

# Sequence Designs for Ultra-Wideband Impulse Radio With Optimal Correlation Properties

Wensong Chu, *Member, IEEE*, and Charles J. Colbourn

**Abstract**—We formulate a combinatorial model of impulse radio sequences (IRSs) to study sequence or signal design for ultra-wideband (UWB) radio with unmodulated time hopping. Using this combinatorial model for IRSs, we develop necessary and sufficient conditions for the existence of IRSs. Several novel constructions for IRSs with optimal correlation properties are given. The constructions involve the Welch construction for Costas arrays, a quadratic polynomial construction over finite fields, recursive techniques for optical orthogonal codes, and combinatorial design techniques using perfect Mendelsohn designs (PMDs).

**Index Terms**—Costas arrays, optical orthogonal codes, perfect Mendelsohn designs (PMDs), ultra-wideband (UWB) radios.

## I. INTRODUCTION

ULTRA-wideband (UWB) refers to an electromagnetic waveform characterized by a radiated spectrum with a very wide bandwidth around a relatively low central frequency. When the 3-dB bandwidth becomes 25% or more of the signal's central frequency, by convention this radio has a *UWB nature*, according to [9]. UWB systems for wireless communication have recently become an important area of research. An important component is the construction of sequences with low correlation, along with a power spectral density that complies with the requirements of the Federal Communications Commission (FCC). Satisfactory coexistence of UWB radio signals with other narrowband and wideband signals requires that UWB radio employ spread-spectrum methods.

Various UWB systems have been studied in the literature, such as a time hopping (TH) spread-spectrum multiple access (TH-SSMA) system (impulse radio) [11], and multistage frequency hopping (FH) SSMA models [12].

In this paper, a general combinatorial method for sequence designs suitable for UWB signals using TH-SSMA is proposed and several families of sequences with optimal correlation are constructed.

## II. TIME HOPPING SIGNAL MODELS

In [9], an unmodulated TH UWB signal generator is given by

$$s^{(i)}(t) = \sum_j p(t - jT_f - c_j^{(i)}T_s) = \sum_n a_n^{(i)} p(t - nT_s)$$

Manuscript received November 19, 2003; revised June 4, 2004. This work was supported by the U. S. Army Research Office under Grant DAAD19-01-1-0406.

W. Chu was with the Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-8809 USA. He is now with CMS BondEdge, Santa Monica, CA 90405 USA.

C. J. Colbourn is with the Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-8809 USA.

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2004.834794

where time is divided into *slots* of width  $T_s$ , and  $N_s$  slots are grouped into a *frame* of duration  $T_f = N_s T_s$ . The integer TH code  $\{c_j^{(i)}\}$ ,  $0 \leq c_j^{(i)} < N_s$  has period  $N_f$ . Then the quantity  $a_n^{(i)}$  is

$$a_n^{(i)} = \begin{cases} 1, & \text{if there is an integer } j \text{ such that } n = jN_s + c_j^{(i)} \\ 0, & \text{otherwise.} \end{cases}$$

We also assume that the time width  $T_w$  of a pulse  $p(t)$  is less than  $T_s$ . Then the normalized periodic correlation between the signals of the  $i$ th user and the  $j$ th user is

$$\Lambda_{ij}(n_\tau T_s) = \frac{1}{N_f N_s} \sum_{n=0}^{N_f N_s - 1} a_n^{(i)} a_{n \ominus n_\tau}^{(j)}$$

where  $\ominus$  denotes subtraction modulo the period. Using this system model, we define a new class of sequences, *impulse radio sequences*.

Let  $n$  be a positive integer. The set of integers from 0 to  $n-1$  is denoted by  $\mathcal{T}_n$  in this paper

$$\mathcal{T}_n = \{0, 1, 2, \dots, n-1\}.$$

**Definition 1:** Let  $\alpha = (a_0, a_1, \dots, a_{n-1})$  be a binary vector of dimension  $n$ . Define the *support* of  $\alpha$ , denoted by  $\text{supp}(\alpha)$  as the set of indices  $i$  for which  $a_i = 1$ , that is,

$$\text{supp}(\alpha) = \{i | a_i = 1, i \in \mathcal{T}_n\}.$$

**Example 1:** The support of  $x = (1, 1, 0, 1, 0, 0, 0)$  is  $\text{supp}(x) = \{0, 1, 3\}$ .

**Definition 2:** An  $(N_s, N_f, \lambda_a, \lambda_c)$  impulse radio sequence (IRS)  $\mathcal{C}$  is a family of  $(0, 1)$  sequences of length  $N_f N_s$  and weight  $N_f$  satisfying the following three properties.

- 1) The *Pulse Position Property*:

For any

$$x = \{x_t\}_{t=0}^{N_f N_s - 1} \in \mathcal{C}$$

there exist  $N_f$  integers  $a_0, a_1, \dots, a_{N_f-1}$  from  $\mathcal{T}_{N_s}$ , such that the support of  $x$  can be expressed as

$$\text{supp}(x) = \{a_i + iN_s \mid i \in \mathcal{T}_{N_f}, a_i \in \mathcal{T}_{N_s}\}$$

i.e., if the  $N_f N_s$  slots are uniformly divided into  $N_f$  frames, then each frame has a unique pulse position among its  $N_s$  slots.

- 2) The *Autocorrelation Property*:

$$\sum_{t=0}^{N_f N_s - 1} x_t x_{t \oplus \tau} \leq \lambda_a$$

for any

$$x = \{x_t\}_{t=0}^{N_f N_s - 1} \in \mathcal{C}$$

and every integer  $\tau$ ,  $\tau \not\equiv 0 \pmod{N_f N_s}$ . Here  $\oplus$  denotes addition modulo  $N_f N_s$ .

