Designs, Codes and Cryptography (2022) 90:1139–1156
https://doi.org/10.1007/s10623-022-01031-5

Phase orthogonal sequence sets for (QS)CDMA communications

WeiGuo Zhang[1,2] · Enes Pasalic[3] · LiuPiao Zhang[4]

Received: 24 September 2021 / Revised: 4 March 2022 / Accepted: 7 March 2022 /
Published online: 23 March 2022

Abstract

For various quasi-synchronous (QS) CDMA systems, to reduce or eliminate the multiple access interference and multipath interference, it is required to design a set of spreading sequences which are mutually orthogonal within a designed shift zone. In this article, we demonstrate that a concept of irregular spatial assignment, with flexibility to assign different number of users to different cells, can be used to provide the maximal number of orthogonal sequences in any three adjacent cells in networks with a regular tessellation of hexagonal cells. We first consider p-phase spreading sequences of length p^m (thus nonbinary p-valued sequences) suitable for synchronous (S)-CDMA applications, for $p > 3$, and give an efficient design method for reaching the maximal cardinality achievable (being p^m). A simple solution for a flexible assignment of our orthogonal sets of spreading sequences to the cells in hexagonal networks is given. To address QS-CDMA applications as well, an efficient method to combine these orthogonal sequences with Zadeoff–Chu sequences is proposed for the purpose of designing sets of zero correlation zone (ZCZ) sequences (within a certain shift zone) with optimal parameters, thus reaching the Tang–Fan–Matsufuji bound. A similar design framework, based on the use of some special classes of Boolean functions, is then employed for the binary case to provide the maximum cardinality of pairwise orthogonal sequences of length 2^m through this irregular spatial assignment. This improves upon the best known results achieved in Zhang et al. (IEEE Trans Inf Theory 62:3757–3767, 2016),

Communicated by K.-U. Schmidt.

✉ WeiGuo Zhang
zwg@xidian.edu.cn

Enes Pasalic
enes.pasalic6@gmail.com

LiuPiao Zhang
zhangliupiao@foxmail.com

1 State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

2 State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

3 FAMNIT & IAM, University of Primorska, Koper, Slovenia

4 School of Cyberspace Security, Dongguan University of Technology, Dongguan, China

which assigns 2^{m-2} orthogonal sequences (users) per cell, by doubling the number of users in one third of the network.

Keywords CDMA systems · Orthogonal sequences · Semi-bent functions · Zero correlation zone

Mathematics Subject Classification 05B20 · 94B99

1 Introduction

Orthogonal sequences are commonly employed in the construction of spreading codes for synchronous code division multiple access (S-CDMA) satellite systems [2, 8, 14] and QS-CDMA terrestrial systems [13, 16]. A traditional concept of orthogonal sequences employed in S-CDMA systems, such as well-known Walsh sequences, refers to achieving this property only at the inphase point (called also zero point), but whenever there is a relative shift between the sequences the result is commonly a loss of orthogonality [10, 12, 18]. To handle this rather practical scenario of having non-synchronized transmitters and prevent from the loss of orthogonality, diverse additional properties of orthogonal sequences are found to be useful. One of the most prominent characterization, capturing these additional properties for QS-CDMA systems, is so called *generalized orthogonality* introduced in [4] which essentially coincides with the concept of zero correlation zone (ZCZ) sequences [5]. This notion simply reflects the property of preserving orthogonality between the sequences provided that their relative shift is restricted to a certain width (zone). A rather dated but excellent survey on many other related concepts and a valuable resource of references in this context is the article of Fan [3]. For more recent works related to ZCZ sequences and various variants of CDMA systems (such as QS-CDMA communication in cognitive radio (CR) that uses CR ZCZ sequences [7]) the reader is referred to e.g. [20, 21] and the references therein.

In general, these communication systems are based on multiple access and their design aims at achieving resistance to interference while comforting as many users as possible. To achieve these contradictory design requirements, there are inevitably certain trade-offs but also some upper bounds related to the cross-correlation value and the cardinality of orthogonal sequences. The simplest way to construct a set of mutually orthogonal sequences of length p^m (for a prime p) of maximum cardinality p^m is to consider the rows of a $p^m \times p^m$ Hadamard matrix. Then adding any other sequence to this set, also called a set of Walsh sequences, would imply a maximum inphase correlation being at least $p^{\frac{m}{2}}$ (this would correspond to addition of a bent sequence). This limitation between the number of orthogonal sequences (spreading codes) and the maximum inphase correlation can be overcome by careful spatial assignment. However, to overcome the constraints imposed by the maximum cardinality of mutually orthogonal sequences, being p^m, for practical applications the same sequences can be reused if their relative distance D in the network is sufficiently large. It is considered to be enough to take the reuse distance D to be in the interval $D \in [3, 4]$ to ensure that the interference from the reused sequence is sufficiently small. At the same time, to prevent interference from the users in neighbouring cells, a standard requirement for the assignment of orthogonal sequences in the network is that the sequences within any cell should be orthogonal to the sequences in the neighbouring cells.

The main contribution this article is an efficient method to construct a large set of sequences (much larger than p^m), using (vectorial) semi-bent functions [1], where (large) subsets of this

set contain mutually orthogonal sequences. Furthermore, these (orthogonal) subsets can be partitioned into several families which are mutually orthogonal to each other. More precisely, for even m and sequences of length p^m, we could specify $p^{(m-1)/2+1}$ orthogonal sequence sets, each of cardinality p^{m-1}. We also propose practical solutions for allocating these orthogonal sets into hexagonal networks so that a low correlation between non-orthogonal sequences is achieved and at the same time the reuse of these subsets satisfy practical requirements governed by the so-called reuse distance (achieving $D = \sqrt{21}$). These orthogonal sequences suitable for S-CDMA systems are then combined with the so-called Zadeoff–Chu sequences to provide several sets of ZCZ sequences with good inter-set correlation properties and optimal parameters in terms of the Tang–Fan–Matsufuji bound.

A similar design framework is used in the construction of orthogonal binary sequences which can be optimally assigned in the network in the above sense. Our method improves upon the currently best design technique proposed in [19] (in terms of the number of users per cell when $p = 2$), which allows for an efficient assignment of 2^{m-2} users per cell and achieves the reuse distance $D = 4$. Notice that the method in [19] was a significant improvement over other approaches, more precisely using the technique in [19] the number of users is doubled compared to [14]. On the other hand, considering any three (mutually) adjacent cells in a hexagonal network, the approach in [19] is still not optimal because $3 \cdot 2^{m-2} < 2^m$, thus not reaching the absolute upper bound 2^m. We show that the technique in [19] can be further optimized so that one third of the network can accommodate 2^{m-1} users per cell, implying that the upper bound on orthogonality is achieved through $2 \cdot 2^{m-2} + 2^{m-1} = 2^m$. There is however a small trade-off for this improvement which is a decrease of the reuse distance to $D = \sqrt{12}$ compared to $D = 4$ in [19], though having $D = \sqrt{12}$ is still sufficient for practical applications.

This paper is organized as follows. Some basic notions and definitions related to sequences are given in Sect. 2. In Sect. 3, two construction methods of p-phase sequences are proposed. The first method treats traditional orthogonal sequences suitable for S-CDMA applications, whereas the second method combine these sequences with Zadeoff–Chu sequences to provide several sets of ZCZ sequences with good inter-set correlation properties. In Sect. 4, we slightly modify the method in [19] to accommodate 2^{m-1} orthogonal sequences per cell in one third of network, thus achieving an optimal assignment in terms of orthogonality constraints. Some concluding remarks are given in Sect. 5.

2 Preliminaries

In this section we present some important notions and tools related to sequences and Boolean functions. Our main tool in the analysis is the Walsh–Hadamard transform.

