Delay-Doppler Channel Estimation with Almost Linear Complexity

Alexander Fish, Shamgar Gurevich, Ronny Hadani, Akbar Sayeed, and Oded Schwartz

To Solomon Golomb for the occasion of his 80 birthday mazel tov

***Abstract*—A fundamental task in wireless communication is *channel estimation*: Compute the channel parameters a signal undergoes while traveling from a transmitter to a receiver. In the case of delay-Doppler channel, a widely used method is the *matched filter* algorithm. It uses a pseudo-random sequence of length N, and, in case of non-trivial relative velocity between transmitter and receiver, its computational complexity is $O(N^2 \log N)$. In this paper we introduce a novel approach of designing sequences that allow faster channel estimation. Using group representation techniques we construct sequences, which enable us to introduce a new algorithm, called the *flag method,* that significantly improves the matched filter algorithm. The flag method finds the channel parameters in $O(m \cdot N \log N)$ operations, for channel of sparsity m. We discuss applications of the flag method to GPS, radar system, and mobile communication as well.**

***Index Terms*—Channel estimation, time-frequency shift problem, fast matched filter, flag method, sequence design, Heisenberg–Weil sequences, fast moving users, high-frequency communication, radar, GPS.**

I. Introduction

A BASIC step in many wireless communication protocols [16] is *channel estimation*: learning the channel parameters a signal undergoes while traveling from a transmitter to a receiver. In this paper we develop an efficient algorithm for delay-Doppler (also called time-frequency) channel estimation. Our algorithm provides a striking improvement over current methods in the presence of high relative velocity between a transmitter and a receiver. The latter scenario occurs in GPS, radar systems, mobile communication of fast moving users, and very high frequency (GHz) communication.

Throughout this paper we denote by $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ the vector space of complex valued functions on the set of integers $\mathbb{Z}_N = \{0, 1, ..., N-1\}$ equipped with addition and multiplication modulo N. We assume that N is an odd prime number. The vector space $\mathcal{H}$ is endowed with the inner product

$$\langle f_1, f_2 \rangle = \sum_{n \in \mathbb{Z}_N} f_1[n] \overline{f_2[n]},$$

for $f_1, f_2 \in \mathcal{H},$ and referred to as the *Hilbert space of (digital) sequences*.

A. Fish is with School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia. Email: alexander.fish@sydney.edu.au.

S. Gurevich is with the Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA. Email: shamgar@math.wisc.edu.

R. Hadani is with the Department of Mathematics, University of Texas, Austin, TX 78712, USA. Email: hadani@math.utexas.edu.

A. Sayeed is with the Department of Electrical and Computer Engineering, University of Wisconsin, Madison, WI 53706, USA. Email: akbar@engr.wisc.edu.

O. Schwartz is with the Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA 94720, USA. Email: odedsc@eecs.berkeley.edu.

Let us start with example.

A. *Example: The GPS Problem*

A client on the earth surface wants to know his/her geographical location. The Global Positioning System (GPS) was built to fulfill this task. Its mathematical model works as follows [12]. Satellites send to earth their location—see Figure 1 for illustration.

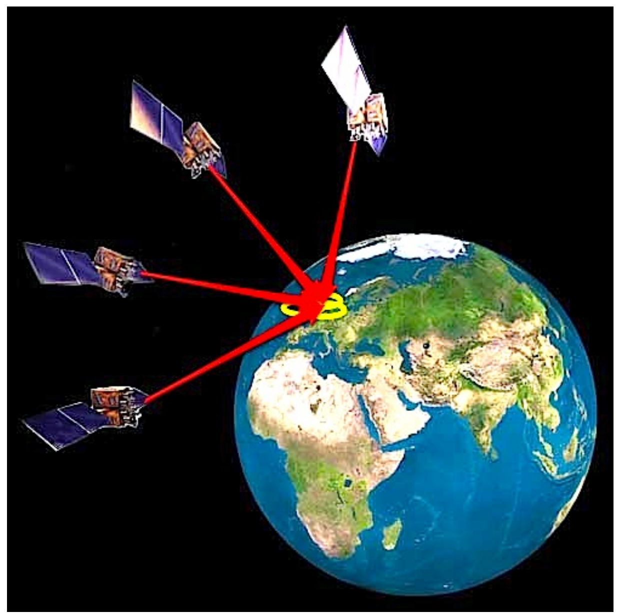

Fig. 1. Satellites communicate location in GPS.

For simplicity, the location of a satellite is a bit $b \in \{\pm 1\}$. The satellite transmits to the earth its sequence $S \in \mathcal{H}$ of norm one multiplied by its location b. We assume, for simplicity, that the sequence travels through only one path. Hence, the client receives the sequence $R \in \mathcal{H}$ of the form[1]

$$R[n] = b \cdot \alpha_0 \cdot e^{\frac{2\pi i}{N} \omega_0 \cdot n} \cdot S[n + \tau_0] \ + \mathcal{W}[n], \qquad \text{(I-A.1)}$$

where $\alpha_0 \in \mathbb{C}$ is the *complex amplitude,* with $|\alpha_0| \leq 1$, $\omega_0 \in \mathbb{Z}_N$ encodes the radial velocity of the satellite with respect to the client, $\tau_0 \in \mathbb{Z}_N$ encodes the distance between the satellite and the client[2], and $\mathcal{W}$ is a random white noise[3]. The problem of GPS

[1] We denote $i = \sqrt{-1}$.

[2] Using τ_0 we can compute [12] the distance from the satellite to the client, assuming a line of sight between them.

[3] In this paper, a random white noise will always be assumed to have mean zero.

can be formulated as follows:

*Problem I-A.1 (**The GPS Problem**):* Design $S \in \mathcal{H}$, and an effective method of extracting (b, τ_0) from S and R satisfying (I-A.1).

In practice, the satellite transmits $S = S_1 + b \cdot S_2$, where S_1, S_2 are almost orthogonal in some appropriate sense. Then $(\alpha_0, \tau_0, \omega_0)$, and $(b \cdot \alpha_0, \tau_0, \omega_0)$ are computed using S_1, and S_2, respectively, concluding with the derivation of the bit b. A client can compute his/her location by knowing the locations of at least three satellites and distances to them. The GPS problem is an example of channel estimation task. We would like now to describe the more general channel estimation problem that we are going to solve.

B. Channel Estimation Problem

We consider the following mathematical model of time-frequency channel estimation [16]. There exists a collection of users, each one holds a sequence from $\mathcal{H}$ known to a base station (receiver). The users transmit their sequences to the base station. Due to multipath effects—see Figure 2 for illustration—the sequences undergo [15], [16] several time-frequency shifts as a result of reflections from various obstacles. We make the standard assumption of almost-orthogonality between sequences of different users. Hence, if a user transmits $S \in \mathcal{H}$, then the base station receives $R \in \mathcal{H}$ of the form

$$R[n] = \sum_{k=1}^{m} \alpha_k \cdot e^{\frac{2\pi i}{N}\omega_k \cdot n} \cdot S[n+\tau_k] + \mathcal{W}[n], \quad n \in \mathbb{Z}_N, \quad \text{(I-B.1)}$$

where m denotes the number of paths the transmitted sequence traveled, $\alpha_k \in \mathbb{C}$ is the *complex multipath amplitude* along path k, with $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\omega_k \in \mathbb{Z}_N$ depends on the relative velocity along path k of the transmitter with respect to a base station, $\tau_k \in \mathbb{Z}_N$ encodes the delay along path k, and $\mathcal{W} \in \mathcal{H}$ denotes a random white noise. The parameter m will be called the *sparsity* of the channel. The objective is:

*Problem I-B.1 (**The Channel Estimatiom Problem**):* Design $S \in \mathcal{H}$, and an effective method of extracting the channel parameters $(\alpha_k, \tau_k, \omega_k)$, $k = 1, ..., m$, from S and R satisfying (I-B.1).

To suggest a solution to Problem I-B.1, we start with a simpler variant.

C. The Time-Frequency Shift (TFS) Problem

Suppose the transmitter and the receiver sequences $S, R \in \mathcal{H}$ are related by

$$R[n] = e^{\frac{2\pi i}{N}\omega_0 \cdot n} \cdot S[n+\tau_0] + \mathcal{W}[n], \quad n \in \mathbb{Z}_N, \quad \text{(I-C.1)}$$

where $\mathcal{W} \in \mathcal{H}$ denotes a random white noise, and $(\tau_0, \omega_0) \in \mathbb{Z}_N \times \mathbb{Z}_N$. The pair (τ_0, ω_0) is called the *time-frequency shift*, and the vector space $V = \mathbb{Z}_N \times \mathbb{Z}_N$ is called the *time-frequency plane*. We would like to solve the following:

*Problem I-C.1 (**Time-Frequency Shift (TFS)**):* Design $S \in \mathcal{H}$, and an effective method of extracting the time-frequency shift (τ_0, ω_0) from S and R satisfying (I-C.1).

