Quasi-Orthogonal Sequences for Code-Division Multiple-Access Systems

Kyeongcheol Yang, *Member, IEEE*, Young-Ky Kim, and P. Vijay Kumar, *Member, IEEE*

***Abstract*—In this paper, the notion of *quasi-orthogonal* sequence (QOS) as a means of increasing the number of channels in synchronous code-division multiple-access (CDMA) systems that employ Walsh sequences for spreading information signals and separating channels is introduced. It is shown that a QOS sequence may be regarded as a class of bent (almost bent) functions possessing, in addition, a certain *window property*. Such sequences while increasing system capacity, minimize interference to the existing set of Walsh sequences. The window property gives the system the ability to handle variable data rates. A general procedure of constructing QOS's from well-known families of binary sequences with good correlation, including the Kasami and Gold sequence families, as well as from the binary Kerdock code is provided. Examples of QOS's are presented for small lengths. Some examples of *quaternary* QOS's drawn from Family $\mathcal{A}$ are also included.**

***Index Terms*—Bent functions, code-division multiple-access systems, Gold sequences, Kasami sequences, Kerdock codes, quasi-orthogonal sequences, Walsh sequences.**

I. Introduction

CODE-division multiple-access (CDMA) systems use pseudo-noise binary sequences as signature sequences to distinguish between the signals of different users. Several spread-spectrum communication systems also use them as spreading codes that help achieve a low probability of intercept by spreading the signal energy over a large bandwidth. Desirable characteristics of pseudo-noise binary sequences used for such applications include long-period, low out-of-phase autocorrelation values, low crosscorrelation values, large linear span, symbol balance, low nontrivial partial-period correlation values, large family size, and ease of implementation [7], [10], [20], [22].

Let $a(t), t=0,1,\cdots,N-1$, be a sequence of length $N=2^m$ over $F_2 = \{0,1\}$. We will sometimes identify the sequence with the binary vector $\boldsymbol{a} = (a(0), a(1), \cdots, a(N-1))$. The correlation R_{ab} between two binary sequences $a(t)$ and $b(t)$ of the same length N is given by

$$R_{ab} := \sum_{t=0}^{N-1} (-1)^{a(t)+b(t)}$$

where $a(t)+b(t)$ is computed modulo 2 for all t. It is easily shown that $R_{ab} = N - 2d_H(\boldsymbol{a}, \boldsymbol{b})$ where $d_H(\boldsymbol{a}, \boldsymbol{b})$ denotes the Hamming distance of two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$. Two sequences are said to be *orthogonal* if their correlation is zero.

Let $\mathcal{F} = \{a_i(t) \,|\, i = 1, 2, \cdots, M\}$ be a family of M binary sequences of period N. The family $\mathcal{F}$ is said to be *orthogonal* if any two sequences are mutually orthogonal, that is, $R_{s_i s_j} = 0$ for any i and $j \neq i$. For example, the Walsh sequence family of length 2^m is orthogonal. Where there is no chance of confusion, we will abbreviate and write R_{ij} instead of $R_{s_i s_j}$.

Consider a synchronous system without multipath time dispersion, where a sequence family $\mathcal{F} = \{a_i(t)\}$ is employed to both spread the signal bandwidth as well as distinguish between different users. We consider the case when binary phase-shift keying (BPSK) is used to modulate the signal. Let $d_i(n)$, $n = 0, 1, 2, \cdots$, be the binary information signal of the ith user at the nth information bit time. Then each bit $d_i(n)$ is spread into N chips by the signature sequence $a_i(t)$ of the ith-user channel during the nth information bit time as follows:

$$(-1)^{d_i(n)}(-1)^{a_i(t)}, \qquad t = 0, 1, \cdots N-1.$$

Ignoring noise added to the signal in the channel, the received signal during the nth information bit time is given by

$$r(t) = (-1)^{d_i(n)}(-1)^{a_i(t)} + \sum_{j \neq i} (-1)^{d_j(n)}(-1)^{a_j(t)}, \qquad t = 0, 1, \cdots N-1.$$

The receiver at the output of the ith-user channel computes

$$\begin{aligned} z_i(n) &= \sum_{t=0}^{N-1} r(t)(-1)^{a_i(t)} \\ &= N(-1)^{d_i(n)} + \sum_{j \neq i} (-1)^{d_j(n)} R_{ij}. \end{aligned} \tag{1}$$

If $\mathcal{F}$ is orthogonal, then $z_i(n) = N(-1)^{d_i(n)}$ and $d_i(n)$ can be easily determined from the sign of $z_i(n)$. When $\mathcal{F}$ is not orthogonal, it is necessary to minimize the second term in (1), i.e., the interference from other channels. Since $d_j(n)$ is typically assumed to take on values 0 or 1 with equal likelihood, it is necessary to minimize the absolute value of the correlations R_{ij} between two distinct sequences in $\mathcal{F}$.

Manuscript received November 30, 1998; revised October 22, 1999. This work was supported in part by the Korea Research Foundation for the program year of 1998 and in part by the National Science Foundation under Grant CCR-9612864. The material in this paper was presented in part at the Conference on Difference Sets, Sequences and Their Correlation Properties, Bad Windsheim, Germany, Aug. 2–14, 1998.

K. Yang is with the Department of Electronic and Electrical Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Kyungbuk 790-784, Korea (e-mail: kcyang@postech.ac.kr).

Y. Kim is with Telecommunications R&D Center, Samsung Electronics Co., Pundang P.O. 32, Sungnam, Kyungki-Do 463-050, Korea (e-mail: ykim@metro.telecom.samsung.co.kr).

P. V. Kumar is with Communication Sciences Institute, Electrical Engineering–Systems, University of Southern California, Los Angeles, CA 90089-2565 USA (e-mail: vijayk@usc.edu).

Communicated by S. W. Golomb, Associate Editor for Sequences.

Publisher Item Identifier S 0018-9448(00)02889-3.

CDMA systems such as the IS-95 system employ Walsh sequences of length 64 in the forward link both as spreading sequences and also to separate the different user channels [24]. Since the IS-95 system is synchronous in the forward link, it is the inner product between the vectors associated with different user sequences rather than periodic correlation, that is a measure of interference from other channels. Walsh sequences are perfect in the sense that there is no interference between any pair of sequences, as Walsh sequences form an orthogonal family. However, the orthogonality limits the size of an orthogonal family—there are only 2^m Walsh sequences of length 2^m. For this reason, it is impossible to increase the number of channels without either increasing the sequence length or else losing orthogonality between a pair of user sequences.

There are many situations where it is not appropriate to increase the length of the sequence. A loss in orthogonality is inevitable in such situations and gives rise to interference from other channels. In [1], Bottomley proposed a set of signature sequences drawn from a Kerdock code for a synchronous direct sequence CDMA system where orthogonal spreading is used. However, in this scheme, signature and spreading sequences are different and there is no requirement on correlation between signature sequences over a subblock.

In this paper, the notion of *quasi-orthogonal* sequence (QOS) as a means of increasing the number of channels in synchronous code-division multiple-access (CDMA) systems that employ Walsh sequences for spreading information signals and separating channels is introduced. It is shown that a QOS sequence may be regarded as a class of bent (almost bent) functions possessing, in addition, a certain *window property*. Such sequences while increasing system capacity, minimize interference to the existing set of Walsh sequences. The window property gives the system the ability to handle variable data rates. A general procedure of constructing QOS's from well-known families of binary sequences with good correlation, including the Kasami and Gold sequence families, as well as from the binary Kerdock code is provided. Examples of QOS's are presented for small lengths.

Complex or quaternary sequences, specifically sequences drawn from Family $\mathcal{A}$ [2], [23], in place of binary sequences, were first considered in [5] in order to expand the set of binary Walsh sequences for CDMA systems. In the final part of this paper, the correlation properties in "windows" of the sequences in Family $\mathcal{A}$ are studied. Computer searches were conducted (under a restriction on the subspaces associated with the windows) and used to provide examples of sets of QOS's for all lengths of the form 2^m, $4 \leq m \leq 8$.

The paper is organized as follows. In Section II, we give some preliminaries and introduce the concept of quasi-orthogonal sequences. The properties of a QOS sequence are studied here. In Section III, a general procedure for the construction of QOS's is provided from well-known families including Kasami sequences, Gold sequences, and binary Kerdock codes. Quaternary quasi-orthogonal sequences are discussed in Section IV, and some examples drawn from the Family $\mathcal{A}$ are provided. Finally, concluding remarks and some open problems are given in Section V.

