The Heisenberg–Weil Representation and Fast Wireless Communication

Shamgar Gurevich

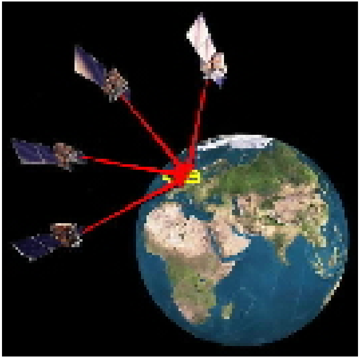
Madison

May 12, 2012

Joint work with:

- **Alexander Fish (Math, Madison)**
- **Ronny Hadani (Math, Austin)**
- **Akbar Sayeed (ECE, Madison)**
- **Oded Schwartz (EECS, Berkeley)**

- **GPS**



CLIENT WANT: Coordinates of satellite and time delay (enables to calculate distance to a satellite)?

Motivation - GPS

- S, $R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ – Hilbert space of digital signals, $N \gg 1000$.

Motivation - GPS

- S, $R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ – Hilbert space of digital signals, $N \gg 1000$.
  - $S, R : \{0, ..., N-1\} \to \mathbb{C}$.

Motivation - GPS

- $S, R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ – Hilbert space of digital signals, $N \gg 1000$.
  - $S, R : \{0, ..., N-1\} \to \mathbb{C}$.
  - Satellite transmits $b \cdot S$, $b =$coordinates.

Motivation - GPS

- $S, R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ – Hilbert space of digital signals, $N \gg 1000$.
    - $S, R : \{0, ..., N-1\} \to \mathbb{C}$.
    - Satellite transmits $b \cdot S$, $b =$coordinates.

Fact (GPS)

Client receives

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

$m = \#$ paths, $\alpha_k \in \mathbb{C}$ intensity, $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\omega_k \in \mathbb{Z}_N$ Doppler, $\tau_k \in \mathbb{Z}_N$ delay, along path k, $\mathcal{W} \in \mathcal{H}$ random noise.

Motivation - GPS

- $S, R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ – Hilbert space of digital signals, $N \gg 1000$.
  - $S, R : \{0, ..., N-1\} \to \mathbb{C}$.
  - Satellite transmits $b \cdot S$, $b =$coordinates.

Fact (GPS)

Client receives

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

$m = \#$ paths, $\alpha_k \in \mathbb{C}$ intensity, $\sum_{k=1}^{m} |\alpha_k|^2 \leq 1$, $\omega_k \in \mathbb{Z}_N$ Doppler, $\tau_k \in \mathbb{Z}_N$ delay, along path k, $\mathcal{W} \in \mathcal{H}$ random noise.

Problem

Design $S \in \mathcal{H}$, and effective method to extract (b, τ), $\tau = \min\{\tau_k\}$, using R and S.

Motivation - TIME-FREQUENCY SHIFT

- Simpler scenario

$$R[n] = e^{\frac{2\pi i}{N}\omega_0 \cdot n} \cdot S[n+\tau_0] \quad + \quad \mathcal{W}[n].$$

Motivation - TIME-FREQUENCY SHIFT

- Simpler scenario

$$R[n] = e^{\frac{2\pi i}{N}\omega_0 \cdot n} \cdot S[n+\tau_0] \quad + \quad \mathcal{W}[n].$$

Problem (Time-Frequency Shift)

Design $S \in \mathcal{H}$, and method of extracting (τ_0, ω_0) from S and R.

