AAECC (2014) 25:393–405
DOI 10.1007/s00200-014-0234-3

ORIGINAL PAPER

Unit time-phase signal sets with the explicit maximum cross ambiguity amplitudes

Chengju Li · Qin Yue

Received: 25 May 2012 / Revised: 30 July 2014 / Accepted: 18 September 2014 /
Published online: 27 September 2014

Abstract Unit time-phase signal sets have many important applications in radar or sonar systems. Upper bounds or lower bounds on the maximum cross ambiguity amplitudes of (n, M) unit time-phase signal sets with $M \geq 2$ have been presented in the literature. In this paper, we use Gauss sums to determine the explicit maximum cross ambiguity amplitudes of some infinite series of unit time-phase signal sets which were constructed by Ding et al. (Cryptogr Commun 5:209–227, 2013).

Keywords Unit time-phase signal sets · Stickelberger's Theorem · Index 2 Gauss sums · Maximum cross ambiguity amplitude

Mathematics Subject Classification 92A12 · 11T24 · 11T71

1 Introduction

Let $\mathbb{H}_n = \mathbb{C}(\mathbb{Z}_n)$ be a set of all complex-valued functions on $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for an integer $n > 1$, which is a Hilbert space with the Hermitian product given by

$$\langle \phi, \varphi \rangle = \sum_{t \in \mathbb{Z}_n} \phi(t)\overline{\varphi(t)}, \text{ for } \phi, \varphi \in \mathbb{H}_n.$$

C. Li · Q. Yue (✉)
Department of Mathematics, Nanjing University of Aeronautics and Astronautics,
Nanjing 211100, People's Republic of China
e-mail: yueqin@nuaa.edu.cn

C. Li
e-mail: lichengju1987@163.com

Q. Yue
SKL of Mathematical Engineering and Advanced Computing,
Wuxi, People's Republic of China

Digital signals are complex-valued functions on $\mathbb{Z}_n$. The function $\phi \in \mathbb{H}_n$ can be viewed as a sequence via the following mapping

$$\phi \mapsto (\phi(0), \phi(1), \ldots, \phi(n-1)).$$

A subset $S \subset \mathbb{H}_n$ is called a signal set, and a unit signal set if the norm $\| \phi \| \triangleq \sqrt{\langle \phi, \phi \rangle} = 1$ for every signal $\phi \in S$. In this paper, we only consider unit signal sets because every signal can be normalized into a unit signal.

Signal sets with certain properties are required in some communication systems (see [1–8,11,12,15]). During the transmission process, a signal ϕ might be distorted in various ways. Two basic types of distortion are the time shift

$$\phi(t) \mapsto \mathbf{L}_\tau \phi(t) = \phi(t+\tau)$$

and the phase shift

$$\phi(t) \mapsto \mathbf{M}_\omega \phi(t) = e^{\frac{2\pi\sqrt{-1}}{n}\omega t}\phi(t),$$

where $\tau, \omega \in \mathbb{Z}_n$. To measure the capability of anti-distortion of a signal set S with respect to the time and phase shift, Gurevich, Hadani and Sochen [7] defined the maximum cross ambiguity amplitude λ of an (n, M) signal set by

$$\lambda = \max\{|\langle \phi, \mathbf{M}_\omega \mathbf{L}_\tau \varphi \rangle| : \text{ either } \phi \neq \varphi \text{ or } (\tau, \omega) \neq (0,0)\}.$$

Then we call S an (n, M, λ) time-phase signal set when both time and phase shifts are considered, where M denotes the total number of signals in S. If only time shift is considered (i.e., $\omega = 0$), we call S an (n, M) time signal set or codebook (see [1,8,15]).

In [7], the authors used the group representation theory to design signal sets which were given by an algorithm. Unfortunately, the explicit form of these signal sets was unknown. Based on their results, Wang and Gong [12] gave an elegant expression for these time-phase signal sets by both multiplicative characters and additive characters of finite fields and presented upper bounds on the maximum cross ambiguity amplitudes. Schmidt [11] presented more constructions of such signal sets and easily obtained the upper bounds by using Weil bound. Moreover, the upper bounds on the maximum cross ambiguity amplitudes of some families of signal sets designed by multiplicative characters or additive characters were given in [13]. Ding et al. [2] proved that the famous Welch's bound and the Levenstein's bound on λ are not good for time-phase signal sets. Moreover, they presented some better bounds from two one-way bridges between time-phase signal sets and time signal sets.

Lemma 1 [2] *For any (n, M, λ) unit time-phase signal set S with $\lambda < 1$ and $M > 1$, we have the improved Levenstein's bound:*

$$\lambda \geq \sqrt{\frac{2nM - n - 1}{(n+1)(nM-1)}}.$$

Let $\mathbb{H}_{(n,q)}$ be the set of all complex-valued functions f on $\mathbb{Z}_n$ such that $\sqrt{n}f(i)$ is a qth root of unity for all $i \in \mathbb{Z}_n$. In [2], we have some better linear programming bounds on M and λ from Levenstein's results as follows.

