The finite harmonic oscillator and its associated sequences

Shamgar Gurevich*†‡, Ronny Hadani†§, and Nir Sochen†¶

*Department of Mathematics, University of California, Berkeley, CA 94720; §Department of Mathematics, University of Chicago, Chicago, IL 60637; ¶School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

Communicated by Joseph Bernstein, Tel Aviv University, Tel Aviv, Israel, and approved April 9, 2008 (received for review October 24, 2007)

A system of functions (signals) on the finite line, called the oscillator system, is described and studied. Applications of this system for discrete radar and digital communication theory are explained.

Weil representation | commutative subgroups | eigenfunctions | random behavior | deterministic construction

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. In both situations the parameter of the line is denoted by t and is referred to as *time.* In this work, 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

$$\langle \phi, \varphi \rangle = \sum_{t \in \mathbb{F}_p} \phi(t)\bar{\varphi}(t).$$

A central problem is to construct interesting and useful systems of signals. Given a system $\mathfrak{S}$, there are various desired properties that 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 $\phi \neq \varphi \in \mathfrak{S}$

$$|\langle \phi, \varphi \rangle| \ll 1.$$

This property is trivially satisfied if $\mathfrak{S}$ is an orthonormal basis. Such a system cannot consist of more than $\dim(\mathcal{H})$ signals; however, for certain applications, e.g., code division multiple access (CDMA) (3) a larger number of signals is desired; in that case, the orthogonality condition is relaxed.

During the transmission process, a signal φ might be distorted in various ways. Two basic types of distortions are *time shift* $\varphi(t) \mapsto \mathrm{L}_\tau\varphi(t) = \varphi(t+\tau)$ and *phase shift* $\varphi(t) \mapsto \mathrm{M}_w\varphi(t) = e^{\frac{2\pi i}{p}wt}\varphi(t)$, 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 $\varphi \mapsto \mathrm{M}_w\mathrm{L}_\tau\varphi$, suggesting that for every $\varphi \neq \phi \in \mathfrak{S}$, it is natural to require (1) the following stronger condition

$$|\langle \phi, \mathrm{M}_w\mathrm{L}_\tau\varphi \rangle| \ll 1.$$

Because of technical restrictions in the transmission process, signals are sometimes required to admit low peak-to-average power ratio (4), i.e., that for every $\varphi \in \mathfrak{S}$ 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 $\mathfrak{S}$ by their Fourier transform.

In this article we construct a system of (unit) signals $\mathfrak{S}_O$, consisting of an order of p^3 signals, where p is an odd prime, 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 $\mathfrak{S}_O$ satisfies the following properties

1. *Autocorrelation (ambiguity function).* For every $\varphi \in \mathfrak{S}_O$ we have

$$|\langle \varphi, \mathrm{M}_w\mathrm{L}_\tau\varphi \rangle| = \begin{cases} 1 & \text{if } (\tau, w) = 0, \\ \leq \frac{2}{\sqrt{p}} & \text{if } (\tau, w) \neq 0. \end{cases} \quad [1]$$

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

$$|\langle \phi, \mathrm{M}_w\mathrm{L}_\tau\varphi \rangle| \leq \frac{4}{\sqrt{p}}, \quad [2]$$

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

3. *Supremum.* For every signal $\varphi \in \mathfrak{S}_O$ we have

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

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

In Figs. 1, 2, and 3, the ambiguity function of a signal from the oscillator system is compared with that of random signal and a typical chirp.

Remark 1. Explicit algorithm that generates the oscillator system is given in supporting information (SI) *Appendix*.

The oscillator system can be extended to a much larger system $\mathfrak{S}_E$, consisting of an 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 $\mathrm{M}_w\mathrm{L}_\tau\varphi$ for $\tau, w \in \mathbb{F}_p$, and $\varphi \in \mathfrak{S}_O$. It is not hard to show that $\#(\mathfrak{S}_E) = p^2 \cdot \#(\mathfrak{S}_O) \approx p^5$. As a consequence of Eqs. **1** and **2** for every $\varphi \neq \phi \in \mathfrak{S}_E$ we have

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

Author contributions: S.G., R.H., and N.S. designed research, performed research, contributed new reagents/analytic tools, analyzed data, and wrote the paper.

The authors declare no conflict of interest.

†S.G., R.H., and N.S. contributed equally to this work.

‡To whom correspondence should be addressed. E-mail: shamgar@math.berkeley.edu.

This article contains supporting information online at www.pnas.org/cgi/content/full/0801656105/DCSupplemental.

