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

Delay-Doppler Channel Estimation in Almost Linear Complexity

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

***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, i.e., a signal undergoes only delay and Doppler shifts, a widely used method to compute the delay-Doppler parameters 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 m delay-Doppler parameters in $O(mN \log N)$ operations. We discuss applications of the flag method to GPS, and radar systems.**

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

I. Introduction

A fundamental building block in many wireless communication protocols is *channel estimation*: learning the channel parameters a signal undergoes while traveling from a transmitter to a receiver [17]. In this paper we develop an efficient algorithm[1] 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 $\mathcal{H}$ the vector space of complex valued functions on the set of integers $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ 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. Finally, we define $e(t) = e^{\frac{2\pi i}{N} t}$, where $i = \sqrt{-1}$.

A. Channel Model

Let us start with the derivation of the discrete channel model that we will consider throughout this paper. We follow closely the works [13]–[16]. The transmitter sends—see Fig. 2 for ilustration—an analog signal $S_A(t)$, $t \in \mathbb{R}$, of (two-sided) bandwidth W. While the actual signal is modulated onto a carrier frequency $f_c \gg W$, we consider a widely used complex baseband model for the multipath channel. In addition, we make the sparsity assumption on the finiteness of the number of signal propagation paths.The complex baseband analog received signal is (see [14, Equation (14)]) given by

$$R_A(t) = \sum_{k=1}^{m} \beta_k \cdot \exp(2\pi i f_k t) \cdot S_A(t - t_k) + \mathcal{W}(t), \quad \text{(I-A.1)}$$

where m denotes the number of propagation paths, $\beta_k \in \mathbb{C}$ is the *path coefficient*, $f_k \in \mathbb{R}$ is the Doppler shift, and $t_k \in \mathbb{R}_+$ is the *path delay* associated with the k-th path, and $\mathcal{W}$ denotes a random white noise. We assume the normalization $\sum_{k=1}^{m} |\beta_k|^2 \leq 1$. The Doppler shift depends on the relative speed between the transmitter and the receiver along the path, and the delay encodes the distance between the transmitter and receiver along the path. The parameter m will be called also the *sparsity* of the channel. We will call

$$(\beta_k, t_k, f_k), \; k = 1, \ldots, m, \quad \text{(I-A.2)}$$

the *channel parameters,* and the main objective of channel estimation is to obtain them. We describe now a process—see Fig. 1 for illustration—allowing to reduce this task to a problem for

Manuscript received September 27, 2012; revised May 03, 2013; accepted July 12, 2013. Date of publication July 18, 2013; date of current version October 16, 2013. This work was supported by the Defense Advanced Research Projects Agency (DARPA) award number N66001-13-1-4052. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of DARPA. This work was also supported in part by NSF Grants DMS-1101660 and DMS-1101698 - "The Heisenberg–Weil Symmetries, their Geometrization and Applications".

A. Fish is with the School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia (e-mail: alexander.fish@sydney.edu.au).

S. Gurevich is with the Department of Mathematics, University of Wisconsin, Madison, WI 53706 USA (e-mail: shamgar@math.wisc.edu).

R. Hadani is with the Department of Mathematics, University of Texas, Austin, TX 78712 USA (e-mail: hadani@math.utexas.edu).

A. M. Sayeed is with the Department of Electrical and Computer Engineering, University of Wisconsin, Madison, WI 53706 USA (e-mail: akbar@engr.wisc.edu).

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

Communicated by D. P. Palomar, Associate Editor for Detection and Estimation.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2013.2273931

[1] Announcement of this result appeared in [3].

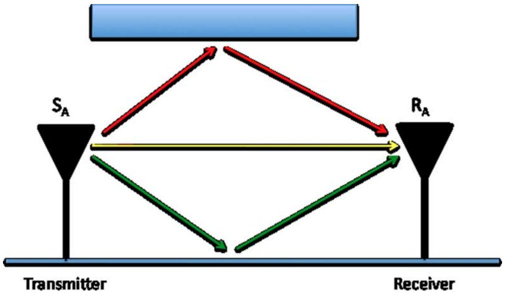

Fig. 1. Three paths scenario.

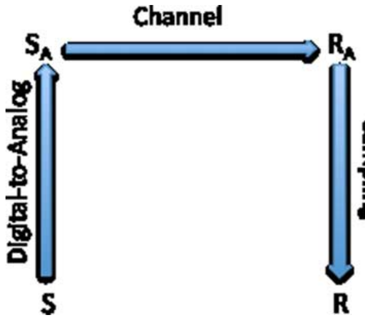

Fig. 2. Illustration of the process allowing the discrete channel model.

sequences. We start with a sequence $S \in \mathcal{H}$, and transmit the analog signal

$$S_A(t) = \sum_{n=0}^{M-1} S[n \bmod(N)] \cdot sinc(Wt - n),$$

where $M \geq N$, and $sinc(t) = \sin(\pi t)/\pi t$. To specify the transmission interval, we denote by T_s the time spread of the channel, i.e., $T_s = \max\{t_k\}$, and we define $K = \lceil WT_s \rceil$, where $\lceil x \rceil$ is the ceiling function. We assume $K \leq N$, and we take $M = N + K$. Then the transmission time of $S_A(t)$ is from $t = 0$ to $t = M/W$. At the receiver, the discrete system representation is obtained by sampling $R_A(t)$, satisfying (I-A.1), with sampling interval $\Delta t = 1/W$ starting from time[2] K/W. As a result, we obtain the following sequence $R \in \mathcal{H}$:

$$R[n] = R_A\left((K + n)/W\right), \qquad \text{(I-A.3)}$$

for $n = 0, \ldots, N - 1$. By a direct calculation we obtain the following:

Proposition I-A.1: Assume that $t_k \in \frac{1}{W}\mathbb{Z}$, and $f_k \in \frac{W}{N}\mathbb{Z}$, $k = 1, \ldots, m$. Then the sequence R given by (I-A.3) satisfies

$$R[n] = \sum_{k=1}^{m} \alpha_k \cdot e(\omega_k n) \cdot S[K + n - \tau_k] + \mathcal{W}[n], \; n \in \mathbb{Z}_N,$$

where $\alpha_k = \beta_k \exp(-2\pi i f_k K/W)$, $\tau_k = t_k W$, and $\omega_k = N f_k/W$.

Remark I-A.2: Even if an actual delay t_k or Doppler shift f_k do not exactly lie on the lattice, they can be well approximated by a few discrete delay-Doppler shifts on the lattice (see [16], Section II-A).

In the next section we formulate the mathematical problem that we will solve in this paper, suggesting, according to Proposition I-A.1, a method to compute the channel parameters (I-A.2).

B. Channel Estimation Problem

Consider sequences $S, R \in \mathcal{H}$, where R is given by the following formula:

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

with $\alpha_k \in \mathbb{C}$, $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\tau_k, \omega_k \in \mathbb{Z}_N$, and $\mathcal{W} \in \mathcal{H}$ denotes a random white noise. For the rest of the paper we assume that all the coordinates of the sequence $\mathcal{W}$ are independent, identically distributed random variables of expectation zero. In analogy with the physical channel model described by Equation (I-A.1), we will call $\alpha_k, \tau_k, \omega_k, k = 1, \ldots, m,$ *path coefficients*, *path delays*, and *Doppler shifts*, respectively. The objective is:

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

Granting the solution of Problem I-B.1, we can compute the channel parameters (I-A.2) using Proposition I-A.1.

Remark I-B.2 ***(Frequency Resolution)****:* From Proposition I-A.1, follows that the resolution of the frequency shifts recognized by our digital method equals to W/N.

