Cryptography and Communications (2024) 16:89–108
https://doi.org/10.1007/s12095-023-00632-8

RESEARCH

New supersets of Zadoff-Chu sequences via the Weil bound

Shilu Liu[1] · Zhengchun Zhou[1] · Avik Ranjan Adhikary[1] · Yang Yang[1]

Received: 16 October 2022 / Accepted: 26 January 2023 / Published online: 13 March 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
Sequences with low correlation have important applications in communications, radar, and cryptography. Recently, Pitaval et al. proposed two enlarged supersets of Zadoff-Chu (ZC) sequences with low correlation zone (LCZ) property to overcome physical random access channel (PRACH) capacity shortfall in 5G. In this paper, we present several classes of generalized supersets of ZC sequences using the Weil bound of exponential sums over finite fields. We employ ZC sequences and traditional sequences like m-sequences, binary Gold sequences and p-phase sequences as covers to propose several new classes of supersets of ZC sequences. The proposed sequence families have more flexible parameters compared to previous constructions. Interestingly, one of the resultant sequence sets is asymptotically optimal with respect to the Welch bound.

Keywords Binary Gold sequences · Exponential sums · Low correlation zone (LCZ) · m-sequences · p-phase sequences · Physical random access channel (PRACH) · Weil bound · Zadoff-Chu (ZC) sequences

Mathematics Subject Classification (2010) 94A55

Zhengchun Zhou, Shilu Liu, Avik Ranjan Adhikary and Yang Yang are contributed equally to this work.

✉ Zhengchun Zhou
zzc@swjtu.edu.cn

Shilu Liu
LSL17@my.swjtu.edu.cn

Avik Ranjan Adhikary
avik.adhikary@ieee.org

Yang Yang
yang_data@swjtu.edu.cn

[1] School of Mathematics, Southwest Jiaotong University, Chengdu, 611756, Sichuan, China

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

1 Introduction

The physical random access channel (PRACH) in a cellular network transmits uplink (UL) synchronisation signals to create initial link between a user equipment (UE) and a base station (BS). To identify several UEs accessing the network at the same time, multiple PRACH signals, also known as preambles, should be supported by the network. The preambles must have low out-of-phase auto-correlation and low cross-correlations in order for the BS to accurately recognise numerous preambles and estimate their timing for synchronisation.

In order to support new features such as high-speed transmissions, millimetre-wave, and low-latency, 5G NR introduces many new preamble formats, designed from a short sequence and wider subcarrier spacings (SCSs). This combination, however, dramatically decreases the number of PRACH preambles that can be used in a network [1, 2]. Working on this problem, the authors in [3] based on [4] redesigned the PRACH preambles from a totally new sequence set. Based on multi-preamble transmissions, several PRACH preamble designs were also proposed in [5–7]. However, none of the constructions improved the PRACH spectral efficiency [7].

To expand an existing sequence set which can be used as 5G PRACH preambles, the additional new sequences should be carefully chosen in order to maintain the correlation properties. Recently in [8, 9], Pitaval et al. designed the ZC_m and ZC_a sequence supersets with low correlation zone (LCZ) property to overcome PRACH capacity shortfall. The ZC_a and ZC_m sequence supersets are constructed by elementwise multiplication of Zadoff-Chu (ZC) sequences [10] with Alltop sequence covers and m-sequence covers of the same period, respectively [8, 9]. In both the constructions, correlation properties of the resultant sequences are similar to that of the ZC sequences, and set sizes are greatly increased compared to ZC sequences.

Motivated by the work of [8, 9], in search of large ZC supersets to overcome the PRACH capacity shortfall, we derive several new classes of generalized supersets of ZC sequences with low correlation and flexible parameters, from the Weil bound on exponential sums over finite fields. In 1948 Weil [11] proved the following celebrated fact.

Fact 1 ([11]) Let p be a prime number, m be a positive integer, and $\mathbb{F}_{p^m}$ denote the finite field with p^m elements. Let χ be a nontrivial additive character of $\mathbb{F}_{p^m}$ and $f(x) \in \mathbb{F}_{p^m}[x]$ with $\deg(f) = d \geq 1$ and $\gcd(d, p) = 1$. Then

$$\left| \sum_{x \in \mathbb{F}_{p^m}} \chi(f(x)) \right| \leq (d-1)\sqrt{p^m}. \tag{1}$$

Fact 2 ([12, 13]) Let χ be a nontrivial additive character of $\mathbb{F}_{p^m}$, and ψ be a nontrivial multiplicative character of $\mathbb{F}_{p^m}$ with order M and define $\psi(0) = 0$. Let $f(x) \in \mathbb{F}_{p^m}[x]$ with degree d, and $g(x) \in \mathbb{F}_{p^m}[x]$ with s distinct roots in $\overline{\mathbb{F}}_{p^m}$ where $g(x) \neq c \cdot h^M(x)$ for some $c \in \mathbb{F}_{p^m}$ and $h(x) \in \mathbb{F}_{p^m}[x]$. Then

$$\left| \sum_{x \in \mathbb{F}_{p^m}} \psi(g(x))\chi(f(x)) \right| \leq (d+s-1)\sqrt{p^m}. \tag{2}$$

In literature, the Weil bound [11] has been efficiently used to design several families of sequences of low correlaton [14–19]. Following those constructions, we construct four new classes of generalized supersets of ZC sequences with low correlation and flexible parameters. First, using the properties of trace function we propose two supersets of ZC sequences

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

by elementwise multiplication of ZC sequences of period L with m-sequence covers of period N, where $N = p^m - 1 = LK$, p is a prime number, and m is a positive integer. The ZC_m sequence subset proposed in [8, 9] can be seen as a special case of one of the proposed constructions. Next, using the Weil bound of exponential sums, we propose two new classes of supersets of ZC sequences, ZC_{bG} and ZC_p. ZC_{bG} consists of ZC sequences with binary Gold sequence covers. ZC_p consists of ZC sequences with p-phase sequence covers. Table 1 gives an overview of the proposed and existing supersets of ZC sequences till date. From Table 1, it can be observed that the proposed sequence set in Theorem 1 provides a flexible tradeoff between the family size and alphabet size without changing the maximum correlation and the sequence period, and the proposed sequence sets in Theorem 2 and 3 have larger PRACH capacities than the previous ZC sequence set and its supersets.

The rest of this paper is organized as follows. In Section 2, we recall the basic notations and definitions. In Section 3, we propose ZC_m sequence sets which consist of ZC sequences of short period with m-sequence covers of long period, and give some examples. In Section 4, we propose ZC_{bG} sequence sets which consist of ZC sequences with binary Gold sequence covers, and give some examples. In Section 5, we propose ZC_p sequence sets which consist of ZC sequences with p-phase sequence covers, and give some examples. In Section 6, we compare the proposed supersets of ZC sequences with previous works. We conclude the paper in Section 7.

2 Preliminaries

Let us fix some notations before we begin.

- a^* denotes the conjugate of a complex number a;
- $\langle x \rangle_y$ denotes the least nonnegative residue of x modulo y for an integer x and a positive integer y;
- $\mathbb{F}_{p^m}$ denotes the finite field with p^m elements, where p is a prime number and m is a positive integer;
- $\zeta_n = e^{\frac{2\pi h\sqrt{-1}}{n}}$ denotes a primitive n-th complex root of unity, where $\gcd(h, n) = 1$;
- The period in this paper represents the minimum positive period.

Definition 1 Let $\mathbf{x} = (x(0), x(1), \cdots, x(N-1))$ and $\mathbf{y} = (y(0), y(1), \cdots, y(N-1))$ be two sequences of period N. Then the periodic crosscorrelation between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$R_{\mathbf{x},\mathbf{y}}(\tau) = \sum_{n=0}^{N-1} x(n)y(\langle n+\tau \rangle_N)^*, \quad 0 \le |\tau| \le N-1. \tag{3}$$

When $\mathbf{x} = \mathbf{y}$, $R_{\mathbf{x},\mathbf{y}}(\tau)$ is called the autocorrelation of $\mathbf{x}$, and is denoted by $R_{\mathbf{x}}(\tau)$.

