GROUP REPRESENTATION DESIGN OF DIGITAL SIGNALS AND SEQUENCES

SHAMGAR GUREVICH, RONNY HADANI, AND NIR SOCHEN

To appear in the proceedings of SETA08

Abstract. In this survey a novel system, called the oscillator system, consisting of order of \( p^3 \) functions (signals) on the finite field \( \mathbb{F}_p \), is described and studied. The new functions are proved to satisfy good auto-correlation, cross-correlation and low peak-to-average power ratio properties. Moreover, the oscillator system is closed under the operation of discrete Fourier transform. Applications of the oscillator system for discrete radar and digital communication theory are explained. Finally, an explicit algorithm to construct the oscillator system is presented.

1. Introduction

One-dimensional analog signals are complex valued functions on the real line \( \mathbb{R} \). In the same spirit, one-dimensional digital signals, also called sequences, might be considered as complex valued functions on the finite line \( \mathbb{F}_p \), i.e., the finite field with \( p \) elements, where \( p \) is an odd prime. In both situations the parameter of the line is denoted by \( t \) and is referred to as time. In this survey, we will consider digital signals only, which will be simply referred to as signals. The space of signals \( \mathcal{H} = \mathbb{C}(\mathbb{F}_p) \) is a Hilbert space with the Hermitian product given by

\[
\langle \phi, \varphi \rangle = \sum_{t \in \mathbb{F}_p} \phi(t) \overline{\varphi(t)}.
\]

A central problem is to construct interesting and useful systems of signals. Given a system \( \mathcal{S} \), there are various desired properties which appear in the engineering wish list. For example, in various situations \([1, 2]\) one requires that the signals will be weakly correlated, i.e., that for every \( \phi \neq \varphi \in \mathcal{S} \)

\[
|\langle \phi, \varphi \rangle| \ll 1.
\]

This property is trivially satisfied if \( \mathcal{S} \) is an orthonormal basis. Such a system cannot consist of more than \( \dim \mathcal{H} \) signals, however, for certain applications, e.g., CDMA (Code Division Multiple Access) \([3]\) a larger number of signals is desired, in that case the orthogonality condition is relaxed.

During the transmission process, a signal \( \varphi \) might be distorted in various ways. Two basic types of distortions are time shift \( \varphi(t) \mapsto L_\tau \varphi(t) = \varphi(t + \tau) \) and phase shift \( \varphi(t) \mapsto M_w \varphi(t) = e^{2\pi i w t} \varphi(t) \), where \( \tau, w \in \mathbb{F}_p \). The first type appears in asynchronous communication and the second type is a Doppler effect due to relative velocity between the transmitting and receiving antennas. In conclusion, a general...
distortion is of the type \( \varphi \mapsto M_w L_\tau \varphi \), suggesting that for every \( \varphi \neq \phi \in \mathcal{S} \) it is natural to require \([2]\) the following stronger condition

\[
|\langle \phi, M_w L_\tau \varphi \rangle| \ll 1.
\]

Due to technical restrictions in the transmission process, signals are sometimes required to admit low peak-to-average power ratio \([4]\), i.e., that for every \( \varphi \in \mathcal{S} \) with \( \|\varphi\|_2 = 1 \)

\[
\max \{ |\varphi(t)| : t \in \mathbb{F}_p \} \ll 1.
\]

Finally, several schemes for digital communication require that the above properties will continue to hold also if we replace signals from \( \mathcal{S} \) by their Fourier transform.

In this survey we demonstrate a construction of a novel system of (unit) signals \( \mathcal{S}_O \), consisting of order of \( p^3 \) signals, called the oscillator system. These signals constitute, in an appropriate formal sense, a finite analogue for the eigenfunctions of the harmonic oscillator in the real setting and, in accordance, they share many of the nice properties of the latter class. In particular, the system \( \mathcal{S}_O \) satisfies the following properties

1. **Auto-correlation (ambiguity function).** For every \( \varphi \in \mathcal{S}_O \) we have

\[
|\langle \varphi, M_w L_\tau \varphi \rangle| = \begin{cases} 1 & \text{if } (\tau, w) = 0, \\ \leq \frac{2}{\sqrt{p}} & \text{if } (\tau, w) \neq 0. \end{cases}
\]

(1.1)

2. **Cross-correlation (cross-ambiguity function).** For every \( \phi \neq \varphi \in \mathcal{S}_O \) we have

\[
|\langle \phi, M_w L_\tau \varphi \rangle| \leq \frac{4}{\sqrt{p}},
\]

for every \( \tau, w \in \mathbb{F}_p \).