C. The GPS Problem

We would like to discuss an important example of channel estimation. A client on the earth surface wants to know his/her geographical location. The Global Positioning System (GPS) is built to fulfill this task. Satellites send to earth their location—see Fig. 3 for illustration. For simplicity, the location of a satellite is modeled by a bit $b \in \{\pm 1\}$. The satellite transmits—for example using the scheme proposed in Section I-A—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 (see [1, Equation (1)]). Hence, by the sampling procedure described in Section I-A, the client receives the sequence $R \in \mathcal{H}$ of the form

$$R[n] = b \cdot \alpha_0 \cdot e(\omega_0 n) \cdot S[n - \tau_0] + \mathcal{W}[n], \quad n \in \mathbb{Z}_N, \quad \text{(I-C.1)}$$

where $\alpha_0 \in \mathbb{C}$, $|\alpha_0| \leq 1$, $\tau_0, \omega_0 \in \mathbb{Z}_N$, and $\mathcal{W} \in \mathcal{H}$ is a random white noise. Using τ_0 we can compute the distance from the satellite to the client[3], assuming a line of sight between them. The problem of GPS can be formulated as follows:

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

In practice, the satellite transmits $S = S_1 + bS_2$, where S_1, S_2 are almost orthogonal in some appropriate sense. Then

[2] We start to sample at time K/W in order to sense all the terms in Equation (I-A.1) at the receiver.

[3] Since we work modulo N, the distance can be found modulo $\frac{N}{W}c$, where W is the bandwidth, and c is the speed of light.

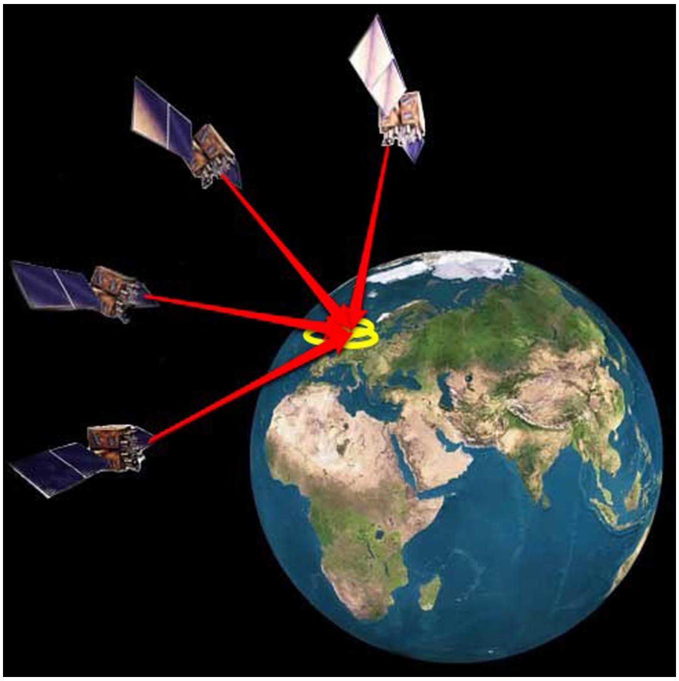

Fig. 3. Satellites communicate location in GPS.

$(\alpha_0, \tau_0, \omega_0)$, and $(b\alpha_0, \tau_0, \omega_0)$ are computed using S_1, and S_2, respectively, concluding with the derivation of the bit b.

D. The Time-Frequency Shift Problem

To suggest a solution to Problem I-C.1, and subsequently to Problem I-B.1, we consider a simpler variant. Suppose the transmitter and the receiver sequences $S, R \in \mathcal{H}$ are related by

$$R[n] = e(\omega_0 n) \cdot S[n - \tau_0] + \mathcal{W}[n], \quad n \in \mathbb{Z}_N, \qquad \text{(I-D.1)}$$

where $(\tau_0, \omega_0) \in \mathbb{Z}_N \times \mathbb{Z}_N$, and $\mathcal{W} \in \mathcal{H}$ denotes a random white noise. 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-D.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-D.1).

E. The Matched Filter Algorithm

A classical solution to Problem I-D.1, is the matched filter algorithm [5], [7], [8], [10], [17]–[19]. We define the following matched filter matrix[4] of R and S:

$$\mathcal{M}(R,S)[\tau, \omega] = \langle R[n],\ e(\omega n) \cdot S[n - \tau] \rangle, \quad (\tau, \omega) \in V.$$

For R and S satisfying (I-D.1), the law of the iterated logarithm implies that, with probability going to one, as N goes to infinity, we have

$$\begin{aligned} &\mathcal{M}(R,S)[\tau, \omega] && \text{(I-E.1)} \\ &= \zeta_0 \cdot \mathcal{M}(S,S)[\tau - \tau_0, \omega - \omega_0] + \varepsilon_N, \end{aligned}$$

where $\zeta_0 = e(\omega\tau_0 - \tau\omega_0)$, $|\varepsilon_N| \leq \sqrt{2 \log \log N} / \sqrt{N \cdot SNR}$, with SNR denotes the *signal-to-noise ratio*[5].

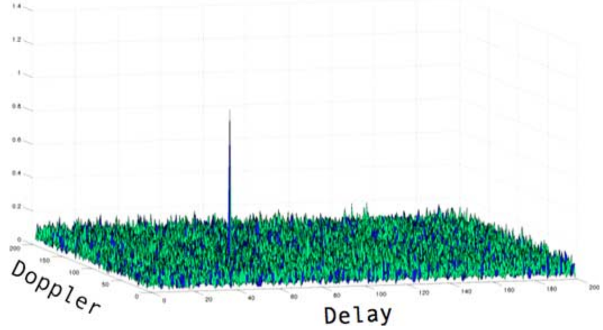

Fig. 4. $|\mathcal{M}(R,S)|$ *with pseudo-random* S, *and* $(\tau_0, \omega_0) = (50, 50)$.

*Remark I-E.1 **(Noise Assumption)**:* For the rest of the paper we assume, for simplicity, that $SNR \geq 2 \log \log N$, i.e., $|\varepsilon_N| \leq 1/\sqrt{N}$ in (I-E.1).

In order to extract the time-frequency shift (τ_0, ω_0), it is "standard"[6] (see [5], [7], [8], [10], [17]–[19]) 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 bounded by $C/\sqrt{N}$, $C > 0$, if $(\tau, \omega) \neq (\tau_0, \omega_0)$. Hence, with probability going to one, as N goes to infinity, we have

$$\mathcal{M}(R,S)[\tau, \omega] = \begin{cases} 1 + \varepsilon_N, & \text{if } (\tau, \omega) = (\tau_0, \omega_0); \\ \epsilon_N, & \text{if } (\tau, \omega) \neq (\tau_0, \omega_0), \end{cases} \qquad \text{(I-E.2)}$$

where $|\varepsilon_N| \leq 1/\sqrt{N}$, and $|\epsilon_N| \leq (C+1)/\sqrt{N}$.

Identity (I-E.2)—see Fig. 4 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 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 following observation:

*Remark I-E.2 **(FFT)**:* The restriction of the matrix $\mathcal{M}(R,S)$ to any line[7] (not necessarily through the origin) in the time-frequency plane V, is a certain convolution—for details see Section V—that can be computed, using the fast Fourier transform[8] (FFT), in $O(N \log N)$ operations.

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

F. The Fast Matched Filter Problem

To the best of our knowledge, the "line-by-line" computation is also the fastest known method [11]. If N is large this may not suffice. For example, in applications to GPS [1], as in Problem I-C.1 above, we have $N \geq 1000$. This leads to the following:

[4] The matched filter matrix is called *ambiguity function* in radar theory.

[5] We define $SNR = \langle S, S \rangle / Var(\mathcal{W})$.

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

[7] In this paper, by a line through the origin we mean all scalar multiples $L = \{au;\ a \in \mathbb{Z}_N\}$ of a fixed non-zero vector $u \in V$. In addition, by a *line* we mean a subset of V of the form $L + v$, where L is a fixed line through the origin, and $v \in V$ is a fixed vector.

[8] The Rader algorithm [12] provides implementation of the FFT for sequences of prime length.

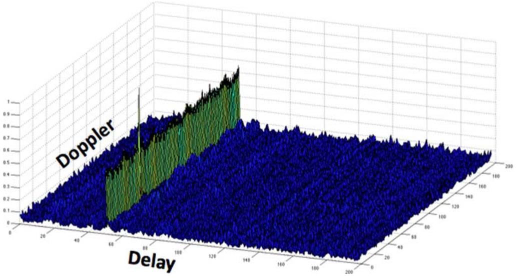

Fig. 5. $|\mathcal{M}(R, S_L)|$ for a flag S_L with $L = \{(0, \omega)\}$, and $(\tau_0, \omega_0) = (50, 50)$.