Definition 2 Let Z be a positive integer, and $\mathcal{S}$ be a family of M polyphase sequences of period N. The maximum correlation of $\mathcal{S}$ with a zone Z is defined by

$$\begin{aligned}\Theta(\mathcal{S}; Z) = \max\{|R_{\mathbf{x},\mathbf{y}}(\tau)| : \mathbf{x}, \mathbf{y} \in \mathcal{S}, (\mathbf{x} = \mathbf{y}, 0 < |\tau| < Z) \\ \text{or } (\mathbf{x} \ne \mathbf{y}, 0 \le |\tau| < Z)\}.\end{aligned} \tag{4}$$

Accordingly, $\mathcal{S}$ is said to be an $(N, M, Z, \Theta(\mathcal{S}; Z))$ sequence set.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Table 1 Properties of proposed supersets compared to original ZC Set and ZC supersets of period N with LCZ of length N_{CS}

	# of sequences per subset	Intra-subset LCZ $\Theta(\mathcal{S}_k; N_{CS})$	# of subsets	Inter-subset Corr. $\Omega(\mathcal{S}_k, \mathcal{S}_j)$	PRACH capacity	Superset optimality factor $\rho^{(\mathcal{S})}$ when $N_{CS} = N$	Constraint
ZC[1]	$\lfloor \frac{N}{N_{CS}} \rfloor$	0	$N-1$	$\sqrt{N}$	$(N-1)\lfloor \frac{N}{N_{CS}} \rfloor$	1	N is a prime number.
	$(N-1)\lfloor \frac{N}{N_{CS}} \rfloor$	$\sqrt{N}$	1	n/a		1	
ZC_m[8]	$(N+1)\lfloor \frac{N}{N_{CS}} \rfloor$	$\sqrt{N+1}$	$N-1$	$\approx 2\sqrt{N+1} + \log_2(N+1)$	$(N^2-1)\lfloor \frac{N}{N_{CS}} \rfloor$	2	$N = p^m - 1$ is a prime number.
ZC_a[9]	$N\lfloor \frac{N}{N_{CS}} \rfloor$ one subset with $(N-1)\lfloor \frac{N}{N_{CS}} \rfloor$	$\sqrt{N}$	N	$\leq 2\sqrt{N}$	$(N^2-1)\lfloor \frac{N}{N_{CS}} \rfloor$	2	N is a prime number.
Theorem 1	$(N+1)\lfloor \frac{L}{N_{CS}} \rfloor$	$\sqrt{N+1}$	1	n/a	$(N+1)\lfloor \frac{L}{N_{CS}} \rfloor$	n/a	$N = p^m - 1 = LK$
Corollary 1	L	$\sqrt{N+1}$	1	n/a	L	1	$N = p^m - 1 = LK$
Theorem 2	$N\lfloor \frac{N}{N_{CS}} \rfloor$ one subset with $(N+1)\lfloor \frac{N}{N_{CS}} \rfloor$	$\leq 3\sqrt{N+1}$	$N+2$	$\leq 3\sqrt{N+1}$	$(N^2+2N+1)\lfloor \frac{N}{N_{CS}} \rfloor$	3	$N = 2^m - 1$, where m is an odd number.
Theorem 3	$N\lfloor \frac{N}{N_{CS}} \rfloor$ one subset with $(N+1)\lfloor \frac{N}{N_{CS}} \rfloor$	$\leq d\sqrt{N+1}$	$(N+1)^{d-1}$	$\leq d\sqrt{N+1}$	$\left(N(N+1)^{d-1}+1\right)\lfloor \frac{N}{N_{CS}} \rfloor$	d	$N = p^m - 1$, where p is an odd number.

1) p is a prime number and m is a positive integer;

2) d is a positive integer with $1 < d < p$; and

3) the superset optimality factor $\rho^{(\mathcal{S})}$ is defined in (15)

Springer
Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Definition 3 Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two disjoint sets, consisting of sequences of the same period N. Then the inter-set correlation is defined as

$$\Omega(\mathcal{S}_1, \mathcal{S}_2) = \max_{\substack{\mathbf{x}\in\mathcal{S}_1, \mathbf{y}\in\mathcal{S}_2 \\ 0\le|\tau|<N}} |R_{\mathbf{x},\mathbf{y}}(\tau)|. \tag{5}$$

Lemma 1 *The Welch bound* [20] *for* $\mathcal{S}$ *is given by*

$$\Theta(\mathcal{S}; N) \ge N\sqrt{\frac{M-1}{MN-1}}, \tag{6}$$

provided that $\sum_{n=0}^{N-1}|x(n)|^2 = N$ *(which is satisfied for polyphase sequences). We call the sequence set* $\mathcal{S}$ *optimal with respect to the Welch bound if* $\Theta(\mathcal{S}; N)$ *satisfies* (6) *with equality. For a given sequence set* $\mathcal{S}$*, we denote the Welch bound by* Θ_{opt}.

Definition 4 The well-known Zadoff-Chu (ZC) [10] sequences $\mathbf{x}_u = (x_u(0), x_u(1), \cdots, x_u(N-1))$ of period N with root u are defined as

$$x_u(n) = \zeta_N^{\frac{un(n+\langle N\rangle_2)}{2}+qn}, \ 0 \le n \le N-1, \tag{7}$$

where q and u are integers, with $\gcd(u, N) = 1$.

Definition 5 The absolute trace function Tr from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ is defined by

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{m-1}}, \ x \in \mathbb{F}_{p^m}. \tag{8}$$

Definition 6 (Additive Character) An additive character of $\mathbb{F}_{p^m}$ is a nonzero function χ from $\mathbb{F}_{p^m}$ to the set of complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \mathbb{F}_{p^m}^2$. For each $a \in \mathbb{F}_{p^m}$, the function

$$\chi(x) = \zeta_p^{\mathrm{Tr}(ax)}, \quad x \in \mathbb{F}_{p^m}, \tag{9}$$

defines an additive character of $\mathbb{F}_{p^m}$. When $a = 0$, $\chi(x) = 1$ for all $x \in \mathbb{F}_{p^m}$, and is called the trivial additive character of $\mathbb{F}_{p^m}$.

Definition 7 (Multiplicative Character) A multiplicative character of $\mathbb{F}_{p^m}$ is a nonzero function ψ from $\mathbb{F}_{p^m}^*$ to the set of complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for any pair $(x, y) \in \mathbb{F}_{p^m}^* \times \mathbb{F}_{p^m}^*$, where $\mathbb{F}_{p^m}^* = \mathbb{F}_{p^m}\backslash\{0\}$ denotes the multiplicative group of $\mathbb{F}_{p^m}$. For $M|(p^m-1)$ and each $j = 0, 1, \cdots, M-1$, the function ψ

$$\psi\left(\alpha^k\right) = \zeta_M^{jk}, \quad \text{for } k = 0, 1, \cdots, p^m - 2, \tag{10}$$

defines a multiplicative character of $\mathbb{F}_{p^m}$ of order M. When $j = 0$, $\psi(x) = 1$ for all $x \in \mathbb{F}_{p^m}^*$, and is called the trivial multiplicative character of $\mathbb{F}_{p^m}$.

Definition 8 Let p be a prime number, m be a positive integer and $N = p^m - 1$. Then the m-sequence [21] $\mathbf{c} = (c(0), c(1), \cdots, c(N-1))$ of period N as

$$c(n) = \chi(\alpha^n), \ 0 \le n \le N-1, \tag{11}$$

where χ denotes the additive canonical character of $\mathbb{F}_{p^m}$ and α is a primitive element of $\mathbb{F}_{p^m}$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Definition 9 Let m be an odd number and $N = 2^m - 1$. Then for $0 \le i \le 2^m$, the Gold [22] sequences $\mathbf{a}_i = (a_i(0), a_i(1), \cdots, a_i(N-1))$ of period N can be defined as

$$a_i(n) = \begin{cases} \chi(\alpha^{i+n} + \alpha^{3n}), & \text{for } 0 \le i \le 2^m - 2, \\ \chi(\alpha^{3n}), & \text{for } i = 2^m - 1, \\ \chi(\alpha^n), & \text{for } i = 2^m, \end{cases} \tag{12}$$

where χ denotes the additive canonical character of $\mathbb{F}_{2^m}$ and α is a primitive element of $\mathbb{F}_{2^m}$.

Definition 10 Let p be an odd prime number, m and d be two positive integers with $1 < d < p$, and $N = p^m - 1$. For all $\Delta = (\delta_1, \delta_2, \cdots, \delta_{d-1}) \in \mathbb{F}_{p^m}^{d-1}$, the sequences $\mathbf{b}_\Delta = (b_\Delta(0), b_\Delta(1), \cdots, b_\Delta(N-1))$ of period N can be defined as

$$b_\Delta(n) = \chi(\alpha^n + \delta_1\alpha^{2n} + \delta_2\alpha^{3n} + \cdots + \delta_{d-1}\alpha^{dn}), \quad 0 \le n \le N-1, \tag{13}$$

where χ denotes the additive canonical character of $\mathbb{F}_{p^m}$ and α is a primitive element of $\mathbb{F}_{p^m}$.

Lemma 2 ([12]) *Let p be a prime number, m be a positive integer, and $a \in \mathbb{F}_{p^m}$. Then*

$$\sum_{n=0}^{p^m-2} \chi(a\alpha^n) = \begin{cases} p^m - 1, & a = 0, \\ -1, & a \ne 0. \end{cases} \tag{14}$$

where χ denotes the additive canonical character of $\mathbb{F}_{p^m}$ and α is a primitive element of $\mathbb{F}_{p^m}$.

Definition 11 For a given superset $\mathcal{S}$ of ZC sequences, consisting of sequences of period N, the superset optimality factor $\rho^{(\mathcal{S})}$ is defined as

$$\rho^{(\mathcal{S})} = \lim_{N\to\infty} \frac{\Theta(\mathcal{S}; N)}{\Theta_{opt}}. \tag{15}$$

When $\rho^{(\mathcal{S})} = 1$, we say that $\mathcal{S}$ is asymptotically optimal with respect to the Welch bound.