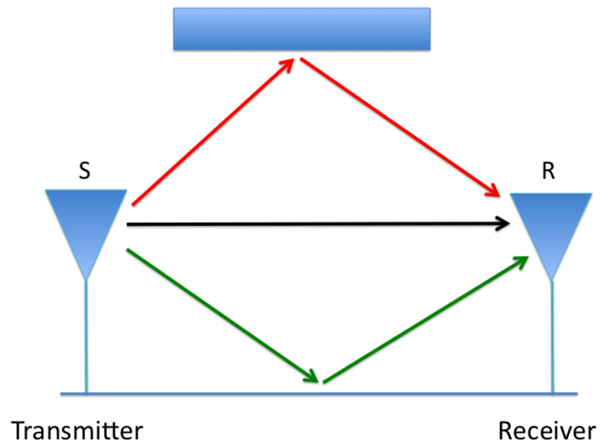

Fig. 2. Three paths scenario.

D. The Matched Filter (MF) Algorithm

A classical solution [6], [8], [9], [11], [16], [17], [18] to Problem I-C.1, is the *matched filter algorithm*. We define the following matched filter (MF) matrix of R and S:

$$\mathcal{M}(R,S)[\tau,\omega] = \left\langle R[n], e^{\frac{2\pi i}{N}\omega \cdot n} \cdot S[n+\tau] \right\rangle, \quad (\tau,\omega) \in V.$$

A direct verification shows that for $\zeta_0 = e^{\frac{2\pi i}{N}(\tau\omega_0 - \omega\tau_0)}$, with probability one, we have

$$\begin{aligned} \mathcal{M}(R,S)[\tau,\omega] &= \zeta_0 \cdot \mathcal{M}(S,S)[\tau-\tau_0, \omega-\omega_0] \\ &\quad + O(\frac{NSR}{\sqrt{N}}), \end{aligned}$$

where $NSR \approx \frac{1}{SNR}$, i.e., essentially[4] the inverse of the signal-to-noise ratio between the sequences S and $\mathcal{W}$. For simplicity, we assume, for the rest of the paper, that the NSR is of size $O(1)$. In order to extract the time-frequency shift (τ_0, ω_0), it is "standard"[5] (see [6], [8], [9], [11], [16], [17], [18]) to use pseudo-random sequence $S \in \mathcal{H}$ of norm one. In this case $\mathcal{M}(S,S)[\tau - \tau_0, \omega - \omega_0] = 1$ for $(\tau, \omega) = (\tau_0, \omega_0)$, and of order $O(\frac{1}{\sqrt{N}})$ if $(\tau, \omega) \neq (\tau_0, \omega_0)$. Hence,

$$\mathcal{M}(R,S)[\tau,\omega] = \begin{cases} 1 + \varepsilon_N, & \text{if } (\tau,\omega) = (\tau_0,\omega_0); \\ \varepsilon_N, & \text{if } (\tau,\omega) \neq (\tau_0,\omega_0), \end{cases} \quad \text{(I-D.1)}$$

where $\varepsilon_N = O(\frac{1}{\sqrt{N}})$.

Identity (I-D.1)—see Figure 3 for a demonstration—suggests the following "entry-by-entry" solution to TFS problem: Compute the matrix $\mathcal{M}(R,S)$, and choose (τ_0, ω_0) for which $\mathcal{M}(R,S)[\tau_0, \omega_0] \approx 1$. However, this solution of TFS problem is significantly expensive in terms of arithmetic complexity, i.e., the number of multiplication and addition operations is $O(N^3)$. One can do better using a "line-by-line" computation. This is due to the next observation.

[4]The precise relation is $NSR = \frac{\sqrt{2\log\log N}}{SNR}$ by the *law of the iterated logarithm.*

[5]For example in spread-spectrum communication systems.

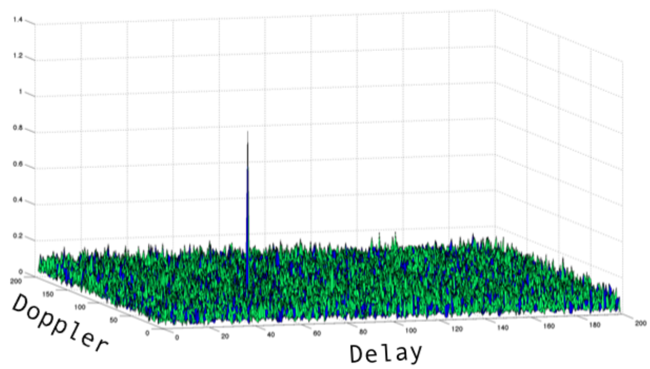

Fig. 3. $|\mathcal{M}(R,S)|$ with pseudo-random S, and $(\tau_0,\omega_0)=(50,50)$.

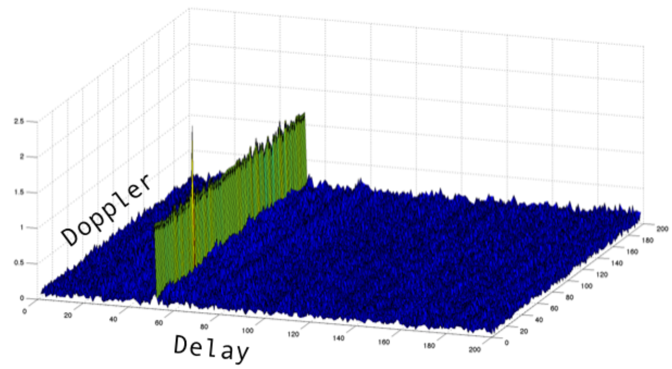

Fig. 4. $|\mathcal{M}(R,S_L)|$ for a flag S_L with $L=\{(0,\omega)\}$, and $(\tau_0,\omega_0)=(50,50)$.

*Remark I-D.1 (**FFT**):* The restriction of the matrix $\mathcal{M}(R,S)$ to any line (not necessarily through the origin) in the time-frequency plane V, is a convolution that can be computed, using the fast Fourier transform (FFT), in $O(N\log N)$ operations. For details see Section V.

As a consequence of Remark I-D.1, one can solve TFS problem in $O(N^2\log N)$ operations.

E. *The Fast Matched Filter (FMF) Problem*

To the best of our knowledge, the "line-by-line" computation is also the fastest known method [14]. If N is large this may not suffice. For example in applications to GPS [1], as in Problem I-A.1 above, we have $N\geq 1000$. This leads to the following:

*Problem I-E.1 (**The Fast Matched Filter Problem**):* Solve the TFS problem in almost linear complexity.

Note that computing one entry in $\mathcal{M}(R,S)$ already takes $O(N)$ operations.

F. *The Flag Method*

In this paper we introduce the *flag method* to propose a solution to FMF problem. The idea is, first, to find a line on which the time-frequency shift is located, and, then, to search on the line to find the time-frequency shift. We associate with the $N+1$ lines L_j, $j=1,...,N+1$, through the origin in V, a system of "almost orthogonal" sequences $S_{L_j}\in\mathcal{H}$, that we call *flags*. They satisfy—see Figure 4 for illustration—the following "flag property"[6]: For a sequence R given by (I-C.1) with $S=S_{L_j}$, we have

$$\mathcal{M}(R,S_{L_j})[\tau,\omega] \tag{I-F.1}$$
$$=\begin{cases} 2+\varepsilon_N, & \text{if } (\tau,\omega)=(\tau_0,\omega_0);\\ 1+\varepsilon_N, & \text{in } |\cdot| \text{ if } (\tau,\omega)\in L_j'\smallsetminus(\tau_0,\omega_0);\\ \varepsilon_N, & \text{if } (\tau,\omega)\in V\smallsetminus L_j', \end{cases}$$

where $\varepsilon_N=O(\frac{1}{\sqrt{N}})$, $|\cdot|$ denotes absolute value, and L_j' is the shifted line $L_j+(\tau_0,\omega_0)$. The "almost orthogonality" of sequences means $\left|\mathcal{M}(S_{L_i},S_{L_j})[\tau,\omega]\right| = O(\frac{1}{\sqrt{N}})$, for every (τ,ω), $i\neq j$.

In addition, for S_L and R satisfying (I-F.1), we have the following search method to solve FMF problem:

Flag Algorithm

Step 1. Choose a line $L^\perp$ transversal to L.

Step 2. Compute $\mathcal{M}(R,S_L)$ on $L^\perp$. Find (τ,ω) such that $|\mathcal{M}(R,S_L)[\tau,\omega]|\approx 1$, i.e., (τ,ω) on the shifted line $L+(\tau_0,\omega_0)$.

Step 3. Compute $\mathcal{M}(R,S_L)$ on $L+(\tau_0,\omega_0)$ and find (τ,ω) such that $|\mathcal{M}(R,S_L)[\tau,\omega]|\approx 2$.

The complexity of the flag algorithm—see Figure 5 for a demonstration—is $O(N\log N)$, using the FFT.

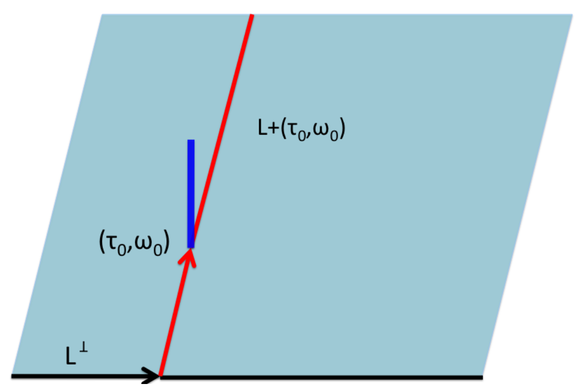

Fig. 5. Diagram of flag algorithm.