3) The *Crosscorrelation Property*:

$$\sum_{t=0}^{N_f N_s - 1} x_t y_{t \oplus \tau} \leq \lambda_c$$

for any

$$x = \{x_t\}_{t=0}^{N_f N_s - 1} \in \mathcal{C}, \quad y = \{y_t\}_{t=0}^{N_f N_s - 1} \in \mathcal{C}$$

with  $x \neq y$  and every integer  $\tau$ . Here  $\oplus$  denotes addition modulo  $N_f N_s$ .

When  $\lambda_a = \lambda_c = \lambda$ , the notation  $(N_s, N_f, \lambda)$ -IRS is used.

The definition of IRSs shows its close relationship with optical orthogonal codes.

*Definition 3:* [4] An  $(n, \omega, \lambda_a, \lambda_c)$  optical orthogonal code (OOC) $\mathcal{C}$  is a family of  $(0, 1)$  sequences of length  $n$  and weight  $\omega$  satisfying the following two properties, where  $\oplus$  denotes addition modulo  $n$ .

1) The *Autocorrelation Property*:

$$\sum_{t=0}^{n-1} x_t x_{t \oplus \tau} \leq \lambda_a$$

for any

$$x = \{x_t\}_{t=0}^{n-1} \in \mathcal{C}$$

and every integer  $\tau$ ,  $\tau \not\equiv 0 \pmod{n}$ .

2) The *Crosscorrelation Property*:

$$\sum_{t=0}^{n-1} x_t y_{t \oplus \tau} \leq \lambda_c$$

for any

$$x = \{x_t\}_{t=0}^{n-1} \in \mathcal{C}, \quad y = \{y_t\}_{t=0}^{n-1} \in \mathcal{C}$$

with  $x \neq y$  and every integer  $\tau$ .

When  $\lambda_a = \lambda_c = \lambda$ , the notation  $(n, \omega, \lambda)$ -OOC is used.

*Theorem 1:* An  $(N_s, N_f, \lambda_a, \lambda_c)$ -IRS is an  $(N_f N_s, N_f, \lambda_a, \lambda_c)$ -OOC.

*Proof:* This follows from the definitions of IRSs and OOCs.  $\square$

Let  $\Phi(N_f, N_s, \lambda_a, \lambda_c)$  denote the maximal possible number of sequences in an  $(N_f, N_s, \lambda_a, \lambda_c)$ -IRS. An  $(N_f, N_s, \lambda_a, \lambda_c)$ -IRS is *optimal* if it consists of  $\Phi(N_f, N_s, \lambda_a, \lambda_c)$  sequences.

Since it is difficult to determine the exact value of  $\Phi(N_f, N_s, \lambda_a, \lambda_c)$ , upper bounds for  $\Phi(N_f, N_s, \lambda_a, \lambda_c)$  are of interest. In the case when  $\lambda_a = \lambda_c$ , Theorem 1 ensures that  $\Phi(N_s, N_f, \lambda, \lambda)$  is bounded by the Johnson bound.

*Theorem 2 ([7]): (Johnson bound)*

$$\begin{aligned} & \Phi(N_s, N_f, \lambda, \lambda) \\ & \leq \left\lfloor \frac{1}{N_f} \left\lfloor \frac{N_f N_s - 1}{N_f - 1} \left\lfloor \frac{N_f N_s - 2}{N_f - 2} \left[ \dots \left\lfloor \frac{N_f N_s - \lambda}{N_f - \lambda} \right\rfloor \dots \right] \right\rfloor \right\rfloor \right\rfloor. \end{aligned}$$

In addition to the binary sequence representations used in the definition of IRSs, there are several other natural representations, such as the doubly periodic matrices used in [9] and the set representations used in most research on OOCs [4]. In order to deal with the pulse position property of IRSs, we use an  $N_f$ -tuple to represent an IRS.

Let  $\mathcal{C}$  be an IRS with  $M$  sequences and

$$x = (x_0, x_1, \dots, x_{N_s N_f - 1}) \in \mathcal{C}$$

be one of its binary sequences. The pulse position property of  $\mathcal{C}$  guarantees that the support of  $x$  is of the following form:

$$\text{supp}(x) = \{a_i + i N_s \mid i \in \mathcal{T}_{N_f}, a_i \in \mathcal{T}_{N_s}\}.$$

Thus, we represent  $x$  as an  $N_f$ -tuple  $X$  over the set  $\mathcal{T}_{N_s}$

$$X = (a_0, a_1, \dots, a_{N_f - 1}).$$

Given two sequences

$$X = (a_0, a_1, \dots, a_{N_f - 1}) \quad \text{and} \quad Y = (b_0, b_1, \dots, b_{N_f - 1})$$

we define a multiset (a multiset can contain an element more than once)  $\Delta_{XY}^t$  to denote all possible differences between elements in  $X$  and  $Y$ , which are  $t$ -apart cyclically, i.e.,

$$\Delta_{XY}^t = \{b_{i \oplus t} - a_i \mid i \in \mathbb{Z}_{N_f}\}.$$

Then  $\Delta_{XY}^t$  is a collection of integers ranging from  $-(N_s - 1)$  to  $N_s - 1$ .

We also define a multiset  $\mathcal{D}_{XY}^t$  to denote all possible differences (modulo  $N_s N_f$ ) between every cyclically  $t$ -apart pair of elements in  $X$  and  $Y$  as follows:

$$\begin{aligned} \mathcal{D}_{XY}^t &= \Delta_{XY}^t + t N_s \\ &= \{t N_s + b_{i \oplus t} - a_i \pmod{N_s N_f} \mid i \in \mathbb{Z}_{N_f}\}. \end{aligned}$$

Thus,  $\mathcal{D}_{XY}^t$  is a collection of elements of  $\mathbb{Z}_{N_s N_f}$ .