II. Quasi-Orthogonal Sequences

Let m be an integer. For a positive integer $i \leq m$, let $x_i(t)$, $t = 0, 1, \cdots, N-1$, be the sequence of length $N = 2^m$, given by

$$\begin{array}{ll} x_1(t): & 01010101\cdots0101 \\ x_2(t): & 00110011\cdots0011 \\ x_3(t): & 00001111\cdots1111 \\ & \vdots \\ x_m(t): & 00000000\cdots1111. \end{array} \tag{2}$$

The sequences $\{x_i(t) \,|\, i = 1, 2, \cdots, m\}$ are said to be the *canonical* sequences of length 2^m. We will abbreviate and write x_i instead of $x_i(t)$ when there is no chance of confusion.

Any binary sequence $f(t)$ of length 2^m has a Boolean expression of the form

$$f(t) = \sum_{r \in F_2^m} a_r x^r \tag{3}$$

where $r = (r_1, r_2, \cdots, r_m) \in F_2^m$, $a_r \in F_2$, $x^r = x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}$ is a sequence obtained via bitwise multiplication, and the addition of sequences is carried out bitwise modulo 2 [14]. For example, the sequence $\boldsymbol{f} = (01010110)$ of length 8 may be expressed in the form $f(t) = x_1 + x_2 x_3$. With (3) and (2) in mind, we will interchangeably write $f(x_1, x_2, \cdots, x_m)$ in place of $f(t)$.

For any integer i, $0 \leq i \leq 2^m - 1$, we have the binary expansion $i = i_1 + i_2 2 + \cdots + i_m 2^{m-1}$, where $i_1, i_2, \cdots, i_m \in F_2$. Using this expansion, we define $w_i(t)$ to be a linear combination of x_i's, given by

$$w_i(t) = i_1 x_1 + i_2 x_2 + \cdots + i_m x_m. \tag{4}$$

It is not difficult to show that $w_i(t)$ and $w_j(t)$ are mutually orthogonal for any i, j, $j \neq i$. The family $\mathcal{W}_m$, defined by

$$\mathcal{W}_m = \{w_i(t) \,|\, i = 0, 1, \cdots, 2^m - 1; t = 0, 1, \cdots 2^m - 1\} \tag{5}$$

is a complete set of orthogonal sequences of length $N = 2^m$ known as the family of Walsh sequences of length 2^m.

The Walsh family $\mathcal{W}_m$ can be interpreted as a subcode of the first-order Reed–Muller code $\mathcal{R}_m$, where $\mathcal{R}_m$ is given by

$$\mathcal{R}_m = \{c(t) \,|\, c(t) = i_0 x_0 + i_1 x_1 + \cdots + i_m x_m; i_0, i_1, \cdots, i_m \in F_2\}$$

where x_0 is the all-one sequence $(11\cdots1)$ and $\{x_l \,|\, l = 1, 2, \cdots, m\}$ are the canonical sequences of length 2^m, given in (2) (see [14]). In many applications, it is important to find the correlation between a binary sequence of length 2^m and the code sequences in $\mathcal{R}_m$. This correlation is closely related to the determination of a parameter of $\mathcal{R}_m$, known as the *covering radius* $\rho(m)$ given by

$$\rho(m) = \max_{\boldsymbol{v}} \min_{\boldsymbol{c} \in \mathcal{R}_m} d_H(\boldsymbol{v}, \boldsymbol{c}) \tag{6}$$

where $\boldsymbol{v}$ runs through all the binary vectors of length 2^m in $F_2^{2^m}$.

The covering radius $\rho(m)$ of the first-order Reed–Muller code $\mathcal{R}_m$ has been intensively studied [4], [9], [15]. It is well known that $\rho(m) = 2^{m-1} - 2^{(m-2)/2}$ for any even integer m, and

$$2^{m-1} - 2^{(m-1)/2} \leq \rho(m) \leq 2^{m-1} - 2^{(m-2)/2} \qquad (7)$$

for odd integer $m \geq 3$. The known values of $\rho(m)$ equal the lower bound in (7) for $m = 3, 5$, and 7. However, Patterson and Wiedemann [18] have shown that $\rho(m)$ is strictly greater than the lower bound in (7) for any odd integer $m \geq 15$. The determination of the exact value of $\rho(m)$ for odd $m \geq 9$ remains an open problem. Known results on $\rho(m)$ are listed in Table I for small values of m.

In the IS-95 CDMA mobile communication system [24], the Walsh sequences $\mathcal{W}_6$ of length 64 are used in the forward link both to spread the signal bandwidth and to distinguish between the signals of different users. The usage of Walsh sequences limits the number of channels to the size $|\mathcal{W}_m|$ of the Walsh sequence family which is equal to the length of the sequences in the family. The size of a Walsh sequence family cannot be increased while maintaining orthogonality between pairs of sequences because there can be no greater than 2^m pairwise orthogonal sequences of length 2^m.

The increasing demand for more service makes it desirable to increase the size of the sequence family. Our goal is to do precisely this while keeping the interference introduced by the additional sequences as small as possible. Note that since the CDMA system is assumed to be synchronous, it is the inner product between pairs of sequences rather than periodic correlation that is the relevant measure of interference.

Consider first, the situation where a single sequence $f(t)$ of length $N = 2^m$ is added to the Walsh sequence family $\mathcal{W}_m$. We define $R_{\max}(f)$ to be the maximum correlation between $f(t)$ and the sequences in $\mathcal{W}_m$, given by

$$R_{\max}(f) = \max_{i_0, w_i(t)} \left| \sum_{t=0}^{N-1} (-1)^{f(t)+i_0+w_i(t)} \right|$$

where i_0 takes on 0 or 1, and $w_i(t)$ runs through $\mathcal{W}_m$. The factor $(-1)^{i_0}$ is introduced to account for the effect of data modulation upon the inner product. Let $\theta_{\min}(N)$ be the minimum achievable correlation value, given by

$$\theta_{\min}(N) = \min_f R_{\max}(f) \qquad (8)$$

where $f(t)$ runs through all sequences of length 2^m. Then the maximum interference introduced to the existing Walsh family $\mathcal{W}_m$ is at least $\theta_{\min}(N)$ for any sequence $f(t)$ of length $N = 2^m$ that is used to augment the family $\mathcal{W}_m$. Our next step is to determine $\theta_{\min}(2^m)$.

Proposition 1: Let $\rho(m)$ be the covering radius of the first-order Reed–Muller code $\mathcal{R}_m$ of length 2^m. Then we have $\theta_{\min}(2^m) = 2^m - 2\rho(m)$. Moreover, we have $\theta_{\min}(2^m) = 2^{m/2}$ for any even integer m, and

$$2^{m/2} \leq \theta_{\min}(2^m) \leq 2^{(m+1)/2}$$

for any odd integer m.

TABLE I
THE COVERING RADIUS OF THE FIRST-ORDER REED–MULLER CODE $\mathcal{R}_m$ FOR SMALL VALUES OF m

$\rho(2) = 1$	$\rho(7) = 56$
$\rho(3) = 2$	$\rho(8) = 120$
$\rho(4) = 6$	$240 \leq \rho(9) \leq 244$
$\rho(5) = 12$	$\rho(10) = 496$
$\rho(6) = 28$	$992 \leq \rho(11) \leq 1002$

TABLE II
$\theta_{\min}(2^m)$ FOR SMALL VALUES OF m

$N = 2^m$	$\theta_{\min}(2^m)$	$N = 2^m$	$\theta_{\min}(2^m)$
4	2	128	16
8	4	256	16
16	4	512	32*
32	8	1024	32
64	8	2048	64*

Proof: Let $f(t) \in F_2^N$ be a sequence of length $N = 2^m$ and let $c(t)$ be a codeword of $\mathcal{R}_m$ with $d_H(f(t), c(t)) = 2^{m-1} - \Delta$, where $d_H(f(t), c(t))$ denotes the Hamming distance between $f(t)$ and $c(t)$ of length N. Then $1 + c(t)$ is also a codeword with $d_H(f(t), 1 + c(t)) = 2^{m-1} + \Delta$, since the all-one vector is a codeword in $\mathcal{R}_m$. Therefore,

$$\max_{c(t) \in \mathcal{R}_m} \left| \sum_{t=0}^{N-1} (-1)^{f(t)+c(t)} \right| = 2^m - 2 \min_{c(t) \in \mathcal{R}_m} d_H(f(t), c(t)).$$

From the definitions in (6) and (8), we have

$$\begin{aligned} \theta_{\min}(2^m) &= \min_{f(t) \in F_2^N} \max_{c(t) \in \mathcal{R}_m} \left| \sum_{t=0}^{N-1} (-1)^{f(t)+c(t)} \right| \\ &= \min_{f(t)} \left(2^m - 2 \min_{c(t)} d_H(f(t), c(t)) \right) \\ &= 2^m - 2 \max_{f(t)} \min_{c(t)} d_H(f(t), c(t)) \\ &= 2^m - 2\rho(m). \end{aligned}$$

The proposition now follows from the well-known results on $\rho(m)$, including (7). □

Proposition 1 tells us that determining $\theta_{\min}(2^m)$ is equivalent to determining the covering radius $\rho(m)$ of the first-order Reed–Muller code of length 2^m. For small values of m, $\theta_{\min}(2^m)$ is listed in Table II, in which a * denotes an upper bound on $\theta_{\min}(2^m)$.