This completes our solution of Problem I-E.1—The Fast Matched Filter Problem.

G. *Solution to the GPS and Channel Estimation Problems*

Let $L\subset V$ be a line through the origin.

*Definition I-G.1 (**Genericity**):* We say that the points $(\tau_k,\omega_k)\in V$, $k=1,...,m$, are *L-generic* if no two of them lie on a shift of L, i.e., on $L+v$, for some $v\in V$.

[6] In linear algebra, a pair (ℓ_0,L) consisting of a line $L\subset V$, and a point $\ell_0\in L$, is called a *flag*.

Looking back to Problem I-B.1, we see that, under genericity assumptions, the flag method provides a fast computation, in $O(m \cdot N \log N)$ operations, of the channel parameters of channel with sparsity m In particular, it calculates the GPS parameters—see Problem I-A.1—in $O(N \log N)$ operations. Indeed, Identity (I-F.1), together with the almost orthogonality between flag sequences, implies that

$$\alpha_k \approx \mathcal{M}(R, S_L)[\tau_k, \omega_k]/2, \quad k = 1, ..., m,$$

where R is the sequence (I-B.1), with $S = S_L$, assuming that and (τ_k, ω_k)'s are L-generic. So we can adjust the flag algorithm as follows:

- Compute $\mathcal{M}(R, S_L)$ on $L^{\perp}$. Find all (τ, ω)'s such that $|\mathcal{M}(R, S_L)[\tau, \omega]|$ is sufficiently large, i.e., find all the shifted lines $L + (\tau_k, \omega_k)$'s.
- Compute $\mathcal{M}(R, S_L)$ on each line $L + (\tau_k, \omega_k)$, and find (τ, ω) such that $|\mathcal{M}(R, S_L)[\tau, \omega]|$ is maximal on that line, i.e., $(\tau, \omega) = (\tau_k, \omega_k)$ and $\alpha_k \approx \mathcal{M}(R, S_L)[\tau_k, \omega_k]/2$.

Figure 6 provides a visual illustration for the matched filter matrix in three paths scenario.

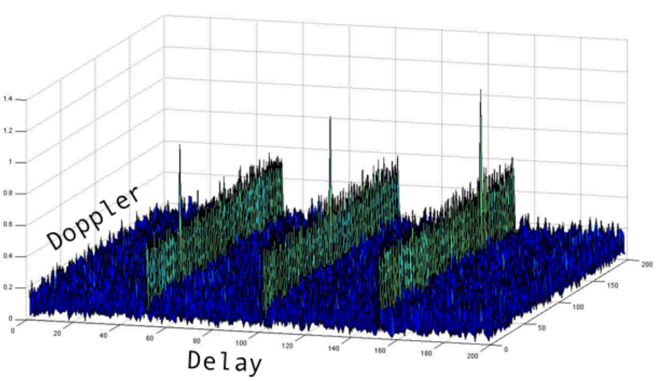

Fig. 6. $|\mathcal{M}(R, S_L)|$, for $L = \{(0, \omega)\}$, and $(\alpha_k, \tau_k, \omega_k) = (\frac{1}{\sqrt{3}}, 50k, 50k)$, $k = 1, 2, 3$.

This completes our solutions of Problem I-B.1—The Channel Estimation Problem, and of Problem I-A.1—The GPS Problem.

H. Applications to Radar and Mobile Communication

The flag method provides a significant improvement over the current channel estimation algorithms in the presence of high velocities. The latter occurs in systems such as GPS, radar, and mobile communication of fast moving users. In Subsection I-A, we described the GPS problem, and in Subsection I-G its effective solution using the flag method. It is easy to see that the flag method suggests a solution to the GPS problem also in the multipath scenario. In this section we demonstrate application of the flag method to radar, and mobile communication.

*1) **Application to Radar**:* The model of radar works as follows [11]. A radar transmits—Figure 7 illustrates the case of one target—a sequence $S \in \mathcal{H}$ which bounces back from m targets. The sequence $R \in \mathcal{H}$ which is received as an echo has the form

$$R[n] = \sum_{k=1}^{m} \alpha_k \cdot e^{\frac{2\pi i}{N}\omega_k \cdot n} \cdot S[n + \tau_k] + \mathcal{W}[n], \ n \in \mathbb{Z}_N,$$

where $\alpha_k \in \mathbb{C}$ is the complex multipath amplitude along path k, with $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\omega_k \in \mathbb{Z}_N$ encodes the radial velocity of target k with respect to the radar, $\tau_k \in \mathbb{Z}_N$ encodes the distance between target k and the radar, and $\mathcal{W}$ is a random white noise.

In order to determine the location of the targets we need to solve [13] the following.

*Problem I-H.1 (**The Radar Problem**):* Having R and S, compute the parameters (τ_k, ω_k), $k = 1, ..., m$.

This is essentially the channel estimation problem. Under the genericity assumption, the flag method solves it in $O(m \cdot N \log N)$ operations. This completes our solution to Problem I-H.1—The Radar Problem.

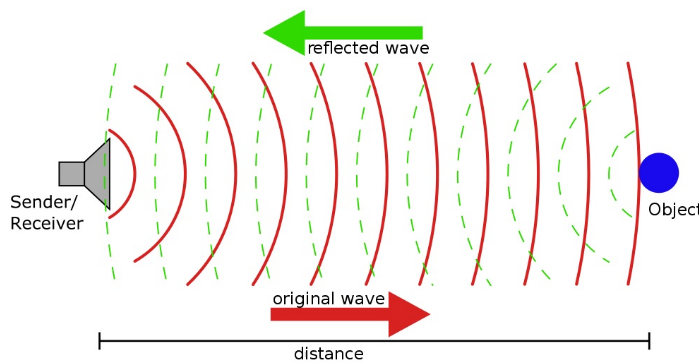

Fig. 7. Radar transmits wave and recieves echo.

*2) **Application to Mobile Communication**:* The model of mobile communication works as follows [16]. A user wants to deliver a bit of information $b \in \{\pm 1\}$ to a base station. The base station assigns a sequence $S \in \mathcal{H}$ to the user, and the user transmits to the base station the sequence $b \cdot S$. The sequence $R \in \mathcal{H}$ which is received by the base station is of the form

$$R[n] = b \cdot \sum_{k=1}^{m} \alpha_k \cdot e^{\frac{2\pi i}{N}\omega_k \cdot n} \cdot S[n + \tau_k] + \mathcal{W}[n], \quad n \in \mathbb{Z}_N,$$

where m denotes the number of paths the transmitted sequence traveled, $\alpha_k \in \mathbb{C}$ is the multipath amplitude along path k, with $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\omega_k \in \mathbb{Z}_N$ depends on the relative velocity along path k of the user with respect to the base station, $\tau_k \in \mathbb{Z}_N$ is the delay along path k, and $\mathcal{W} \in \mathcal{H}$ denotes a random white noise. The main task at the base station is the following:

*Problem I-H.2 (**The Mobile Communication Problem**):* Having R and S, compute the bit b.

In practice, first the user sends S, and the channel estimation is done. Then the bit b is communicated by sending $b \cdot S$. Finally, knowing the channel parameters $(\alpha_k, \tau_k, \omega_k)$, $k = 1, ..., m$, the bit is extracted using the formula[7]

$$b \cdot \sum_{k=1}^{m} |\alpha_k|^2 \approx \langle R, \sum_{k=1}^{m} \alpha_k \cdot e^{\frac{2\pi i}{N}\omega_k \cdot n} \cdot S[n+\tau_k] \rangle.$$

The main computational step is the channel estimation which is done by flag method in $O(m{\cdot}N \log N)$ operations. This completes our solution to Problem I-H.2—The Mobile Communication Problem.

I. *What you can find in this paper*

- *In Section I:* You can read about the flag method for effective delay-Doppler channel estimation. In addition, concrete applications to GPS, radar, and mobile communication are discussed.
- *In Section II:* You can find the definition and explicit formulas for the Heisenberg and Weil operators. These operators are our basic tool in the development of the flag method, in general, and the flag sequences, in particular.
- *In Section III:* You can see the design of the Heisenberg–Weil flag sequences, using the Heisenberg–Weil operators, and diagonalization techniques of commuting operators. In addition, the investigation of the correlation properties of the flag sequences is done in this section. These properties are formulated in Theorem III-C.1, which guarantees applicability of the Heisenberg-Weil sequences to the flag method.
- *In Section IV:* You can get explicit formulas for large collection of the Heisenberg–Weil flag sequences. In particular, these formulas enable to generate the sequences using low complexity algorithm.
- *In Section V:* You can find the formulas that suggest fast computation of the matched filter matrix on any line in the time-frequency plane. These formulas are of crucial importance for the effectiveness of the flag method.
- *In Section VI:* You can find needed proofs and justifications for all the claims and formulas that appear in the body of the paper.

Acknowledgement. Warm thanks to J. Bernstein for his support and encouragement in interdisciplinary research. We are grateful to A. Sahai, for sharing with us his thoughts, and ideas on many aspects of signal processing and wireless communication. The project described in this paper was initiated by a question of M. Goresky and A. Klapper during the conference SETA2008, we thank them very much. We appreciate the support and encouragement of N. Boston, R. Calderbank, S. Golomb, G. Gong, O. Holtz, R. Howe, P. Sarnak, N. Sochen, D. Tse, and A. Weinstein. The research reported in this paper was partially supported by NSF Grants DMS-1101660, and DMS-1101698.

