\, 2^n,\, 1+2^n)$ $(n = 2k)$signal set, proposed by Olsen *et al.* [49] in 1982.

D. D. Kerdock code construction: $(2^{2n}-1,\, 2^{2n-1},\, 1+2^n)$, see [41], [27].

Interleaved Case:

E. Interleaved construction: $((2^n-1)^2,\, 2^n,\, 1+2^{n+1})$ signal set, the column sequences are chosen as m-se quences, constructed in 1995 by the author [17].

Nonbinary Case: $p > 2$

For $p > 2$, only constructions A.1. and C. among the constructions of the binary case have been 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 [55], [22] 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.* [35]).

C. Bent construction: $(p^n-1,\, p^n+1,\, 1+\sqrt{p^n})$ signal sets, n even [35], [34].

Helleseth has a good survey paper [22] 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..

Remark 2: The correlation of the signal sets produced by all of the above constructions is optimal with respect to the Welch bound. We would like to point out that this bound is not sensitive to family size. For example, the Kasami signal set, from Construction B, and the Kerdock code set, from Construction D, have the same maximal correlation. But the Kerdock code set has a much larger size than the Kasami signal set. For more discussion along this line see [27].

In this paper, we will generalize Construction E for both binary and nonbinary cases by employing short sequences with two-level autocorrelation. The resulting signal sets have the following types of parameters:

$\left((p^n-1)^2,\, p^n-1,\, 1+2p^n\right)$ signal sets
for any n, $p=2$ or $p>2$, and
$(v^2,\, v,\, 2v+3)$ signal sets, v is prime and $p=2$.

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

C. Two Extensions

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 two-level autocorrelation sequence of period p^m-1. Let $\sigma(x)$ be a GMW function of length r [30], [14] 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.,

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

where $\circ$ is a function composition operator and s_i 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 two-level autocorrelation sequence of period $p^n - 1$. (Such sequences are called generalized GMW sequences over $\mathbb{F}_p$.)

A proof of this result can be derived from the work of Gordon, Mill, and Welch in [12] as early as 1962, and it also explicitly follows from repeatedly using the result of Klapper, Chan, and Goresky in [31] of 1993.

For an easy reference in Sections IV and VI, we will use X to represent the set of two-level autocorrelation sequences constructed from Construction X

$$X \in \{A, B, C.1, C.2, D, E, F, G\}$$

in Section II-A. In particular, we will set B_0 to represent the set of evaluations of GMW functions of length r. Then $B_0 \subset B$.

Proposition 2: Let S be a set consisting of 2^n sequences obtained by the functions in (5) where $g(x)$ is an arbitrary function whose evaluation is a two-level autocorrelation sequence over $\mathbb{F}_2$. Then the cross correlation of any two sequences in S and out-of-phase autocorrelation values of any sequence in S are three-valued and belong to the set $\{-1, -1-2^n, 2^n - 1\}$. S is called a *generalized Kasami signal set.*

A proof of Proposition 2 can be obtained by applying a similar method that No *et al.* used for proving [48, Theorem 2], so we omit it.

Remark 3: According to Proposition 1, all other results in [48] by No *et al.* can be written into the form of (5). By applying Proposition 2, these results follows directly.

III. Interleaved Constructions 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.

A. A Procedure

Procedure 1

1) Choose

$$\underline{\boldsymbol{a}} = (a_0, a_1, \ldots, a_{v-1})$$

and

$$\underline{\boldsymbol{b}} = (b_0, b_1, \ldots, b_{v-1})$$

two sequence over $\mathbb{F}_p$ of period v with two-level autocorrelation.

2) Choose $\underline{\boldsymbol{e}} = (e_0, e_1, \ldots, e_{v-1})$, an integer sequence whose elements are taken from $\boldsymbol{Z}_v$.

3) Construct $\underline{\boldsymbol{u}} = (u_0, u_1, \ldots, u_{v^2-1})$, a (v, v) interleaved sequence whose jth column sequence is given by $L^{e_j}(\underline{\boldsymbol{a}})$, $j = 0, 1, \ldots, v-1$.

4) Set

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

whose elements are defined by

$$s_{j,i} = u_i + b_{j+i}, \qquad 0 \le i, j < v$$

or, equivalently, $\underline{\boldsymbol{s}}_j = \underline{\boldsymbol{u}} + L^j(\underline{\boldsymbol{b}})$.

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

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

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

For convenience of notation, we will write $\underline{\boldsymbol{u}} = \underline{\boldsymbol{s}}_\infty$ because we can consider that $u_i = u_i + 0$ of Step 4) in Procedure 1. As a convention, we define $\infty \pm r = \infty$ and $\infty \pm \infty = \infty$ where r is an nonnegative integer. From Steps 1)–4) in Procedure 1, for $k \in Z_v$, $\underline{\boldsymbol{s}}_k \in S$ has a matrix form $S_k = A + B_k$ where

$$A = \begin{bmatrix} a_{e_0} & a_{e_1} & \cdots & a_{e_{v-1}} \\ a_{e_0+1} & a_{e_1+1} & \cdots & a_{e_{v-1}+1} \\ a_{e_0+2} & a_{e_1+2} & \cdots & a_{e_{v-1}+2} \\ \vdots & & & \\ a_{e_0+v-1} & a_{e_1+v-1} & \cdots & a_{e_{v-1}+v-1} \end{bmatrix}$$

and

$$B_k = \begin{bmatrix} b_k & b_{k+1} & \cdots & b_{v-1} \\ b_k & b_{k+1} & \cdots & b_{v-1} \\ \vdots & & & \\ b_k & b_{k+1} & \cdots & b_{v-1} \end{bmatrix}.$$

If we write $S_k = (S_{k,0}, S_{k,1}, \ldots, S_{k,v-1})$, then column j of S_k is given by

$$S_{k,j} = L^{e_j}(\underline{\boldsymbol{a}}) + b_{j+k}, \qquad 0 \le j < v. \tag{6}$$

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

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

1) Choose $\underline{\boldsymbol{a}} = (1110100)$ and $\underline{\boldsymbol{b}} = (1001011)$, m-sequences of period 7.

2) Choose $\underline{\boldsymbol{e}} = (3, 6, 5, 5, 2, 3, 5)$.

3) Construct the interleaved sequence $\underline{\boldsymbol{u}}$ which is the same as in Example 1 and has the matrix form A.

4) Construct $\underline{\boldsymbol{s}}_k$: $k = 0, 1, \ldots, 6$. We have

$$S_0 = A + B_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$+\begin{bmatrix} 1&0&0&1&0&1&1\\ 1&0&0&1&0&1&1\\ 1&0&0&1&0&1&1\\ 1&0&0&1&0&1&1\\ 1&0&0&1&0&1&1\\ 1&0&0&1&0&1&1\\ 1&0&0&1&0&1&1 \end{bmatrix}$$

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

The top row of B_1 is the sequence $L(\underline{\boldsymbol{b}})$, a phase shift 1 of $\underline{\boldsymbol{b}}$, the top row of B_2 is the sequence $L^2(\underline{\boldsymbol{b}})$, and so on. In this fashion, we obtain that seven sequences in S are

$$\begin{aligned} \underline{\boldsymbol{s}}_0 &= 1001111010100111101101110010001000000101\\ &\quad 1010010100\\ \underline{\boldsymbol{s}}_1 &= 0010011111010101010100101110100110011 10\\ &\quad 0011001000\\ \underline{\boldsymbol{s}}_2 &= 0101010100110000100110010111111101011001\\ &\quad 0001110001\\ \underline{\boldsymbol{s}}_3 &= 1011000011111011000011100101000011101 11\\ &\quad 0100000011\\ \underline{\boldsymbol{s}}_4 &= 0111101101101100001000000000110001010 11\\ &\quad 1111100110\\ \underline{\boldsymbol{s}}_5 &= 1110110001000010011111100101101010010010\\ &\quad 1000101101\\ \underline{\boldsymbol{s}}_6 &= 1100001000011110110001011100011111000 00\\ &\quad 0110111010. \end{aligned}$$

5) Set $S = \{\underline{\boldsymbol{s}}_0, \underline{\boldsymbol{s}}_1, \ldots, \underline{\boldsymbol{s}}_6\}$.

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

1) Choose

$$\underline{\boldsymbol{a}} = (2, 1, 0, 1, 1, 2, 0, 1)$$

and

$$\underline{\boldsymbol{b}} = (2, 2, 0, 2, 1, 1, 0, 1)$$

which are two shift distinct m-sequences over $\mathbb{F}_3$ of degree 2 with period 8.

2) Choose a shift sequence $\underline{\boldsymbol{e}} = (0, 5, 6, 5, 7, 7, 3, 6) \in \mathbb{Z}_8^{(8)}$.

3) Construct an $(8, 8)$ interleaved sequence $\underline{\boldsymbol{u}}$ which is given in the matrix form as follows:

$$A = \begin{bmatrix} 2&2&0&2&1&1&1&0\\ 1&0&1&0&2&2&1&1\\ 0&1&2&1&1&1&2&2\\ 1&2&1&2&0&0&0&1\\ 1&1&0&1&1&1&1&0\\ 2&0&1&0&1&1&2&1\\ 0&1&1&1&2&2&1&1\\ 1&1&2&1&0&0&0&2 \end{bmatrix}.$$

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

$$\begin{aligned} S_0 &= A + B_0\\ &= A + \begin{bmatrix} 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1\\ 2&2&0&2&1&1&0&1 \end{bmatrix}\\ &= \begin{bmatrix} 1&1&0&1&2&2&1&1\\ 0&2&1&2&0&0&1&2\\ 2&0&2&0&2&2&2&0\\ 0&1&1&1&1&1&0&2\\ 0&0&0&0&2&2&1&1\\ 1&2&1&2&2&2&2&2\\ 2&0&1&0&0&0&1&2\\ 0&0&2&0&1&1&0&0 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} S_5 &= A + B_5\\ &= A + \begin{bmatrix} 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1\\ 1&0&1&2&2&0&2&1 \end{bmatrix}\\ &= \begin{bmatrix} 0&2&1&1&0&1&0&1\\ 2&0&2&2&1&2&0&2\\ 1&1&0&0&0&1&1&0\\ 2&2&2&1&2&0&2&2\\ 2&1&1&0&0&1&0&1\\ 0&0&2&2&0&1&1&2\\ 1&1&2&0&1&2&0&2\\ 2&1&0&0&2&0&2&0 \end{bmatrix}. \end{aligned}$$

B. The Balance Property of $S(\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}, \underline{\boldsymbol{e}})$

We will show that any sequence in $S = S(\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}, \underline{\boldsymbol{e}})$ 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. Consequently, 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. Thus, it is balanced.

Proof: For $\underline{\boldsymbol{s}}_k \in S$, according to (6), the column sequences $A_{k,j}$ of $\underline{\boldsymbol{s}}_k$ can be represented by

$$A_{k,j} = L^{e_j}(\underline{\boldsymbol{a}}) + b_{k+j}, \qquad 0 \le j < v. \tag{7}$$

Binary Case: $p = 2$.