© 2008 by The National Academy of Sciences of the USA

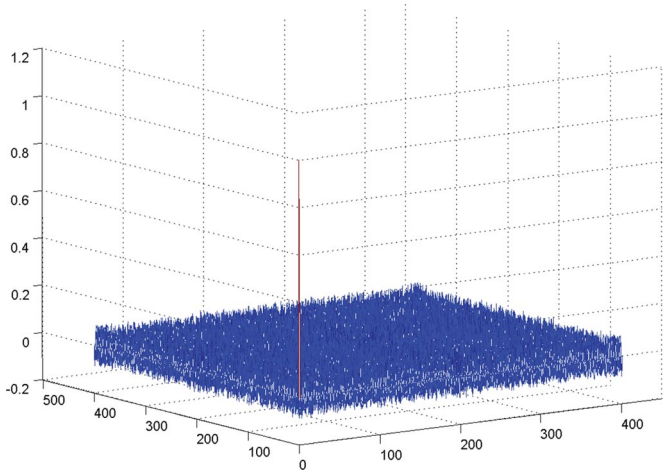

Fig. 1. Ambiguity function of an ''oscillator'' signal.

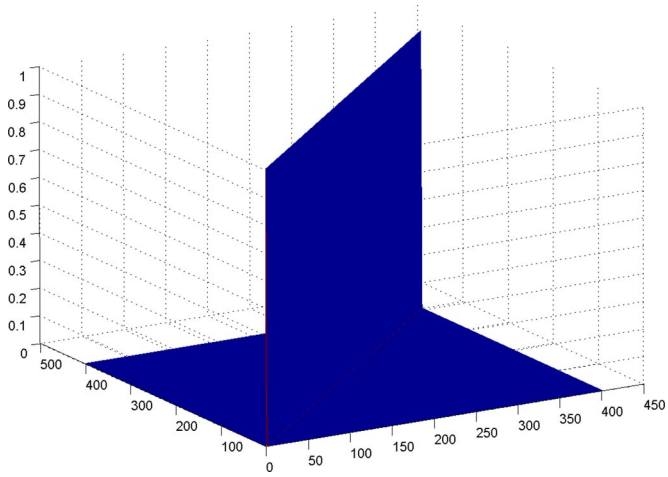

Fig. 3. Ambiguity function of a chirp.

The characterization and construction of the oscillator system is representation theoretic and we devote the rest of the article 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 refs. 2 and 5 for a more comprehensive treatment).

Model Example (Heisenberg System)

Let us denote by $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ the character $\psi(t) = e^{\frac{2\pi i}{p}t}$. 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 $\psi_a(t) = 1/\sqrt{p}\psi(at)$, and δ_a is the Kronecker delta function, $\delta_a(t) = 1$, if $t = a$ and $\delta_a(t) = 0$ if $t \neq a$.

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

Elements of the basis $\Delta^\vee$ are character vectors with respect to the action L, i.e., $\mathrm{L}_\tau\psi_a = \psi(a\tau)\psi_a$ for any $\tau \in \mathbb{F}_p$. In the same fashion, the basis Δ consists of character vectors with respect to the homomorphism $\mathrm{M} : \mathbb{F}_p \to U(\mathrm{H})$ given by the phase shift operators $\mathrm{M}_{w_\varphi}(t) = \psi(t)\varphi(t)$.

The Heisenberg Representation. The homomorphisms L and M can be combined into a single map $\tilde{\pi} : \mathbb{F}_p \times \mathbb{F}_p \to U(\mathcal{H})$ which sends a pair (τ, w) to the unitary operator $\tilde{\pi}(\tau, w) = \psi(-1/2\tau w)\,\mathrm{M}_w \circ \mathrm{L}_\tau$. The plane $\mathbb{F}_p \times \mathbb{F}_p$ is called the time-frequency plane and will be denoted by V. The map $\tilde{\pi}$ is not an homomorphism since, in general, the operators L_τ 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

$$(\tau, w, z)\cdot(\tau', w', z') = \left(\tau + \tau', w + w', z + z' + \frac{1}{2}(\tau w' - \tau' w)\right).$$

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

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

The group H is called the *Heisenberg* group and the homomorphism π is called the *Heisenberg representation.*

Maximal Commutative Subgroups. The Heisenberg group is no longer commutative; however, it contains various commutative subgroups which can be easily described. To every line $L \subset V$ that passes 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.