(1.2)

3. **Supremum.** For every signal \( \varphi \in \mathcal{S}_O \) we have

\[
\max \{ |\varphi(t)| : t \in \mathbb{F}_p \} \leq \frac{2}{\sqrt{p}}.
\]

(4) **Fourier invariance.** For every signal \( \varphi \in \mathcal{S}_O \) its Fourier transform \( \hat{\varphi} \) is (up to multiplication by a unitary scalar) also in \( \mathcal{S}_O \).

The oscillator system can be extended to a much larger system \( \mathcal{S}_E \), consisting of order of \( p^5 \) signals if one is willing to compromise Properties 1 and 2 for a weaker condition. The extended system consists of all signals of the form \( M_w L_\tau \varphi \) for \( \tau, w \in \mathbb{F}_p \) and \( \varphi \in \mathcal{S}_O \). It is not hard to show that \( \#(\mathcal{S}_E) = p^2 \cdot \#(\mathcal{S}_O) \approx p^5 \).

As a consequence of (1.1) and (1.2) for every \( \varphi \neq \phi \in \mathcal{S}_E \) we have

\[
|\langle \varphi, \phi \rangle| \leq \frac{4}{\sqrt{p}}.
\]

The characterization and construction of the oscillator system is representation theoretic and we devote the rest of the survey to an intuitive explanation of the main underlying ideas. As a suggestive model example we explain first the construction of the well known system of chirp (Heisenberg) signals, deliberately taking a representation theoretic point of view (see \([2, 5]\) for a more comprehensive treatment).
2. Model example (Heisenberg system)

Let us denote by \( \psi : \mathbb{F}_p \to \mathbb{C}^\times \) the character \( \psi(t) = e^{\frac{2\pi it}{\mathbb{F}_p}} \). We consider the pair of orthonormal bases \( \Delta = \{ \delta_a : a \in \mathbb{F}_p \} \) and \( \Delta^\vee = \{ \psi_a : a \in \mathbb{F}_p \} \), where \( \psi_a(t) = \frac{1}{\sqrt{p}} \psi(at) \).

2.1. Characterization of the bases \( \Delta \) and \( \Delta^\vee \). Let \( L : \mathcal{H} \to \mathcal{H} \) be the time shift operator \( L \varphi(t) = \varphi(t+1) \). This operator is unitary and it induces a homomorphism of groups \( L : \mathbb{F}_p \to U(\mathcal{H}) \) given by \( L \varphi(t) = \varphi(t+\tau) \) for any \( \tau \in \mathbb{F}_p \).

Elements of the basis \( \Delta^\vee \) are character vectors with respect to the homomorphism \( L \) i.e., \( L \psi_a = \psi(a\tau) \psi_a \) for any \( \tau \in \mathbb{F}_p \). In the same fashion, the basis \( \Delta \) consists of character vectors with respect to the homomorphism \( \mathbb{F}_p \to U(\mathcal{H}) \) generated by the phase shift operator \( M \varphi(t) = \psi(t) \varphi(t) \).

2.2. The Heisenberg representation. The homomorphisms \( L \) and \( M \) can be combined into a single map \( \bar{\pi} : \mathbb{F}_p \times \mathbb{F}_p \to U(\mathcal{H}) \) which sends a pair \((\tau, w)\) to the unitary operator \( \bar{\pi}(\tau, \omega) = \psi(-\frac{1}{2} \tau w) M_w \circ L_\tau \). The plane \( \mathbb{F}_p \times \mathbb{F}_p \) is called the time-frequency plane and will be denoted by \( V \). The map \( \bar{\pi} \) is not an homomorphism since, in general, the operators \( L_\tau \) and \( M_w \) do not commute. This deficiency can be corrected if we consider the group \( H = V \times \mathbb{F}_p \) with multiplication given by

\[
(\tau, w, z) \cdot (\tau', w', z') = (\tau + \tau', w + w', z + z' + \frac{1}{2}(\tau w' - \tau' w)).
\]

The map \( \bar{\pi} \) extends to a homomorphism \( \pi : H \to U(\mathcal{H}) \) given by

\[
\pi(\tau, w, z) = \psi(-\frac{1}{2} \tau w + z) M_w \circ L_\tau.
\]

The group \( H \) is called the Heisenberg group and the homomorphism \( \pi \) is called the Heisenberg representation.

2.3. Maximal commutative subgroups. The Heisenberg group is no longer commutative, however, it contains various commutative subgroups which can be easily described. To every line \( L \subset V \), which pass through the origin, one can associate a maximal commutative subgroup \( A_L = \{ (l,0) \in V \times \mathbb{F}_p : l \in L \} \). It will be convenient to identify the subgroup \( A_L \) with the line \( L \).