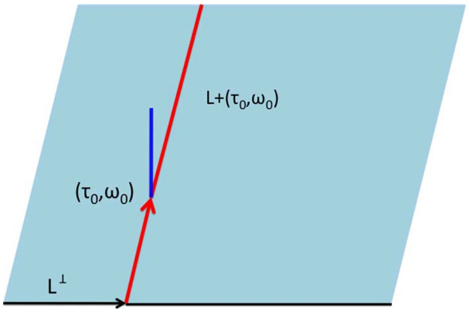

Fig. 6. Diagram of flag algorithm.

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

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

G. *The Flag Method*

We introduce the *flag method* to propose a solution to solve the TFS problem with algorithm which reduces the computational complexity from $O(N^2 \log N)$ to $O(N \log N)$ operations. The idea is to use a new set of sequences, which enable, 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. With each line L through the origin in V, we associate sequence $S_L \in \mathcal{H}$ of norm one, that we call *flag*. Since there are $N + 1$ lines through the origin in V, we obtain $N + 1$ different flag sequences. Each flag sequence satisfies—see Fig. 5 for illustration—the following "flag property"[9]: For a sequence R given by (I-D.1) with $S = S_L$, we have with probability going to one, as N goes to infinity,

$$\mathcal{M}(R, S_L)[\tau, \omega] \tag{I-G.1}$$
$$= \begin{cases} 1 + \varepsilon_N, & \text{if } (\tau, \omega) = (\tau_0, \omega_0); \\ \frac{1}{2} + \epsilon_N, & \text{in } |\cdot| \text{ if } (\tau, \omega) \in L' \backslash (\tau_0, \omega_0); \\ \epsilon_N, & \text{if } (\tau, \omega) \in V \backslash L', \end{cases}$$

where $|\varepsilon_N| \leq 1/\sqrt{N}$, $|\epsilon_N| \leq 5/\sqrt{N}$, $|\cdot|$ denotes absolute value, and L' is the shifted line $L + (\tau_0, \omega_0)$. In addition[10], the flag sequences will satisfy the following "almost orthogonality" property: If L, M are two different lines, then $|\mathcal{M}(S_L, S_M)[\tau, \omega]| \leq 3/\sqrt{N}$, for every $(\tau, \omega) \in V$.

As a consequence of Equation (I-G.1), we can apply the **Flag Algorithm**, as described below, to solve the matched filter problem, with probability going to one as N goes to infinity. The complexity of the flag algorithm—see Fig. 6 for a demonstration—is $O(N \log N)$, using FFT. This completes our solution of Problem I-F.1—The Fast Matched Filter Problem.

The Flag Algorithm

Input. The line $L \subset V$, and S_L, R as in **(I-D.1)**.
Output. The time-frequency shift (τ_0, ω_0).

Step 1. Choose a line $L^{\perp}$ transversal to L.
Step 2. Compute $\mathcal{M}(R, S_L)$ on $L^{\perp}$, and find (τ, ω) such that $||\mathcal{M}(R, S_L)[\tau, \omega]| - 1/2| \leq 5/\sqrt{N}$, 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 $|\mathcal{M}(R, S_L)[\tau, \omega] - 1| \leq 1/\sqrt{N}$, i.e., $(\tau_0, \omega_0) = (\tau, \omega)$.

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

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

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

Looking back to Problem I-B.1, we see that, under genericity assumption, the flag method provides a fast computation, in $O(mN \log N)$ operations, of the channel parameters of channel with sparsity m. In particular, it calculates the GPS parameters—see Problem I-C.1—in $O(N \log N)$ operations. Indeed, Identity (I-G.1), together with bilinearity of inner product, implies that

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

where R is the sequence (I-B.1), with $S = S_L$, assuming that (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 $\alpha_k \approx \mathcal{M}(R, S_L)[\tau_k, \omega_k]$.

Fig. 7 provides a visual illustration for the matched filter matrix in three paths scenario. This completes our solutions of Problem I-B.1—The Channel Estimation Problem, and of Problem I-C.1—The GPS Problem.

I. *Applications to Radar*

The model of radar works as follows [10]. A radar transmits—see Fig. 8 for illustration—a sequence $S \in \mathcal{H}$ which bounces back from m targets. Using the sampling procedure described in Section I-A, the radar receives as an echo the following sequence $R \in \mathcal{H}$:

$$R[n] = \sum_{k=1}^{m} \alpha_k \cdot e(\omega_k n) \cdot S[n - \tau_k] + \mathcal{W}[n], \; n \in \mathbb{Z}_N,$$

[9] 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*.

[10] This is important in various real-world applications, e.g., in GPS, radar, and CDMA communication.

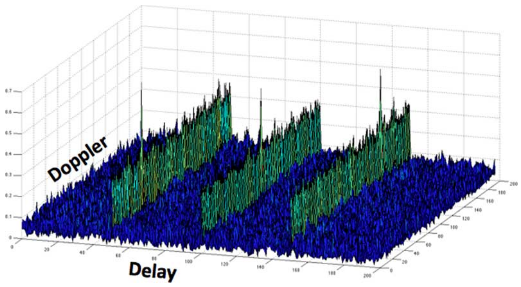

Fig. 7. $|\mathcal{M}(R, S_L)|$, for $L = \{(0, \omega)\}$, and $(\alpha_k, \tau_k, \omega_k) = (\frac{1}{\sqrt{3}}, 50k, 50k)$, $k = 1, 2, 3$.

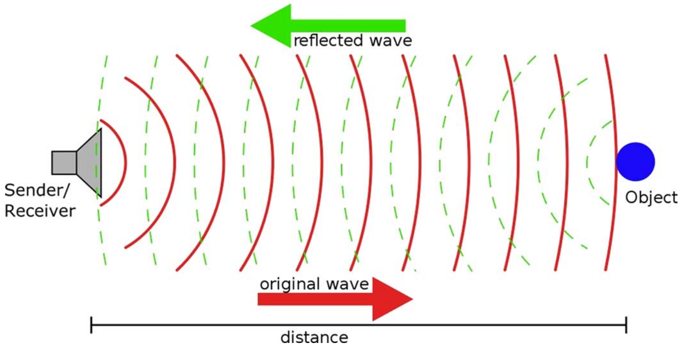

Fig. 8. Radar transmits wave and recieves echo.

where $\alpha_k \in \mathbb{C}$, $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\omega_k \in \mathbb{Z}_N$ 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 distances to the targets, and their relative radial velocities with respect to the radar, we need to solve the following:

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

This is a particular case of the channel estimation problem. Under the genericity assumption, the flag method solves it in $O(mN \log N)$ operations.

Remark I-I.2 ***(Velocity Resolution)****:* From Remark I-B.2, follows that larger N used by the radar implies better resolution of recognized radial velocities of the targets.

J. What You Can Find in This Paper

- In the Section I: You can read about the derivation of the discrete delay-Doppler channel model, and the flag method for effective channel estimation. In addition, concrete applications to GPS, and radar 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.

II. The Heisenberg and Weil Operators

The flag sequences (see Section I-G) are defined, constructed and analyzed using two special classes of operators that act on the Hilbert space of 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 sequences by

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

where $f \in \mathcal{H}$, $n \in \mathbb{Z}_N$, and for the rest of this paper we use 2^{-1} to denote $\frac{N+1}{2}$ which is the inverse of 2 modulo N.

B. The Weil Operators

Consider the discrete Fourier transform

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

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

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

where $\pi(\tau, \omega)$ are the Heisenberg operators, and $\circ$ denotes composition of transformations. In [20] Weil found a large family of operators, which includes the DFT. His operators satisfy identities analogous to (II-B.1). In more details, consider the 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* with respect to the operation of matrix multiplication (see [2] for the notion of a group). 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

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

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:

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

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 $DFT \in \mathrm{Sol}(\Sigma_{\mathrm{w}})$. Using results, from group representation theory, known as Stone-von Neumann (S-vN) theorem and Schur's lemma, one can show (see [6, Section 2.3]) 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 [20]:

*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 $\rho(gh) = \rho(g) \circ \rho(h)$, for every $g, h \in G$.