(I) Solution - MATCHED FILTER

Definition

Matched filter

$$\begin{cases} \mathcal{M}(R,S) : \overbrace{\mathbb{Z}_N \times \mathbb{Z}_N}^{\text{Time-Frequency}} \rightarrow \mathbb{C}, \\ \mathcal{M}(R,S)[\tau,\omega] = \left\langle R[n] \ , \ e^{\frac{2\pi i}{N}\omega \cdot n} \cdot S[n+\tau] \right\rangle . \end{cases}$$

(I) Solution - MATCHED FILTER

Definition

Matched filter

$$\begin{cases} \mathcal{M}(R,S) : \overbrace{\mathbb{Z}_N \times \mathbb{Z}_N}^{\text{Time-Frequency}} \to \mathbb{C}, \\ \mathcal{M}(R,S)[\tau,\omega] = \left\langle R[n]\ ,\ e^{\frac{2\pi i}{N}\omega \cdot n} \cdot S[n+\tau] \right\rangle . \end{cases}$$

- Identity

$$\mathcal{M}(R,S)[\tau,\omega] = \mathcal{M}(S,S)[\tau-\tau_0,\omega-\omega_0] + O(\frac{NSR}{\sqrt{N}}).$$

(I) Solution - MATCHED FILTER

Definition

Matched filter

$$\begin{cases} \mathcal{M}(R,S) : \overbrace{\mathbb{Z}_N \times \mathbb{Z}_N}^{\text{Time-Frequency}} \rightarrow \mathbb{C}, \\ \mathcal{M}(R,S)[\tau,\omega] = \left\langle R[n] \ , \ e^{\frac{2\pi i}{N}\omega \cdot n} \cdot S[n+\tau] \right\rangle . \end{cases}$$

- Identity

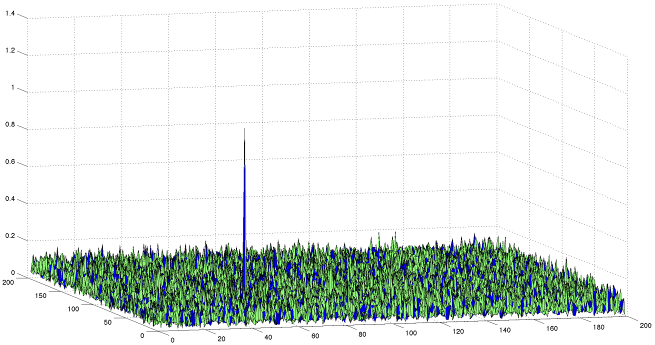
$$\mathcal{M}(R,S)[\tau,\omega] = \mathcal{M}(S,S)[\tau-\tau_0, \omega-\omega_0] + O(\frac{NSR}{\sqrt{N}}).$$

- Question: What S to use for extracting (τ_0, ω_0) from $\mathcal{M}(R,S)$?

Solution - MATCHED FILTER

- Typical solution: S = pseudo-random.

Example



$$|\mathcal{M}(R,S)|, \; S = \text{pseudo-random}, \; (\tau_0, \omega_0) = (50, 50).$$

Solution - MATCHED FILTER

- Complexity of **Pixel-by-Pixel Algorithm**

$$\underbrace{N}_{\text{for each pixel}} \times \underbrace{N^2}_{\#\text{ of pixels}} = N^3.$$

Solution - MATCHED FILTER

- Complexity of **Pixel-by-Pixel Algorithm**

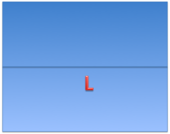
$$\underbrace{N}_{\text{for each pixel}} \times \underbrace{N^2}_{\#\text{ of pixels}} = N^3.$$

Problem

Faster algorithm.

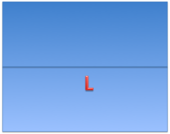
MATCHED FILTER - FFT Reduction

- Suppose $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ line



MATCHED FILTER - FFT Reduction

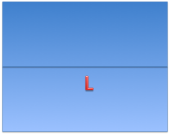
- Suppose $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ line



- Compute $\mathcal{M}(R, S)$ on L in $O(N \cdot \log(N))$ operations!