Lemma 2 [2] *Let $S \subset \mathbb{H}_{(n,q)}$ be any (n, M, λ) unit time-phase signal set, where $q = 2$. Then*

$$nM \leq \begin{cases} \frac{1-\lambda^2}{1-n\lambda^2}, & \text{if } 0 \leq \lambda^2 \leq \frac{n-2}{n^2}, \\ \frac{n^2(1-\lambda^2)}{3n-2-n^2\lambda^2}, & \text{if } \frac{n-2}{n^2} \leq \lambda^2 \leq \frac{3n-8}{n^2}, \\ \frac{n(1-\lambda^2)[(n-2)(n^2-3n+8)-(n^2-n+2)n^2\lambda^2]}{6n(n-2)-4(3n-4)n^2\lambda^2+2n^4\lambda^4}, & \text{if } \frac{3n-8}{n^2} \leq \lambda^2 \leq \frac{3n-10+\sqrt{6n^2-42n+76}}{n^2}, \\ \frac{n^2(1-\lambda^2)}{6}\,\frac{3n^3-23n^2+90n-136-(n^2-3n+8)n^2\lambda^2}{15n^2-50n+24-10(n-2)n^2\lambda^2+n^4\lambda^4}, & \text{if } \frac{3n-10+\sqrt{6n^2-42n+76}}{n^2} \leq \lambda^2 \\ & \leq \frac{5(n-4)+\sqrt{10n^2-90n+216}}{n^2} \end{cases}$$

Lemma 3 [2] *Let $S \subset \mathbb{H}_{(n,q)}$ be any (n, M, λ) unit time-phase signal set, where $q \geq 3$. Then*

$$nM \leq \begin{cases} \frac{1-\lambda^2}{1-n\lambda^2}, & \text{if } 0 \leq \lambda^2 \leq \frac{n-1}{n^2}, \\ \frac{n^2(1-\lambda^2)}{2n-1-n^2\lambda^2}, & \text{if } \frac{n-1}{n^2} \leq \lambda^2 \leq \frac{2n^2-5n+4}{n^2(n-1)}, \\ \frac{n(1-\lambda^2)[(n^2-n+1)n^2\lambda^2-n^3+3n^2-5n+4]}{n[4(n-1)n^2\lambda^2-n^4\lambda^4-2n^2+3n]}, & \text{if } \frac{2n^2-5n+4}{n^2(n-1)} \leq \lambda^2 \leq \frac{2n-2+\sqrt{2n^2-5n+4}}{n^2}. \end{cases}$$

When $q \geq 3$ and $\frac{n-1}{n^2} \leq \lambda^2 \leq \frac{2n^2-5n+4}{n^2(n-1)}$, an infinite series of optimal $(n, 1)$ unit time-phase signal sets were firstly constructed by Ding et al. [2], who also presented $(n, M > 1)$ unit time-phase signal sets and obtained the upper bounds on the maximum cross ambiguity amplitudes. Based on the construction in [2], we study some infinite series of $(n, M > 1)$ unit time-phase signal sets for all cases in Lemmas 2 and 3 with the exception of the second case in Lemma 3 and use the Stickelberger's Theorem and index 2 Gauss sums to give the explicit maximum cross ambiguity amplitudes.

The paper is organized as follows. In Sect. 2, we introduce some basic concepts and results about Gauss sums. In Sect. 3, we use Gauss sums to determine the explicit maximum cross ambiguity amplitudes of some infinite series of $(n, M > 1)$ unit time-phase signal sets.

For convenience, we introduce the following notations:

$\mathbb{Z}_N, \mathbb{Z}_N^*$	the ring of integers modulo N, the multiplicative group of $\mathbb{Z}_N$,
$\langle p \rangle$	the cyclic subgroup of $\mathbb{Z}_N^*$ generated by p,
$\Phi(N)$	the number of integers k with $1 \leq k \leq N$ such that $\gcd(k, N) = 1$,
$\mathrm{ord}_N(p)$	the order of p modulo N,
$\mathbb{F}_q$	the finite field of order q,
Tr	the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$,
ψ	the additive character of $\mathbb{F}_q$,
χ	the multiplicative character of $\mathbb{F}_q$,
$o(\chi)$	the order of the multiplicative character χ,

$G(\chi)$ the Gauss sum over $\mathbb{F}_q$,
$(\frac{p_1}{p_2})$ the Legendre symbol.

2 Gauss sums

Let $\mathbb{F}_q$ be a finite field with $q = p^f$ elements, p a prime, and f a positive integer. Define an additive character of $\mathbb{F}_q$ as follows:

$$\psi_b : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi_b(x) = \zeta_p^{\mathrm{Tr}(bx)}, \text{ for } b \in \mathbb{F}_q, \tag{1}$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a pth primitive root of unity and Tr denotes the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. For $b = 1$, ψ_1 is called the canonical additive character of $\mathbb{F}_q$. Let $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ be a multiplicative character of $\mathbb{F}_q^*$. We have the Gauss sum:

$$G(\psi_b, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi_b(x)\chi(x).$$

Now we recall some properties of Gauss sums.