For an even integer m, a binary-valued function $f(t)$ of length 2^m is said to be *bent* if the correlation R_{fw} between $f(t)$ and any sequence $w(t)$ in $\mathcal{W}_m$ has magnitude $2^{m/2}$ [10], [14], [19]. In the case of an odd integer m, there are no bent functions of length 2^m since $2^{m/2}$ is not an integer. Instead, for an odd integer m, a binary-valued function $f(t)$ of length 2^m will be said to be *almost bent* if the correlation R_{fw} between $f(t)$ and any sequence $w(t)$ in $\mathcal{W}_m$ has magnitude $\leq 2^{(m+1)/2}$ (cf. [3]).

We are now in a position to introduce the concept of quasi-orthogonal sequence.

Definition 2: Let $\mathcal{W}_m = \{w_j(t) \,|\, j = 0, 1, \cdots, 2^m - 1\}$ be the Walsh family of length 2^m, given by (5). A family $\mathcal{F} = \{f_i(t) \,|\, i = 1, 2, \cdots, M\}$ of M sequences of length $N = 2^m$ is said to be *quasi-orthogonal* if the following are satisfied:

a) $\mathcal{F}$ contains $\mathcal{W}_m$.
b) $|R_{ij}| \leq \theta_{\min}(N)$ for any i and j $(\neq i)$.
c) For any $f(t) \in \mathcal{F}\backslash\mathcal{W}_m$, any $w(t) \in \mathcal{W}_m$, and any integers L, r, where $L = 2^l$, $2 \leq l \leq m$, and $0 \leq r \leq N/L - 1$

$$\left| \sum_{t=rL}^{rL+L-1} (-1)^{f(t)+w(t)} \right| \leq \theta_{\min}(L).$$

Remark 3: When m is an odd integer ≥ 9, we use the upper bound $2^{(m+1)/2}$ instead of the exact value of $\theta_{\min}(2^m)$, since $\theta_{\min}(2^m)$ is unknown.

Condition b) for quasi-orthogonality requires that the correlation between any two distinct sequences in $\mathcal{F}$ should be as small as possible. Conditions a) and b) imply that any sequence in $\mathcal{F}\backslash\mathcal{W}_m$ should cause minimal possible interference to the existing Walsh family, i.e., $|R_{fw}| \leq \theta_{\min}(N)$ for any $f(t) \in \mathcal{F}\backslash\mathcal{W}_m$ and $w(t) \in \mathcal{W}_m$. This requires that any $f(t) \in \mathcal{F}$ not belonging to $\mathcal{W}_m$ should be either bent or almost bent depending on m.

Condition c), which we will refer to as the *window property*, requires that when any sequence $f(t) \in \mathcal{F}\backslash\mathcal{W}_m$ is divided into N/L consecutive subblocks of length $L = 2^l$, $2 \leq l \leq m$, the *partial correlation* between $f(t)$ and $w(t)$ over every subblock be as small as possible for any $w(t) \in \mathcal{W}_m$. Since every subblock of length L in $\mathcal{W}_m$ corresponds to a sequence in $\mathcal{R}_l$, the condition requires that every consecutive subblock of $s(t)$ corresponds either to a bent or almost bent function of length L, depending on L. This requirement is motivated by practical applications, where repeating a sequence in $\mathcal{W}_{m-1}$ twice yields a sequence in $\mathcal{W}_m$, and therefore all sequences in $\mathcal{W}_{m-1}$ can be used for the transmission of data at twice the normal data rate. In such a situation, Condition c) is necessary to ensure minimum possible interference to the higher data rate users who will employ correlation over a window of size 2^{m-1} rather than 2^m.

Remark 4: In terms of Boolean expressions, the window property in part c) of Definition 2 can be reformulated as follows: If $f(t) \in \mathcal{F}\backslash\mathcal{W}_m$, then

$$f(x_1, x_2, \cdots, x_m)|_{x_{l+1}=a_{l+1}, x_{l+2}=a_{l+2}, \cdots, x_m=a_m}$$

should be a bent or almost bent function of length 2^l for any $a_{l+1}, a_{l+2}, \cdots, a_m \in F_2$, where $2 \leq l \leq m$.

Example 5: Consider the canonical sequences of length 4, given by

$$\begin{aligned} x_1(t): &\quad 0 \quad 1 \quad 0 \quad 1 \\ x_2(t): &\quad 0 \quad 0 \quad 1 \quad 1. \end{aligned}$$

Then the Walsh sequence of length 4 is

$$\mathcal{W}_2 = \{(0000), (0101), (0011), (1010)\}.$$

It is easily checked that

$$\mathcal{F} = \mathcal{W}_2 \cup \{(0001), (0100), (0010), (1011)\}$$

satisfies the Conditions a), b), and c), and therefore is quasi-orthogonal.

Lemma 6: Let $f(t)$ be a bent (almost bent) function of length 2^m with the window property. Let

$$f(t) + \mathcal{W}_m = \{f(t) + w_i(t) \,|\, i = 0, 1, \cdots, N - 1\}.$$

Then the set $\mathcal{F} = \mathcal{W}_m \cup (f(t) + \mathcal{W}_m)$ is quasi-orthogonal.

Proof: For any $w(t)$, $f(t) + w(t)$ is also a bent (almost bent) function of length 2^m. It also has the window property. Furthermore, $f(t) + w_i(t)$ and $f(t) + w_j(t)$ are orthogonal for any i and j $(\neq i)$, since $w_i(t)$ and $w_j(t)$ are orthogonal. □

It will be convenient to define an equivalence relation between Boolean functions of length 2^m in terms of the first-order Reed–Muller code $\mathcal{R}_m$.

Definition 7: Two binary-valued Boolean functions $f(t)$ and $g(t)$ of the same length 2^m are said to be *equivalent* (with respect to $\mathcal{R}_m$) if $f(t) - g(t) \in \mathcal{R}_m$; in other words, $f(t) - g(t)$ is a linear combination of the canonical sequences and the all-one sequence of length 2^m. Otherwise, they are said to be *inequivalent* (with respect to $\mathcal{R}_m$).

The following is a direct consequence of Lemma 6 and Definition 7.

Theorem 8: Let $f_1(t), f_2(t), \cdots, f_k(t)$ be k inequivalent bent (almost bent) functions of length $N = 2^m$ with the window property. If $f_i(t) + f_j(t)$ is also bent (almost bent) for any i and j, $i \neq j$, then the set

$$\mathcal{F} = \bigcup_{i=0}^{k} (f_i(t) + \mathcal{W}_m)$$

is quasi-orthogonal, where $f_0(t) = 0$. Furthermore, the size of $\mathcal{F}$ is $(k + 1) \cdot 2^m$.

Any quasi-orthogonal sequence (QOS) $\mathcal{F}$ constructed from Theorem 8 consists of $k + 1$ cosets of $\mathcal{W}_m$. Note that $f_0(t), f_1(t), \cdots, f_k(t)$ are the coset leaders in $\mathcal{F}$ with respect to $\mathcal{W}_m$. Since any sequence $f(t)$ in $\mathcal{F}$ can be expressed as $f(t) = f_i(t) + w_j(t)$ for some $f_i(t)$ and $w_j(t)$, the k nonzero functions $f_1(t), f_2(t), \cdots, f_k(t)$ are often called the *masking functions* of $\mathcal{F}$ in practical applications. In order to maximize the size of $\mathcal{F}$, it is necessary to maximize k. The definition below relates to the maximum possible value of k.