Let $\mathbb{F}_{p^m}$ denote the finite field $GF(p^m)$ and $\mathbb{F}_p^m$ be its corresponding vector space. The set of all m-variable functions from $\mathbb{F}_p^m$ to $\mathbb{F}_p$ is denoted by $\mathcal{B}_{(m,p)}$. For simplicity, we take "+" and $\sum_i$ to denote the addition operations over $\mathbb{F}_p^m$ and $\mathbb{F}_{p^m}$ respectively. In general, a function $f \in \mathcal{B}_{(m,p)}$ can be represented by

$$f(x_1, \ldots, x_m) = \sum_{b \in \mathbb{F}_p^m} \lambda_b \Big(\prod_{i=1}^{m} x_i^{b_i}\Big),$$

where $\lambda_b \in \mathbb{F}_p$, $b = (b_1, \ldots, b_m) \in \mathbb{F}_p^m$. For $a = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$, $b = (b_1, \ldots, b_m) \in \mathbb{F}_p^m$, define the *inner product* of a and b by

$$a \star b = \sum_{i=1}^{m} a_i b_i,$$

where the sum is calculated mod p. Let $\mathcal{L}_m = \{\omega \star x \mid \omega \in \mathbb{F}_p^m\}$. The Walsh–Hadamard (or Fourier) transform of $f \in \mathcal{B}_{(m,p)}$ at point ω, denoted by $W_f(\omega)$, is defined as

$$W_f(\omega) = \sum_{x \in \mathbb{F}_p^m} \xi^{f(x) - \omega \star x}.$$

where where "-" denotes addition inverse and $\xi = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity.

The *corresponding sequence* of $f \in \mathcal{B}_{(m,p)}$ is a p-phase sequence of length $N = p^m$ defined as

$$\overline{f} = \left(\xi^{f(0,\ldots,0,0)}, \xi^{f(0,\ldots,0,1)}, \ldots, \xi^{f(p-1,\ldots,p-1,p-1)}\right).$$

For a linear function $l(x) = \omega \star x \in \mathcal{L}_m$ and arbitrary $f \in \mathcal{B}_{(m,p)}$ we clearly have

$$W_f(\omega) = \overline{f} \star \overline{l}^* = \overline{f - l},$$

where $\overline{l}^*$ denotes the element-wise complex conjugation of the sequence $\overline{l}$.

In general, for any two complex sequences $a = \{a(t)\}_{t=0}^{N-1}$ and $b = \{b(t)\}_{t=0}^{N-1}$ of length N, the periodic cross-correlation function at $0 \le \tau < N$ is defined as $R_{a,b}(\tau) = \sum_{t=0}^{N-1} a(t) b^*(t+\tau)$, where $t+\tau$ is taken module N. If $a = b$, we use R_a in place of $R_{a,b}(\tau)$ to denote the periodic autocorrelation function. Obviously, $W_f(\omega) = \overline{f} \star \overline{l}^*$ stands for the in-phase cross-correlation of the sequences $\overline{f}$ and $\overline{l}$, where $l(x) = \omega \star x$.

Definition 1 Let $f_1, f_2 \in \mathcal{B}_{(m,p)}$. $\overline{f_1}$ and $\overline{f_2}$ are orthogonal, denoted by $\overline{f_1} \perp \overline{f_2}$, if the in-phase correlation between $\overline{f_1}$ and $\overline{f_2}$ is zero, i.e.,

$$\overline{f_1} \star \overline{f_2}^* = \sum_{x \in \mathbb{F}_p^m} \xi^{f_1(x) - f_2(x)} = 0.$$

Let $S = \{\overline{f_i} \mid f_i \in \mathcal{B}_{(m,p)}, i = 1, 2, \ldots, \kappa\}$. S is referred to as a orthogonal sequence set of cardinality κ if the sequences in S are pairwise orthogonal. Let S_1 and S_2 be two orthogonal sequence set. S_1 and S_2 are said to be mutual orthogonal, denoted by $S_1 \perp S_2$, if $\overline{f_1} \star \overline{f_2}^* = 0$ always holds for any $\overline{f_1} \in S_1$ and $\overline{f_2} \in S_2$.

The following simple characterization of orthogonal sequences was deduced in [19].

Lemma 1 [19] *Let $f_1, f_2 \in \mathcal{B}_{(m,p)}$. Then $\overline{f_1} \perp \overline{f_2}$ if and only if $W_{f_1 - f_2}(\mathbf{0}_m) = 0$.*

For any two different linear functions $l, l' \in \mathcal{L}_m$, $W_{l-l'}(\mathbf{0}_m) = 0$, which implies that $\overline{l} \perp \overline{l'}$ always holds.

Definition 2 $f \in \mathcal{B}_{(m,p)}$ is called a bent function if $|W_f(\alpha)| = p^{m/2}$, for any $\alpha \in \mathbb{F}_p^m$. Also, $f \in \mathcal{B}_{(m,p)}$ is called a semi-bent function if $|W_f(\alpha)| \in \{0, p^{\lfloor (m+2)/2 \rfloor}\}$ for any $\alpha \in \mathbb{F}_p^m$. $\overline{f}$ is called a semi-bent sequence if f is a semi-bent function.

Definition 3 Let $F : \mathbb{F}_p^m \mapsto \mathbb{F}_p^t$ with $F(x) = (f_1, \ldots, f_t)$, where $f_1, \ldots, f_t \in \mathcal{B}_{(m,p)}$. F is called a vectorial semi-bent function if for any $c \in {\mathbb{F}_p^t}^*$ and $\alpha \in \mathbb{F}_p^m$, $|W_{f_c}(\alpha)| \in \{0, p^{\lfloor (m+2)/2 \rfloor}\}$, where $f_c = c \star F$. F is called a vectorial bent function if $|W_{f_c}(\alpha)| = p^{m/2}$, for any $c \in {\mathbb{F}_p^t}^*$.

Let $C = \{c_0, c_1, \ldots, c_{M-1}\}$ denote a set of sequences of length N of cardinality M. The set C is said to be an (N, M, Z_{cz})-ZCZ sequence set of width Z_{cz} if

$$R_{c_i,c_j}(\tau) = \begin{cases} N, & i = j, \tau = 0 \\ 0, & i = j, 0 < \tau \le Z - 1 \\ 0, & i \ne j, 0 \le \tau \le Z - 1, \end{cases}$$

where Z_{cz} is the maximum positive integer Z achieving this zero correlation.

Lemma 2 [15] (Tang–Fan–Matsufuji bound) *Let C be a sequence set of cardinality M, sequence period N, and ZCZ width Z_{cz}, then*

$$MZ_{cz} \le N. \tag{1}$$

A ZCZ sequence set is referred to as optimal if the equality is achieved.

3 *p*-phase spreading codes for odd prime *p*

We first notice that in hexagonal networks no more than three cells can be mutually adjacent to each other. Therefore, to provide a maximal cardinality (being p^m) of orthogonal sequences of length p^m contained in any three adjacent cells (ensuring at the same time a sufficiently large reuse distance D), we need to design a set of much larger cardinality than p^m and to distribute these sequences over the network so that the optimality is achieved in the above sense. For this purpose, we use in the background vectorial bent functions over $\mathbb{F}_p^m$ from which suitable vectorial semi-bent functions are derived. This way, we design p^{u+1} sequence sets (where $u = (m-1)/2$), each of cardinality p^{m-1}, which are later allocated to different cells with respect to their orthogonality relation. Clearly, the total number of the designed sequences equals to $p^{u+1}p^{m-1} = p^{u+m}$ which is much larger than p^m and this is the main reason that we can achieve an optimal assignment of these sequences in hexagonal networks.