3 ZC Sequences of short period with *m*-sequence covers (ZC$_m$)

In this section, we use m-sequence to cover ZC sequences of short period and propose two families of sequences with low correlation. We hereby define $N = p^m - 1 = LK$ until the end of this section to avoid definition confusion, where p is a prime number and m, L, K are three positive integers.

According to (7), the ZC sequence $\mathbf{y}_u = (y_u(0), y_u(1), \cdots, y_u(L-1))$ of period L is defined as

$$y_u(n) = \zeta_L^{\frac{un(n+\langle L\rangle_2)}{2}+qn}, \quad 0 \le n \le L-1. \tag{16}$$

$\mathbf{y}_u$ is shifted with a constant value $0 < N_{CS} \le L$ such that it enables unambiguous detection with timing uncertainty $|\tau| < N_{CS}$. Then cyclically-shifted ZC sequences are generated as

$$y_{(u,v)}(n) = y_u(\langle n + C_v\rangle_L), \quad 0 \le n \le L-1, \tag{17}$$

where $C_v = vN_{CS}$ with $0 \le v \le \lfloor \frac{L}{N_{CS}} \rfloor - 1$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Next, we construct new sequences $\mathbf{z}_{(u,v,w)}$ of period N by elementwise multiplication of $\mathbf{y}_{(u,v)}$ with $\mathbf{c}_w$ for $0 \le w \le N-1$, as

$$z_{(u,v,w)}(n) = y_{(u,v)}(n) \cdot c_w(n), \quad 0 \le n \le N-1, \tag{18}$$

where

$$c_w(n) = c(\langle n+w \rangle_N), \quad 0 \le n \le N-1, \tag{19}$$

are cyclic-shifts of m-sequences, given in (11) and u is a constant with $gcd(u, L) = 1$.

Theorem 1 *Let p be a prime number, and N, m, L, K be four positive integers satisfying $N = p^m - 1 = LK$. Let N_{CS} be an integer with $0 < N_{CS} \le L$ and u be a constant with $gcd(u, L) = 1$. Then, the sequence family*

$$\mathcal{S}_1 = \{\mathbf{y}_{(u,v)}\}_{v=0}^{\lfloor \frac{L}{N_{CS}} \rfloor - 1} \bigcup_{w=0}^{N-1} \{\mathbf{z}_{(u,v,w)}\}_{v=0}^{\lfloor \frac{L}{N_{CS}} \rfloor - 1},$$

is an $\left(N, (N+1)\lfloor \frac{L}{N_{CS}} \rfloor, N_{CS}, \sqrt{N+1}\right)$ sequence set with the following properties:

- *If $\mathbf{y} = \mathbf{y}_{(u,v)}$ and $\mathbf{y}' = \mathbf{y}_{(u,v')}$, then we have*

$$|R_{\mathbf{y},\mathbf{y}'}(\tau)| = \begin{cases} N, & \text{if } L \mid C_v - C_{v'} - \tau, \\ 0, & \text{if } L \nmid C_v - C_{v'} - \tau. \end{cases} \tag{20}$$

- *If $\mathbf{y} = \mathbf{y}_{(u,v)}$ and $\mathbf{z} = \mathbf{z}_{(u,v',w)}$, then we have*

$$|R_{\mathbf{y},\mathbf{z}}(\tau)| = \begin{cases} 1, & \text{if } L \mid C_v - C_{v'} - \tau, \\ \sqrt{N+1}, & \text{if } L \nmid C_v - C_{v'} - \tau, \end{cases} \tag{21}$$

and

$$|R_{\mathbf{z},\mathbf{y}}(\tau)| = \begin{cases} 1, & \text{if } L \mid C_{v'} - C_v - \tau, \\ \sqrt{N+1}, & \text{if } L \nmid C_{v'} - C_v - \tau. \end{cases} \tag{22}$$

- *If $\mathbf{x} = \mathbf{z}_{(u,v,w)}$ and $\mathbf{x}' = \mathbf{z}_{(u,v',w')}$, then we have*

$$|R_{\mathbf{x},\mathbf{x}'}(\tau)| = \begin{cases} N, & \text{if } \tau = \langle w - w' \rangle_N \text{ and } L \mid C_v - C_{v'} - \tau, \\ 0, & \text{if } \tau = \langle w - w' \rangle_N \text{ and } L \nmid C_v - C_{v'} - \tau, \\ 1, & \text{if } \tau \ne \langle w - w' \rangle_N \text{ and } L \mid C_v - C_{v'} - \tau, \\ \sqrt{N+1}, & \text{if } \tau \ne \langle w - w' \rangle_N \text{ and } L \nmid C_v - C_{v'} - \tau, \end{cases} \tag{23}$$

where $\mathbf{y}_{(u,v)}$ and $\mathbf{z}_{(u,v,w)}$ are given in (17) and (18) respectively.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Proof For $\mathbf{y} = \mathbf{y}_{(u,v)}$ and $\mathbf{y}' = \mathbf{y}_{(u,v')}$, we have

$$\begin{aligned} |R_{\mathbf{y},\mathbf{y}'}(\tau)| &= |\zeta_L^{\frac{u(C_v - C_{v'} - \tau)(C_v + C_{v'} + \tau + \langle L \rangle_2)}{2} + q(C_v - C_{v'} - \tau)} \cdot \sum_{n=0}^{N-1} \zeta_L^{un(C_v - C_{v'} - \tau)}| \\ &= |\sum_{n=0}^{N-1} \zeta_L^{un(C_v - C_{v'} - \tau)}| \\ &= \begin{cases} N, & \text{if } L \mid C_v - C_{v'} - \tau, \\ 0, & \text{if } L \nmid C_v - C_{v'} - \tau. \end{cases} \end{aligned} \tag{24}$$

Hence (20) is derived.

For $\mathbf{y} = \mathbf{y}_{(u,v)}$ and $\mathbf{z} = \mathbf{z}_{(u,v',w)}$, we have

$$\begin{aligned} |R_{\mathbf{y},\mathbf{z}}(\tau)| &= \left| \zeta_L^{\frac{u(C_v - C_{v'} - \tau)(C_v + C_{v'} + \tau + \langle L \rangle_2)}{2} + q(C_v - C_{v'} - \tau)} \right. \\ &\quad \left. \cdot \sum_{n=0}^{N-1} \zeta_L^{un(C_v - C_{v'} - \tau)} \cdot \chi(-\alpha^{n+\tau+w}) \right| \\ &= \left| \sum_{n=0}^{N-1} \zeta_L^{un(C_v - C_{v'} - \tau)} \cdot \chi(-\alpha^{n+\tau+w}) \right|. \end{aligned} \tag{25}$$

When $L \mid C_v - C_{v'} - \tau$, using Lemma 2, we get from (25),

$$\begin{aligned} |R_{\mathbf{y},\mathbf{z}}(\tau)| &= \left| \sum_{n=0}^{N-1} \chi(-\alpha^{n+\tau+w}) \right| = \left| \sum_{n=0}^{p^m-2} \chi(-\alpha^{\tau+w} \cdot \alpha^n) \right| \\ &= 1. \end{aligned} \tag{26}$$

When $L \nmid C_v - C_{v'} - \tau$, squaring both sides of (25), we have

$$\begin{aligned} |R_{\mathbf{y},\mathbf{z}}(\tau)|^2 &= \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} \chi(\alpha^{\tau+w}(\alpha^{n_2} - \alpha^{n_1})) \cdot \zeta_L^{u(n_1-n_2)(C_v - C_{v'} - \tau)} \\ &= \sum_{n_1=0}^{N-1} \sum_{j=1-N+n_1}^{n_1} \chi(\alpha^{\tau+w}(\alpha^{n_1-j} - \alpha^{n_1})) \cdot \zeta_L^{uj(C_v - C_{v'} - \tau)} \\ &= \sum_{n_1=0}^{N-1} \sum_{j=0}^{N-1} \chi(\alpha^{\tau+w}(\alpha^{n_1-j} - \alpha^{n_1})) \cdot \zeta_L^{uj(C_v - C_{v'} - \tau)} \\ &= \sum_{j=0}^{N-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \sum_{n_1=0}^{p^m-2} \chi(\alpha^{\tau+w}(\alpha^{n_1-j} - \alpha^{n_1})) \\ &= p^m - 1 + \sum_{j=1}^{N-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \cdot (-1) \text{ (using Lemma 2)} \\ &= p^m + \sum_{j=0}^{N-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \cdot (-1) \\ &= p^m = N + 1. \end{aligned} \tag{27}$$

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Therefore we have $|R_{\mathbf{y},\mathbf{z}}(\tau)| = \sqrt{N+1}$, and hence, (21) is obtained. The results in (22) can be obtained similarly.

