Delay-Doppler Channel Estimation in Almost Linear Complexity

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

Alexander Fish
Department of Mathematics
University of Wisconsin
Madison, WI 53706, USA
Email: afish@math.wisc.edu

Shamgar Gurevich
Department of Mathematics
University of Wisconsin
Madison, WI 53706, USA
Email: shamgar@math.wisc.edu

Ronny Hadani
Department of Mathematics
University of Texas
Austin, TX 78712, USA
Email: hadani@math.utexas.edu

Akbar Sayeed
Department of Electrical Engineering
University of Wisconsin
Madison, WI 53706, USA
Email: akbar@engr.wisc.edu

Oded Schwartz
Department of Computer Science
University of California
Berkeley, CA 94720, USA
Email: odedsc@eecs.berkeley.edu

***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 waveform of length N, and, in case of non-trivial relative velocity between transmitter and receiver, its arithmetic complexity is $O(N^2 \log(N))$. In this paper we introduce a novel approach of designing waveforms that allow faster channel estimation. Using group representation techniques we construct waveforms, 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, and mobile communication.**

I. Introduction

A basic step in many wireless communication protocols [12] is *channel estimation*: learning the channel parameters a signal undergoes while traveling from a transmitter to a receiver. In these notes 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, and mobile communication of fast moving users. We start by describing the channel estimation problem that we are going to solve.

A. Channel Estimation Problem

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 will 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 will be referred to as the *Hilbert space of digital signals*.

We consider the following mathematical model of time-frequency channel estimation [12]. There exists a collection of users, each one holds a waveform from $\mathcal{H}$ known to the base station (receiver). The users transmit their waveforms to the base station. Due to multipath effects, the waveforms undergo [11], [12] several time-frequency shifts as a result of reflections from

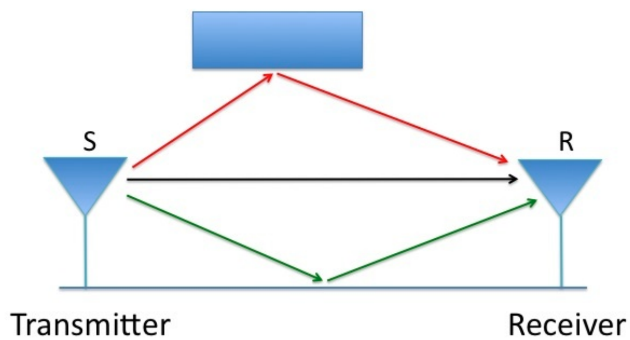

Fig. 1. Three paths scenario

various obstacles. We make the standard assumption of almost-orthogonality between waveforms of different users. Hence, if a user transmits $S \in \mathcal{H}$, then the base station receives $R \in \mathcal{H}$ of the form[1]

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

where m denotes the number of paths the transmitted signal 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 base station with respect to the transmitter, $\tau_k \in \mathbb{Z}_N$ encodes the delay along path k, and $\mathcal{W} \in \mathcal{H}$ denotes a random white noise of mean zero. The parameter m will be called the *sparsity* of the channel.

The objective is:

Problem I.1 (Channel estimatiom): 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.1).

Let us start with a simpler variant.

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

B. The Time-Frequency Shift (TFS) Problem

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

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

where $\mathcal{W} \in \mathcal{H}$ denotes a random white noise of mean zero, 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.2 (Time-frequency (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.2).

C. The Matched Filter (MF) Algorithm

A classical solution [4], [5], [6], [8], [12], [13], [14] to Problem I.2, is the *matched filter algorithm*. We define the following matched filter (MF) matrix of S and R:

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

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 $NSR \approx \frac{1}{SNR}$ is essentially (up to logarithmic factor) the inverse of the signal-to-noise ratio between the waveforms S and $\mathcal{W}$. For simplicity, we assume that the NSR is of size $O(1)$.