In the remainder of this paper,  $\oplus$  and  $\ominus$  denote addition and subtraction modulo certain integers.

### III. NECESSARY AND SUFFICIENT CONDITIONS FOR IRSS

In this section, we begin with some necessary conditions for an IRS to have the desired correlation properties. Since any IRS is an OOC, some techniques for OOCs can be applied here. To study OOCs, instead of viewing its sequences as binary vectors, it is convenient to use their supports. Thus, an OOC can be viewed as a families of subsets.

*Theorem 3([4]):* Let  $\mathcal{C}$  be a family of  $\omega$ -subsets (subsets of size  $\omega$ ) of  $\mathbb{Z}_n$ .  $\mathcal{C}$  is an  $(n, \omega, \lambda_a, \lambda_c)$  optical orthogonal code if and only if the following two conditions hold.

- 1) For each  $X \in \mathcal{C}$ , any nonzero  $c \in \mathbb{Z}_n$  can be represented as a difference  $x - x'$ , with  $x, x' \in X$  in at most  $\lambda_a$  ways.
- 2) For each pair of  $X \in \mathcal{C}$  and  $Y \in \mathcal{C}$  with  $X \neq Y$ , any  $c \in \mathbb{Z}_n$  can be represented as the difference  $x - y$  with  $x \in X$  and  $y \in Y$ , in at most  $\lambda_c$  ways.

Let  $X = (a_0, a_1, \dots, a_{N_f-1})$  and  $Y = (b_0, b_1, \dots, b_{N_f-1})$  be two sequences in an  $(N_s, N_f, \lambda_a, \lambda_c)$ -IRS. According to Theorem 3, we need to check the collection of differences

$$\bigcup_{t=d_0}^{N_f-1} D_{XY}^t$$

where  $\cup$  represents union of multisets, and  $d_0 = 1$  if  $X = Y$  and  $d_0 = 0$  if  $X \neq Y$ . It is convenient to study instead the multiset

$$\bigcup_{t=d_0}^{N_f-1} \Delta_{XY}^t.$$

First we derive some necessary conditions for IRSs based on Theorem 3.

*Lemma 1:* Let  $\mathcal{C}$  be an  $(N_s, N_f, \lambda_a, \lambda_c)$ -IRS. Let

$$X = (a_0, a_1, \dots, a_{N_f-1}) \quad \text{and} \quad Y = (b_0, b_1, \dots, b_{N_f-1})$$

with  $a_i, b_i \in \mathcal{T}_{N_s}$  be two sequences in  $\mathcal{C}$ . Then for any given  $g$  with  $-N_s+1 \leq g \leq N_s-1$  and for any given  $d$  with  $d_0 \leq d \leq N_f-1$ , the multiset  $\Delta_{XY}^d$  contains  $g$  at most  $\lambda$  times, where  $\lambda = \lambda_a$  and  $d_0 = 1$  if  $X = Y$ , and  $\lambda = \lambda_c$  and  $d_0 = 0$  if  $X \neq Y$ .

*Proof:* Since  $\mathcal{C}$  is also an  $(N_s N_f, N_f, \lambda_a, \lambda_c)$ -OOC, Theorem 3 ensures that the set

$$\bigcup_{d=d_0}^{N_f-1} D_{XY}^d$$

contains each element no more than  $\lambda$  times. Thus, for every  $d$ ,  $\mathcal{D}_{XY}^d$  contains each element no more than  $\lambda$  times. Since  $\mathcal{D}_{XY}^d = \Delta_{XY}^d + dN_s$ , for given  $g$ ,  $\Delta_{XY}^d$  contains each element no more than  $\lambda$  times.  $\lambda$  takes the value  $\lambda_a$  and  $d_0 = 1$  if  $X = Y$  and takes the value  $\lambda_c$  and  $d_0 = 0$  if  $X \neq Y$ .  $\square$

*Lemma 2:* Let  $\mathcal{C}$  be an  $(N_s, N_f, \lambda_a, \lambda_c)$ -IRS. Let

$$X = (a_0, a_1, \dots, a_{N_f-1}) \quad \text{and} \quad Y = (b_0, b_1, \dots, b_{N_f-1})$$

with  $a_i, b_i \in \mathcal{T}_{N_s}$  be two sequences in  $\mathcal{C}$ . Then for every  $g$  with  $0 \leq g \leq N_s-1$  and for any given  $d$  with  $d_0 \leq d \leq N_f-1$ , if  $g$  appears in  $\Delta_{XY}^d$  for  $t_1$  times and  $-N_s+g$  appears in  $\Delta_{XY}^{d+1}$  for  $t_2$  times, then  $t_1+t_2 \leq \lambda$ , where  $\lambda = \lambda_a$  and  $d_0 = 1$  if  $X = Y$  and  $\lambda = \lambda_c$  and  $d_0 = 0$  if  $X \neq Y$ .

*Proof:* If  $g$  appears in  $\Delta_{XY}^d$ , then it represents a difference  $dN_s + g \pmod{N_s N_f}$  in  $\mathcal{D}_{XY}^d$ ; if  $-N_s + g$  appears in  $\Delta_{XY}^{d+1}$ , then it represents a difference

$$(d+1)N_s - N_s + g = dN_s + g \pmod{N_s N_f}.$$

They result in the same difference in

$$\bigcup_{d=d_0}^{N_f-1} D_{XY}^d.$$

Thus, the total number of appearances is no more than  $\lambda$ . Here  $\lambda$  and  $d_0$  are defined as usual.  $\square$

Lemma 2 strengthens Lemma 1. Indeed, the necessary conditions in Lemma 2 are also sufficient for the existence of IRSs.

