素数幂长度最优对称 Z 补码集的直接构造

Praveen Kumar *、Sudhan Majhi†、Subhabrata Paul*
*印度理工学院巴特那分校数学系，印度 {praveen_2021ma03, subhabrata}@iitp.ac.in
†印度理工学院班加罗尔分校电气通信工程系，印度，smajhi@iisc.ac.in

arXiv:2305.01442v1 [cs.IT] 2 May 2023

摘要—本文利用多变量函数（MVF），提出了一种素数幂长度最优对称 Z 补码集（SZCCS）的直接构造方法。SZCCS 是 Z 补码集（ZCCS）的自然扩展；后者仅具有前端零相关区（ZCZ）宽度，而 SZCCS 同时具有前端和尾端 ZCZ 宽度。由于在首尾两端均具有 ZCZ 宽度，SZCCS 可用于为频率选择性信道上的宽带广义空间调制系统设计最优训练序列。本文首次提出了具有较大集合大小和素数幂长度的最优 SZCCS 构造方法。此外，值得注意的是，已有的若干 ZCCS 和 SZCCS 研究均可视为所提构造的特例。

一、引言

Z 补码对（ZCP）的概念由 Fan 等人提出 [1]。ZCP 中两条序列的非周期自相关函数（AACF）之和在特定区域内为零，该区域称为零相关区（ZCZ）。当该 ZCZ 宽度 Z 等于序列长度 N时，ZCP 就成为 Golay 互补对（GCP）。与 GCP 不同，ZCP 可具有任意长度以及不同的 ZCZ 宽度 [2]–[6]。

[1] 中提出的 ZCP 概念由 Feng 等人在 [7]中推广为零相关区互补集（ZCCS）。ZCCS 仅考虑非周期自相关函数（AACF）和非周期互相关函数（ACCF）的前端 ZCZ。文献中已有若干基于广义布尔函数（GBF）的非二次幂长度 ZCCS 构造方法 [8]–[13]。具有 K 个码、每个码包含 M条长度为 N 且 ZCZ 宽度为 Z 的序列的 ZCCS，记为（K，M，N，Z）-ZCCS。在特殊情况下，$K = M$和 $N = Z$，它被称为完全互补码（CCC），记为（K，K，N）-CCC。最近，Li 等人利用多变量函数（MVF）提出了素数幂长度、具有码间 ZCZ 宽度的多个 CCC 的直接构造方法 [14]。将这些多个 CCC 合并后，可得到最优的（p^{n+v}，p^n，p^m，p^{m-v}）-ZCCS [14]。

近年来，零相关区互补集（ZCCS）的概念已扩展为对称零相关区互补集（SZCCS），其在前端和尾端均具有零相关区（ZCZ）特性 [15]。[15] 中的作者提出了一种基于广义布尔函数（GBF）的 (8, 2, $2^m, 2^{m-2} - 1$)- SZCCS 构造。在实际应用中，前端零相关区和尾端零相关区分别在抑制小时延和大时延干扰方面发挥着特定作用。集合大小较大的 SZCCS 可用于设计宽带广义空间调制（GSM）系统在频率选择性信道上的训练序列[15]。鉴于 SZCCS 在 GSM 系统中的广泛应用，以及目前缺乏在集合大小、簇大小和长度方面参数灵活的构造方法，作者因此在本文提出了一种素数幂长度 SZCCS 的直接构造。

所提出的基于MVF的SZCCS构造的集合大小为 $p^{k+\delta}$，远大于簇大小 p^k，其中 $m \geq 3$, $0 \leq \delta < m$, $1 \leq k \leq m-\delta$. 此外，所提出的SZCCS具有较大的零相关区宽度 $p^{m-\delta} - 1$，并满足最优性条件。许多现有的零相关区互补集和SZCCS构造都可视为所提构造的特例。

本文其余部分的结构安排如下：第二节介绍预备知识，第三节给出基于MVF的SZCCS构造。第四节对所提构造与现有工作进行全面比较，并提供详细分析。随后，第五节对全文进行总结。

II. 预备知识

本节将阐述所提构造所需的基本概念、符号以及已有研究成果。

定义1：设u $=(u_0, u_1, \ldots, u_{N-1})$和v $=(v_0, v_1, \ldots, v_{N-1})$为两个长度为 N、取值于 $\mathbb{Z}_q$的序列。在移位 τ处，非周期互相关函数定义为

$$\mathcal{C}(\mathbf{u}, \mathbf{v})(\tau) = \begin{cases} \sum_{i=0}^{N-1-\tau} \omega_q^{u_i - v_{i+\tau}}, & 0 \leq \tau \leq N-1, \\ \sum_{i=0}^{N-1+\tau} \omega_q^{u_{i-\tau} - v_i}, & -N+1 \leq \tau \leq -1, \\ 0, & |\tau| \geq N, \end{cases} \tag{1}$$

