

# New Sequences Design from Weil Representation with Low Two-Dimensional Correlation in Both Time and Phase Shifts

Zilong Wang<sup>\*1,2</sup> and Guang Gong<sup>2</sup>

<sup>1</sup> School of Mathematical Sciences, Peking University,  
Beijing, 100871, P.R.CHINA

<sup>2</sup> Department of Electrical and Computer Engineering, University of Waterloo  
Waterloo, Ontario N2L 3G1, CANADA

Email: wzlmath@gmail.com    ggong@calliope.uwaterloo.ca

## Abstract

For a given prime  $p$ , a new construction of families of the complex valued sequences of period  $p$  with efficient implementation is given by applying both multiplicative characters and additive characters of finite field  $\mathbb{F}_p$ . Such a signal set consists of  $p^2(p-2)$  time-shift distinct sequences, the magnitude of the two-dimensional autocorrelation function (i.e., the ambiguity function) in both time and phase of each sequence is upper bounded by  $2\sqrt{p}$  at any shift not equal to  $(0,0)$ , and the magnitude of the ambiguity function of any pair of phase-shift distinct sequences is upper bounded by  $4\sqrt{p}$ . Furthermore, the magnitude of their Fourier transform spectrum is less than or equal to 2. A proof is given through finding a simple elementary construction for the sequences constructed from the Weil representation by Gurevich, Hadani and Sochen. An open problem for directly establishing these assertions without involving the Weil representation is addressed.

**Index Terms.** Sequence, autocorrelation, cross correlation, ambiguity function, Fourier transform, and Weil representation.

## 1 Introduction

Sequence design for good correlation finds many important applications in various transmission systems in communication networks, and radar systems.

### A. Low Correlation

In code division multiple access (CDMA) applications of spread spectral communication, multiple users share a common channel. Each user is assigned a different spreading sequence (or spread code) for transmission. At an intended receiver, despreading (recovering the original data) is accomplished by the correlation of the received spread signal with a synchronized replica of the spreading sequence used to spread the information where the spreading sequences used by other users are treated as interference,

---

<sup>0\*</sup>Zilong Wang is currently a visiting Ph.D student at the Department of ECE in University of Waterloo from September 2008 to August 2009.

which is referred to as *multiple access interference*. This type of interference which is different from interference that arise in radio-frequency (RF) communication channels can be reduced by a proper design of a spreading signal set. The performance of a signal (or sequence) set used in a CDMA system is measured by the parameters  $L$ , the length or period of a sequence in the set,  $r$ , the number of the time-shift distinct sequences, and  $\rho$ , the maximum magnitude of the out-of-phase autocorrelation of any sequence and cross correlation of any pair of the sequences in the set. This is referred to as an  $(L, r, \rho)$  *signal set*. The trade-off of these three parameters are bounded by the Welch bound, established in 1974 by Welch [30]. The research for constructing good signal sets has been flourished in the literature. The reader is referring to [5] [1] for sequences with large alphabetic sizes, [20] [15] for  $\mathbb{Z}_4$  sequences, [8] [22] for interleaved sequences, and [26] [18] [9] in general, just listed a few here.

### B. Minimized Fourier Spectrum

The orthogonal frequency division multiplexing (OFDM) utilizes concept of parsing the input data into  $N$  symbol streams, and each of which in turn is used to modulate parallel, synchronous subcarriers. With an OFDM system having  $N$  subchannels, the symbol rate on each subcarrier is reduced by a factor of  $N$  relative to the symbol rate on a single carrier system that employs the entire bandwidth and transmits data at the same rate as OFDM. An OFDM signal can be implemented by computing an inverse Fourier transform and Fourier transform at the transmitter side and receiver side, respectively. A major problem with the multicarrier modulation in general and OFDM system in particular is the high peak-to-average power ratio (PAPR) that is inherent in the transmitted signal. PAPR is determined by the maximum magnitude of the Fourier transform spectrum of employed signals. A bound on PAPR through the magnitude of the Fourier transform is shown by Paterson and Tarokh in [23]. One way to achieve low PAPR is to employ Golay complementary sequences which is first shown by Davis and Jedwab in [7], for which a tremendous amount of work has been done along this line since then.

### C. Low Valued Ambiguity Functions

In radar or sonar applications, a sequence should be designed in such a way that the *ambiguity function* (the two-dimensional autocorrelation function in both time and frequency or equivalently phase, will be formally defined later), having the value of the length of the sequence at  $(0, 0)$ , and small values at any shift not  $(0, 0)$ . The low *ambiguity function* is required for determining the *range* (proportional to the time-shift) and *Doppler* (the velocity to or from the observer, proportional to the frequency shift) of a target. The sequences with low ambiguity function can be achieved by Costas arrays, which yield the so-called *ideal* or *thumb-tack* ambiguity function (for which it has only the values 0 or 1 at any shift not  $(0, 0)$ ) [6], [10].

A question that we would like to ask is as follows.

**Problem.** Does there exist any construction for a signal set which simultaneously satisfies the require-

ments that arise from the above three transmission scenarios, i.e., having low correlation, low PAPR, and low ambiguity function, but with moderate implementation cost and large size?

It is anticipated that employing those sequences will improve the performance of communication systems with multi-carrier CDMA transmission [24], radar networks, and transmission systems in future cognitive radio networks [25].

In this paper, we provide a solution to the above addressed problem using both multiplicative characters and additive characters of the finite field  $\mathbb{F}_p$  where  $p$  is a prime. It is interesting to observe that to date, almost all the sequences with low correlation or low PAPR in the literature are related to use additive characters of the finite field  $\mathbb{F}_p$  or  $\mathbb{F}_{p^n}$  or Galois rings together with functions (with trace representation for  $n > 1$ ) mapping from those fields or rings to the residue rings modulo  $l$ .

Recently, researchers look at some other mathematical tools, such as the group representation theory for sequence design. For example, mutually unbiased bases has been discussed by Howe in [17], sequences constructed from the Heisenberg representation have been investigated by Howard, Calderbank, and Moranin in [16], and sequences from the Weil representation, which referred to as a finite oscillator system  $\mathfrak{S}$ , was introduced by Gurevich, Hadani, and Sochen in [11] [13].

Sequences from the Heisenberg representation are turned out similarly as extended Chu sequences [5] by phase-shift, which are complex valued sequences with period  $p$ . After normalized by the energy, the values of their ambiguity functions (will be precisely defined in the next section) is bounded by  $\frac{1}{\sqrt{p}}$  for most sequences except for some special case. While the sequences from the Weil representation, which will be introduced later, have the desired properties in the above mentioned three application scenarios, but having very complicated form. Gurevich, Hadani, and Sochen investigated how to implement their sequences in [13] in terms of an algorithm. The goal of this paper is to find a simple elementary construction for the finite oscillator system, then drop those having heavy computations for implementation, and extend the subset with fast implementation to a larger set for keeping a similar size as the original set.

The rest of the paper is organized as follows. In Section 2, we introduce some basic concepts and notations in this paper. In Section 3, we present our new constructions and the main results. In Section 4, we first introduce definitions of the Heisenberg and Weil representations, then we introduce the finite oscillator system constructed by Gurevich, Hadani and Sochen in [11] [13]. We show a simple elementary construction for this finite oscillator system, and present the proof for the new constructions in Section 5. Comparisons of the new constructions with some known constructions are made in Section 6. Section 7 is for concluding remarks and addressing some open problems.

## 2 Basic Concepts and Definitions

In this section, we introduce some basic concepts and notations which are frequently used in this paper. For a given prime  $p$ , let  $\theta$  and  $\eta$  denote the  $(p-1)$ th and  $p$ th primitive roots of unity in complex field respectively, i.e.,

$$\theta = \exp\left(\frac{2\pi i}{p-1}\right) \quad \text{and} \quad \eta = \exp\left(\frac{2\pi i}{p}\right).$$

We denote  $\mathbb{F}_p$  as the finite field with  $p$  elements, and  $\mathbb{F}_p^*$  as the multiplicative group of  $\mathbb{F}_p$  with a generator  $a$ . Then for every element  $b \in \mathbb{F}_p^*$ , there exist  $i$  with  $0 \leq i \leq p-2$ , such that  $b = a^i$ . In other words,  $i = \log_a b$ . We set  $\theta^{\log_a 0} = 0$  throughout this paper.