Note that both $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ are two-level autocorrelation sequences. Thus, they are balanced. So, there are $\frac{v+1}{2}$ 1's and $\frac{v-1}{2}$ 0's in each of them. For j: $0 \le j < v$, there are $\frac{v+1}{2}$ j's such that the

$$H_1(L^{e_j}(\underline{\boldsymbol{a}}) + b_{k+j}) = \frac{v-1}{2}$$

and $\frac{v-1}{2}$ j's such that

$$H_1(L^{e_j}(\underline{\boldsymbol{a}}) + b_{k+j}) = \frac{v+1}{2}.$$

Thus, the Hamming weight of $\underline{\boldsymbol{s}}_k \in S$ is given by

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

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

Nonbinary Case: $p > 2$

In this case, we have $v = p^n - 1$ from Section II-A. Since $\underline{\boldsymbol{a}}$ is balanced, for each j: $0 \le j < v$, we have

$$H_c\left(L^{e_j}(\underline{\boldsymbol{a}})\right) = \begin{cases} p^{n-1}, & \text{if } c \in \mathbb{F}_p^* \\ p^{n-1} - 1, & \text{if } c = 0 \end{cases} \tag{8}$$

where $H_c(.)$ is defined by (2) in Section I. From (7), if $b_{k+j} = 0$, then

$$H_d(A_{k,j}) = H_d\left(L^{e_j}(\underline{\boldsymbol{a}})\right). \tag{9}$$

If $b_{k+j} \ne 0$, then there are $p-2$ nonzeros 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

$$\begin{aligned} &H_d\left(L^{e_j}(\underline{\boldsymbol{a}}) + b_{k+j}\right) \\ &\quad = \begin{cases} p^{n-1}, & d \ne 0 \text{ for } p-2\, c\text{s in } \mathbb{F}_p^* \\ p^{n-1}, & d = 0 \text{ for } c = -b_{k+j} \ne 0 \\ p^{n-1} - 1, & d \ne 0 \text{ for } c = 0. \end{cases} \end{aligned} \tag{10}$$

First applying (6), then applying (8)–(10), for each $d \in F_p^*$, we obtain that

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

Hence,

$$\begin{aligned} H_0(\underline{\boldsymbol{s}}_k) &= (p^n-1)^2 - (p-1)\left(p^{2n-1} - 2p^{n-1}\right) \\ &= p^{2n-1} - 2p^{n-1} + 1 \end{aligned}$$

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

C. 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 $\underline{\boldsymbol{a}} = (a_0, a_1, \ldots, a_{v-1})$ and $\underline{\boldsymbol{b}} = (b_0, b_1, \ldots, b_{v-1})$ be two vectors of $\mathbb{F}_p^v$. We define

$$\langle \underline{\boldsymbol{a}}, \underline{\boldsymbol{b}} \rangle = \sum_{i=0}^{v-1} \omega^{a_i + b_i} \tag{11}$$

which is an inner product of two complex vectors

$$(\omega^{a_0}, \omega^{a_1}, \ldots, \omega^{a_{v-1}}) \quad \text{and} \quad (\omega^{b_0}, \omega^{b_1}, \ldots, \omega^{b_{v-1}}).$$

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

a) $\langle \underline{\boldsymbol{a}}, \underline{\boldsymbol{b}} \rangle = C_{\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}}(0)$;

b) $\langle \underline{\boldsymbol{a}}, L^\tau(\underline{\boldsymbol{b}}) \rangle = C_{\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}}(\tau)$;

c) $\langle L^i(\underline{\boldsymbol{a}}), L^{j+\tau}(\underline{\boldsymbol{a}}) \rangle = C_{L^i(\underline{\boldsymbol{a}}), L^j(\underline{\boldsymbol{a}})}(\tau) = C_{\underline{\boldsymbol{a}}}(j-i+\tau)$ where $i, j \ge 0$;

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

$$\langle \underline{\boldsymbol{a}} + c, \underline{\boldsymbol{b}} + d \rangle = \omega^{c+d} \langle \underline{\boldsymbol{a}}, \underline{\boldsymbol{b}} \rangle.$$

Proof: Assertions a)–d) are immediate from the definition of the correlation function and (11). □

For a (v, v) interleaved sequence $\underline{\boldsymbol{u}}$ associated with $(\underline{\boldsymbol{a}}, \underline{\boldsymbol{e}})$, in order to conveniently study a cyclic shift of $\underline{\boldsymbol{u}}$, we extend its shift sequence

$$\underline{\boldsymbol{e}} = (e_0, e_1, \ldots, e_{v-1}) \in Z_v^v$$

to

$$(e_0, e_1, \ldots, e_{2v-1}) \in Z_v^{2v}$$

by defining

$$e_{v+j} = 1 + e_j, \qquad 0 \le j < v. \tag{12}$$

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

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

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

Proof: Let $A = (A_0, A_1, \ldots, A_{v-1}) = (a_{i,j})$ be the matrix form of $\underline{\boldsymbol{u}}$. From the definition, $A_j = L^{e_j}\underline{\boldsymbol{a}}$, $0 \le j < v$. Note that the first element in the sequence $L^\tau(\underline{\boldsymbol{u}})$ 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 matrix form:

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

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

$$T_j = L^r(A_{s+j}) = L^r(L^{e_{s+j}}(\underline{\boldsymbol{a}})) = L^{r+e_{s+j}}(\underline{\boldsymbol{a}}). \tag{13}$$

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

$$\begin{aligned} T_j =& L^{r+1}(A_{j-(v-s)}) = L^{r+1}(L^{e_{j-(v-s)}}(\underline{\boldsymbol{a}})) \\ =& L^{r+1+e_{j-(v-s)}}(\underline{\boldsymbol{a}}). \end{aligned} \tag{14}$$

Applying (12)

$$1 + e_{j-(v-s)} = e_{j-(v-s)+v} = e_{s+j}$$

for $v - s \le j < v$. Substituting it into (14), we get that $T_j = L^{r+e_{j+s}}(\underline{\boldsymbol{a}})$ with $v - s \le j < v$. Together with (13), the result follows. □

From Proposition 4 and (6), the following result is immediate.

Lemma 1: For $\underline{\boldsymbol{s}}_k \in S$ and $\tau = rv + s$ with $0 \le s < v$ and $r \ge 0$, the jth column sequence of $L^\tau(\underline{\boldsymbol{s}}_k)$ is given by

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

Remark 4: Let $\underline{\boldsymbol{u}}$ and $\underline{\boldsymbol{w}}$ be two $(v,\,v)$ interleaved sequences over $\mathbb{F}_p$. Let

$$A = (A_0,\, A_1,\, \ldots,\, A_{v-1})$$

and

$$T = (T_0,\, T_1,\, \ldots,\, T_{v-1})$$

be the matrix forms of $\underline{\boldsymbol{u}}$ and $L^\tau(\underline{\boldsymbol{w}})$, respectively, where $\tau \ge 0$. From Proposition 3 b) and Proposition 4, the cross correlation between $\underline{\boldsymbol{u}}$ and $\underline{\boldsymbol{w}}$ can be computed by

$$C_{\underline{\boldsymbol{u}},\,\underline{\boldsymbol{w}}}(\tau) = \sum_{j=0}^{v-1} \langle A_j,\, T_j \rangle. \tag{15}$$

Lemma 2: Let $\underline{\boldsymbol{s}}_h$ and $\underline{\boldsymbol{s}}_k$ 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 $\underline{\boldsymbol{s}}_h$ and $\underline{\boldsymbol{s}}_k$, can be computed by

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

where

$$d_j = b_{h+j} - b_{k+s+j} \tag{16}$$

$$t_j = e_{j+s} - e_j + r. \tag{17}$$

Proof: Let

$$D = (D_0,\, D_1,\, \ldots,\, D_{v-1})$$

and

$$T = (T_0,\, T_1,\, \ldots,\, T_{v-1})$$

be the matrix forms of $\underline{\boldsymbol{s}}_h$ and $L^\tau(\underline{\boldsymbol{s}}_k)$, respectively. According to (15)

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

From (6) and Lemma 1, for $0 \le j < v$, we have

$$\begin{aligned} D_j =& L^{e_j}(\underline{\boldsymbol{a}}) + b_{k+j} \\ T_j =& L^{r+e_{s+j}}(\underline{\boldsymbol{a}}) + b_{k+s+j}. \end{aligned}$$

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

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

where d_j and t_j are defined by (16) and (17). Thus, the assertion follows. □

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

IV. Constructions for $(v^2,\, v,\, 2v+3)$ Signal Sets

In this section, first we will give a criterion for the shift sequence $\underline{\boldsymbol{e}}$ 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 $\underline{\boldsymbol{e}} = (e_0,\, e_1,\, \ldots,\, e_{v-1})$, satisfying the criterion.

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

$$|\{e_j - e_{j+s} | 0 \le j < v - s\}| = v - s, \qquad \text{for all } 1 \le s < v. \tag{18}$$

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 autocorrelation 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 correlation of S is $2v+3$. In this following, we will separate the first two results as two lemmas.

Lemma 3: Let S be constructed by Procedure 1. If the shift sequence $\underline{\boldsymbol{e}} = (e_0,\, e_1,\, \ldots,\, e_{v-1})$ satisfies (18), any pair of sequences in S are shift distinct.

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

$$\underline{\boldsymbol{s}}_h = L^\tau(\underline{\boldsymbol{s}}_k). \tag{19}$$

Let $D = (D_0, D_1, \ldots, D_{v-1})$ and $T = (T_0, T_1, \ldots, T_{v-1})$ be the matrix forms of $\underline{\boldsymbol{s}}_h$ and $L^\tau(\underline{\boldsymbol{s}}_k)$, respectively. We write $\tau = rv+s$ with $0 \le s < v$, $r \ge 0$. Applying (6) and Lemma 2, we have

$$\begin{aligned} D_j &= L^{e_j}(\underline{\boldsymbol{a}}) + b_{h+j}, \qquad 0 \le j < v \\ T_j &= L^{r+e_{s+j}}(\underline{\boldsymbol{a}}) + b_{k+s+j}, \qquad 0 \le j < v. \end{aligned}$$

From (19), we have

$$D_j = T_j, \qquad 0 \le j < v. \tag{20}$$

Next we will show that (20) implies that $h \equiv k+s \mod v$. If not, then there exists some j for which $b_{h+j} = 0$ and $b_{k+s+j} = c \neq 0$. Since $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ are two-level autocorrelation sequences, then two sequences $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ together with their all phase shifts are balanced. Consequently

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

Therefore, $D_j \neq T_j$ for such a j would be a contradiction with (20). Thus, from (20), we derive that

$$h \equiv k + s \mod v. \tag{21}$$

Therefore, $s \neq 0$ since $h \neq k$. Again using (20), we get

$$L^{e_j}(\underline{\boldsymbol{a}}) = L^{r+e_{s+j}}(\underline{\boldsymbol{a}}), \qquad 0 \le j < v. \tag{22}$$

The above identities are true if and only if

$$e_j \equiv r + e_{s+j} \pmod{v}, \qquad 0 \le j < v. \tag{23}$$

Since $(e_0, e_1, \ldots, e_{v-1})$ satisfies the condition (18), then there are at most two j's with $0 \le j < v$ such that the above identities are true, which is a contradiction. Therefore, $\underline{\boldsymbol{s}}_h$ and $\underline{\boldsymbol{s}}_k$ are shift distinct if $h \neq k$. □

Lemma 4: Let S be constructed by Procedure 1. If the shift sequence $\underline{\boldsymbol{e}} = (e_0, e_1, \ldots, e_{v-1})$ satisfies (18), then each sequence in S has period v^2.