*Theorem 4 (Necessary and Sufficient Conditions):* Let  $\mathcal{C}$  be a collection of  $N_f$ -tuples over the set  $\mathcal{T}_{N_s}$ . Then  $\mathcal{C}$  forms an  $(N_s, N_f, \lambda_a, \lambda_c)$ -IRS if and only if for every  $X = (a_0, a_1, \dots, a_{N_f-1}) \in \mathcal{C}$  and  $Y = (b_0, b_1, \dots, b_{N_f-1}) \in \mathcal{C}$ , for every  $g$  with  $0 \leq g \leq N_s-1$ , and for every  $d$  with  $d_0 \leq d \leq N_f-1$ , if  $g$  appears in  $\Delta_{XY}^d$   $t_1$  times and  $-N_s+g$  appears in  $\Delta_{XY}^{d+1}$   $t_2$  times, then  $t_1+t_2 \leq \lambda$ , where  $\lambda = \lambda_a$  and  $d_0 = 1$  if  $X = Y$  and  $\lambda = \lambda_c$  and  $d_0 = 0$  if  $X \neq Y$ .

*Proof:* Since  $\mathcal{C}$  is a collection of  $N_f$ -tuples over the set  $\mathcal{T}_{N_s}$ ,  $\mathcal{C}$  satisfies the pulse position property. We only need to show  $\mathcal{C}$  is also  $(N_s N_f, N_f, \lambda_a, \lambda_c)$ -OOC. Based on Theorem 3 and Lemma 2, it is sufficient to show that the multiset  $\mathcal{U}$

$$U = \bigcup_{d=d_0}^{N_f-1} D_{XY}^d$$

contains each element no more than  $\lambda$  times, where  $\lambda$  is as above.

For any  $u \in \mathcal{U}$ ,  $u$  must be of the form  $dN_s + g$  with  $d_0 \leq d \leq N_f-1$  and  $-N_s+1 \leq g \leq N_s-1$ . If there are two sets of elements  $(d_1, g_1)$  and  $(d_2, g_2)$ , such that

$$u = d_1 N_s + g_1 = d_2 N_s + g_2, \pmod{N_s N_f}$$

then

$$d_1 N_s - d_2 N_s = g_2 - g_1, \pmod{N_s N_f}.$$

It also implies that

$$d_1 N_s - d_2 N_s = g_2 - g_1, \pmod{N_s}.$$

Since  $-N_s+1 \leq g_1, g_2 \leq N_s-1$  and  $d_0 \leq d_1, d_2 \leq N_f-1$ , the relationships between  $g_1$  and  $g_2$  and between  $d_1$  and  $d_2$  can be classified into the following cases:

- $g_1 = g_2$ , then  $d_1 = d_2$ ;
- $g_1 \neq g_2$  and  $g_1 \geq 0$ , then  $g_2 = -N_s + g_1$ ; it further implies that  $d_2 = d_1 + 1$ ;
- $g_1 \neq g_2$  and  $g_1 \leq 0$ , then  $g_2 = N_s + g_1$ ; it further implies that  $d_2 = d_1 - 1$ .

Given  $a \in X$  and  $b \in Y$ , suppose that  $a$  is cyclically  $d$ -apart from  $b$ , the difference  $a - b$  can be expressed as  $dN_s + g$  with  $d_0 \leq d \leq N_f-1$  and  $-N_s+1 \leq g \leq N_s-1$ . We need to show that  $\mathcal{U}$  contains  $dN_s + g \pmod{N_s N_f}$  no more than  $\lambda$  times.

We divide the proof into two cases:

- 1) If  $0 \leq g \leq N_s-1$  and the difference  $dN_s + g$  appears in  $\mathcal{D}_{XY}^d$   $t_1$  times with  $g \in \Delta_{XY}^d$ , by the above analysis, any element outside  $\mathcal{D}_{XY}^d$  equal to  $dN_s + g$  in  $\mathcal{U}$  is of form  $(d+1)N_s + (-N_s + g)$ , i.e., it appears in  $\mathcal{D}_{XY}^{d+1}$  with  $-N_s + g \in \Delta_{XY}^{d+1}$ . Suppose  $-N_s + g$  appears in  $\Delta_{XY}^{d+1}$   $t_2$  times, then  $t_1+t_2 \leq \lambda$ , i.e.,  $dN_s + g$  appears in  $\mathcal{U}$  at most  $\lambda$  times.
- 2) If  $-N_s+1 \leq g \leq 0$ , the difference  $dN_s + g$  either appear in  $\mathcal{D}_{XY}^d$  with  $g \in \Delta_{XY}^d$  or appears in  $\mathcal{D}_{XY}^{d-1}$  with  $N_s + g \in \Delta_{XY}^{d-1}$ . Since  $N_s + g$  ranges from 0 to  $N_s-1$ , the second case can be treated in the same manner as the first case.  $\square$

## IV. IRSS WITH OPTIMAL AUTOCORRELATION

In this section, we give two constructions for IRSs consisting of a single sequence that are optimal with respect to the Johnson bound. The basic idea employs a simple fact, that if  $a - b \not\equiv c - d \pmod{v}$ , then  $a - b \neq c - d$  as integers.

*Theorem 5 (Welch Construction [5]):* Let  $\alpha$  be a primitive root modulo an odd prime  $p$ . Then the vector

$$x = (1, \alpha, \alpha^2, \dots, \alpha^{p-2})$$

has the property that for every  $d$  with  $1 \leq d \leq p - 2$ , and for every  $g \in \mathbb{Z}_p$  with  $g \neq 0$ , there exists a unique pair  $(i, i + d) \pmod{p - 1}$  such that  $\alpha^{i+d} - \alpha^i = g \pmod{p}$ .

The Welch construction is used to construct Costas arrays [5], [6]. There are three typical methods to construct Costas arrays. However, only this construction has the *singly periodic* property. It is a long-standing open question whether the Welch construction is the only possible way to obtain a singly periodic Costas array.