II. The Heisenberg and Weil Operators

The flag sequences (see Subsection I-F) are defined, constructed and analyzed using two special classes of operators that act on the Hilbert space of digital sequences. The first class consists of the Heisenberg operators and is a generalization of the time-shift and frequency-shift operators. The second class consists of the Weil operators and is a generalization of the discrete Fourier transform. In this section we recall the definitions and explicit formulas of these operators.

A. *The Heisenberg Operators*

The Heisenberg operators are the unitary transformations that act on the Hilbert space of digital sequences by

$$\begin{cases} \pi(\tau,\omega) : \mathcal{H} \to \mathcal{H}, \quad \tau,\omega \in \mathbb{Z}_N; \\ [\pi(\tau,\omega)f][n] = e^{\frac{2\pi i}{N}\omega \cdot n} \cdot f[n+\tau], \end{cases} \quad \text{(II-A.1)}$$

for every $f \in \mathcal{H}$, $n \in \mathbb{Z}_N$.

B. *The Weil Operators*

Consider the discrete Fourier transform

$$\begin{cases} DFT : \mathcal{H} \to \mathcal{H}, \\ [DFT(f)][\omega] = \frac{1}{\sqrt{N}} \sum\limits_{n=0}^{N-1} e^{-\frac{2\pi i}{N}\omega \cdot n} \cdot f[n], \end{cases}$$

for every $f \in \mathcal{H}$, $\omega \in \mathbb{Z}_N$. It is easy to check that DFT satisfies the following N^2 identities:

$$DFT \circ \pi(\tau,\omega) = \pi(-\omega,\tau) \circ DFT, \quad \tau,\omega \in \mathbb{Z}_N, \quad \text{(II-B.1)}$$

where $\pi(\tau,\omega)$ are the Heisenberg operators, and $\circ$ denotes composition of transformations. A version of the celebrated Stone–von Neumann (S–vN) theorem implies that up to scalar multiple the DFT is the unique operator that satisfies (II-B.1). This means that (II-B.1) is a characterization of the DFT. In [19] Weil generalized this method and defined many other operators that act on $\mathcal{H}$. Consider the following collection of matrices

$$SL_2(\mathbb{Z}_N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a,b,c,d \in \mathbb{Z}_N, \text{ and } ad - bc = 1 \right\}.$$

Note that $G = SL_2(\mathbb{Z}_N)$ is a *group* [2] with respect to the operation of matrix multiplication. It is called the *special linear group* of order two over $\mathbb{Z}_N$. Each element

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G,$$

acts on the time-frequency plane $V = \mathbb{Z}_N \times \mathbb{Z}_N$ via the change of coordinates

$$(\tau,\omega) \mapsto g \cdot (\tau,\omega) = (a\tau + b\omega, c\tau + d\omega).$$

For $g \in G$, let $\rho(g)$ be a linear operator on $\mathcal{H}$ which is a solution of the following system of N^2 linear equations:

$$\Sigma_g : \ \rho(g) \circ \pi(\tau,\omega) = \pi(g \cdot (\tau,\omega)) \circ \rho(g), \quad \tau,\omega \in \mathbb{Z}_N, \quad \text{(II-B.2)}$$

Denote by $\mathrm{Sol}(\Sigma_g)$ the space of all solutions to System (II-B.2). For example for

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

which is called the *Weyl* element, we have by (II-B.1) that $DFT \in \mathrm{Sol}(\Sigma_{\mathrm{w}})$. The general version of the S–vN theorem implies that $\dim \mathrm{Sol}(\Sigma_g) = 1$, for every $g \in G$. In fact there exists a special set of solutions. This is the content of the following result [19]:

[7]It is analogous to data modulation using a delay-Doppler rake receiver in spread-spectrum systems [16].

*Theorem II-B.1 (**Weil operators**):* There exists a unique collection of solutions $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\ \ g \in G\}$, which are unitary operators, and satisfy the homomorphism condition $\rho(g \cdot h) = \rho(g) \circ \rho(h)$, for every $g, h \in G$.

Denote by $U(\mathcal{H})$ the collection of all unitary operators on the Hilbert space $\mathcal{H}$ of digital sequences. Theorem II-B.1 establishes the map

$$\rho : G \to U(\mathcal{H}), \tag{II-B.3}$$

which is called the *Weil representation* [19]. We will call each $\rho(g)$, $g \in G$, a *Weil operator.*

*1) **Formulas for Weil Operators**:* It will be important for our study to have the following [5], [7] explicit formulas for the Weil operators:

- *Fourier.* We have
$$\left[\rho\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} f\right][n] = i^{\frac{N-1}{2}} \cdot DFT(f)[n]; \tag{II-B.4}$$
- *Chirp.* We have
$$\left[\rho\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} f\right][n] = e^{\frac{2\pi i}{N}(-2^{-1}cn^2)} \cdot f[n]; \tag{II-B.5}$$
- *Scaling. We have*
$$\left[\rho\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} f\right][n] = \left(\frac{a}{N}\right) f[a^{-1}n], \tag{II-B.6}$$

for every $f \in \mathcal{H},\ \ 0 \neq a, c, n \in \mathbb{Z}_N$, where $\left(\frac{a}{N}\right)$ is the *Legendre symbol* which is equal to 1 if a is a square modulo N, and -1 otherwise, and in (II-B.5) we denote $2^{-1} = \frac{N+1}{2}$ the inverse of 2 modulo N.

The group G admits [3] the *Bruhat decomposition*

$$G = UA \cup U\mathrm{w}UA,$$

where $U \subset G$ denotes the *unipotent* subgroup

$$U = \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix};\ \ c \in \mathbb{Z}_N \right\},$$

and $A \subset G$ denotes the *diagonal* subgroup

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix};\ \ 0 \neq a \in \mathbb{Z}_N \right\}. \tag{II-B.7}$$

This means that every element $g \in G$ can be written in the form

$$g = u \cdot s \quad \text{or} \quad g = u' \cdot \mathrm{w} \cdot u'' \cdot s'$$

where $u, u', u'' \in U$, $s, s' \in A$, and w is the Weyl element. Hence, because ρ is homomorphism, i.e., $\rho(g \cdot h) = \rho(g) \circ \rho(h)$ for every $g, h \in G$, we deduce that formulas (II-B.4), (II-B.5), and (II-B.6), extend to describe all the Weil operators.

III. Sequence Design: Heisenberg–Weil Flags

The flag sequences, that play the main role in the flag method, are of a special type. Each of them is a sum of a pseudorandom sequence and a structural sequence. The first has the MF matrix which is almost delta function at the origin, and the MF matrix of the second is supported on a line. The design of these sequences is done using group representation theory. The pseudorandom sequences are designed [8], [9], [18] using the Weil representation operators (II-B.3), and will be called *Weil (spike) sequences*[8]. The structural sequences are designed [10], [11] using the Heisenberg representation operators (II-A.1), and will be called *Heisenberg (line) sequences.* We call the collection of all flag sequences, the Heisenberg–Weil flag system. In this section we study constructions, and properties of these sequences.

A. *The Heisenberg (Lines) System*

The operators (II-A.1) obey the Heisenberg commutation relations

$$\pi(\tau,\omega) \circ \pi(\tau',\omega') = e^{\frac{2\pi i}{N}(\tau\omega' - \omega\tau')} \cdot \pi(\tau',\omega') \circ \pi(\tau,\omega).$$

The expression $\tau\omega' - \omega\tau'$ vanishes if (τ,ω), (τ',ω') are on the same line through the origin. Hence, for a given line $L \subset V = \mathbb{Z}_N \times \mathbb{Z}_N$ we have a commutative collection of unitary operators

$$\pi(\ell) : \mathcal{H} \to \mathcal{H},\ \ell \in L. \tag{III-A.1}$$

Explicit version of simultaneous diagonalization theorem from linear algebra implies [10], [11] the existence of a natural orthonormal basis $\mathcal{B}_L$ for $\mathcal{H}$ consisting of common eigensequences for all the operators (III-A.1)

$$\begin{cases} \qquad \mathcal{B}_L = \{f_{L_\psi}\}; \\ \pi(\ell) f_{L_\psi} = \psi(\ell) f_{L_\psi}, \quad \ell \in L, \end{cases}$$

where ψ runs over *characters* of L, i.e., functions $\psi : L \to \mathbb{C}^* = \mathbb{C} - 0$, with $\psi(\ell + \ell') = \psi(\ell)\psi(\ell')$, for every $\ell, \ell' \in L$. The system of all such bases $\mathcal{B}_L$, where L runs over all lines through the origin in V, will be called the *Heisenberg (lines) system*. We use the following result [10], [11]:

Theorem III-A.1: The Heisenberg system satisfies the following properties:

1) *Line.* For every line $L \subset V$, and every $f_L \in \mathcal{B}_L$, we have
$$\mathcal{M}(f_L, f_L)[\tau,\omega] = \begin{cases} 1, \text{ if } (\tau,\omega) = (0,0); \\ 1, \text{ in } |\cdot| \text{ if } (\tau,\omega) \in L \smallsetminus (0,0); \\ 0, \text{ if } (\tau,\omega) \notin L. \end{cases}$$
2) *Almost-orthogonality.* For every two lines $L_1 \neq L_2 \subset V$, and every $f_{L_1} \in \mathcal{B}_{L_1}$, $f_{L_2} \in \mathcal{B}_{L_2}$, we have
$$|\mathcal{M}(f_{L_1}, f_{L_2})[\tau,\omega]| = \frac{1}{\sqrt{N}},$$
for every $(\tau,\omega) \in V$.