Definition 9: Let Γ be the ensemble of sets $\mathcal{S}$ of inequivalent functions of length 2^m (with respect to $\mathcal{R}_m$) such that

a) any function in $\mathcal{S}$ is bent (almost bent);
b) the sum of any two functions is also bent (almost bent);
c) any function in $\mathcal{S}$ has the window property.

The number $k_{\max}(m)$ is defined to be the maximum of $|\mathcal{S}|$ where $\mathcal{S}$ runs through Γ, that is,

$$k_{\max}(m) = \max_{\mathcal{S} \in \Gamma} |\mathcal{S}|.$$

It is well known [14, Corollary 11, p. 429] that

$$f(x_1, x_2, \cdots, x_m) = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$$

is bent, for any even $m \geq 2$. It is easily checked that this function has the window property. It follows from this and the theorem below that there exists at least one bent (almost bent) function of length 2^m with the window property, i.e.,

$$k_{\max}(m) \geq 1 \tag{9}$$

for any integer $m \geq 2$.

Theorem 10: For any positive integer m, we have

$$k_{\max}(2m) \leq k_{\max}(2m+1).$$

Proof: Let $\mathcal{S}$ be a set of inequivalent functions of length 2^{2m} satisfying the conditions given in Definition 9, which achieves $k_{\max}(2m)$. Then any function $f(t)$ in $\mathcal{S}$ can be considered as a bent function $f(x_1, x_2, \cdots, x_{2m})$. Now let $\hat{f} = (f\|f)$ be a concatenation of f and f, which is of length 2^{2m+1}. In the notation of Boolean functions, we have

$$\hat{f}(x_1, x_2, \cdots, x_{2m}, x_{2m+1}) = f(x_1, x_2, \cdots, x_{2m}).$$

The theorem follows from the fact that $\hat{f}$ is almost bent, since

$$\begin{aligned}\left|\sum_{x\in F_2^{2m+1}} (-1)^{\hat{f}(x)+c(x)}\right| &\leq \left|\sum_x (-1)^{\hat{f}(x)+c(x)}\right|_{x_{2m+1}=0} \\ &\quad + \left|\sum_x (-1)^{\hat{f}(x)+c(x)}\right|_{x_{2m+1}=1} \\ &\leq 2^m + 2^m = 2^{m+1}\end{aligned}$$

for any $c(x) \in \mathcal{R}_{2m+1}$. □

It is quite interesting to determine $k_{\max}(m)$ exactly, but this does not appear to be an easy problem. For small values of m, it can be checked that $k_{\max}(2) = 1$, $k_{\max}(3) = 4$, $k_{\max}(4) = 4$. In the following section, we know from a computer search that $k_{\max}(5) \geq 10$, $k_{\max}(6) \geq 8$, $k_{\max}(7) \geq 22$, $k_{\max}(8) \geq 20$, $k_{\max}(9) \geq 48$, etc.

Example 11: In the case of $m = 4$, consider the set $\mathcal{S}$ of four inequivalent bent functions of length 16, given by

$$\begin{aligned}f_1(t) &= x_1x_2 + x_3x_4, \\ f_2(t) &= x_1x_2 + x_1x_4 + x_2x_3 \\ f_3(t) &= x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 \\ f_4(t) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4.\end{aligned}$$

Note that $f_i(t)$ has the window property and $f_i(t) + f_j(t)$ are also bent for any i and j $(\neq i)$, Hence the set

$$\bigcup_{i=0}^{4} (f_i(t) + \mathcal{W}_4)$$

is quasi-orthogonal, where $f_0(t) = 0$.

III. Quasi-Orthogonal Sequences from Known Families

In Section II, QOS's are defined and their existence is verified for any length 2^m in (9). A natural question at this stage is to find an efficient way to construct QOS's. In this section we give a systematic procedure to construct QOS's from known families with good correlation properties, including Gold sequences, Kasami sequences, and Kerdock codes.

A. Construction of QOS's from Known Sequences with Optimal Correlation

Consider a family $\mathcal{S} = \{s_i(t) \,|\, i = 0, 1, \cdots, M-1\}$ of M binary sequences of period $N = 2^m - 1$, satisfying the following conditions.

a) An m-sequence of period N belongs to $\mathcal{S}$ (Here, $s_0(t)$ is usually assumed to be an m-sequence).
b) Any two sequences are cyclically distinct, that is, for any i and j $(\neq i)$ there does not exist τ, $0 < \tau < N$, such that $s_i(t+\tau) = s_j(t)$ for all t, $t = 0, 1, \cdots, N-1$.
c) When 1 is added to the out-of-phase auto- and crosscorrelation values, the result has magnitude $\leq 2^{\lfloor (m+1)/2 \rfloor}$, i.e.,

$$\left|1 + \sum_{i=0}^{N-1} (-1)^{s_i(t+\tau)+s_j(t)}\right| \leq 2^{\lfloor (m+1)/2 \rfloor}$$

for all i, j, τ except for $i = j$ and $\tau = 0 \pmod N$. Here $\lfloor r \rfloor$ is the largest integer less than or equal to r.

Our goal is to construct a quasi-orthogonal sequence $\mathcal{F}$ from $\mathcal{S}$. Since the Walsh sequence $\mathcal{W}_m$ is obtained by permuting $s_0(t)$ and its shifts properly, $\mathcal{W}_m$ is included in $\mathcal{F}$ by the Condition a). Condition b) allows $s_i(t)$ to be the coset leaders in $\mathcal{F}$ with respect to $\mathcal{W}_m$, if properly permuted. Condition c) guarantees that $s_i(t)$ is bent (almost bent) for any $i \geq 1$, and $s_i(t) + s_j(t)$ is also bent (almost bent), if properly defined. The remaining work is to check if $s_i(t)$ has the window property.

Algorithm $\mathcal{I}$ to Construct a QOS $\mathcal{F}$ from a Given Family $\mathcal{S}$

(A.1) Using an m-sequence $s_0(t)$, we define a mapping σ : $\{0, 1, \cdots, 2^m - 2\} \to \{1, 2, \cdots, 2^m - 1\}$, given by

$$\sigma(t) = \sum_{i=0}^{m-1} s_0(t+i)\, 2^{m-1-i}.$$

(A.2) For each i, $i = 1, 2, \cdots, M-1$, we define a sequence $e_i(t)$, $t = 0, 1, \cdots, 2^m - 1$, of length 2^m by

$$e_i(t) = \begin{cases} 0, & \text{if } t = 0 \\ s_i(\sigma^{-1}(t)), & \text{if } t = 1, 2, \cdots, 2^m - 1 \end{cases}$$

where σ^{-1} is the inverse mapping of σ.

(A.3) Choose all sequences $e_i(t)$ having the window property, and call them $f_1(t)$, $f_2(t), \cdots, f_k(t)$. Define

$$\mathcal{F} = \bigcup_{i=0}^{m} (f_i(t) + \mathcal{W}_m)$$

where $f_0(t) = 0$. Then the family $\mathcal{F}$ is a quasi-orthogonal sequence of size $(k+1) \cdot 2^m$. □

Let m be an integer and let F_{2^m} be a finite field of 2^m elements. The trace function $\mathrm{Tr}_m(\cdot)$ is a mapping from F_{2^m} to F_2, given by

$$\mathrm{Tr}_m(x) = \sum_{i=0}^{m-1} x^{2^i}.$$

Every primitive element α in F_{2^m} is associated with an m-sequence $c(t)$ of length 2^m-1, via $c(t) = \mathrm{Tr}_m(a\alpha^t)$ for $a \in F_{2^m}$. (See [13] for more details.)

For an even integer m, let $b(t)$ be a sequence decimated from $c(t)$ by $2^{m/2}+1$, that is,

$$b(t) = c((2^{m/2}+1)t + \Delta)$$

where $0 \le \Delta \le 2^{m/2}$ and Δ is chosen so that $b(t)$ is not the all-zero sequence. Note that $b(t)$ is an m-sequence of period $2^{m/2}-1$. The small set $K(m)$ of Kasami sequences can be defined as

$$K(m) = \{c(t) + b(t+\tau) \,|\, 0 \le \tau < 2^{m/2}-1\} \cup \{c(t)\}. \quad (10)$$

Note that the size of $K(m)$ is $2^{m/2}$. (See [10], [20], or [22] for details.)