2.4. Bases associated with lines. Restricting the Heisenberg representation \( \pi \) to a subgroup \( L \) yields a decomposition of the Hilbert space \( \mathcal{H} \) into a direct sum of one-dimensional subspaces \( \mathcal{H} = \bigoplus_\chi \mathcal{H}_\chi \), where \( \chi \) runs in the set \( L^\vee \) (of (complex valued) characters of the group \( L \). The subspace \( \mathcal{H}_\chi \) consists of vectors \( \varphi \in \mathcal{H} \) such that \( \pi(l) \varphi = \chi(l) \varphi \). In other words, the space \( \mathcal{H}_\chi \) consists of common eigenvectors with respect to the commutative system of unitary operators \( \{ \pi(l) \}_{l \in L} \) such that the operator \( \pi(l) \) has eigenvalue \( \chi(l) \).

Choosing a unit vector \( \varphi_\chi \in \mathcal{H}_\chi \) for every \( \chi \in L^\vee \) we obtain an orthonormal basis \( B_L = \{ \varphi_\chi : \chi \in L^\vee \} \). In particular, \( \Delta^\vee \) and \( \Delta \) are recovered as the bases associated with the lines \( T = \{ (\tau,0) : \tau \in \mathbb{F}_p \} \) and \( W = \{ (0,w) : w \in \mathbb{F}_p \} \) respectively. For a general \( L \) the signals in \( B_L \) are certain kind of chirps. Concluding, we associated with every line \( L \subset V \) an orthonormal basis \( B_L \), and overall we constructed a system of signals consisting of a union of orthonormal bases

\[
\mathcal{S}_H = \{ \varphi \in B_L : L \subset V \}.
\]

For obvious reasons, the system \( \mathcal{S}_H \) will be called the Heisenberg system.
2.5. Properties of the Heisenberg system. It will be convenient to introduce the following general notion. Given two signals \( \phi, \varphi \in \mathcal{H} \), their matrix coefficient is the function \( m_{\phi, \varphi} : \mathcal{H} \to \mathbb{C} \) given by \( m_{\phi, \varphi}(h) = \langle \phi, \pi(h) \varphi \rangle \). In coordinates, if we write \( h = (\tau, w, z) \) then \( m_{\phi, \varphi}(h) = \psi(-\frac{1}{2}\tau w + z) \langle \phi, M_w \circ L_\tau \varphi \rangle \). When \( \phi = \varphi \) the function \( m_{\phi, \varphi} \) is called the ambiguity function of the vector \( \varphi \) and is denoted by \( A_{\varphi} = m_{\varphi, \varphi} \).

The system \( \mathcal{S}_H \) consists of \( p + 1 \) orthonormal bases\(^1\) altogether \( p(p + 1) \) signals and it satisfies the following properties \(^2\), \(^5\)

1. **Auto-correlation.** For every signal \( \varphi \in \mathcal{B}_L \) the function \( |A_{\varphi}| \) is the characteristic function of the line \( L \), i.e.,
   \[
   |A_{\varphi}(v)| = \begin{cases} 
   0, & v \notin L, \\
   1, & v \in L.
   \end{cases}
   \]

2. **Cross-correlation.** For every \( \phi \in \mathcal{B}_L \) and \( \varphi \in \mathcal{B}_M \) where \( L \neq M \) we have
   \[
   |m_{\varphi, \phi}(v)| \leq \frac{1}{\sqrt{p}},
   \]
   for every \( v \in V \). If \( L = M \) then \( |m_{\varphi, \phi}| \) is the characteristic function of some translation of the line \( L \).

3. **Supremum.** A signal \( \varphi \in \mathcal{S}_H \) is a unimodular function, i.e., \( |\varphi(t)| = \frac{1}{\sqrt{p}} \) for every \( t \in \mathbb{F}_p \), in particular we have
   \[
   \max \{|\varphi(t)| : t \in \mathbb{F}_p\} = \frac{1}{\sqrt{p}} \ll 1.
   \]

**Remark 1.** Note the main differences between the Heisenberg and the oscillator systems. The oscillator system consists of order of \( p^3 \) signals, while the Heisenberg system consists of order of \( p^2 \) signals. Signals in the oscillator system admit an ambiguity function concentrated at \( 0 \in V \) (thumbtack pattern) while signals in the Heisenberg system admit ambiguity function concentrated on a line.