Lemma 4 [10] *Let ψ and χ be an additive character and a multiplicative character of $\mathbb{F}_q$, respectively. Then*

$$G(\psi, \chi) = \begin{cases} q-1, & \text{if } \psi = 1 \text{ and } \chi = 1, \\ -1, & \text{if } \psi \neq 1 \text{ and } \chi = 1, \\ 0, & \text{if } \psi = 1 \text{ and } \chi \neq 1. \end{cases}$$

If $\psi = \psi_b \neq 1$ (i.e., $b \neq 0$) and $\chi \neq 1$, then

$$|G(\psi, \chi)| = \sqrt{q},$$

and

$$G(\psi_b, \chi) = \overline{\chi}(b)G(\chi),$$

where

$$G(\chi) = G(\psi_1, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi_1(x)\chi(x) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\zeta_p^{\mathrm{Tr}(x)}.$$

While it is easy to know the absolute value of a nontrivial Gauss sum $G(\psi, \chi)$ is equal to $\sqrt{q}$, the explicit determination of Gauss sum is a difficult problem. However, the Gauss sums can be explicitly evaluated in a few cases. For future use, we state the Stickelberger's Theorem.

Lemma 5 (Stickelberger's Theorem [10]) *Let $q = p^{2l}$ with p a prime and l a positive integer, let χ be a nontrivial multiplicative character of $\mathbb{F}_q$ of order m dividing $p^l + 1$, and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Then*

$$G(\chi) = G(\psi_1, \chi) = \begin{cases} p^l, & \text{if } m \text{ odd or } \frac{p^l+1}{m} \text{ even,} \\ -p^l, & \text{if } m \text{ even and } \frac{p^l+1}{m} \text{ odd.} \end{cases}$$

Below we introduce a result on one case of the index 2 Gauss sums which involves class numbers of number fields. The definition of the class number can be found in any algebraic number theory and we refer the readers to [6] and [9].

Lemma 6 [14] *Let $N = p_1^{r_1} p_2^{r_2}$, where p_1, p_2 are distinct odd primes with $p_1 \equiv 3 \pmod 4$. Assume that p is a prime such that $-1 \notin \langle p \rangle \leq \mathbb{Z}_N^*$ and $f = ord_N(p) = \frac{\Phi(N)}{2}$, where f is the smallest positive integer such that $p^f \equiv 1 \pmod N$. Let $q = p^f$ and χ a multiplicative character of order N over $\mathbb{F}_q$. Suppose that $ord_{p_1^{r_1}}(p) = \frac{\Phi(p_1^{r_1})}{2}$, $ord_{p_2^{r_2}}(p) = \Phi(p_2^{r_2})$. For $0 \leq t_1 < r_1, 0 \leq t_2 < r_2$, we have*

$$G(\chi^{p_1^{t_1} p_2^{t_2}}) = \begin{cases} p^{\frac{f}{2}}, & \text{if } (\frac{p_2}{p_1}) = 1, \\ p^{\frac{f}{2} - h p_1^{t_1} p_2^{t_2}} (\frac{b + c\sqrt{-p_1}}{2})^{2 p_1^{t_1} p_2^{t_2}}, & \text{if } (\frac{p_2}{p_1}) = -1; \end{cases}$$

$$G(\chi^{p_1^{r_1} p_2^{t_2}}) = p^{\frac{f}{2}};$$

$$G(\chi^{p_1^{t_1} p_2^{r_2}}) = -p^{\frac{1}{2}(f - h p_1^{t_1} \Phi(p_2^{r_2}))} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^{p_1^{t_1} \Phi(p_2^{r_2})},$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$ and b, c are determined by

$$\begin{cases} (1)\ 4p^h = b^2 + p_1 c^2, \\ (2)\ b \equiv 2p^{\frac{p_1 - 1 + 2h}{4}} \pmod{p_1}. \end{cases}$$

3 ($n, M > 1$) unit time-phase signal sets

In this section, we use Gauss sums to determine the explicit maximum cross ambiguity amplitudes of some infinite series of unit time-phase signal sets which were constructed by Ding et al. [2]. Now we introduce the results on their constructions of $(n, 1)$ and $(n, M > 1)$ unit time-phase signal sets.

The construction of case $(n, 1)$ can be described as follows [2]. Let $q = p^f$, p a prime, $n = q - 1$, $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ the trace mapping, and γ a primitive element of $\mathbb{F}_q$. Let

$$\phi = \frac{1}{\sqrt{n}} (\phi(0), \phi(1), \ldots, \phi(n-1)) \in \mathbb{C}^n,$$

where

$$\phi(i) = \zeta_p^{\mathrm{Tr}(\gamma^i)}, \quad 0 \leq i \leq n-1.$$

Then $S = \{\phi\}$ is an $(n, 1, \frac{\sqrt{n+1}}{n})$ unit time-phase set. Moreover, S is optimal if $p \geq 3$. This is the first time that an infinite family of optimal time-phase signal sets was constructed.