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

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

which is called the *Weil representation* [20] . We will call each $\rho(g)$, $g \in G$, a *Weil operator.*

1) Formulas for Weil Operators: It is important for our study to have the following explicit formulas [4], [6] for the Weil operators:

- *Fourier.* We have

$$\left[\rho\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} f\right][n] = i^{\frac{N-1}{2}} DFT(f)[n]; \quad \text{(II-B.4)}$$

- *Chirp.* We have

$$\left[\rho\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} f\right][n] = e(2^{-1}cn^2) f[n]; \quad \text{(II-B.5)}$$

- Scaling. We have

$$\left[\rho\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} f\right][n] = \left(\frac{a}{N}\right) f[a^{-1}n], \quad \text{(II-B.6)}$$

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.

The group G admits 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

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

and w is the Weyl element. This means that every element $g \in G$ can be written in the form

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

where $u, u', u'' \in U,\ s, s' \in A$, and w is the Weyl element. Hence, because ρ is homomorphism, i.e., $\rho(gh) = \rho(g) \circ \rho(h)$ 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. We define them as a sum of a pseudorandom sequence and a structural sequence. The design of these sequences is done using group representation theory. The pseudorandom sequences are designed [7], [8], [19] using the Weil representation operators (II-B.3), and will be called Weil (spike) sequences[11]. The structural sequences are designed [9], [10] using the Heisenberg representation operators (II-A.1), and will be called Heisenberg (line) sequences. Finally, the flag sequences are defined as a sum of Heisenberg sequence, and a Weil sequence, and will be called Heisenberg-Weil flag sequences.

A. The Heisenberg (Lines) Sequences

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

$$\pi(\tau, \omega) \circ \pi(\tau', \omega') = e(\omega\tau' - \tau\omega') \cdot \pi(\tau', \omega') \circ \pi(\tau, \omega). \quad \text{(III-A.1)}$$

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

$$\pi(l) : \mathcal{H} \to \mathcal{H},\ l \in L. \quad \text{(III-A.2)}$$

The simultaneous diagonalization theorem from linear algebra implies the existence of orthonormal basis $\mathcal{B}_L$ for $\mathcal{H}$, consisting of common eigensequences for all the operators (III-A.2). Moreover, in our specific case there exists an explicit basis (see Section IV-A for explicit formulas) $\mathcal{B}_L = \{f_{L,\psi}\}$, parametrized by *characters*[12] ψ of L. We will call the sequences $f_{L,\psi}$ Heisenberg sequences, and they satisfy

$$\pi(l) f_{L,\psi} = \psi(l) f_{L,\psi}, \text{ for every } l \in L.$$

The following theorem—see Fig. 9 for a demonstration of Property 1—describes their correlations properties:

[11] For the purpose of the Flag method, other pseudorandom signals may work.

[12] A functions $\psi : L \to \mathbb{C}^* = \mathbb{C} - 0$, is called *character* if it satisfies $\psi(l + l') = \psi(l)\psi(l')$, for every $l, l' \in L$.

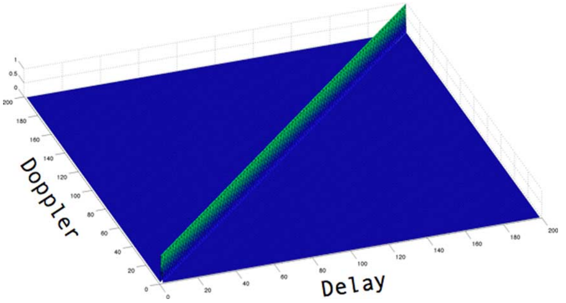

Fig. 9. $|\mathcal{M}(f_L, f_L)|$ for $L = \{(\tau, \tau)\}$.

Theorem III-A.1: The Heisenberg sequences satisfy the following properties:

1) *Line.* For every line $L \subset V$, and every $f_L \in \mathcal{B}_L$, we have

$$|\mathcal{M}(f_L, f_L)[\tau, \omega]| = \begin{cases} 1, & \text{if } (\tau, \omega) \in L; \\ 0, & \text{if } (\tau, \omega) \notin L, \end{cases}$$

and moreover, $\mathcal{M}(f_L, f_L)[0, 0] = 1$.

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

$$|\mathcal{M}(f_{L_1}, f_{L_2})[\tau, \omega]| = 1/\sqrt{N},$$

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

Theorem III-A.1 can be deduced from general results obtained in [9], [10]. However, for the sake of completeness we supply a direct proof in Section VI-A.

B. The Weil (Spikes) Sequences

We follow closely the works [7], [8]. The group $G = SL_2(\mathbb{Z}_N)$ is non-commutative, but contains a special class of maximal commutative subgroups called tori [7]. There are two types of tori in G, split and non-split . A subgroup $T \subset G$ is called *split torus* if there exists $g \in G$ such that

$$T = gAg^{-1} = \{gsg^{-1};\ s \in A\},$$

where A is the subgroup (II-B.7) of diagonal matrices in G. A subgroup $T \subset G$ is called *non-split* torus if there exists $g \in G$ such that

$$T = gKg^{-1},$$

where

$$K = \left\{g \in G;\ g^t g_\epsilon g = g_\epsilon\right\},\quad g_\epsilon = \begin{pmatrix} 1 & 0 \\ 0 & -\epsilon \end{pmatrix},$$

with $\epsilon \in \mathbb{Z}_N$ a fixed non-square[13].

Example III-B.1: If $N - 3$ is divisible by 4, then $\epsilon = -1$ is a non-square in $\mathbb{Z}_N$. In this case, an example of a non-split torus is the group

$$K = \{g \in SL_2(\mathbb{Z}_N); g^t g = I\} = SO_2(\mathbb{Z}_N),$$

of orthogonal matrices with determinant equal to one. This group is also called the special orthogonal group.

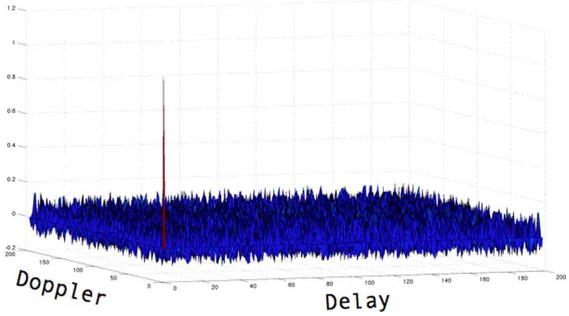

Fig. 10. $\mathcal{M}(\varphi_T, \varphi_T)$ for $T = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}; 0 \neq a \in \mathbb{Z}_N\}$.

Claim III-B.2: There are $(N+1)N/2$ split tori, and $(N-1)N/2$ non-split tori in G.

For a proof of Claim III-B.2 see Section VI-B.

For a given torus $T \subset G$, we have by (II-B.3) a commutative collection of diagonalizable Weil operators

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

The simultaneous diagonalization theorem from linear algebra implies the existence of orthonormal basis $\mathcal{B}_T$ for $\mathcal{H}$, consisting of common eigensequences for all the operators (III-B.1). Moreover, in our specific case there exists [7], [8] an explicit basis (see Section IV-B for explicit formulas in the case T is a split torus) $\mathcal{B}_T = \{\varphi_{T,\chi}\}$, parametrized by *characters*[14] χ of T. The sequences $\varphi_{T,\chi}$ satisfy

$$\rho(g)\varphi_{T,\chi} = \chi(g)\varphi_{T,\chi},\ \text{for every}\ g \in T. \qquad \text{(III-B.2)}$$

Remark III-B.3: There is a small abuse of notation in (III-B.2). The torus T admits a unique non-trivial character χ_q—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 φ_{T,χ_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 [7], [8].