Construction 1 *Let $m \ge 3$ be odd and $x \in \mathbb{F}_p^{m-1}$. Let $G : \mathbb{F}_p^{m-1} \to \mathbb{F}_p^{(m-1)/2}$ defined by*

$$G(x) = (g_1(x), g_2(x), \ldots, g_u(x)),$$

be a vectorial bent function, where $u = (m-1)/2$. For $i = 1, \ldots, u$ and $y \in \mathbb{F}_p$, define

$$f_i(y, x) = i \cdot y \pmod p + g_i(x),$$

where " $\cdot$" denotes the multiplication in $\mathbb{F}_p$. Let now $F : \mathbb{F}_p^m \to \mathbb{F}_p^u$ be defined by

$$F(y, x) = (f_1, \ldots, f_u).$$

For any $c = (c_1, \ldots, c_u) \in \mathbb{F}_p^u$, let $f_c(y, x) = c \star F(y, x) = c_1 f_1 + \cdots + c_u f_u$, and for $\beta \in \mathbb{F}_p$

$$L_\beta = \{\beta \star y + \alpha \star x \mid \alpha \in \mathbb{F}_p^{m-1}\}.$$

We construct p^{u+1} sequence sets $H_\beta^{f_c}$ (for different $c \in \mathbb{F}_p^u$ and $\beta \in \mathbb{F}_p$), as follows:

$$H_\beta^{f_c} = \{\overline{f_c - l} \mid l \in L_\beta\}, \tag{2}$$

where $\sharp H_\beta^{f_c} = p^{m-1}$. Then, denoting $i_c = \sum_{i=1}^u c_i \cdot i \pmod p$, we have

(i) All the sequences in $H_\beta^{f_c}$ are mutually orthogonal, for any fixed $\beta \in \mathbb{F}_p$ and $c \in \mathbb{F}_p^u$;

(ii) For $c, c' \in \mathbb{F}_p^u$ and $\beta, \beta' \in \mathbb{F}_p$, $H_\beta^{f_c} \perp H_{\beta'}^{f_{c'}}$ if and only if $\beta' - \beta \not\equiv i_c - i_{c'} \pmod p$;

(iii) Let $s \in H_\beta^{f_c}$ and $s' \in H_{\beta'}^{f_{c'}}$ with $0 \neq \beta' - \beta \equiv i_c - i_{c'} \pmod p$. Then, $|s \star s'^*| = p^{(m+1)/2}$.

Proof (i) Let $\overline{f_c - l}, \overline{f_c - l'} \in H_\beta^{f_c}$, where $l = \beta \star y + \alpha \star x$ and $l' = \beta \star y + \alpha' \star x$. For any $\alpha \neq \alpha'$, we have

$$\begin{aligned}
&\overline{f_c - l} \star \overline{f_c - l'}^* \\
&= \sum_{(y,x) \in \mathbb{F}_p^m} \xi^{f_c(y,x) - \beta \cdot y - \alpha \cdot x} \xi^{-f_c(y,x) + \beta \star y + \alpha' \star x} \\
&= \sum_{(y,x) \in \mathbb{F}_p^m} \xi^{(\alpha' - \alpha) \star x} \\
&= 0.
\end{aligned}$$

(ii) For any $s = \overline{f_c - \beta \star y - \alpha \star x} \in H_\beta^{f_c}$ and $s' = \overline{f_{c'} - \beta' \star y - \alpha' \star x} \in H_{\beta'}^{f_{c'}}$, the in-phase correlation between s and s' can be written as

$$\begin{aligned}
s \star s'^* &= \sum_{(y,x) \in \mathbb{F}_p^m} \xi^{f_c(y,x) - \beta \cdot y - \alpha \star x} \xi^{-f_{c'}(y,x) + \beta' \cdot y + \alpha' \star x} \\
&= \sum_{(y,x) \in \mathbb{F}_p^m} \xi^{f_c(y,x) - f_{c'}(y,x) + (\beta' - \beta) \cdot y + (\alpha' - \alpha) \star x} \\
&= \sum_{y \in \mathbb{F}_p} \xi^{((i_c - i_{c'}) - (\beta' - \beta)) \cdot y} \times W_{(g_c - g_{c'})}(\alpha' - \alpha).
\end{aligned}$$

Note that for different sequence sets $H_\beta^{f_c}$ and $H_{\beta'}^{f_{c'}}$, we always have $\beta \neq \beta'$ or $f_c \neq f_{c'}$. Furthermore, $f_c = f_{c'} \Leftrightarrow g_c = g_{c'} \Leftrightarrow i_c = i_{c'}$. So, if $i_c = i_{c'}$ then necessarily $\beta' \neq \beta$. Thus,

$$\begin{aligned}
H_\beta^{f_c} \perp H_{\beta'}^{f_{c'}} &\Leftrightarrow s \star s'^* = 0 \\
&\Leftrightarrow \sum_{y \in \mathbb{F}_p} \xi^{((i_c - i_{c'}) - (\beta' - \beta)) \cdot y} = 0 \\
&\Leftrightarrow \beta' - \beta \not\equiv i_c - i_{c'} \pmod p,
\end{aligned}$$

which proves the statement.

(iii) When $0 \neq \beta' - \beta \equiv i_c - i_{c'} \pmod p$, we have

$$|W_{(g_c - g_{c'})}(\alpha' - \alpha)| = p^{(m-1)/2}$$

and

$$\sum_{y \in \mathbb{F}_p} \xi^{((i_c - i_{c'}) - (\beta' - \beta)) \cdot y} = p,$$

which implies $|s \star s'^*| = p^{(m+1)/2}$.

3.1 Allocating the sequence sets $H_\beta^{f_c}$

In this section we address the problem of allocations the sets of orthogonal sequences $H_\beta^{f_c}$ in a network of regular hexagon cells with respect to the basic assignment rules mentioned

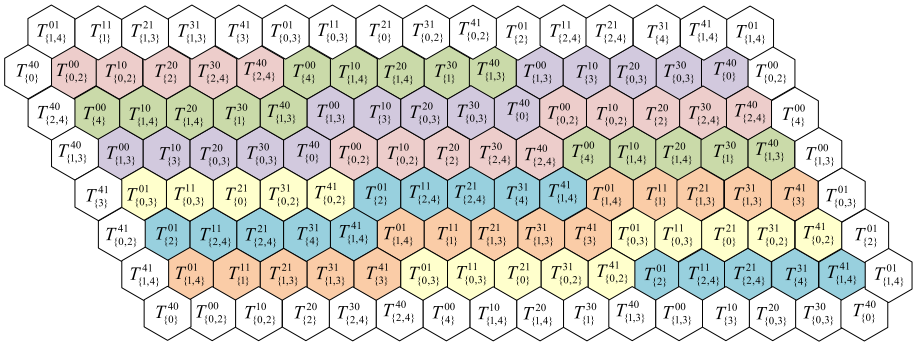

Fig. 1 An assignment of the sets $H_\beta^{f_c}$ in regular hexagonal network for $p = 5, m = 5$

earlier. The flexibility of assignment is based on a simple partition of the underlying prime field.

Let N_1, N_2 and N_3 be three positive integers such that $N_1 + N_2 + N_3 = p$. Let $I = \{i_1, \ldots, i_{N_1}\}$, $J = \{j_1, \ldots, j_{N_2}\}$, and $W = \{w_1, \ldots, w_{N_3}\}$ be any three disjoint sets such that

$$I \cup J \cup W = \mathbb{F}_p.$$

For fixed $c \in \mathbb{F}_p^u$ and the corresponding function $f_c(y, x) = c \star F(y, x)$, where F is defined in Construction 1, let

$$T_I^c = \bigcup_{\beta \in I} H_\beta^{f_c}, \quad T_J^c = \bigcup_{\beta \in J} H_\beta^{f_c}, \quad T_W^c = \bigcup_{\beta \in W} H_\beta^{f_c}. \tag{3}$$

Then, T_I^c,T_J^c, T_W^c are mutually orthogonal sequence sets with cardinality $N_1 p^{m-1}$, $N_2 p^{m-1}$ and $N_3 p^{m-1}$, respectively. Using the properties of Construction 1, namely the orthogonality relation in (ii), we can determine whether two sequence sets T_I^c and $T_{I'}^{c'}$ are orthogonal, where $I, I' \subset \mathbb{F}_p$. If these sets are orthogonal to each other, then they can be merged into a set of cardinality which is twice as large compared to the constituent sets. This is an efficient way to increase the size of certain cells in a regular hexagonal network and to achieve the optimality as previously discussed.