In order to extract the time-frequency shift (τ_0, ω_0), it is "standard" (see [4], [5], [6], [8], [12], [13], [14]) to use pseudo-random signal $S \in \mathcal{H}$ 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,

$$|\mathcal{M}(R,S)[\tau,\omega]| = \begin{cases} 1+\varepsilon_N, & \text{if } (\tau,\omega) = (\tau_0,\omega_0); \\ \varepsilon_N, & \text{if } (\tau,\omega) \neq (\tau_0,\omega_0), \end{cases} \qquad \text{(I.3)}$$

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

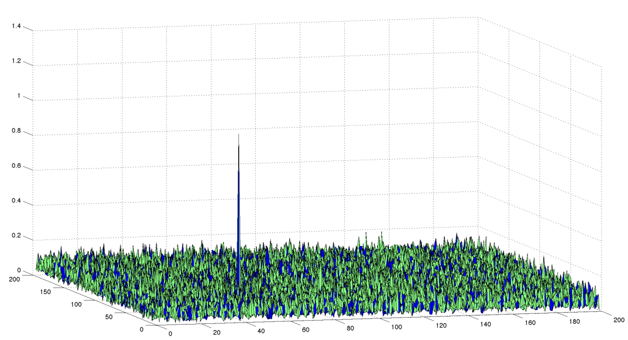

Fig. 2. $|\mathcal{M}(R,S)|$ *with pseudo-random* S, *and* $(\tau_0,\omega_0) = (50,50)$

Identity (I.3) 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 arithmetic (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.

Remark I.3 (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.

As a consequence of Remark I.3, one can solve TFS problem in $O(N^2\log(N))$ operations. To the best of our knowledge, the "line-by-line" computation is also the fastest known method [10]. This might be insufficient in case of large N. For example [1] in applications to GPS $N \geq 1000$. This leads to the following:

Problem I.4 (Fast matched filter (FMF)): Solve TFS problem in almost linear complexity.

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

D. The Flag Method

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" waveforms $S_{L_j} \in \mathcal{H}$, that we will call *flags*. They satisfy the following "flag property": For a receiver waveform R given by (I.2) with $S = S_{L_j}$, we have

$$\left|\mathcal{M}(R,S_{L_j})[\tau,\omega]\right| = \begin{cases} 2+\varepsilon_N, & \text{if } (\tau,\omega) = (\tau_0,\omega_0); \\ 1+\varepsilon_N, & \text{if } (\tau,\omega) \in L_j' \smallsetminus (\tau_0,\omega_0); \\ \varepsilon_N, & \text{if } (\tau,\omega) \in V \smallsetminus L_j', \end{cases} \qquad \text{(I.4)}$$

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

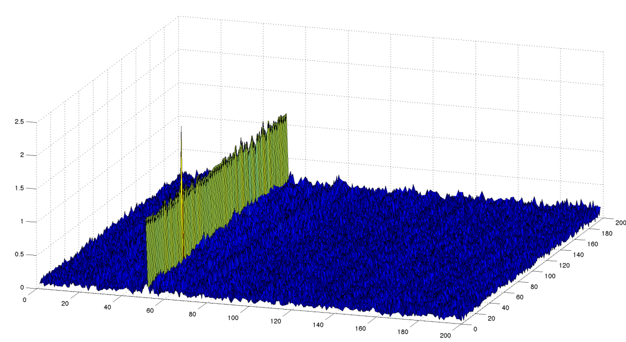

Fig. 3. $|M(R,S_L)|$ *for a flag* S_L, $L = \{(\tau,0)\}$, and $(\tau_0,\omega_0) = (50,50)$

Finally, for S_L and R satisfying (I.4), we have the following search method to solve FMF problem:

Flag Algorithm

- Choose a line $L^{\perp}$ transversal to L.
- 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 $L + (\tau_0,\omega_0)$.

- 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 is $O(N \log(N))$, using the FFT.