Figure 8 demonstrates Property 1 of Theorem III-A.1 for the diagonal line.

B. *The Weil (Spikes) System*

The group $G = SL_2(\mathbb{Z}_N)$ is non-commutative, but contains a special class of maximal commutative subgroups called tori[9] [8], [9], [3]. Each torus $T \subset G$ acts via the Weil operators

$$\rho(g) : \mathcal{H} \to \mathcal{H},\ \ g \in T. \tag{III-B.1}$$

[8]For the purpose of the Flag method, other pseudorandom signals may work.
[9]There are order of N^2 tori in $SL_2(\mathbb{Z}_N)$.

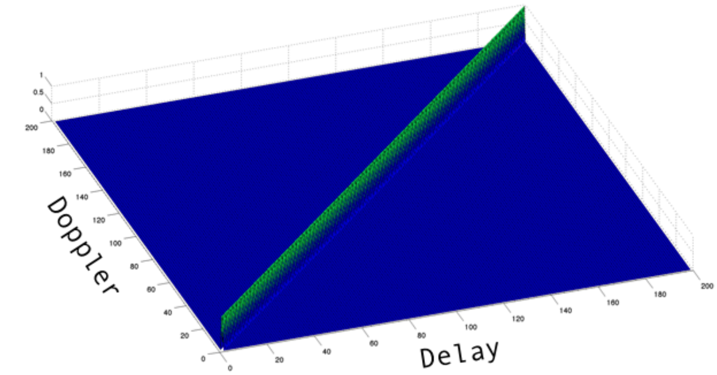

Fig. 8. $|\mathcal{M}(f_L, f_L)|$ for $L = \{(\tau, \tau))\}$.

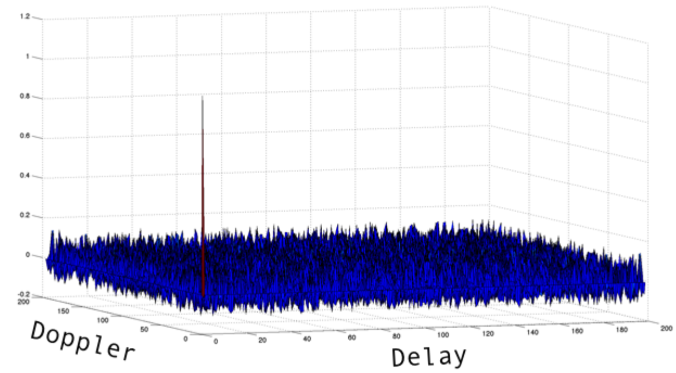

Fig. 9. $\mathcal{M}[\varphi_T, \varphi_T]$ for $T = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}; 0 \neq a \in \mathbb{Z}_N\}$.

This is a commutative collection of diagonalizable operators, and it admits [8], [9] a natural orthonormal basis $\mathcal{B}_T$ for $\mathcal{H}$, consisting of common eigensequences for all the operators (III-B.1)

$$\begin{cases} \mathcal{B}_T = \{\varphi_{T_\chi}\}; \\ \rho(g)\varphi_{T_\chi} = \chi(g)\varphi_{T_\chi}, \quad g \in T, \end{cases} \tag{III-B.2}$$

where χ runs over *characters* of T, i.e., functions $\chi : T \to \mathbb{C}^*$ with $\chi(g \cdot g') = \chi(g)\chi(g')$, for every $g, g' \in T$.

Remark III-B.1: There is a small abuse of notation in III-B.2. There are two types of tori in G, split tori and non-split tori [8], [9]. In each case, the torus T admits a unique non-trivial character χ_q of T—called the *quadratic character*—which takes the values $\chi_q(g) \in \{\pm 1\}$, $g \in T$. The dimension of the space $\mathcal{H}_{\chi_q}$ of sequences $\varphi_{T_{\chi_q}}$, which satisfy $\rho(g)\varphi_{T_{\chi_q}} = \chi_q(g)\varphi_{T_{\chi_q}}$ is equal to 2 or 0, if T is a split or non-split torus, respectively [8], [9].

Let us denote by

$$\mathcal{S}_T = \mathcal{B}_T \smallsetminus \mathcal{H}_{\chi_q},$$

the set of sequences in $\mathcal{B}_T$, which are not associated with the quadratic character. The system of all such sets $\mathcal{S}_T$, where T runs over all tori in G, will be called the *Weil (spikes) system*. We use the following result [8], [9]:

Theorem III-B.2: The Weil system satisfies the following properties:

1) *Spike.* For every torus $T \subset G$, and every $\varphi_T \in \mathcal{S}_T$, we have

$$\mathcal{M}(\varphi_T, \varphi_T)[\tau, \omega] = \begin{cases} 1, \text{ if } (\tau, \omega) = (0,0); \\ \leq \frac{2}{\sqrt{N}}, \text{ in } |\cdot| \text{ if } (\tau, \omega) \neq (0,0). \end{cases}$$

2) *Almost-orthogonality.* For every two tori T_1, $T_2 \subset G$, and every $\varphi_{T_1} \in \mathcal{S}_{T_1}$, $\varphi_{T_2} \in \mathcal{S}_{T_2}$, with $\varphi_{T_1} \neq \varphi_{T_2}$, we have

$$\left|\mathcal{M}(\varphi_{T_1}, \varphi_{T_2})[\tau, \omega]\right| \leq \begin{cases} \frac{4}{\sqrt{N}}, \text{ if } T_1 \neq T_2; \\ \frac{2}{\sqrt{N}}, \text{ if } T_1 = T_2, \end{cases}$$

for every $(\tau, \omega) \in V$.

Figure 9 illustrates Property 1 of Theorem III-B.2, applied to the commutative subgroup of diagonal matrices in G.

C. *The Heisenberg–Weil System*

We define the *Heisenberg–Weil system* of sequences. This is the collection of sequences in $\mathcal{H}$, which are of the form $S_L = f_L + \varphi_T$, where f_L and φ_T are Heisenberg and Weil sequences, respectively. The main technical result of this paper is:

Theorem III-C.1: The Heisenberg–Weil system satisfies the properties

1) *Flag.* For every line $L \subset V$, torus $T \subset G$, and every flag $S_L = f_L + \varphi_T$, with $f_L \in \mathcal{B}_L$, $\varphi_T \in \mathcal{S}_T$, we have

$$\mathcal{M}(S_L, S_L)[\tau, \omega] = \begin{cases} 2 + \epsilon_N, & \text{if } (\tau, \omega) = (0,0); \\ 1 + \varepsilon_N, & \text{in } |\cdot| \text{ if } (\tau, \omega) \in L \smallsetminus (0,0); \\ \varepsilon_N, & \text{if } (\tau, \omega) \in V \smallsetminus L, \end{cases}$$

where $|\epsilon_N| \leq \frac{4}{\sqrt{N}}$, and $|\varepsilon_N| \leq \frac{6}{\sqrt{N}}$.

2) *Almost-orthogonality.* For every two lines $L_1 \neq L_2 \subset V$, tori T_1, $T_2 \subset G$, and every two flags $S_{L_j} = f_{L_j} + \varphi_{T_j}$, with $f_{L_j} \in \mathcal{B}_{L_j}$, $\varphi_{T_j} \in \mathcal{S}_{T_j}$, $j = 1, 2$, $\varphi_{T_1} \neq \varphi_{T_2}$, we have

$$|\mathcal{M}(S_{L_1}, S_{L_2})[\tau, \omega]| \leq \begin{cases} \frac{9}{\sqrt{N}}, \text{ if } T_1 \neq T_2; \\ \frac{7}{\sqrt{N}}, \text{ if } T_1 = T_2, \end{cases}$$

for every $(\tau, \omega) \in V$.

For a proof of Theorem III-C.1 see Subsection VI-A.

Figure 10 demonstrates Property 1 of Theorem III-C.1 applied to the diagonal line L and a torus T as in Figure 9.

Remark III-C.2: As a consequence of Theorem III-C.1 we obtain families of $N+1$ almost-orthogonal flag sequences which can be used for solving the TFS problem in $O(N \log N)$ operations, and GPS, channel estimation, radar, and mobile communication problems in $O(m \cdot N \log N)$ operations for channel of sparsity m.

This completes our design of the Heisenberg–Weil flag sequences.

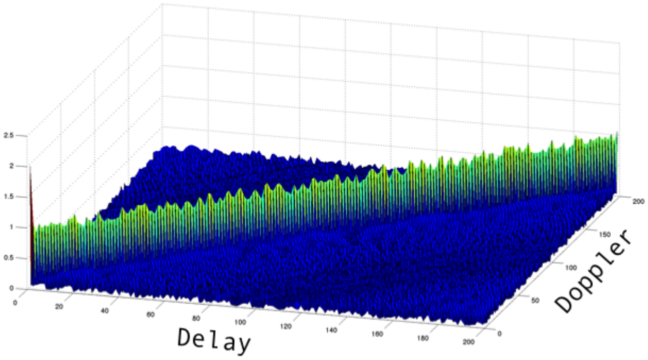

Fig. 10. $|\mathcal{M}[S_L, S_L]|$ for Heisenberg–Weil flag with $L = \{(\tau, \tau)\}$.