Next, consider $\mathbf{x} = \mathbf{z}_{(u,v,w)}$ and $\mathbf{x}' = \mathbf{z}_{(u,v',w')}$, then we have

$$\begin{aligned} |R_{\mathbf{x},\mathbf{x}'}(\tau)| &= \Bigg| \zeta_L^{\frac{u(C_v - C_{v'} - \tau)(C_v + C_{v'} + \tau + \langle L \rangle_2)}{2} + q(C_v - C_{v'} - \tau)} \\ &\quad \cdot \sum_{n=0}^{N-1} \zeta_L^{un(C_v - C_{v'} - \tau)} \cdot \chi(\alpha^n(\alpha^w - \alpha^{w'+\tau})) \Bigg| \\ &= \Bigg| \sum_{n=0}^{N-1} \zeta_L^{un(C_v - C_{v'} - \tau)} \cdot \chi(\alpha^n(\alpha^w - \alpha^{w'+\tau})) \Bigg|. \end{aligned} \tag{28}$$

For $\tau = \langle w - w' \rangle_N$ and $L \mid C_v - C_{v'} - \tau$, we have $\zeta_L^{un(C_v - C_{v'} - \tau)} = 1$ and $\chi(\alpha^n(\alpha^w - \alpha^{w'+\tau})) = 1$ for any $0 \le n \le N-1$. Hence from (28) we have $|R_{\mathbf{x},\mathbf{x}'}(\tau)| = N$. For $\tau = \langle w - w' \rangle_N$ and $L \nmid C_v - C_{v'} - \tau$, we have $\chi(\alpha^n(\alpha^w - \alpha^{w'+\tau})) = 1$ for any $0 \le n \le N-1$. Hence from (28) we have $|R_{\mathbf{x},\mathbf{x}'}(\tau)| = 0$. For $\tau \ne \langle w - w' \rangle_N$ and $L \mid C_v - C_{v'} - \tau$, we have $\zeta_L^{un(C_v - C_{v'} - \tau)} = 1$ for any $0 \le n \le N-1$. Hence from (28) we have $|R_{\mathbf{x},\mathbf{x}'}(\tau)| = |\sum_{n=0}^{N-1} \chi(\alpha^n(\alpha^w - \alpha^{w'+\tau}))| = 1$.

For $\tau \ne \langle w - w' \rangle_N$ and $L \nmid C_v - C_{v'} - \tau$. Squaring both sides of (28), we have

$$\begin{aligned} &|R_{\mathbf{x},\mathbf{x}'}(\tau)|^2 \\ &= \sum_{n_2=0}^{N-1} \sum_{n_1=0}^{N-1} \zeta_L^{u(n_1-n_2)(C_v - C_{v'} - \tau)} \cdot \chi((\alpha^{n_1} - \alpha^{n_2})(\alpha^w - \alpha^{w'+\tau})) \\ &= \sum_{n_2=0}^{N-1} \sum_{j=-n_2}^{N-n_2-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \cdot \chi((\alpha^{n_2+j} - \alpha^{n_2})(\alpha^w - \alpha^{w'+\tau})) \\ &= \sum_{n_2=0}^{N-1} \sum_{j=0}^{N-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \cdot \chi((\alpha^{n_2+j} - \alpha^{n_2})(\alpha^w - \alpha^{w'+\tau})) \\ &= \sum_{j=0}^{N-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \sum_{n_2=0}^{p^m-2} \chi((\alpha^{n_2+j} - \alpha^{n_2})(\alpha^w - \alpha^{w'+\tau})) \\ &= p^m - 1 + \sum_{j=1}^{N-1} \zeta_L^{uj(C_v - C_{v'} - \tau)} \cdot (-1) \text{ (using Lemma 2)} \\ &= p^m = N + 1. \end{aligned} \tag{29}$$

Therefore, we have $|R_{\mathbf{x},\mathbf{x}'}(\tau)| = \sqrt{N+1}$, and hence (23) is obtained. □

Example 1 Let $p = 3$, $m = 6$, $q = 1$, $N_{CS} = 60$, and then let $N = 3^6 - 1 = 182 \times 4$, i.e. $L = 182$ and $K = 4$. Various periodic correlations between the sequences of $\mathcal{S}_1$ are shown in Fig. 1. It displays the auto-correlation of $\mathbf{z}_{(1,1,1)}$, the cross-correlation between $\mathbf{y}_{(1,0)}$ and $\mathbf{z}_{(1,1,20)}$, and the cross-correlation between $\mathbf{y}_{(1,0)}$ and $\mathbf{y}_{(1,2)}$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

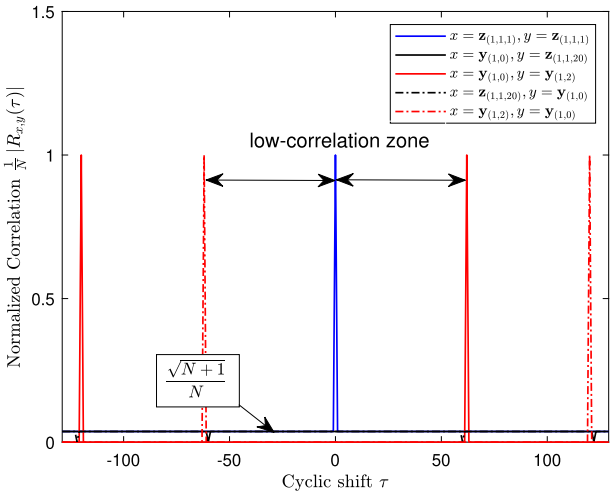


Fig. 1 Correlations between sequences of $\mathcal{S}_1$, $N = 728$

Corollary 1 *The sequence family* $\mathcal{S}_2 = \left\{\mathbf{z}_{(u,0,w)}\right\}_{w=0}^{L-1} \subset \mathcal{S}_1$ *is a sequence set with parameters* $(N, L, N, \sqrt{N+1})$*, and it has the following properties:*

$$|R_{\mathbf{z},\mathbf{z}'}(\tau)| = \begin{cases} N, & \text{if } \tau = \langle w - w' \rangle_N \text{ and } L \mid \tau, \\ 0, & \text{if } \tau = \langle w - w' \rangle_N \text{ and } L \nmid \tau, \\ 1, & \text{if } \tau \neq \langle w - w' \rangle_N \text{ and } L \mid \tau, \\ \sqrt{N+1}, & \text{if } \tau \neq \langle w - w' \rangle_N \text{ and } L \nmid \tau, \end{cases} \tag{30}$$

where $\mathbf{z} = \mathbf{z}_{(u,0,w)}$ *and* $\mathbf{z}' = \mathbf{z}_{(u,0,w')}$.

Proof The proof is similar to Theorem 1. Hence omitted. □

3.1 Discussion on optimality

For the sequence family $\mathcal{S}_2$ in Corollary 1, consider K as a constant integer, thus L increases as N increases. Let Θ_{opt} denote the optimal correlation value with respect to the Welch bound. For a fixed K, when $N \to \infty$, we have the optimality ratio, as follows

$$\begin{aligned} \rho^{\mathcal{S}_2} = \lim_{N\to\infty} \frac{\Theta(\mathcal{S}_2;N)}{\Theta_{opt}} &= \lim_{N\to\infty} \frac{\sqrt{N+1}}{\sqrt{\frac{N^2(L-1)}{LN-1}}} \\ &= \lim_{N\to\infty} \sqrt{\frac{N^3+N^2-KN-K}{N^3-KN^2}} \\ &= 1, \end{aligned} \tag{31}$$

which means that $\mathcal{S}_2$ is asymptotically optimal with respect to the Welch bound. This can also be intuitively verified by Table 2.

Example 2 Take $p = 2$, $m = 9$, $q = 1$, $L = 73$, $K = 7$, and $N = 2^9 - 1 = 73 \times 7$. Various periodic correlations between the sequences of $\mathcal{S}_2$ are shown in Fig. 2. It displays the auto-correlation of $\mathbf{z}_{(1,0,0)}$ and the cross-correlation between $\mathbf{z}_{(1,0,20)}$ and $\mathbf{z}_{(1,0,72)}$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Table 2 For $K = 4$, the comparison between $\Theta(\mathcal{S}_2; N)$ and Θ_{opt}

N	L	$\Theta(\mathcal{S}_2; N)$	Θ_{opt}
$3^2 - 1$	2	3	2.0656
$3^6 - 1$	182	27	26.9073
$3^{10} - 1$	14762	243	242.9897
$3^{12} - 1$	132860	729	728.9966

4 ZC Sequences with binary Gold sequence covers (ZC_{bG})

In this section, we use binary Gold sequences to cover ZC sequences and propose a family of sequences with LCZ. We hereby define $N = 2^m - 1$ until the end of this section to avoid definition confusion, where m is an odd number.

Cyclically-shifted ZC sequences $\mathbf{x}_{(u,v)}$ of period N are defined as

$$x_{(u,v)}(n) = x_u(\langle n + C_v\rangle_N) = \zeta_N^{\frac{u\langle n+C_v\rangle_N(\langle n+C_v\rangle_N+\langle N\rangle_2)}{2}+q\langle n+C_v\rangle_N}, \quad 0 \le n \le N-1, \quad (32)$$

where $C_v = vN_{CS}$ with $0 < N_{CS} \le N$ and $0 \le v \le \left\lfloor \frac{N}{N_{CS}} \right\rfloor - 1$.