其中，q 是大于 2 的正整数，且 ω_q =exp($2\pi\sqrt{-1}/q$)。对于特殊情形，u =v $\mathcal{C}$(u, v)(τ) 称为 u 的非周期自相关函数，记作 $\mathcal{A}$(u)(τ)。

考虑一个集合 C $= \{C^0, C^1, \ldots, C^{K-1}\}$，其中每个集合 C^e 由 M个序列组成，即 $C^e = \{\mathrm{c}_0^e, \mathrm{c}_1^e, \ldots\ldots, \mathrm{c}_{M-1}^e\}$，且每个序列 c_l^e的长度为 N，其中 $0 \leq e \leq K-1$ 且$0 \leq l \leq M-1$。

定义 2：上述定义的集合 C 称为零相关区互补集，记作 (K, M, N, Z)-零相关区互补集，若 C^e 和 $C^{e'}$的非周期互相关函数满足

$$\mathcal{C}\left(C^e, C^{e'}\right)(\tau) = \sum_{l=0}^{M-1} \mathcal{C}\left(\mathbf{c}_l^e, \mathbf{c}_l^{e'}\right)(\tau) = \begin{cases} MN, & \tau = 0, e = e', \\ 0, & 0 < |\tau| < Z, e = e', \\ 0, & |\tau| < Z, e \neq e', \end{cases} \tag{2}$$

其中 $0 \le e$、$e' \le K-1$。对于一般的 (K, M, N, Z)-零相关区互补集，$K \le M\lfloor N/Z \rfloor$；而在特殊情形 $K = M\lfloor N/Z \rfloor$ 下，它成为一个最优零相关互补集 [16]。同样，在特殊情形 $K = M$ 和 $Z = N$ 下，该零相关区互补集称为阶数为 K、长度为 N 的互补码集，记为 (K, K, N)-互补码集。

定义 3：上述定义的集合 C 称为 SZCSS，记为 (K, M, N, Z)-SZCCS；若对于满足 $Z \le N$ 的 $\mathcal{T}_1 = \{1, 2, \cdots, Z\}$ 和 $\mathcal{T}_2 = \{N - Z, N - Z + 1, \cdots, N - 1\}$，它满足以下性质：

$$\begin{aligned} &P1: \sum_{i=0}^{M-1} \mathcal{A}(\mathbf{c}_i^e)(\tau) = 0, \quad \text{for all } |\tau| \in (\mathcal{T}_1 \cup \mathcal{T}_2) \cap \mathcal{T}; \\ &P2: \sum_{i=0}^{M-1} \mathcal{C}(\mathbf{c}_i^e, \mathbf{c}_i^{e'})(\tau) = 0, \quad \text{for all } |\tau| \in \{0\} \cup \mathcal{T}_1 \cup \mathcal{T}_2; \end{aligned} \tag{3}$$

其中 $\mathcal{T} = \{1, 2, \ldots, N-1\}$ 和 $e \neq e'$。对于 (K, M, N, Z)-SZCCS，K、M、N 和 Z 分别称为集合大小、簇大小、序列长度和零相关区宽度。

对于一个多变量函数 f：$\{0, 1, \ldots, p-1\}^m \to \mathbb{Z}_q$ 以 m p 元变量 $x_1, x_2, \ldots, x_m$ 表示，对应的 $\mathbb{Z}_q$ 值序列记为 $\mathbf{f}$，计算为 $\mathbf{f} = (f_0, f_1, \ldots, f_{p^m-1})$，其中 $f_r = f(r_1, r_2, \ldots, r_m)$，而 $r = (r_1, r_2, \ldots, r_m)$ 是整数 r 的 p 进制表示，即 $r = \sum_{i=1}^{m} r_i p^{i-1}$。与 $\mathbf{f}$ 相关联的复值序列表示为 $\Psi(f) = \left(\omega_q^{f_0}, \omega_q^{f_1}, \ldots, \omega_q^{f_{p^m-1}}\right)$，其中 ω_q 是单位根 [14] 的第 q 个（$q \ge 2$）单位根。

引理 1 (*[15], [16]*): 任意恒模 (K, M, N, Z)- SZCCS 满足 $K \le M\left\lfloor \frac{N}{Z+1} \right\rfloor$；当 $K = M\left\lfloor \frac{N}{Z+1} \right\rfloor$ 时，称其为最优 (K, M, N, Z)-SZCCS。