Using the Welch construction, we give our first construction for optimal IRSs.

*Theorem 6:* Let  $p$  be an odd prime and  $\alpha$  be a primitive element of  $\mathbb{Z}_p$ . Then the vector

$$X = (1, \alpha, \alpha^2, \dots, \alpha^{p-2})$$

is an optimal  $(2(p - 2), p - 1, 1)$ -IRS.

*Proof:* From the Welch construction, for every  $g \in \mathbb{Z}_p$  with  $g \neq 0$  and every  $d$  with  $1 \leq d \leq p - 2$  there exists a unique way to represent  $\alpha^{i+d} - \alpha^i = g \pmod{p}$ . It implies that each  $g$  with  $-p + 2 \leq g \leq p - 2$  appears at most once in  $\Delta_{XX}^d$ .

We now check the necessary and sufficient conditions for  $X$  given in Theorem 4. We divide our discussion into three different cases:

- 1) For each  $g$  with  $0 \leq g \leq p - 3$ , and every  $d$  with  $1 \leq d \leq p - 2$ ,  $\Delta_{XX}^d$  contains  $g$  at most once ( $t_1 \leq 1$ ) and  $\Delta_{XX}^{d+1}$  contains

$$-N_s + g = -2(p - 2) + g \leq -(p - 1)$$

zero ( $t_2 = 0$ ) times. Thus,  $t_1 + t_2 \leq 1$ .

- 2) For each  $g$  with  $p - 1 \leq g \leq 2(p - 2)$ , and every  $d$  with  $1 \leq d \leq p - 2$ ,  $\Delta_{XX}^d$  contains  $g$  zero times ( $t_1 = 0$ ) and  $\Delta_{XX}^{d+1}$  contains  $-N_s + g$  at most once ( $t_2 \leq 1$ ). Thus,  $t_1 + t_2 \leq 1$ .

- 3) If  $g = p - 2$ , then  $p - 2 \in \Delta_{XX}^{d_0}$  with  $d_0 = \frac{p-1}{2}$ . We need to show that

$$-N_s + g = -(p - 2) \notin \Delta_{XX}^{d_0+1}$$

and it follows a simple fact that for any other  $d \neq d_0$ , the  $\min \Delta_{XX}^d \geq -(p - 3)$ . Thus,  $t_1 + t_2 \leq 1$  when  $g = p - 2$ .

By Theorem 4,  $X$  is a  $(2(p - 2), p - 1, 1)$ -IRS, with  $N_s = 2(p - 2)$

$$\left| \frac{2(p - 2)(p - 1) - 1}{(p - 1)(p - 2)} \right| = 1.$$

Thus, the Johnson bound is attained and  $\mathcal{C}$  is optimal.  $\square$

*Example 2:* Let  $p = 7$  and  $\alpha = 3$ . Then  $X = (1, 3, 2, 6, 4, 5)$  is an optimal  $(10, 6, 1)$ -IRS.

*Theorem 7:* Let  $p$  be an odd prime. Let  $f(x) = ax^2$  be a quadratic polynomial over  $\mathbb{Z}_p$ , with  $a \neq 0$  and  $a \neq -4$ . Then the vector  $X = (f(0), f(1), f(2), \dots, f(p - 1))$  is an optimal  $(2(p - 1), p, 1)$ -IRS with a single sequence.

*Proof:* The difference

$$f(x + d) - f(x) = a(x + d)^2 - ax^2 = 2adx + d^2$$

is a linear polynomial with  $1 \leq d \leq p - 1$ . Thus, for each  $g \in \mathbb{Z}_p$  and  $d$ , there exists a unique way to represent  $g$  as  $f(i + d) - f(i) \pmod{p}$  with  $i \in \mathbb{Z}_p$ .

According to Theorem 4, for  $g$  with  $0 \leq g \leq 2(p - 1) - 1$  and every  $d$  with  $1 \leq d \leq p - 1$ , we need to estimate the value  $t_1 + t_2$ , the total appearances of  $g$  in  $\Delta_{XX}^d$  and  $\Delta_{XX}^{d+1}$ . We treat four cases.

- 1) If  $0 \leq g \leq p - 2$ , then  $-N_s + g = -2(p - 1) + g \leq -p$ . Then  $t_1 \leq 1$  and  $t_2 = 0$ . Thus,  $t_1 + t_2 \leq 1$ .
- 2) If  $g \geq p$ , then  $t_1 = 0$ ,  $t_2 \leq 1$  and  $t_1 + t_2 \leq 1$ .
- 3) If  $g = p - 1$  and there exists a  $d_0 \in \mathbb{Z}_p$  such that  $ad_0^2 = -1$ , then  $g$  appears and only appears in the following multiset:  $\Delta_{XX}^{d_0}$  and  $\Delta_{XX}^{p-d_0}$ . In addition,  $-N_s + g = -(p - 1)$  appears and only appears in  $\Delta_{XX}^{p-d_0}$  and  $\Delta_{XX}^{d_0}$ .  $t_1 + t_2$  exceeds 1 if and only if  $d_0 = \frac{p-1}{2}$  and  $ad_0^2 = -1$ , which only happens when  $a = -4$ .
- 4) If  $g = p - 1$  and there does not exist  $d_0 \in \mathbb{Z}_p$  such that  $ad_0^2 = -1$ , then  $\max |\Delta_{XX}^d| \leq p - 2$ .  $N_s = 2(p - 1)$  guarantees that  $t_1 + t_2 \leq 1$ .

Thus,  $X$  forms a  $(2(p - 1), p, 1)$ -IRS by Theorem 4. It is optimal with respect to the Johnson bound.  $\square$

If we collect all the possible vectors in Theorem 7, we form a new IRS.