The construction of the case $(n, M > 1)$ can be described in the following lemma.

Lemma 7 [2] *Let $q = p^f$, p a prime, $q - 1 = en$ $(e \geq 2)$, $Tr : \mathbb{F}_q \to \mathbb{F}_p$ the trace mapping, and γ a primitive element of $\mathbb{F}_q$. For $0 \leq i \leq e - 1$, let*

$$\phi_i = \frac{1}{\sqrt{n}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(n-1)) \in \mathbb{C}^n,$$

where

$$\phi_i(t) = \zeta_p^{Tr(\gamma^{i+et})}, \quad 0 \leq t \leq n-1.$$

Then $S = \{\phi_i : 0 \leq i \leq e-1\}$ is a $(\frac{q-1}{e}, e, \lambda)$ unit time-phase signal set with $\lambda \leq \frac{\sqrt{en+1}}{n}$.

Proof For completeness, we give a proof here. For $0 \leq i, j \leq e-1, 0 \leq \omega, \tau \leq n-1, (i-j, \omega, \tau) \neq (0,0,0)$, we have

$$\begin{aligned}
\langle \phi_i, \mathbf{M}_\omega \mathbf{L}_\tau(\phi_j) \rangle &= \frac{1}{n} \sum_{t=0}^{n-1} \zeta_p^{\mathrm{Tr}(\gamma^{i+et})} \overline{\zeta}_p^{\mathrm{Tr}(\gamma^{j+e(t+\tau)})} \overline{\zeta}_n^{\omega t} \\
&= \frac{1}{n} \sum_{t=0}^{n-1} \zeta_p^{\mathrm{Tr}(\gamma^{et}(\gamma^i - \gamma^{j+e\tau}))} \overline{\zeta}_n^{\omega t} \\
&= \frac{1}{n} \sum_{t=0}^{n-1} \zeta_p^{\mathrm{Tr}(\beta\gamma^{et})} \chi^\omega(\gamma^{et}),
\end{aligned}$$

where $\beta = \gamma^i - \gamma^{j+e\tau}$ and χ is the multiplicative character of $\mathbb{F}_q^*$ defined by $\chi(\gamma) = \overline{\zeta}_{q-1}$. Note that for $0 \leq r \leq q-2$, we have

$$\sum_{s=0}^{e-1} \chi^{ns}(\gamma^r) = \sum_{s=0}^{e-1} \overline{\zeta}_e^{rs} = \begin{cases} e, & \text{if } e \mid r \\ 0, & \text{otherwise .} \end{cases}$$

Thus

$$\begin{aligned}
\frac{1}{n} \sum_{t=0}^{n-1} \zeta_p^{\mathrm{Tr}(\beta\gamma^{et})} \chi^\omega(\gamma^{et}) &= \frac{1}{en} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}(\beta x)} \chi^\omega(x) \sum_{s=0}^{e-1} \chi^{ns}(x) \\
&= \frac{1}{en} \sum_{s=0}^{e-1} \sum_{x \in \mathbb{F}_q^*} \chi^{ns+\omega}(x) \zeta_p^{\mathrm{Tr}(\beta x)}.
\end{aligned}$$

If $(j-i,\tau)=(0,0)$, we have $1\le\omega\le n-1$, $\beta=\gamma^i-\gamma^{j+\tau e}=0$, and $\chi^{ns+\omega}\ne 1$ for all s, $0\le s\le e-1$. Then

$$\langle\phi_i,\mathbf{M}_\omega\mathbf{L}_\tau(\phi_j)\rangle=\frac{1}{en}\sum_{s=0}^{e-1}\sum_{x\in\mathbb{F}_q^*}\chi^{ns+\omega}(x)=\frac{1}{en}\sum_{s=0}^{e-1}0=0.$$

If $(j-i,\tau)\ne(0,0)$, i.e., $\beta\ne 0$, then

$$\begin{aligned}\langle\phi_i,\mathbf{M}_\omega\mathbf{L}_\tau(\phi_j)\rangle&=\frac{1}{en}\sum_{s=0}^{e-1}\overline{\chi}^{ns+\omega}(\beta)G(\chi^{ns+\omega})\\&\le\frac{1}{en}\sum_{s=0}^{e-1}|G(\chi^{ns+\omega})|\le\frac{e\sqrt{q}}{en}=\frac{\sqrt{en+1}}{n}.\end{aligned}$$

Therefore the upper bound on λ follows. □

It is very difficult to compute the explicit value λ for the time-phase signal set S in Lemma 7, and thus unable to know if it is optimal. In the following, we determine the explicit values of λ in some special cases. For $p\ge 3$, the case that $\lambda^2\in[\frac{n-1}{n^2},\frac{2n^2-5n+4}{n^2(n-1)}]$ had been studied by Ding et al. [2]. In the following, we shall consider all cases stated in Lemmas 2 and 3 with the exception of the above case.