III. 所提构造

本节介绍一种基于多变量函数的最优 $(p^{k+\delta}, p^k, p^m, p^{m-\delta}-1)$-SZCCS 构造。

定理1：对于任意正整数 $m \ge 3$ 和 $0 \le \delta < m$，我们将集合 $\{1, 2, \ldots, m-\delta\}$ 划分为 k 个集合，S_1，S_2，…，S_k，其中 $1 \le k \le m - \delta$。设集合 S_β 的基数为 m_β，且 π_β 是从 $\{1, 2, \ldots, m_\beta\}$ 到 S_β的一一映 onto 映射，其中 $\beta = 1, 2, \ldots, k.$。定义多变量函数 g：$\{0, 1, \ldots, p-1\}^m \to \mathbb{Z}_q$ 为

$$g = \frac{q}{p} \sum_{\beta=1}^{k} \sum_{\gamma=1}^{m_\beta - 1} x_{\pi_\beta(\gamma)} x_{\pi_\beta(\gamma+1)} + \sum_{l=1}^{m} \lambda_l x_l + \lambda_0, \tag{4}$$

其中 p是一个素数，且 $p \mid q$，$\lambda_l \in \mathbb{Z}_q$，$0 \le l \le m$。那么集合 $A = \left\{A^0, A^1, \ldots, A^{p^{k+\delta}-1}\right\}$是一个 $(p^{k+\delta}, p^k, p^m, p^{m-\delta}-1)$- SZCCS，其中 $A^t = \{\mathbf{a}_0^t, \mathbf{a}_1^t, ..., \mathbf{a}_{p^k-1}^t\}$，且

$$\mathbf{a}_\sigma^t = \boldsymbol{g} + \frac{q}{p}\left(\sum_{\beta=1}^{k} \sigma_\beta \boldsymbol{x}_{\pi_\beta(1)} + \sum_{\beta=1}^{k} t_\beta \boldsymbol{x}_{\pi_\beta(m_\beta)} + \sum_{\beta=1}^{\delta} t_{k+\beta} \boldsymbol{x}_{m-\delta+\beta}\right), \tag{5}$$

对于 $\sigma = 0$、1、…、$p^k - 1$ 和 $t = 0$、1、…、$p^{k+\delta} - 1$，其 p 元向量表示分别为 $(\sigma_1, \sigma_2, \ldots, \sigma_k)$ 和 $(t_1, t_2, \ldots, t_k, \ldots, t_{k+\delta})$。

证明：我们将证明由定理得到的集合 $A = \left\{A^0\ A^1\ \ldots\ A^{p^{k+\delta}-1}\right\}$ 1 , , , 满足定义 3 中给出的两个条件 $P1$ 和 $P2$，其中 $K = p^{k+\delta}$、$M = p^k$、$N = p^m$ 和 $Z = p^{m-\delta} - 1$，因此构成一个 $(p^{k+\delta}, p^k, p^m, p^{m-\delta} - 1)$-SZCCS。设 $0 \le r$、$s < p^m$ 的 p 元表示分别为 $(r_1, r_2, \ldots, r_m)$ 和 $(s_1, s_2, \ldots, s_m)$。设 $\mathbf{a}_\sigma^t = (a_{\sigma,\ 0}^t,\ a_{\sigma,\ 1}^t,\ \ldots,\ a_{\sigma,\ p^m-1}^t)$。

首先，我们证明定义 3 的性质 $P1$ ，即，对于 $\mathcal{T}_1 = \{1, 2, \ldots, p^{m-\delta} - 1\}$ 和 $\mathcal{T}_2 = \{p^m - p^{m-\delta} - 1, p^m - p^{m-\delta}$、.....、$p^m - 1\}$，每个 A^t 的 AACF 均为零，即：

$$\sum_{\sigma=0}^{p^k-1} \mathcal{A}(\mathbf{a}_\sigma^t)(\tau) = \sum_{r=0}^{p^m-\tau-1} \sum_{\sigma=0}^{p^k-1} \omega_q^{\left(a_{\sigma,r}^t - a_{\sigma,r+\tau}^t\right)} = 0, \tag{6}$$

对于所有 $|\tau| \in (\mathcal{T}_1 \cup \mathcal{T}_2) \cap \mathcal{T}$，其中 $\mathcal{T} = \{1, 2, \ldots, p^m - 1\}$。令 $s = r + \tau$，其中 r为任意整数。下面考虑列出的两种情况。

情况 I：$r_{\pi_\beta(1)} \neq s_{\pi_\beta(1)}$ 对于某个 $\beta \in \{1, 2, \ldots, k\}$成立。于是存在一个 $\mathbf{a}_{\sigma^j}^t = (a_{\sigma^j,\ 0}^t,\ a_{\sigma^j,\ 1}^t$、.....、$a_{\sigma^j,\ p^m-1}^t) =$ 和一个 $\mathbf{a}_\sigma^t + (jq/p)\boldsymbol{x}_{\pi_\beta(1)} \in A^t$，其中 $1 \le j \le p-1$，使得

$$a_{\sigma^j,r}^t - a_{\sigma,r}^t = \frac{jq}{p} r_{\pi_\beta(1)}, \tag{7}$$

and

$$a_{\sigma^j,s}^t - a_{\sigma,s}^t = \frac{jq}{p} s_{\pi_\beta(1)}. \tag{8}$$

因此，由上述两个方程可得

$$\left(a_{\sigma^j,r}^t - a_{\sigma^j,s}^t\right) - \left(a_{\sigma,r}^t - a_{\sigma,s}^t\right) = \frac{jq}{p}\left(r_{\pi_\beta(1)} - s_{\pi_\beta(1)}\right). \tag{9}$$