*Corollary 1:* Let  $p$  be an odd prime. Let  $f_a(x) = ax^2$  be a quadratic polynomial over  $\mathbb{Z}_p$ , with  $a \neq 0$ . Then the  $p - 1$  vectors

$$X_a = (f_a(0), f_a(1), f_a(2), \dots, f_a(p - 1)), \quad a \neq 0$$

form a  $(2p - 1, p, 1, 2)$ -IRS with  $p - 1$  sequences.

*Proof:* First we check the value of  $\lambda_a$ . Since we take

$$N_s = 2p - 1 = (p - 1) + (p - 1) + 1$$

for each pair  $(x, x \oplus d)$ , and for every  $a$ ,  $f_a(x + d) - f_a(x)$  is in the range from  $-(p - 1)$  to  $p - 1$ .  $N_s = 2p - 1$  guarantees that for each  $g$  with  $0 \leq g \leq 2p - 2$ , and for each  $d$  with  $1 \leq d \leq p - 1$ ,  $t_1 + t_2 \leq 1$  and, thus,  $\lambda_a = 1$  in terms of Theorem 4.

To check the value of  $\lambda_c$ , we notice that  $f_a(x + d) - f_b(x)$  is a polynomial of degree 2. For each  $g$  with  $0 \leq g \leq 2p - 2$ , and for each  $d$  with  $1 \leq d \leq p - 1$ ,  $f_b(x + d) - f_a(x)$  ranges from  $-(p - 1)$  and  $(p - 1)$ .  $N_s = 2p - 1$  guarantees that  $\lambda_c = 2$ .  $\square$

*Example 3:* When  $p = 11$ , we have the 10 sequences

$$X_a = a * (0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1), \quad a \in \mathbb{Z}_{11}, \quad a \neq 0.$$

These form a  $(21, 11, 1, 2)$ -IRS. The condition that  $N_s \geq 2p - 1$  is not necessary. Indeed, this IRS is a  $(19, 11, 1, 2)$ -IRS, and the statement that  $N_s = 21$  is conservative.

For each  $a$ , except for  $a = -4$ , by Theorem 7,  $X_a$  is a  $(20, 11, 1, 1)$ -IRS. Similarly, 20 is not the smallest value for  $N_s$ . In [9], the same example is given with  $N_s = 11$ . When  $N_s = 11$ , from Theorem 4, an  $(11, 11, 2, 4)$ -IRS results.

## V. IRSS WITH $N_s \gg N_f$

According to the Johnson bound, to achieve optimality with a single sequence for an  $(N_s, N_f, 1, 1)$ -IRS, we need

$$\left\lfloor \frac{N_s N_f - 1}{N_f (N_f - 1)} \right\rfloor = 1.$$

This suggests that  $N_f \leq N_s \leq 2(N_f - 1)$ . We attain optimality with  $N_s = 2(N_f - 1)$  in Section IV. It remains unclear whether there is an optimal  $(N_f, N_f, 1, 1)$ -IRS with a single sequence. In general, the Johnson bound suggests that  $\Phi(N_s N_f, N_f, \lambda)$  is approximately  $\frac{N_s \lambda}{N_f}$ . Thus, if we allow that  $N_s \gg N_f$ , we can construct some IRSSs with  $\lambda = 1$ . Such kinds of IRSSs are much easier to find. We introduce two methods.

### A. IRSSs Via a Recursive Construction for OOCs

In [3], we give a general recursive construction for OOCs that can be applied to any OOC provided that certain  $r$ -simple matrices exist. We begin with a definition.

**Definition 4:** Let  $G$  be an Abelian group of size  $n$ . Let  $r$  be a positive integer. An  $s \times t$  matrix  $A = (a_{ij})$  over  $G$  is  $r$ -simple if the difference of any two column vectors of  $A$  contains each element in  $G$  at most  $r - 1$  times.

**Theorem 8 ([3]): (The Basic Construction)** Let  $\mathcal{C}$  be an  $(n, \omega, \lambda_a, \lambda_c)$  OOC. If there exists an  $\omega \times N$   $r$ -simple matrix over  $\mathbb{Z}_g$ , then there exists an  $(ng, \omega, \lambda_a, \max\{\lambda_a, \lambda_c, r - 1\})$  OOC  $\mathcal{C}'$  with  $|\mathcal{C}'| = N|\mathcal{C}|$ , where  $|\mathcal{C}'|$  and  $|\mathcal{C}|$  denote the number of codewords in the new and original codes, respectively.

The existence and constructions of  $r$ -simple matrices over  $\mathbb{Z}_p$  are also given in [3].

**Lemma 3 ([3]):** For any prime  $p$  and integer  $r$  with  $2 \leq r \leq p$ , there exists a  $p \times p^{r-1}$   $r$ -simple matrix over  $\mathbb{Z}_p$ .

In particular, for  $r = 2$ , let  $R = (i \cdot j)_{p \times p} \pmod{p}$  be the multiplication table of  $\mathbb{Z}_p$ . Then  $R$  is a  $p \times p$  2-simple matrix over  $\mathbb{Z}_p$ .

**Theorem 9 ([2]):** Let  $q$  be a prime power. Then there exists an optimal  $(q^2 - 1, q, 1, 1)$ -OOC with a single sequence.

We apply the Basic Construction to the optimal OOC from Theorem 9 to obtain the following.