Proposition 12: The out-of-phase autocorrelation and cross-correlation between sequences of the Kasami sequence $K(m)$ in (10) take on three values: -1, $-1 \pm 2^{m/2}$.

Example 13: For an even integer m, the Kasami sequence $K(m)$ in (10) can be used to construct quasi-orthogonal sequences of length 2^m by Proposition 12. Put $s_0(t) = c(t)$, $s_i(t) = c(t) + b(t+i)$ for $1 \le i \le 2^{m/2}-1$, and apply Algorithm $\mathcal{I}$ described above to $s_i(t)$.

For an odd integer m, let r be an integer relatively prime to m. Let $b(t)$ be a sequence decimated by 2^r+1 from an m-sequence $c(t)$ of length 2^m-1, that is,

$$b(t) = c((2^r+1)t).$$

The Gold sequence can be defined as

$$G(m) = \{c(t) + b(t+\tau) \,|\, 0 \le \tau < 2^m - 1\} \cup \{c(t), b(t)\}. \quad (11)$$

Note that $G(m)$ is a family of size 2^m+1. (See [10], [20], or [22] for details.)

Proposition 14: The out-of-phase autocorrelation and cross-correlation between sequences of the Gold sequence $G(m)$ in (11) take on three values: -1, $-1 \pm 2^{(m+1)/2}$, where m is odd.

Example 15: For an odd integer m, the Gold sequence $G(m)$ in (11) can be used to construct quasi-orthogonal sequences of length 2^m by Proposition 12. Put

$$\begin{aligned} s_0(t) &= c(t), \\ s_i(t) &= c(t) + b(t+i), \qquad \text{for } 1 \le i \le 2^m - 1 \\ s_{2^m}(t) &= b(t) \end{aligned}$$

and apply Algorithm $\mathcal{I}$ to $s_i(t)$.

B. Construction of QOS's from Binary Kerdock Codes

Let m be an even integer ≥ 4. Note that $m-1$ is odd. For simplicity, let $\sigma_1(x) = \mathrm{Tr}_{m-1}(x)$, and let $\sigma_2(x)$ be the quadratic form given by

$$\sigma_2(x) = \sum_{i=1}^{(m-2)/2} \mathrm{Tr}_{m-1}\left(x^{1+2^i}\right).$$

The binary Kerdock code $\mathcal{K}_2(m)$ of length 2^m can be described as

$$\mathcal{K}_2(m) = \left\{(c_x)_{x \in F_{2^{m-1}}} \,|\, \gamma, \eta \in F_{2^{m-1}}, c_0, c_1 \in F_2\right\}$$

where $c_x = (l(x), r(x))$ and

$$\begin{aligned} l(x) &= \sigma_2(\gamma x) + \sigma_1(\eta x) + c_1 \\ r(x) &= \sigma_2(\gamma x) + \sigma_1(\eta x) + \sigma_1(\gamma x) + (c_0 + c_1). \end{aligned}$$

It is shown in [8] that the binary Kerdock code $\mathcal{K}_2(m)$ can be described as the image of the Gray map of a linear code over a quaternary alphabet. The weight distribution of $\mathcal{K}_2(m)$ is well known [14].

Proposition 16: For even $m \ge 4$, let A_i be the number of codewords of weight i in the binary Kerdock code $\mathcal{K}_2(m)$ of length 2^m. Then

$$A_i = \begin{cases} 1, & \text{for } i = 0 \text{ or } 2^m \\ 2^m(2^{m-1}-1), & \text{for } i = 2^{m-1} \pm 2^{(m-2)/2} \\ 2^{m+1}-2, & \text{for } i = 2^{m-1} \end{cases}$$

In order to express $l(x)$ and $r(x)$ in a unified way, we introduce a variable $x_1 \in F_2$ and put $c_x := c(x, x_1)$, where

$$c(x, x_1) = Q_\gamma(x, x_1) + L_{\eta, c_0, c_1}(x, x_1) \quad (12)$$

where

$$Q_\gamma(x, x_1) := \sigma_2(\gamma x) + x_1 \sigma_1(\gamma x)$$

is the quadratic part of $c(x, x_1)$, and

$$L_{\eta, c_0, c_1}(x, x_1) := \sigma_1(\eta x) + c_0 x_1 + c_1$$

is the linear part of $c(x, x_1)$. This implies that if we take $\gamma = 0$ in $c(x, x_1)$, we get all codewords of the first-order Reed–Muller code $\mathcal{R}_m$ by proper permutation of $L_{\eta, c_0, c_1}(x, x_1)$ using $\sigma_1(\eta x)$ as in Algorithm $\mathcal{A}$. Thus the Kerdock code $\mathcal{K}_2(m)$ consists of 2^{m-1} cosets of $\mathcal{R}_m$, corresponding to the forms $Q(x, x_1)$ depending on γ.

Let $\{\gamma_2, \gamma_3, \cdots, \gamma_m\}$ be a basis for $F_{2^{m-1}}$ over F_2. Then every element $x \in F_{2^{m-1}}$ can be expressed as

$$x = \sum_{i=2}^{m} \gamma_i x_i \quad (13)$$

where $x_i \in F_2$ for $i = 2, 3, \cdots, m$. Using this expression, we put

$$f_\gamma(x_1, x_2, \cdots, x_m) := Q_\gamma(x, x_1).$$

From the weight distribution of $\mathcal{K}_2(m)$ in Proposition 16, it is easily checked that $f_\gamma(x_1, x_2, \cdots, x_m)$ is a bent function of length 2^m and that for any γ_1 and γ_2 $(\neq\gamma_1)$

$$f_{\gamma_1}(x_1, x_2, \cdots, x_m) + f_{\gamma_2}(x_1, x_2, \cdots, x_m)$$

is also bent. These facts give a way to construct QOS's from binary Kerdock codes, if we properly choose bent functions with window property from them.

Lemma 17: There are 2^{m-2} inequivalent bent functions from the Kerdock code $\mathcal{K}_2(m)$, which have the window property of size 4.

Proof: There are 2^{m-1} inequivalent bent functions $f_\gamma(x_1, x_2, \cdots, x_m)$ in $\mathcal{K}_2(m)$. From (13) and linearity of the trace function, we have

$$\begin{aligned} &f_\gamma(x_1, x_2, \cdots, x_m) \\ &\quad = \sigma_2\left(\gamma\sum_{i=2}^{m}\gamma_i x_i\right) + x_1\sigma_1\left(\gamma\sum_{i=2}^{m}\gamma_i x_i\right) \\ &\quad = \mathrm{Tr}_{m-1}(\gamma\gamma_2)x_1x_2 + x_2 g_1(x_3, \cdots, x_m) + g_2(x_3, \cdots, x_m) \end{aligned}$$

where $g_1(x_3, \cdots, x_m)$ is a linear function and $g_2(x_3, \cdots, x_m)$ is a quadratic function. Therefore, $f_\gamma(x_1, x_2, \cdots, x_m)$ is a bent function of length 4 for any fixed value

$$(x_3, \cdots, x_m) = (a_3, \cdots, a_m)$$

if and only if it has the term x_1x_2, that is, $\mathrm{Tr}_{m-1}(\gamma\gamma_2) \neq 0$. There are exactly 2^{m-2} such γ's in $F_{2^{m-1}}$ for a fixed γ_2. □.

The lemma implies that the number of inequivalent bent functions of length 2^m with window property, which can be obtained from the Kerdock code $\mathcal{K}_2(m)$, is at most 2^{m-2}.

C. Simulation Results for QOS's from Known Families

Computer simulations were done to find QOS's of length 2^m from known families. For even m, Kasami sequences and Kerdock codes can be used. In general, it is possible to get larger QOS's from the Kerdock codes than those from Kasami sequences. For example, there are 4, 8, and 20 inequivalent bent functions with window property from Kerdock codes in the case of $m = 4, 6, 8$, respectively, while there are 2, 3, and 6 such functions from Kasami sequences in each case. It may be natural because there are more candidates for inequivalent bent functions with window property in the case of Kerdock codes (2^{m-1} candidates) than $2^{m/2}$ candidates in Kasami sequences. For an odd integer m, the Gold sequence $G(m)$ in (11) has 2^m candidates for inequivalent almost bent functions with window property.