(1) **When** $p\ge 3$.

For the case $\lambda^2\in[0,\frac{n-1}{n^2}]$, we have

$$\lambda^2\ge\frac{nM-1}{n^2M-1}$$

from the first bound of Lemma 3. Thus it is easily verified that $n=M=1$, it is trivial. Now we study the $(n,2)$ and $(n,3)$ unit time-phase signal sets for the case $\lambda^2\in[\frac{2n^2-5n+4}{n^2(n-1)},\frac{2n-2+\sqrt{2n^2-5n+4}}{n^2}]$.

Theorem 1 *Let $q=p^{2l}$, $p\equiv 3\pmod 4$ a prime, l odd, $n=\frac{q-1}{2}$, $Tr:\mathbb{F}_q\to\mathbb{F}_p$ the trace mapping, and γ a primitive element of $\mathbb{F}_q$. For $i=0,1$, let*

$$\phi_i=\frac{1}{\sqrt{n}}(\phi_i(0),\phi_i(1),\ldots,\phi_i(n-1))\in\mathbb{C}^n,$$

where

$$\phi_i(t)=\zeta_p^{Tr(\gamma^{i+2t})},\quad 0\le t\le n-1.$$

Then $S=\{\phi_0,\phi_1\}$ is a $(\frac{q-1}{2},2,\frac{\sqrt{2n+1}}{n})$ unit time-phase signal set, which falls into the third case of Lemma 3.

Proof From the proof of Lemma 7, we have

$$\langle \phi_i, \mathbf{M}_\omega \mathbf{L}_\tau(\phi_j)\rangle = \frac{1}{2n}(\overline{\chi}^\omega(\beta)G(\chi^\omega) + \overline{\chi}^{n+\omega}(\beta)G(\chi^{n+\omega})),$$

for $i, j \in \{0, 1\}$, $0 \le \omega, \tau \le n-1$, $(i-j, \omega, \tau) \ne (0, 0, 0)$, where $\beta = \gamma^i - \gamma^{j+2\tau}$.

For arbitrary $i \in \{0, 1\}$, $j \in \{0, 1\}$ and $\tau \in \{0, \ldots, n-1\}$, we can always take some (i_0, j_0, τ_0) such that $\beta = \gamma^{i_0} - \gamma^{j_0+2\tau_0} = 1$, thus $\overline{\chi}^\omega(\beta) = \overline{\chi}^{n+\omega}(\beta) = 1$. Take $\omega = \frac{q-1}{4}$, then the orders of both χ^ω and $\chi^{n+\omega}$ are equal to 4. Since $p \equiv 3 \pmod 4$ and l is odd, $4 \mid (p^l + 1)$. By Stickelberger's Theorem, we have

$$G(\chi^{\frac{q-1}{4}}) = G(\chi^{n+\frac{q-1}{4}})$$

and

$$\lambda \ge |\langle \phi_{i_0}, \mathbf{M}_\omega \mathbf{L}_{\tau_0}(\phi_{j_0})\rangle| = \frac{2\sqrt{q}}{2n} = \frac{\sqrt{2n+1}}{n}.$$

By Lemma 7, we have $\lambda = \frac{\sqrt{2n+1}}{n}$ which falls into the third case of Lemma 3. Hence $S = \{\phi_0, \phi_1\}$ is a $(\frac{q-1}{2}, 2, \frac{\sqrt{2n+1}}{n})$ unit time-phase signal set. □

Example 1 Let $q = 3^2$, $n = 4$, and γ a primitive element of $\mathbb{F}_q$. For $i = 0, 1$, let

$$\phi_i = \frac{1}{2}(\phi_i(0), \phi_i(1), \phi(2), \phi_i(3)) \in \mathbb{C}^4,$$

where

$$\phi_i(t) = \zeta_3^{\mathrm{Tr}(\gamma^{i+2t})}, \quad 0 \le t \le 3.$$

Then $S = \{\phi_0, \phi_1\}$ is an $(4, 2, \frac{3}{4})$ unit time-phase signal set, which falls into the third case of Lemma 3.

Theorem 2 *Let $q = p^{2l}$, $p \equiv 2 \pmod 3$ an odd prime, l odd, $n = \frac{q-1}{3}$, $Tr : \mathbb{F}_q \to \mathbb{F}_p$ the trace mapping, and γ a primitive element of $\mathbb{F}_q$. For $0 \le i \le 2$, let*

$$\phi_i = \frac{1}{\sqrt{n}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(n-1)) \in \mathbb{C}^n,$$

where

$$\phi_i(t) = \zeta_p^{Tr(\gamma^{i+3t})}, \quad 0 \le t \le n-1.$$

Then $S = \{\phi_0, \phi_1, \phi_2\}$ is a $(\frac{q-1}{3}, 3, \frac{\sqrt{3n+1}}{n})$ unit time-phase signal set, which falls into the third case of Lemma 3.