**Theorem 10:** Let  $p$  be an odd prime. Then there exists a  $(p^2 - 1, p, 1, 1)$ -IRS with  $p - 1$  sequences.

**Proof:** Construct a  $(p^2 - 1, p, 1, 1)$ -OOC from [2]. Since it has only one sequence, denote its support by  $X = \{a_0, a_1, \dots, a_{p-1}\}$ . Let  $M$  be the  $p \times (p - 1)$  2-simple matrix constructed from the multiplication table of  $\mathbb{Z}_p$  (Lemma 3) by deleting the first all-zero column. So each column of  $M$  is a permutation of  $\mathbb{Z}_p$ . Apply the Basic Construction to  $X$  as follows. For a column in  $M$ , say  $(b_0, b_1, \dots, b_{p-1})^T$ , construct a sequence with support

$$\{a_0 + (p^2 - 1)b_0, a_1 + (p^2 - 1)b_1, \dots, a_{p-1} + (p^2 - 1)b_{p-1}\}.$$

The resulting  $p - 1$  codewords form a  $(p^3 - p, p, 1, 1)$ -OOC according to the Basic Construction. To make it an IRS, we

check the pulse position property. Because each column of  $M$  is a permutation of  $\mathbb{Z}_p$ , the pulse position property holds.  $\square$

We would need one more sequence to make this IRS optimal with respect to the Johnson bound.

### B. IRSSs Via Perfect Mendelsohn Designs (PMDs)

The necessary and sufficient conditions derived in Section III suggest that perfect Mendelsohn designs (PMDs) are closely related to IRSSs.

**Definition 5:** A set of  $k$  distinct elements  $\{a_1, a_2, \dots, a_k\}$  is *cyclically ordered* by  $a_1 < a_2 < \dots < a_k < a_1$  and the pair  $a_i$  and  $a_{i+t}$  are  $t$ -apart in a cyclic  $k$ -tuple  $(a_1, a_2, \dots, a_k)$  where  $i + t$  is taken modulo  $k$ .

**Definition 6 ([8]):** Let  $v, k$ , and  $\lambda$  be positive integers. A  $(v, k, \lambda)$  *Mendelsohn design* (briefly,  $(v, k, \lambda)$ -MD) is a pair  $(X, \mathcal{B})$  where  $X$  is a  $v$ -set (of points) and  $\mathcal{B}$  is a collection of cyclically ordered  $k$ -subsets of  $X$  (called blocks) such that every ordered pair of points of  $X$  are consecutive in exactly  $\lambda$  of the blocks of  $\mathcal{B}$ . If for all  $t = 1, 2, \dots, k - 1$ , every ordered pair of points of  $X$  are  $t$ -apart in exactly  $\lambda$  of the blocks of  $\mathcal{B}$ , then the  $(v, k, \lambda)$ -MD is a PMD and denoted by  $(v, k, \lambda)$ -PMD.

**Example 4 ([1]):** Let  $X = \mathbb{Z}_8$ , and  $\mathcal{B}$  consist of the following blocks:

$$\begin{array}{ll} (1, 2, 3, 0, 4, 5, 6), & (1, 3, 5, 7, 6, 4, 0) \\ (1, 4, 6, 3, 7, 0, 2), & (1, 5, 4, 2, 0, 6, 7) \\ (1, 6, 0, 5, 2, 7, 3), & (1, 7, 2, 6, 5, 3, 4) \\ (1, 0, 7, 4, 3, 2, 5), & (2, 4, 7, 5, 0, 3, 6). \end{array}$$

Then  $(X, \mathcal{B})$  is a  $(8, 7, 1)$ -PMD.

We use existence results from [8] to demonstrate the constructions via PMDs. For detailed information, refer to [1] and [8].

**Theorem 11 ([8]):** Let  $p$  be an odd prime and  $r \geq 1$ . Then there exists a  $(p^r, p, 1)$ -PMD.

**Theorem 12:** Let  $p$  be an odd prime and  $r \geq 1$ , then there exists a  $(p^{2r} - 1, p, 1, 1)$ -IRS with  $p^{r-1}(p^r - 1)$  sequences.

**Proof:** Given  $p$  and  $r$ , we can construct a  $(p^{2r} - 1, p^r, 1)$ -OOC using Theorem 9 with a single sequence, say

$$D = \{A(0), A(1), \dots, A(p^r - 1)\}.$$

We can also construct a  $(p^r, p, 1)$ -PMD with  $M = p^{r-1}(p^r - 1)$  blocks. Let us denote them by

$$B_i = (b_{i,0}, b_{i,1}, \dots, b_{i,p-1}), \quad 1 \leq i \leq M.$$

For each  $B_i$ , we construct a  $p$ -dimensional vector as follows:

$$C_i = (A(b_{i,0}), A(b_{i,1}), \dots, A(b_{i,p-1})), \quad 1 \leq i \leq M.$$

We claim that these  $M$   $p$ -dimensional vectors  $\{C_i \mid 1 \leq i \leq M\}$  form a  $(p^{2r} - 1, p, 1, 1)$ -IRS. The resulting system has the following property: Given  $d$  with  $1 \leq d \leq p^r - 1$ , for each difference  $g \in \mathbb{Z}_{p^{2r}-1}$ , if there exists  $(s, t)$  with  $0 \leq s, t \leq p^r - 1$  such that  $A(t) - A(s) = g$ , then the pair  $(A(t), A(s))$  is contained in exactly one of the  $\{C_i\}$  with  $A(t)$   $d$ -apart from  $A(s)$ .

This property, together with the fact that each  $C_i$  is a permutation of a subset of  $D$ , ensures that for every  $g \in \mathbb{Z}_{p^{2r}-1}$ , and

for every  $d$  with  $1 \leq d \leq p^r - 1$ , if  $t_1 = 1$ , then  $t_2 = 0$  in terms of Theorem 4. Since it holds modulo  $p^{2r} - 1$ , it is true for all integers.  $\square$

The Johnson bound for a  $(p^{2r} - 1, p, 1)$ -IRS is  $p^{2r-1} + p^{2r-2} + \dots + p$ . Taking  $r = 1$  essentially reconstructs the method of Theorem 10. Indeed, it is a generalization of Theorem 10. We can make a small improvement by taking other PMDs.