3. The oscillator system

Reflecting back on the Heisenberg system we see that each vector \( \varphi \in \mathcal{S}_H \) is characterized in terms of action of the additive group \( G_\alpha = \mathbb{F}_p \). Roughly, in comparison, each vector in the oscillator system is characterized in terms of action of the multiplicative group \( G_m = \mathbb{F}_p^\times \). Our next goal is to explain the last assertion. We begin by giving a model example.

Given a multiplicative character\(^2\) \( \chi : G_m \to \mathbb{C}^\times \), we define a vector \( \chi \in \mathcal{H} \) by
   \[
   \chi(t) = \begin{cases} 
   \frac{1}{\sqrt{p}} \chi(t), & t \neq 0, \\
   0, & t = 0.
   \end{cases}
   \]

We consider the system \( \mathcal{B}_{std} = \{\chi : \chi \in G_m^\vee, \chi \neq 1\} \), where \( G_m^\vee \) is the dual group of characters.

---

\(^1\)Note that \( p + 1 \) is the number of lines in \( V \).

\(^2\)A multiplicative character is a function \( \chi : G_m \to \mathbb{C}^\times \) which satisfies \( \chi(xy) = \chi(x)\chi(y) \) for every \( x, y \in G_m \).
3.1. Characterizing the system $B_{std}$. For each element $a \in G_m$ let $\rho_a : \mathcal{H} \rightarrow \mathcal{H}$ be the unitary operator acting by scaling $\rho_a \varphi(t) = \varphi(at)$. This collection of operators form a homomorphism $\rho : G_m \rightarrow U(\mathcal{H})$.

Elements of $B_{std}$ are character vectors with respect to $\rho$, i.e., the vector $\chi$ satisfies $\rho_a(\chi) = \chi(a)\chi$ for every $a \in G_m$. In more conceptual terms, the action $\rho$ yields a decomposition of the Hilbert space $\mathcal{H}$ into character spaces $\mathcal{H} = \bigoplus \mathcal{H}_\chi$, where $\chi$ runs in the group $G'_m$. The system $B_{std}$ consists of a representative unit vector for each space $\mathcal{H}_\chi$, $\chi \neq 1$.

3.2. The Weil representation. We would like to generalize the system $B_{std}$ in a similar fashion to the way we generalized the bases $\Delta$ and $\Delta^\vee$ in the Heisenberg setting. In order to this we need to introduce several auxiliary operators.

Let $\rho_a : \mathcal{H} \rightarrow \mathcal{H}$, $a \in \mathbb{F}_p^\times$, be the operators acting by $\rho_a \varphi(t) = \sigma(a)\varphi(a^{-1}t)$ (scaling), where $\sigma$ is the unique quadratic character of $\mathbb{F}_p^\times$, let $\rho_T : \mathcal{H} \rightarrow \mathcal{H}$ be the operator acting by $\rho_T \varphi(t) = \psi(t^2)\varphi(t)$ (quadratic modulation), and finally let $\rho_S : \mathcal{H} \rightarrow \mathcal{H}$ be the operator of Fourier transform

$$\rho_S \varphi(t) = \frac{\nu}{\sqrt{p}} \sum_{s \in \mathbb{F}_p} \psi(ts)\varphi(s),$$

where $\nu$ is a normalization constant [6]. The operators $\rho_a$, $\rho_T$ and $\rho_S$ are unitary. Let us consider the subgroup of unitary operators generated by $\rho_a$, $\rho_S$ and $\rho_T$. This group turns out to be isomorphic to the finite group $Sp = SL_2(\mathbb{F}_p)$, therefore we obtained a homomorphism $\rho : Sp \rightarrow U(\mathcal{H})$. The representation $\rho$ is called the Weil representation [7] and it will play a prominent role in this survey.

3.3. Systems associated with maximal (split) tori. The group $Sp$ consists of various types of commutative subgroups. We will be interested in maximal diagonalizable commutative subgroups. A subgroup of this type is called maximal split torus. The standard example is the subgroup consisting of all diagonal matrices

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in G_m \right\},$$

which is called the standard torus. The restriction of the Weil representation to a split torus $T \subset Sp$ yields a decomposition of the Hilbert space $\mathcal{H}$ into a direct sum of character spaces $\mathcal{H} = \bigoplus \mathcal{H}_\chi$, where $\chi$ runs in the set of characters $T^\vee$. Choosing a unit vector $\varphi_\chi \in \mathcal{H}_\chi$ for every $\chi$ we obtain a collection of orthonormal vectors $B_T = \{ \varphi_\chi : \chi \in T^\vee, \chi \neq 1 \}$. Overall, we constructed a system

$$\mathcal{S}_T^\phi = \{ \varphi \in B_T : T \subset Sp \text{ split} \},$$

which will be referred to as the split oscillator system. We note that our initial system $B_{std}$ is recovered as $B_{std} = B_A$.