将两边提升至 q次单位根的幂，然后对 $1 \le j \le p-1$求和，可得

$$\sum_{j=1}^{p-1} \omega_q^{\left(a_{\sigma^j,r}^t - a_{\sigma^j,s}^t\right) - \left(a_{\sigma,r}^t - a_{\sigma,s}^t\right)} = \sum_{j=1}^{p-1} \omega_p^{j\left(r_{\pi_\beta(1)} - s_{\pi_\beta(1)}\right)} = -1. \tag{10}$$

因此，

$$\omega_q^{\left(a_{\sigma,r}^t - a_{\sigma,s}^t\right)} + \sum_{j=1}^{p-1} \omega_q^{\left(a_{\sigma^j,r}^t - a_{\sigma^j,s}^t\right)} = 0. \tag{11}$$

因此，非周期自相关函数之和为零。即，

$$\sum_{\sigma=0}^{p^k-1}\mathcal{A}(\mathbf{a}_\sigma^t)(\tau)=0. \tag{12}$$

情况 II: $r_{\pi_\beta(1)}=s_{\pi_\beta(1)}$ 对所有 $\beta\in\{1,2,\ldots,k\}$均成立。于是，存在整数 β 和 $\hat{}\gamma$，使得 β 是满足以下条件的最大整数$\hat{}$：对所有 $\beta=1$、2、...、$\beta-1$ 以及 $\gamma=1$、2、...、m_α，$r_{\pi_\beta(\gamma)}=s_{\pi_\beta(\gamma)}$；而 $\hat{}\gamma$ 是满足 $r_{\pi_{\hat{\beta}}(\hat{\gamma})}\neq s_{\pi_{\hat{\beta}}(\hat{\gamma})}$ 的最小整数。如果上述陈述不成立，则由于 $\bigcup_{\alpha=1}^{k}I_\alpha=\{1,2,\ldots,m-\delta\}$，对于 $i=1$、2、...、$m-\delta$，我们有 $r_i=s_i$。因此，τ 的下界估计为，

$$\tau=s-r=\sum_{i=m-\delta+1}^{m}(s_i-r_i)p^{i-1}\geq p^{m-\delta}, \tag{13}$$

τ 的上界也估计为，

$$\begin{aligned}\tau=&s-r=\sum_{i=m-\delta+1}^{m}(s_i-r_i)p^{i-1}\\&\leq p^{m-\delta}+p^{m-\delta+1}+\ldots+p^{m-1}=p^m-p^{m-\delta}.\end{aligned} \tag{14}$$

上述两个方程 (13) 和 (14) 与假设 $\tau\in(\mathcal{T}_1\cup\mathcal{T}_2)\cap\mathcal{T}$ 矛盾。因此，这保证了满足上述条件的整数 $\hat{}\beta$ 和 $\hat{}\gamma$ 的存在。设 r^j和 s^j 是两个整数，它们分别与 r 和 s仅在其 p进制表示的一个位置 $\pi_{\hat{\beta}}(\hat{}\gamma-1)$ 上不同，即 $r^j_{\pi_{\hat{\beta}}(\hat{\gamma}-1)}=r_{\pi_{\hat{\beta}}(\hat{\gamma}-1)}-j$ and $s^j_{\pi_{\hat{\beta}}(\hat{\gamma}-1)}=s_{\pi_{\hat{\beta}}(\hat{\gamma}-1)}-j$，其中 $1\leq j\leq p-1$。由于 $s=r+\tau$，我们得到 $s^j=r^j+\tau$。项 $a^t_{\sigma,r}-a^t_{\sigma,r^j}$ 之间的差值计算如下

$$\begin{aligned}a^t_{\sigma,r}-a^t_{\sigma,r^j}&=g_r-g_{r^j}\\&=j\left(\frac{q}{p}r_{\pi_{\hat{\beta}}(\hat{\gamma}-2)}+\frac{q}{p}r_{\pi_{\hat{\beta}}(\hat{\gamma})}+\lambda_{\pi_{\hat{\beta}}(\hat{\gamma}-1)}\right).\end{aligned} \tag{15}$$

同理，可以计算得出

$$a^t_{\sigma,s}-a^t_{\sigma,s^j}=j\left(\frac{q}{p}s_{\pi_{\hat{\beta}}(\hat{\gamma}-2)}+\frac{q}{p}s_{\pi_{\hat{\beta}}(\hat{\gamma})}+\lambda_{\pi_{\hat{\beta}}(\hat{\gamma}-1)}\right). \tag{16}$$