IV. Formulas for Heisenberg–Weil Sequences

In order to implement the flag method it is important to have explicit formulas for the Heisenberg and Weil sequences, which in particular enable one to generate them with a low complexity procedure. In this section we supply such effective description for all Heisenberg sequences, and for Weil sequences associated with split tori

A. *Formulas for Heisenberg Sequences*

First we parametrize the lines in the time-frequency plane, and then we provide explicit formulas for the orthonormal bases of sequences associated with the lines.

*1) **Parametrization of Lines**:* The $N+1$ lines in the time-frequency plane $V = \mathbb{Z}_N \times \mathbb{Z}_N$ can be described in terms of their slopes. We have

- *Lines with finite slope.* These are the lines of the form L_c =span$\{(1, c)\}$, $c \in \mathbb{Z}_N$.
- *Line with infinite slope.* This is the line L_∞ =span$\{(0, 1)\}$.

*2) **Formulas**:* Using the above parametrization, we obtain

- *Formulas for Heisenberg sequences associated with lines of finite slope.* For $c \in \mathbb{Z}_N$ we have the orthonormal basis

$$\mathcal{B}_{L_c} = \{f_{c,b}[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N}(-2^{-1}cn^2 + bn)} \; ; \; b \in \mathbb{Z}_N\},$$

  of Heisenberg sequences associated with the line L_c.
- *Formulas for Heisenberg sequences associated with the line of infinite slope.* We have the orthonormal basis

$$\mathcal{B}_{L_\infty} = \{\delta_b ; \; b \in \mathbb{Z}_N\},$$

  of Heisenberg sequences associated with the line L_∞, where the δ_b's denote the Dirac delta functions.

B. *Formulas for the Weil Sequences*

We describe explicit formulas for the Weil sequences associated with split tori [6], [8], [9]. First we parametrize the split tori in $G = SL_2(\mathbb{Z}_N)$, and then we write the explicit expressions for the orthonormal bases of sequences associated with these tori.

*1) **Parametrization of Split Tori**:* A commutative subgroup $T \subset G$ is called *split torus* [3] if for some $g \in G$ it is of the form $T = T_g$, with

$$T_g = g \cdot A \cdot g^{-1},$$

where $A \subset G$ is the subgroup of all diagonal matrices, also called the *standard* torus, i.e.,

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} ; \quad 0 \neq a \in \mathbb{Z}_N \right\}.$$

We denote by $\mathcal{T} = \{T_g ; \, g \in G\}$ the set of all split tori in G. It is not hard to verify that the number of elements in $\mathcal{T}$ is $\frac{N(N+1)}{2}$. A direct computation shows that the collection of all T_g's with

$$g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}, \quad b, c \in \mathbb{Z}_N, \tag{IV-B.1}$$

exhausts the set $\mathcal{T}$. Moreover, in (IV-B.1) the torus T_g can be written also as $T_{g'}$, for $g \neq g'$, only if $b \neq 0$ and

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

*2) **Formulas**:* In order to provide the explicit formulas we need to develop some basic facts and notations from the theory of multiplicative characters [2]. Consider the group $\mathbb{Z}_N^*$ of all non-zero elements in $\mathbb{Z}_N$, with multiplication modulo N. A basic fact about this group is that it is *cyclic,* i.e., there exists an element $r \in \mathbb{Z}_N^*$ such that

$$\mathbb{Z}_N^* = \{1, r, r^2, ..., r^{N-2}\}.$$

A function $\chi : \mathbb{Z}_N^* \to \mathbb{C}^*$ is called *multiplicative character* if $\chi(x \cdot y) = \chi(x) \cdot \chi(y)$ for every $x, y \in \mathbb{Z}_N^*$. A way to write formulas for such functions is the following. Choose $\zeta \in \mathbb{C}$ which satisfies $\zeta^{N-1} = 1$, i.e., $\zeta \in \mu_{N-1} = \{e^{\frac{2\pi i}{N-1}k} ; \, k = 0, ..., N-2\}$, and define a multiplicative character by

$$\chi_\zeta(r^d) = \zeta^d, \; d = 0, 1, ..., N-2.$$

Running over all the $N-1$ possible such ζ's, we obtain all the multiplicative characters of $\mathbb{Z}_N^*$. We are ready to write, in terms of the parametrization (IV-B.1), the concrete eigensequences associated with each of the tori (see Subsection III-B). We obtain

- *Formulas for Weil sequences associated with the diagonal torus.* For the diagonal torus A we have

$$\mathcal{S}_A = \left\{ \varphi_{\chi_\zeta} ; \quad -1 \neq \zeta \in \mu_{N-1} \right\},$$

  where $\varphi_{\chi_\zeta} \in \mathcal{H}$ is the sequence defined by

$$\varphi_{\chi_\zeta}[n] = \begin{cases} \frac{1}{\sqrt{N-1}} \chi_\zeta[n] & \text{if} \quad n \neq 0, \\ 0 & \text{if} \quad n = 0. \end{cases} \tag{IV-B.2}$$

- *Formulas for Weil sequences associated with the torus T_{u_c}, for unipotent $u_c \in G$.* For the torus T_{u_c} associated with the unipotent element

$$u_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \; c \in \mathbb{Z}_N,$$

we have

$$\mathcal{S}_{T_{u_c}} = \left\{ \varphi_{\chi_\zeta^{u_c}};\ \ -1 \neq \zeta \in \mu_{N-1} \right\},$$

where $\varphi_{\chi_\zeta^{u_c}} \in \mathcal{H}$ is the sequence defined by

$$\varphi_{\chi_\zeta^{u_c}}[n] = e^{\frac{2\pi i}{N}(-2^{-1}cn^2)} \cdot \varphi_{\chi_\zeta}[n], \qquad \text{(IV-B.3)}$$

for every $n \in \mathbb{Z}_N$, and φ_{χ_ζ} is the sequence given by (IV-B.2).

- *Formulas for Weil sequences associated with the torus T_g, for non-unipotent $g \in G$.* For the torus T_g associated with the element

$$g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}, \quad b, c \in \mathbb{Z}_N,\ b \neq 0,$$

we have

$$\mathcal{S}_{T_g} = \left\{ \varphi_{\chi_\zeta^g}\ ;\ \ -1 \neq \zeta \in \mu_{N-1} \right\},$$

where $\varphi_{\chi_\zeta^g} \in \mathcal{H}$ is the sequence defined by

$$\begin{aligned} \varphi_{\chi_\zeta^g}[n] &= C_b \cdot \frac{e^{\frac{2\pi i}{N}(2^{-1}\frac{1+bc}{b}n^2)}}{\sqrt{N}} \times \qquad \text{(IV-B.4)} \\ &\times \sum_{\omega \in \mathbb{Z}_N} e^{\frac{2\pi i}{N}\omega \cdot n} \cdot \left[e^{\frac{2\pi i}{N}(-2^{-1}b\omega^2)} \cdot \varphi_{\chi_\zeta}[b\omega] \right], \end{aligned}$$

for every $n \in \mathbb{Z}_N$, and φ_{χ_ζ} the sequence given by (IV-B.2), $C_b = i^{-\frac{N-1}{2}} \left(\frac{b}{N}\right)$, with $\left(\frac{\cdot}{N}\right)$ the Legendre symbol.

The validity of Formula (IV-B.2) is immediate from Identity (II-B.6). For a verification of Formulas (IV-B.3) and (IV-B.4), see Subsection VI-B.

*Remark IV-B.1 (**Complexity of Heisenberg-Weil sequences**):* For concrete applications it is important to have low arithmetic complexity algorithm generating the sequences. Note that the sequence (IV-B.4) can be computed in $O(N \log N)$ operations using FFT. We conclude that the all Heisenberg sequences, and all Weil sequences associated with split tori, and in particular the associated flag sequence, can be computed in at most $O(N \log N)$ operations.

V. Computing the Matched Filter on a Line

Implementing the flag method, we need to compute in $O(N \log N)$ operations the restriction of the MF matrix to any line in the time-frequency plane (see Remark I-D.1). In this section we provide algorithm that fulfills this task. The upshot is—see Figure 11 for illustration of the case of the diagonal line—that the restriction of the MF matrix to a line is a certain convolution that can be computed fast using FFT. Denote by $\mathcal{M}(\varphi,\phi)[\tau,\omega] = \langle \varphi,\ \pi(\tau,\omega)\phi \rangle$ the matched filter associated with sequences $\varphi, \phi \in \mathcal{H}$, and by $\varphi * \phi \in \mathcal{H}$ their convolution

$$(\varphi * \phi)[\tau] = \sum_{n \in \mathbb{Z}_N} \varphi_-[n] \cdot \phi_\tau[n], \qquad \text{(V-.1)}$$

where $\varphi_-[n] = \varphi[-n]$, and $\phi_\tau[n] = \phi[\tau + n]$, for every $\tau, n \in \mathbb{Z}_N$.