Then the ZC_{bG} sequences $\mathbf{d}_{(u,v,i,w)} = (d_{(u,v,i,w)}(0), d_{(u,v,i,w)}(1), \cdots, d_{(u,v,i,w)}(N-1))$ are constructed by element-by-element multiplication of sequences $\mathbf{x}_{(u,v)}$ with covers as

$$d_{(u,v,i,w)}(n) = x_{(u,v)}(n) \cdot a_{(i,w)}(n), \quad 0 \le n \le N-1, \quad (33)$$

where the cover sequences $\mathbf{a}_{(i,w)} = (a_{(i,w)}(0), a_{(i,w)}(1), \cdots, a_{(i,w)}(N-1))$ with $0 \le i \le 2^m$ and $0 \le w \le N-1$ are cyclic-shifts of the cover in (12)

$$a_{(i,w)}(n) = a_i(\langle n + w\rangle_N), \quad 0 \le n \le N-1. \quad (34)$$

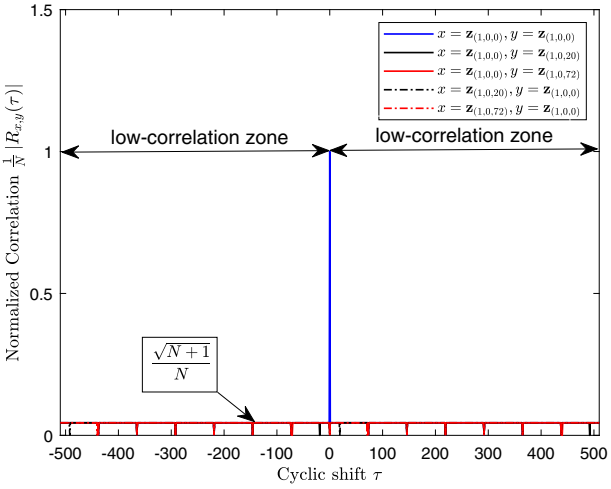


Fig. 2 Correlations between sequences of $\mathcal{S}_2$, $N = 511$

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

From this definition, we generate the following set

$$\mathcal{D} = \bigcup_{i=0}^{2^m} \mathcal{D}_i, \tag{35}$$

where the last subset with $i = 2^m$, which contains cyclically-shifted ZC sequences and ZC sequences with m-sequence covers, is defined as

$$\mathcal{D}_{2^m} = \{\mathbf{x}_{(u,v)}\}_{v=0}^{\lfloor \frac{N}{N_{CS}} \rfloor - 1} \bigcup_{w=0}^{N-1} \{\mathbf{d}_{(u,v,2^m,w)}\}_{v=0}^{\lfloor \frac{N}{N_{CS}} \rfloor - 1}, \tag{36}$$

and for $0 \leq i < 2^m$, subsets are defined as

$$\mathcal{D}_i = \bigcup_{w=0}^{N-1} \{\mathbf{d}_{(u,v,i,w)}\}_{v=0}^{\lfloor \frac{N}{N_{CS}} \rfloor - 1}, \tag{37}$$

where u is a constant with $gcd(u, N) = 1$ for all i.

In the above construction, we use the parameter i of the Gold sequences as the index of sequence subsets, and generate $N + 2$ sequence subsets. In the sequence subset with index $i = 2^m$, not only ZC_{bG} sequences, but also cyclically-shifted ZC sequences are included. Then for sequence subsets with index $0 \leq i \leq 2^m - 1$, the size of their sequence sets is $N\lfloor \frac{N}{N_{CS}} \rfloor$, and for the sequence subset with index 2^m, the size of sequence set is $(N + 1)\lfloor \frac{N}{N_{CS}} \rfloor$. We refer to the PRACH capacity as the total number of sequences available for ZC_{bG} sequences, so we can get

$$\mathrm{PRACHcapacity}^{(\mathrm{ZC}_{bG})} = (N^2 + 2N + 1)\lfloor \frac{N}{N_{CS}} \rfloor. \tag{38}$$

At the same time, the collection of $N + 2$ subsets has the following properties:

Theorem 2 *Let m be an odd number and $N = 2^m - 1$. Let N_{CS} be an integer with $0 < N_{CS} \leq N$, for each subset $\mathcal{D}_i$ in (36) and (37) we have*

$$\Theta(\mathcal{D}_i; N_{CS}) \leq 3\sqrt{N+1}, \tag{39}$$

and for any two subsets $\mathcal{D}_i$ and $\mathcal{D}_j$, $i \neq j$, we have

$$\Omega\left(\mathcal{D}_i, \mathcal{D}_j\right) \leq 3\sqrt{N+1}. \tag{40}$$

Proof Let us consider the correlation between $\mathcal{D}_{i_1}$ and $\mathcal{D}_{i_2}$. For $0 \leq i_1, i_2 \leq 2^m - 2$, we have

$$\begin{aligned}
&|R_{\mathbf{d}_{(u,v_1,i_1,w_1)},\mathbf{d}_{(u,v_2,i_2,w_2)}}(\tau)| \\
&= \left| \sum_{n=0}^{N-1} \zeta_N^{un(C_{v_1} - C_{v_2} - \tau)} \cdot \chi\left(\alpha^{i_1+n+w_1} + \alpha^{3(n+w_1)} - \alpha^{i_2+n+w_2+\tau} - \alpha^{3(n+w_2+\tau)}\right) \right| \\
&= \left| \sum_{n=0}^{N-1} \zeta_N^{un(C_{v_1} - C_{v_2} - \tau)} \cdot \chi\left(\alpha^n(\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau}) + \alpha^{3n}(\alpha^{3w_1} - \alpha^{3(w_2+\tau)})\right) \right|. \qquad (41)
\end{aligned}$$

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

When $\langle C_{v_1} - C_{v_2} - \tau\rangle_N = 0$ and $\langle w_1 - w_2 - \tau\rangle_N = 0$, we have $\alpha^{3w_1} - \alpha^{3(w_2+\tau)} = 0$ and $\zeta_N^{un(C_{v_1}-C_{v_2}-\tau)} = 1$. Using Lemma 2, the left side of (41) is equal to

$$\begin{aligned} |R_{\mathbf{d}_{(u,v_1,i_1,w_1)},\mathbf{d}_{(u,v_2,i_2,w_2)}}(\tau)| &= \Big| \sum_{n=0}^{N-1} \chi\left(\alpha^n(\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})\right) \Big| \\ &= \begin{cases} N, & \text{if} \quad i_1 = i_2, \\ 1, & \text{if} \quad i_1 \neq i_2. \end{cases} \end{aligned} \tag{42}$$

When $\langle C_{v_1} - C_{v_2} - \tau\rangle_N = 0$ and $\langle w_1 - w_2 - \tau\rangle_N \neq 0$, we know that $\zeta_N^{un(C_{v_1}-C_{v_2}-\tau)} = 1$ and $\alpha^{w_1} \neq \alpha^{w_2+\tau}$. Since $(3, 2^m - 1) = 1$, we can also get $\alpha^{3w_1} \neq \alpha^{3(w_2+\tau)}$. So (41) can be written as

$$\begin{aligned} &|R_{\mathbf{d}_{(u,v_1,i_1,w_1)},\mathbf{d}_{(u,v_2,i_2,w_2)}}(\tau)| \\ &= \Big| \sum_{n=0}^{N-1} \chi\left(\alpha^n(\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau}) + \alpha^{3n}(\alpha^{3w_1} - \alpha^{3(w_2+\tau)})\right) \Big| \\ &= \Big| \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left((\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})x + (\alpha^{3w_1} - \alpha^{3(w_2+\tau)})x^3\right) \Big| \\ &= \Big| -1 + \sum_{x\in\mathbb{F}_{2^m}} \chi\left((\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})x + (\alpha^{3w_1} - \alpha^{3(w_2+\tau)})x^3\right) \Big| \\ &\leq 2\sqrt{2^m} + 1 \text{ (using Fact 1)} \\ &= 2\sqrt{N+1} + 1. \end{aligned} \tag{43}$$

When $\langle C_{v_1} - C_{v_2} - \tau\rangle_N \neq 0$ and $\langle w_1 - w_2 - \tau\rangle_N = 0$, then $\alpha^{3w_1} - \alpha^{3(w_2+\tau)} = 0$. Let $s = (\langle u(C_{v_1} - C_{v_2} - \tau)\rangle_N, N)$, $M = N/s$, $r = \langle u(C_{v_1} - C_{v_2} - \tau)\rangle_N/s$. Then (41) can be written as

$$\begin{aligned} |R_{\mathbf{d}_{(u,v_1,i_1,w_1)},\mathbf{d}_{(u,v_2,i_2,w_2)}}(\tau)| &= \Big| \sum_{n=0}^{N-1} \zeta_M^{rn} \cdot \chi\left(\alpha^n(\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})\right) \Big| \\ &= \Big| \sum_{x\in\mathbb{F}_{2^m}} \psi(x) \cdot \chi\left((\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})x\right) \Big| \\ &\begin{cases} = \left| s\sum_{n=0}^{M-1} \zeta_M^{rn} \right| = 0, & \text{if} \quad i_1 = i_2, \\ \leq \sqrt{2^m} = \sqrt{N+1}, & \text{if} \quad i_1 \neq i_2 \text{ (using Fact 2)}, \end{cases} \end{aligned} \tag{44}$$

where the inequality comes from the fact that $g(x) = x$ with one root in $\overline{\mathbb{F}}_{2^m}$ and $M \neq 1$, at the same time, $f(x) = (\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})x$ with degree $d = 1$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