To illustrate the assignment of the orthogonal sets in Construction 1, we give some brief details of the design procedure for a particular case when $p = 5$, $m = 5$, see Fig. 1. In this case, we first construct a vectorial bent function $G : \mathbb{F}_5^4 \to \mathbb{F}_5^2$, represented as $G(x) = (g_1(x), g_2(x))$, which can for instance be taken from the class of vectorial Mariaona-McFarland bent functions.

Then, for any $c = (c_1, c_2) \in \mathbb{F}_5^2$, we define $f_c = (c_1 + 2c_2)y + g_c(x)$ along with its associated sequence $\overline{f}_c$. Using the orthogonality relation given in Construction 1 by item (ii), the assignment scheme of the sets T_I^c,T_J^c, T_W^c is given as in Fig. 1. The reuse distance is $\sqrt{21}$ and is computed as $D = \sqrt{i^2 + j^2 + ij}$ (thus $D = \sqrt{21}$ is obtained for $i = 4$ and $j = 1$), where the integers $0 \le i, j \le \sqrt{3 \cdot 2^k}$ determine the distance between the same cells in two-dimensional vector space.

The assignment given in Fig. 1 is obviously optimal in the sense of packing, thus any tree neighbouring cells comprise 5^m mutually orthogonal sequences which is the largest amount possible.

Remark 1 Note that $u = (m-1)/2$, and the number of the constructed sequence sets is p^{u+1}, thus different m may yield the same u. The reuse distance D depends on u and its value is governed by the request that all the constructed sequence sets can be easily allocated to the network of hexagonal cells (respecting the basic assignment rules). This also means, that for sufficiently large p, the condition that $\beta' - \beta \not\equiv i_c - i_{c'} \pmod p$ (i.e., $H_\beta^{f_c} \perp H_{\beta'}^{f_{c'}}$) can be easily satisfied. This way, one preserves the same reuse distance $D = \sqrt{21}$ though in the special case $p = 3$ this reuse distance is slightly reduced (but still practical). In general, the reuse distance D gets larger when p increases.

The above assignment can can be generalized to deal with arbitrary prime p by splitting $\mathbb{F}_p$ into three disjoint subsets I, J, W, so that $\sharp I + \sharp J + \sharp W = p$. Let $m = 7$ so that $u = 3$ in Construction 1. Then, for any $c = (c_1, c_2, c_3) \in \mathbb{F}_p^3$ and for any fixed $e \in \mathbb{F}_p$, we define

$$S(e) = \{c \in \mathbb{F}_p^3 \mid c_1 + 2c_2 + 3c_3 = e \pmod p\}.$$

For instance, if $p = 5$ one can easily verify that $\sharp S(e) = 25$ for any $e \in \mathbb{F}_5$.

Then assigning $i_c = c_1 + 2c_2 + 3c_3 \pmod p$ we take $i_c = 0$, and consider $c \in S(0)$. The following orthogonal sets of sequences are then assigned into the network (see Fig. 2):

$$\begin{aligned} &T_I^c,\ c \in S(0) && \text{Marked by red color in Fig. 2} \\ &T_J^c,\ c \in S(0) && \text{Marked by yellow color in Fig. 2} \\ &T_W^c,\ c \in S(0) && \text{Marked by green color in Fig. 2} \end{aligned}$$

In general, the cardinality of T_I^c, T_J^c, T_W^c are $\sharp I \cdot p^{m-1}, \sharp J \cdot p^{m-1}$ and $\sharp W \cdot p^{m-1}$, respectively. In the particular case when $p = 5$ and $m = 7$, there are $3 \times 5^2 = 75$ (in general the number is $3 \times p^{u-1}$) sets of orthogonal sequences T_I^c, T_J^c, T_W^c when c goes through $S(0)$, which are not necessarily mutually orthogonal sets. To ensure mutual orthogonality between the sets so that $T_S^c \perp T_{S'}^{c'}$, where $S, S' \in \{I, J, W\}$, it is sufficient that $S \neq S'$ and that $c, c' \in S(0)$. This is an easy consequence of Eq. (3) and the orthogonality condition (ii) in Construction 1. Therefore, the adjacent cells are in different colors (thus having different indices taken from the set $\{I, J, W\}$). Out of these 75 different orthogonal sets of sequences, we employ $12 \times 6 = 72$ sets corresponding to 12 rows and 6 column in Fig. 2. The reuse distance is obviously $D = \sqrt{6^2 + 3^2 + 6 \cdot 3} = 3\sqrt{7}$, see also Fig. 2.

In general, for any p, there are $3 \cdot p^{u-1}$ orthogonal sets ($T_I^c, T_J^c, T_W^c, c \in S(e), e \in \mathbb{F}_p$ fixed) which can be easily assigned to a network of hexagonal cells using the above approach.

3.2 Sequences for QS-CDMA systems

The orthogonal sequence sets $H_\beta^{f_c}, c \in \mathbb{F}_p^u, \beta \in \mathbb{F}_p$, are suitable for applications in S-CDMA satellite systems. However, to design spreading codes for QS-CDMA systems we must ensure that the ZCZ property of certain width is also embedded in design. In what follows, we employ the sets $H_\beta^{f_c}$ defined by (2) and combine these with Zadoff-Chu sequences to construct multiple ZCZ sequence sets with optimal parameters. The following design approach is relevant in our context.

Lemma 3 [11] *A generalized chirp-like (GCL) sequence $\{c(t)\}$ of length N is defined as*

$$c(t) = a(t)b(t \bmod v), \quad t = 0, 1, \ldots, N-1$$

where N, u, v are positive integer with $N = uv$, the term $b(t \bmod v)$ is a "modulation" sequence of v arbitrary complex numbers (for instance $b(t) = e^{\frac{t2\pi\sqrt{-1}}{v}}$), and $\{a(t)\}$ is a

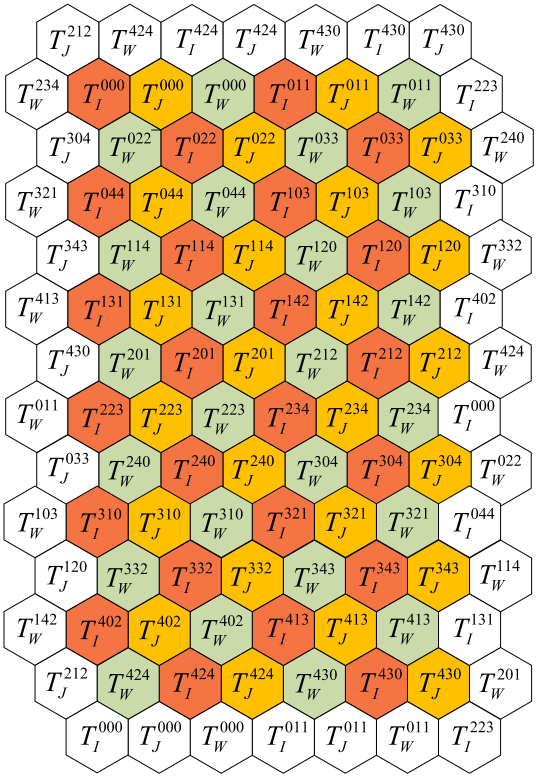

Fig. 2 An assignment of the sets $H_\beta^{f_c}$ in regular hexagonal network for $p = 5, m = 7$

Zadoff-Chu sequence defined as

$$a(t) = \xi_N^{t(t+(N \bmod 2))/2+qt}, \quad t = 0, 1, \ldots, N-1, \tag{4}$$

where $\xi_N = e^{-2\pi ir/N}$, $gcd(r, N) = 1$ and q is any integer. Then, any two GCL sequences that use the same $\{a(t)\}$ but different $\{b_x(t)\}$ and $\{b_y(t)\}$ have a ZCZ of width $u - 1$.