3.4. Systems associated with maximal (non-split) tori. From the point of view of this survey, the most interesting maximal commutative subgroups in $Sp$ are those which are diagonalizable over an extension field rather than over the base field $\mathbb{F}_p$. A subgroup of this type is called maximal non-split torus. It might be suggestive to first explain the analogue notion in the more familiar setting of the field $\mathbb{R}$. Here, the standard example of a maximal non-split torus is the circle group $SO(2) \subset SL_2(\mathbb{R})$. Indeed, it is a maximal commutative subgroup which becomes diagonalizable when considered over the extension field $\mathbb{C}$ of complex numbers.
The above analogy suggests a way to construct examples of maximal non-split tori in the finite field setting as well. Let us assume for simplicity that $-1$ does not admit a square root in $\mathbb{F}_p$. The group $Sp$ acts naturally on the plane $V = \mathbb{F}_p \times \mathbb{F}_p$. Consider the symmetric bilinear form $B$ on $V$ given by

$$B((t, w), (t', w')) = tt' + ww'.$$

An example of maximal non-split torus is the subgroup $T_{ns} \subset Sp$ consisting of all elements $g \in Sp$ preserving the form $B$, i.e., $g \in T_{ns}$ if and only if $B(gu, gv) = B(u, v)$ for every $u, v \in V$.

In the same fashion like in the split case, restricting the Weil representation to a non-split torus $T$ yields a decomposition into character spaces $H = \bigoplus H_\chi$. Choosing a unit vector $\varphi_\chi \in H_\chi$ for every $\chi \in T^\vee$ we obtain an orthonormal basis $\mathcal{B}_T$. Overall, we constructed a system of signals

$$\mathcal{S}^*_O = \{ \varphi \in \mathcal{B}_T : T \subset Sp \text{ non-split} \}.$$  

The system $\mathcal{S}^*_O$ will be referred to as the non-split oscillator system. The construction of the system $\mathcal{S}_O = \mathcal{S}^*_O \cup \mathcal{S}^*_O$ together with the formulation of some of its properties are the main contribution of this survey.

### 3.5. Behavior under Fourier transform.

The oscillator system is closed under the operation of Fourier transform, i.e., for every $\varphi \in \mathcal{S}_O$ we have $\hat{\varphi} \in \mathcal{S}_O$. The Fourier transform on the space $\mathbb{C}(\mathbb{F}_p)$ appears as a specific operator $\rho(w)$ in the Weil representation, where

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in Sp.$$

Given a signal $\varphi \in \mathcal{B}_T \subset \mathcal{S}_O$, its Fourier transform $\hat{\varphi} = \rho(w) \varphi$ is, up to a unitary scalar, a signal in $\mathcal{B}_{T'}$, where $T' = wTw^{-1}$. In fact, $\mathcal{S}_O$ is closed under all the operators in the Weil representation! Given an element $g \in Sp$ and a signal $\varphi \in \mathcal{B}_T$ we have, up to a unitary scalar, that $\rho(g) \varphi \in \mathcal{B}_{T'}$, where $T' = gTg^{-1}$.

In addition, the Weyl element $w$ is an element in some maximal torus $T_w$ (the split type of $T_w$ depends on the characteristic $p$ of the field) and as a result signals $\varphi \in \mathcal{B}_{T_w}$ are, in particular, eigenvectors of the Fourier transform. As a consequences a signal $\varphi \in \mathcal{B}_{T_w}$ and its Fourier transform $\hat{\varphi}$ differ by a unitary constant, therefore are practically the "same" for all essential matters.

These properties might be relevant for applications to OFDM (Orthogonal Frequency Division Multiplexing) where one requires good properties both from the signal and its Fourier transform.

### 3.6. Relation to the harmonic oscillator.

Here we give the explanation why functions in the non-split oscillator system $\mathcal{S}^*_O$ constitute a finite analogue of the eigenfunctions of the harmonic oscillator in the real setting. The Weil representation establishes the dictionary between these two, seemingly, unrelated objects. The argument works as follows.

The one-dimensional harmonic oscillator is given by the differential operator $D = \partial^2 - t^2$. The operator $D$ can be exponentiated to give a unitary representation of the circle group $\rho : SO(2, \mathbb{R}) \rightarrow U(L^2(\mathbb{R}))$ where $\rho(e^{i\theta}) = e^{i\theta D}$. Eigenfunctions of $D$ are naturally identified with character vectors with respect to $\rho$. The crucial point is that $\rho$ is the restriction of the Weil representation of $SL_2(\mathbb{R})$ to the maximal non-split torus $SO(2, \mathbb{R}) \subset SL_2(\mathbb{R})$. 