由上述两个方程并利用 $r_{\pi_{\hat{\beta}}(\hat{\gamma}-2)}\neq s_{\pi_{\hat{\beta}}(\hat{\gamma}-2)}$，可得以下等式

$$a^t_{\sigma,r^j}-a^t_{\sigma,s^j}-\left(a^t_{\sigma,r}-a^t_{\sigma,s}\right)=j\frac{q}{p}\left(s_{\pi_{\hat{\beta}}(\hat{\gamma})}-r_{\pi_{\hat{\beta}}(\hat{\gamma})}\right). \tag{17}$$

将其提升到 q 次单位根的幂，并对 $1\leq j\leq p-1$ 求和，可得以下表达式

$$\sum_{j=1}^{p-1}\omega_q^{\left(a^t_{\sigma,r^j}-a^t_{\sigma,s^j}\right)-\left(a^t_{\sigma,r}-a^t_{\sigma,s}\right)}=\sum_{j=1}^{p-1}\omega_p^{j\left(s_{\pi_{\hat{\beta}}(\hat{\gamma})}-r_{\pi_{\hat{\beta}}(\hat{\gamma})}\right)}=-1. \tag{18}$$

因此，

$$\omega_q^{\left(a^t_{\sigma,r}-a^t_{\sigma,s}\right)}+\sum_{j=1}^{p-1}\omega_q^{\left(a^t_{\sigma,r^j}-a^t_{\sigma,s^j}\right)}=0. \tag{19}$$

因此，非周期自相关函数为零。结合情形 I 和情形 II，我们得到，对于 $\tau\in(\mathcal{T}_1\cup\mathcal{T}_2)\cap\mathcal{T}$，$A^t$ 的非周期自相关函数为零。

接下来，我们将在下文证明，任意两个不同的集合 A^{t_1} 和 A^{t_2} 对所有 $|\tau|\in\{0\}\cup\mathcal{T}_1\cup\mathcal{T}_2$的非周期互相关函数均为零，即:

$$\sum_{\sigma=0}^{p^k-1}\mathcal{C}(\mathbf{a}_\sigma^{t_1},\mathbf{a}_\sigma^{t_2})(\tau)=\sum_{r=0}^{p^m-\tau-1}\sum_{\sigma=0}^{p^k-1}\omega_q^{\left(a^{t_1}_{\sigma,r}-a^{t_2}_{\sigma,r+\tau}\right)}=0. \tag{20}$$

与第一部分类似，对于任意整数 r，令 $s=r+\tau$，并考虑两种情况。

情况 I: 假设对于某个 $\beta\in\{1,2,\ldots,k\}$，有 $r_{\pi_\beta(1)}\neq s_{\pi_\beta(1)}$。按照第一部分情况 I 中相同的方式，存在一个 $\mathbf{a}^t_{\sigma^j}=(a^t_{\sigma^j,0},a^t_{\sigma^j,1},\ldots,a^t_{\sigma^j,p^m-1})=\mathbf{a}^t_\sigma+(jq/p)\boldsymbol{x}_{\pi_\beta(1)}\in A^t$，其中 $t=t_1,t_2$，且 $1\leq j\leq p-1$，使得

$$\sum_{j=1}^{p-1}\omega_q^{\left(a^{t_1}_{\sigma^j,r}-a^{t_2}_{\sigma^j,s}\right)-\left(a^{t_1}_{\sigma,r}-a^{t_2}_{\sigma,s}\right)}=\sum_{j=1}^{p-1}\omega_p^{j\left(r_{\pi_\beta(1)}-s_{\pi_\beta(1)}\right)}=-1. \tag{21}$$

因此，与第一部分类似，非周期互相关函数为零，即

$$\sum_{\sigma=0}^{p^k-1}\omega_q^{\left(a^{t_1}_{\sigma,r}-a^{t_2}_{\sigma,s}\right)}=0. \tag{22}$$

情况 II: 假设对于所有 $\beta\in\{1,2,\ldots,k\}$，均有 $r_{\pi_\beta(1)}=s_{\pi_\beta(1)}$。如第一部分的情况 II 中所述，可得到类似结果，即

$$\omega_q^{\left(a^{t_1}_{\sigma,r}-a^{t_2}_{\sigma,s}\right)}+\sum_{j=1}^{p-1}\omega_q^{\left(a^{t_1}_{\sigma,r^j}-a^{t_2}_{\sigma,s^j}\right)}=0. \tag{23}$$