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

$$\underline{\boldsymbol{u}} = L^\tau(\underline{\boldsymbol{u}}). \tag{24}$$

Applying a similar argument used in the proof of Lemma 3, we can get (23). If $s \neq 0$, then $\underline{\boldsymbol{e}} = (e_0, e_1, \ldots, e_{v-1})$ satisfies (18). Therefore, there are at most two j's with $0 \le j < v$ satisfying (23), which is a contradiction. Hence, $s = 0 \Longrightarrow \tau = rv$. From (22) with $s = 0$, it follows that each column sequence of $\underline{\boldsymbol{u}}$ has period r. Note that $\mathrm{per}\,(\underline{\boldsymbol{a}}) = v$ and all column sequences of $\underline{\boldsymbol{u}}$ are phase shifts of $\underline{\boldsymbol{a}}$. So, all column sequences of $\underline{\boldsymbol{u}}$ have period v. Thus, $r = v \Longrightarrow \mathrm{per}\,(\underline{\boldsymbol{u}}) = v^2 \Longrightarrow \mathrm{per}\,(\underline{\boldsymbol{s}}_k) = v^2$, which completes the proof. □

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

Property 1: Let $\underline{\boldsymbol{d}} = \{d_i\}$ 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 $\underline{\boldsymbol{d}}$ is balanced, then

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

Proof of Theorem 2: According to Lemma 4, each sequence in S has period v^2. From Lemma 3, 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 $\tau = rv + s$, $0 \le s < v$, $r \ge 0$. For two different sequences $\underline{\boldsymbol{s}}_h$, $\underline{\boldsymbol{s}}_k$ in S, according to Lemma 2, we have

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} \omega^{d_j} C_{\underline{\boldsymbol{a}}}(t_j) \tag{25}$$

where the d_j and t_j are defined in Lemma 2. Since $\underline{\boldsymbol{a}}$ is a two-level autocorrelation sequence, then

$$C_{\underline{\boldsymbol{a}}}(t_j) = \begin{cases} v, & \text{for } t_j \equiv 0 \,(\mathrm{mod}\, v) \\ -1, & \text{for } t_j \not\equiv 0 \,(\mathrm{mod} v). \end{cases}$$

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

$$\underline{\boldsymbol{d}} = L^h(\underline{\boldsymbol{b}}) - L^{k+s}(\underline{\boldsymbol{b}}). \tag{26}$$

Notice that $\underline{\boldsymbol{b}}$ is also a two-level autocorrelation sequence. Therefore, $\underline{\boldsymbol{d}}$ is a balanced sequence if $\underline{\boldsymbol{d}} \neq 0$. Thus,

$$H_0(\underline{\boldsymbol{d}}) = \begin{cases} v, & \text{if } h \equiv k+s \mod v \\ (v+1)/p - 1, & \text{if } h \not\equiv k+s \mod v. \end{cases} \tag{27}$$

Case 1. $s = 0$.

In this case, $t_j = r$ from (17). Since $\underline{\boldsymbol{d}} \neq 0$, from (25) and Property 1, we have

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

which gives that

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

Case 2. $s \neq 0$.

Let N be the number of j with $0 \le j < v$ such that $t_j \equiv 0 \mod v$. Then

$$N = |\{0 \le j < v | e_j - e_{j+s} \equiv r \mod v\}|. \tag{28}$$

Note that r is a constant. Since the shift sequence $\underline{\boldsymbol{e}}$ satisfies (18), then $N \in \{0, 1, 2\}$. Thus, we have the following three cases.

c1) $N = 0$. Thus, $t_j \not\equiv 0$ for all j with $0 \le j < v$ and $C_{\underline{\boldsymbol{a}}}(t_j) = -1$ for all j with $0 \le j < v$.

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

c3) $N = 2$. In this case, there are two j's with $0 \le j < v$ such that $C_{\underline{\boldsymbol{a}}}(t_j) = v$ and for all the other j, $C_{\underline{\boldsymbol{a}}}(t_j) = -1$. 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 subcases.

Case 2.1. $h \equiv k + s \mod v$. In this case, we have $d_j = 0$ for all j. From (25), we have

$$C_{h,k}(\tau) = \sum_{j=0}^{v-1} C_{\underline{\boldsymbol{a}}}(t_j). \tag{29}$$

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

Case 2.2. $h \not\equiv k + s \mod v$. In this case, $\underline{\boldsymbol{d}} \neq 0$. So

$$\sum_{i=0}^{v-1} \omega^{d_i} = -1. \tag{30}$$

For $N = 0$, using (25) and (30), we have

$$C_{h,k}(\tau) = (-1) \sum_{j=0}^{v-1} \omega^{d_j} = (-1)(-1) = 1. \tag{31}$$

For $N = 1$, (25) gives that

$$\begin{aligned} C_{h,k}(\tau) &= \omega^{d_0} v + (-1) \sum_{j=0}^{v-1} \omega^{d_j} + \omega^{d_0} \\ &= \omega^{d_0}(v+1) + 1. \end{aligned} \tag{32}$$

Thus,

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

In particular, if $p = 2$, from (32), we get that $C_{h,k}(\tau) = v + 2$ if $d_0 = 0$ and $C_{h,k}(\tau) = -v$ if $d_0 = 1$.

For $N = 2$

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

Thus,

$$\begin{aligned} |C_{h,k}(\tau)| &= |(\omega^{d_0} + \omega^{d_1})(v+1) + 1| \\ &\le |(\omega^{d_0}(v+1)| + |(\omega^{d_1}(v+1)| + 1 = 2v + 3. \end{aligned}$$

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

Case $C_{k,k}(\tau)$ either belongs to Case 1 where $r \neq 0$, which gives that $C_{k,k}(rv) = 1$, or belongs to Case 2.2. The proof is now completed.

Example 4: We can verify that the shift sequences in Examples 2 and 3 satisfy (18). 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: Let $\underline{\boldsymbol{u}}$ be an (v, v) interleaved sequence associated with $(\underline{\boldsymbol{a}}, \underline{\boldsymbol{e}})$. If the shift sequence of $\underline{\boldsymbol{u}}$ satisfies (18), then the out-of-phase autocorrelation of $\underline{\boldsymbol{u}}$ is three-valued. Precisely, let N be defined by (28), then

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

where $\tau = rv + s$ with $0 \le s < v$ and $r \ge 0$.

Proof: Note that $d_j = 0$, $0 \le j < v$ in this case. From Lemma 2

$$C_{\underline{\boldsymbol{u}}}(\tau) = \sum_{j=0}^{v-1} C_{\underline{\boldsymbol{a}}}(t_j). \tag{33}$$

If $s = 0$, then $t_j = r$ where $r \neq 0$ since $\tau \neq 0$. Thus, $C_{\underline{\boldsymbol{a}}}(t_j) = C_{\underline{\boldsymbol{a}}}(r) = -1$ for all j with $0 \le j < v$. Therefore, $C_{\underline{\boldsymbol{u}}}(\tau) = -v$. If $s \neq 0$, (33) is Case 2.1 in the proof of Theorem 2. Thus, the result is true. □

Remark 5: The author ([17], 1995) introduced the idea of Procedure 1 for constructing $((2^n - 1)^2, 2^n - 1, 1 + 2^{n+1})$ binary signal sets where $v = 2^n - 1$, $\underline{\boldsymbol{a}}$ is a binary m-sequence of period $2^n - 1$, and $\underline{\boldsymbol{b}}$ 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 (18).

(*Note.* For $\underline{\boldsymbol{e}} = (e_0, \ldots, e_{v-1})$, $e_i \in \mathbb{Z}_v$, if $\{e_0, \ldots, e_{v-1}\}$ is a difference triangle set (for its definition, see [6]), then $\underline{\boldsymbol{e}}$ satisfies (18). Thus, theoretically, if there exists a difference triangle set $\{e_0, \ldots, e_{v-1}\}$ for $v = p^n - 1$ or v a prime, then we can construct a $(v^2, v, 2v + 3)$ signal set.)

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

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

$$\beta^{e_j} = \mathrm{Tr}_n^{2n}(\eta\alpha^{j+1}), \qquad 0 \le j < p^n - 1 \tag{34}$$

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

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

1) Choose $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$, two two-level autocorrelation sequences over $\mathbb{F}_2$ with a prime period v constructed in Section II-A.
2) Choose α, a primitive element of $\mathbb{F}_v$.
3) Set

$$e_j = \alpha^j, \qquad 0 \le j < v. \tag{35}$$

Lemma 5: The shift sequence $\underline{\boldsymbol{e}} = (e_0, e_1, \ldots, e_{v-1})$, constructed from Construction A for $v = p^n - 1$ or Construction B for v a prime, satisfies the condition (18) in Theorem 2.

A proof of this Lemma can be found in [17].

Remark 6: Recall that X represents the set of two-level autocorrelation sequences over $\mathbb{F}_p$ constructed by Construction $X \in \{A, B, C.1, C.2, D, E, F, G\}$ in Section II-A.

1) When $p > 2$, we have Construction A for constructing a shift sequence of S and $A \cup B \cup G$ as a domain for choosing two base sequences.
2) When $p = 2$ 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) When $p = 2$ and v is a prime number but v cannot 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) When $p = 2$ 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 $h(x) = x^6 + x + 1$. (Thus, $h(\alpha) = 0$ 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 roots.) 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 $\{e_j\colon 0 \le j < 7\}$ in the following way:

$$\beta^{e_j} = \mathrm{Tr}_3^6(\alpha^{j+1}), \qquad j = 0, 1, \ldots, 6, \eta = 1$$

where $\mathrm{Tr}_3^6(x)$ 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:

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

According to Lemma 5, $\underline{\boldsymbol{e}}$ satisfies (18), 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 $\{e_j\colon 0 \le j < 8\}$ in the following way:

$$\beta^{e_j} = \mathrm{Tr}_2^4(\alpha^6\alpha^{j+1}), \qquad j = 0, 1, \ldots, 7, \eta = \alpha^6$$

where $\mathrm{Tr}_2^4(x)$ 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:

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

According to Lemma 5, $\underline{\boldsymbol{e}}$ satisfies (18). 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 for the case of Remark 6, item 3).