We consider two cases:

1) *Formula on lines with finite slope and their shifts.* For $c \in \mathbb{Z}_N$ consider the line $L_c = \{\tau \cdot (1,c)\ ;\ \tau \in \mathbb{Z}_N\}$, and for a fixed $\omega \in \mathbb{Z}_N$ the shifted line $L_c' = L_c + (0,\omega)$. On L_c' we have

$$\begin{aligned} &\mathcal{M}(\varphi,\phi)[\tau \cdot (1,c) + (0,\omega)] \qquad \text{(V-.2)} \\ &= \left[\mathsf{m}_{\exp(2^{-1}cn^2+\omega n)}\varphi_- * \mathsf{m}_{\exp(-2^{-1}cn^2)}\overline{\phi} \right][\tau], \end{aligned}$$

where $\left[\mathsf{m}_{\exp(2^{-1}cn^2+\omega n)}\varphi_-\right][n] = e^{\frac{2\pi i}{N}(2^{-1}cn^2+\omega n)} \times \varphi_-[n]$, $n \in \mathbb{Z}_N$, and similar definition for the second expression, with $\overline{\phi}$ the complex conjugate of the sequence ϕ.

2) *Formula on the line with infinite slope and its shifts.* Consider the line $L_\infty = \{\omega \cdot (0,1)\ ;\ \omega \in \mathbb{Z}_N\}$, and for a fixed $\tau \in \mathbb{Z}_N$ the shifted line $L_\infty' = L_\infty + (\tau, 0)$. On L_∞' we have

$$\mathcal{M}(\varphi,\phi)[\omega \cdot (0,1) + (\tau,0)] = DFT(\varphi \cdot \overline{\phi_\tau})[\omega], \qquad \text{(V-.3)}$$

for every $\omega \in \mathbb{Z}_N$.

The validity of Formula (V-.3) is immediate from the definition of the matched filter. For a verification of Formula (V-.2) see Subsection VI-C.

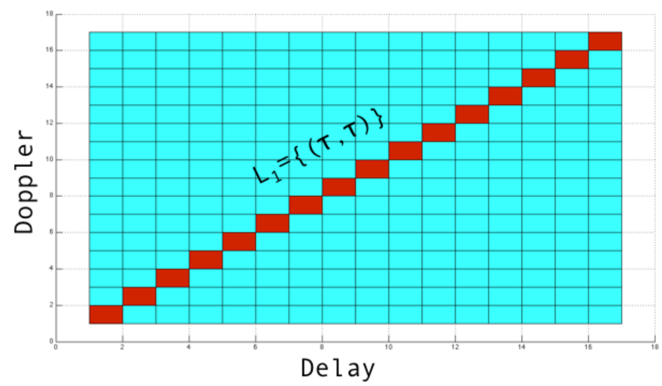

Fig. 11. $\mathcal{M}(\varphi,\phi)[\tau,\tau] = \left[\mathsf{m}_{\exp(2^{-1}n^2)}\varphi_- * \mathsf{m}_{\exp(-2^{-1}n^2)}\overline{\phi} \right][\tau]$ on L_1.

VI. Proofs

A. Proof of Theorem III-C.1

*1) **Flag Property**:* Let $S_L = f_L + \varphi_T$. We have

$$\begin{aligned} \mathcal{M}(S_L, S_L) &= \mathcal{M}(f_L, f_L) + \mathcal{M}(f_L, \varphi_T) \\ &\quad + \mathcal{M}(\varphi_T, f_L) + \mathcal{M}(\varphi_T, \varphi_T). \end{aligned}$$

We will show that

$$|\mathcal{M}(\varphi_T, f_L)[\tau,\omega]| \leq \frac{2}{\sqrt{N}}, \quad \tau, \omega \in \mathbb{Z}_N. \qquad \text{(VI-A.1)}$$

Noting that $\mathcal{M}(f_L, \varphi_T)[\tau,\omega] = \overline{\mathcal{M}(\varphi_T, f_L)[-\tau,-\omega]}$ we get from (VI-A.1) also the same bound for $\mathcal{M}(f_L, \varphi_T)$. Having this, using Theorems III-A.1 and III-B.2 we can deduce the Flag Property. So assume $\pi(\ell) f_L = \psi(\ell) f_L$ for $\ell \in L$. We proceed in several steps:

Step 1. *For every $v \in V$ we have $\pi(v)f_L \in \mathcal{B}_L$.* Indeed, for $\ell \in L$ we have

$$\begin{aligned}\pi(\ell)[\pi(v)f_L] &= e^{\frac{2\pi i}{N}(-\Omega(\ell,v))}\pi(v)\pi(\ell)f_L \\ &= e^{\frac{2\pi i}{N}(-\Omega(\ell,v))}\psi(\ell)[\pi(v)f_L],\end{aligned}$$

where $\Omega : V \times V \to \mathbb{Z}_N$ is the symplectic form $\Omega[(\tau,\omega),(\tau',\omega')] = \tau\omega' - \omega\tau'$. Namely, $\pi(v)f_L$ is eigensequence for $\pi(\ell)$ with character $\psi_v(\ell) = e^{\frac{2\pi i}{N}(-\Omega(\ell,v))}\psi(\ell)$.

By step 1, it is enough to bound the inner product

$$|\langle \varphi_T, f_L\rangle| \leq \frac{2}{\sqrt{N}}. \qquad \text{(VI-A.2)}$$

Step 2. *The bound (VI-A.1) holds for L_∞.* Indeed, then $f_{L_\infty} = \delta_b$ for some $b \in \mathbb{Z}_N$, hence

$$|\langle \varphi_T, f_{L_\infty}\rangle| = |\varphi_T[b]| \leq \sup_{n\in\mathbb{Z}_N} |\varphi_T[n]|.$$

In [9] it was shown that for every Weil sequence φ_T we have

$$\sup_{n\in\mathbb{Z}_N} |\varphi_T[n]| \leq \frac{2}{\sqrt{N}}.$$

Step 3. *The bound (VI-A.1) holds for every line L.* We will use two lemmas. First, let $L, M \subset V$ be two lines, and $g \in G$ such that $gL = \{g\cdot\ell\ ;\ \ell \in L\} = M$. For a character $\psi : L \to \mathbb{C}^*$, define the character $\psi^g : M \to \mathbb{C}^*$, by $\psi^g(g\cdot\ell) = \psi(\ell)$, for every $\ell \in L$. We have

Lemma VI-A.1: Suppose f_L is a ψ-eigensequence for L, i.e., $\pi(\ell)f_L = \psi(\ell)f_L$, for every $\ell \in L$. Then the sequence $f_M = \rho(g)f_L$ is ψ^g-eigensequence for M.

For a proof of Lemma VI-A.1, see Subsection VI-A1a.

For the second lemma, consider a torus $T \subset G$, and an element $g \in G$. Then we can define a new torus $T_g = gTg^{-1} = \{g\cdot h\cdot g^{-1};\ h \in T\}$. For a character $\chi : T \to \mathbb{C}^*$, we can associate a character $\chi^g : T_g \to \mathbb{C}^*$, by $\chi^g(g\cdot h\cdot g^{-1}) = \chi(h)$, for every $h \in T$. We have

Lemma VI-A.2: Suppose φ_T is a χ-eigensequence for T, i.e., $\rho(h)\varphi_T = \chi(h)\varphi_T$, for every $h \in T$. Then the sequence $\varphi_{T_g} = \rho(g)\varphi_T$ is χ^g-eigensequence for T_g.

For a proof of Lemma VI-A.2, see Subsection VI-A1b.

Now we can verify Step 3. Indeed, given a line $L \subset V$, there exists $g \in G$ such that $g \cdot L = L_\infty$. In particular, by Lemma VI-A.1 we get that $f_{L_\infty} = \rho(g)f_L$ is up to a unitary scalar in $\mathcal{B}_{L_\infty}$. In addition, by Lemma VI-A.2 we know that $\varphi_{T_g} = \rho(g)\varphi_T$ is up to a unitary scalar in $\mathcal{B}_{T_g}$. Finally, we have

$$\begin{aligned}\langle \varphi_T, f_L\rangle &= \langle \rho(g)\varphi_T, \rho(g)f_L\rangle \\ &= \left\langle \varphi_{Tg}, f_{L_\infty}\right\rangle,\end{aligned}$$

where the first equality is by the unitarity of $\rho(g)$. Hence, by Step 2, we get the desired bound also in this case.

*a) **Proof of Lemma VI-A.1** :* For $\ell \in L$ we have

$$\begin{aligned}\pi(g\cdot\ell)f_M &= \pi(g\cdot\ell)\rho(g)f_L \\ &= \rho(g)\pi(\ell)f_L \\ &= \psi(\ell)\rho(g)f_L \\ &= \psi^g(g\cdot\ell)f_M,\end{aligned}$$

where the second equality is by Identity (II-B.2). This completes the proof of Lemma VI-A.1.

*b) **Proof of Lemma VI-A.2** :* For $h \in T$ we have

$$\begin{aligned}\rho(g\cdot h\cdot g^{-1})\varphi_{T_g} &= \rho(g\cdot h\cdot g^{-1})\rho(g)\varphi_T \\ &= \rho(g)\rho(h)\varphi_T \\ &= \chi(h)\rho(g)\varphi_T \\ &= \chi^g(g\cdot h\cdot g^{-1})\varphi_{T_g},\end{aligned}$$

where the second equality is because ρ is homomorphism (see Theorem II-B.1). This completes our proof of Lemma VI-A.2, and of the Flag Property.