Proof From the proof of Lemma 7, we have

$$\langle \phi_i, \mathbf{M}_\omega \mathbf{L}_\tau(\phi_j)\rangle = \frac{1}{3n}(\overline{\chi}^{\omega}(\beta)G(\chi^{\omega}) + \overline{\chi}^{n+\omega}(\beta)G(\chi^{n+\omega}) + \overline{\chi}^{2n+\omega}(\beta)G(\chi^{2n+\omega})),$$

for $0 \le i, j \le 2, 0 \le \omega, \tau \le n-1, (i-j, \omega, \tau) \ne (0,0,0)$, where $\beta = \gamma^i - \gamma^{j+3\tau}$.

For arbitrary $i, j \in \{0,1,2\}$ and $\tau \in \{0, \ldots, n-1\}$, we can always take some (i_0, j_0, τ_0) such that $\beta = \gamma^{i_0} - \gamma^{j_0+3\tau_0} = 1$, thus $\overline{\chi}^{\omega}(\beta) = \overline{\chi}^{n+\omega}(\beta) = \overline{\chi}^{2n+\omega}(\beta) = 1$. Take $\omega = \frac{q-1}{6}$, then there are three orders:

$$o(\chi^{\omega}) = 6, o(\chi^{2n+\omega}) = 6 \quad \text{and} \quad o(\chi^{n+\omega}) = 2.$$

Since $p \equiv 2 \pmod 3$ is an odd prime and l is odd, $6 \mid (p^l+1)$ and $2 \mid (p^l+1)$. By Stickelberger's Theorem, we have

$$G(\chi^{\frac{q-1}{6}}) = G(\chi^{n+\frac{q-1}{6}}) = G(\chi^{2n+\frac{q-1}{6}})$$

and

$$\lambda \ge |\langle \phi_{i_0}, \mathbf{M}_\omega \mathbf{L}_{\tau_0}(\phi_{j_0})\rangle| = \frac{3\sqrt{q}}{3n} = \frac{\sqrt{3n+1}}{n}.$$

By Lemma 7, we know that $\lambda = \frac{\sqrt{3n+1}}{n}$ which falls into the third case of Lemma 3. Hence $S = \{\phi_0, \phi_1, \phi_2\}$ is a $(\frac{q-1}{3}, 3, \frac{\sqrt{3n+1}}{n})$ unit time-phase signal set. □

Example 2 Let $q = 5^2, n = 8$, and γ a primitive element of $\mathbb{F}_q$. For $0 \le i \le 2$, let

$$\phi_i = \frac{1}{2\sqrt{2}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(7)) \in \mathbb{C}^8,$$

where

$$\phi_i(t) = \zeta_5^{\mathrm{Tr}(\gamma^{i+3t})}, \quad 0 \le t \le 7.$$

Then $S = \{\phi_0, \phi_1, \phi_2\}$ is an $(8, 3, \frac{5}{8})$ unit time-phase signal set, which falls into the third case of Lemma 3.

(2) **When** $p = 2$.

For the case $\lambda^2 \in [0, \frac{n-2}{n^2}]$, we have

$$\lambda^2 \ge \frac{nM-1}{n^2M-1}$$

from the fist bound of Lemma 2. Thus it is easily verified that $n = M = 1$, it is trivial. The $(n, 1, \frac{\sqrt{n+1}}{n})$ unit time-phase signal set constructed in [2] falls into the second

case of Lemma 2 when $p = 2$. In the following, we study the other cases in Lemma 2 using Stickelberger's Theorem and index 2 Gauss sums.

For the third case of Lemma 2, we use Stickelberger's Theorem to give the explicit maximum cross ambiguity amplitude.

Theorem 3 *Let* $q = 2^{2l}, l \equiv 5 \pmod{10}, n = \frac{q-1}{3}$, $Tr : \mathbb{F}_q \to \mathbb{F}_2$ *the trace mapping, and* γ *a primitive element of* $\mathbb{F}_q$. *For* $0 \le i \le 2$, *let*

$$\phi_i = \frac{1}{\sqrt{n}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(n-1)) \in \mathbb{C}^n,$$

where

$$\phi_i(t) = (-1)^{Tr(\gamma^{i+3t})}, \quad 0 \le t \le n-1.$$

Then $S = \{\phi_0, \phi_1, \phi_2\}$ *is a* $(\frac{q-1}{3}, 3, \frac{\sqrt{3n+1}}{n})$ *unit time-phase signal set, which falls into the third case of Lemma 2.*