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

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

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 compute $e_j \equiv 2^j \bmod 11$, $0 \le j < 11$. Thus,

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

From $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{e}}$ we can construct the interleaved sequence $\underline{\boldsymbol{u}}$ whose jth column sequence is Ł$^{e_j}(\underline{\boldsymbol{a}})$. The following is the matrix form A of $\underline{\boldsymbol{u}}$:

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

The top row of the matrix B_0 is $\underline{\boldsymbol{b}}$ and the remaining rows are identical to the top row. According to Procedure 1, we have the matrix form of $\underline{\boldsymbol{s}}_0$

$$S_0 = A + B_0 = \begin{bmatrix} 0&0&0&0&1&0&0&1&0&0&0\\ 1&1&0&1&0&1&1&1&0&0&1\\ 0&1&1&0&0&1&0&0&0&0&0\\ 0&1&1&1&0&0&0&1&1&1&0\\ 0&0&1&1&1&1&1&0&1&0&0\\ 1&0&0&0&0&1&0&0&1&1&1\\ 1&0&1&1&1&1&0&1&0&1&1\\ 1&1&0&1&1&0&0&0&1&0&1\\ 0&0&0&1&0&0&1&0&0&1&0\\ 1&1&1&0&1&0&1&0&0&1&1\\ 0&1&0&0&1&1&1&1&1&1&0 \end{bmatrix}.$$

The remaining ten sequences are $A + B_k$, $k = 1, \ldots, 10$ where the top row of B_k is $L_k(\underline{\boldsymbol{b}})$. According to Lemma 5 and Theorem 2, S is a $(121, 11, 25)$ signal set over $\mathbb{F}_2$.

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

1) Let β be a primitive element in $\mathbb{F}_{p^n}$, $f(x) = f_1(x) \cdots f_s(x)$ the minimal polynomial of the base sequence $\underline{\boldsymbol{a}}$ over $\mathbb{F}_p$ where the f_i's are irreducible over $\mathbb{F}_p$, and γ_i a root of $f_i(x)$ in $\mathbb{F}_{p^n}$, where $\gamma_i = \beta^{r_i}$ for which r_i is the smallest integer in the set $\{r_i, pr_i, \ldots, p^{n-1}r_i\}$ modulo $p^n - 1$ and $r_i \le \frac{p^n-1}{2}$ for all $i = 1, \ldots, s$. If $\underline{\boldsymbol{e}}$ is given by Construction A (here $v = p^n - 1$, we suppose that $n > 1$), then the linear span of any sequence $\underline{\boldsymbol{s}}_k$ in S, $0 \le k < v$, is lower-bounded by

$$\mathrm{LS}\,(\underline{\boldsymbol{s}}_k) \ge \frac{p^n - 1}{2}\,\mathrm{LS}\,(\underline{\boldsymbol{a}}) + \mathrm{LS}\,(\underline{\boldsymbol{b}}), \qquad 0 \le k < v$$

and

$$\mathrm{LS}\,(\underline{\boldsymbol{u}}) \ge \frac{p^n - 1}{2}\,\mathrm{LS}\,(\underline{\boldsymbol{a}}).$$

2) Let $f(x) = f_1(x) \cdots f_s(x)$ be the minimal polynomial of the base sequence $\underline{\boldsymbol{a}}$ 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

$$\mathrm{LS}\,(\underline{\boldsymbol{s}}_k) = v\,\mathrm{LS}\,(\underline{\boldsymbol{a}}) + \mathrm{LS}\,(\underline{\boldsymbol{b}}), \qquad 0 \le k < v$$

and

$$\mathrm{LS}\,(\underline{\boldsymbol{u}}) = v\,\mathrm{LS}\,(\underline{\boldsymbol{a}}). \tag{36}$$

3) If $\underline{\boldsymbol{e}}$ 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 (2). In particular, if both $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ 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 $\underline{\boldsymbol{u}}$ associated with $(\underline{\boldsymbol{a}}, \underline{\boldsymbol{e}})$ where the minimal polynomial of $\underline{\boldsymbol{a}}$ is reducible.

In the following, we first investigate some basic properties of the minimal polynomial of $\underline{\boldsymbol{u}}$ and the linear span of the sum of $\underline{\boldsymbol{u}}$ 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 $\underline{\boldsymbol{u}}$ when the shift sequence is given by Construction A. Then we give a proof for Theorem 3.

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

A. 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 $\mathrm{per}\,(s)$ as a period of a sequence s which means that $\mathrm{per}\,(s)$ is the smallest integer such that $s_{t+i} = s_i$, $i = 0, 1, \ldots$, for $s = s_0, s_1, \ldots$ or a period of a polynomial s. This means that $\mathrm{per}\,(s)$ is the smallest integer such that $s(x) | x^t - 1$ for $s = s(x)$.

Fact 1: Let $\underline{\boldsymbol{a}}$ be a sequence over $\mathbb{F}_p$ of period v. Then the minimal polynomial of $\underline{\boldsymbol{a}}$ has no multiple roots if and only if $\gcd(v, p) = 1$. In particular, if v is a prime, then the minimal polynomial of $\underline{\boldsymbol{a}}$ has no multiple roots.

Fact 2: Let $\underline{\boldsymbol{c}} = \underline{\boldsymbol{c}}_1 + \underline{\boldsymbol{c}}_2$ where $\underline{\boldsymbol{c}}_1$ and $\underline{\boldsymbol{c}}_2$ are 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 $\underline{\boldsymbol{c}}_1$ and $\underline{\boldsymbol{c}}_2$ 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 $\underline{\boldsymbol{c}}$;
2) $\mathrm{per}\,(\underline{\boldsymbol{c}}_i) | per(\underline{\boldsymbol{c}})$.
   Moreover, if f_i, $i = 1, 2$ are irreducible then
3) $\mathrm{per}\,(f_i) = \mathrm{per}\,(\underline{\boldsymbol{c}}_i)$, $i = 1, 2$;
4) $\mathrm{per}\,(f) = \mathrm{lcm}\{\mathrm{per}\,(f_1), \mathrm{per}\,(f_2)\}$;
5) $\mathrm{per}\,(f) = \mathrm{per}\,(\underline{\boldsymbol{c}})$.

Fact 2 can be generalized to the case that $\underline{\boldsymbol{c}}$ is a sum of any $s \ge 1$ sequences over $\mathbb{F}_p$. (For a proof, see [23], [18].)

Fact 3: Let $\underline{\boldsymbol{c}}$ be any nonzero 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 $\underline{\boldsymbol{c}}$ over $\mathbb{F}_p$ where the g_j is irreducible over $\mathbb{F}_p$. Then $\underline{\boldsymbol{c}}$ can be decomposed into

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

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

This result directly follows the trace representation in Section I-E. The following result comes from [37, Theorem 3.35].

Fact 4: Let $f_1(x), \ldots, f_N(x)$ be all the distinct monic irreducible polynomial over $\mathbb{F}_p$ of degree n and period r; let $t \ge 2$ be an integer of prime factors that divide r but not $(p^n - 1)/r$. Assume that $p^n \equiv 1 \bmod 4$ if $t \equiv 0 \bmod 4$. Then, $f_1(x^t), \ldots, f_N(x^t)$ are all the distinct monics irreducible over $\mathbb{F}_p$ of degree nt and period rt.

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 m such that $v | p^m - 1$. Let $f(x)$ be the minimal polynomial of $\underline{\boldsymbol{a}}$. If $f(x)$ is primitive, then $v = p^n - 1$, and the minimal polynomial of $\underline{\boldsymbol{u}}$ is equal to $f(x^v)$, which is still irreducible over $\mathbb{F}_p$ from Fact 4. If $f(x) = f_1(x) \cdots f_s(x)$, where the $f_i(x)$'s are distinct irreducible polynomials over $\mathbb{F}_p$ of degree n_i, then $n_i | n$ if $v = p^n - 1$ and $n_i = m$ if v is prime. From Fact 3, $\underline{\boldsymbol{a}}$ can be decomposed as

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

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

$$A_j = L^{e_j}(\underline{\boldsymbol{a}}) = L^{e_j}\left(\sum_{k=1}^{s} \underline{\boldsymbol{a}}_k\right) = \sum_{k=1}^{s} L^{e_j}(\underline{\boldsymbol{a}}_k), \qquad 0 \le j < v. \tag{37}$$

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

$$\underline{\boldsymbol{u}} = \underline{\boldsymbol{u}}_1 + \cdots + \underline{\boldsymbol{u}}_s \tag{38}$$

where $\underline{\boldsymbol{u}}_i$ is a (v, v) interleaved sequence associated with $(\underline{\boldsymbol{a}}_i, \underline{\boldsymbol{e}})$. Thus, the minimal polynomial of $\underline{\boldsymbol{u}}_i$, say $h_i(x)$, divides $f_i(x^v)$, $1 \le i \le s$. Together with Fact 4 and Fact 2, item 1), the following result is immediate.

Lemma 6: With the above notation, if for each i: $1 \le i \le s$, f_i has the same period v, then $h_i(x) = f_i(x^v)$ which is irreducible over $\mathbb{F}_p$. In other words, the minimal polynomial of $\underline{\boldsymbol{u}}_i$ is $f_i(x^v)$. Thus, the minimal polynomial of $\underline{\boldsymbol{u}}$ is $f(x^v) = f_1(x^v) \cdots f_s(x^v)$. In particular, if v is prime, then the minimal polynomial of $\underline{\boldsymbol{u}}$ is $f(x^v)$.

From Lemma 6, if for each i: $1 \le i \le s$, $\mathrm{per}\,(f_i) = v$, 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 $\underline{\boldsymbol{u}}$ without the imposed condition for $f_i(x)$. In other words, we want to establish the following assertion.

Theorem 4: We keep the above notation

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

In other words, the minimal polynomials, $h_i(x)$, $1 \leq i \leq s$, of the $\underline{\boldsymbol{u}}_i$'s are pairwise relatively prime. Therefore, $h(x) = \prod_{i=1}^{s} h_i(x)$.

From Lemma 6, if v is prime, then the result is true. Thus, it suffices to consider the case that there is some i such that $\mathrm{per}\,(f_i) < v$ (note that $\mathrm{per}\,(f_i)|v$) where $v = p^n - 1$. We need several lemmas for this purpose. Henceforth, we will sometimes use the notation $q = p^n$.