MATCHED FILTER - FFT Reduction

- Suppose $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ line

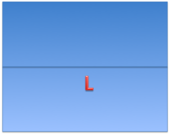


- Compute $\mathcal{M}(R, S)$ on L in $O(N \cdot \log(N))$ operations!
- Example:

$$\mathcal{M}(R, S)[\tau, 0] = \langle R[n], S[n+\tau] \rangle = (S * R)[\tau] \quad \text{– Fast by FFT.}$$

MATCHED FILTER - FFT Reduction

- Suppose $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ line



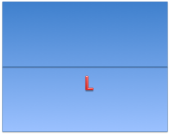
- Compute $\mathcal{M}(R,S)$ on L in $O(N \cdot \log(N))$ operations!
- Example:

$$\mathcal{M}(R,S)[\tau,0] = \langle R[n], S[n+\tau] \rangle = (S * R)[\tau] \quad \text{– Fast by FFT.}$$

- Compute entire $\mathcal{M}(R,S)$ in $O(N^2 \cdot \log(N))$ operations.

MATCHED FILTER - FFT Reduction

- Suppose $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ line



- Compute $\mathcal{M}(R, S)$ on L in $O(N \cdot \log(N))$ operations!
- Example:

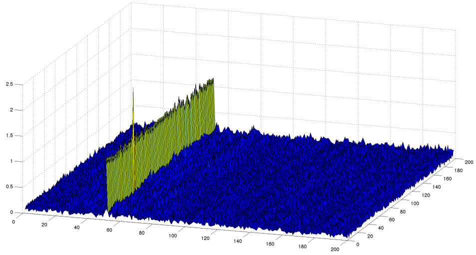
$$\mathcal{M}(R, S)[\tau, 0] = \langle R[n], S[n+\tau] \rangle = (S * R)[\tau] \quad \text{– Fast by FFT.}$$

- Compute entire $\mathcal{M}(R, S)$ in $O(N^2 \cdot \log(N))$ operations.

- **Question:** Can you design S and method to make almost linear number of operations?

(II) Flag Algorithm - IDEA

- Suppose for a line $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ we construct a signal $S_L \in \mathcal{H}$ with $\mathcal{M}(R, S_L)$ of the form



$$|\mathcal{M}(R, S_L)|, \ (\tau_0, \omega_0) = (50, 50)$$

Then we have algorithm of complexity $O(N \cdot \log(N))$!!

Flag Algorithm - WAVEFORM DESIGN PROBLEM

Problem (Waveform Design)

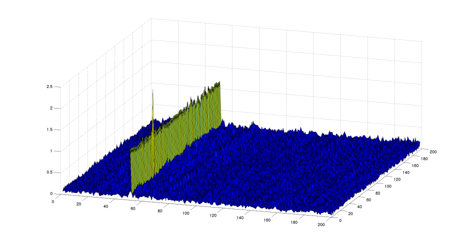
For every $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ *construct* $S_L \in \mathcal{H}$ *with*

Flag Algorithm - WAVEFORM DESIGN PROBLEM

Problem (Waveform Design)

For every $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ *construct* $S_L \in \mathcal{H}$ *with*

1. **Flag.** *Matched filter* $\mathcal{M}(R, S_L)$ *of the form*



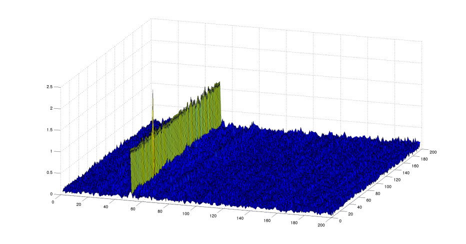
$|\mathcal{M}(R, S_L)|$

Flag Algorithm - WAVEFORM DESIGN PROBLEM

Problem (Waveform Design)

For every $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$ construct $S_L \in \mathcal{H}$ with

1. **Flag.** *Matched filter $\mathcal{M}(R, S_L)$ of the form*



$$|\mathcal{M}(R, S_L)|$$

2. **Almost orthogonality.** *For $L \neq M$ the cross-correlations* $|\mathcal{M}(S_L, S_M)[\tau, \omega]| = O(\frac{1}{\sqrt{N}})$.

(III) Waveform Design - EXAMPLE

- Consider waveform $f[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} n}$.