When $\langle C_{v_1} - C_{v_2} - \tau\rangle_N \neq 0$ and $\langle w_1 - w_2 - \tau\rangle_N \neq 0$, then (41) can be written as

$$\begin{aligned}
&|R_{\mathbf{d}_{(u,v_1,i_1,w_1)},\mathbf{d}_{(u,v_2,i_2,w_2)}}(\tau)| \\
&= \Big|\sum_{n=0}^{N-1} \zeta_M^{rn} \cdot \chi\left((\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})\alpha^n + (\alpha^{3w_1} - \alpha^{3(w_2+\tau)})\alpha^{3n}\right)\Big| \\
&= \Big|\sum_{x\in\mathbb{F}_{2^m}} \psi(x)\chi\left((\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})x + (\alpha^{3w_1} - \alpha^{3(w_2+\tau)})x^3\right)\Big| \\
&\leq 3\sqrt{2^m} \text{ (using Fact 2)} \\
&= 3\sqrt{N+1}, \qquad (45)
\end{aligned}$$

where the inequality comes from the fact that $g(x) = x$ with one root in $\overline{\mathbb{F}}_{2^m}$ and $M \neq 1$, at the same time, $f(x) = (\alpha^{i_1+w_1} - \alpha^{i_2+w_2+\tau})x + (\alpha^{3w_1} - \alpha^{3(w_2+\tau)})x^3$ with degree $d = 3$.

Therefore, we get that $\Theta(\mathcal{D}_i; N_{CS}) \leq 3\sqrt{N+1}$ holds for $0 \leq i \leq 2^m - 2$ from (44) and (45). At the same time, we can also get that $\Omega\left(\mathcal{D}_i, \mathcal{D}_j\right) \leq 3\sqrt{N+1}$ holds for $0 \leq i \neq j \leq 2^m - 2$ from above four cases. Similarly, we can also get that $\Theta(\mathcal{D}_i; N_{CS}) \leq 3\sqrt{N+1}$ and $\Omega\left(\mathcal{D}_i, \mathcal{D}_j\right) \leq 3\sqrt{N+1}$ hold for $0 \leq i \neq j \leq 2^m$. □

For each subset, we have a LCZ with the correlation magnitude below $3\sqrt{N+1}$. This LCZ is illustrated in Fig. 3(a) where $N = 127$ and $N_{CS} = 20$. It shows the auto-correlation of the ZC_{bG} sequence $\mathbf{d}_{(1,0,8,0)}$ and its cross correlation with three other ZC_{bG} sequences. The periodic correlation between sequences from different subsets is illustrated in Fig. 3(b), where we can see that the inter-set correlation is between $2\sqrt{N+1}$ and $3\sqrt{N+1}$.

5 ZC Sequences with *p*-phase sequence covers (ZC_p)

In this section, we use the sequences in (13) to cover ZC sequences and propose a family of sequences with LCZ . We hereby define $N = p^m - 1$ until the end of this section to avoid definition confusion, where p is an odd prime number and m is a positive integer. Note that d is an integer with $1 < d < p$ in this section.

ZC_p sequences $\mathbf{g}_{(u,v,\Delta,w)}$ of period N are constructed by element-by-element multiplication of sequences $\mathbf{x}_{(u,v)}$ in (32) of period N with covers as

$$g_{(u,v,\Delta,w)}(n) = x_{(u,v)}(n) \cdot b_{(\Delta,w)}(n), \quad 0 \leq n \leq N-1, \qquad (46)$$

where the cover sequences $\mathbf{b}_{(\Delta,w)} = (b_{(\Delta,w)}(0), b_{(\Delta,w)}(1), \cdots, b_{(\Delta,w)}(N-1))$ with $0 \leq w \leq N-1$ are cyclic-shifts of the cover in (13)

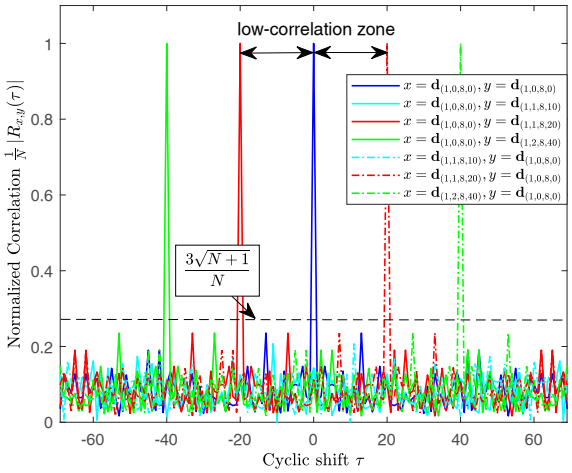
$$b_{(\Delta,w)}(n) = b_\Delta(\langle n + w\rangle_N), \quad 0 \leq n \leq N-1. \qquad (47)$$

Note that when $\Delta = (0, 0, \cdots, 0) \in \mathbb{F}_{p^m}^{d-1}$, ZC_p sequences are actually the ZC_m sequence subset with root u in [8, 9].

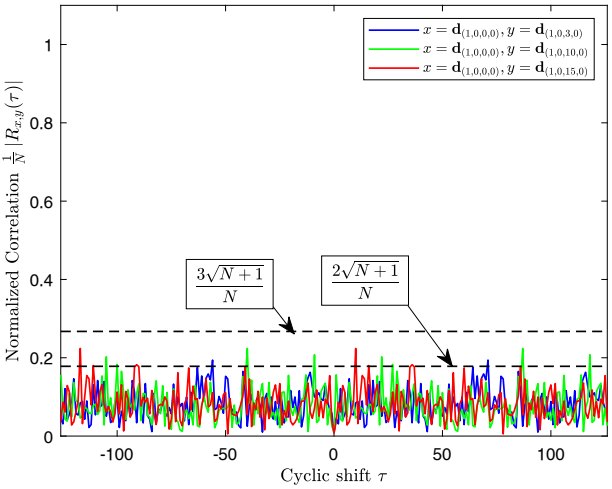
From this definition, we generate the following set

$$\mathcal{G} = \bigcup_{\Delta\in\mathbb{F}_{p^m}^{d-1}} \mathcal{G}_\Delta, \qquad (48)$$

Content courtesy of Springer Nature, terms of use apply. Rights reserved.



(a) Intra-subset correlation $N = 127$



(b) Inter-subset correlation $N = 127$

Fig. 3 Illustration of the LCZ of ZC_{bG} sequences

where the first subset with $\Delta = (0, 0, \cdots, 0) \in \mathbb{F}_{p^m}^{d-1}$, which contains cyclically-shifted ZC sequences with root u and ZC sequences with p-ary m-sequence covers, is defined as

$$\mathcal{G}_{\mathbf{0}} = \{\mathbf{x}_{(u,v)}\}_{v=0}^{\lfloor \frac{N}{N_{CS}} \rfloor - 1} \bigcup_{w=0}^{N-1} \{\mathbf{g}_{(u,v,\mathbf{0},w)}(n)\}_{v=0}^{\lfloor \frac{N}{N_{CS}} \rfloor - 1}, \tag{49}$$

where $\mathbf{0} = (0, 0, \cdots, 0) \in \mathbb{F}_{p^m}^{d-1}$ and for $\Delta \in \mathbb{F}_{p^m}^{d-1}$ and $\Delta \neq \mathbf{0}$, subsets are defined as

$$\mathcal{G}_{\Delta} = \bigcup_{w=0}^{N-1} \{\mathbf{g}_{(u,v,\Delta,w)}(n)\}_{v=0}^{\lfloor \frac{N}{N_{CS}} \rfloor - 1}, \tag{50}$$

where u is a constant with $gcd(u, N) = 1$ for all Δ.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

From the above construction, we can see that the size of the sequence subset with index $\Delta = \mathbf{0}$ is $(N+1)\lfloor\frac{N}{N_{CS}}\rfloor$, while the size of other sequence subsets for all index $\Delta \in \mathbb{F}_{p^m}^{d-1}$ and $\Delta \neq \mathbf{0}$ is $N\lfloor\frac{N}{N_{CS}}\rfloor$. Therefore, we have

$$\text{PRACHcapacity}^{(\text{ZC}_p)} = \left(N(N+1)^{d-1}+1\right)\lfloor\frac{N}{N_{CS}}\rfloor. \tag{51}$$

At the same time, the collection of $(N+1)^{d-1}$ subsets has the following properties:

Theorem 3 *Let p be an odd prime number, N, m and N_{CS} be three positive integers with $N = p^m - 1$ and $0 < N_{CS} \leq N$. For each subset $\mathcal{G}_\Delta$ in (49) and (50) we have*

$$\Theta(\mathcal{G}_\Delta; N_{CS}) \leq d\sqrt{N+1}, \tag{52}$$

and for any two subsets $\mathcal{G}_{\Delta_1}$ and $\mathcal{G}_{\Delta_2}$, $\Delta_1 \neq \Delta_2 \in \mathbb{F}_{p^m}^{d-1}$, we have

$$\Omega\left(\mathcal{G}_{\Delta_1}, \mathcal{G}_{\Delta_2}\right) \leq d\sqrt{N+1}, \tag{53}$$

where d is an integer with $1 < d < p$.