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 $n_i|n$ [37]. Let $\underline{\boldsymbol{a}}_i = \{a_{i,t}\}$ have the following trace representation (see Section I):

$$a_{i,t} = \mathrm{Tr}_1^{n_i}(\eta_i \gamma_i^t), \qquad 0 \neq \eta_i \in \mathbb{F}_{p^{n_i}},\, t = 0, 1, \ldots. \quad (39)$$

From (38), the elements of $\underline{\boldsymbol{u}}_i = \{u_{i,t}\}$ can be represented as

$$u_{i,kv+j} = \mathrm{Tr}_1^{n_i}(\eta_i \gamma_i^{k+e_j}), \qquad 0 \leq j < v,\, k \geq 0. \quad (40)$$

Let

$$\rho_{i,kv+j} = \eta_i \gamma_i^{k+e_j}, \qquad 0 \leq j < v,\, k \geq 0 \quad (41)$$

and $\Pi_i = \{\rho_{i,t}\}_{t \geq 0}$, $1 \leq i \leq s$. Note that Π_i is a sequence over $\mathbb{F}_q$. We then have

$$u_{i,t} = \mathrm{Tr}_1^{n_i}(\rho_{i,t}), \qquad t = 0, 1, \ldots. \quad (42)$$

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

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

$\sigma_i(\varphi(x))$ is said to be the *conjugate* of $\varphi(x)$ with respect to p. We have the following result the proof of which can be found in [28].

Proposition 5: With the above notation. Then

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

Property 2: Let $\varphi_i(x) = x^v - \gamma_i$. Then

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

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

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

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. □

Proof of Theorem 4: For $v = p^n - 1$, note that $\varphi_i(x)$ is a characteristic polynomial of Π_i over $\mathbb{F}_q$. Thus, $g_i(x)|\varphi_i(x)$. Since σ^k restricted on $\mathbb{F}_q$ is an automorphism of $\mathbb{F}_q$, applying Property 2, we have $\gcd(g_i, \sigma^k(g_j)) = 1$ for $i \neq j$ and $k = 0, 1, \ldots, n-1$. From Proposition 5, $h_i(x)$ is the product of $\sigma^k(g_i)$, $k = 0, 1, \ldots, n_i - 1$. Consequently

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

Together with Lemma 6, the proof is completed.

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

$$\mathrm{LS}\,(\underline{\boldsymbol{u}}) = \sum_{i=1}^{s} \deg(f_i)\deg(g_i).$$

Proof: Since $\mathrm{LS}\,(\underline{\boldsymbol{u}}) = \deg(h)$, the result follows from Theorem 4 and Proposition 5. □

Lemma 7: With the above notation, assume that $f(x)$, the minimal polynomial of $\underline{\boldsymbol{a}}$, is an irreducible polynomial over $\mathbb{F}_p$ of degree n and period $s < p^n - 1$. Let $v = p^n - 1$, $n > 1$. Then the period of each irreducible factor of $h(x)$, the minimal polynomial of $\underline{\boldsymbol{u}}$, is not a divisor of v.

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

$$A_j = L^{e_j}(\underline{\boldsymbol{a}}) \neq 0, \qquad 0 \leq j < v,\, e_j \in \mathbb{Z}_v \quad (43)$$

where the minimal polynomial of each column sequence of $\underline{\boldsymbol{u}}$ 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, $\mathrm{per}\,(d)|v$, and $\gcd(d(x), H(x)) = 1$. Therefore, $\underline{\boldsymbol{u}}$ can be decomposed as

$$\underline{\boldsymbol{u}} = \underline{\boldsymbol{c}} + \underline{\boldsymbol{z}} \quad (44)$$

where the minimal polynomials of $\underline{\boldsymbol{c}}$ and $\underline{\boldsymbol{z}}$ are $d(x)$ and $H(x)$, respectively. From Fact 2 item 3), the period of $\underline{\boldsymbol{c}}$ is equal to the period of $d(x)$, which is a factor of v. Thus, the jth column sequence A_j of $\underline{\boldsymbol{u}}$ can be written as $A_j = c_j + \underline{\boldsymbol{z}}_j$. Since $0 \neq \underline{\boldsymbol{c}} = \{c_j\}$, there exists some j such that $c_j \neq 0$ which contradicts (43). Therefore, there are no irreducible factors of $h(x)$ whose period is a divisor of v. □

Note that Lemma 7 has established the following result. Assume that $f(x)$ is an irreducible polynomial over $\mathbb{F}_p$ of degree n with period $s < p^n - 1$. Then the period of any irreducible factor of $f(x^v)$, where $v = p^n - 1$, is not a divisor of v.

Theorem 5: Let $\underline{\boldsymbol{u}}$ be a (v, v) interleaved sequence over $\mathbb{F}_p$ of period v^2 associated with $(\underline{\boldsymbol{a}}, \underline{\boldsymbol{e}})$ where v is prime or $v = p^n - 1$ and $\underline{\boldsymbol{e}} \in \mathbb{Z}_v^v$, $\underline{\boldsymbol{b}}$ a sequence over $\mathbb{F}_p$ of period v and $\underline{\boldsymbol{c}} = \underline{\boldsymbol{u}} + \underline{\boldsymbol{b}}$. Let $h(x)$, $t(x)$, and $g(x)$ be the minimal polynomials of $\underline{\boldsymbol{u}}$, $\underline{\boldsymbol{b}}$, and $\underline{\boldsymbol{c}}$, respectively. If each irreducible factor of the minimal polynomial of $\underline{\boldsymbol{a}}$ has degree greater than 1, then

1) $\gcd(h(x), t(x)) = 1$, so that $g(x) = h(x)t(x)$;

2) the linear span of $\underline{\boldsymbol{c}}$ is given by $\mathrm{LS}\,(\underline{\boldsymbol{c}}) = \mathrm{LS}\,(\underline{\boldsymbol{u}}) + \mathrm{LS}\,(\underline{\boldsymbol{b}})$.

Proof: With the same $\underline{\boldsymbol{u}}_i$, $h_i(x)$ as in Theorem 4. According to Theorem 4, $h_i(x)$'s, the minimal polynomials of $\underline{\boldsymbol{u}}_i$, 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 6, $h_i(x) = f_i(x^v)$ 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 greater degree than v. Since $\underline{\boldsymbol{b}}$ has period v, then $\deg(t(x)) < v$. Therefore, any irreducible factor of $t(x)$ has degree less than v. So $\gcd(f(x^v), t(x)) = 1$ which gives the first assertion. From Fact 2, item1), $g(x) = h(x)t(x)$. Therefore,

$$\begin{aligned}\mathrm{LS}\,(\underline{\boldsymbol{u}} + \underline{\boldsymbol{b}}) &= \deg(f(x^v)t(x)) \\ &= \deg(f(x^v)) + \deg(t(x)) \\ &= v\deg(f(x)) + \deg(t(x) \\ &= v\,\mathrm{LS}\,(\underline{\boldsymbol{a}}) + \mathrm{LS}\,(\underline{\boldsymbol{b}})).\end{aligned}$$

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

If $f_i(x)$ is primitive, from Lemma 6, $h_i(x) = f_i(x^v)$, which is irreducible. By using similar argument to that 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. In this case, applying Lemma 7, any irreducible factor of $h_i(x)$ has period which is not a factor of v. On the other hand, $\underline{\boldsymbol{b}}$ is a sequence over $\mathbb{F}_p$ of period $p^n - 1$. Thus, any irreducible factor of $t(x)$ has period which divides v. Hence,

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

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

We have now established Assertion 2 and the first part of Assertion 3 in Theorem 3.

B. A Lower Bound for the Linear Span of $\underline{\boldsymbol{u}}$

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 latter is called an *irreducible interleaved sequence* in [17] by the author. In [17], 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 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 IV.

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

$$u_i = \mathrm{Tr}_1^n(\rho_i), \qquad i = 0, 1, \ldots \tag{45}$$

where

$$\rho_{kv+j} = \zeta\gamma^{e_j}\gamma^k, \qquad 0 \le j < v,\, k \ge 0,\, \zeta \in \mathbb{F}_q \tag{46}$$

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

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

$$\mathrm{LS}\,(\underline{\boldsymbol{u}}) = \mathrm{LS}\,(\underline{\boldsymbol{a}})\mathrm{LS}\,(\Pi) = n\,\mathrm{LS}\,(\Pi). \tag{47}$$

Therefore, in order to establish a lower bound for the linear span of the irreducible interleaved sequence $\underline{\boldsymbol{u}}$, it suffices to find a lower bound for the linear span of the sequence Π over $\mathbb{F}_q$, defined by (46). In the following, we will assume that the shift sequence $\underline{\boldsymbol{e}}$ of $\underline{\boldsymbol{u}}$ is given by Construction A. Under this assumption, we have the following relation:

$$\beta^{e_j} = \mathrm{Tr}_n^{2n}(\eta\alpha^{j+1}), \qquad 0 \le j < v,\ \mathrm{Tr}_n^{2n}(\eta) = 0,\ \eta \in F_{q^2} \tag{48}$$

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

$$\gamma = \beta^r. \tag{49}$$

Substituting (49) into (46), we get

$$\rho_{kv+j} = \zeta\beta^{re_j}\gamma^k, \qquad 0 \le j < v,\, k \ge 0. \tag{50}$$

Let

$$\theta_j = \mathrm{Tr}_n^{2n}(\eta\alpha^{j+1}), \qquad j = 0, 1, \ldots \tag{51}$$

where η is the same as in (48). Let $\Theta = \{\theta_j\}$. Then Θ is an m-sequence over $\mathbb{F}_q$ of degree 2. Together with (48)–(50), we have

$$\rho_{kv+j} = \zeta\theta_j^r\gamma^k, \qquad 0 \le j < v,\, k \ge 0. \tag{52}$$

If $\gcd(r, v) = 1$, then $f(x)$ is primitive. Thus, $h(x) = f(x^v)$. Therefore, $\mathrm{LS}\,(\underline{\boldsymbol{u}}) = vn$. 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 $\Theta^r = \{\theta_j^r\}_{j \ge 0}$ 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 mid 1980s [23]. From his work, we have the following result.

Proposition 6: With the above notation, let

$$r = r_0 + r_1 p + \cdots + r_{n-1}p^{n-1}, \qquad 0 \le r_i < p.$$

Then $\mathrm{LS}\,(\Theta^r)$, the linear span of Θ^r, is given by

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

Lemma 8: With the same Θ as above, let $0 < r \le \frac{p^n-1}{2}$. Then $\mathrm{LS}\,(\Theta^r)$, the linear span of Θ^r, is bounded by

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

Proof: Note that

$$r \le \frac{p^n-1}{2}. \tag{53}$$

We write

$$r = r_0 + r_1 p + \cdots + r_{n-1}p^{n-1}, \qquad 0 \le r_i < p.$$

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 to (53). So, $r_{n-1} < p-1$. Applying Proposition 6, the maximal value of $\mathrm{LS}\,(\Theta^r)$ can only be achieved for such r's where $r_i = p-1$, $i = 0, 1, \ldots, p-2$, and $r_{n-1} < p-1$. Thus, we have

$$\mathrm{LS}\,(\Theta^r) = p^{n-1}(r_{n-1}+1) \tag{54}$$

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

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

which is a contradiction to (53). Therefore, $r_{n-1} \le \frac{p-1}{2} - 1$. Substituting this into (54), we get

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

which establishes the assertion. □

We list the following properties on linear span profiles the proofs of which can be found in [40].