Every sequence with period  $p$  can be denoted by  $\varphi = (\varphi(0), \varphi(1), \dots, \varphi(p-1))$ , and also considered as a vector in the Hilbert space  $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$  with the inner product given by the standard formula:  $\langle \varphi, \psi \rangle = \sum_{i \in \mathbb{F}_p} \varphi(i) \overline{\psi(i)}$  where  $\bar{x}$  is the complex conjugate of  $x$ . We denote  $U(\mathcal{H})$  as the group of unitary operators on  $\mathcal{H}$ . Let  $L_t, M_w$  and  $F$  be the unitary operators of the time-shift, phase-shift and Fourier transform respectively, which are defined as follows

$$L_t[\varphi](i) = \varphi(i+t) \quad M_w[\varphi](i) = \eta^{wi} \varphi(i) \quad \text{and} \quad F[\varphi](j) = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{F}_p} \eta^{ji} \varphi(i), \quad \varphi \in \mathcal{H}. \quad (1)$$

We also use the notation  $\widehat{\varphi}$  for  $F[\varphi]$  for simplicity. If  $\psi = L_t \varphi$  or  $\psi = M_w \varphi$ , then we say that  $\varphi$  and  $\psi$  are *time-shift equivalent* or *phase-shift equivalent*. Otherwise, they are *time-shift distinct* or *phase-shift distinct*.

We denote  $C_\varphi(t)$  and  $C_{\varphi, \psi}(t)$  their respective *autocorrelation* and *cross correlation* functions, which are defined by

$$C_\varphi(t) = \sum_{i \in \mathbb{F}_p} \varphi(i) \overline{\varphi(i+t)} \quad \text{and} \quad C_{\varphi, \psi}(t) = \sum_{i \in \mathbb{F}_p} \varphi(i) \overline{\psi(i+t)}. \quad (2)$$

**Definition 1** Let  $S \subset \mathcal{H}$ . We say that  $S$  is a  $(p, r, \sigma, \rho)$  signal set if each sequence in  $S$  has period  $p$ , there are  $r$  time-shift distinct sequences in  $S$ , and the maximum magnitude of out-of-phase autocorrelation values and cross correlation values are upper bounded by  $\sigma$  and  $\rho$  respectively, i.e.,

$$|C_\varphi(t)| \leq \sigma, \quad t \neq 0, \forall \varphi \in S \quad \text{and} \quad (3)$$

$$|C_{\varphi, \psi}(t)| \leq \rho, \quad \forall t \in \mathbb{F}_p, \forall \varphi \neq \psi \in S. \quad (4)$$

In this paper, we also say that auto and cross correlation of  $S$  is upper bounded by  $\sigma$  and  $\rho$  respectively.

The *auto and cross ambiguity functions* of sequences are defined as two-dimensional autocorrelation and cross correlation function in both time and phase which are given by

$$A_\varphi(t, w) = \langle \varphi, M_w L_t \varphi \rangle \quad \text{and} \quad A_{\varphi, \psi}(t, w) = \langle \varphi, M_w L_t \psi \rangle. \quad (5)$$

Together with the definitions of the auto and cross correlation functions, we know that they are equal to their respective auto and cross ambiguity functions for the case  $w = 0$ .

### Parseval Formulae

$$\langle \widehat{\varphi}, L_t \widehat{\psi} \rangle = \langle \varphi, M_{-t} \psi \rangle \quad \text{and} \quad \langle \widehat{\varphi}, M_w \widehat{\psi} \rangle = \langle \varphi, L_t \psi \rangle. \quad (6)$$

According to the definition of the auto and cross ambiguity functions and the Parseval formulae, we have the following assertions.

**Property 1** *Let  $S$  be a signal set with  $r$  time-shift distinct sequences, and the auto and cross ambiguity functions satisfy the following bounds. For  $\forall \varphi, \psi \in S$ ,*

$$\begin{aligned} |A_\varphi(t, w)| &\leq \sigma \quad \text{for } (t, w) \neq (0, 0) \\ |A_{\varphi, \psi}(t, w)| &\leq \rho \quad \text{if } \varphi \text{ and } \psi \text{ are phase-shift distinct.} \end{aligned} \quad (7)$$

*Then  $(\sigma, \rho)$  are also the upper bounds of the auto and cross correlation functions, and as well as the auto and cross ambiguity functions of the Fourier transform of sequences in  $S$ , i.e.,*

$$\begin{aligned} |C_\varphi(t)| &\leq \sigma \quad \text{for } t \neq 0 \\ |C_{\varphi, \psi}(t)| &\leq \rho \quad \text{for } \varphi \neq \psi \end{aligned} \quad (8)$$

and

$$\begin{aligned} |A_{\widehat{\varphi}}(t, w)| &\leq \sigma \quad \text{for } (t, w) \neq (0, 0) \\ |A_{\widehat{\varphi}, \widehat{\psi}}(t, w)| &\leq \rho \quad \text{if } \varphi \text{ and } \psi \text{ are phase-shift distinct.} \end{aligned} \quad (9)$$

**Remark 1** If  $S$  consists of both time-shift and phase-shift distinct sequences, the conditions (7) and (9) are replaced by  $\varphi \neq \psi$ .

**Definition 2** *If  $S$  is a signal set consisting of  $r$  time-shift distinct sequences with period  $p$ , and the auto and cross ambiguity functions are upper bounded by (7) in Property 1, then we say that  $S$  is a  $(p, r, \sigma, \rho)$  ambiguity signal set.*

From Property 1, a  $(p, r, \sigma, \rho)$  ambiguity signal set  $S$  is also a  $(p, r, \sigma, \rho)$  signal set, and the auto and cross ambiguity functions of the Fourier transform of any sequence in  $S$  are also upper bounded by  $\sigma$  and  $\rho$ .

Thus, in this paper, we investigate the auto and cross ambiguity functions of the sequences, which are stronger requirements than just the auto and cross correlation functions of the sequences.

**Remark 2** All the definitions and notations are stated for the sequences with period  $p$  in this section. However, they are valid for the sequences with period  $n$  when  $p$  and  $\mathbb{F}_p$  are replaced by  $n$  and  $\mathbb{Z}_n$  respectively.

### 3 Main Results

**Construction A.** Let  $a$  be a generator of  $\mathbb{F}_p^*$ . For a given prime  $p$  ( $p \geq 5$ ),  $n \in \mathbb{Z}$  and  $0 \leq n < p^2(p-2)$ ,  $n$  has a  $p$ -adic decomposition given by:  $n = (x-1)p^2 + yp + z$  where  $1 \leq x \leq p-2, 0 \leq y, z \leq p-1$ . Let  $\varphi_n = \{\varphi_n(i)\}$  be a sequence in  $\mathcal{H}$  whose elements are defined as

$$\varphi_n(i) = \theta^{x \cdot \log_a i} \cdot \eta^{yi^2 + zi}, \quad 0 \leq i \leq p-1$$

and

$$\Omega = \{\varphi_n : 0 \leq n < p^2(p-2)\}.$$

**Theorem 1** *The sequences in  $\Omega$  satisfy the following properties.*

- (a) *The elements of each sequence  $\varphi$  in  $\Omega$  lie on the unit circle in the complex plane except  $\varphi(0) = 0$ .*
- (b) *Fourier transform of  $\varphi$  is bounded by  $|\widehat{\varphi}(i)| \leq 2, \forall i \in \mathbb{F}_p$ .*
- (c)  *$\Omega$  is a  $(p, p^2(p-2), 2\sqrt{p}, 4\sqrt{p})$  ambiguity signal set, i.e., for  $\forall \varphi, \psi \in \Omega$*

$$\begin{aligned} |A_\varphi(t, w)| &\leq 2\sqrt{p} && \text{for } (t, w) \neq (0, 0), \\ |A_{\varphi, \psi}(t, w)| &\leq 4\sqrt{p} && \text{if } \varphi \text{ and } \psi \text{ are phase-shift distinct.} \end{aligned} \quad (10)$$

**Example 1** For  $p = 5$ ,  $a = 2$  is a generator of  $\mathbb{F}_5$ , the elements of the sequences  $\varphi_x, \varphi_y$ , and  $\varphi_z$  are defined as  $\varphi_x(i) = \theta^{x \cdot \log_a i}$ ,  $\varphi_y(i) = \eta^{yi^2}$ , and  $\varphi_z(i) = \eta^{zi}$  respectively, which are given as follows.