---

*SHAMGAR GUREVICH, RONNY HADANI, AND NIR SOCHEN*
Summarizing, the eigenfunctions of the harmonic oscillator and functions in $\mathfrak{g}_O^{\text{ns}}$ are governed by the same mechanism, namely both are character vectors with respect to the restriction of the Weil representation to a maximal non-split torus in $SL_2$. The only difference appears to be the field of definition, which for the harmonic oscillator is the reals and for the oscillator functions is the finite field.

4. Applications

Two applications of the oscillator system will be described. The first application is to the theory of discrete radar. The second application is to CDMA systems. We will give a brief explanation of these problems, while emphasizing the relation to the Heisenberg representation.

4.1. Discrete Radar. The theory of discrete radar is closely related to the finite Heisenberg group $H$. A radar sends a signal $\varphi(t)$ and obtains an echo $e(t)$. The goal is to reconstruct, in maximal accuracy, the target range and velocity. The signal $\varphi(t)$ and the echo $e(t)$ are, principally, related by the transformation

$$e(t) = e^{2\pi i wt} \varphi(t + \tau) = M_w L_\tau \varphi(t),$$

where the time shift $\tau$ encodes the distance of the target from the radar and the phase shift encodes the velocity of the target. Equivalently saying, the transmitted signal $\varphi$ and the received echo $e$ are related by an action of an element $h_0 \in H$, i.e., $e = \pi(h_0)\varphi$. The problem of discrete radar can be described as follows. Given a signal $\varphi$ and an echo $e = \pi(h_0)\varphi$ extract the value of $h_0$.

It is easy to show that $|m_{\varphi,e}(h)| = |A_{\varphi}(h \cdot h_0)|$ and it obtains its maximum at $h_0^{-1}$. This suggests that a desired signal $\varphi$ for discrete radar should admit an ambiguity function $A_{\varphi}$ which is highly concentrated around $0 \in H$, which is a property satisfied by signals in the oscillator system (Property 2).

**Remark 2.** It should be noted that the system $\mathfrak{g}_O$ is "large" consisting of approximately $p^3$ signals. This property becomes important in a jamming scenario.

4.2. Code Division Multiple Access (CDMA). We are considering the following setting.

- There exists a collection of users $i \in I$, each holding a bit of information $b_i \in \mathbb{C}$ (usually $b_i$ is taken to be an $N$th root of unity).
- Each user transmits his bit of information, say, to a central antenna. In order to do that, he multiplies his bit $b_i$ by a private signal $\varphi_i \in H$ and forms a message $u_i = b_i \varphi_i$.
- The transmission is carried through a single channel (for example in the case of cellular communication the channel is the atmosphere), therefore the message received by the antenna is the sum

$$u = \sum_i u_i.$$

The main problem is to extract the individual bits $b_i$ from the message $u$. The bit $b_i$ can be estimated by calculating the inner product

$$\langle \varphi_i, u \rangle = \sum_i \langle \varphi_i, u_j \rangle = \sum_j b_j \langle \varphi_i, \varphi_j \rangle = b_i + \sum_{j \neq i} b_j \langle \varphi_i, \varphi_j \rangle.$$

The last expression above should be considered as a sum of the information bit $b_i$ and an additional noise caused by the interference of the other messages. This
is the standard scenario also called the *Synchronous* scenario. In practice, more complicated scenarios appear, e.g., *asynchronous scenario* - in which each message \( u_i \) is allowed to acquire an arbitrary time shift \( u_i(t) \mapsto u_i(t + \tau_i) \). *Phase shift scenario* - in which each message \( u_i \) is allowed to acquire an arbitrary phase shift \( u_i(t) \mapsto \, \text{e}^{2\pi i \, \phi_i(t)} \), and probably also a combination of the two where each message \( u_i \) is allowed to acquire an arbitrary distortion of the form 
\[
\text{e}^{2\pi i \, \phi_i(t)} \mapsto \text{e}^{2\pi i \, \phi_i(t + \tau_i)}.
\]

The previous discussion suggests that what we are seeking for is a large system \( S \) of signals which will enable a reliable extraction of each bit \( b_i \) for as many users transmitting through the channel simultaneously.