In Tables III–V, inequivalent bent (almost bent) functions with window property (called masking functions) for QOS's are listed for small values of m, which are of importance in practical systems. In Tables IV and V, ij implies that the term x_ix_j belongs to the masking function in its Boolean expression. Gold sequences have been used in the case of odd integers m, Kerdock codes have been used in the case of even integers m. An interesting point in these simulations is that the maximum number k of inequivalent bent (almost bent) functions from these families depends on the choice of an m-sequence $c(t)$ or the choice of primitive elements.

IV. Quaternary Quasi-Orthogonal Sequences

When a CDMA communication system uses QPSK (quadrature phase-shift keying) modulation instead of BPSK (binary phase-shift keying) modulation, it is natural to use quadrature phase sequences as signature sequences rather than binary sequences and this is the approach taken in [5]. Also, as pointed out in [5], when it is desired to expand the set of binary Walsh functions currently used on the forward link of the IS-95 CDMA system, one advantage using quaternary rather than binary sequences to augment the family is that the maximum full-period correlation between a Walsh function and a new sequence belonging to the augmented set, is lower in the quaternary case by a factor of $\sqrt{2}$ for the case when the full period is of the form 2^m, m odd.

For these reasons, we investigate in this paper, the question of whether it is possible to construct a QOS family (i.e., a family that in addition to full-period correlation, also enjoys good correlation properties in every window) that consists of binary Walsh sequences and quaternary sequences. From the theory of quaternary sequences, a natural candidate to use is the sequences set known as Family $\mathcal{A}$ [2], [23]. These sequences were also the basis of the quaternary sequences studied in [5], where the focus was on the full-period correlation properties.[1]

The construction of quaternary QOS's from sequences in Family $\mathcal{A}$ depends on the choice of certain subspaces of a finite field. The results of an exhaustive search conducted over a subset of all possible choices of subspaces are presented in this section.

A. Definition of Quaternary Quasi-Orthogonal Sequences

Let $Z_4 = \{0, 1, 2, 3\}$ be the ring of integers modulo 4. A sequence $a(t), t = 0, 1, \cdots, N-1$ is called a *quaternary* sequence of length N if $a(t) \in Z_4$ for all t. The correlation between two quaternary sequences $a(t)$ and $b(t)$ of the same length N is given by

$$R_{ab} := \sum_{t=0}^{N-1}\omega^{a(t)}\left(\omega^{b(t)}\right)^* = \sum_{t=0}^{N-1}\omega^{a(t)-b(t)}$$

where * denotes complex conjugation, $a(t) - b(t)$ is computed modulo 4 for each t, and ω is a primitive fourth root of unity, that is, $\omega = \sqrt{-1}$. Two sequences are said to be *orthogonal* if their correlation is zero.

The following result is well-known from the theory of orthogonal transforms. As a special case, it gives a lower bound on the maximum of coefficients of the Walsh transform.

[1]At the time of initial writing of this paper, the authors were unware of [21], where the QOS properties of Family $\mathcal{A}$ are also considered and some methods of construction provided. However, the techniques used there and the sequences presented are distinct from ours.

TABLE III
MASKING FUNCTIONS FOR QOS'S OF LENGTH 2^m

m	Nonzero Masking Functions of Length 2^m
3	$f_1 = x_1x_2$
	$f_2 = x_1x_2 + x_1x_3$
	$f_3 = x_1x_2 + x_2x_3$
	$f_4 = x_1x_2 + x_1x_3 + x_2x_3$
4	$f_1 = x_1x_2 + x_1x_3 + x_2x_3 + x_3x_4$
	$f_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4$
	$f_3 = x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4$
	$f_4 = x_1x_2 + x_1x_4 + x_3x_4$
5	$f_1 = x_1x_2 + x_2x_4 + x_3x_4$
	$f_2 = x_1x_2 + x_1x_5 + x_2x_5 + x_3x_4 + x_4x_5$
	$f_3 = x_1x_2 + x_1x_4 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_5$
	$f_4 = x_1x_2 + x_1x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5$
	$f_5 = x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5$
	$f_6 = x_1x_2 + x_1x_3 + x_2x_4 + x_2x_5 + x_3x_5$
	$f_7 = x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 + x_2x_5 + x_4x_5$
	$f_8 = x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5 + x_4x_5$
	$f_9 = x_1x_2 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_3x_5$
	$f_{10} = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_3x_5$
6	$f_1 = x_1x_2 + x_1x_3 + x_1x_5 + x_2x_4 + x_2x_6 + x_4x_5$
	$f_2 = x_1x_2 + x_1x_5 + x_1x_6 + x_2x_3 + x_2x_5 + x_3x_4 + x_3x_6 + x_4x_6 + x_5x_6$
	$f_3 = x_1x_2 + x_1x_3 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_6 + x_4x_5 + x_4x_6 + x_5x_6$
	$f_4 = x_1x_2 + x_1x_4 + x_1x_5 + x_1x_6 + x_2x_3 + x_2x_6 + x_5x_6$
	$f_5 = x_1x_2 + x_1x_6 + x_2x_5 + x_2x_6 + x_3x_4$
	$f_6 = x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6 + x_2x_3 + x_2x_5 + x_2x_6 + x_3x_5 + x_3x_6 + x_4x_6$
	$f_7 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_2x_5 + x_2x_6 + x_3x_6 + x_4x_6 + x_5x_6$
	$f_8 = x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_2x_6 + x_3x_4 + x_4x_5 + x_5x_6$

Proposition 18: Let $\boldsymbol{z} = (z_0, z_1, \cdots, z_{L-1})$ be a complex vector with $|\boldsymbol{z}| = 1$ and let $\boldsymbol{y} = U\boldsymbol{z}$, where U is an $L \times L$ unitary matrix, i.e., $U^H U = I$. Then

$$\max_i |y_i| \geq \frac{1}{\sqrt{L}}.$$

Proof: Note that the maximum of $|y_i|^2$ is at least the average of $|y_i|^2$. It is easily checked that the average of $|y_i|^2$ is equal to $1/L$. □

Corollary 19: Let $a(t)$ be a quaternary sequence of length $N = 2^m$ and let $\mathcal{W}_m$ be the binary Walsh sequence of the same length. Then the maximum of absolute correlation values between $a(t)$ and any $w(t)$ in $\mathcal{W}_m$ is at least $\sqrt{2^m}$, that is,

$$\max_{w(t)\in\mathcal{W}_m} |R_{aw}| \geq \sqrt{2^m}$$

where

$$R_{aw} = \sum_{t=0}^{N-1} \omega^{a(t)}(-1)^{w(t)}.$$

Using the relation $\omega^2 = -1$, for any binary sequence $b(t)$, the correlation becomes

$$R_{ab} = \sum_{t=0}^{N-1} \omega^{a(t)}(-1)^{b(t)} = \sum_{t=0}^{N-1} \omega^{a(t)+2b(t)}$$

where $a(t) + 2b(t)$ is computed modulo 4, so $b(t)$ can be regarded as a special case of quaternary sequence, which we will denote by $2b(t)$. Note that $2b(t)$ takes on two values: 0 or 2. For an integer m, it is natural to identify the binary Walsh sequence $\mathcal{W}_m$ with the set $2\mathcal{W}_m$ over Z_4, given by

$$2\mathcal{W}_m = \{2w(t) \,|\, w(t) \in \mathcal{W}_m\}.$$

TABLE IV
MASKING FUNCTIONS FOR QOS' S OF LENGTH 128 ($m = 7$)

f_1: 12, 13, 14, 23, 25, 27, 35, 36, 37, 45, 46, 56, 57
f_2: 12, 13, 14, 16, 17, 23, 24, 25, 26, 27, 34, 35, 36, 37, 47, 56, 57, 67
f_3: 12, 13, 14, 15, 16, 17, 26, 34, 35, 36, 37, 45, 46, 47, 67
f_4: 12, 17, 25, 34, 35, 36, 45, 46, 56
f_5: 12, 13, 15, 16, 17, 23, 25, 34, 36, 37, 45, 67
f_6: 12, 15, 23, 34, 37, 45, 47, 56, 67
f_7: 12, 13, 17, 23, 25, 26, 27, 34, 35, 36, 37, 45, 56, 67
f_8: 12, 13, 15, 16, 17, 24, 27, 56, 67
f_9: 12, 14, 16, 25, 27, 34, 37, 45, 46, 67
f_{10}: 12, 14, 15, 17, 24, 25, 26, 27, 34, 36, 46, 47, 57
f_{11}: 12, 15, 16, 24, 25, 26, 34, 35, 37, 46, 47, 56, 57, 67
f_{12}: 12, 14, 16, 17, 24, 25, 34, 35, 36, 46, 47, 56, 57
f_{13}: 12, 13, 15, 23, 24, 25, 26, 36, 37, 46, 47
f_{14}: 12, 13, 14, 16, 24, 26, 27, 36, 37, 56
f_{15}: 12, 16, 17, 23, 24, 26, 34, 36, 56, 57
f_{16}: 12, 16, 23, 26, 27, 34, 35, 37, 45, 47, 67
f_{17}: 12, 13, 15, 26, 27, 34, 45, 46, 47, 56
f_{18}: 12, 15, 17, 23, 24, 27, 34, 35, 36, 57
f_{19}: 12, 13, 16, 34, 35, 45, 46, 47
f_{20}: 12, 14, 16, 23, 24, 36, 46, 56, 67
f_{21}: 12, 15, 16, 17, 25, 26, 27, 34, 36, 45, 46
f_{22}: 12, 13, 14, 15, 24, 35, 36, 37