$x$	$\varphi_x(i) = \theta^{x \cdot \log_a i}$	$y$	$\varphi_y(i) = \eta^{yi^2}$	$z$	$\varphi_z(i) = \eta^{zi}$
		0	{1, 1, 1, 1, 1}	0	{1, 1, 1, 1, 1}
1	{0, 1, $\theta$ , $\theta^3$ , $\theta^2$ }	1	{1, $\eta$ , $\eta^4$ , $\eta^4$ , $\eta$ }	1	{1, $\eta$ , $\eta^2$ , $\eta^3$ , $\eta^4$ }
2	{0, 1, $\theta^2$ , $\theta^2$ , 1}	2	{1, $\eta^2$ , $\eta^3$ , $\eta^3$ , $\eta^2$ }	2	{1, $\eta^2$ , $\eta^4$ , $\eta$ , $\eta^3$ }
3	{0, 1, $\theta^3$ , $\theta$ , $\theta^2$ }	3	{1, $\eta^3$ , $\eta^2$ , $\eta^2$ , $\eta^3$ }	3	{1, $\eta^3$ , $\eta$ , $\eta^4$ , $\eta^2$ }
		4	{1, $\eta^4$ , $\eta$ , $\eta$ , $\eta^4$ }	4	{1, $\eta^4$ , $\eta^3$ , $\eta^2$ , $\eta$ }

Then the elements of each sequence in the signal set  $\Omega$  are constructed by term-by-term products of the elements of  $\varphi_x, \varphi_y$ , and  $\varphi_z$ . The first three sequences and last two sequences are given as follows.

$$\begin{aligned}
\varphi_0 &= \varphi_{1,0,0} = (0, 1, \theta, \theta^3, \theta^2), \\
\varphi_1 &= \varphi_{1,0,1} = (0, \eta, \theta\eta^2, \theta^3\eta^3, \theta^2\eta^4), \\
\varphi_2 &= \varphi_{1,0,2} = (0, \eta^2, \theta\eta^4, \theta^3\eta, \theta^2\eta^3), \\
&\vdots \\
\varphi_{73} &= \varphi_{3,4,3} = (0, \eta^2, \theta^3\eta^2, \theta, \theta^2\eta), \\
\varphi_{74} &= \varphi_{3,4,4} = (0, \eta^3, \theta^3\eta^4, \theta\eta^3, \theta^2).
\end{aligned}$$

In order to prove the assertions of Theorem 1, we use some results from the group representation theory. Note that the sequences in *finite oscillator system*  $\mathfrak{S}$ , which will be introduced in next section, satisfy the properties in Theory 1, but have a very complicated form which cannot be implemented efficiently. There are two types of sequences in the set of the finite oscillator system  $\mathfrak{S}$ . One is from the split case, denoted as  $\mathfrak{S}^s$ , and the other from non-split case, denoted as  $\mathfrak{S}^{ns}$ . In other words,

$$\mathfrak{S} = \mathfrak{S}^s \cup \mathfrak{S}^{ns}.$$

Surprisingly, we found a simple elementary construction for the sequences in  $\mathfrak{S}^s$ , which is presented as follows.

**Construction B.** Let

$$\Omega^* = \varphi_{x,y,b} = \{\varphi_{x,y,b} \mid 1 \leq x \leq p-2, 0 \leq y \leq p-1, 0 \leq b \leq (p-1)/2\}$$

where  $\varphi_{x,y,b} = \{\varphi_{x,y,b}(i)\}$  is a normalized sequence with period  $p$  whose elements are given by

$$\varphi_{x,y,0}(i) = \frac{1}{\sqrt{p-1}} \theta^{x \cdot \log_a i} \eta^{yi^2}$$

and

$$\varphi_{x,y,b}(i) = \frac{\eta^{yi^2}}{\sqrt{p(p-1)}} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-(2b)^{-1}(j-i)^2} \text{ for } b \neq 0.$$

**Theorem 2**  $\mathfrak{S}^s = \Omega^*$ .

We now extend the signal set  $\mathfrak{S}$  to a new signal set  $\overline{\mathfrak{S}}$  which is given by

$$\overline{\mathfrak{S}} = \overline{\mathfrak{S}}^s \cup \overline{\mathfrak{S}}^{ns} \tag{11}$$

where

$$\overline{\mathfrak{S}}^s = \{M_w \varphi \mid \varphi \in \mathfrak{S}^s\} \text{ and } \overline{\mathfrak{S}}^{ns} = \{M_w \varphi \mid \varphi \in \mathfrak{S}^{ns}\}. \tag{12}$$

**Theorem 3** *The signal set  $\overline{\mathfrak{S}}$  is a  $(p, p^4, \frac{2}{\sqrt{p}}, \frac{4}{\sqrt{p}})$  ambiguity signal set. Furthermore, for  $\forall \varphi \in \overline{\mathfrak{S}}$ , their respective magnitudes of the elements in  $\varphi$  and  $\widehat{\varphi}$ , the Fourier transform of  $\varphi$ , are bounded by  $|\varphi(i)| \leq \frac{2}{\sqrt{p}}$  and  $|\widehat{\varphi}(i)| \leq \frac{2}{\sqrt{p}}$  for any  $i \in \mathbb{F}_p$ .*

From the constructions A, B and (12), we see that  $\Omega$  is a subset of  $\overline{\mathfrak{S}}$  (up to multiplication by  $\sqrt{p-1}$ ). In [13], the authors have mentioned that  $\mathfrak{S}$  can be enlarged by applying both time-shift and phase-shift operators to the sequences in  $\mathfrak{S}$ . They also determined the inner product of any two sequences in the resulting signal set. However, applying time-shift operators results only time-shift equivalent sequences. Thus, we only consider the extension by applying phase-shift operators to  $\mathfrak{S}$ . In the rest of the sections, we first prove Theorem 2, and then complete the proof for Theorem 3. In order to do so, in the next section, we introduce some basic concepts and definitions on the Heisenberg and Weil representations, and then introduce the oscillator system signal set.

## 4 The Heisenberg and Weil Representations and Finite Oscillator System

### 4.1 The Heisenberg Representation

Let  $(V, \omega)$  be a two-dimensional symplectic vector space over the finite field  $\mathbb{F}_p$ . For  $\forall (t_i, w_i) \in V = \mathbb{F}_p \times \mathbb{F}_p$  ( $i = 1, 2$ ), the symplectic form  $\omega$  is given by

$$\omega((t_1, w_1), (t_2, w_2)) = t_1 w_2 - t_2 w_1.$$

Considering  $V$  as an Abelian group, it admits a non-trivial central extension called the *Heisenberg group*  $H$  ( $p \neq 2$ ). The group  $H$  can be presented as  $H = V \times F_p$  with the multiplication given by

$$(t_1, w_1, z_1) \cdot (t_2, w_2, z_2) = (t_1 + t_2, w_1 + w_2, z_1 + z_2 + 2^{-1}\omega((t_1, w_1), (t_2, w_2))).$$

It's easy to verify the center of  $H$  is  $Z = Z(H) = \{(0, 0, z) : z \in \mathbb{F}_p\}$ .

One important property of the Heisenberg group  $H$  is, for a given non-trivial one dimensional representation  $\phi$  of center  $Z$ , it admits a unique irreducible representation of  $H$ . The precise statement is as follows:

**Theorem 4** *(Stone-Von Neuman) Up to isomorphism, there exists a unique irreducible unitary representation  $\pi : H \rightarrow U(\mathcal{H})$  with central character  $\phi$ , that is,  $\pi|_Z = \phi \cdot Id_{\mathcal{H}}$ .*

The representation  $\pi$  which appears in the above Theorem will be called the *Heisenberg representation*. In this paper, we take one dimensional representation of  $Z$  as  $\phi((0, 0, z)) = \eta^z$ . Then the unique

irreducible unitary representation  $\pi$  corresponding to  $\phi$  has the following formula

$$\pi(t, w, z)[\varphi](i) = \eta^{2^{-1}tw+z+wi}\varphi(i+t) \quad (13)$$

for  $\forall \varphi \in \mathbb{C}(\mathbb{F}_p)$ ,  $(t, w, z) \in H$ . Consequently, we have

$$\pi(t, 0, 0)[\varphi](i) = \varphi(i+t)$$

$$\pi(0, w, 0)[\varphi](i) = \eta^{wi}\varphi(i)$$

$$\pi(0, 0, z)[\varphi](i) = \eta^z\varphi(i).$$

Thus  $\pi(t, 0, 0), \pi(0, w, 0)$  are equal to the unitary operators time-shift  $L_t$  and phase-shift  $M_w$ , respectively, defined in (1).