Proposition 7: 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 $c_0, c_1, \ldots, c_i$ for $i \ge 0$ where $l_i = \deg(d_i)$. Then

1) $d_i = d(x)$ and $l_i = l$, for all $i \ge 2l$;
2) $l_0 \le l_1 \le l_2 \cdots \le l_i \le \cdots$.

In the following, we will use the Berlekamp–Massey algorithm (see [40] or [18, Ch. 6]) to establish a lower bound of the linear span of Π.

Lemma 9: 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 $r \le \frac{p^n-1}{2}$. Let $\Pi = \{\rho_i\}$ be a sequence over $\mathbb{F}_q$ whose elements are given by

$$\rho_{kv+j} = \theta_j^r \gamma^k, \qquad v = q-1,\ i = kv + j$$

where

$$0 \le j < v, \quad k \ge 0.$$

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

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

Proof: From the assumption, we have

$$\rho_j = \theta_j^r, \qquad j = 0, 1, \ldots, v-1 = p^n - 2. \tag{55}$$

Let $d(x)$ be the minimal polynomial of $\Theta^r = \theta_0^r, \theta_1^r, \ldots$ and let $l = \deg(d(x))$. Assume that $d_i(x)$ is the polynomial computed by the Berlekamp–Massey algorithm which generates the sequence $\rho_0, \rho_1, \ldots, \rho_i$ and $l_i = \deg(d_i)$, $i \ge 0$. From (55), we get that d_i is the same polynomial computed by the Berlekamp–Massey algorithm, which generates the sequence $\theta_0^r, \theta_1^r, \ldots, \theta_i^r$ for $i = 0, 1, \ldots, p^n - 2$. Note that from Lemma 8, we have $l = \mathrm{LS}\,(\Theta^r) < \frac{p^n-1}{2}$. So $2l < p^n - 1$. Applying Proposition 7, item 1)

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

Note that from (51) that $\theta_{v+1} = 0 \Longrightarrow \theta_{v+1}^v = 0$. But from (50), $\rho_{v+1} = \zeta\theta_1\gamma \ne 0$. So $d_{v-1}(x) = d(x)$ cannot generate $\rho_0, \rho_1, \ldots, \rho_{v+1}$. There are two cases that may happen.

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

From Lemma 8, we have

$$2l_j = 2l < p^n - 1 = v \tag{56}$$

where $j = v-1$ in the first case and $j = v$ in case 2. 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 $0 \le m < v$, $l_m < l$, $b = j + 1 - l$ and $a < l$. Whenever $j = v-1$ or $j = v$, we have

$$\begin{aligned} l_{j+1} &= \deg(d_{j+1}) = b - a + l = j + 1 - l - a + l \\ &= j + 1 - a > j + 1 - l > v - \frac{p^n-1}{2} = \frac{p^n-1}{2}. \end{aligned}$$

Therefore, $\mathrm{LS}\,(\rho) \ge l_{j+1} > \frac{p^n-1}{2}$, which completes the proof. □

Lemma 10: Let β be a primitive element in $\mathbb{F}_{p^n}$, $f(x) = f_1(x)\cdots f_s(x)$ where the f_i's are irreducible over $\mathbb{F}_p$, and γ_i is a root of $f_i(x)$ in $\mathbb{F}_{p^n}$ where $\gamma_i = \beta^{r_i}$, for which r_i is the smallest integer in the set $\{r_1, pr_i, \ldots, p^{n-1}r_i\}$ modulo $p^n - 1$ and $r_i \le \frac{p^n-1}{2}$ for all $i = 1, \ldots, s$. Let $\underline{\mathbf{a}} = \underline{\mathbf{a}}_1 + \cdots + \underline{\mathbf{a}}_s$ be a two-level autocorrelation 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

$$\mathrm{LS}\,(\underline{\mathbf{u}}_i) > \deg(f_i)\,\frac{p^n-1}{2}$$

and

$$\mathrm{LS}\,(\underline{\mathbf{u}}) > \frac{p^n-1}{2}\,\mathrm{LS}\,(\underline{\mathbf{a}}).$$

Proof: We use the same notation as in Section V-A. Since $\underline{\mathbf{a}}$ is a two-level autocorrelation sequence, without loss of generality, we can set $\eta_i = 1$, $1 \le i \le s$ in (39), the trace representation of $\underline{\mathbf{a}}$. Consequently, for each i: $1 \le i \le s$, the elements of

Π_i have a representation of (52) 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 9. Therefore, we have

$$\deg(g_i) = \mathrm{LS}\,(\Pi_i) > \frac{p^n - 1}{2}, \qquad 1 \le i \le s. \tag{57}$$

Applying Proposition 5, we get

$$\mathrm{LS}\,(\underline{\boldsymbol{u}}_i) = \deg(h_i(x)) = \deg(f_i)\deg(g_i) \overset{(57)}{>} \deg(f_i)\,\frac{p^n - 1}{2}$$

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

$$\begin{aligned}\mathrm{LS}\,(\underline{\boldsymbol{u}}) &= \sum_{i=1}^{s} \mathrm{LS}\,(\underline{\boldsymbol{u}}_i) > \sum_{i=1}^{s} \deg(f_i)\,\frac{p^n - 1}{2} \\ &= \frac{p^n - 1}{2} \sum_{i=1}^{s} \deg(f_i) = \frac{p^n - 1}{2}\,\mathrm{LS}\,(\underline{\boldsymbol{a}})\end{aligned}$$

where the last identity comes from

$$\sum_{i=1}^{s} \deg(f_i) = \deg(f) = \mathrm{LS}\,(\underline{\boldsymbol{a}}).$$

□

Corollary 4: Let $v = p^n - 1$. Let $\underline{\boldsymbol{u}}$ be a (v, v) interleaved sequence associated with $(\underline{\boldsymbol{a}}, \underline{\boldsymbol{e}})$, where $\underline{\boldsymbol{a}}$ is a sequence over $\mathbb{F}_p$ of period v whose minimal polynomial satisfies the condition of Lemma 10, and $\underline{\boldsymbol{e}}$ is given by Construction A. Let $\underline{\boldsymbol{b}}$ be a sequence over $\mathbb{F}_p$ of period v. Let $\underline{\boldsymbol{c}} = \underline{\boldsymbol{u}} + \underline{\boldsymbol{b}}$. Then $\mathrm{LS}\,(\underline{\boldsymbol{c}})$, the linear span of $\underline{\boldsymbol{c}}$, is bounded by

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

Proof: This follows directly from Theorem 5 and Lemma 10. □

In the next subsection, we will use Corollary 4 for proof of Assertion 1 in Theorem 3, and Lemma 6 and Theorem 5 for Assertions 2 and 3 in Theorem 3.

C. Proof of Theorem 3

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

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

1) Since all shifts of $\underline{\boldsymbol{b}}$ have the minimal polynomial, then the result directly follows from Corollary 4.

2) If $\mathrm{per}\,(f_i) = v$, according to Lemma 6, the minimal polynomial of $\underline{\boldsymbol{u}}$ is $f(x^v)$. Applying Theorem 5, the minimal polynomial of $\underline{\boldsymbol{s}}_k$ is equal to $f(x^v)t(x)$ where $t(x)$ is the minimal polynomial of $\underline{\boldsymbol{b}}$. Thus, the result follows.

3) The first assertion follows from Lemma 6 and Theorem 5 immediately.

For the second assertion, if $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ are both quadratic sequences, according to [19], we have

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

Applying Theorem 5

$$\begin{aligned}\mathrm{LS},(s_k) &= v\,\mathrm{LS}\,(\underline{\boldsymbol{a}}) + \underline{\boldsymbol{b}} = v\,\frac{v - 1}{2} + \frac{v - 1}{2} \\ &= \frac{(v+1)(v-1)}{2} = \frac{v^2 - 1}{2}.\end{aligned}$$

Note that the result on linear spans of two-level autocorrelation sequences of period $2^n - 1$ which were developed by the author and Golomb in [19] 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 two-level autocorrelation function. Therefore, if v is prime, then each sequence in a $(v^2, v, 2v + 3)$ signal set achieves the maximal linear span.

Before we move to the next section, we would like to point out the representation of the interleaved sequence $\underline{\boldsymbol{u}}$ associated with $(\underline{\boldsymbol{a}}, \underline{\boldsymbol{e}})$ that we frequently used in this section for the purpose of implementation. Let $g(x)$ be the trace representation of $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{e}}$, constructed by Construction A. According to the discussions of (45)–(52) in Section V-B, any element of $\underline{\boldsymbol{u}} = \{u_i\}$ is given by

$$u_{iv+j} = g\left(\mathrm{Tr}_n^{2n}(\alpha^{j+1})\gamma^i\right), \qquad 0 \le j < v,\ i \ge 0. \tag{58}$$

Here, we set $\eta = 1$. Since $\gamma^i \in \mathbb{F}_q$, the above identity becomes

$$u_{iv+j} = g\left(\mathrm{Tr}_n^{2n}(\gamma^i\alpha^{j+1})\right), \qquad 0 \le j < v,\ i \ge 0.$$

Then

$$\begin{aligned}u_{iv+j} &= g\left(\mathrm{Tr}_n^{2n}(\alpha^{di+j+1})\right) \\ g &= \left(\mathrm{Tr}_n^{2n}(\alpha\alpha^k)^r\right),\ k = id + j,\ 0 \le j < v,\ i \ge 0.\end{aligned}$$

Let $f(x) = g(x) \circ \mathrm{Tr}_n^{2n}(\alpha x)$ and $v_i = f(\alpha^i)$, $i = 0, 1, \ldots$. According to Proposition 1, $\{v_i\}$ is a generalized GMW sequence. Thus, it has two-level autocorrelation. Under this assumption, $\{u_i\}$ is shrunk from $\{v_i\}$ in the following way:

$$u_{iv+j} = v_{id+j}, \qquad 0 \le j < v,\ i \ge 0. \tag{59}$$

In other words, the matrix form of $\{u_i\}$ is made from the first v columns of the matrix form of $\{v_i\}$ when it is considered as a (v, d) interleaved sequence.

VI. An Architecture for Implementation and Comparisons With the Known Designs

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

A. Implementation

1) *For Small Fields:* $v \le 2^{40}$: In this case, for both Constructions A and B, we have efficient implementation for all interleaved signal sets by means of either pre-storage of the shift sequence $\underline{\boldsymbol{e}}$ or the two-level autocorrelation sequences $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$. If $v = p^n - 1$, from (58) at the end of Section V-C, we can also efficiently implement it in finite field circuits.