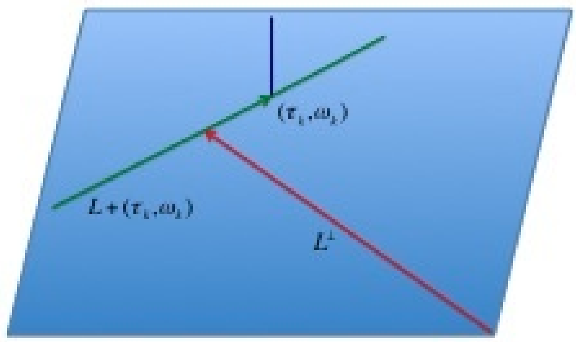

Fig. 4. Diagram of the flag algorithm

E. *The Cross Method*

Another solution to TFS problem, is the *cross method.* The idea is similar to the flag method. We will show how to associate with the $\frac{N+1}{2}$ distinct pairs of lines $L, M \subset V$ a system of almost-orthogonal waveforms $S_{L,M}$, that we will call *crosses.* The system satisfies

$$|\mathcal{M}(R, S_{L,M})[\tau, \omega]| = \begin{cases} 2+\varepsilon_N, \text{ if } (\tau,\omega)=(\tau_0,\omega_0); \\ 1+\varepsilon_N, \text{ if } (\tau,\omega)\in(L'\cup M')\smallsetminus(\tau_0,\omega_0); \\ \varepsilon_N, \text{ if } (\tau,\omega)\in V\smallsetminus(L'\cup M'), \end{cases}$$

where $\varepsilon_N = O(\frac{1}{\sqrt{N}})$, R is the receiver waveform (I.2), with $S = S_{L,M}$, and $L' = L + (\tau_0, \omega_0)$, $M' = M + (\tau_0, \omega_0)$.

The complexity of the cross method is $O(N \log(N))$. First, we find a line on which the time-frequency shift is located, and then searching for the spike on the line. However, applications of the cross method for channel estimation problem (I.1) is more involved, due to fake intersections, and will not be discussed in these notes.

F. *Solution to the Channel Estimation Problem*

Looking back to Problem I.1, we see that the flag method provides a fast solution, in $O(m \cdot N \log(N))$ operations, for channel estimation of channel with sparsity m. Indeed, identity (I.4), and almost orthogonality property, imply that $\alpha_k \approx \mathcal{M}(R, S_L)[\tau_k, \omega_k]/2$, $k = 1, ..., m$, where R is the waveform (I.1), with $S = S_L$.

II. The Heisenberg–Weil Flag System

The flag waveforms, that play the main role in the flag method, are of a special type. Each of them is a sum of a pseudorandom signal and a structural signal. 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 waveforms is done using group representation theory. The pseudorandom signals are designed [5], [6], [14] using the Weil representation, and will be called Weil (peak) signals[2]. The structural signals are designed [7], [8] using the Heisenberg representation, and will be called Heisenberg (lines) signals. We will call the collection of all flag waveforms, the Heisenberg–Weil flag system. In this section we briefly recall constructions, and properties of these waveforms. A more comprehensive treatment, including proofs, will appear in [3].

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

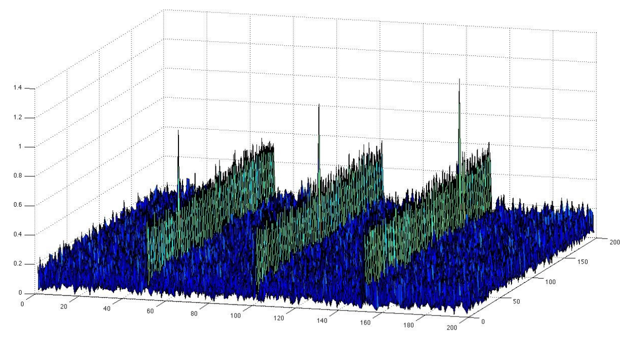

Fig. 5. $|\mathcal{M}(R, S_L)|$, $L = \{(\tau, 0)\}$, $(\alpha_k, \tau_k, \omega_k) = (\frac{1}{\sqrt{3}}, 50k, 50k)$, $k = 1, 2, 3$.