## 4.2 The Weil Representation

The symplectic group  $Sp = Sp(V, \omega)$ , which is isomorphic to  $SL_2(\mathbb{F}_p)$ , acts by automorphism of  $H$

through its action on the  $V$ -coordinate, i.e., for  $\forall (t, w, z) \in H$  and a matrix  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$ ,

$g$  acts on  $H$  is defined as

$$g \cdot (t, w, z) = (at + bw, ct + dw, z). \quad (14)$$

Due to Weil [29], a projective unitary representation  $\tilde{\rho} : Sp \rightarrow PGL(\mathcal{H})$  is constructed as follows. Considering the Heisenberg representation  $\pi : H \rightarrow U(\mathcal{H})$  and  $\forall g \in Sp$ , a new representation is define as:  $\pi^g : H \rightarrow U(\mathcal{H})$  by  $\pi^g(h) = \pi(g(h))$ . Because both  $\pi$  and  $\pi^g$  have the same central character  $\phi$ , they are isomorphic by Theorem 4. By Schur's Lemma [27],  $Hom_H(\pi, \pi^g) \cong \mathbb{C}^*$ , so there exist a projective representation  $\tilde{\rho} : Sp \rightarrow PGL(\mathcal{H})$ . This projective representation  $\tilde{\rho}$  is characterized by the formula:

$$\tilde{\rho}(g)\pi(h)\tilde{\rho}(g^{-1}) = \pi(g(h)) \quad (15)$$

for every  $g \in Sp$  and  $h \in H$ . A more delicate statement is that there exists a unique lifting of  $\tilde{\rho}$  into a unitary representation.

**Theorem 5** *The projective Weil representation uniquely lifts to a unitary representation*

$$\rho : Sp \rightarrow U(\mathcal{H})$$

that satisfies equation (15).

The existence of  $\rho$  follows from the fact [2] that any projective representation of  $SL_2(\mathbb{F}_p)$  can be lifted to an honest representation, while the uniqueness of  $\rho$  follows from the fact [14] that the group  $SL_2(\mathbb{F}_p)$  has no non-trivial characters when  $p \neq 3$ .

Note that  $SL_2(\mathbb{F}_p)$  can be generated by  $g_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ ,  $g_b = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ ,  $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  where  $a \in \mathbb{F}_p^*$  and  $b \in \mathbb{F}_p$ . the formulae of Weil representation for  $g_a, g_b, w$  are given in [12] as follows

$$\rho(g_a)[\varphi](i) = \sigma(a)\varphi(a^{-1}i) \quad (16)$$

$$\rho(g_b)[\varphi](i) = \eta^{-2^{-1}bi^2} \varphi(i) \quad (17)$$

$$\rho(w)[\varphi](j) = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{F}_p} \eta^{ji} \varphi(i) \quad (18)$$

where  $\sigma : \mathbb{F}_p^* \rightarrow \{\pm 1\}$  is the Legendre character, i.e.,  $\sigma(a) = a^{\frac{p-1}{2}}$  in  $\mathbb{F}_p$ . The above formulae in [11] have some mistakes, while the correct formulae are given in [12].

Obviously,  $\rho(w)$  is equal to the discrete Fourier transform  $F$  defined in (1). We denote  $\rho(g_a) = S_a, \rho(g_b) = N_b, \rho(w) = F$  for convenience. Then for  $\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$ ,

If  $b \neq 0$ ,

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ (ad-1)b^{-1} & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ bd & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ab^{-1} & 1 \end{pmatrix}.$$

Then the Weil representation of  $g$  is given by

$$\rho(g) = S_b \circ N_{bd} \circ F \circ N_{ab^{-1}}. \quad (19)$$

If  $b = 0$ , then

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ac & 1 \end{pmatrix}.$$

Hence the Weil representation of  $g$  is as follows

$$\rho(g) = S_a \circ N_{ac}. \quad (20)$$

For more details about the Heisenberg and weil representations, please see [11] [16] [17].

### 4.3 The Finite Oscillator System

In this subsection, we introduce the main results of [11].

#### A. Maximal Algebraic Tori

The commutative subgroups in  $SL_2(\mathbb{F}_p)$  that we consider are called *maximal algebraic tori* [4]. A maximal algebraic torus in  $SL_2(\mathbb{F}_p)$  is a maximal commutative subgroup which becomes diagonalizable over the field or quadratic extension of the field. One standard example of a maximal algebraic torus in  $SL_2(\mathbb{F}_p)$  is the standard diagonal torus

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_p^* \right\}.$$

Up to conjugation, there are two classes of the maximal algebraic tori in  $SL_2(\mathbb{F}_p)$ . The first class, called *split tori*, consists of those tori which are diagonalizable over  $\mathbb{F}_p$ . Every split torus  $T$  is conjugated to the standard diagonal torus  $A$ , i.e., there exists an element  $g \in SL_2(\mathbb{F}_p)$  such that  $g \cdot T \cdot g^{-1} = A$ . The second class, called *non-split tori*, consists of those tori which are not diagonalizable over  $\mathbb{F}_p$ , but become diagonalizable over the quadratic extension  $\mathbb{F}_{p^2}$ . In fact, a split torus is a cyclic subgroup of  $SL_2(\mathbb{F}_p)$  with order  $p - 1$ , while a non-split torus is a cyclic subgroup of  $SL_2(\mathbb{F}_p)$  with order  $p + 1$ .

All split (non-split) tori are conjugated to one another, so the number of split (non-split) tori is the number of elements in the coset space  $SL_2(\mathbb{F}_p)/N$  ( $SL_2(\mathbb{F}_p)/M$ ) (see [28] for basics of group theory), where  $N$  ( $M$ ) is the normalizer group of  $A$  (some non-split torus). Thus

$$\#(SL_2(\mathbb{F}_p)/N) = \frac{1}{2}p(p+1) \quad \text{and} \quad \#(SL_2(\mathbb{F}_p)/M) = \frac{1}{2}p(p-1). \quad (21)$$

**Remark 3** It is a mistake in [11] that the number of non-split tori is equal to  $p(p-1)$ . A direct calculation shows that it should be equal to  $\frac{1}{2}p(p-1)$ .

#### B. Decomposition of Weil representation Associated with Maximal Tori

Because every maximal torus  $T \in SL_2(\mathbb{F}_p)$  is a cyclic group, restricting the Weil representation to  $T$ :  $\rho|_T : T \rightarrow U(\mathcal{H})$ , we obtain a one dimensional subrepresentation decomposition of  $\rho|_T$  corresponding to an orthogonal decomposition of  $\mathcal{H}$  (see [27] for basics of group representation theory).

$$\rho|_T = \bigoplus_{\chi \in \Lambda_T} \chi \quad \text{and} \quad \mathcal{H} = \bigoplus_{\chi \in \Lambda_T} \mathcal{H}_\chi \quad (22)$$

where  $\Lambda_T$  is a collection of all the one dimensional subrepresentation (character)  $\chi : T \rightarrow \mathbb{C}$  in the decomposition of weil representation restricted on the torus  $T$ .

The decomposition (22) depends on the type of  $T$ . In the case where  $T$  is a split torus,  $\chi$  is the character given by  $\chi : \mathbb{Z}_{p-1} \rightarrow \mathbb{C}$ . We have  $\dim \mathcal{H}_\chi = 1$  unless  $\chi = \sigma$  where  $\sigma$  is the Legendre character of  $T$ , and  $\dim \mathcal{H}_\sigma = 2$ . In the case where  $T$  is a non-split torus,  $\chi$  is the character given by  $\chi : \mathbb{Z}_{p+1} \rightarrow \mathbb{C}$ . There is only one character which does not appear in the decomposition. For the other  $p$  characters  $\chi$  which appear in the decomposition, we have  $\dim \mathcal{H}_\chi = 1$ .

An efficient way to specify the decomposition (22) is by choosing a generator  $t \in T$ , the character is generated by the eigenvalue  $\chi(t)$  of linear operator  $\rho(t)$ , and the character space  $\mathcal{H}_\chi$  naturally corresponds to the eigenspace of  $\chi(t)$ .