Let us denote by

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

the set of sequences in $\mathcal{B}_T$, which are not associated with the quadratic character. We will call them *Weil sequences.* The following theorem [7], [8]—see Fig. 10 for illustration of Property 1—describes their correlations properties:

Theorem III-B.4: The Weil sequences satisfy the following properties:

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

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

[13] An element $y \in \mathbb{Z}_N$ is called *square (non-square)* if there exists (does not exist) $x \in \mathbb{Z}_N$ such that $y = x^2$.

[14] A functions $\chi : T \to \mathbb{C}^*$, is called *character* if it satisfies $\chi(gg') = \chi(g)\chi(g')$, for every $g, g' \in T$.

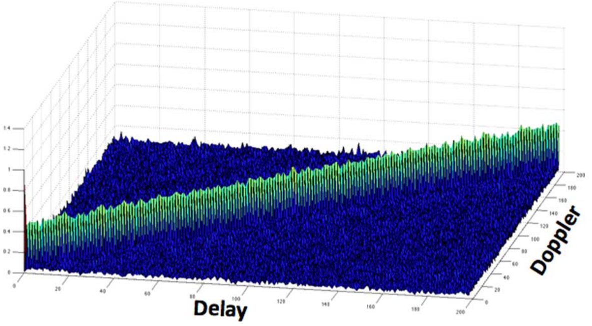

Fig. 11. $|\mathcal{M}(S_L, S_L)|$ for Heisenberg-Weil flag with $L = \{(\tau, \tau)\}$.

and moreover, $\mathcal{M}(\varphi_T, \varphi_T)[0, 0] = 1$.

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

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

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

C. The Heisenberg-Weil Sequences

We define the *Heisenberg-Weil* sequences. These are sequences in $\mathcal{H}$, which are of the form $S_L = (f_L + \varphi_T)/\sqrt{2}$, where f_L and φ_T are Heisenberg and Weil sequences, respectively. The following theorem—see Fig. 11 for illustration of Property 1—is the main technical result of this paper, and it describes their correlations properties:

Theorem III-C.1: The Heisenberg-Weil sequences satisfy the properties

1) *Flag.* For every line through the origin $L \subset V$, torus $T \subset G$, and every flag $S_L = (f_L + \varphi_T)/\sqrt{2}$, with $f_L \in \mathcal{B}_L$, $\varphi_T \in \mathcal{S}_T$, we have

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

where $|\epsilon_N| \leq 2/\sqrt{N}$, and $|\varepsilon_N| \leq 3/\sqrt{N}$, and moreover, $\mathcal{M}(S_L, S_L)[0, 0] = 1 + \epsilon_N$.

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 $S_{L_j} = \left(f_{L_j} + \varphi_{T_j}\right)/\sqrt{2}$, 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 for every $(\tau, \omega) \in V$

$$|\mathcal{M}(S_{L_1}, S_{L_2})[\tau, \omega]| \leq \begin{cases} 9/(2\sqrt{N}), & \text{if } T_1 \neq T_2; \\ 7/(2\sqrt{N}), & \text{if } T_1 = T_2. \end{cases}$$

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

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 and GPS problems in $O(N \log N)$ operations, and channel estimation, and radar problems in $O(mN \log N)$ operations for channel of sparsity m (see details in Section I).

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

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 an efficient algorithm. 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 $L_c = \text{span}\,\{(1, c)\}$, $c \in \mathbb{Z}_N$.
- Line with infinite slope. This is the line $L_\infty = \text{span}\,\{(0, 1)\}$.

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

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

  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

$$\mathcal{B}_{L_\infty} = \{\delta_b; \; b \in \mathbb{Z}_N\}, \qquad \text{(IV-A.2)}$$

  of Heisenberg sequences associated with the line L_∞, where the δ_b's denote the Dirac delta functions, $\delta_b[n] = 1$ if $n = b$, and $= 0$ otherwise.

The validity of Formula (IV-A.2) is immediate from Definition (II-A.1). For a derivation of Formulas (IV-A.1), see Section VI-D.

B. Formulas for the Weil Sequences

We describe explicit formulas for the Weil sequences associated with split tori [5], [7], [8]. 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: Recall (see Section III-B) that a split torus $T \subset G$ is a subgroup of the form $T = T_g$, $g \in G$, with

$$T_g = gAg^{-1},$$

where $A \subset G$ is the subgroup of all diagonal matrices (II-B.7).

We denote by $\mathcal{T}=\{T_g;\ g\in G\}$ the set of all split tori in G. A direct computation shows that the collection of all T_g's with

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

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. Consider the group $\mathbb{Z}_N^*$ of all nonzero 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—called *generator* (sometime called *primitive root)*— $r\in\mathbb{Z}_N^*$ such that

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

We fix, for the rest of this section, a generator $r\in\mathbb{Z}_N^*$, and we define the discrete logarithm map $\log_r:\mathbb{Z}_N^*\to\mathbb{Z}_{N-1}$ by

$$\log_r(n)=d,\ \text{ if }\ n=r^d.$$

A function $\chi:\mathbb{Z}_N^*\to\mathbb{C}^*$ is called *multiplicative character* if $\chi(xy)=\chi(x)\chi(y)$ 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., $\zeta\in\mu_{N-1}=\{\exp\left(\frac{2\pi i}{N-1}k\right);\ k=0,\dots,N-2\}$, and define a multiplicative character by

$$\chi_\zeta(n)=\zeta^{\log_r(n)},\ n\in\mathbb{Z}_N^*. \qquad \text{(IV-B.2)}$$

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. We obtain

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

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

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

  $$\varphi_{\chi_\zeta}[n]=\begin{cases}\frac{1}{\sqrt{N-1}}\chi_\zeta(n) & \text{if } n\neq 0;\\ 0 & \text{if } n=0,\end{cases} \qquad \text{(IV-B.3)}$$

  where χ_ζ is the character defined by (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 the set of Weil sequences

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

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

  $$\varphi_{\chi_\zeta^{u_c}}[n]=e(2^{-1}cn^2)\varphi_{\chi_\zeta}[n], \qquad \text{(IV-B.4)}$$

  for every $n\in\mathbb{Z}_N$, and φ_{χ_ζ} is the sequence given by (IV-B.3).
- Formulas for Weil sequences associated with other tori $T_g,\ g\in G$. For $k\in\mathbb{Z}_N$, and $f\in\mathcal{H}$, we define $(\mathsf{h}_k f)[n]=f[kn]$, and $(\mathsf{m}_k f)[n]=e(2^{-1}kn^2)f[n]$. In addition, for $0\neq y\in\mathbb{Z}_N$ we denote by $\left(\frac{y}{N}\right)$ the Legendre symbol of y, which is equal 1, or -1, if x is a square, or not, respectively. Then, for the torus T_g associated with the element

  $$g=\begin{pmatrix}1 & b\\ c & 1+bc\end{pmatrix},\ b,c\in\mathbb{Z}_N,\ b\neq 0, \qquad \text{(IV-B.5)}$$

  we have the set of Weil sequences

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

  where $\varphi_{\chi_\zeta^g}\in\mathcal{H}$ denotes the sequence

  $$\varphi_{\chi_\zeta^g}[n]=C_b\cdot\mathsf{m}_{\frac{1+bc}{b}}DFT\left(\mathsf{m}_b\mathsf{h}_b\varphi_{\chi_\zeta}\right)[n], \qquad \text{(IV-B.6)}$$

  with φ_{χ_ζ} the sequence given by (IV-B.3), and $C_b=i^{\frac{N-1}{2}}\left(\frac{b}{N}\right)$.

The fact that Formula (IV-B.3) defines a set of Weil sequences is immediate from Identity (II-B.6). For a derivation of Weil sequences with Formulas (IV-B.4) and (IV-B.6), see Section VI-E.

C. Examples of Explicit Flag Sequences

We fix $N=37$, and note that $r=2$ is a generator for $\mathbb{Z}_{37}^*$, i.e., $\mathbb{Z}_{37}^*=\{2^d \bmod(37);\ d=0,1,\dots,35\}$. We give two examples.