A set of GCL-ZCZ sequences can be generated by selecting $\{b(t)\}$ from the set of Hadamard sequences [11]. Instead of using an orthogonal (Hadamard) matrix as in [11], we will consider a set of correlation constrained Hadamard matrices. More precisely, for a set $H_\beta^{f_c}$ defined as in (2) we denote $H^{f_c} = \cup_{\beta \in \mathbb{F}_p} H_\beta^{f_c}$, for any $c \in \mathbb{F}_p^u$. Then, since $\sharp H^{f_c} = p^m$, we associate to each H^{f_c} a Hadamard matrix of order $p^m \times p^m$ (called correlation constrained), and denote its j-th row by $h_j^{f_c}$.

Theorem 1 *Let $a(t)$ be a Zadeoff–Chu sequence of length N defined by (4), where $N = dp^m$ and $d > 1$. For any $c \in \mathbb{F}_p^u$, define the set C^{f_c} of cardinality p^m as:*

$$C^{f_c} = \{c(t) \stackrel{\triangle}{=} a(t) h_j^{f_c}(t \bmod p^m), t = 0, 1, \ldots, N-1\}_{j=1,\ldots,p^m},$$

where $h_j^{f_c} \in H^{f_c}$ is defined as above. Then,

(i) For any $c(t) \in C^{f_c}$ and $c'(t) \in C^{f_{c'}}$, with $c \neq c'$, we have $|R_{c,c'}(0)| \in \{0, dp^{(m+1)/2}\}$.

(ii) If $H^{f_c} \perp H^{f_{c'}}$, then the sequences $c(t) \in C^{f_c}$ and $c'(t) \in C^{f_{c'}}$, $c \neq c'$, have zero correlation zone d.

(iii) Each C^{f_c}, $c \in \mathbb{F}_p^u$, is an (N, p^m, d)-ZCZ sequence set satisfying the bound of Tang–Fan–Matsufuji with equality.

Proof For $h_j^{f_c} \in H^{f_c}$ and $h_j^{f_{c'}} \in H^{f_{c'}}$, let

$$c(t) = a(t)h_j^{f_c}(t \bmod p^m); \qquad c'(t) = a(t)h_{j'}^{f_{c'}}(t \bmod p^m).$$

The cross-correlation between $c(t)$ and $c'(t)$ can be written as:

$$\begin{aligned} R_{c,c'}(\tau) &= \sum_{t=0}^{N-1} c(t)c'(t+\tau)^* \\ &= \sum_{t=0}^{N-1} a(t)h_j^{f_c}(t \bmod p^m)a(t+\tau)^* h_{j'}^{f_{c'}*}((t+\tau) \bmod p^m). \end{aligned}$$

By (4), we have $a(t)a(t+\tau)^* = e(\tau)\xi_N^{-t\tau}$, where $e(\tau) = \xi_N^{-\frac{1}{2}\tau^2 - \frac{1}{2}\tau(N \bmod 2) - q\tau}$. Let $t = t_1 p^m + t_2$, where $0 \le t_1 < d$ and $0 \le t_2 < p^m$. We obtain

$$\begin{aligned} R_{c,c'}(\tau) &= e(\tau) \sum_{t=0}^{N-1} \xi_N^{-t\tau} h_j^{f_c}(t \bmod p^m) h_{j'}^{f_{c'}*}((t+\tau) \bmod p^m) \\ &= e(\tau) \sum_{t_1=0}^{d-1} \sum_{t_2=0}^{p^m-1} \xi_N^{-(t_1 p^m + t_2)\tau} h_j^{f_c}(t_2 \bmod p^m) h_{j'}^{f_{c'}*}((t_2+\tau) \bmod p^m) \\ &= e(\tau) \sum_{t_1=0}^{d-1} \xi_d^{-t_1\tau} \sum_{t_2=0}^{p^m-1} \xi_N^{-t_2\tau} h_j^{f_c}(t_2 \bmod p^m) h_{j'}^{f_{c'}*}((t_2+\tau) \bmod p^m). \end{aligned}$$

It can be easily verified that $\sum_{t_1=0}^{d-1} \xi_d^{-t_1\tau} = 0$, if τ is not a multiple of d. If $c = c'$, we have

$$\sum_{t_2=0}^{p^m-1} h_j^{f_c}(t_2 \bmod p^m) h_{j'}^{f_{c'}*}((t_2+\tau) \bmod p^m) = 0,$$

for $\tau = 0$. If $c \neq c'$,

$$R_{c,c'}(0) = d \times \sum_{t_2=0}^{p^m-1} h_j^{f_c}(t_2) h_{j'}^{f_{c'}*}(t_2). \tag{5}$$

Let $h_j^{f_c} = \overline{f_c - \beta \star y - \alpha \star x}$, $h_{j'}^{f_{c'}} = \overline{f_{c'} - \beta' \star y - \alpha' \star x}$. Then

$$\begin{aligned} &\sum_{t_2=0}^{p^m-1} h_j^{f_c}(t_2) h_{j'}^{f_{c'}*}(t_2) \\ &= \overline{f_c - \beta \star y - \alpha \star x} \star \overline{f_{c'} - \beta' \star y - \alpha' \star x}^* \\ &= \overline{f_c - f_{c'} - (\beta - \beta') \star y - (\alpha - \alpha') \star x} \\ &= W_{f_c - f_{c'}}(\beta - \beta', \alpha - \alpha') \end{aligned}$$

Thus, for an element $(\beta - \beta', \alpha - \alpha')$ we have

$$W_{f_c - f_{c'}}(\alpha) = \sum_{t_2=0}^{p^m-1} h_j^{f_c}(t_2) h_{j'}^{f_{c'}*}(t_2).$$

Note that $f_c - f_{c'}$ is a semi-bent function and consequently $|W_{f_c - f_{c'}}(\beta - \beta', \alpha - \alpha')|$ takes values in $\{0, p^{(m+1)/2}\}$ which gives

$$\begin{aligned} |c(t) \star c'(t)^*| &= |R_{c,c'}(0)| = d|W_{f_c - f_{c'}}(\beta - \beta', \alpha - \alpha') \\ &= dp^{(m+1)/2}. \end{aligned}$$

This proves (i).

(ii) Note that $R_{c,c'}(\tau) = 0$ for $0 < |\tau| < d$. When $H^{f_c} \perp H^{f_{c'}}$, we have $h_j^{f_c} \perp h_j^{f_{c'}}$. By (5), $R_{c,c'}(0) = 0$. Thus, $R_{c,c'}(\tau) = 0$ for $|\tau| < d$.

(iii) By (1), and noticing $\sharp C^{f_c} = \sharp H^{f_c} = p^m$, the statement follows trivially due to the relation $N = dp^m$.

Remark 2 A convenient assignment of ZCZ sets to a network of hexagonal cells is as follows.

- Let $S = \{C^{f_c} \mid c \in \mathbb{F}_p^u\}$. Obviously, $\sharp S = p^u$.
- Each C^{f_c} can be divided into three parts:

$$\begin{aligned} C_I^c &= \{a(t) h_j^{f_c}(t \bmod p^m) \mid h_j^{f_c} \in T_I^c\} \\ C_J^c &= \{a(t) h_j^{f_c}(t \bmod p^m) \mid h_j^{f_c} \in T_J^c\} \\ C_W^c &= \{a(t) h_j^{f_c}(t \bmod p^m) \mid h_j^{f_c} \in T_W^c\} \end{aligned}$$

The assignment for QS-CDMA systems is then obtained by substituting T_I^c, T_J^c, T_W^c in Figs. 1 and 2 by C_I^c, C_J^c, C_W^c, respectively.