(III) Waveform Design - EXAMPLE

- Consider waveform $f[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} n}$.
- $f[n+\tau] = e^{\frac{2\pi i}{N}\tau} \cdot f[n]$, so

$$\begin{aligned} \mathcal{M}(f,f)[\tau,\omega] &= \left\langle f[n], e^{\frac{2\pi i}{N}\omega\cdot n} \cdot f[n+\tau] \right\rangle \\ &= \begin{cases} |\cdot| = 1, & \text{if } \omega = 0; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

(III) Waveform Design - EXAMPLE

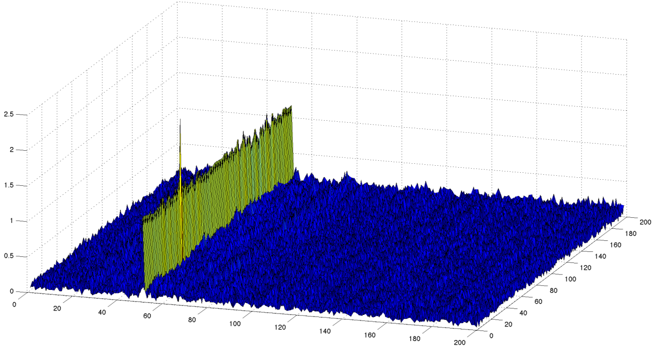
- Consider waveform $f[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} n}$.
- $f[n+\tau] = e^{\frac{2\pi i}{N}\tau} \cdot f[n]$, so

$$\begin{aligned} \mathcal{M}(f,f)[\tau,\omega] &= \left\langle f[n], e^{\frac{2\pi i}{N}\omega \cdot n} \cdot f[n+\tau] \right\rangle \\ &= \begin{cases} |\cdot| = 1, \text{ if } \omega = 0; \\ 0, \quad\quad \text{otherwise.} \end{cases} \end{aligned}$$

- Take $S = \underbrace{f}_{\text{exp}} + \underbrace{\varphi}_{\text{pseudo-random}}$, then

$$|\mathcal{M}(R,S)[\tau,\omega]| \approx \begin{cases} 2, & \text{if } (\tau,\omega) = (\tau_0,\omega_0); \\ 1, & \text{on the line } \omega = \omega_0; \\ O(\frac{1}{\sqrt{N}}), & \text{otherwise.} \end{cases}$$

FLAG - Numerics



$$|\mathcal{M}(R,S)|,\ S = \underbrace{f}_{\text{exp}} + \underbrace{\varphi}_{\text{pseudo-random}},\ (\tau_0,\omega_0) = (50,50)$$

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Question:** How to generalize the "good" orthonormal basis of $\mathcal{H}$

$$\mathcal{B} = \{f_a[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} an};\ a \in \mathbb{Z}_N\} \ ?$$

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Question:** How to generalize the "good" orthonormal basis of $\mathcal{H}$

$$\mathcal{B} = \{f_a[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} an};\ a \in \mathbb{Z}_N\} \ ?$$

- Answer: Consider the Heisenberg operators on $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$

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

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Question:** How to generalize the "good" orthonormal basis of $\mathcal{H}$

$$\mathcal{B} = \{f_a[n] = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} an};\ a \in \mathbb{Z}_N\} \text{ ?}$$

- Answer: Consider the Heisenberg operators on $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$

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

- Property:

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

- Restrict π to the line $L = \{(\tau, 0);\ \tau \in \mathbb{Z}_N\}$, obtain commutative collection of operators

$$\overbrace{\pi(\tau,0)}^{\text{time shift}} : \mathcal{H} \to \mathcal{H}, \quad \tau \in \mathbb{Z}_N.$$

- Restrict π to the line $L = \{(\tau, 0);\ \tau \in \mathbb{Z}_N\}$, obtain commutative collection of operators

$$\overbrace{\pi(\tau,0)}^{\text{time shift}} : \mathcal{H} \to \mathcal{H}, \quad \tau \in \mathbb{Z}_N.$$

Theorem (Linear Algebra – Simultaneous Diagonalization)