### C. Sequences Associated with Finite Oscillator System

For a given torus  $T$ , choosing a vector  $\varphi_\chi \in \mathcal{H}_\chi$  of unit norm for each character  $\chi \in \Lambda_T$ , we obtain a collection of orthonormal vectors

$$\mathcal{B}_T = \{\varphi_\chi : \chi \in \Lambda_T, \chi \neq \sigma \text{ if } T \text{ split}\}. \quad (23)$$

Considering the union of all these collection, we obtain all the sequences in finite oscillator system

$$\mathfrak{S} = \{\varphi \in \mathcal{B}_T : T \subset SL_2(\mathbb{F}_p)\}. \quad (24)$$

$\mathfrak{S}$  is naturally separated into two sub-system  $\mathfrak{S}^s$  and  $\mathfrak{S}^{ns}$  which correspond to the split tori and the non-split tori respectively. The sub-system  $\mathfrak{S}^s$  ( $\mathfrak{S}^{ns}$ ) consists of the union of  $B_T$ , where  $T$  runs through all the split tori (non-split tori) in  $SL_2(\mathbb{F}_p)$ . Altogether there are  $\frac{1}{2}p(p+1)$  ( $\frac{1}{2}p(p-1)$ ) tori where each consisting of  $p-2$  ( $p$ ) orthonormal sequences. Hence

$$\#\mathfrak{S}^s = \frac{1}{2}p(p+1)(p-2) \quad \text{and} \quad \#\mathfrak{S}^{ns} = \frac{1}{2}p^2(p-1). \quad (25)$$

**Theorem 6** *Sequences in the set  $\mathfrak{S}$  satisfy the following properties. For  $\forall \varphi, \psi \in \mathfrak{S}$  and  $(t, w) \in V = \mathbb{F}_p \times \mathbb{F}_p$ ,*

(a) *Auto and cross ambiguity functions are upper bounded as*

$$A_{\varphi, \psi}(t, w) \leq \begin{cases} \frac{2}{\sqrt{p}}, & \varphi = \psi, (t, w) \neq (0, 0) \\ \frac{4}{\sqrt{p}}, & \varphi \neq \psi. \end{cases}$$

(b) *Supremum of  $\varphi$  is given by  $\max\{|\varphi(i)| : i \in \mathbb{F}_p\} \leq \frac{2}{\sqrt{p}}$ .*

(c) *For every sequences  $\varphi \in \mathfrak{S}$ , its Fourier transform  $\hat{\varphi}$  is (up to multiplication by a unitary scalar) also in  $\mathfrak{S}$ .*

**Remark 4** The bounds of auto and cross ambiguity function in Theorem 6 are not precise. In fact, for the split case, the auto and cross ambiguity function are upper bounded by  $\frac{2\sqrt{p}}{p-1}$  and  $\frac{4\sqrt{p}}{p-1}$  respectively, while for the non-split case, they are upper bounded by  $\frac{2\sqrt{p}}{p+1}$  and  $\frac{4\sqrt{p}}{p+1}$  respectively, and the cross ambiguity function between one sequence from the split case and the other from the non-split case is bounded by  $\frac{4\sqrt{p}}{\sqrt{(p-1)(p+1)}}$ . For simplicity, approximate bounds which are as same as Theorem 6 are adopted in [11] expect its proof part. We also adopt approximate bounds in Theorem 6 and Theorem 3 in this paper, so the reader should keep this remark in mind for the proof of Theorem 3 later.

## 5 Proof of Main results

There are three steps to establish the sequences in the split case of finite oscillator system  $\mathfrak{S}^s$ .

Step 1: Compute the generator  $g_a$  for the standard torus  $A$  and  $\mathcal{B}_A$ . In other words, the collection of the eigenvectors of  $\rho(g_a)$  which are not corresponding to eigenvalue  $-1$ .

Step 2: Compute all the representative elements  $g$  in the coset  $\{gN(A) : g \in SL_2(\mathbb{F}_p)\}$  where  $N(A)$  is the normalizer group of  $A$ .

Step 3: Compute all the sequences  $\rho(g)\varphi$  where  $g$  is representative element presented in Step 2 and  $\varphi \in \mathcal{B}_A$  calculated in Step 1.

Considering  $\{\delta_i : i \in \mathbb{F}_p\}$  is the orthonormal basis of Hilbert space  $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ , where  $\delta_i$  is defined as  $\delta_i(j) = \delta_{ij}$  for  $\forall j \in \mathbb{F}_p$ , every sequence  $\varphi = \{\varphi(i)\}$  with period  $p$  can be written as the function form  $\varphi = \sum_{i=0}^{p-1} \varphi(i)\delta_i$ . Recall  $SL_2(\mathbb{F}_p)$  can be generated by  $g_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ ,  $g_b = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$  and  $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  where  $a \in \mathbb{F}_p^*$  and  $b \in \mathbb{F}_p$ , the Weil representation(16)(17)(18) of  $g_a, g_b, w$  can be rewritten as follows

$$\rho(g_a)\delta_i = S_a\delta_i = \sigma(a)\delta_{ai} \quad (26)$$

$$\rho(g_b)\delta_i = N_b\delta_i = \eta^{-2^{-1}bi^2}\delta_i \quad (27)$$

$$\rho(w)\delta_j = F\delta_j = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{F}_p} \eta^{ji}\delta_i. \quad (28)$$

**Lemma 1** Let  $a$  be a generator of  $\mathbb{F}_p^*$ , and  $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_p^* \right\}$  be the standard diagonal torus, then

$$\mathcal{B}_A = \left\{ \varphi_x = \frac{1}{\sqrt{p-1}} \sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} \delta_i : 1 \leq x \leq p-2 \right\}.$$

Proof: The set  $\mathcal{B}_A$  is a collection of  $\varphi_\chi$  with unit norm where  $\varphi_\chi \in \mathcal{H}_\chi$  for every character  $\chi \neq \sigma$ . In other words, the set  $\mathcal{B}_A$  is a collection of unit eigenvector (not belong to eigenvalue  $-1$ ) of  $\rho(g_a)$  where  $g_a$  is a generator of Torus  $A$ .

Let  $a$  be a generator of  $\mathbb{F}_p^*$ , then  $g_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$  is a generator of torus  $A$ . From (26), we have

$$\rho(g_a)\delta_i = \sigma(a)\delta_{ai} = -\delta_{ai}.$$

The eigenfunction of  $\rho(g_a)$  is  $(x+1)(x^{p-1}-1)$ , so the eigenvalues of  $\rho(g_a)$  are  $-1, \theta^0, \theta^1, \theta^2, \dots, \theta^{p-2}$ . Obviously,  $-1 = \theta^{\frac{p-1}{2}}$  occurs twice in the eigenvalues set. We assert that  $\sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)\log_a i} \delta_i$  is the eigenvector associated to the eigenvalue  $\theta^j$  ( $0 \leq j < p-2$ ), and it can be verified as follows

$$\begin{aligned} \rho(g_a)\left(\sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)\log_a i} \delta_i\right) &= -\sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)\log_a i} \delta_{ai} \\ &= -\sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)\log_a (a^{-1}i)} \delta_i \\ &= \theta^{\frac{p-1}{2}} \sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)(\log_a i-1)} \delta_i \\ &= \theta^{\frac{p-1}{2}} \theta^j \sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)\log_a i} \delta_i \\ &= \theta^j \sum_{i=1}^{p-1} \theta^{(\frac{p-1}{2}-j)\log_a i} \delta_i. \end{aligned}$$

Let  $x = \frac{p-1}{2} - j$ , then  $\{\sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} \delta_i \mid (1 \leq x \leq p-2)\}$  is the set of the eigenvectors corresponds to all the eigenvalues not equal to  $-1$ . By normalizing the eigenvectors, we complete the proof.  $\square$

**Lemma 2** Let  $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_p^* \right\}$  be the standard diagonal torus, then

$$R = \left\{ \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} : 0 \leq b \leq \frac{p-1}{2}, c \in \mathbb{F}_p \right\}$$

is a set which contains all the representative elements of the coset  $\{gN(A) : g \in SL_2(\mathbb{F}_p)\}$  where  $N(A)$  is the normalizer group of  $A$ .