3.2.1 A comparison to other design methods

In Table 1, we compare the most relevant parameters for various design methods. Notice that the choice of our main parameters d and m is governed by the sequence length being $N = dp^m = uv$, where the parameters u and v are used in the definition of a GCL sequence by means of Lemma 3. Notice that in a recent article [6] the parameter k can be taken in the range $1 \leq k < m$. This approach appears to be the best known method in terms of the trade-offs induced on the main parameters. More precisely, when $k = 1$ the cross-correlation between the sequences becomes optimal in the sense of the Welch bound, thus the maximum correlation is approximately $\sqrt{N}$. On the other hand, it is not clear whether these sequences have a certain ZCZ width (which is at most one since in this case $N = M = p^m - 1$ and we have $MZ_{CZ} \leq N$).

4 Construction of binary spreading codes

The construction 1 is not suitable for constructing orthogonal binary sequences. We will present a method to construct orthogonal binary sequences for $m = 2k + 2$. In this section, we give a construction to demonstrate that a portion of cells, corresponding to one third of the cells assigned to a network, can have increased number of users namely 2^{m-1} instead of

Table 1 Some known multiple ZCZ sequence sets—a comparison

ZCZ sequence sets	Phase	Period	Set size	Z_{CZ}	The number of sets	Maximum inphase inter-set correlation
Tang et al.[16]	3	$2^{m+1}d + 2d - 2$	2^{m+1}	d	2^{m-1}	$2^{(m+2)/2}d$
Tang et al.[16]	3	$2^{m+1}d + 2d - 2$	2^{m+1}	d	2^{m}	$2^{(m+3)/2}d$
Tang et al.[17]	2	$2^{m+2}(d-1)$	2^{m+1}	d	2^{m-1}	$2^{(m+4)/2}(d-1)$
Tang et al. [17]	2	$2^{m+2}(d-1)$	2^{m+1}	d	2^{m}	$2^{(m+5)/2}(d-1)$
Li et al.[9]	4	2^{m+2}	2^{m}	4	2^{m}	$2^{(m+4)/2}$
Zhou et al. [21]	p	p^2	p	p	$p-1$	p
Gu et al. [6]	p	$p^m - 1$	$p^m - 1$	–	$p^{km} - 1$	$p^{k-1}p^{m/2}$
Ours	p	dp^m	p^m	d	$p^{(m-1)/2}$	$p^{(m+1)/2}d$

2^{m-2} as in the original construction given in [19]. Thus, we keep the same level of cross-correlation $2^{m/2+1}$ between non-orthogonal sequences as in [19] while at the same doubling the number of users in one third of the network.

Construction 2 *Let m, and k be two positive integers with $m = 2k+2$ and $k \geq 2$. Let γ be a primitive element of $\mathbb{F}_{2^k}$, and $\{1, \gamma, \ldots, \gamma^{k-1}\}$ be a polynomial basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. Define the isomorphism π: $\mathbb{F}_{2^k} \mapsto \mathbb{F}_2^k$ by*

$$\pi(b_1 + b_2\gamma + \cdots + b_k\gamma^{k-1}) = (b_1, b_2, \ldots, b_k).$$

For $i = 1, \ldots, k$, let $\phi_i : \mathbb{F}_2^k \to \mathbb{F}_2^k$ be a bijective mapping defined by

$$\phi_i(y) = \begin{cases} \boldsymbol{0}_k, & y = \boldsymbol{0}_k \\ \pi(\gamma^{[y]+i}), & y \in \mathbb{F}_2^{k*} \end{cases}$$

where $[y]$ denotes the integer representation of y. Let $y, x \in \mathbb{F}_2^k$, $z \in \mathbb{F}_2^2$. For $i = 1, \ldots, k$, define a collection of Boolean functions $f_i : \mathbb{F}_2^m \to \mathbb{F}_2$ by

$$f_i(y, x, z) = (\phi_i(y), 00)\star(x, z).$$

We define a vectorial semi-bent function $F : \mathbb{F}_2^m \mapsto \mathbb{F}_2^k$ by

$$F(y, x, z) = (f_1, \ldots, f_k).$$

For any $c \in \mathbb{F}_2^k$, let $f_c(y, x, z) = c\star F(y, x, z) = c_1 f_1 + \ldots + c_k f_k$. For any fixed $\delta \in \mathbb{F}_2^2$, we define

$$L_\delta = \{(\beta, \alpha, \delta)\star(y, x, z) \mid \beta, \alpha \in \mathbb{F}_2^k)\}.$$

Let $T_0 = L_{00} \cup L_{11}$, $T_1 = L_{01}$ and $T_2 = L_{10}$. We construct $3 \cdot 2^k$ disjoint sets of sequences as follows:

$$S_{c,i} = \{\overline{f_c + l} \mid l \in T_i\}, \quad \text{for } c \in \mathbb{F}_2^k, i \in \{0, 1, 2\}. \tag{6}$$

Theorem 2 *Let $m = 2k+2$. For $c \in \mathbb{F}_2^k$, $i \in \{0, 1, 2\}$, let the sets of sequences $S_{c,i}$ be defined by (6) as in Construction 2. Then, we always have*

(i) For $c \in \mathbb{F}_2^k$, $\sharp S_{c,0} = 2^{m-1}$, $\sharp S_{c,1} = \sharp S_{c,2} = 2^{m-2}$;
(ii) For $c \in \mathbb{F}_2^{k*}$, $i \in \{0, 1, 2\}$, $S_{c,i}$ is a set of orthogonal semi-bent sequences;
(iii) For $c, c' \in \mathbb{F}_2^k$, $i, i' \in \{0, 1, 2\}$, $S_{c,i} \perp S_{c',i'}$ if and only if $i \neq i'$.

Proof Note that $\sharp L_\delta = 2^{2k} = 2^{m-2}$, which implies that (i) holds.
(ii) For $c = (c_1, \ldots, c_k) \in \mathbb{F}_2^{k*}$ and $y, x \in \mathbb{F}_2^k$, $z \in \mathbb{F}_2^2$, we have

$$\begin{aligned} f_c(y, x, z) &= \sum_{i=1}^{k} c_i f_i(y, x, z) = \sum_{i=1}^{k} c_i (\phi_i(y), 00)\star(x, z) \\ &= \pi\Big(\sum_{i=1}^{k} c_i \gamma^{[y]+i}\Big)\star x \\ &= \pi(\gamma^{i_c + [y]})\star x, \end{aligned} \tag{7}$$

where the last equality is due to the fact that there exists a unique $0 \leq i_c \leq 2^k - 2$ such that $\gamma^{i_c} = c\star(1, \ldots, \gamma^{k-1})$ if γ is primitive in $\mathbb{F}_{2^k}$. For any $(\beta, \alpha, \delta) \in \mathbb{F}_2^k \times \mathbb{F}_2^k \times \mathbb{F}_2^2$, we have

$$W_{f_c}(\beta, \alpha, \delta) = \sum_{(y,x,z) \in \mathbb{F}_2^m} (-1)^{f_c(y,x,z) + \beta\star y + \alpha\star x + \delta\star z}$$

Table 2 The operations between $T_i, i = 1, 2, 3$

$\oplus$	T_0	T_1	T_2
T_0	$L_{00} \cup L_{11}$	$L_{01} \cup L_{10}$	$L_{01} \cup L_{10}$
T_1	$L_{01} \cup L_{10}$	L_{00}	L_{11}
T_2	$L_{01} \cup L_{10}$	L_{11}	L_{00}

$$= \sum_{z\in\mathbb{F}_2^2}(-1)^{\delta\star z}\sum_{y\in\mathbb{F}_2^k}(-1)^{\beta\star y}\sum_{x\in\mathbb{F}_2^k}(-1)^{\pi(\gamma^{[y]+i_c})\star x+\alpha\star x}.$$