2) *For Large Fields:* $v > 2^{40}$: For Construction A, from (59), the interleaved signal sets, which are constructed from shrunk generalized GMW, can be implemented by an LFSR over $\mathbb{F}_{p^n}$ of

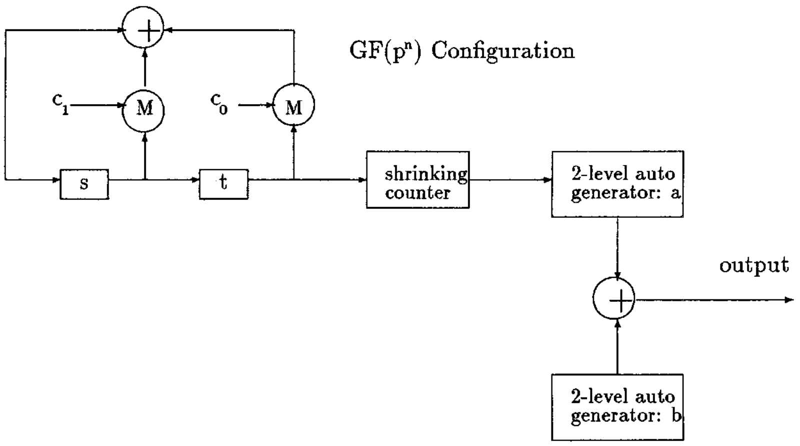

Fig. 1. Galois configuration of $((p^n - 1)^2, p^n, 1 + 2p^n)$ signal sets.

TABLE I
PROFILE OF $(v^2, v, 2v + 3)$ SIGNAL SET S

Period (or length of code): v^2 The number of members in S: v The maximal correlation: $2v + 3$ Each sequence in S is balanced		
	Linear Span	Having Efficient Implementation
$v = p^n - 1$ for both binary and nonbinary	$\geq \frac{p^n-1}{2} LS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}})$ where $\underline{\mathbf{e}}$ from Construction A, or $= (p^n - 1)LS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}})$ where $\underline{\mathbf{a}}$ is a sum of m-sequences	(i) $p^n \leq 2^{40}$, or (ii) $\underline{\mathbf{u}}$ is a shrunk GMW: Fig. 1, $\underline{\mathbf{a}}, \underline{\mathbf{b}} \in A \cup B_0 \cup D$
v prime, binary	$vLS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}})$	$v \leq 2^{40}$

order 2 and two two-level autocorrelation sequence generators together with a *shrinking counter* which deletes two consecutive outputs of the LFSR at each v interval clock cycles. See Fig. 1.

In Fig. 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 depends only on the complexity of these two two-level autocorrelation sequence generators. If we take two base sequences $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ from $A \cup B_0 \cup D$ in Section II-A, then the resulting signal sets can be efficiently implemented in both hardware and software. In general, the cost of implementation of the new signal sets is roughly the same as that of generalized Kasami sets or the bent function sequence sets, since both these signal sets also utilize finite field computations.

For Construction B, which generates $(v^2, v, 2v + 3)$ signal sets where v is prime, it can be implemented by employing a division circuit, see [17].

Up to now, we have shown all properties of families of the sequences constructed by the interleaved design. We summarize these features in the Table I in order to provide guidance of applications of these sequences in practice. (*Note:* In code-division multiple access (CDMA) applications, the code length is much shorter than 2^{20}.)

B. Comparisons

In the Tables II and III, we give profiles for the new designs in comparison with the known designs in the Galois field configuration.

* If $g(x)$ is taken from either Construction D or F in Section II-A, then it may have large linear span for some particular $g(x)$.

** In [36], Kumar presented an example of the bent sequence family with period p^4 and linear span on the order of p^3. In general, they can be made similarly to have large linear span.

We have the following advantages of the new design.

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

For the binary case, among the previously known constructions, only the generalized Kasami designs can utilize all two-level sequences of period $2^n - 1$ (see Section II-B). According to the Welch bound [56], the correlation of signal sets constructed from both the generalized Kasami design and the new design are optimal. However, from Table I, the new design has the following better aspects in comparison with the generalized Kasami design.

1) *Linear Span*
For the new design, the two-level autocorrelation sequence $\underline{\boldsymbol{a}}$ having linear span n can only happen when $\underline{\boldsymbol{a}}$ is chosen as an m-sequence. For other cases, the linear span of $\underline{\boldsymbol{a}}$ is greater than n. So the linear span of $\underline{\boldsymbol{a}}$ 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.

TABLE II
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	$4n+2^*$	$[1, 1+2^{n+1}]$
Boztas *et al.*	$(2^{2n+1}-1, 1+2^{2n+1}, 1+\sqrt{2}2^n)$	$n(2n+3)$	1 (for some n)
Kasami	$(2^{2n}-1, 2^n, 1+2^n)$	$3n$	$[1, 1+2^n]$
Gen. Kasami (No *et al.*)	$(2^{2n}-1, 2^n, 1+2^n)$	$\geq n^2$ $\leq n(2^n-1)$	$[1, 1+2^n]$
Kerdock	$(2^{2n}-1, 2^{2n-1}, 1+2^n)$	$n(2n+1)$	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)	$(p^2, p+1, 2p+3)$ (p prime)	$(p^2-1)/2$	1

TABLE III
COMPARISON WITH THE KNOWN DESIGNS: NONBINARY CASE

Construction	(N, r, δ) Signal Set	Linear Span	Balance ?
Gold Pair	$(p^{2n+1}-1, 1+p^{2n+1}, 1+pp^n)$ (Trachtenberg [55])	$4n+2$	No
	$(p^{2n}-1, p^{2n}, 2p^n-1)$ (Helleseth [24])	$4n$	No
	$(p^n-1, p^n, 1+\sqrt{p^n})$ (Sidelnikov [52], Kumar, *et al.* [34])	$2n$	No
Bent [35] (Kumar. *et al.*)	$(p^{2n}-1, p^n, 1+p^n)$	Large**	Yes
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

TABLE IV
$n = 5$

Constructions	(v, r, δ) Signal Set	Linear Span	Number of Balanced Seq.	Total Number of Sets
Kasami	$(1023, 32, 33)$	15	0	$1 \times 60 = 60$
Gen. Kasami (No *et al.*)	$(1023, 32, 33)$	$\geq 25, \leq 155$	0	$8 \times 60 = 480$
New Design (Interleave)	$(961, 31, 65)$	$\{160, 480\}$	31	$64 \times 8 \times 60$ $= 512 \times 60$ $= 30720$

2) *The Number of Different Signal Sets*
Let N_g be the number of different two-level autocorrelation functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. According to Proposition 2 in Section I, 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 two-level autocorrelation 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 Construction 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 sets 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 sets is $N(\underline{\mathbf{e}}_B)N_q$ times as many as the number of $(2^{2n} - 1, 2^n, 1 + 2^n)$ signal sets 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 generalized 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.

Remark 7: The maximal correlation of the binary interleaved signal set is not as good as the Kasami or the generalized Kasami set. This is a tradeoff between correlation and the other randomness properties. For the interleaved design, we sacrifice correlation to trade for the balance property and a much larger linear span. This is not the first example for doing so. Z_4 code [33] is such an example. The maximal correlation of Z_4 codes is not as good as the Gold sequences, but they have tremendously huge family sizes compared with those of Gold families. In practice, the type of performance required determines the appropriate design to be used.

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

Example 7: Let $v = 2^5 - 1 = 31$ (see Table IV).

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 $\frac{\phi(2^{2\times5}-1)}{2\times5} = 60$, which is

TABLE V
SIGNAL SETS WITH THE BALANCE PROPERTY
($\underline{\boldsymbol{a}}$ AND $\underline{\boldsymbol{b}}$ 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

TABLE VI
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 = 320
Kumar *et al.*	(6560, 6561, 82)	16	81	7 × 320 = 2240
New Sets	(6400, 80, 163)	$\{164, 172, 484, 492\}$	80	256 × 320 = 81920

the number of shift-distinct shift sequences by Constructions A, $N(\underline{\boldsymbol{e}}_B) = 8$, the number of shift-distinct shift sequences by Constructions B, and $N_g = 8$, the number of shift-distinct binary two-level autocorrelation sequences of period 31.

Case 2. Binary Signal Sets With Period v^2 Where v is prime

The new design for $(v^2, v, 2v+3)$ signal sets where $p = 2$ and v is prime are completely new sets. In this case, the shift sequences are obtained from Construction B, and two base sequences can be chosen from the set consisting of quadratic sequences and the Hall sextic sequences. (Note that when v is prime, according to Section II-A-C), there are only three constructions to construct a binary sequence with two-level autocorrelation. 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.

Case 3. Nonbinary Signal Sets

For nonbinary cases, the new design provides a variety of

$$((p^n - 1)^2, p^n - 1, 1 + 2p^n)$$

signal sets whose cross correlations are optimal with respect to the Welch bound. Note that for the Gold-pair construction, there are only few choices for r in $g(x) = \mathrm{Tr}_1^n(x^r)$ defined by Construction A.1 in Section II-B. 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* (see Table V) if each sequence in the set is balanced. Otherwise, it is said to be *unbalanced*.) Table VI lists a profile of the new design for $p = 3$ and $n = 4$ in comparison with the signal sets with the closest length.

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

C. A Complete Design Process

In the following we will give an example to show a complete process for the 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 V, there are 256 × 320 = 81 920 different such signal sets.) Let $p = 3$ and $n = 4$. Then $v = 3^4 - 1 = 80 \Longrightarrow v^2 = 6400$. We will give a design $\underline{\boldsymbol{u}}$ which is shrunk from the GMW sequences with length 3.

1) *Select two base sequences $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$*: Since $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ can be taken from the set, say Ω, consisting of all two-level autocorrelation sequences of period $3^4 - 1 = 80$ over $\mathbb{F}_3$. From Section II-A, we know that Ω consists of m-sequences of period 80 of degree 4, the GMW sequences, and some sequences from the miscellaneous construction G. We choose $\underline{\boldsymbol{a}} = \{a_i\}$ and $\underline{\boldsymbol{b}} = \{b_i\}$ as two GMW sequences whose elements are given by

$$a_i = \mathrm{Tr}_1^2\left(\mathrm{Tr}_2^4(\beta^i)^5\right), \qquad i = 0, 1, \ldots$$

and

$$b_i = \mathrm{Tr}_1^2\left(\mathrm{Tr}_2^4(\beta^{7i})^5\right), \qquad i = 0, 1, \ldots$$

where β is a primitive element of $\mathbb{F}_{3^4}$. According to Fig. 1, we need to compute an LFSR over the finite field $\mathbb{F}_{3^4}$ for implementing the shift sequence $\underline{\boldsymbol{e}}$. Since $\underline{\boldsymbol{b}}$ is a GMW sequence, it can be implemented by an LFSR over the finite field $\mathbb{F}_{3^2}$ together with a finite field circuit for computing $\mathrm{Tr}_1^2(x^5)$.