因此，根据情况 I 和情况 II，我们得到 $\sum_{\sigma=0}^{p^k-1}\mathcal{C}(\mathbf{a}^{t_1}_\sigma,\mathbf{a}^{t_2}_\sigma)(\tau)=0$，其中 $|\tau|\in\mathcal{T}_1\cup\mathcal{T}_2$。只需证明

$$\sum_{\sigma=0}^{p^k-1}\mathcal{C}(\mathbf{a}_\sigma^{t_1},\mathbf{a}_\sigma^{t_2})(0)=\sum_{\sigma=0}^{p^k-1}\sum_{r=0}^{p^m-1}\omega_q^{\left(a^{t_1}_{\sigma,r}-a^{t_2}_{\sigma,r}\right)}=0. \tag{24}$$

令 $\oplus$ 表示模-p 加法；令 $(t_{11},t_{12},\ldots,t_{1k+\delta})$ 和 $(t_{21},t_{22},\ldots,t_{2k+\delta})$ 分别表示 t_1 和 t_2 的 p 进制表示。于是，对于 $\sigma=0,1,\ldots,p^k-1$，有 $\mathbf{a}^{t_1}_\sigma-\mathbf{a}^{t_2}_\sigma\equiv(q/p)\mathbf{d}\pmod q$，其中 $\mathbf{d}=(t_{11}\oplus t_{21})\boldsymbol{x}_{\pi_1(m_1)}\oplus(t_{12}\oplus t_{22})\boldsymbol{x}_{\pi_2(m_2)}\oplus\cdots\oplus(t_{1k}\oplus t_{2k})\boldsymbol{x}_{\pi_k(m_k)}\oplus(t_{1k+1}\oplus t_{1k+1})\boldsymbol{x}_{m-\delta+1}\oplus\cdots\oplus(t_{1k+\delta}\oplus t_{2k+\delta})\boldsymbol{x}_{m\circ}$ 对于每个 $1\leq\beta\leq k$，$\boldsymbol{x}_{\pi_\beta(m_\beta)}$ 从 $\{0,1,\ldots,p-1\}$ 中恰好取每个值 p^{m-1} 次。此外，对于 $1\leq\beta\leq\delta$，$\boldsymbol{x}_{m-\delta+\beta}$ 从 $\{0,1,\ldots,p-1\}$ 中恰好取每个值 p^{m-1} 次。因此，$\mathbf{d}$ 也从 $\{0,1,\ldots,p-1\}$ 中恰好取每个值 p^{m-1} 次，即 $\mathbf{d}$ 是平衡的。因此，

$$\sum_{r=0}^{p^m-1}\omega_q^{\left(a^{t_1}_{\sigma,r}-a^{t_2}_{\sigma,r}\right)}=\sum_{r=0}^{p^m-1}\omega_p^{d_r}=0. \tag{25}$$

因此，由式(24)和式(25)可知，移位 $\tau=0$ 处的非周期互相关函数为零，即

$$\sum_{\sigma=0}^{p^k-1}\mathcal{C}(\mathbf{a}_\sigma^{t_1},\mathbf{a}_\sigma^{t_2})(0)=0. \tag{26}$$

定理1中提出的SZCCS是最优的，因为 $K = p^{k+\delta} = p^k(p^m/p^{m-\delta}) = M(N/(Z+1))$。

注1：对于 $\delta = 0$，所提构造生成 (p^k, p^k, p^m)-互补码集。因此，[17], [18] 中 (p^k, p^k, p^m)-互补码集的构造是所提构造的一个特例。

注2：对于 $p = 2$，所提构造生成 $(2^{k+\delta}, 2^k, 2^m, 2^{m-\delta})$-零相关区互补集，因此，[19] 中已有的零相关区互补集构造是所提构造的一个特例。

注3：[20]，中给出了 $(p^{\delta+1}, p, p^m, p^{m-\delta})$-零相关区互补集的直接构造，而结合 $k = 1$ 的所提构造可生成具有相同参数的零相关区互补集。

注4：由于每个 SZCCS 都是零相关区互补集，[14] 中 $(p^{n+v}, p^n, p^m, p^{m-v})$-零相关区互补集的构造是定理1中所提构造的一个特例。

备注5：文献 [15],给出了$(8, 2, 2^m, 2^{m-2}-1)$-SZCCS的构造；当 $p = 2, \delta = 2, k = 1$.时，该构造是所提构造的一个特例。

下面给出一个例子，说明如何由定理1得到最优SZCCS。

例1：对于 $m = 3, \delta = 1$，令 $\pi_1 = \pi$ 为 $\{1, 2\}$上的恒等置换，即 $\pi(1) = 1$ 且 $\pi(2) = 2$。进一步取 $p = 3$ 和 $q = 3$，并定义多变量函数g：$\{0, 1, 2\}^3 \to \mathbb{Z}_3$ 为 $g(x_1, x_2, x_3) = x_1x_2$。再定义集合 $A^t = \{\mathrm{f} + \sigma_1 x_1 + t_1x_2 + t_2x_3 : \sigma_1 \in \{0, 1, 2\}\}$，其中 $t = 0$取$1, \ldots, 8$，且其 p进制表示为(t_1, t_2)。因此，由定理1可知，$\mathrm{A} = \{A^0, A^1, \ldots, A^8\}$ 是一个(9, 3, 27, 8)-SZCCS。码 $A^0, A^1, \ldots, A^8$ 在表I中明确列出，其中整数 i表示 ω^i，其中 $\omega = exp(2\pi\sqrt{-1}/3)$；$A^0$ 的非周期自相关函数图绘于图1，而 A^2 和 A^8 的非周期互相关函数图绘于图2。