Proof Let us consider the correlation between $\mathcal{G}_{\Delta_1}$ and $\mathcal{G}_{\Delta_2}$, for $\Delta_1 = (\delta_{(1,1)}, \delta_{(2,1)}, \cdots, \delta_{(d-1,1)})$, $\Delta_2 = (\delta_{(1,2)}, \delta_{(2,2)}, \cdots, \delta_{(d-1,2)}) \in \mathbb{F}_{p^m}^{d-1}$, we have

$$\begin{aligned} &|R_{\mathbf{g}_{(u,v_1,\Delta_1,w_1)},\mathbf{g}_{(u,v_2,\Delta_2,w_2)}}(\tau)| \\ &= \left|\sum_{n=0}^{N-1} \zeta_N^{un(C_{v_1}-C_{v_2}-\tau)} \cdot \chi\left(f(\alpha^n)\right)\right|, \end{aligned} \tag{54}$$

where $f(x) = (\alpha^{w_1} - \alpha^{w_2+\tau})x + (\delta_{(1,1)}\alpha^{2w_1} - \delta_{(1,2)}\alpha^{2w_2+2\tau})x^2 + \cdots + (\delta_{(d-1,1)}\,\alpha^{dw_1} - \delta_{(d-1,2)}\alpha^{d(w_2+\tau)})x^d$.

When $\langle C_{v_1} - C_{v_2} - \tau\rangle_N = 0$ and $\langle w_1 - w_2 - \tau\rangle_N = 0$, we know that $\zeta_N^{un(C_{v_1}-C_{v_2}-\tau)} = 1$ and $\alpha^{w_1} = \alpha^{w_2+\tau}$, (54) can be written as

$$\begin{aligned} &|R_{\mathbf{g}_{(u,v_1,\Delta_1,w_1)},\mathbf{g}_{(u,v_2,\Delta_2,w_2)}}(\tau)| \\ &= \left|\sum_{n=0}^{N-1} \chi\left(f(\alpha^n)\right)\right| \\ &= \left|-1 + \sum_{x\in\mathbb{F}_{p^m}} \chi\left(f(x)\right)\right| \\ &\begin{cases} = p^m - 1 = N, & \text{if} \quad \Delta_1 = \Delta_2, \\ \leq 1 + (d-1)\sqrt{p^m} = 1 + (d-1)\sqrt{N+1}, & \text{if} \quad \Delta_1 \neq \Delta_2 \text{ (using Fact 1)}, \end{cases} \end{aligned} \tag{55}$$

where the second case comes from the fact that $f(x) = (\delta_{(1,1)}\alpha^{2w_1} - \delta_{(1,2)}\alpha^{2w_2+2\tau})x^2 + \cdots + (\delta_{(d-1,1)}\alpha^{dw_1} - \delta_{(d-1,2)}\alpha^{d(w_2+\tau)})x^d$ with degree d_1, and $(d_1, p^m) = 1$ for all $2 \leq d_1 \leq d < p$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

When $\langle C_{v_1} - C_{v_2} - \tau \rangle_N = 0$ and $\langle w_1 - w_2 - \tau \rangle_N \neq 0$, we know that $\zeta_N^{un(C_{v_1} - C_{v_2} - \tau)} = 1$ and $\alpha^{w_1} \neq \alpha^{w_2+\tau}$, then the left side of (54) is equal to

$$\begin{aligned} & |R_{\mathbf{g}_{(u,v_1,\Delta_1,w_1)},\mathbf{g}_{(u,v_2,\Delta_2,w_2)}}(\tau)| \\ = & \left| \sum_{n=0}^{N-1} \chi\left(f(\alpha^n)\right) \right| \\ \leq & 1 + (d-1)\sqrt{p^m} \text{ (using Fact 1)} \\ = & 1 + (d-1)\sqrt{N+1}, \end{aligned} \tag{56}$$

where the inequality comes from the fact that $f(x) = (\alpha^{w_1} - \alpha^{w_2+\tau})x + (\delta_{(1,1)}\alpha^{2w_1} - \delta_{(1,2)}\alpha^{2w_2+2\tau})x^2 + \cdots + (\delta_{(d-1,1)}\alpha^{dw_1} - \delta_{(d-1,2)}\alpha^{d(w_2+\tau)})x^d$ with degree d_2, and $(d_2, p^m) = 1$ for all $1 \leq d_2 \leq d < p$.

When $\langle C_{v_1} - C_{v_2} - \tau \rangle_N \neq 0$ and $\langle w_1 - w_2 - \tau \rangle_N = 0$, we know that $\zeta_N^{un(C_{v_1} - C_{v_2} - \tau)} \neq 1$ and $\alpha^{w_1} = \alpha^{w_2+\tau}$. Let $s = (\langle u(C_{v_1} - C_{v_2} - \tau) \rangle_N, N)$, $M = N/s$, $r = \langle u(C_{v_1} - C_{v_2} - \tau) \rangle_N / s$. Then the left side of (54) is equal to

$$\begin{aligned} & |R_{\mathbf{g}_{(u,v_1,\Delta_1,w_1)},\mathbf{g}_{(u,v_2,\Delta_2,w_2)}}(\tau)| \\ = & \left| \sum_{n=0}^{N-1} \zeta_M^{rn} \cdot \chi\left(f(\alpha^n)\right) \right| \\ = & \left| \sum_{x \in \mathbb{F}_{p^m}} \psi(x)\chi\left(f(x)\right) \right| \\ & \begin{cases} = \left| s \sum_{n=0}^{M-1} \zeta_M^{rn} \right| = 0, & \text{if} \quad \Delta_1 = \Delta_2, \\ \leq d\sqrt{p^m} = d\sqrt{N+1}, & \text{if} \quad \Delta_1 \neq \Delta_2 \text{ (using Fact 2)}, \end{cases} \end{aligned} \tag{57}$$

where the inequality comes from the fact that $g(x) = x$ with one root in $\overline{\mathbb{F}}_{p^m}$ and $M \neq 1$, at the same time, $f(x) = (\delta_{(1,1)}\alpha^{2w_1} - \delta_{(1,2)}\alpha^{2w_2+2\tau})x^2 + \cdots + (\delta_{(d-1,1)}\alpha^{dw_1} - \delta_{(d-1,2)}\alpha^{d(w_2+\tau)})x^d$ with degree $d_3 \in [2, d]$.

When $\langle C_{v_1} - C_{v_2} - \tau \rangle_N \neq 0$ and $\langle w_1 - w_2 - \tau \rangle_N \neq 0$. The left side of (54) is equal to

$$\begin{aligned} & |R_{\mathbf{g}_{(u,v_1,\Delta_1,w_1)},\mathbf{g}_{(u,v_2,\Delta_2,w_2)}}(\tau)| \\ = & \left| \sum_{n=0}^{N-1} \zeta_M^{rn} \cdot \chi\left(f(\alpha^n)\right) \right| \\ = & \left| \sum_{x \in \mathbb{F}_{p^m}} \psi(x)\chi\left(f(x)\right) \right| \\ \leq & d\sqrt{p^m} \text{ (using Fact 2)} \\ = & d\sqrt{N+1}, \end{aligned} \tag{58}$$

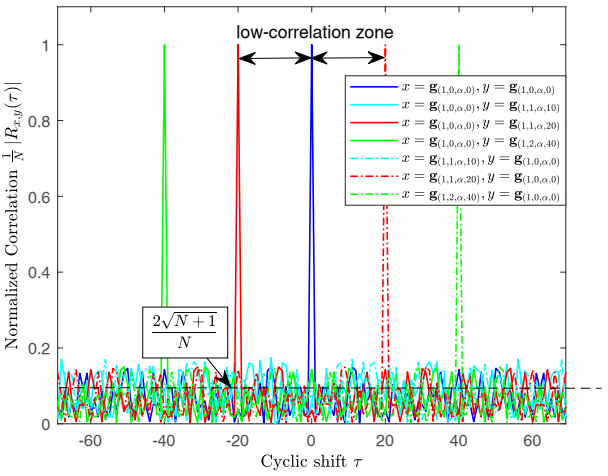
where the inequality comes from the fact that $g(x) = x$ with one root in $\overline{\mathbb{F}}_{p^m}$ and $M \neq 1$, at the same time, $f(x) = (\alpha^{w_1} - \alpha^{w_2+\tau})x + (\delta_{(1,1)}\alpha^{2w_1} - \delta_{(1,2)}\alpha^{2w_2+2\tau})x^2 + \cdots + (\delta_{(d-1,1)}\alpha^{dw_1} - \delta_{(d-1,2)}\alpha^{d(w_2+\tau)})x^d$ with degree $d_4 \in [1, d]$.

Proofs for other cases can be obtained similarly.