A. *The Heisenberg (Lines) System*

Consider the following collection of unitary operators, called Heisenberg operators, that act on the Hilbert space of digital signals by:

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

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

The operators (II.1) do not commute in general, but rather obey the Heisenberg commutation relations $\pi(\tau, \omega) \circ \pi(\tau', \omega') = e^{\frac{2\pi i}{N}(\tau\omega' - \omega\tau')} \cdot \pi(\tau', \omega') \circ \pi(\tau, \omega)$, where $\circ$ denotes composition of operators. The expression $\tau\omega' - \omega\tau'$ vanishes if (τ, ω), (τ', ω') belong to the same line. Hence, for a given line $L \subset V = \mathbb{Z}_N \times \mathbb{Z}_N$ we have a commutative collection of unitary operators

$$\pi(\ell) : \mathcal{H} \to \mathcal{H}, \ \ell \in L. \tag{II.2}$$

We use the theorem from linear algebra about simultaneous diagonalization of commuting unitary operators, and obtain [7], [8] a natural orthonormal basis $\mathcal{B}_L \subset \mathcal{H}$ consisting of common eigenfunctions for all the operators (II.2). 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 will need the following result [7], [8]:

Theorem II.1: The Heisenberg system satisfies the properties

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

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

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

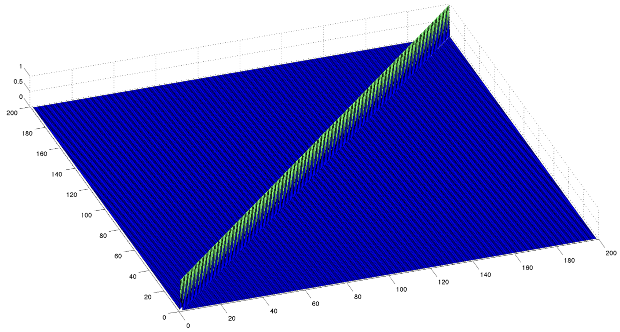

Fig. 6. $|\mathcal{M}(f_L, f_L)|$ for $L = \{(\tau, \tau)\}$

B. The Weil (Peaks) System

Consider the following collection of matrices

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

Note that G 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 $g \in G$ acts on the time-frequency plane V via the change of coordinates $v \mapsto g \cdot v$. 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:

$$\Sigma_g: \ \rho(g) \circ \pi(\tau, \omega) = \pi(g \cdot (\tau, \omega)) \circ \rho(g), \quad \tau, \omega \in \mathbb{Z}_N, \quad \text{(II.3)}$$

where π is defined by (II.1). Denote by $\mathrm{Sol}(\Sigma_g)$ the space of all solutions to System (II.3). The following is a basic result [15]:

Theorem II.2 (Stone–von Neumann–Schur-Weil): There exist a unique collection of solutions $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\ g \in G\}$, which are unitary operators, and satisfy the homomorphism condition $\rho(g \cdot h) = \rho(g) \circ \rho(h)$.

Denote by $U(\mathcal{H})$ the collection of all unitary operators on the Hilbert space of digital signals $\mathcal{H}$. Theorem II.2 establishes the map $\rho : G \to U(\mathcal{H})$, which is called the *Weil representation* [15]. The group G is not commutative, but contains a special class of maximal commutative subgroups called tori[3] [5], [6]. Each torus $T \subset G$ acts via the Weil operators

$$\rho(g) : \mathcal{H} \to \mathcal{H}, \ \ g \in T. \quad \text{(II.4)}$$

This is a commutative collection of diagonalizable operators, and it admits [5], [6] a natural orthonormal basis $\mathcal{B}_T$ for $\mathcal{H}$, consisting of common eigenfunctions. The system of all such bases $\mathcal{B}_T$, where T runs over all tori in G, will be called the *Weil (peaks) system*. We will need the following result [5], [6]:

Theorem II.3: The Weil system satisfies the properties

1) *Peak.* For every torus $T \subset G$, and every $\varphi_T \in \mathcal{B}_T$, we have
$$|\mathcal{M}[\varphi_T, \varphi_T](\tau, \omega)| = \begin{cases} 1, \text{ if } (\tau, \omega) = (0,0); \\ \leq \frac{2}{\sqrt{N}}, \text{ if } (\tau, \omega) \neq (0,0). \end{cases}$$
2) *Almost-orthogonality.* For every two tori $T_1, T_2 \subset G$, and every $\varphi_{T_1} \in \mathcal{B}_{T_1}$, $\varphi_{T_2} \in \mathcal{B}_{T_2}$, with $\varphi_{T_1} \neq \varphi_{T_2}$, we have
$$|\mathcal{M}[\varphi_{T_1}, \varphi_{T_2}](\tau, \omega)| \leq \begin{cases} \frac{4}{\sqrt{N}}, \text{ if } T_1 \neq T_2; \\ \frac{2}{\sqrt{N}}, \text{ if } T_1 = T_2, \end{cases}$$
for every $(\tau, \omega) \in V$.