表I：由示例1获得的不同 SZCSS 码

A^0	A^1
000012021000012021000012021	012021000012021000012021000
000120210000120210000120210	012102222012102222012102222
000201102000201102000201102	012210111012210111012210111
A^2	A^3
021000012021000012021000012	000012021111201022222012102
021111201021111201021111201	000120210111201021222012102
021222120021222120021222120	000201102111012210222120021
A^4	A^5
012021000120102111201210222	021000012102111120210222201
012102222120210000201021111	021111201102222012210000120
012210111120021222201102000	021222120102000201210111012
A^6	A^7
000012021222201210111120102	012021000201210222120102111
000120210222012102111201021	012102222201021111120210000
000201102222120021111012210	012210111201102000120021222
A^8	
021000012210222201102111120	
021111201210000120102222012	
021222120210111012102000201	

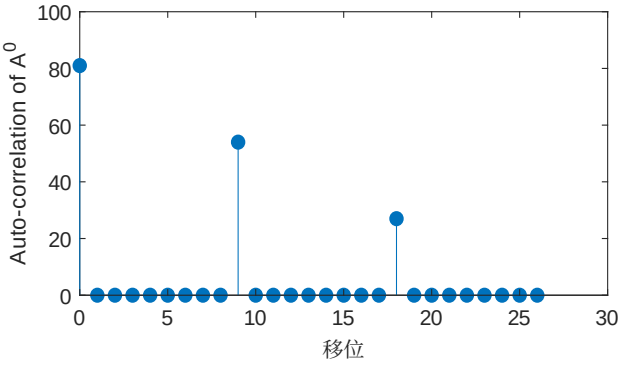


图1：A^0 的非周期自相关函数。

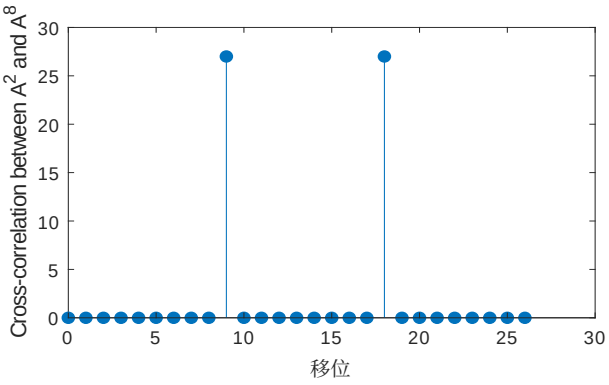


图2：A^2 和 A^8 的非周期互相关函数。

IV. 与现有工作的比较

在现有文献中，对 SZCCS 的研究相对较新，目前仅有针对 $(8, 2, 2^m, 2^{m-2}-1)$- SZCCS [15] 和 $(2, 2, 2^{m-1}+2^v, 2^v-1)$-SZCCS [21]的构造。最优片段零相关互补集用于设计 GSM系统的最优训练序列，与其他序列类相比，可实现更优的信道估计性能 [15], [21]。定理1中的所提构造可生成变量集大小为 $(p^{k+\delta})$、簇大小为 (p^k)、序列长度为 (p^m)、零相关区宽度为 $(p^{m-\delta}-1)$ 的最优片段零相关互补集。因此，凭借参数的灵活性，所提 SZCCS 能够灵活地为具有多个活动发射天线的 GSM系统生成最优训练矩阵 [21]。

根据定义 2 和 3，显然，零相关区互补集可视为片段零相关互补集的一种特殊情况，其中 $\mathcal{T}_2 = \phi$和 $\mathcal{T}_1 = \{1, 2, \ldots, Z-1\}$。此外，根据引理 1，片段零相关互补集的最优性意味着零相关区互补集也具有最优性。因此，正如注释1–4中所述，[17], [18] 中的现有互补码集构造以及 [14], [19], [20] 中的现有零相关区互补集构造，均可视为所提构造的特例。

V. 结论

本文直接利用多变量函数构造了素数幂长度的最优 SZCCS。由于 SZCCS 具有前端和尾端零相关区宽度，因此可用于

为频率选择性信道上的宽带 GSM 系统设计最优训练序列。所提出的基于多变量函数的构造可生成最优 ($p^{k+\delta}, p^k, p^m, p^{m-\delta}$ –1)-SZCCS，从而推广了许多现有的零相关区互补集和 SZCCS 研究成果。