**Definition 1** (Stability conditions). Two unit signals \( \phi \neq \varphi \) are called **stably cross-correlated** if \( |m_{\phi,\varphi}(v)| \ll 1 \) for every \( v \in V \). A unit signal \( \varphi \) is called **stably auto-correlated** if \( |A_{\varphi}(v)| \ll 1 \), for \( v \neq 0 \). A system \( S \) of signals is called a **stable** system if every signal \( \varphi \in S \) is stably auto-correlated and any two different signals \( \phi, \varphi \in S \) are stably cross-correlated.

Formally what we require for CDMA is a stable system \( S \). Let us explain why this corresponds to a reasonable solution to our problem. At a certain time \( t \) the antenna receives a message

\[
u = \sum_{i \in J} u_i,
\]

which is transmitted from a subset of users \( J \subset I \). Each message \( u_i, i \in J \) is of the form \( u_i = b_i \text{e}^{2\pi i \, \varphi_i(t + \tau_i)} = b_i \pi(h_i)\varphi_i \), where \( h_i \in H \). In order to extract the bit \( b_i \) we compute the matrix coefficient

\[
m_{\varphi_i,u} = b_i R_{h_i} A_{\varphi_i} + #(J - \{i\})o(1),
\]

where \( R_{h_i} \) is the operator of right translation \( R_{h_i} A_{\varphi_i}(h) = A_{\varphi_i}(hh_i) \).

If the cardinality of the set \( J \) is not too big then by evaluating \( m_{\varphi_i,u} \) at \( h = h_i^{-1} \) we can reconstruct the bit \( b_i \). It follows from \( (1.1) \) and \( (1.2) \) that the oscillator system \( SO \) can support order of \( p^3 \) users, enabling reliable reconstruction when order of \( \sqrt{p} \) users are transmitting simultaneously.

**Appendix A. Algorithmic construction of the oscillator system**

**A.1. Algorithm.** We describe an explicit algorithm that generates the oscillator system \( SO \) associated with the collection of split tori in \( Sp \).

**A.1.1. Tori.** Consider the standard diagonal torus

\[
A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}; \, a \in F_p^\times \right\}.
\]

Every split torus in \( Sp \) is conjugated to the torus \( A \), which means that the collection \( T \) of all split tori in \( Sp \) can be written as

\[
T = \{ gAg^{-1}; \, g \in Sp \}.
\]
A.1.2. **Parametrization.** A direct calculation reveals that every torus in $\mathcal{T}$ can be written as $gAg^{-1}$ for an element $g$ of the form

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

If $b = 0$, this presentation is unique: In the case $b \neq 0$, an element $\tilde{g}$ represents the same torus as $g$ if and only if it is of the form

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

Let us choose a set of elements of the form (A.1) representing each torus in $\mathcal{T}$ exactly once and denote this set of representative elements by $R$.

A.1.3. **Generators.** The group $A$ is a cyclic group and we can find a generator $g_A$ for $A$. This task is simple from the computational perspective, since the group $A$ is finite, consisting of $p - 1$ elements.

Now we make the following two observations. First observation is that the oscillator basis $B_A$ is the basis of eigenfunctions of the operator $\rho(g_A)$.

The second observation is that, other bases in the oscillator system $\mathcal{S}_O$ can be obtained from $B_A$ by applying elements from the set $R$. More specifically, for a torus $T$ of the form $T = gAg^{-1}, g \in R$, we have

$$B_{gAg^{-1}} = \{ \rho(g)\varphi; \varphi \in B_A \}.$$

Concluding, we described the (split) oscillator system $\mathcal{S}_O = \{ \rho(g) \varphi; g \in R, \varphi \in B_A \}$.

A.2. **Formulas.** We are left to explain how to write explicit formulas (matrices) for the operators $\rho(g), g \in R$.

First, we recall that the group $Sp$ admits a Bruhat decomposition $Sp = B \cup BwB$, where $B$ is the Borel subgroup consisting of upper triangular matrices in $Sp$ and $w$ denotes the Weyl element

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Furthermore, the Borel subgroup $B$ can be written as a product $B = AU = UA$, where $A$ is the standard diagonal torus and $U$ is the standard unipotent group

$$U = \left\{ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}; u \in \mathbb{F}_p \right\}.$$

Therefore, we can write the Bruhat decomposition also as $Sp = UA \cup UAwU$.

Second, we give an explicit description (which can be easily verified) of operators in the Weil representation which are associated with different types of elements in $Sp$. The operators are specified up to a unitary scalar, which is enough for our needs.

- The standard torus $A$ acts by (normalized) scaling: An element

$$a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

acts by

$$S_a [f] (t) = \sigma(a) f (a^{-1}t),$$

where $\sigma: \mathbb{F}_p^\times \rightarrow \{ \pm 1 \}$ is the Legendre character, $\sigma(a) = a^{\frac{p-1}{2}} \pmod{p}$. 