2) *Implementation of $\underline{\boldsymbol{e}}$ by an LFSR over $\mathbb{F}_{3^4}$*: We need a two-stage LFSR over $\mathbb{F}_{3^4}$ to implement $\underline{\boldsymbol{e}}$. 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.

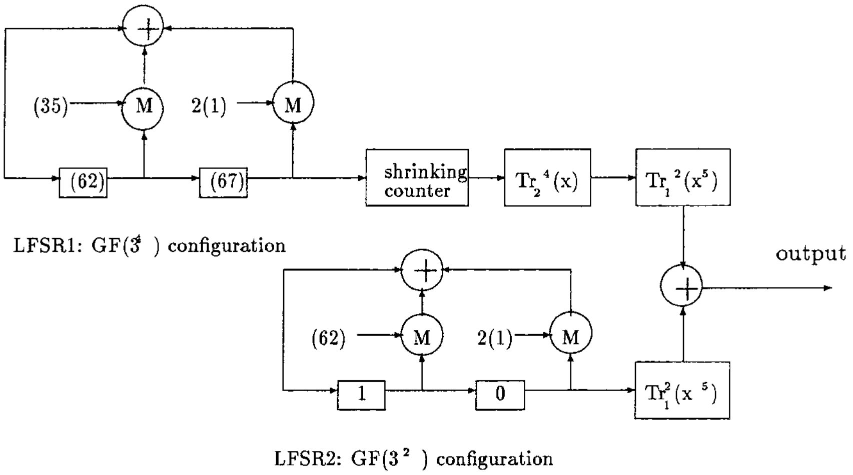

Fig. 2. Galois configuration of a $(6400, 80, 163)$ signal set.

Therefore, we have an LFSR over $\mathbb{F}_{3^4}$ with $g(x)$ as its characteristic polynomial. Set an initial state (β^{67}, β^{62}) for this LFSR.

3) *Implementation of* $\underline{\boldsymbol{b}}$ *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 characteristic polynomial. Fig. 2 presents an implementation in terms of the finite field circuit. We obtain all sequences in S by varying different initial states of the LFSR2 in Fig. 2.

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

According to Lemma 5 and Theorem 2, the signal set $S = S(\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}, \underline{\boldsymbol{e}})$, implemented by Fig. 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 Fig. 2 can be efficiently implemented in both hardware and software.

VII. Conclusion

We have presented a new design for constructions of families of p-ary sequences with low cross correlation, balance property, and large linear span. The construction uses short p-ary two-level autocorrelation sequences of period v together with the interleaved structure to construct a set of long sequences of period v^2. More precisely, each sequence can be arranged into a v by v matrix, which is a sum of two matrices A and B, where columns of A are shifts of $\underline{\boldsymbol{a}}$, a p-ary two-level autocorrelation sequence of period v, and the top row of B is a shift of $\underline{\boldsymbol{b}}$, a p-ary two-level autocorrelation sequence of period v; the remaining rows of B are identical to the top row. The parameter v is of the form $p^n - 1$ or a prime. There are v shift distinct sequences in one family. Each sequence is balanced. The maximal correlation is $2v + 3$ which is optimal with respect to the Welch bound. The linear span is exponentially increased in n for $v = p^n - 1$ and the linear span is maximal when v is prime and the short sequences are quadratic sequences. The construction allows for utilization of all two-level autocorrelation sequences in a free mode. Some families of the sequences can be efficiently implemented in both hardware and software.

Acknowledgment

The author wishes to thank P. Vijay Kumar for pointing out to her Kerdock code sequences and several other references on constructions of sequences with low correlation and large linear span.

References

[1] K. T. Arash and K. J. Player, "A new family of cyclic difference sets with Singer parameters in characteristic three," presented at the Second Int. Workshop in Coding and Cryptography, Paris, France, Jan. 8–12, 2001.

[2] L. D. Baumert, *Cyclic Difference Sets (Lecture Notes in Mathematics)*. Berlin, Germany: Springer-Verlag, 1971, vol. 182.

[3] S. Boztas and P. V. Kumar, "Binary sequences with Gold-like correlation but larger linear span," *IEEE Trans. Inform. Theory*, vol. 40, pp. 532–537, Mar. 1994.

[4] M. Antweiler and L. Bõmer, "Complex sequences over $GF(p)$ with a two-level autocorrelation function and a large linear span," *IEEE Trans. Inform. Theory*, vol. 38, pp. 120–130, Jan. 1992.

[5] A. H. Chan, M. Goresky, and A. M. Klapper, "Correlation functions of geometric sequences," in *Advances in Cryptology—EUROCRYPT '90 (Aarhus, 1990) (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 473, pp. 214–221.

[6] C. J. Colbourn, "Difference triangle sets," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. San Diego, CA: CRC, 1995, ch. IV.14.

[7] J. Dillon, "Classified all cyclic difference sets with Singer parameters in characteristic $p > 2$," unpublished, Aug. 2001, private communication.

[8] J. Dillon and H. Dobbertin, "New cyclic difference sets with Springer parameters," preprint, Aug. 1999.

[9] H. Dobbertin, "Kasami power functions, permutations and cyclic difference sets," in *Proc. NATO ASI Workshop*, Bad Windsheim, Germany, Aug. 3–14, 1998.

[10] R. A. Games, "Cross correlation of m-sequences and GMW sequences with the same primitive polynomial," *Discr. Appl. Math.*, vol. 12, pp. 139–146, 1985.

[11] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 154–156, Jan. 1968.

[12] B. Gordon, W. H. Mill, and L. R. Welch, "Some new difference sets," *Can. J. Math.*, vol. 14, no. 4, pp. 614–625, 1962.

[13] S. W. Golomb, *Shift Register Sequences*, revised ed. Laguna Hills, CA: Aegean Park, 1982, p. 39.

[14] G. Gong, "On q-ary cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 263–267, Jan. 1996.

[15] 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. Inform. Theory*, vol. 46, pp. 474–484, Mar. 2000.

[16] G. Gong, P. Gaal, and S. W. Golomb, "A suspected infinity class of cyclic Hadamard difference sets," in *Proc. 1997 IEEE Information Theory Workshop*, Longyearbyen, Svalbard, Norway, July 6–12, 1997.

[17] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 400–411, Mar. 1995.

[18] ——, *Sequence Analysis*. Waterloo, ON, Canada: Univ. Waterloo, Lecture Notes for Course CO739x, ch. 5. [Online]. Available: http://calliope.uwaterloo.ca/~ggong.

[19] G. Gong and S. W. Golomb, "Binary sequences with two-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, pp. 692–693, Mar. 1999.

[20] Marshall Jr. Hall, "A survey of difference sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975–986, 1956.

[21] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2868–2872, Dec. 2002.

[22] T. Helleseth, "Correlation of m-sequences and related topics," in *Sequences and Their Applications—Proc. SETA'98 (Discrete Mathematics and Theoretical Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, pp. 49–66.

[23] T. Herlestam, "On functions of linear shift register sequences," in *Advances in Cryptology—EuroCrypt'85 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1985, vol. 219, pp. 119–129.

[24] T. Helleseth, "Correlation of m-sequences and related topics," in *Sequences and Their Applications—Proc. SETA'98 (Discrete Mathematics and Theoretical Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, pp. 49–66.

[25] ——, "Some results about the cross-correlation functions between two maximal length linear sequences," *Discr. Math.*, vol. 16, pp. 209–232, 1978.

[26] T. Helleseth, P.V. Kumar, and H. Martinson, "A new family of ternary sequences with ideal two-level autocorrelation function," *Des., Codes, Cryptogr.*, vol. 23, no. 2, pp. 157–166, July 2001.

[27] T. Helleseth and V. J. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier , 1998.

[28] S. Jiang, Z. D. Dai, and G. Gong, "Notes on q-ary interleaved sequences," in *Sequences and Their Applications—Proc. SETA'98 (Discrete Mathematics and Theoretical Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, pp. 273–283.

[29] T. Kasami, "Weight distribution of Bose–Chaudhuri–Hocquenghem codes," in *Combinatorial Mathematics and Its Applications*. Chapel Hill, NC: Univ. North Carolina Press, 1969.

[30] A. M. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 39, pp. 177–183, Jan. 1993.

[31] ——, "Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences," *Discr. Appl. Math.*, vol. 46, no. 1, pp. 1–20, 1993.

[32] A. M. Klapper, "Large families of sequences with near-optimal correlations and large linear span," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1241–1248, July 1996.

[33] P.V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons, "Large families of quaternary sequences with low correlation," *IEEE Trans. Inform. Theory*, vol. 42, pp. 579–592, Mar. 1996.

[34] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, pp. 603–616, May 1991.

[35] P. V. Kumar, "On bent sequences and generalized bent functions," Ph.D. dissertation, Univ. Southern Calif., Los Angeles, CA, 1983.

[36] ——, "Frequency-hopping code sequence designs having large linear span," *IEEE Trans. Inform. Theory*, vol. 34, pp. 146–151, Jan. 1988.

[37] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983, vol. 20, Theorem 3.35, pp. 97–98.

[38] M. Ludkovski and G. Gong, "New families of ideal 2-level autocorrelation ternary sequences from second order DHT," in *Proc. 2nd Int. Workshop on Coding and Cryptography*, Paris, France, Jan. 8–12, 2001, pp. 345–354.

[39] A. Maschietti, "Difference sets and hyperovals," *Des., Codes, Cryptogr.*, vol. 14, pp. 89–98, 1998.

[40] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, Jan. 1969.

[41] F. J. McWilliams and N. J. A. Sloane, *Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977, ch. 15.

[42] J. S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, Univ. Southern Calif., Los Angeles, CA, May 1988.

[43] ——, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 260–262, Jan. 1996.

[44] ——, "New cyclic difference sets with Singer parameters constructed from d-homogeneous functions," in *Proc. Int. Conf. Sequences and Their Applications*, Bergen, Norway, May 13–17, 2001.

[45] J. S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, "New binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 814–817, Mar. 1998.

[46] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371–379, Mar. 1989.

[47] J.-S. No, H. Chung, and M.-S. 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, pp. 1278–1282, May 1998.

[48] 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, pp. 1596–1602, Sept. 1997.

[49] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 858–864, Nov. 1982.

[50] J. G. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.

[51] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT–30, pp. 548–553, May 1984.

[52] V. M. Sidelnikov, "On mutual correlation of sequences," *Probl. Kybern.*, vol. 24, pp. 537–545, Sept. 1978.

[53] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1–38.

[54] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1991.

[55] H. M. Trachtenberg, "On the cross-correlation functions of maximal linear sequences," Ph.D. dissertation, Univ. Southern Calif., Los Angeles, CA, 1970.

[56] L. R. Welch, "Lower bounds on the minimum correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.

[57] N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.*, vol. 7, pp. 31–48, 1959.