*Theorem 13 ([8]):* Let  $v = p^r$  be a prime power and  $k > 2$  be such that  $k \mid (v - 1)$ . Then there exists a  $(v, k, 1)$ -PMD.

*Corollary 2:* For every  $r \geq 1$ , there exists a  $(2^r, 2^r - 1, 1)$ -PMD.

We also employ a well-known optimal OOC related to prime powers.

*Theorem 14 ([10]):* Let  $q$  be a prime power. Then there exists an optimal  $(q^2 + q + 1, q + 1, 1)$ -OOC with a single sequence.

*Theorem 15:* If  $p = 2^r - 1$  is a prime (a Mersenne prime), then there exists a  $(2^{2r} - 2^r + 1, 2^r - 1, 1, 1)$ -IRS.

*Proof:* Construct a  $(p^2 + p + 1, p + 1, 1)$ -OOC with a single sequence and a  $(p + 1, p, 1)$ -PMD with  $p + 1$  sequences. Applying Theorem 12, we get a  $(p^2 + p + 1, p, 1, 1)$ -IRS. With a simple calculation, it is a  $(2^{2r} - 2^r + 1, 2^r - 1, 1, 1)$ -IRS. We omit the details here.  $\square$

The Johnson bound for a  $(2^{2r} - 2^r + 1, 2^r - 1, 1)$ -IRS is  $2^r + 1$ . The  $(2^{2r} - 2^r + 1, 2^r - 1, 1, 1)$ -IRS constructed is one short of the Johnson bound.

The first Mersenne prime is  $2^2 - 1 = 3$  and the second one is  $2^3 - 1 = 7$ . Here we have an explicit example to show the construction in Theorems 12 and 15.

*Example 5:* The block  $\{0, 1, 5, 7, 17, 35, 49\}$  forms a  $(57, 8, 1)$ -OOC, also known as a  $(57, 8, 1)$  cyclic difference set [10].

We have constructed an  $(8, 7, 1)$ -PMD in Example 4. Then we can construct eight vectors of dimension 7 over  $\mathbb{Z}_{57}$  as follows:

$$\begin{pmatrix} 0 & 1 & 5 & 49 & 7 & 17 & 35 \\ 0 & 5 & 17 & 38 & 35 & 7 & 49 \\ 0 & 7 & 35 & 5 & 38 & 49 & 1 \\ 0 & 17 & 7 & 1 & 49 & 35 & 38 \\ 0 & 35 & 49 & 17 & 1 & 38 & 5 \\ 0 & 38 & 1 & 35 & 17 & 5 & 7 \\ 0 & 49 & 38 & 7 & 5 & 1 & 17 \\ 1 & 7 & 38 & 17 & 49 & 5 & 35 \end{pmatrix}.$$

These eight vectors form a  $(57, 7, 1, 1)$ -IRS.

## VI. CONCLUSION

A general combinatorial model is proposed to study the sequence designs for UWB impulse radios. Several constructions based on Costas arrays, polynomial over finite fields and optical orthogonal codes, are presented.

The construction for  $(N_s, N_f, \lambda_a, \lambda_c)$ -IRS with  $N_s \gg N_f$  is much easier than the case when these two numbers are close. It is still a challenging problem to construct IRSs with optimal correlation for which  $N_s$  and  $N_f$  are very close, such as the best possible  $(N_s, N_s, 1, 1)$ -IRS. The authors believe that such a "perfect" IRS does not exist.

The cases with  $N_s \gg N_f$  are of interest in the context of optical orthogonal codes, since any IRS is also an OOC. So we have given several new constructions for OOCs. All of the constructions given here with  $\lambda_a = \lambda_c = 1$  are *asymptotically optimal*. Refer to [3] for details.

We have not attempted to list all possible parameters of IRSs for which we have constructions. Instead, we emphasize the general models to study IRSs, in order to attract more research interest in the sequence/signal designs for impulse radios.

## REFERENCES

- [1] F. E. Bennett, B. Du, and L. Zhu, "On the existence of  $(v, 7, 1)$ -perfect Mendelsohn designs," *Discr. Math.*, vol. 84, pp. 221–239, 1990.
- [2] R. C. Bose, "An affine analogue of Singer's theorem," *J. Indian Math. Soc.*, vol. 6, pp. 1–15, 1942.
- [3] W. Chu and S. W. Golomb, "A new recursive construction for optical orthogonal codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 3072–3076, Nov. 2003.
- [4] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis and applications," *IEEE Trans. Inform. Theory*, vol. 35, pp. 595–604, May 1989.
- [5] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Comb. Theory*, ser. A, vol. 37, no. 1, pp. 13–21, 1984.
- [6] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proc. IEEE*, vol. 72, pp. 1143–1163, Sept. 1984.
- [7] S. M. Johnson, "A new upper bound for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, Apr. 1962.
- [8] N. S. Mendelsohn, "Perfect cyclic designs," *Discr. Math.*, vol. 20, pp. 63–68, 1977.
- [9] R. A. Scholtz, P. V. Kumar, and C. J. Corrada-Bravo, "Signal design for ultra-wideband radio," in *Sequences and their Applications—SETA'01*, T. Hellesteth, P. Kumar, and K. Yang, Eds. London, U.K.: Springer, 2001, pp. 72–87.
- [10] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1938.
- [11] M. Z. Win and R. A. Scholtz, "Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications," *IEEE Trans. Commun.*, vol. 48, pp. 679–691, Apr. 2002.
- [12] L.-L. Yang, "Residue number system assisted fast frequency-hopped synchronous ultra-wideband spread-spectrum multiple-access: A design alternative to impulse radio," *IEEE J. Select. Areas Commun.*, vol. 20, pp. 1652–1663, Dec. 2002.