Bases Associated with Lines. Restricting the Heisenberg representation π 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 χ 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 $\mathcal{B}_L = \{\varphi_\chi : \chi \in L^\vee\}$. In particular, $\Delta^\vee$ and Δ 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 $\mathcal{B}_L$ are certain kind of chirps. Concluding, we associated with every line $L \subset V$ an orthonormal basis $\mathcal{B}_L$, and overall we constructed a system of signals consisting of a union of orthonormal bases

$$\mathfrak{S}_H = \{\varphi \in B_L : L \subset V\}.$$

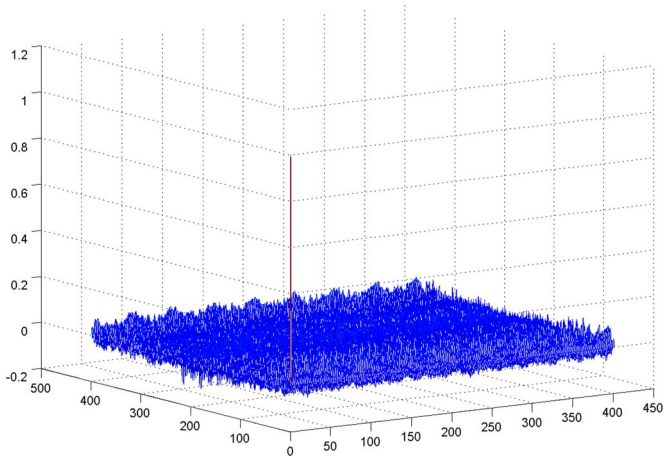

Fig. 2. Ambiguity function of a random signal.

For obvious reasons, the system $\mathfrak{S}_H$ will be called the *Heisenberg* system.

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 $m_{\phi,\varphi} : H \to \mathbb{C}$ given by $m_{\phi,\varphi}(h) = \langle \phi, \pi(h)\varphi \rangle$. In coordinates, if we write $h = (\tau, w, z)$, then $m_{\phi,\varphi}(h) = \psi(-(1/2)\tau w + z)\langle \phi, \mathrm{M}_w \circ \mathrm{L}_\tau \varphi \rangle$. When $\phi = \varphi$ the function $m_{\varphi,\varphi}$ is called the ambiguity function of the vector φ and is denoted by $A_\varphi = m_{\varphi,\varphi}$.

The system $\mathfrak{S}_H$ consists of $p + 1$ orthonormal bases,[‖] altogether $p\,(p + 1)$ signals and it satisfies the following properties (2, 5):

1. *Autocorrelation.* 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. *Crosscorrelation.* 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 $\varphi \in \mathfrak{S}_H$ is a unimodular function, i.e., $|\varphi(t)| = 1/\sqrt{p}$ for every $t \in \mathbb{F}_p$; in particular, we have
$$\max\{|\varphi(t)| : t \in \mathbb{Z}_p\} = \frac{1}{\sqrt{p}} \ll 1.$$

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

The Oscillator System

Reflecting back on the Heisenberg system we see that each vector $\varphi \in \mathfrak{S}_H$ is characterized in terms of action of the additive group $G_a = \mathbb{F}_p$. 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[**] $\chi : G_m \to \mathbb{C}^\times$, we define a vector $\underline{\chi} \in \mathcal{H}$ by
$$\underline{\chi}(t) = \begin{cases} \frac{1}{\sqrt{p-1}}\chi(t), & t \neq 0, \\ 0, & t = 0. \end{cases}$$
We consider the system $\mathcal{B}_{std} = \{\underline{\chi} : \chi \in G_m^\vee, \chi \neq 1\}$, where $G_m^\vee$ is the dual group of characters.

Characterizing the System $\mathcal{B}_{std}$. For each element $a \in G_m$ let $\rho_a : \mathcal{H} \to \mathcal{H}$ be the unitary operator acting by scaling $\rho_a\varphi(t) = \varphi(at)$. This collection of operators form a homomorphism $\rho : G_m \to U(\mathcal{H})$.

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

The Weil Representation. We would like to generalize the system $\mathcal{B}_{std}$ in a similar fashion as we generalized the bases Δ and $\Delta^\vee$ in the Heisenberg setting. To do this we need to introduce several auxiliary operators.