Proof: Denote  $B = \left\{ \begin{pmatrix} 0 & -b \\ b^{-1} & 0 \end{pmatrix} : b \in \mathbb{F}_p^* \right\}$ , then it's not hard to verify

$$N(A) = \{g : gAg^{-1} = A, g \in SL_2(\mathbb{F}_p)\} = AB.$$

Thus every representative element  $g$  can be written as the form

$$g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} \quad b, c \in \mathbb{F}_p$$

and  $g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}, g' = \begin{pmatrix} 1 & b' \\ c' & 1+b'c' \end{pmatrix}$  in the same coset, i.e.,  $g^{-1}g' \in N(A)$ , if and only if

$$\begin{aligned} \begin{pmatrix} 1 & b' \\ c' & 1+b'c' \end{pmatrix} &= \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} \begin{pmatrix} 0 & -b \\ b^{-1} & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -b \\ b^{-1}+c & -bc \end{pmatrix} \\ &= \begin{pmatrix} 1 & -b \\ b^{-1}+c & 1+(-b)(b^{-1}+c) \end{pmatrix}, \end{aligned}$$

if and only if  $b' = -b$  and  $c' = b^{-1} + c$ . So  $R$  contains all the representative elements in the coset  $\{gN(A) : g \in SL_2(\mathbb{F}_p)\}$ .  $\square$

**Lemma 3** *There are two types vectors in  $\mathfrak{S}^s$ .*

*The first type is*

$$\varphi_{x,y,0} = \frac{1}{\sqrt{p-1}} \sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} \eta^{y i^2} \delta_i$$

where  $1 \leq x \leq p-2, 0 \leq y \leq p-1$ .

*The second type is*

$$\varphi_{x,y,c} = \frac{1}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{y i^2 - (2b)^{-1} (j-i)^2} \delta_i$$

where  $1 \leq x \leq p-2, 0 \leq y \leq p-1, 1 \leq b \leq \frac{p-1}{2}$ .

Proof: Every split torus  $T \subset SL_2(\mathbb{F}_p)$  can be written as the form  $gAg^{-1}$  where  $A$  is the diagonal torus

and  $g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} \in R$  is presented in Lemma 2. Then

$$\mathcal{B}_T = \mathcal{B}_{gAg^{-1}} = \{\rho(g)\varphi : \varphi \in \mathcal{B}_A\}$$

and

$$\mathfrak{S}^s = \bigcup_{g \in R} \mathcal{B}_{gTg^{-1}} = \{\rho(g)\varphi : g \in R, \varphi \in \mathcal{B}_A\}.$$

If  $b = 0$ ,  $g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}$  has the form  $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$  ( $0 \leq c \leq p-1$ ), then from (27), we have

$$\begin{aligned} \rho(g)\varphi_x &= N_c \left( \frac{1}{\sqrt{p-1}} \sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} \delta_i \right) \\ &= \frac{1}{\sqrt{p-1}} \sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} N_c \delta_i \\ &= \frac{1}{\sqrt{p-1}} \sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} \eta^{-2^{-1}ci^2} \delta_i. \end{aligned}$$

If  $b \neq 0$ ,  $g$  has following decomposition

$$g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b(1+bc) & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b^{-1} & 1 \end{pmatrix}.$$

Then Applying (26)(27)(28), we have

$$\begin{aligned} \rho(g)\varphi_x &= S_b \circ N_{b(1+bc)} \circ F \circ N_{b^{-1}} \left( \frac{1}{\sqrt{p-1}} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \delta_j \right) \\ &= S_b \circ N_{b(1+bc)} \circ F \left( \frac{1}{\sqrt{p-1}} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-2^{-1}b^{-1}j^2} \delta_j \right) \\ &= S_b \circ N_{b(1+bc)} \left( \frac{1}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-2^{-1}b^{-1}j^2} \eta^{ij} \delta_i \right) \\ &= S_b \left( \frac{1}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-2^{-1}b^{-1}j^2} \eta^{ij} \eta^{-2^{-1}b(1+bc)i^2} \delta_i \right) \\ &= \sigma(b) \left( \frac{1}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-2^{-1}b^{-1}j^2} \eta^{ij} \eta^{-2^{-1}b(1+bc)i^2} \delta_{bi} \right) \\ &= \sigma(b) \left( \frac{1}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-2^{-1}b^{-1}j^2} \eta^{b^{-1}ij} \eta^{-2^{-1}b^{-1}(1+bc)i^2} \delta_i \right) \\ &= \frac{\sigma(b)}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-(2b)^{-1}(j-i)^2 - 2^{-1}ci^2} \delta_i. \end{aligned}$$

Let  $y = -2^{-1}c$ , if  $c$  runs through  $\mathbb{F}_p$ , then  $y$  also runs through  $\mathbb{F}_p$ . Note that  $\sigma(b) = \pm 1$  is a constant, then  $\frac{1}{\sqrt{p-1}} \sum_{i=1}^{p-1} \theta^{x \cdot \log_a i} \eta^{yi^2} \delta_i$  and  $\frac{1}{\sqrt{p(p-1)}} \sum_{i=0}^{p-1} \eta^{yi^2} \sum_{j=1}^{p-1} \theta^{x \cdot \log_a j} \eta^{-(2b)^{-1}(j-i)^2} \delta_i$  with  $1 \leq x \leq p-2$ ,  $0 \leq y \leq p-1$ ,  $1 \leq b \leq \frac{p-1}{2}$  are the all vectors in  $\mathfrak{S}^s$ , which complete the proof.  $\square$

**Proof of Theorem 2.** It follows from Lemma 3. Thus, we have found a simple elementary representation for the split case of finite oscillator system.  $\square$

Recall the extended signal set  $\overline{\mathfrak{S}}$  from oscillator system introduced in Section 3, which is given by

$$\overline{\mathfrak{S}} = \{M_w \varphi : \forall \varphi \in \mathfrak{S}, w \in \mathbb{F}_p\}.$$

In order to prove  $\overline{\mathfrak{S}}$  satisfies Theorem 3, we need the following lemma which is easy to verify using the notion of unitary operation in Hilbert space.

**Lemma 4** For  $\forall \varphi, \psi$  be the sequences with period  $p$ ,  $\forall t, w, z \in \mathbb{F}_p$ , and  $L_t, M_w, F$  be defined in (1), we have:

- (a)  $C_\varphi(t) = \langle \varphi, L_t \varphi \rangle$  and  $C_{\varphi, \psi}(t) = \langle \varphi, L_t \psi \rangle$ .
- (b)  $|\langle \varphi, \pi(t, w, z) \psi \rangle| = |\langle \varphi, M_w \cdot L_t \psi \rangle| = |\langle \varphi, L_t \cdot M_w \psi \rangle|$ .
- (c)  $L_t \cdot F = F \cdot M_t$  and  $FL_{-t} = M_t \cdot F$ .

**Proof of Theorem 3.**

For  $\forall M_{w_1} \varphi, M_{w_2} \psi \in \overline{\mathfrak{S}}$  where  $\varphi, \psi \in \mathfrak{S}$  and  $w_1, w_2 \in \mathbb{F}_p$ , applying Lemma 4-(a), we have

$$\begin{aligned} A_{M_{w_1} \varphi, M_{w_2} \psi}(t, w) &= \langle M_{w_1} \varphi, M_w L_t M_{w_2} \psi \rangle \\ &= \langle \varphi, M_{w_1}^{-1} M_w L_t M_{w_2} \psi \rangle \\ &= \langle \varphi, M_{-w_1} M_w L_t M_{w_2} \psi \rangle. \end{aligned}$$

From Lemma 4-(b), we have

$$\begin{aligned} |A_{M_{w_1} \varphi, M_{w_2} \psi}(t, w)| &= |\langle \varphi, M_{-w_1} M_w L_t M_{w_2} \psi \rangle| \\ &= |\langle \varphi, M_{-w_1} M_w M_{w_2} L_t \psi \rangle| \\ &= |\langle \varphi, M_{w+w_2-w_1} L_t \psi \rangle|. \end{aligned}$$

Theorem 6-(a) indicates all the sequences in  $\mathfrak{S}$  are phase-shift distinct. Thus, if  $M_{w_1} \varphi = M_{w_2} \psi$ , we have  $w_1 = w_2$  and  $\varphi = \psi$ , then  $|A_{M_{w_1} \varphi}(t, w)| = |\langle \varphi, M_w L_t \varphi \rangle|$ . By applying Theorem 6-(a), we know  $|A_{M_{w_1} \varphi}(t, w)| \leq \frac{2}{\sqrt{p}}$  for  $(t, w) \neq (0, 0)$ . If  $M_{w_1} \varphi$  and  $M_{w_2} \psi$  are phase-shift distinct sequences,

then  $\varphi \neq \psi$ , by applying Theorem 6-(a), we have  $|A_{M_{w_1}\varphi, M_{w_2}\psi}(t, w)| \leq \frac{4}{\sqrt{p}}$ . So  $\overline{\mathfrak{S}}$  is a  $(p, p^4, \frac{2}{\sqrt{p}}, \frac{4}{\sqrt{p}})$  ambiguity signal set.