Proof Since $l \equiv 5 \pmod{10}$, $l = 5l_1$ and l_1 is odd. Then $q-1 = 2^{2l}-1 = (2^{10}-1)d_1$ and $2^l + 1 = (2^5+1)d_2$, where d_1, d_2 are integers, so $33 \mid (q-1)$ and $33 \mid (2^l+1)$. Take $\omega = \frac{q-1}{33}$, then there are three orders:

$$o(\chi^w) = o(\chi^{2n+w}) = 33 \quad \text{and} \quad o(\chi^{n+w}) = 11.$$

By Lemma 7 and Stickelberger's Theorem, we have $\lambda = \frac{\sqrt{3n+1}}{n}$ which falls into the third case of Lemma 2. Then we finish the proof. □

Example 3 Let $q = 2^{10}, n = \frac{q-1}{3} = 341$, and γ a primitive element of $\mathbb{F}_q$. For $0 \le i \le 2$, let

$$\phi_i = \frac{1}{\sqrt{341}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(340)) \in \mathbb{C}^{341},$$

where

$$\phi_i(t) = (-1)^{\mathrm{Tr}(\gamma^{i+3t})}, \quad 0 \le t \le 340.$$

Then $S = \{\phi_0, \phi_1, \phi_2\}$ is a $(341, 3, \frac{32}{341})$ unit time-phase signal set, which falls into the third case of Lemma 2.

Theorem 4 *Let* $q = 2^{2l}, l \equiv 6 \pmod{12}, n = \frac{q-1}{5}$, $Tr : \mathbb{F}_q \to \mathbb{F}_2$ *the trace mapping, and* γ *a primitive element of* $\mathbb{F}_q$. *For* $0 \le i \le 4$, *let*

$$\phi_i = \frac{1}{\sqrt{n}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(n-1)) \in \mathbb{C}^n,$$

where

$$\phi_i(t) = (-1)^{Tr(\gamma^{i+5t})}, \quad 0 \le t \le n-1.$$

Then $S = \{\phi_i : 0 \le i \le 4\}$ *is a* $(\frac{q-1}{5}, 5, \frac{\sqrt{5n+1}}{n})$ *unit time-phase signal set, which falls into the third case of Lemma* 2.

Proof Since $l \equiv 6 \pmod{12}$, $l = 6l_1$ and l_1 is odd. Then $q-1 = 2^{2l}-1 = (2^{12}-1)d_1$ and $2^l + 1 = (2^6+1)d_2$, where d_1, d_2 are integers, so $65|(q-1)$ and $65|2^l+1$. Take $\omega = \frac{q-1}{65}$, then there are five orders:

$$o(\chi^{sn+w}) = 65 (s = 0, 1, 2, 4) \quad \text{and} \quad o(\chi^{3n+w}) = 13.$$

By Lemma 7 and Stickelberger's Theorem, we have $\lambda = \frac{\sqrt{5n+1}}{n}$ which falls into the third case of Lemma 2. Then we finish the proof. □

Example 4 Let $q = 2^{12}, n = \frac{q-1}{5} = 819$, and γ a primitive element of $\mathbb{F}_q$. For $0 \le i \le 4$, let

$$\phi_i = \frac{1}{\sqrt{819}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(818)) \in \mathbb{C}^{819},$$

where

$$\phi_i(t) = (-1)^{\mathrm{Tr}(\gamma^{i+5t})}, \quad 0 \le t \le 818.$$

Then $S = \{\phi_i : 0 \le i \le 4\}$ is an $(819, 5, \frac{64}{819})$ unit time-phase signal set, which falls into the third case of Lemma 2.

In the following, we use the index 2 Gauss sums to study the fourth case of Lemma 2.

Theorem 5 *Let* $q = 2^f, 30 \mid f, n = \frac{q-1}{7}$, $Tr : \mathbb{F}_q \to \mathbb{F}_2$ *the trace mapping, and* γ *a primitive element of* $\mathbb{F}_q$. *For* $0 \le i \le 6$, *let*

$$\phi_i = \frac{1}{\sqrt{n}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(n-1)) \in \mathbb{C}^n,$$

where

$$\phi_i(t) = (-1)^{Tr(\gamma^{i+7t})}, \quad 0 \le t \le n-1.$$

Then $S = \{\phi_i : 0 \le i \le 6\}$ *is a* $(\frac{q-1}{7}, 7, \frac{\sqrt{7n+1}}{n})$ *unit time-phase signal set, which falls into the fourth case of Lemma* 2.

Proof Since $30 \mid f$, we have $f = 30f_1$ and f_1 is an integer. Then $q-1 = 2^f - 1 = (2^{30}-1)d$, where d is an integer, so $77 \mid (2^{30}-1)$ and $77 \mid (q-1)$.

From the proof of Lemma 7, we have

$$\langle \phi_i, \mathbf{M}_\omega \mathbf{L}_\tau(\phi_j)\rangle = \frac{1}{7n}\sum_{s=0}^{6} \overline{\chi}^{ns+\omega}(\beta) G(\chi^{ns+\omega})$$

for $0 \le i, j \le 6$, $0 \le \omega, \tau \le n-1$, $(i-j, \omega, \tau) \ne (0,0,0)$, where $\beta = \gamma^i - \gamma^{j+7\tau}$.