1) Flag Associated With the Time Line and the Diagonal Torus: We show how to use Formulas (IV-A.1), and (IV-B.3), to obtain explicit flag sequence

$$S_{L_0}[n]=\left(f_{0,1}[n]+\varphi_{\chi_{-1}}[n]\right)/\sqrt{2},\ n\in\mathbb{Z}_{37},$$

associated with the line L_0, and the diagonal torus A.

- Heisenberg sequence associated with the time line. We take in (IV-A.1), $c=0$, $b=1$, and obtain the Heisenberg sequence

  $$f_{0,1}[n]=\frac{1}{\sqrt{37}}\exp(2\pi in/37),\ n\in\mathbb{Z}_{37}.$$

- Weil sequence associated with the diagonal torus. We choose $\mu_{36}\ni\zeta=\exp(\frac{2\pi i}{36}18)=-1$. We have then the character χ_{-1} of $\mathbb{Z}_{37}^*$, given by $\chi_{-1}(2^d \bmod(37))=(-1)^d$, $d=0,1,\dots,35$. Hence, using formula (IV-B.3) we obtain the Weil sequence $\varphi_{\chi_{-1}}[n]$, $n\in\mathbb{Z}_{37}$, given by

  $$\varphi_{\chi_{-1}}[n]=\begin{cases}\frac{1}{\sqrt{36}}(-1)^{\log_2(n)} & \text{if } n\neq 0;\\ 0 & \text{if } n=0.\end{cases}$$

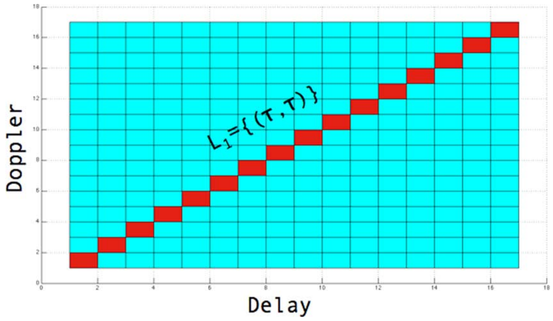

Fig. 12. $\mathcal{M}(\varphi,\phi)[\tau,\tau]=\left[\mathsf{m}_{-1,0}(\varphi)*\mathsf{m}_{1,0}(\overline{\phi})_{\text{-}}\right][\tau]$ on L_1.

2) Flag Associated With the Diagonal Line and a Non-Diagonal Torus: We show how to use Formulas (IV-A.1), and (IV-B.6), to obtain explicit flag sequence

$$S_{L_1}[n]=\left(f_{1,0}[n]+\varphi^g_{\chi_i}[n]\right)/\sqrt{2},\ n\in\mathbb{Z}_{37},$$

associated with the line L_1, and the torus $T_g=gAg^{-1}$, with g given by (IV-B.5), with $c=0$ and $b=1$.

- Heisenberg sequence associated with the diagonal line. We take in (IV-A.1), $c=1$, $b=0$, and obtain the Heisenberg sequence

$$f_{1,0}[n]=\frac{1}{\sqrt{37}}\exp(\pi i n^2/37),\ n\in\mathbb{Z}_{37}.$$

- Weil sequence associated with the torus T_g . We choose $\mu_{36}\ni\zeta=\exp(\frac{2\pi i}{36}9)=i$. We have then the character χ_i of $\mathbb{Z}^*_{37}$, given by $\chi_i(2^d \bmod(37))=i^d$, $d=0,1,\ldots,35$. Hence, using formula (IV-B.6) we obtain the Weil sequence

$$\varphi_{\chi_i^g}[n]=-\mathsf{m}_1 DFT\left(\mathsf{m}_1\varphi_{\chi_i}\right)[n],$$

where $\varphi_{\chi_i}[n]=\frac{1}{\sqrt{36}}i^{\log_2(n)}$ if $n\neq 0$, and $\varphi_{\chi_i}[0]=0$.

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 matched filter matrix to any given line in the time-frequency plane (see Remark I-E.2). In this section we provide an algorithm for this task. The upshot is—see Fig. 12 for illustration of the case of the diagonal line—that the restriction of the matched filter matrix to a line is a certain convolution that can be computed fast using FFT. For $a,b\in\mathbb{Z}_N$, $\varphi\in\mathcal{H}$, we define

$$\mathsf{m}_{a,b}(\varphi)[n]=e(2^{-1}an^2+bn)\varphi[n],\ \text{and}\ \varphi_-[n]=\varphi[-n].\tag{V-.1}$$

In addition, for sequences $\varphi,\phi\in\mathcal{H}$, we denote by $\varphi*\phi\in\mathcal{H}$ their convolution

$$\left(\varphi*\phi\right)[\tau]=\sum_{n\in\mathbb{Z}_N}\varphi[n]\phi[\tau-n],\ \tau\in\mathbb{Z}_N.\tag{V-.2}$$

We consider two cases:

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

$$\begin{aligned}&\mathcal{M}(\varphi,\phi)[\tau(1,c)+(0,\omega)]\\&=\left[\mathsf{m}_{-c,-\omega}(\varphi)*\mathsf{m}_{c,0}(\overline{\phi})_{\text{-}}\right][\tau],\end{aligned}\tag{V-.3}$$

where $\overline{\phi}$ denotes the complex conjugate of the sequence ϕ.

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

$$\mathcal{M}(\varphi,\phi)[\omega(0,1)+(\tau,0)]=\sqrt{N}DFT(\varphi\cdot\overline{\phi}_{-\tau})[\omega],\tag{V-.4}$$

where $\overline{\phi}_{-\tau}[n]=\overline{\phi}[n-\tau]$..

The validity of Formula (V-.4) is immediate from the definition of the matched filter. For a verification of Formula (V-.3) see Section VI-F.

VI. Proofs

A. Proof of Theorem III-A.1

We will use two lemmas. First, let $L\subset V$ be a line, and for a character $\psi:L\to\mathbb{C}^*$, and vector $v\in V$, define the character $\psi_v:L\to\mathbb{C}^*$, by $\psi_v(l)=e(\Omega(v,l))\psi(l)$, $l\in L$, where $\Omega:V\times V\to\mathbb{Z}_N$ is the symplectic form $\Omega[(\tau,\omega),(\tau',\omega')]=\tau\omega'-\omega\tau'$. We have

Lemma VI-A.1: Suppose $f_L\in\mathcal{H}$ is a ψ-eigensequence for L, i.e., $\pi(l)f_L=\psi(l)f_L$, for every $l\in L$. Then the sequence $\pi(v)f_L$ is ψ_v-eigensequence for L.

For the second Lemma, let $L,M\subset V$ be two lines, and $g\in G=SL_2(\mathbb{Z}_N)$ such that $M=gL=\{gl;\ l\in L\}$. For a character $\psi:L\to\mathbb{C}^*$, define the character $\psi^g:M\to\mathbb{C}^*$, by $\psi^g(m)=\psi(g^{-1}m)$, for every $m\in M$. We have

Lemma VI-A.2: Suppose f_L is a ψ-eigensequence for L, i.e., $\pi(l)f_L=\psi(l)f_L$, for every $l\in L$. Then the sequence $f_M=\rho(g)f_L$ is ψ^g-eigensequence for M.

We verify Lemmas VI-A.1, and VI-A.2, after the proof of the line, and almost-orthogonality properties.

1) Proof of Line Property: Let $f_L\in\mathcal{B}_L$ be a ψ-eigensequence. For $v\in V$ we have

$$\begin{aligned}|\mathcal{M}(f_L,f_L)[v]|&=|\langle f_L,\ \pi(v)f_L\rangle|\\&=\begin{cases}1, & \text{if } v\in L;\\ 0, & \text{if } v\notin L,\end{cases}\end{aligned}$$

where in the first equality we use the definition of $\mathcal{M}$, and in the second we use Lemma VI-A.1. This completes the proof of the line property.