Note that π is bijective and there exists a unique $y \in \mathbb{F}_2^s$ such that $\pi(\gamma^{[y]+i_c}) = \alpha$, which implies

$$\sum_{x\in\mathbb{F}_2^k}(-1)^{\pi(\gamma^{[y]+i_c})\star x+\alpha\star x} = \begin{cases} \pm 2^k, & \text{if} \quad \pi^{-1}(\alpha) = \gamma^{[y]+i_c} \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, for any $\beta, \alpha \in \mathbb{F}_2^k$, we always have

$$\sum_{y\in\mathbb{F}_2^k}(-1)^{\beta\cdot y}\sum_{x\in\mathbb{F}_2^k}(-1)^{\pi(\gamma^{[y]+i_c})\star x+\alpha\star x} = \pm 2^k.$$

Noticing that

$$\sum_{z\in\mathbb{F}_2^2}(-1)^{\delta\star z} = \begin{cases} 4, & \text{if} \quad \delta = 0 \\ 0, & \text{otherwise,} \end{cases}$$

we have that for any $c \in \mathbb{F}_2^{k*}$,

$$W_{f_c}(\beta, \alpha, \delta) = \begin{cases} 0, & \text{if} \quad \delta \neq 0 \\ \pm 2^{k+2}, & \text{otherwise.} \end{cases} \tag{8}$$

By Definition 3, when $k = (m-2)/2$, F is a vectorial semi-bent function.
(iii) Let $\overline{f_c + l} \in S_{c,i}$ and $\overline{f_{c'} + l'} \in S_{c',i'}$, where $l \in T_i$ and $l' \in T_{i'}$. To analyze the orthogonality between $f_c + l$ and $f_{c'} + l'$ we consider

$$h = (f_c + l) + (f_{c'} + l') = f_{c+c'} + (l + l'),$$

where $l + l' \in T_i \oplus T_{i'}$ and $T \oplus T' = \{t + t' \mid t \in T, t' \in T'\}$. The equality $f_c + f_{c'} = f_{c+c'}$ comes easily from (7) by noting that

$$f_c(y, x, z) + f_{c'}(y, x, z) = \sum_{i=1}^{k}(c_i + c_i')\phi(y)\star x = f_{c+c'}(y, x, z).$$

By (8), $W_h(\mathbf{0}_m) = 0$ if and only if $l + l' \notin L_{00}$. Thanks to Table 2, $L_{00} \cap (T_i \oplus T_{i'}) = \emptyset$ if and only if $i \neq i'$. This means $S_{c,i} \perp S_{c',i'}$ if and only if $i \neq i'$.

We notice that the fact that f_i are semi-bent functions is easily deduced form the fact that $f_i'(y, x) = \phi(y) \cdot x$ are bent functions when ϕ is a permutation and therefore $f_i(y, x, z) = \phi(y) \cdot x$ can be viewed as concatenation of four identical functions $f_i(y, x)$ when $z \in \mathbb{F}_2^2$. The following example illustrates the assignment of orthogonal sets of sequences $S_{c,i}$ when $m = 8$, where $S_{c,0}$ corresponds to the cells having larger number of users 2^{m-1}.

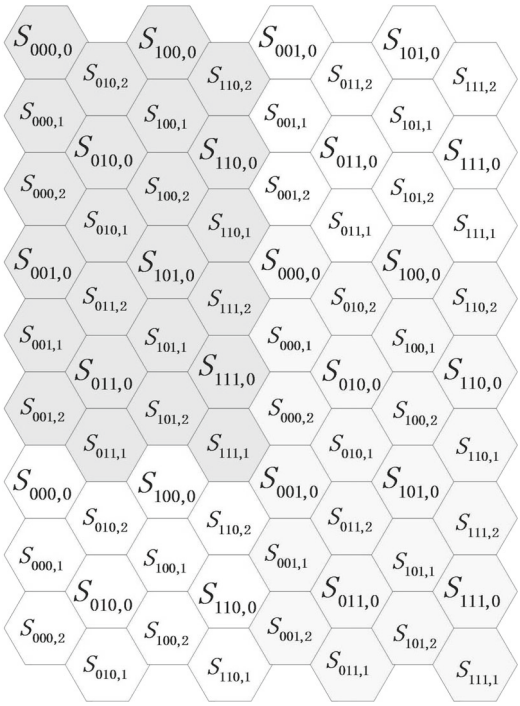

Fig. 3 Assignment of orthogonal cells for $m = 8$

Example 1 Let $m = 8$ so that $k = 3$. Using Construction 2, we can generate $3 \times 2^3 = 24$ disjoint sets of orthogonal semi-bent sequences

$$S_{c,i} = \{\overline{f_c + l} \mid l \in T_i\}, \quad \text{for } c \in \mathbb{F}_2^3, i \in \{0, 1, 2\},$$

where the sets $S_{c,0}$ have $2^{m-1} = 128$ users and the remaining sets have 64 users. The re-use distance is $D = \sqrt{21}$ according to the arrangement given in Fig. 3.

Remark 3 In Fig. 3 the cells containing 2^{m-1} users are depicted using larger fonts than the smaller ones. Notice that each large cell is surrounded by 6 small cells, whereas each small cell has exactly 3 small cells and 3 large cells as its neighbors. This also implies that one third of the cells in the network are large cells with 2^{m-1} users.

4.1 Allocation problem for arbitrary even *m*

Our design method can be employed for any even $m \geq 6$ though an efficient allocation is considered for $m = 8$ which resulted in the re-use distance $D = \sqrt{21}$. For practical applications, there are many indications that the re-use distance $D = 4$ is quite sufficient. The main problem related to our method is that for $m > 8$ the number of orthogonal cells $S_{c,i}$ becomes larger and therefore the assignment in hexagonal networks is more complicated. Moreover, the re-use distance of these orthogonal cells becomes unnecessarily large as illustrated in Table 3 and the array size to allocate these cells efficiently varies. Recall that the reuse distance D is computed as $D = \sqrt{i^2 + j^2 + ij}$, as mentioned previously.

To avoid large re-use distances and the problem of efficient packing of orthogonal cells in hexagonal networks, we suggest the use of method proposed in [19]. The main idea of this

Table 3 The re-use distance D and array size for different m

m	$3 \cdot 2^k$	D^2	Array size	i	j
6	12	12	6×2	2	2
8	24	21	6×4	4	1
10	48	48	12×4	4	4
12	96	93	24×4	7	4
14	192	192	24×4	8	8
16	384	381	384×1	19	1
18	768	768	48×16	16	16

approach is to keep an efficient cell assignment specified for a fixed m (in our case $m = 8$ and the assignment is given in Fig. 3) and for larger m one employs vectorial bent functions of suitable dimension. The details of this method are given in [19] but for self-completeness we briefly discuss the main idea. In order to keep the cell assignment given for $m = 8$ and at the same time to increase the number of users (which for $m = 8$ equals to 128 and 64 in large and small cells, respectively) we proceed as follows. To assign sets of orthogonal sequences to different cells in the network for $m > 8$, we utilize a vectorial bent function $H : \mathbb{F}_2^u \to \mathbb{F}_2^k$, where $u \geq 2k$ and u is even, as follows.

Let us define $G : \mathbb{F}_2^{m+u} \to \mathbb{F}_2^k$ as a direct sum of $F(y, x, z)$ defined as in Construction 2 (thus $F : \mathbb{F}_2^m \to \mathbb{F}_2^k$) and $H(v)$, so that $G = F(x, y, z) + H(v)$. It can be easily verified, due to the fact that H is vectorial bent, that the linear combinations $g_c = f_c + h_c$, where $f_c = c \cdot F$ and $h_c = c \cdot H$, are semi-bent functions for $c \in \mathbb{F}_2^{k*}$. Then, for $c \in \mathbb{F}_2^k$, $i = 0, 1, 2$, let $S_{c,i} = \{\overline{f_c + l} \mid l \in T_i\}$ be constructed by using F as defined in Construction 2, thus $\sharp S_{c,0} = 2^{m-1}$, $\sharp S_{c,1} = \sharp S_{c,2} = 2^{m-2}$. Then, defining $S'_{c,i} = \{\overline{g_c + l} \mid l \in T'_i\}$, where the set of linear functions $T'_i = T_i + \gamma \cdot v$ for $\gamma \in \mathbb{F}_2^u$, we have $\sharp T'_i = 2^u \sharp T_i$. It is easy to verify that the sets $S'_{c,i}$ and $S'_{c,j}$ are orthogonal to each other when $i \neq j$, and apparently $\sharp S'_{c,0} = 2^{u+m-1}$, $\sharp S'_{c,1} = \sharp S'_{c,2} = 2^{u+m-2}$.