For  $\forall M_w\varphi \in \overline{\mathfrak{S}}$ , it's obvious that the magnitude of  $M_w\varphi(i)$  is as same as  $\varphi(i)$ . By applying Lemma 4-(c), the Fourier transform of  $M_w\varphi$  can be written as  $F \cdot M_w\varphi = L_w \cdot F\varphi$ . We can see  $F\varphi \in \mathfrak{S}$  from Theorem 6-(c) and  $|F\varphi(i)| \leq \frac{2}{\sqrt{p}}$  from Theorem 6-(b). Thus  $|F \cdot M_w\varphi(i)| = |L_w \cdot F\varphi(i)| \leq \frac{2}{\sqrt{p}}$ , which complete the proof.  $\square$

### Proof of Theorem 1

Recall the precise upper bounds for split case presented in Remark 2. The auto and cross ambiguity functions are upper bounded by  $\frac{2\sqrt{p}}{p-1}$  and  $\frac{4\sqrt{p}}{p-1}$  respectively in  $\mathfrak{S}^s$ , so  $\overline{\mathfrak{S}}^s$  is a  $(p, \frac{1}{2}p^2(p+1)(p-2), \frac{2\sqrt{p}}{p-1}, \frac{4\sqrt{p}}{p-1})$  ambiguity signal set by Theorem 2. Considering the construction of new signal set  $\Omega = \{\varphi_n : 0 \leq n < p^2(p-2)\}$  and the elementary construction of the split case of the finite oscillator system, it is obvious that  $\Omega$  is a subset of  $\overline{\mathfrak{S}}^s$  up to multiplication by  $\sqrt{p-1}$ . Thus  $\Omega$  is a  $(p, p^2(p-2), 2\sqrt{p}, 4\sqrt{p})$  ambiguity signal set, and the Fourier transform of  $\varphi$  is bounded by  $|\widehat{\varphi}(i)| \leq 2$  for  $\forall \varphi \in \Omega$  and  $\forall i \in \mathbb{F}_p$ .  $\square$

## 6 Comparisons of the New Constructions with Some Known Constructions

### A. Complex Valued Sequences with Almost Good Ambiguity Function and Fourier Transform

For the construction B (the split case of the finite oscillator system  $\mathfrak{S}^s$ ) and the extended construction  $\overline{\mathfrak{S}}$  in (12), they can be efficient implemented for a moderate  $p$ . However, for a large  $p$ , since they need to compute the exponential sum of  $p$  elements, they are not so efficient. Therefore, in this section, we only make some comparisons for the new construction A ( $\Omega$ ) with some known constructions.

The elements in a sequence from Heisenberg representation [16] have the form  $\varphi_{y,z}(i) = \eta^{yi^2+zi}$  where  $0 \leq y, z \leq p-1$ . The magnitude of the auto ambiguity function of such sequences can reach  $p$  with  $\frac{1}{p}$  probability, which is very poor, while the upper bound of the cross ambiguity function between two phase-shift distinct sequences is given by  $\sqrt{p}$ , and the magnitude of the Fourier transform of these sequences is equal to 1 for  $y \neq 0$ .

Chu sequences [5] and Alltop quadratic sequences [1] with period  $p$  can be considered as a subset of the above sequences for  $z = 0$  whose elements are given by  $\varphi_y(i) = \eta^{yi^2}$  where  $1 \leq y \leq p-1$ . The out-of-phase auto correlation of these sequences is equal to 0, the cross ambiguity function is bounded by  $\sqrt{p}$ , and the magnitude of the Fourier transform of these sequences is equal to 1. However, the magnitude of auto ambiguity function can reach  $p$  with  $\frac{1}{p}$  probability.

The elements in Alltop cubic sequences [1] with period  $p$  are given by  $\varphi_y(i) = \eta^{i^3+yi}$  where  $0 \leq y \leq p-1$ . The auto and cross ambiguity function can reach  $p$  with  $\frac{1}{p}$  probability, and the magnitude of the Fourier transform of these sequences is not considered in the literature.

The properties of the ambiguity function and Fourier transform of above three classes of the sequences can be proved by Lemma 1 in [1].

For the new construction  $\Omega$ , there are  $p^2(p-2)$  time-shift distinct sequences, and the elements in every sequence have the form  $\varphi_{x,y,z}(i) = \theta^{x \cdot \log_a i} \cdot \eta^{yi^2+zi}$ . The auto and cross ambiguity functions of phase-shift distinct sequences in the set are upper bounded by  $2\sqrt{p}$  and  $4\sqrt{p}$ , respectively, and the magnitude of the Fourier transform of these sequences is upper bounded by 2.

We summarize the above discussions in Table 1.

Table 1:

Family	$i$ th element	Size	Comments
Chu [5] Alltop quadratic [1]	$\varphi_y(i) = \eta^{yi^2}$ ( $1 \leq y \leq p-1$ )	$p-1$	Auto ambiguity: not bounded. Cross ambiguity: bounded by $\sqrt{p}$ . Fourier transform: bounded by 1.
Alltop cubic [1]	$\varphi_y(i) = \eta^{i^3+yi^2}$ ( $0 \leq y \leq p-1$ )	$p$	Auto ambiguity: not bounded. Cross ambiguity: not bounded. Fourier transform: N. <sup>(1)</sup>
Sequences from Heisenberg representation [16]	$\varphi_{y,z}(i) = \eta^{yi^2+zi}$ ( $0 \leq y, z \leq p-1$ )	$p^2$	Auto ambiguity: not bounded. Cross ambiguity: bounded by $\sqrt{p}$ . <sup>(2)</sup> Fourier transform: bounded by 1 for $y \neq 0$ .
New construction from Weil representation $\Omega$	$\varphi_{x,y,z}(i) = \theta^{\log_a x} \eta^{yi^2+zi}$ ( $0 \leq y, z \leq p-1,$ $1 \leq x \leq p-2$ )	$p^2(p-2)$	Auto ambiguity: bounded by $2\sqrt{p}$ . Cross ambiguity: bounded by $4\sqrt{p}$ . <sup>(2)</sup> Fourier transform: bounded by 2

<sup>(1)</sup> N: no reported results in the literature.

<sup>(2)</sup> It is the bound of cross ambiguity of phase-shift distinct sequences.

## B. Signal Sets with Sizes in the Order of $p^3$ and Low Correlation

Signal sets which can reach the family size in the order of  $p^3$  with low correlation in the literature are shown in table 2. The bounds of the auto and cross correlation function of new construction  $\Omega$  are better than or as good as the sequences in [3],  $\mathbb{Z}_4$  sequences  $S(2)$  [19], and the sequences in [31], while the maximum magnitudes of the ambiguity function and the Fourier transform (FT) are only discussed in the set  $\Omega$ .

Table 2:

Family	Period $L$	Size	Correlation	Ambiguity	FT
Blake and Mark [3] <sup>(3)</sup>	$p - 1$	$(L + 1)^3$	$4\sqrt{L + 1} + 1$	N	N
$\mathbb{Z}_4$ sequences $S(2)$ [19]	$2^k - 1$	$L^3 + 4L^2 + 5L + 2$	$4\sqrt{L + 1} + 1$	N	N
Yu and Gong [31]	$2^k - 1$	$(L + 1)^3$	$2^{2.5}\sqrt{L + 1}$	N	N
$\Omega$	$p$	$L^2(L - 2)$	$2\sqrt{L}, 4\sqrt{L}$	$2\sqrt{L}, 4\sqrt{L}$	2

<sup>(3)</sup> This family can be easily extended to the sequences over the finite field  $\mathbb{F}_p$  with period  $p^n - 1$  and the same correlation property from the work in [21].

## 7 Concluding Remarks and An Open Problem

We have discovered a simple elementary representation of the sequences in the finite oscillator system from the Weil representation, introduced by Gurevich, Hadani, and Sochen. From this, we have shown a new construction (Construction A in Section 3) of families of complex valued sequences of period  $p$  having low valued two-dimensional auto and cross correlation functions in both time and phase, i.e., low valued auto and cross ambiguity functions, as well as efficient implementation and large sizes. The new construction produces a signal set with  $p^2(p - 2)$  time-shift distinct sequences. The magnitude of the auto and cross ambiguity functions of the phase-shift distinct sequences in the set are upper bounded by  $2\sqrt{p}$  and  $4\sqrt{p}$ , respectively. The Fourier transform of every sequence in the signal set is upper bounded by 2. This signal set can be enlarged, at the expense of implementation, to the size of  $\frac{1}{2}p^2(p - 2)(p + 1)$  (Construction B and (12)) where the upper bounds for the magnitude of the auto and cross ambiguity functions and the upper bound for the magnitude of the Fourier spectrum are unchanged when the normalization factor is removed. This is the first signal set which have good two-dimensional auto and cross correlation in both time and phase with efficient implementation and large size. However, the proofs of those results requires very deep mathematics, i.e., the representation theory and  $l$ -adic algebraic geometry.