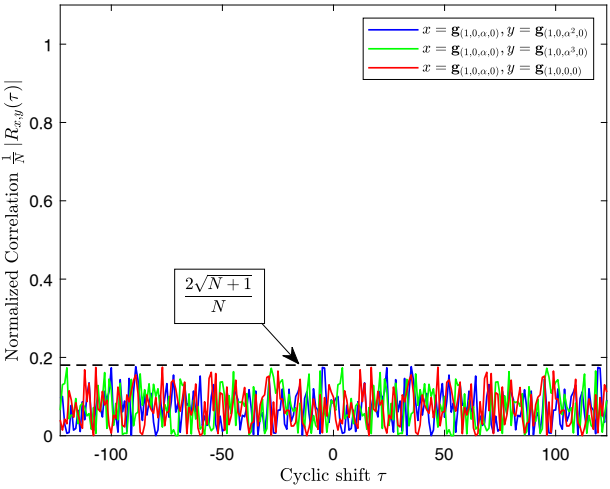
We can see from (57) and (58) that when $\Delta_1 = \Delta_2$, the maximum correlation amplitude of $\mathcal{G}_{\Delta_1}$ in the zone of length N_{CS} is less than or equal to $d\sqrt{N+1}$, so $\Theta(\mathcal{G}_\Delta; N_{CS}) \leq d\sqrt{N+1}$ holds. At the same time, it can be seen from above four cases that the maximum cross-correlation amplitude of $\mathcal{G}_{\Delta_1}$ and $\mathcal{G}_{\Delta_2}$ is also less than or equal to $d\sqrt{N+1}$, so $\Omega\left(\mathcal{G}_{\Delta_1}, \mathcal{G}_{\Delta_2}\right) \leq d\sqrt{N+1}$ is established. □

When we set $d = 2$, we can obtain $N+1$ sequence subsets with LCZ through the above construction. This LCZ is illustrated in Fig. 4(a) where $N = 5^3 - 1 = 124$ and $N_{CS} = 20$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.



(a) Intra-subset correlation $N = 124$



(b) Inter-subset correlation $N = 124$

Fig. 4 Illustration of the LCZ of ZC_p sequences with $d = 2$

We assume that the primitive element of $\mathbb{F}_{5^3}$ is α, then Fig. 4(a) shows the auto-correlation of the ZC_p sequence $\mathbf{g}_{(1,0,\alpha,0)}$ and its cross-correlation with three other ZC_p sequences. The periodic correlation between sequences from different subsets is illustrated in Fig. 4(b), where we can see that the inter-set correlation is lower than $2\sqrt{N+1}$.

6 Comparison with previous works

In this section, we have compared the new sequences in this paper with the sequences in [8, 9]. The comparison can be summarised as follows:

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

1. Considering ZC sequences and m-sequence covers in Theorem 1 have the same period, i.e. $L = N$, then the sequence family $\mathcal{S}_1$ is the ZC_m sequence subset with root u in [8, 9]. Therefore, the proposed sequence family $\mathcal{S}_1$, in Theorem 1, can be regarded as an extension of ZC_m sequence subset.
2. The sizes of sequence families in Theorem 1 and Corollary 1 can be changed with respect to L, so the proposed construction provides a flexible tradeoff between the family size and alphabet size, when the period of sequences is fixed.
3. The two ZC sequence supersets, i.e., $\mathcal{D}_{2^m}$ which is constructed using ZC sequences with binary Gold sequence covers, and $\mathcal{G}_{\mathbf{0}}$, which is constructed using ZC sequences with p-phase sequence covers, both contain the ZC_m sequence subset proposed in [8, 9].
4. For the ZC_p sequence set with $d = 2$, its inter-set correlation is $2\sqrt{N+1} \approx 2\sqrt{N}$, which is approximate to the ZC_a sequence set in [9], and our PRACH capacity is $(N^2 + N + 1)\lfloor \frac{N}{N_{CS}} \rfloor$ larger than the ZC_a set. Hence, the proposed superset is more advantageous in overcoming inter-cell interference in small cells.
5. Table 1 provides a comparison on superset optimality factors and PRACH capacities of ZC sequence supersets, proposed till date. For proposed constructions, we see that the correlation of ZC_p sets $\mathcal{G}$ is close to optimal when the parameter value $d = 2$. Also note that, the PRACH capacity of ZC_p set is much larger than $(N+1)^{d-1}$ times of the ZC sequence set as N increases.

7 Concluding and remarks

In this paper, we constructed four supersets of ZC sequences. Along with the ZC sequences, we have used m sequences, binary Gold sequences and p-phase sequences as covers. We have exploited the properties of exponential sums to find the correlation properties of the proposed supersets of ZC sequences. The parameters of the proposed supersets are more flexible and the PRACH capacities are also higher as compared to the existing ZC supersets.

Acknowledgments The authors are very grateful to the editor and the anonymous reviewers for their valuable comments and suggestions that improved the quality of this paper. This work was supported in part by the National Natural Science Foundation of China Under Grants 62131016, 12001450, and 62071397, in part Natural Science Foundation of Sichuan Under Grants 2023NSFSC1912 and 2022NSFSC0906, and also supported by projects of central government to guide local scientific and technological development under Grant 2022ZYD0004.

References

1. PRACH preamble sequences for NR, document R1-1705055, Huawei, HiSilicon, 3GPP TSG RAN WG1, Meeting 88bis, Spokane, USA, 2017. Available from: http://www.3gpp.org
2. PRACH preamble sequences and formats, document R1-1708164, Huawei, HiSilicon, 3GPP TSG RAN WG1, Meeting 89, Hangzhou, China, 2017. Available from: http://www.3gpp.org
3. NR PRACH design and evaluations, document R1-1706014, Ericsson, 3GPP TSG RAN WG1, Meeting 88bis, Spokane, WA, USA, 2017. Available from: http://www.3gpp.org
4. Schmidt, K.: Sequence families with low correlation derived from multiplicative and additive characters. IEEE Trans. Inf. Theory **57**, 2291–2294 (2011)
5. PRACH design consideration, document R1-1700790, Qualcomm Incorporated, 3GPP TSG RAN WG1, Meeting NR#1, Spokane, USA, 2017. Available from: http://www.3gpp.org
6. Discussion on PRACH preamble for capacity enhancement, document R1-170269, LG Electronics, 3GPP TSG RAN WG1, Meeting NR#2, Qingdao, China, 2017. Available from: http://www.3gpp.org

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

7. RACH preamble sequences and formats for capacity enhancement and beam management, document R1-1712152, Huawei, HiSilicon, 3GPP TSG RAN WG1, Meeting 90, Prague, Czech Republic, 2017. Available from: http://www.3gpp.org
8. Pitaval, R.A., Popović, B.M., Berggren, F., Wang, P.: Overcoming 5G PRACH capacity shortfall by combining Zadoff-Chu and m-sequences. In: 2018 IEEE International Conference on Communications (ICC) 2018
9. Pitaval, R.A., Popović, B.M., Wang, P., Berggren, F.: Overcoming 5G PRACH capacity shortfall: supersets of Zadoff–Chu sequences with low-correlation zone. IEEE Trans. Commun. **68**, 5673–5688 (2020)
10. Chu, D.: Polyphase codes with good periodic correlation properties. IEEE Trans. Inf. Theory **18**, 531–532 (1972)
11. Weil, A.: On some exponential sums. Proc. Natl. Acad. Sci. USA **34**, 204–207 (1948)
12. Lidl, R., Niederreiter, H.: Finite Fields (Encyclopedia of Mathematics and Its Applications). Cambridge university press (1997)
13. Wan, D.: Generators and irreducible polynomials over finite fields. Math. Comput. **66**, 1195–1212 (1997)
14. Wang, Z., Gong, G., Yu, N.Y.: New polyphase sequence families with low correlation derived from the Weil bound of exponential sums. IEEE Trans. Inf. Theory **59**, 3990–3998 (2013)
15. Alltop, W.: Complex sequences with low periodic correlations. IEEE Trans. Inf. Theory **26**, 350–354 (1980)
16. Frank, R., Zadoff, S., Heimiller, R.: Phase shift pulse codes with good periodic correlation properties. IRE Trans. Inform. Theory **8**, 381–382 (1962)
17. Schmidt, K.U.: Sequence families with low correlation derived from multiplicative and additive characters. IEEE Trans. Inf. Theory **57**, 2291–2294 (2011)
18. Sidelnikov, V.M.: Some k-valued pseudo-random sequences and nearly equidistant codes. Probl. Inf. Transm. **5**, 12–16 (1969)
19. Gurevich, S., Hadani, R., Sochen, N.: The finite harmonic oscillator and its applications to sequences, communication and radar. IEEE Trans. Inf. Theory **54**, 4239–4253 (2008)
20. Welch, L.: Lower bounds on the maximum cross correlation of signals (Corresp). IEEE Trans. Inf. Theory **20**, 397–399 (1974)
21. Golomb, S.W., Gong, G.: Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar. Cambridge University Press (2005)
22. Gold, R.: Optimal binary sequences for spread spectrum multiplexing (Corresp). IEEE Trans. Inf. Theory **13**, 619–621 (1967)

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com