Thus, the same cell allocation as given in Fig. 3 can be employed for assigning 2^{8+u-1} users to large cells and 2^{8+u-2} many users to small cells, using the codewords of length 2^{8+u} for any even $u \geq 6$. This way we preserve the original re-use distance $D = \sqrt{21}$ and avoid complicated cell assignments when larger codewords are used. To cover the remaining even values of m (notice that the above approach provides a general solution for $m \geq 14$) it would be of interest to consider the case $m = 6$ and the assignment of $3 \cdot 4 = 12$ orthogonal sets in hexagonal network. One such assignment is given in Fig. 4, where the re-use distance $D = \sqrt{12}$. This efficiently resolves the cases $m \in \{6, 10, 12\}$ though giving a slightly smaller re-use distance $D = \sqrt{12}$.

Remark 4 One can show that this particular approach cannot be improved further in terms of achieving even larger number of users per cell.

5 Conclusions

In this paper, we have provided an efficient design method of constructing multiple sets of orthogonal sequences for S-CDMA and QS-CDMA applications. Most notably, our design ensures that the number of orthogonal sequences in any three adjacent cells (referring to regular hexagonal networks) is equal to p^m for the sequences of length p^m. This is the

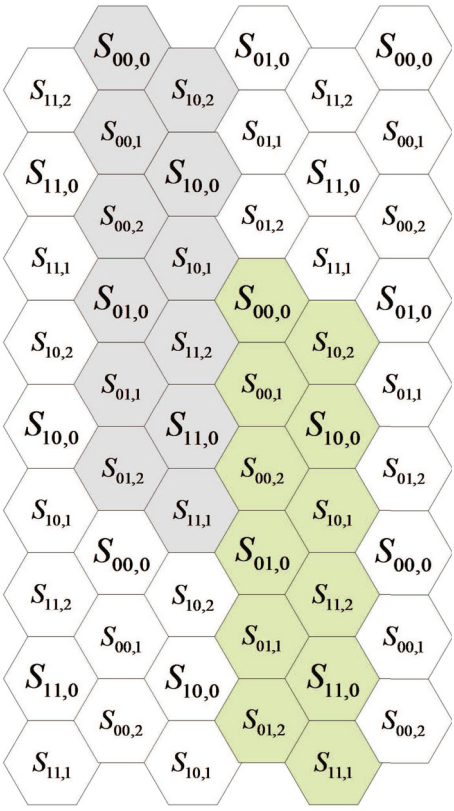

Fig. 4 Assignment of orthogonal cells for $m = 6$

maximal cardinality that can be achieved and therefore our method is optimized and cannot be improved further in this aspect. To address QS-CDMA applications as well, an efficient method to combine these orthogonal sequences with Zadeoff–Chu sequences is proposed for the purpose of designing sets of zero correlation zone (ZCZ) sequences (within a certain shift zone) with optimal parameters, thus reaching the Tang–Fan–Matsufuji bound. Finally, using vectorial semi-bent functions, we provide an efficient design of binary orthogonal sequences of length 2^m so that one third of the network contains cells that comprise 2^{m-1} users whereas two thirds of the network have cells that accommodate 2^{m-2} users. This is an improvement over [19] where 2^{m-2} users were assigned to each cell in a hexagonal network.

Acknowledgements W.-G. Zhang is supported by the National Natural Science Foundation of China (No. 61972303). E. Pasalic is supported in part by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694, N1-0159, J1-2451).

References

1. Chee S., Lee S., Kim K.: Semi-bent functions. In: Advances in Cryptology-ASIACRYPT'94, vol. 917, pp. 107–118. LNCS. Springer, Berlin (1994).
2. Dinan E., Jabbari B.: Spreading codes for direct sequence CDMA and wideband CDMA cellular networks. IEEE Commun. Mag. **36**, 48–54 (1998).

3. Fan P.: Spreading sequence design and theoretical limits for quasisynchronous CDMA systems. EURASIP J. Wirel. Commun. Netw. **1**, 19–31 (2004).
4. Fan P., Hao L.: Generalized orthogonal sequences and their applications in synchronous CDMA systems. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E83-A, 2054–2069 (2000).
5. Fan P., Suehiro N., Kuroyanagi N., Deng X.M.: Class of binary sequences with zero correlation zone. Electron. Lett. **35**, 777–779 (1999).
6. Gu Z., Zhou Z., Mesnager S., Parampalli U.: A new family of polyphase sequences with low correlation. Cryptogr. Commun. **14**, 135–144 (2022).
7. Hu S., Liu Z., Guan Y.L., Xiong W., Bi G., Li S.: Sequence design for cognitive CDMA communications under arbitrary spectrum hole constraint. IEEE J. Sel. Areas Commun. **32**, 1974–1986 (2014).
8. Hunt F.H., Smith D.H.: The construction of orthogonal variable spreading factor codes from semi-bent functions. IEEE Trans. Wirel. Commun. **11**, 2970–2975 (2012).
9. Li J., Fan J., Tang X.: A Generic construction of generalized chirp-Like sequence sets with optimal zero correlation property. IEEE Commun. Lett. **17**, 549–552 (2013).
10. Matsufuji S., Suehiro N.: Complex Hadamard matrices related to bent sequences. IEEE Trans. Inf. Theory **42**, 637 (1996).
11. Popovic B.M., Mauritz O.: Generalized chirp-like sequences with zero correlation zone. IEEE Trans. Inf. Theory **56**, 2957–2960 (2010).
12. Popovic B.M., Suehiro N., Fan P.: Orthogonal sets of quadriphase sequences with good correlation properties. IEEE Trans. Inf. Theory **48**, 956–959 (2002).
13. Smith D.H., Ward R.P., Perkins S.: Gold codes, Hadamard partitions and the security of CDMA systems. Des. Codes Cryptogr. **51**, 231–243 (2009).
14. Smith D.H., Hunt F.H., Perkins S.: Exploiting spatial separations in CDMA systems with correlation constrained sets of Hadamard matrices. IEEE Trans. Inf. Theory **56**, 5757–5761 (2010).
15. Tang X., Fan P., Matsufuji S.: Lower bounds on correlation of spreading sequence set with low or zero correlation zone. Electron. Lett. **30**, 551–552 (2000).
16. Tang X., Mow W.H.: Design of spreading codes for quasi-synchronous CDMA with intercell interference. IEEE J. Sel. Areas Commun. **24**, 84–93 (2006).
17. Tang X., Fan P., Lindner J.: Multiple binay ZCZ sequence sets with good cross-correlation property based on complementary sequence sets. IEEE Trans. Inf. Theory **56**, 4038–4045 (2010).
18. Yang K., Kim Y.K., Kumar P.V.L.: Quasi-orthogonal sequences for code-division multiple-access systems. IEEE Trans. Inf. Theory **46**, 982–993 (2000).
19. Zhang W.G., Xie C.L., Pasalic E.: Large sets of orthogonal sequences suitable for applications in CDMA systems. IEEE Trans. Inf. Theory **62**, 3757–3767 (2016).
20. Zhang L., Sun Y.: The optimal assignment of orthogonal polyphase sequences in CDMA systems. IEEE Commun. Lett. **22**, 109–112 (2018).
21. Zhou Z., Zhang D., Helleseth T., Wen J.: A construction of multiple optimal ZCZ sequence sets with good cross correlation. IEEE Trans. Inf. Theory **64**, 1340–1346 (2018).