2) Proof of Almost-Orthogonality Property: Consider the time and frequency lines, $L_0=\{(\tau,0)\}$, and $L_\infty=\{(0,\omega)\}$, respectively. Recall that (see Section IV-A.2) $\mathcal{B}_{L_0}=\{f_a;\ a\in\mathbb{Z}_N\}$, where $f_a[n]=\frac{1}{\sqrt{N}}e(an)$, $n\in\mathbb{Z}_N$, and $\mathcal{B}_{L_\infty}=\{h_b, b\in\mathbb{Z}_N\}$, where $h_b=\delta_b$. Hence, for every $a,b\in\mathbb{Z}_N$ we have

$$|\mathcal{M}(f_a,h_b)[v]|=1/\sqrt{N},\ v\in V.$$

This implies

Step 1. The almost-orthogonality holds for every $f_{L_0} \in \mathcal{B}_{L_0}$, and $f_{L_\infty} \in \mathcal{B}_{L_\infty}$.

Next, let $L, M \subset V$ be any two distinct lines in V, and let $f_L \in \mathcal{B}_L$, $f_M \in \mathcal{B}_M$.

Step 2. The almost-orthogonality holds for f_L and f_M. Indeed, it is easy to see that there exists $g \in G = SL_2(\mathbb{Z}_N)$ such that $gL = L_0$, and $gM = L_\infty$. From Lemma VI-A.2 and the unitarity of $\rho(g)$ we have that up to unitary scalars $f_{L_0} = \rho(g) f_L \in \mathcal{B}_{L_0}$, and $f_{L_\infty} = \rho(g) f_M \in \mathcal{B}_{L_\infty}$. Hence, we obtain for every $v \in V$

$$\begin{aligned} |\mathcal{M}(f_L, f_M)[v]| &= |\langle f_L,\ \pi(v) f_M\rangle| \\ &= |\langle \rho(g) f_L,\ \rho(g)\pi(v) f_M\rangle| \\ &= |\langle \rho(g) f_L,\ \pi(gv)\rho(g) f_M\rangle| \\ &= |\mathcal{M}(f_{L_0}, f_{L_\infty})[gv]| \\ &= 1/\sqrt{N}, \end{aligned}$$

where in the second equality we use the unitarity of $\rho(g)$, in the third equality we use Identity (II-B.2), and finally in the last equality we use Step 1. This completes the proof of the almost orthogonality property, and of Theorem III-A.1.

3) Proof of Lemma VI-A.1: For $l \in L$ we have

$$\begin{aligned} \pi(l)[\pi(v) f_L] &= e(\Omega(v, l))\pi(v)\pi(l) f_L \\ &= e(\Omega(v, l))\psi(l)[\pi(v) f_L], \end{aligned}$$

where in the first equality we use Identity (III-A.1). This completes the Proof of Lemma VI-A.1.

4) Proof of Lemma VI-A.2: For $l \in L$ we have

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

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

B. Proof of Claim III-B.2

We use standard facts on $G = SL_2(\mathbb{Z}_N)$ and its toral subgroups. Denote by $\mathcal{T}_s$ and $\mathcal{T}_{ns}$, the collection of all split, and non-split tori, respectively. The group G acts, by conjugation, transitively, on both $\mathcal{T}_s$ and $\mathcal{T}_{ns}$. For a torus $T \subset G$ its *stabilizer* with respect to this action is its *normalizer* subgroup $N(T) = \{g \in G;\ gTg^{-1} = T)$. Hence, we have $\#\mathcal{T}_s = \#G/\#N(A)$, and $\#\mathcal{T}_{ns} = \#G/\#N(K)$. A direct calculation shows that $\#G = (N^2 - 1)N$, and $\#N(A) = 2(N-1)$, $\#N(K) = 2(N+1)$. Hence,

$$\#\mathcal{T}_s = (N+1)N/2, \text{ and } \#\mathcal{T}_{ns} = (N-1)N/2.$$

This completes the proof of Claim III-B.2.

C. Proof of Theorem III-C.1

1) Flag Property: Let $S_L = (f_L + \varphi_T)/\sqrt{2}$. We have

$$\begin{aligned} \mathcal{M}(S_L, S_L) = [&\mathcal{M}(f_L, f_L) + \mathcal{M}(f_L, \varphi_T) \\ &+ \mathcal{M}(\varphi_T, f_L) + \mathcal{M}(\varphi_T, \varphi_T)]/2. \end{aligned}$$

We will show that

$$|\mathcal{M}(\varphi_T, f_L)[\tau, \omega]| \leq 2/\sqrt{N},\ \tau, \omega \in \mathbb{Z}_N. \tag{VI-C.1}$$

Noting that $\mathcal{M}(f_L, \varphi_T)[\tau, \omega] = \overline{\mathcal{M}(\varphi_T, f_L)[-\tau, -\omega]}$ we obtain from (VI-C.1) also the same bound for $\mathcal{M}(f_L, \varphi_T)$. Having this, using Theorems III-A.1 and III-B.4 we can deduce the Flag Property. So assume $\pi(l) f_L = \psi(l) f_L$ for $l \in L$. By Lemma VI-A.1, it is enough to bound the inner product

$$|\langle \varphi_T, f_L\rangle| \leq 2/\sqrt{N}. \tag{VI-C.2}$$

We proceed in two steps.

Step 1. The bound (VI-C.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 [8] it was shown that for every Weil sequence φ_T we have

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

Step 2. The bound (VI-C.1) holds for every line L. We will use the following lemma. Consider a torus $T \subset G$, and an element $g \in G$. Then we can define a new torus $T_g = gTg^{-1} = \{ghg^{-1};\ h \in T\}$. For a character $\chi : T \to \mathbb{C}^*$, we can associate a character $\chi^g : T_g \to \mathbb{C}^*$, by $\chi^g(ghg^{-1}) = \chi(h)$, for every $h \in T$. We have

Lemma VI-C.1: 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-C.1, see Section VI-C.2.

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

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

where the first equality is by the unitarity of $\rho(g)$. Hence, by Step 1, we obtain the desired bound also in this case.

2) Proof of Lemma VI-C.1: For $h \in T$ we have

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

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

3) Almost Orthogonality: Let $S_{L_j} = \left(f_{L_j} + \varphi_{Tj}\right)/\sqrt{2}, j = 1, 2$, as in the assumptions. We have

$$\begin{aligned}\mathcal{M}(S_{L_1}, S_{L_2}) = [&\mathcal{M}(f_{L_1}, f_{L_2}) + \mathcal{M}(f_{L_1}, \varphi_{T_2}) \\ &+ \mathcal{M}(\varphi_{T_1}, f_{L_2}) + \mathcal{M}(\varphi_{T_1}, \varphi_{T_2})]/2.\end{aligned}$$

The result now follows from Theorem III-A.1, Theorem III-B.4, and the bound (VI-C.1). This completes our proof of the Almost Orthogonality Property, and of Theorem III-C.1.

D. Derivation of Formula IV-A.1

We have for the line L_0, i.e., for the operators $\pi(\tau, 0)$, $\tau \in \mathbb{Z}_N$, the following orthonormal basis of eigensequences:

$$\mathcal{B}_{L_0} = \{f_{0,b}[n] = \frac{1}{\sqrt{N}} e(bn); \quad b \in \mathbb{Z}_N\}.$$

Let us derive formulas for basis parametrized by a line with finite slope. From Lemma VI-A.2, we know that the Weil operator $\rho(u_c)$ associated with the unipotent element

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

maps $\mathcal{B}_{L_0}$ to the orthonormal basis $\mathcal{B}_{L_c} = \{f_{c,b} = \rho(u_c) f_{0,b}; \; b \in \mathbb{Z}_N\}$ of common eigensequences for the operators $\pi(\tau(1, c))$, $\tau \in \mathbb{Z}_N$. Hence, using Formula (II-B.5) we derive our desired basis

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

E. Derivation of Formulas (IV-B.4), and (IV-B.6)

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 $\chi^g(ghg^{-1}) = \chi(h)$, for every $h \in A$. Using Lemma VI-C.1, we deduce that for $g \in G$ the set

$$\mathcal{S}_{T_g} = \{\varphi_{\chi^g} = \rho(g)\varphi_\chi \; ; \; \chi \text{ is character of } A, \; \chi \neq \chi_q\},$$

is a set of Weil sequences associated with T_g. Specializing to the characters $\chi = \chi_\zeta$, $1 \neq \zeta \in \mu_{N-1}$, of A, and the associated sequence $\varphi_{\chi_\zeta} \in \mathcal{S}_A$ given by (IV-B.3), we can proceed to derive the formulas.