TABLE V
MASKING FUNCTIONS FOR QOS' S OF LENGTH 256 ($m = 8$)

f_1: 12, 15, 16, 24, 25, 34, 37, 45, 67, 78
f_2: 12, 15, 16, 18, 23, 26, 27, 28, 34, 38, 46, 47, 48, 56, 57, 67, 68
f_3: 12, 13, 16, 17, 18, 23, 25, 27, 34, 36, 38, 45, 78
f_4: 12, 14, 15, 17, 23, 24, 26, 35, 37, 45, 46, 47, 57, 58, 67, 68
f_5: 12, 14, 16, 23, 25, 36, 38, 46, 47, 48, 57, 67, 68, 78
f_6: 12, 13, 16, 18, 24, 26, 27, 28, 36, 45, 46, 47, 48, 56, 57, 68
f_7: 12, 13, 15, 16, 17, 25, 26, 27, 28, 34, 35, 37, 45, 47, 48, 67, 78
f_8: 12, 14, 15, 18, 24, 25, 26, 27, 34, 35, 36, 37, 47, 56, 57, 68, 78
f_9: 12, 13, 14, 16, 24, 25, 26, 27, 28, 36, 38, 46, 48, 56, 57, 67, 68, 78
f_{10}: 12, 13, 15, 16, 18, 27, 34, 35, 37, 38, 48, 56, 57, 58, 68
f_{11}: 12, 13, 14, 15, 18, 28, 34, 35, 36, 45, 46, 56, 58, 67, 68, 78
f_{12}: 12, 16, 17, 18, 24, 28, 34, 35, 36, 37, 38, 46, 47, 56, 57, 58, 67, 78
f_{13}: 12, 14, 15, 16, 17, 18, 23, 24, 27, 28, 35, 38, 57, 67, 68
f_{14}: 12, 13, 16, 17, 23, 24, 25, 26, 27, 28, 35, 38, 47, 48, 78
f_{15}: 12, 13, 14, 18, 25, 26, 27, 34, 35, 38, 45, 47, 56, 57, 67, 68, 78
f_{16}: 12, 17, 26, 34, 37, 38, 45, 46, 47, 48, 56, 58
f_{17}: 12, 14, 15, 23, 24, 37, 48, 56, 57, 58, 67, 68
f_{18}: 12, 15, 17, 18, 24, 25, 27, 34, 36, 37, 46, 47, 48, 57, 68, 78
f_{19}: 12, 13, 14, 15, 16, 17, 23, 24, 25, 27, 28, 34, 35, 37, 45, 57, 68, 78
f_{20}: 12, 16, 25, 34, 38, 78

TABLE VI
MASKING FUNCTIONS FOR QUATERNARY QOS'S OF LENGTH 2^m

m	Masking Sequences of Length 2^m
3	f_1: 02221113 f_2: 01122132 f_3: 02111322 f_4: 01213212
4	f_1: 0013332020113100 f_2: 0200111333132000 f_3: 0332013012011003 f_4: 0112100330230310
5	f_1: 02332213203300132213023322310211 f_2: 03322132231201123203100312233023 f_3: 01303023122323302132320332212110 f_4: 02332231223120113320132231003320
6	f_1: 00131120221311022011312220331322112000133320003131222011310002 11 f_2: 03010121212301211030121010303032232103232321210130101012123210 12 f_3: 00021311311122023313200002001113022233131113202213112220002031 11 f_4: 01032101121032123032321223212101012103013010323030101012012121 23
7	f_1: 03233010010310123230232130100323123203233230010323211012032312 32 30100323101201030103101221011232032312320103323032300103301021 01 f_2: 01033230103001211210212321013010123203230301303201211030323001 03 03011210301003233230232123031030103023032321323021011232303221 23 f_3: 02003331220213331311000233132000313322203313200020221113220213 33 02001113002013333133000233130222313300021131200002001113220231 11 f_4: 02221113020011313313020011132000002031332220133313330002131100 20 11130222331320220200331302223331313300203111000200021333220231 33

(Continued on the following page)

In the same way as in the binary case, it is natural to use $\theta_{\min}(2^m) = \sqrt{2^m}$ by Corollary 19 in order to define *quaternary quasi-orthogonal* sequences in the following.

Definition 20: A family $\mathcal{F} = \{f_i(t) \,|\, i = 1, 2, \cdots, M\}$ of M quaternary sequences of length $N = 2^m$ over Z_4 is said to be *quaternary quasi-orthogonal* if the following are satisfied:

a) $\mathcal{F}$ contains $2\mathcal{W}_m$.

b) For any distinct two sequences $f_i(t), f_j(t) \in \mathcal{F}$

$$\left| \sum_{t=0}^{N-1} \omega^{f_i(t) - f_j(t)} \right| \leq \sqrt{2^m}.$$

c) For any $f(t) \in \mathcal{F} \backslash 2\mathcal{W}_m$, any $w(t) \in 2\mathcal{W}_m$, and any integers L, r, where $L = 2^l$, $2 \leq l \leq m$, and $0 \leq r \leq N/L - 1$

$$\left| \sum_{t=rL}^{rL+L-1} \omega^{f(t)+w(t)} \right| \leq \sqrt{L}.$$

Remark 21: Compared with the conditions for binary QOS's, Conditions b) and c) in Definition 20 are stronger when m or l are odd, in the sense that maximum correlation values are reduced by a factor of $\sqrt{2}$. Condition c) is also called the *window property* in the quaternary case, as in the binary case.

Definition 22: Two quaternary sequences $f(t)$ and $g(t)$ of the same length 2^m are said to be *equivalent* (with respect to $\mathcal{R}_m$) if $f(t) - g(t)$ is in $\langle 2\mathcal{W}_m, \mathbf{2} \rangle$, where $\mathbf{2} = (2, 2, \cdots, 2)$ and $\langle 2\mathcal{W}_m, \mathbf{2} \rangle$ is a module[2] generated by $2\mathcal{W}_m$ and $\mathbf{2}$ over Z_4.

In the same way as in the binary case, we get the following theorem.

Theorem 23: Let $f_1(t), f_2(t), \cdots, f_k(t) \notin 2\mathcal{W}_m$ be k inequivalent sequences of length $N = 2^m$ over Z_4 with window property. If $f_i(t)$ and $f_j(t)$ satisfy Condition b) in Definition 20 for any i and j, $i \neq j$, then the set

$$\mathcal{F} = \bigcup_{i=0}^{k} (f_i(t) + 2\mathcal{W}_m)$$

is quasi-orthogonal, where $f_0(t) = 0$. Furthermore, the size of $\mathcal{F}$ is $(k+1) \cdot 2^m$.

As in the binary case, the nonzero quaternary sequences $f_1(t), f_2(t), \cdots, f_k(t)$ given in Theorem 23 will be called the *masking sequences* of the family $\mathcal{F}$.

[2]See [12] for details.