There exists a basis for $\mathcal{H}$ of common eigenfunctions

$$\mathcal{B}_L = \{f_\psi;\ \ \pi(\tau,0)[f_\psi] = \overbrace{\psi(\tau)}^{e.v.} \cdot f_\psi, \ \ \textit{for all } \tau \in \mathbb{Z}_N\}.$$

Waveform Design - HEISENBERG (LINES) SYSTEM

- Restrict π to the line $L = \{(\tau, 0);\ \tau \in \mathbb{Z}_N\}$, obtain commutative collection of operators

$$\overbrace{\pi(\tau, 0)}^{\text{time shift}} : \mathcal{H} \to \mathcal{H}, \quad \tau \in \mathbb{Z}_N.$$

Theorem (Linear Algebra – Simultaneous Diagonalization)

There exists a basis for $\mathcal{H}$ of common eigenfunctions

$$\mathcal{B}_L = \{f_\psi;\quad \pi(\tau, 0)[f_\psi] = \overbrace{\psi(\tau)}^{e.v.} \cdot f_\psi, \quad \textit{for all } \tau \in \mathbb{Z}_N\}.$$

- Of course $\mathcal{B}_L = \mathcal{B}$.

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Mechanism to generate 'good waveforms':**

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Mechanism to generate 'good waveforms':**
  - Take any line $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$;

- **Mechanism to generate 'good waveforms':**
  - Take any line $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$;
  - Restrict π to L and obtain commutative collection of operators

$$\pi(\ell) : \mathcal{H} \to \mathcal{H}, \quad \ell \in L;$$

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Mechanism to generate 'good waveforms':**
  - Take any line $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$;
  - Restrict π to L and obtain commutative collection of operators

$$\pi(\ell) : \mathcal{H} \to \mathcal{H}, \quad \ell \in L;$$

  - Get a basis for $\mathcal{H}$ of common eigenfunctions

$$\mathcal{B}_L = \{f_\psi; \quad \pi(\ell)[\ f_\psi] = \overbrace{\psi(\ell)}^{\text{e.v.}} \cdot f_\psi, \quad \text{for all } \ell \in L\}.$$

Waveform Design - HEISENBERG (LINES) SYSTEM

- **Mechanism to generate 'good waveforms':**
  - Take any line $L \subset \mathbb{Z}_N \times \mathbb{Z}_N$;
  - Restrict π to L and obtain commutative collection of operators

$$\pi(\ell) : \mathcal{H} \to \mathcal{H}, \quad \ell \in L;$$

  - Get a basis for $\mathcal{H}$ of common eigenfunctions

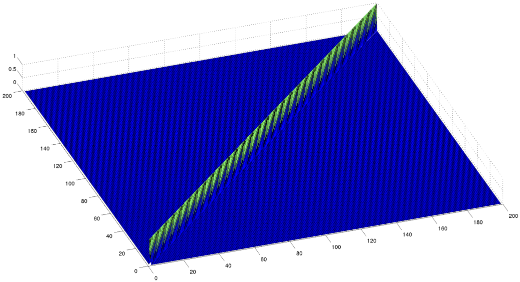
$$\mathcal{B}_L = \{ f_\psi; \quad \pi(\ell)[\, f_\psi] = \overbrace{\psi(\ell)}^{\text{e.v.}} \cdot f_\psi, \quad \text{for all } \ell \in L \}.$$

Theorem (Support, [Calderbank–Howard–Moran, Howe])

We have

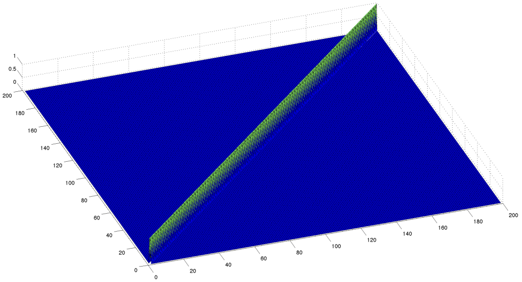
$$\left| \mathcal{M}(f_\psi, f_\psi)[\tau, \omega] \right| = \begin{cases} 1, & (\tau, \omega) \in L; \\ 0, & (\tau, \omega) \notin L. \end{cases}$$