If we look at the construction again, we find that it is very simple, since each sequence  $\varphi_n = \{\varphi_n(i)\}_{i \geq 0}$  is the term-by-term product of the sequences  $\{\theta^{x \log_a i}\}_{i \geq 0}$  and  $\{\eta^{y i^2 + z i}\}_{i \geq 0}$  where  $n = (x - 1)p^2 + yp + z$  with  $1 \leq x \leq p - 2, 0 \leq y, z < p$ , and  $\theta$  and  $\eta$  are the  $(p - 1)$ th and  $p$ th primitive roots of unity, respectively. Going back to the literature, all the known constructions only involve one type of the characters of finite field  $\mathbb{F}_p$ . However, here we use both. In other words, the sequences constructed from the Weil representation result from a hybrid construction utilizing both multiplicative and additive characters of finite field  $\mathbb{F}_p$ . This is an amazing phenomenon. This fact seems suggested that it is worth to look at a direct proof for the construction we found here, which will have a two-fold effect. One is

for better promotion of those sequences in practice without introducing the Weil representation theory. The other is that it may lead to more discoveries of new signal sets with good auto and cross ambiguity functions as well as low magnitude of the Fourier transform spectrum.

The sequences with low magnitude of the Fourier transform spectrum employed in OFDM systems can reduce PAPR [23] and the sequences with good two-dimensional auto and cross correlation in both time and phase can reduce the interference in a multiple access scenario and can combat the Doppler effect in radar applications. Research findings recorded in the literature show that the sequences with those properties simultaneously are hard to find by classic methods, since there is none. Fairly speaking, the new construction produces the signal set having not only good correlation but also good ambiguity functions and low valued Fourier transform spectrum due to the benefit of a deep mathematical method, the Weil representation, which is relatively new to sequence design.

**Open Problem.** For  $\Omega = \{\varphi_n \mid 0 \leq n \leq p^2(p-2)\}$ , directly show that  $\Omega$  is a  $(p, p^2(p-2), 2\sqrt{p}, 4\sqrt{p})$  ambiguity signal set and the Fourier spectrum of every sequence in the set is upper bounded by 2 without introducing the sequences in the finite oscillator system from the Weil representation.

## Acknowledgment

The authors would like to thank Grevich, Hadani and Sochen for their help during the course of conducting this work.

## References

- [1] W.O. Alltop, Complex sequences with low periodic correlations, *IEEE Trans. Inform. Theory*, Vol. 26, No. 3, May 1980, pp. 350-354.
- [2] F.R. Beyl, The Schur multiplier of  $SL(2, \mathbb{Z}/m\mathbb{Z})$  and the congruence subgroup property, *Math. Zeit.*, 191, 1986.
- [3] L.F. Blake and J.W. Mark, A note on complex sequences with low periodic correlations, *IEEE Trans. Inform. Theory*, Vol. 28, No. 5, September 1982, pp. 814-816.
- [4] A. Borel, *Linear Algebraic Groups*. Graduate Texts in Mathematics, vol. 126, Springer, New York, 1991.
- [5] C. Chu, Polyphase codes with good periodic correlation properties, *IEEE Trans. Inform. Theory*, Vol. 18, No. 4, Jul. 1972, pp. 531-532.
- [6] J.P. Costas, A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties, *Proc. IEEE*, **72** (1984), 996-1009.

- [7] J.A. Davis and J. Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, *IEEE Trans. Inform. Theory*, vol. 45, No. 7, Nov. 1999, pp. 2397-2416.
- [8] G. Gong, Theory and applications of q-ary interleaved sequences, *IEEE Trans. Inform. Theory*, vol. 41, No. 2, March 1995, pp. 400-411.
- [9] S.W. Golomb and G. Gong, *Signal Design with Good Correlation: for Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, 2005.
- [10] S.W. Golomb and G. Gong, The Status of Costas Arrays, *IEEE Trans. Information Theory*, Vol. 53, No. 11, Nov. 2007, pp. 4260 - 4265.
- [11] S. Gurevich, R. Hadani, and N. Sochen. The finite harmonic oscillator and its applications to sequences, communication and radar. *IEEE Trans. Inform. Theory*, Vol. 54, No. 9, September 2008, pp. 4239-4253.
- [12] S. Gurevich, R. Hadani, and N. Sochen, On some deterministic dictionaries supporting sparsity, *Journal of Fourier Analysis and Applications*, Vol. 14, No. 5-6, December 2008, pp. 859-876.
- [13] S. Gurevich, R. Hadani, and N. Sochen, Group representation design of digital signals and sequences, *the Proceedings of the International Conference on Sequences and Their Applications (SETA)*, 2008, Sep. 14-18, 2008, Lexington, KY, USA. *Sequences and Their Applications-SETA 2008*, LNCS 5203, S.W. Golomb, et al. (Eds.), Springer, 2008, pp. 153-166.
- [14] S. Gurevich and R. Hadani, On the diagonalization of the discrete Fourier transform, *Applied and Computational Harmonic Analysis*, to appear 2008.
- [15] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole, The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 301-319, 1994.
- [16] S.D. Howard, A.R. Calderbank, and W. Moran, The finite Heisenberg- Weyl groups in radar and communications, *EURASIP J. Appl. Signal Process*, Vol. 2006, pp.1-12.
- [17] R. Howe, Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries, *Indag. Math. (N.S.)*, vol. 16, no. 3-4, 2005, pp. 553-583.
- [18] T. Helleseth and P.V. Kumar, Sequences with low correlation, a chapter in *Handbook of Coding Theory*, edited by V. Pless and C. Huffman, Elsevier Science Publishers, 1998, pp. 1765-1853.
- [19] P.V. Kumar, T. Helleseth, A.R. Calderbank, and A.R. Hammons, Large families of quaternary sequences with low correlation, *IEEE Trans. Inform. Theory*, Vol. 42, No. 2, March 1996, pp. 579-592.

- [20] P.V. Kumar and Oscar Moreno, Prime-phase sequences with periodic correlation properties better than binary sequences, *IEEE Trans. Inform. Theory*, vol. 37, No. 3, May 1991, pp. 603-616.
- [21] O. Moreno, C.J. Moreno, The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes. *IEEE Trans. Inform. Theory*, vol. 40, No.6, November 1994, pp. 1894-1907.
- [22] K.G. Paterson, Binary sequence sets with favorable correlations from difference sets and MDS codes, *IEEE Trans. Inform. Theory*, Vol. 44, No. 1, January 1998, pp. 172-180.
- [23] K.G. Paterson and V. Tarokh, On the existence and construction of good codes with low peak-to-average power ratios, *IEEE Trans. Inform. Theory*, vol. 46, No. 6, 2000, pp. 1974-1987.
- [24] J.G. Proakis, *Digital Communications*, McGraw-Hill, Inc., 3rd ed., 1995.
- [25] A. Sampath, D. Hui, H. Zheng and B.Y. Zhao, Multi-channel jamming attacks using cognitive radios, *Proceedings of 16th International Conference on Computer Communications and Networks, 2007 (ICCCN 2007)*, 2007, pp. 352-357
- [26] D.V. Sarwate and M.B. Pursley, Cross correlation properties of pseudorandom and related sequences, *Proc. of the IEEE*, vol. 68, No. 5, May 1980, pp. 593-619.
- [27] J.P. Serre, *Linear Representations of Finite Groups*. Graduate Texts in Mathematics, vol. 42, Springer, New York, 1977.
- [28] B. L. van der Waerden, *Moderne Algebra*, Springer, 1931.
- [29] A. Weil, Sur certains groupes d'opérateurs unitaires, *Acta. Math.*, vol. 111, 1964, pp. 143-211.
- [30] L.R. Welch, Lower bounds on the minimum correlation of signals, *IEEE Trans. Inform. Theory*, Vol. 20, No. 3, May 1974, pp. 397-399.
- [31] N.Y. Yu, and G. Gong, A new binary sequence family with low correlation and large size, *IEEE Trans. Inform. Theory*, Vol. 52, No. 4, April 2006, pp. 1624-1636.