• The subgroup of strictly lower diagonal elements $U \subset Sp$ acts by quadratic exponents (chirps): An element $u = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$, acts by $M_u[f](t) = \psi(-\frac{u}{2}t^2)f(t)$, where $\psi: \mathbb{F}_p \rightarrow \mathbb{C}^\times$ is the character $\psi(t) = e^{\frac{2\pi it}{p}}$.

• The Weyl element $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, acts by discrete Fourier transform $F[f](w) = \frac{1}{\sqrt{p}} \sum_{t \in \mathbb{F}_p} \psi(wt)f(t)$.

Using the Bruhat decomposition we conclude that every operator $\rho(g)$, $g \in Sp$, can be written either in the form $\rho(g) = M_u \circ S_a$ or in the form $\rho(g) = M_u \circ S_a \circ F \circ M_u$, where $M_u$, $S_a$ and $F$ are the explicit operators above.

Example 1. For $g \in R$, with $b \neq 0$, the Bruhat decomposition of $g$ is given explicitly by $g = \begin{pmatrix} 1 & b \cdot u \cdot w \\ 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b^{-1} & 1 \end{pmatrix}$, and consequently $\rho(g) = M_{\frac{1}{b} + \frac{1}{b^{-1}}} \circ S_b \circ F \circ M_{\frac{1}{b^{-1}}}$.

For $g \in R$, with $c = 0$, we have $g = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$, and $\rho(g) = M_u$.

A.3. Pseudocode. Below, is given a pseudo-code description of the construction of the (split) oscillator system $\mathcal{S}_L$.

1. Choose a prime $p$.
2. Compute generator $g_A$ for the standard torus $A$.
3. Diagonalize $\rho(g_A)$ and obtain the basis of eigenfunctions $B_A$.
4. For every $g \in R$:
   (a) Calculate the Bruhat decomposition of $g$, namely, write $g$ in the form $g = u_2 \cdot a \cdot w \cdot u_1$ or $g = u \cdot a$.
   (b) Calculate the operator $\rho(g)$, namely, take $\rho(g) = M_{u_2} \circ S_a \circ F \circ M_{u_1}$ or $\rho(g) = M_u \circ S_a$.
5. Compute the vectors $\rho(g)\varphi$, for every $\varphi \in B_A$ and obtain the system $B_{gA}$.

Remark 3 (Running time). It is easy to verify that the time complexity of the algorithm presented above is $O(p^4 \log p)$. This is, in fact, an optimal time.
**Remark about field extensions.** All the results in this survey were stated for the basic finite field $\mathbb{F}_p$ for the reason of making the terminology more accessible. However, they are valid for any field extension of the form $\mathbb{F}_q$ with $q = p^n$. Complete proofs appear in [6].

**Acknowledgement.** The authors would like to thank J. Bernstein for his interest and guidance in the mathematical aspects of this work. We are grateful to S. Golomb and G. Gong for their interest in this project. We appreciate the many talks we had with A. Sahai. We thank B. Sturmfels for encouraging us to proceed in this line of research. We would like to thank V. Anantharam, A. Grünbaum for interesting conversations. Finally, the second author is indebted to B. Porat for so many discussions where each tried to understand the cryptic terminology of the other.

**References**

[1] Golomb S.W. and Gong G., Signal design for good correlation. For wireless communication, cryptography, and radar. *Cambridge University Press, Cambridge* (2005).

[2] Howard S. D., Calderbank A. R. and Moran W., The finite Heisenberg-Weyl groups in radar and communications. *EURASIP J. Appl. Signal Process.* (2006).

[3] Viterbi A.J., CDMA: Principles of Spread Spectrum Communication. *Addison-Wesley Wireless Communications* (1995).

[4] Paterson, K.G. and Tarokh V., On the existence and construction of good codes with low peak-to-average power ratios. *IEEE Trans. Inform. Theory* 46 (2000).

[5] Howe R., Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indag. Math. (N.S.)* 16 (2005), no. 3-4, 553–583.

[6] Gurevich S., Hadani R. and Sochen N., The finite harmonic oscillator and its applications to sequences, communication and radar. *To appear in IEEE Transactions on Information Theory* (Accepted: March 2008).

[7] Weil A., Sur certains groupes d’operateurs unitaires. *Acta Math.* 111 (1964) 143-211.

[8] Chang R.W., Synthesis of Band-Limited Orthogonal Signals for Multichannel Data Transmission. *Bell System Technical Journal* 45 (1966).

[9] Woodward P.M., Probability and Information theory, with Applications to Radar. *Pergamon Press, New York* (1953).