TABLE VI *(Continued)*

m	Masking Sequences of Length 2^m
	f_1: 0310102123121201213210212312302303323221233030012110322123301223 2312302303103203013030230310102123301223033210030112122303323221 3023231232030310120123123203213230010112322121101223011232210332 1021031012012312320303101201013010032110122301123221211012232330
8	f_2: 0002331320221333111322023133022233132220311120220020111302221311 2022311100021131131102223331220231110200331300022000131122021113 1113220231330222000233132022133300201113022213113313222031112022 3133200011130020020013332220331302223133002033311333202211312220
	f_3: 0200131131330200022231113111200022023313113122022220111311130002 2202113133132202222033313331000220221311313320222000311131110222 1113222022203331331322020020331331110222022213331311020020221311 1333022202222311131330200202231331113000200023331331300202023313
	f_4: 0301121012322101212312101232032332122303010332303212012123213230 2303321210122321230310303230232112100301032330103032030103231232 1232210121233032301021012123121001033230103001210103101232120121 3230010323033212323023210121321221011232121003010323123212102123

B. Construction of Quaternary Quasi-Orthogonal Sequences

The Galois ring $R_m = \mathrm{GR}(4, m)$ is an extension of Z_4 of degree m. R_m is a local ring having a unique maximal ideal $M = 2R$ and the quotient ring R/M is isomorphic to a finite field F_{2^m} with 2^m elements (see [8], [11] for details). As a multiplicative group the set R_m^* of units in R_m has a cyclic subgroup of order $2^m - 1$. Let $\beta \in R_m^*$ be an element of order $2^m - 1$, and let $\mathcal{T}_m = \{0, 1, \beta, \cdots, \beta^{2^m-2}\}$. Any element $z \in R_m$ can be expressed uniquely as $z = a + 2b$ for $a, b \in \mathcal{T}_m$. Let μ be the modulo-2 reduction map. Note that $\alpha = \mu(\beta)$ is a primitive element in in F_{2^m}. The trace map from R_m to Z_4 is defined by

$$T(z) = \sum_{j=0}^{m-1} \left(a^{2^j} + 2b^{2^j}\right).$$

Note that it is a Z_4-linear map.

Let η_i, $1 \le i \le 2^m$, be an ordering of the the elements of $\mathcal{T}_m$. The Family $\mathcal{A}_m$ of Z_4-sequences of period $2^m - 1$ is defined by

$$\mathcal{A}_m = \{s_i(t) \,|\, 0 \le i \le 2^m\} \tag{14}$$

where

$$s_0(t) = T(2\beta^t),$$
$$s_i(t) = T([1 + 2\eta_i]\beta^t), \qquad \text{for } 1 \le i \le 2^m.$$

Note that the size of $\mathcal{A}_m$ is $2^m + 1$ and $\mathcal{A}_m$ is referred to as the *Family* $\mathcal{A}$, whose correlation distribution is well known in the following proposition [2], [10], [23].

Proposition 24: The out-of-phase autocorrelation and cross-correlation between sequences of $\mathcal{A}_m$ in (14) take on only the following values:

$$\begin{aligned} -1, -1 + \epsilon\sqrt{2^m}, &\qquad \text{for odd } m \\ -1, -1 \pm \sqrt{2^m}, -1 \pm \omega\sqrt{2^m}, &\qquad \text{for even } m \end{aligned}$$

where $\epsilon = (\pm 1 \pm \omega)/\sqrt{2}$ and $\omega = \sqrt{-1}$.

The sequence $s_0(t) = T(2\beta^t)$, $t = 0, 1, \cdots, 2^m - 2$ is an m-sequence of length $2^m - 1$ multiplied by $2 \pmod 4$. Thus $2\mathcal{W}_m$ can be obtained from $s_0(t)$ and its shifts by a proper permutation in a similar way as Algorithm $\mathcal{I}$ in Section III-A. Combined with Proposition 24, the family $\mathcal{A}_m$ is a good candidate for construction of quaternary QOS's. In Table VI, examples of masking functions for quaternary QOS's are listed for small values of m. There have been found four nonzero masking functions for quaternary QOS's for $m \le 8$.

V. Concluding Remarks

We have introduced quasi-orthogonal sequences which can be used in CDMA systems that employ the Walsh sequence family for channel separation. A general procedure for construction of QOS's is provided from well-known families of binary sequences with good correlation, including Kasami sequences, Gold sequences, and binary Kerdock codes. In particular, examples of masking functions for QOS's are presented for small lengths. Some examples of quaternary QOS's drawn from Family $\mathcal{A}$ are also included.

Some open problems relating to QOS's are listed as follows.

i) What is $\theta_{\min}(2^m)$ for odd $m \geq 9$? In other words, what is the covering radius $\rho(m)$ of the first-order Reed–Muller code $\mathcal{R}_m$ for odd $m \geq 9$?
ii) Find the exact value of $k_{\max}(m)$ for any $m \geq 5$. In other words, find a maximal set of masking functions for quasi-orthogonal sequences of a given length 2^m in the binary and quaternary cases.
iii) Find a systematic method to construct QOS's in the binary and quaternary cases.

ACKNOWLEDGMENT

The authors wish to thank Prof. J. S. No, Prof. H. Chung, and H. W. Kang for some valuable discussions. They would also like to thank C. K. Park and H. Y. Lee for their computer assistance.

REFERENCES

[1] G. E. Bottomley, "Signature sequence selection in a CDMA system with orthogonal coding," *IEEE Trans. Veh. Technol.*, vol. 42, pp. 62–68, Feb. 1993.
[2] S. Boztas, R. Hammons, and P. V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1101–1113, May 1992.
[3] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des., Codes Cryptogr.*, vol. 15, no. 2, pp. 125–156, Nov. 1998.
[4] G. D. Cohen, M. G. Karpovsky, and H. F. Mattson Jr., "Covering radius—Survey and recent results," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 328–343, May 1985.
[5] O. Glauser, J. Holtzman, A. Shanbhag, and E. G. Tiedemann, "Proposal for improved quasi-orthogonal functions," Tech. Rep. TR-45.5.3.1/98.08.18.13, Portland, OR, Aug. 17, 1998.
[6] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619–621, Oct. 1967.
[7] S. W. Golomb, *Shift-Register Sequences*. San Francisco, CA: Holden-Day, 1967. Laguna Hills, CA: Aegean Park, 1982.
[8] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.
[9] T. Helleseth, T. Kløve, and J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 257–258, 1978.
[10] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998.
[11] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inform. Theory*, vol. 41, pp. 456–468, Mar. 1995.
[12] S. Lang, *Algebra*, 2nd ed. Menlo Park, CA: Addison-Wesley, 1984.
[13] R. Lidl and H. Niederreiter, *Finite Fields of Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983, vol. 20.
[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[15] J. Mykkeltveit, "The covering radius of the $(128, 8)$ Reed–Muller code is 56," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 359–262, 1980.
[16] C.-K. Park and K. Yang, "Generation of quasi-orthogonal sequences using bent functions," in *1997 Fall Conf. Korean Institute of Communication Sciences*, vol. 16, Seoul, Korea, Nov. 15, 1997, pp. 1187–1190. in Korean.
[17] C.-K. Park, K. Yang, Y. Kim, and H.-W. Kang, "Generation of quasi-orthogonal sequences for CDMA systems," in *8th Joint Conf. Communications and Informations (JCCI'98)*, vol. 8, Chunju, Korea, Apr. 22–24, 1998, pp. 1144–1148. in Korean.
[18] N. J. Patterson and D. H. J. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 354–256, May 1983. Correction to "The covering radius of the $(215, 16)$ Reed-Muller code is at least 16276" *IEEE Trans. Inform. Theory*, vol. 36, pp. 443, Mar. 1990.
[19] O. Rothaus, "On 'bent' functions," *J. Comb. Theory*, ser. A, vol. 20, pp. 300–305, 1976.
[20] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, May 1980.
[21] A. Shanbhag, J. Holtzman, E. G. Tiedemann, and J. Odenwalder, "Revised Proposal for Improved Quasi-Orthogonal Functions," Tech. Rep. TR-45.5/98.10.19.19, Burlington, TX, Oct. 19, 1998.
[22] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville, MD: Computer Sci., 1985, vol. 1.
[23] P. Solé, "A quaternary cyclic code and a family of quadriphase sequences with low correlation properties," in *Coding Theory and Applications, Lecture Notes in Computer Science*. New York: Springer-Verlag, 1989, vol. 388, pp. 193–201.
[24] TIA/EIA Interim Std., *Mobile Station-Base Station Compatibility Standard for Dual Mode Wideband Spread Spectrum Cellular System*, Telecommunications Industry Assoc., July 1993.
[25] L. R. Welch, "Lower bounds on the maximum cross-correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.