For arbitrary i, j, τ, we can always take some (i_0, j_0, τ_0) such that $\beta = \gamma^{i_0} - \gamma^{j_0+7\tau_0} = 1$, thus $\overline{\chi}^{ns+\omega}(\beta) = 1$ for $0 \le s \le 6$. Take $\omega = \frac{q-1}{77}$, then

$$o(\chi^{ns+\omega}) = 77 (s = 0, 1, 2, 3, 4, 6) \quad \text{and} \quad o(\chi^{5n+\omega}) = 11.$$

Note that $\mathrm{ord}_7(2) = \frac{\phi(7)}{2}$, $\mathrm{ord}_{11}(2) = \phi(11)$, $\mathrm{ord}_{77}(2) = \frac{\phi(77)}{2}$, and the Legendre symbol $(\frac{11}{7}) = 1$. By Lemma 6 and Davenport–Hasse Lifting Theorem (see [10]), we have

$$G(\chi^{ns+\frac{q-1}{6}}) = (-1)^{f_1-1}\sqrt{q}, s = 0, 1, \ldots, 6.$$

Therefore

$$\lambda \ge |\langle \phi_{i_0}, \mathbf{M}_\omega \mathbf{L}_{\tau_0}(\phi_{j_0})\rangle| = \frac{7\sqrt{q}}{7n} = \frac{\sqrt{7n+1}}{n}.$$

By Lemma 7, we have $\lambda = \frac{\sqrt{7n+1}}{n}$ which falls into the fourth case of Lemma 2. Hence $S = \{\phi_i : 0 \le i \le 6\}$ is a $(\frac{q-1}{7}, 7, \frac{\sqrt{7n+1}}{n})$ unit time-phase signal set. □

Example 5 Let $q = 2^{30}$, $n = \frac{2^{30}-1}{7}$, and γ a primitive element of $\mathbb{F}_q$. For $0 \le i \le 6$, let

$$\phi_i = \frac{1}{\sqrt{n}}(\phi_i(0), \phi_i(1), \ldots, \phi_i(n-1)) \in \mathbb{C}^n,$$

where

$$\phi_i(t) = (-1)^{\mathrm{Tr}(\gamma^{i+7t})}, \quad 0 \le t \le n-1.$$

Then $S = \{\phi_i : 0 \le i \le 6\}$ is an $(n, 7, \frac{2^{15}}{n})$ unit time-phase signal set, which falls into the fourth case of Lemma 2.

Acknowledgments The authors are very grateful to the two anonymous reviewers and the editor for their valuable comments and suggestions that improved the quality of this paper. The paper is supported by NNSF of China (No. 11171150) and Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-13-001).

References

1. Ding, C.: Complex codebooks from combinatorial designs. IEEE Trans. Inf. Theory **52**(9), 4229–4235 (2006)
2. Ding, C., Feng, K., Feng, R., Xiong, M., Zhang, A.: Unit time-phase signal sets: Bounds and constructions. Cryptogr. Commun. **5**, 209–227 (2013)
3. Ding, C., Feng, T.: A generic construction of complex codebooks meeting the Welch bound. IEEE Trans. Inf. Theory **53**(11), 4245–4250 (2007)
4. Ding, C., Feng, T.: Codebooks from almost difference sets. Des. Codes Cryptogr. **46**, 113–126 (2008)
5. Ding, C., Yin, J.: Signal sets from functions with optimum nonlinearity. IEEE Trans. Commun. **55**(5), 936–940 (2007)
6. Feng, K.: Algebraic Number Theory (in Chinese). Science Press, Beijing (2000)
7. Gurevich, S., Hadani, R., Sochen, N.: The finite harmonic oscillator and its applications to sequences, communication and radar. IEEE Trans. Inf. Theory **54**(9), 4239–4253 (2008)
8. Hu, L., Yue, Q.: Gauss periods and codebooks from generalized cyclotomic sets of order four. Des. Codes Cryptogr. **69**, 233–246 (2013)
9. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory, 2nd edn, GTM 84. Springer, New York (1990)
10. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley, Bostan (1983)
11. Schmidt, K.: Sequences families with low correlation derived from multiplicative and addtive characters. IEEE Trans. Inf. Theory **57**(4), 2291–2294 (2011)
12. Wang, Z., Gong, G.: New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts. IEEE Trans. Inf. Theory **57**(7), 4600–4611 (2011)
13. 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**(6), 3990–3998 (2013)
14. Yang, J., Xia, L.: Complete solving of explicit evaluation of Gauss sums in the index 2 case. Sci. China Math. **53**, 2525–2542 (2010)
15. Zhang, A., Feng, K.: Construction of cyclotomic codebooks nearly meeting the Welch bound. Des. Codes Cryptogr. **63**, 209–224 (2012)