HEISENBERG (LINES) SYSTEM – Numerics



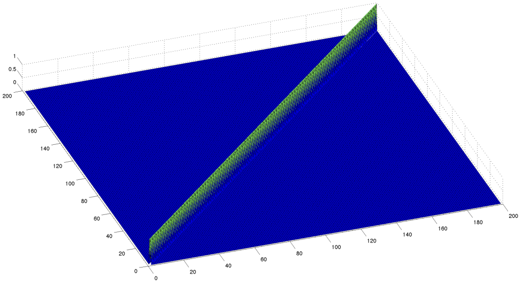
- $$\left|\mathcal{M}[f_\psi, f_\psi]\right|,\ f_\psi \in \mathcal{B}_L,\ L = \{(\tau, \tau)\}$$

HEISENBERG (LINES) SYSTEM – Numerics



$$\left|\mathcal{M}[f_\psi, f_\psi]\right|,\ f_\psi \in \mathcal{B}_L,\ L = \{(\tau,\tau)\}$$

-
- What is next?



$$\left|\mathcal{M}[f_{\psi}, f_{\psi}]\right|,\ f_{\psi} \in \mathcal{B}_L,\ L = \{(\tau, \tau)\}$$

-
- What is next?
- Just add any pseudo-random waveform.

Waveform Design - WEIL (PEAK) SYSTEM

- Discrete Fourier transform (DFT) is defined by system

$$\Sigma_W : \qquad DFT \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{W} \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ DFT, \quad \tau, \omega \in \mathbb{Z}_N.$$

Waveform Design - WEIL (PEAK) SYSTEM

- Discrete Fourier transform (DFT) is defined by system

$$\Sigma_W : \quad DFT \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{W} \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ DFT, \quad \tau, \omega \in \mathbb{Z}_N.$$

- Special linear group

$$W \in SL_2(\mathbb{Z}_N) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \, a, b, c, d \in \mathbb{Z}_N, \ \det(g) = 1\}.$$

Waveform Design - WEIL (PEAK) SYSTEM

- Discrete Fourier transform (DFT) is defined by system

$$\Sigma_W : \quad DFT \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{W} \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ DFT, \quad \tau, \omega \in \mathbb{Z}_N.$$

- Special linear group

$$W \in SL_2(\mathbb{Z}_N) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{Z}_N,\ \det(g) = 1\}.$$

Problem (André Weil)

For each $g \in SL_2(\mathbb{Z}_N)$ find operator $\rho(g)$ on $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$, which solves the system of N^2 linear conditions

$$\Sigma_g : \quad \underbrace{\rho(g)}_{?} \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(g \cdot \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ \underbrace{\rho(g)}_{?}, \quad \tau, \omega \in \mathbb{Z}_N.$$

Waveform Design - WEIL (PEAK) SYSTEM

Theorem (Stone–von Neumann–Schur–Weil)

$\exists!$ *collection* $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\, g \in SL_2(\mathbb{Z}_N)\}$ *such that*

$$\begin{cases} \rho : SL_2(\mathbb{Z}_N) \to U(\mathcal{H}), \\ \rho(g \cdot h) = \rho(g) \circ \rho(h). \end{cases} \quad \text{— } \textit{Weil representation}$$

Waveform Design - WEIL (PEAK) SYSTEM

Theorem (Stone–von Neumann–Schur–Weil)

$\exists!$ *collection* $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\ g \in SL_2(\mathbb{Z}_N)\}$ *such that*

$$\begin{cases} \rho : SL_2(\mathbb{Z}_N) \to U(\mathcal{H}), \\ \rho(g \cdot h) = \rho(g) \circ \rho(h). \end{cases} \quad \text{— } \textit{Weil representation}$$

- **Mechanism to generate 'good waveforms':**

Waveform Design - WEIL (PEAK) SYSTEM

Theorem (Stone–von Neumann–Schur–Weil)