Let $\rho_a : \mathcal{H} \to \mathcal{H}$, $a \in \mathbb{F}_p^\times$, be the operators acting by $\rho_a\varphi(t) = \sigma(a)\varphi(a^{-1}t)$ (scaling), where σ is the unique quadratic character of $\mathbb{F}_p^\times$; let $\rho_T : \mathcal{H} \to \mathcal{H}$ be the operator acting by $\rho_T\varphi(t) = \psi(t^2)\varphi(t)$ (quadratic modulation); and finally, let $\rho_S : \mathcal{H} \to \mathcal{H}$ 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 ν is a normalization constant (6). The operators ρ_a, ρ_T and ρ_S are unitary. Let us consider the subgroup of unitary operators generated by ρ_a, ρ_S, and ρ_T. This group turns out to be isomorphic to the finite group $Sp = SL_2(\mathbb{F}_p)$; therefore, we obtained a homomorphism $\rho : Sp \to U(\mathcal{H})$. The representation ρ is called the *Weil representation* (7) and it will play a prominent role in this article.

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 $\mathcal{H} = \oplus\, \mathcal{H}_\chi$, where χ runs in the set of characters $T^\vee$. Choosing a unit vector $\varphi_\chi \in \mathcal{H}_\chi$ for every χ we obtain a collection of orthonormal vectors $\mathcal{B}_T = \{\varphi_\chi : \chi \in T^\vee, \chi \neq \sigma\}$. Overall, we constructed a system
$$\mathfrak{S}_O^s = \{\varphi \in \mathcal{B}_T : T \subset Sp \text{ split}\},$$
which will be referred to as the *split oscillator system*. We note that our initial system $\mathcal{B}_{std}$ is recovered as $\mathcal{B}_{std} = \mathcal{B}_A$.

Systems Associated with Maximal (Nonsplit) Tori. From the point of view of this article, the most interesting maximal commutative subgroups in Sp are those that are diagonalizable over an extension field rather than over the base field $\mathbb{F}_p$. A subgroup of this type is called maximal *nonsplit 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 nonsplit torus is the circle group $SO(2) \subset SL_2(\mathbb{R})$. Indeed, it is a maximal commutative subgroup that becomes diagonalizable when considered over the extension field $\mathbb{C}$ of complex numbers.

The analogy above suggests a way to construct examples of maximal nonsplit 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
$$B((t, w),(t', w')) = tt' + ww'.$$

[‖] Note that $p + 1$ is the number of lines in V.

[**] A multiplicative character is a function $\chi : G_m \to \mathbb{C}^\times$ which satisfies $\chi(xy) = \chi(x)\chi(y)$ for every $x, y \in G_m$.

An example of maximal nonsplit 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, as in the split case, restricting the Weil representation to a nonsplit torus T yields a decomposition into character spaces $\mathcal{H} = \oplus \mathcal{H}_\chi$. Choosing a unit vector $\varphi_\chi \in \mathcal{H}_\chi$ for every $\chi \in T^\vee$ we obtain an orthonormal basis $\mathcal{B}_T$. Overall, we constructed a system of signals

$$\mathfrak{S}_O^{ns} = \{\varphi \in \mathcal{B}_T : T \subset Sp \text{ nonsplit}\}.$$

The system $\mathfrak{S}_O^{ns}$ will be referred to as the *nonsplit oscillator* system. The construction of the system $\mathfrak{S}_O = \mathfrak{S}_O^s \cup \mathfrak{S}_O^{ns}$, together with the formulation of some of its properties, is the main contribution of this article.

Behavior Under Fourier Transform. The oscillator system is closed under the operation of Fourier transform, i.e., for every $\varphi \in \mathfrak{S}_O$ we have (up to a multiplication by a unitary scalar) that $\hat{\varphi} \in \mathfrak{S}_O$. Indeed, the Fourier transform on the space $\mathbb{C}$ ($\mathbb{F}_p$) appears as a specific operator ρ (w) in the Weil representation, where

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

Given a signal $\varphi \in \mathcal{B}_T \subset \mathfrak{S}_O$, 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, $\mathfrak{S}_O$ 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 consequence, a signal $\varphi \in \mathcal{B}_{T_w}$ and its Fourier transform $\hat{\varphi}$ differ by a unitary constant, and therefore are practically the "same" for all essential matters.

These properties might be relevant for applications to orthogonal frequency division multiplexing (OFDM) (8) where one requires good properties both from the signal and its Fourier transform.

Relation to the Harmonic Oscillator. Here, we give the explanation why functions in the nonsplit oscillator system $\mathfrak{S}_O^{ns}$ 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 $\rho : SO(2, \mathbb{R}) \to U(L^2(\mathbb{R}))$, where $\rho(\theta) = e^{i\theta D}$. Eigenfunctions of D are naturally identified with character vectors with respect to ρ. The crucial point is that ρ is the restriction of the Weil representation of $SL_2(\mathbb{R})$ to the maximal nonsplit torus $SO(2, \mathbb{R}) \subset SL_2(\mathbb{R})$.