参考文献

[1] P. Fan、W. Yuan 和 Y. Tu，“Z-互补二进制序列”，IEEE《信号处理快报》，第 14 卷，第 8 期，第 509–512 页，2007 年 8 月。[2] C.-Y. Pai、S.-W. Wu 和 C.-Y. Chen，“基于广义布尔函数的灵活长度 Z 补码对”，IEEE《通信快报》，第 24 卷，第 6 期，第 1183–1187 页，2020 年。[3] C.-Y. Chen，“一种基于广义布尔函数构造 Z 补码对的新方法”，IEEE《信号处理快报》，第 24 卷，第 7 期，第 987–990 页，2017 年。[4] A. R. Adhikary、P. Sarkar 和 S. Majhi，“利用广义布尔函数直接构造 q 元偶数长度 Z 补码对”，IEEE《信号处理快报》，第 27 卷，第 146–150 页，2020 年。[5] A. R. Adhikary、S. Majhi、Z. Liu 和 Y. L. Guan，“新型最优奇长度二进制 Z 补码对集”，IEEE《信息论汇刊》，第 66 卷，第 1 期，第 669–678 页，2020 年。[6] P. Kumar、P. Sarkar、S. Majhi 和 S. Paul，“具有较大 ZCZ 比率的偶数长度 ZCP 的直接构造”，《密码学与通信》，第 15 卷，第 85–94 页，2023 年。[7] L. Feng、P. Fan、X. Tang 和 K. K. Loo，“广义成对 Z 互补码”，IEEE《信号处理快报》，第 15 卷，第 380 页，2008 年，第 377 页。[8] S.-W. Wu、A. Sahin、Z.-M. Huang 和 C.-Y. Chen，“基于广义布尔函数的灵活长度 Z-互补码集”，IEEE Access，第 9 卷，第 4642–4652 页，2021 年。[9] P. Sarkar、S. Majhi 和 Z. Liu，“由广义 Reed-Muller 码构造的最优 Z-互补码集”，IEEE《通信汇刊》，第 67 卷，第 3 期，第 1783–1796 页，2019 年。[10] B. Shen、Y. Yang、P. Fan 和 Z. Zhou，“具有非 2 的幂次长度和低峰均功率比的新型 Z 互补／互补序列集”，《密码学与通信》，2022 年。[11] G. Ghosh、S. Majhi、P. Sarkar 和 A. K. Upadhaya，“利用广义布尔函数直接构造最优偶数长度 Z-互补码集”，IEEE《信号处理快报》，第 29 卷，第 872–876 页，2022 年。[12] C. Xie、Y. Sun 和 Y. Ming，“具有较大零相关区的最优二进制 Z-互补序列集的构造”，IEEE《信号处理快报》，第 28 卷，第 1694–1698 页，2021 年。[13] L. Tian、Y. Li、Z. Zhou 和 C. Xu，“通过酉多项式矩阵得到的两类具有良好互相关子集的 Z-互补码集”，IEEE《通信汇刊》，第 69 卷，第 5 期，第 2935–2947 页，2021 年。[14] X. Men 和 Y. Li，“具有组间零互相关区的新型多组完全互补码构造”，IEEE《信号处理快报》，第 29 卷，第 1958–1962 页，2022 年。[15] Y. Zhou、Z. Zhou、Z. Liu、Y. Yang、P. Yang 和 P. Fan，“用于广义空间调制最优训练的对称 z 互补码集”，载于第 10 届国际信号设计与应用研讨会（IWSDA），2022 年，第 1–5 页。[16] L. Feng、P. Fan 和 X. Zhou，“Z-互补码集相关性的下界”，《Wireless Personal Communications》，第 1475–1488 页，2013 年。[17] P. Sarkar、Z. Liu 和 S. Majhi，“用于构造任意长度新型完全互补码的多变量函数”，2021 年。 [在线]。可访问：https://arxiv.org/abs/ 2102 10517 。[18] N. Kumar、S. Majhi 和 A. K. Upadhyay，“针对素数幂长度，具有零相关区特性的完全互补码的直接构造”，2022 年。 [在线]。可访问：https://arxiv.org/abs/ 2207.13642[19] S.-W. Wu 和 C.-Y. Chen，“具有良好峰均功率比特性的最优 Z-互补序列集”，IEEE《信号处理快报》，第 25 卷，第 10 期，第 1500–1504 页，2018 年。[20] B. Shen、H. Meng、Y. Yang 和 Z. Zhou，“Z-互补码集和互相正交互补序列集的新构造”，《设计、代码与密码学》，2022 年。

[21] Y. Zhou、Z. Zhou、Z. Liu、Y. Yang、P. Yang 和 P. Fan，“用于广义空间调制最优训练的对称 z 互补码集”，《信号处理》，第 208 卷，文章号 108990，2023 年。[在线]。可访问：https://www.sciencedirect.com/science/article/pii/ S0165168423000646