[3]There are order of N^2 tori in $SL_2(\mathbb{Z}_N)$.

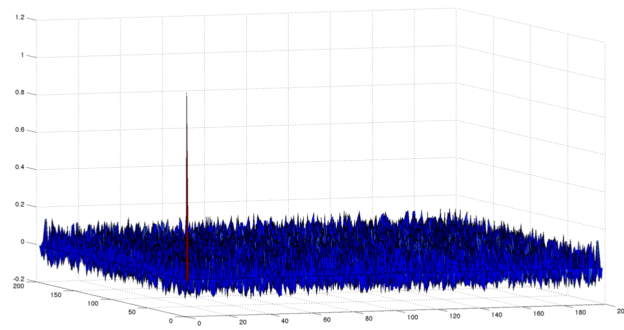

Fig. 7. $\mathcal{M}[\varphi_T, \varphi_T]$ for $T = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}; 0 \neq a \in \mathbb{Z}_N\}$

C. The Heisenberg–Weil System

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

Theorem II.4: 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 $f_L \in \mathcal{B}_L$, $\varphi_T \in \mathcal{B}_T$, we have
$$|\mathcal{M}[S_L, S_L](\tau, \omega)| = \begin{cases} 2 + \epsilon_N, \text{ if } (\tau, \omega) = (0,0); \\ 1 + \varepsilon_N, \text{ if } (\tau, \omega) \in L \smallsetminus (0,0); \\ \varepsilon_N, \text{ if } (\tau, \omega) \in V \smallsetminus L, \end{cases}$$
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 $f_{L_j} \in \mathcal{B}_{L_j}$, $\varphi_{T_j} \in \mathcal{B}_{T_j}$, $j = 1, 2$, $\varphi_{T_1} \neq \varphi_{T_2}$, 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 $(\tau, \omega) \in V$.

A proof of Theorem II.4 will appear in [3].

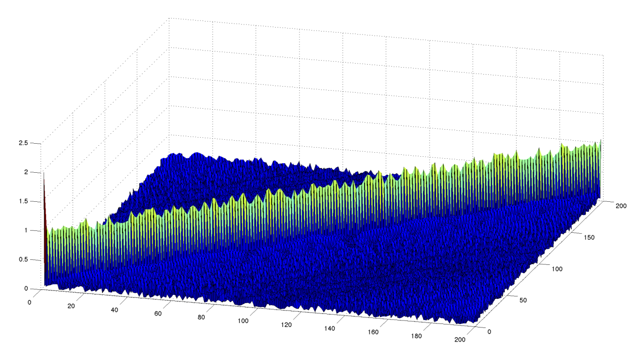

Fig. 8. $|\mathcal{M}[S_L, S_L]|$ for Heisenberg–Weil flag with $L = \{(\tau, \tau)\}$

Remark II.5: As a consequence of Theorem II.4 we obtain families of $N + 1$ almost-orthogonal flag waveforms which can be used for solving the TFS problem in $O(N\log(N))$ operations, and channel estimation problem in $O(m\cdot N\log(N))$ for channel of sparsity m.