Summarizing, the eigenfunctions of the harmonic oscillator and functions in $\mathfrak{S}_O^{ns}$ are governed by the same mechanism, namely, both are character vectors with respect to the restriction of the Weil representation to a maximal nonsplit 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.

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.

Discrete Radar. The theory of discrete radar is closely related (2) to the finite Heisenberg group H. A radar sends a signal $\varphi(t)$ and obtains an echo $e(t)$. The goal (9) is to reconstruct, in maximal accuracy, the target range and velocity. The signal $\varphi(t)$ and the echo $e(t)$ are, in principal, related by the transformation

$$e(t) = e^{2\pi i w t}\varphi(t + \tau) = \mathrm{M}_w \mathrm{L}_\chi \varphi(t),$$

where the time shift τ encodes the distance of the target from the radar and the phase shift encodes the velocity of the target. Equivalently saying, the transmitted signal φ 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 φ 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 φ for discrete radar should admit an ambiguity function A_φ, 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 $\mathfrak{S}_O$ is "large" consisting of approximately p^3 signals. This property becomes important in a *jamming* scenario.

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 Nth 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 $\varphi_i \in \mathcal{H}$ 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 (3) is to extract the individual bits b_i from the message u. The bit b_i can be estimated by calculating the inner product

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

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 $u_i(t) \mapsto e^{\frac{2\pi i}{p}wt}u_i(t)$ and probably also a combination of the two where each message u_i is allowed to acquire an arbitrary distortion of the form $u_i(t) \mapsto e^{\frac{2\pi i}{p}wt}u_i(t + \tau_i)$.

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

Definition 3 (stability conditions). Two unit signals $\phi \neq \varphi$ are called stably cross-correlated if $|m_{\varphi,\psi}(v)| \ll 1$ for every $v \in V$. A unit

signal φ is called stably autocorrelated if $|A_\varphi(v)| \ll 1$, for every $v \neq 0$. A system $\mathfrak{S}$ of signals is called a stable system if every signal $\varphi \in \mathfrak{S}$ is stably autocorrelated and any two different signals $\phi, \varphi \in \mathfrak{S}$ are stably cross-correlated.

Formally what we require for CDMA is a stable system $\mathfrak{S}$. 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 $u_i = b_i e^{\frac{2\pi i}{p} w_i t} \varphi_i(t+\tau_i) = b_i \pi(h_i)\varphi_i$, 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 Eqs. **1** and **2** that the oscillator system $\mathfrak{S}_O$ can support an order of p^3 users, enabling reliable reconstruction when an order of $\sqrt{p}$ users are transmitting simultaneously.

Remark about field extensions. All the results in this article 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 F_q with $q = p^n$. Complete proofs appear in ref. 6.

ACKNOWLEDGMENTS. We thank J. Bernstein for his interest and guidance in the mathematical aspects of this work, S. Golomb and G. Gong for their interest in this project, B. Sturmfels for encouraging us to proceed in this line of research, V. Anantharam, A. Grunbaum and A. Sahai for interesting discussions. Finally, R.H. thanks B. Porat for so many discussions where each tried to understand the cryptic terminology of the other.

1. Golomb SW, Gong G (2005) *Signal Design for Good Correlation. For Wireless Communication, Cryptography, and Radar,* (Cambridge Univ Press, Cambridge).
2. Howard SD, Calderbank AR, Moran W (2006) The finite Heisenberg-Weyl groups in radar and communications. *URASIP J Appl Signal Process* 2006:85685.
3. Viterbi AJ (1995) CDMA: Principles of Spread Spectrum Communication. (Addison-Wesley Wireless Communications) (Prentice Hall, Upper Saddle River, NJ).
4. Paterson KG, Tarokh V (2000). On the existence and construction of good codes with low peak-to-average power ratios. *IEEE Trans Inform Theory* 46:1974–1987.
5. Howe R (2005) Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indag Math (NS)* 16(3–4):553–583.
6. Gurevich S, Hadani R, Sochen N (2008) The finite harmonic oscillator and its applications to sequences, communication and radar. *IEEE Trans Inform Theory,* in press.
7. Weil A (1964). Sur certains groupes d'operateurs unitaires. *Acta Math* 111:143–211.
8. Chang RW (1966) Synthesis of band-limited orthogonal signals for multi-channel data transmission. *Bell System Tech J* 45:1775–1796.
9. Woodward PM (1953) *Probability and Information Theory, with Applications to Radar* (Pergamon Press, New York).