*2) **Almost Orthogonality** :* Let $S_{L_j} = f_{L_j} + \varphi_{Tj}$, $j = 1, 2$, as in the assumptions. We have

$$\begin{aligned}\mathcal{M}(S_{L_1}, S_{L_2}) &= \mathcal{M}(f_{L_1}, f_{L_2}) + \mathcal{M}(f_{L_1}, \varphi_{T_2}) \\ &\quad + \mathcal{M}(\varphi_{T_1}, f_{L_2}) + \mathcal{M}(\varphi_{T_1}, \varphi_{T_2}).\end{aligned}$$

The result now follows from Theorem III-A.1, Theorem III-B.2, and the bound (VI-A.1). This completes our proof of the Almost Orthogonality Property, and of Theorem III-C.1.

B. *Verification of Formulas (IV-B.3), and (IV-B.4)*

The idea is to use the fact that for $g \in G$, the explicit Weil operator $\rho(g)$ maps the explicit set $\mathcal{S}_A$ to the set $\mathcal{S}_{T_g}$, $T_g = gAg^{-1}$. In details, for a character $\chi : A \to \mathbb{C}^*$ and an element $g \in G$ define the character $\chi^g : T_g \to \mathbb{C}^*$, by $\chi^g(g\cdot h\cdot g^{-1}) = \chi(h)$, for every $h \in A$. Using Lemma VI-A.2 we deduce that if $\varphi_\chi \in \mathcal{S}_A$ is eigensequence of A with character χ, then $\varphi_{\chi^g} = \rho(g)\varphi_\chi \in \mathcal{S}_{T_g}$ is eigensequence of T_g with character χ^g. Specializing to the character $\chi = \chi_\zeta$, $-1 \neq \zeta \in \mu_{N-1}$, of A, and the associated sequence $\varphi_{\chi_\zeta} \in \mathcal{S}_A$ given by (IV-B.2), we can proceed to verify the formulas.

*1) **Verification of Formula (IV-B.3)**:* For the unipotent element

$$u_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix},\ c \in \mathbb{Z}_N,$$

we have

$$\begin{aligned}\varphi_{\chi_\zeta^{u_c}}[n] &= \left[\rho(u_c)\varphi_{\chi_\zeta}\right][n] \\ &= e^{\frac{2\pi i}{N}(-2^{-1}cn^2)} \cdot \varphi_{\chi_\zeta}[n]\ ,\end{aligned}$$

where the second equality is by Formula (II-B.5). This completes our verification of Formula (IV-B.3).

2) ***Verification of Formula (IV-B.4):*** For the element

$$g = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}, \quad b, c \in \mathbb{Z}_N, \ b \neq 0,$$

its Bruhat decomposition is

$$\begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1+bc}{b} & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix}. \tag{VI-B.1}$$

This implies that for $n \in \mathbb{Z}_N$ we have

$$\begin{aligned} \varphi_{\chi_\zeta^g}[n] &= \left[\rho(g)\varphi_{\chi_\zeta}\right][n] \\ &= C_b \cdot \frac{e^{\frac{2\pi i}{N}(-2^{-1}\frac{1+bc}{b}n^2)}}{\sqrt{N}} \times \\ &\quad \times \sum_{\omega \in \mathbb{Z}_N} e^{\frac{2\pi i}{N}\omega \cdot n} \cdot \left[e^{\frac{2\pi i}{N}(-2^{-1}b\omega^2)} \cdot \varphi_{\chi_\zeta}[b\omega]\right], \end{aligned}$$

with $C_b = i^{-\frac{N-1}{2}}\left(\frac{b}{N}\right)$, where in the second equality we use identity (VI-B.1), the fact that ρ is homomorphism, and the Formulas (II-B.4), (II-B.5), (II-B.6). This completes our verification of Formula (IV-B.4).

C. *Verification of Formula (V-.2)*

We verify Formula (V-.2) for the matched filter $\mathcal{M}(\varphi, \phi)$, $\varphi, \phi \in \mathcal{H}$, restricted to a line with finite slope. We proceed in two steps:

Step 1. *The formula holds for the line L_0 and its shifts.* Indeed, for a fixed $\omega \in \mathbb{Z}_N$ we compute the matched filter on $L_0' = L_0 + (0, \omega) = \{(\tau, \omega);\ \tau \in \mathbb{Z}_N\}$. We get

$$\begin{aligned} \mathcal{M}(\varphi, \phi)[\tau, \omega] &= \langle \varphi,\ \pi(\tau, \omega)\phi \rangle \\ &= \left\langle \varphi,\ e^{\frac{2\pi i}{N}\omega n} \cdot \phi[n+\tau] \right\rangle \\ &= \left\langle\ e^{-\frac{2\pi i}{N}\omega \cdot n} \cdot \varphi[n],\ \phi[n+\tau] \right\rangle \\ &= \left[\mathsf{m}_{\exp(\omega n)}\varphi_- * \overline{\phi}\right][\tau], \end{aligned}$$

where the fourth equality is by the definition (V-.1) of $*$, and the definition (V-.2) of $\mathsf{m}_{\exp(\cdot)}$.

Step 2. *The formula holds for the lines L_c, $c \in \mathbb{Z}_N$, and their shifts.* Indeed, the element

$$u_{-c} = \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix} \in G,$$

satisfies

$$\begin{cases} u_{-c} \cdot (1, c) = (1, 0), \\ u_{-c} \cdot (0, \omega) = (0, \omega). \end{cases} \tag{VI-C.1}$$

For a fixed $\omega \in \mathbb{Z}_N$ we compute the matched filter on $L_c' = L_c + (0, \omega) = \{\tau \cdot (1, c) + (0, \omega);\ \tau \in \mathbb{Z}_N\}$. We get

$$\begin{aligned} & \mathcal{M}(\varphi, \phi)[\tau \cdot (1, c) + (0, \omega)] \\ =\ & \langle \varphi,\ \pi[\tau \cdot (1, c) + (0, \omega)]\phi \rangle \\ =\ & \langle \rho(u_{-c})\varphi,\ \rho(u_{-c})\pi[\tau \cdot (1, c) + (0, \omega)]\phi \rangle \\ =\ & \langle \rho(u_{-c})\varphi,\ \pi(\tau, \omega)\rho(u_{-c})\phi \rangle \\ =\ & \mathcal{M}(\rho(u_{-c})\varphi, \rho(u_{-c})\phi)[\tau, \omega] \\ =\ & \left[\mathsf{m}_{\exp(2^{-1}cn^2 + \omega n)}\varphi_- * \mathsf{m}_{\exp(-2^{-1}cn^2)}\overline{\phi}\right][\tau], \end{aligned}$$

where, the second equality is by the unitarity of ρ, the third equality is by Identities (II-B.2), (VI-C.1), and the last equality is by Formula (II-B.5) and Step 1 above.

This confirms Step 2, and completes our verification of Formula (V-.2).

REFERENCES

[1] Agarwal N. et. al., Algorithms for GPS Operation Indoors and Downtown. *GPS Solutions 6, 149-160, 2002.*

[2] Artin M., Algebra. *Prentice Hall, Inc., Englewood Cliffs, NJ (1991).*

[3] Borel, A.: Linear Algebraic Groups. *Graduate Texts in Mathematics, vol. 126. Springer, New York (1991).*

[4] Fish A., Gurevich S., Hadani R., Sayeed A., and Schwartz O. Delay-Doppler Channel Estimation with Almost Linear Complexity. *Proceedings of ISIT 2012 - IEEE International Symposium on Information Theory, Cambridge, MA, USA, July 1–6, 2012.*

[5] P. Gerardin. Weil representations associated to finite fields. *J. Algebra 46 (1977), 54–101.*

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

[7] Gurevich S., Hadani R., Howe R. - Quadratic Reciprocity and the Sign of Gauss Sum via the Finite Weil Representation . *IMRN, 2010. 17 pages.*

[8] Gurevich S., Hadani R., Sochen N., The finite harmonic oscillator and its associated sequences. *PNAS, July 22, 2008 vol. 105 no. 29 9869–9873.*

[9] Gurevich S., Hadani R., Sochen N., The finite harmonic oscillator and its applications to sequences, communication and radar . *IEEE Transactions on Information Theory, vol. 54, no. 9, September 2008.*

[10] 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.*

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

[12] Kaplan E., Understanding GPS Principles and Applications. *Artech house, INC (1996).*

[13] Levanon N., Radar Principles. *J. Wiley & Sons (Interscience Div.) New York, 1988.*

[14] O'Toole J.M., Mesbah M., and Boashash B., Accurate and efficient implementation of the time–frequency matched filter. *IET Signal Process., 2010, Vol. 4, Iss. 4, pp. 428–437.*

[15] Sayeed, A.M., Aazhang B., Joint Multipath-Doppler Diversity in Mobile Wireless Communications. *IEEE Transactions on Communications, pp. 123-132, January 1999.*

[16] Tse D., and Viswanath P., Fundamentals of Wireless Communication. *Cambridge University Press (2005).*

[17] Verdu S., Multiuser Detection, *Cambridge University Press (1998).*

[18] Wang Z., and Gong G., New Sequences Design From Weil Representation With Low Two-Dimensional Correlation in Both Time and Phase Shifts. *IEEE Transactions on Information Theory, vol. 57, no. 7, July 2011.*

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