1) Derivation of Formula (IV-B.4): For the unipotent element

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

we have

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

for every $n \in \mathbb{Z}_N$, where the second equality is by Formula (II-B.5). This completes our verification of Formula (IV-B.4).

2) Derivation of Formula (IV-B.6): For the element

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

its Bruhat decomposition is

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

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

$$\begin{aligned}\varphi_{\chi_\zeta^g}[n] &= \left[\rho(g)\varphi_{\chi_\zeta}\right][n] \\ &= C_b \cdot \mathsf{m}_{\frac{1+bc}{b}} DFT\left(\mathsf{m}_b \mathsf{h}_b \varphi_{\chi_\zeta}\right)[n],\end{aligned}$$

where, in the second equality we use identity (VI-E.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.6).

F. Verification of Formula (V-.3)

We verify Formula (V-.3) for the matched filter $\mathcal{M}(\varphi, \phi)$, $\varphi, \phi \in \mathcal{H}$, restricted to a line with finite slope. We define $\mathcal{M}_\pi(\varphi, \phi)[\tau, \omega] = \langle \varphi, \pi(\tau, \omega)\phi \rangle$, where $\pi(\tau, \omega)$ are the Heisenberg operators (II-A.1). We note that

$$\mathcal{M}_\pi(\varphi, \phi)[\tau, \omega] = e(2^{-1}\tau\omega)\mathcal{M}(\varphi, \phi)[\tau, \omega]. \tag{VI-F.1}$$

The element

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

satisfies

$$\begin{cases} u_{-c}(1, c) = (1, 0), \\ u_{-c}(0, \omega) = (0, \omega). \end{cases} \tag{VI-F.2}$$

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

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

where, the second equality is by the unitarity of ρ, the third equality is by Identities (II-B.2), (VI-F.2), the forth equality is by Formula (II-B.5) and the definition (V-.1), and the last equality is by definition (V-.2) of $*$. Using Identity (VI-F.1), we obtain Formula (V-.3).

ACKNOWLEDGMENT

Warm thanks to J. Bernstein for his support and encouragement in interdisciplinary research. We are grateful to J. Lima, and A. Sahai, for sharing with us their 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. Finally, we thank the referees for many important remarks.

References

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

[2] M. Artin, *Algebra*. Englewood Cliffs, NJ, USA: Prentice Hall, 1991.

[3] A. Fish, S. Gurevich, R. Hadani, A. Sayeed, and O. Schwartz, "Delay-Doppler channel estimation with almost linear complexity," presented at the IEEE Int. Symp. Information Theory, Cambridge, MA, USA, Jul. 1–6, 2012.

[4] P. Gerardin, "Weil representations associated to finite fields," *J. Algebra*, vol. 46, pp. 54–101, 1977.

[5] S. W. Golomb and G. Gong, "Signal design for good correlation," in *For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[6] S. Gurevich, R. Hadani, and R. Howe, "Quadratic reciprocity and the sign of Gauss sum via the finite Weil representation," *Int. Math. Res. Notices*, vol. 2010, no. 19, pp. 3729–3745.

[7] S. Gurevich, R. Hadani, and N. Sochen, "The finite harmonic oscillator and its associated sequences," in *Proc. PNAS*, Jul. 22, 2008, vol. 105, pp. 9869–9873, 29.

[8] S. Gurevich, R. Hadani, and N. Sochen, "The finite harmonic oscillator and its applications to sequences, communication and radar," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, Sep. 2008.

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

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

[11] J. M. O'Toole, M. Mesbah, and B. Boashash, "Accurate and efficient implementation of the time-frequency matched filter," *IET Signal Process.*, vol. 4, no. 4, pp. 428–437, 2010.

[12] C. M. Rader, "Discrete Fourier transforms when the number of data samples is prime," *Proc. IEEE*, vol. 56, pp. 1107–1108, 1968.

[13] S. Rickard, R. Balan, H. V. Poor, and S. Verdu, "Canonical Time-Frequency, time-scale and frequency-scale representations of time-varying channels," *Commun. Inf. Syst.*, vol. 5, no. 1, pp. 197–226, 2005.

[14] A. Sayeed, "Sparse and multipath wireless channels: Modeling and implications," presented at the ASAP, 2006.

[15] A. M. Sayeed and B. Aazhang, "Joint multipath-Doppler diversity in mobile wireless communications," *IEEE Trans. Commun.*, pp. 123–132, Jan. 1999.

[16] A. Sayeed and T. Sivanadyan, "Wireless communication and sensing in multipath environments using multiantenna transceivers," in *Handbook on Array Processing and Sensor Networks*, S. Haykin and K. J. R. Liu, Eds. Hoboken, NJ, USA: Wiley, 2010.

[17] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[18] S. Verdu, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[19] Z. Wang and G. Gong, "New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, Jul. 2011.

[20] A. Weil, "Sur certains groupes d'operateurs unitaires," *Acta. Math.*, vol. 111, pp. 143–211, 1964.

Alexander Fish obtained a Ph.D. in mathematics in 2007 from Hebrew University, Jerusalem, Israel. He conducts research in ergodic theory, and wireless communication. He had post-doc positions in Ohio State University, Mathematical Sciences Research Institute in Berkeley, and University of Wisconsin-Madison. From July 2012 he is a faculty member at the University of Sydney, Australia, in the School of Mathematics and Statistics.

Shamgar Gurevich obtained a Ph.D. in mathematics in 2006, from Tel Aviv University, Israel. He conducted research in group representation, applied algebra, and wireless communications. He had a post-doc position at UC Berkeley, California, 2006–2009, was a member at IAS, Princeton during 2009–2010, and joined the faculty of mathematics at the University of Wisconsin–Madison in August 2010.

Ronny Hadani obtained a Master degree in Applied Mathematics from the Weizmann Institute, Rehovot, Israel, in 2000. He obtained a Ph.D. in mathematics from Tel Aviv University, Israel, in 2006. He conducted research in group representation and its applications to cryo-electron microscopy, and wireless communications. He had a post-doc position at the University of Chicago during 2006–2009, and joined the faculty of mathematics at the University of Texas–Austin in August 2009.

Akbar M. Sayeed is Professor of Electrical and Computer Engineering at the University of Wisconsin-Madison. He received the B.S. degree from the University of Wisconsin-Madison in 1991, and the M.S. and Ph.D. degrees from the University of Illinois at Urbana-Champaign in 1993 and 1996, all in Electrical and Computer Engineering. He was a postdoctoral fellow at Rice University from 1996 to 1997. His research interests include wireless communications, statistical signal processing, multi-dimensional communication theory, time-frequency analysis, information theory, and applications in wireless communication and sensor networks. Dr. Sayeed is a recipient of the Robert T. Chien Memorial Award (1996) for his doctoral work at Illinois, the NSF CAREER Award (1999), the ONR Young Investigator Award (2001), and the UW Grainger Junior Faculty Fellowship (2003). He is a Fellow of the IEEE (2012), and has served the IEEE in a number of capacities, including as a member of the Signal Processing for Communications and Networking Technical Committee of the IEEE Signal Processing Society (2007–2012), as an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS (1999–2002), as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2005) and the IEEE JOURNAL ON SELECTED TOPICS IN SIGNAL PROCESSING (2008), and as the Technical Program co-chair for the 2007 IEEE Statistical Signal Processing Workshop and the 2008 IEEE Communication Theory Workshop.

Oded Schwartz is a postdoctoral researcher, working in the Parallel Computing Lab at UC Berkeley. He graduated with a Ph.D. in Computer Science from Tel-Aviv University and spent two years at TU-Berlin, and a few months at the Weizmann Institute of Science. Oded's research includes parallel computing, algorithmic linear algebra, high performance computing, and accelerating algorithms by reducing communication costs. In 2014 Oded will join the school of computer science and engineering at the Hebrew University, Jerusalem, Israel.