III. The Heisenberg Cross System

We define the *Heisenberg cross system* of waveforms. This is the collection of signals in $\mathcal{H}$, which are of the form $S_{L,M}=f_L+f_M$, where f_L, f_M, $L\neq M$, are Heisenberg waveforms defined in Section II-A. The following is an immediate consequence of Theorem II.1:

Theorem III.1: The Heisenberg cross system satisfies the properties

1) *Cross.* For every pair of distinct lines $L, M\subset V$, and every cross $S_{L,M}=f_L+f_M$, with $f_L\in\mathcal{B}_L$, $f_M\in\mathcal{B}_M$, we have
$$|\mathcal{M}[S_{L,M},S_{L,M}](\tau,\omega)|=\begin{cases}2+\varepsilon_N, & \text{if } (\tau,\omega)=(0,0);\\ 1+\varepsilon_N, & \text{if } (\tau,\omega)\in(L\cup M)\smallsetminus(0,0);\\ \varepsilon_N, & \text{if } (\tau,\omega)\in V\smallsetminus(L\cup M),\end{cases}$$
where $|\varepsilon_N|\leq\frac{2}{\sqrt{N}}$.
2) *Almost-orthogonality.* For every four distinct lines $L_1, M_1, L_2, M_2\subset V$, and every two crosses $S_{L_j,M_j}=f_{L_j}+f_{M_j}$, $j=1,2$, we have
$$\left|\mathcal{M}[S_{L_1,M_1},S_{L_2,M_2}](\tau,\omega)\right|\leq\frac{4}{\sqrt{N}}.$$
for every $(\tau,\omega)\in V$.

Remark III.2: As a consequence of Theorem III.1 we obtain families of $\frac{N+1}{2}$ almost-orthogonal cross waveforms which can be used for solving the TFS problem in $O(N\log(N))$.

IV. Applications to Radar and GPS

The flag method provides a significant improvement over the current channel estimation algorithms in the presence of high velocities. The latter occurs in radar and GPS systems. We discuss applications to these fields.

A. Application to Radar

The model of digital radar works as follows [8]. A radar transmits a waveform $S\in\mathcal{H}$ which bounds back from m targets. The waveform $R\in\mathcal{H}$ which is received as an echo has the form
$$R[n]=\sum_{k=1}^{m}\alpha_k\cdot e^{\frac{2\pi i}{N}\omega_k\cdot n}\cdot S[n+\tau_k]\ +\mathcal{W}[n],\quad n\in\mathbb{Z}_N$$
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.

Problem IV.1 (Digital radar): Find (τ_k,ω_k), $k=1,...,m$.

This is essentially a channel estimation problem, so the flag method solves it in $O(m\cdot N\log(N))$ operations.

B. Application to Global Positioning System (GPS)

The model of GPS works as follows [9]. A client on the earth surface wants to know his geographical location. Satellites send to earth their location. For simplicity, the location of a satellite is a bit $b\in\{\pm1\}$. The satellite transmits to the earth its signal $S\in\mathcal{H}$ multiplied by its location b. The client receives the signal
$$R[n]=b\cdot\sum_{k=1}^{m}\alpha_k\cdot e^{\frac{2\pi i}{N}\omega_k\cdot n}\cdot S[n+\tau_k]\ +\mathcal{W}[n],$$
where ω_k encodes the radial velocity of the satellite with respect to the client along the path k, τ_k encode the distance between the satellite and the client[4], α_k's are complex multipath amplitudes, and $\mathcal{W}$ is a random white noise.

Problem IV.2 (GPS problem): Find b given that S and R are known.

In practice, first, S is sent and the channel estimation is done. In the second step, the bit b is communicated by sending $b\cdot S$. Then the bit is extracted using the formula
$$b\cdot\sum_{k=1}^{m}|\alpha_k|^2\approx\langle R,\sum_{k=1}^{m}\alpha_k\cdot e^{\frac{2\pi i}{N}\omega_k\cdot n}\cdot S[n+\tau_k]\rangle.$$

A client can compute his location by knowing the locations of at least three satellites and distances to them.

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, and A. Weinstein.

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] Fish A., Gurevich S., Hadani R., Sayeed A., Schwartz O., Delay-Doppler Channel Estimation in Almost Linear Complexity. *In preparation (2012).*

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

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

[6] 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.*

[7] 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.*

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

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

[10] 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.*

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

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

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

[14] 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.*

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

[4] From the τ_k's we can compute [9] the distance from the satellite to the client, assuming that there is a line of sight between them.