$\exists!$ collection $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\ g \in SL_2(\mathbb{Z}_N)\}$ such that

$$\begin{cases} \rho : SL_2(\mathbb{Z}_N) \to U(\mathcal{H}), \\ \rho(g \cdot h) = \rho(g) \circ \rho(h). \end{cases} \quad \text{— \textit{Weil representation}}$$

- **Mechanism to generate 'good waveforms':**
  - Take maximal commutative subgroup $T \subset SL_2(\mathbb{Z}_N)$, i.e., $gh = hg$ for every $g, h \in T$.

Waveform Design - WEIL (PEAK) SYSTEM

Theorem (Stone–von Neumann–Schur–Weil)

∃! collection $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\, g \in SL_2(\mathbb{Z}_N)\}$ *such that*

$$\begin{cases} \rho : SL_2(\mathbb{Z}_N) \to U(\mathcal{H}), \\ \rho(g \cdot h) = \rho(g) \circ \rho(h). \end{cases} \quad \text{— } \textit{Weil representation}$$

- **Mechanism to generate 'good waveforms':**
  - Take maximal commutative subgroup $T \subset SL_2(\mathbb{Z}_N)$, i.e., $gh = hg$ for every $g, h \in T$.
  - Get a <u>commutative</u> collection of operators

$$\rho(g) : \mathcal{H} \to \mathcal{H}, \;\; g \in T.$$

Waveform Design - WEIL (PEAK) SYSTEM

Theorem (Stone–von Neumann–Schur–Weil)

$\exists!$ *collection* $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\ g \in SL_2(\mathbb{Z}_N)\}$ *such that*

$$\begin{cases} \rho : SL_2(\mathbb{Z}_N) \to U(\mathcal{H}), \\ \rho(g \cdot h) = \rho(g) \circ \rho(h). \end{cases} \quad \text{— } \textit{Weil representation}$$

- **Mechanism to generate 'good waveforms':**
  - Take maximal commutative subgroup $T \subset SL_2(\mathbb{Z}_N)$, i.e., $gh = hg$ for every $g, h \in T$.
  - Get a commutative collection of operators

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

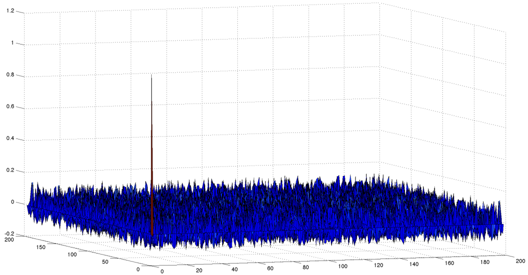
  - Get a basis for $\mathcal{H}$ of common eigenfunctions

$$\mathcal{B}_T = \{\varphi_\chi; \ \ \rho(g)[\ \varphi_\chi] = \overbrace{\chi(g)}^{\text{e.v.}} \cdot \varphi_\chi, \ \ \text{for all } g \in T\}.$$

Waveform Design - WEIL (PEAK) SYSTEM

Theorem (Pseudo-Randomness [G–Hadani–Sochen])

For $\varphi_\chi \in \mathcal{B}_T$ *we have* $\left|\mathcal{M}(\varphi_\chi, \varphi_\chi)[\tau, \omega]\right| = \begin{cases} 1, & (\tau, \omega) = (0,0); \\ \leq \frac{2}{\sqrt{N}}, & (\tau, \omega) \neq (0,0). \end{cases}$



$$\mathcal{M}(\varphi_\chi, \varphi_\chi),\ T = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\right\},\ \varphi_\chi \in \mathcal{B}_T$$

HEISENBERG+WEIL (FLAG) SYSTEM

Theorem ([Fish–G–Hadani–Sayeed–Schwartz])

Take $S_L = \underbrace{f_L}_{\in \mathcal{B}_L} + \underbrace{\varphi_\chi}_{\in \mathcal{B}_T}$. *Then*

HEISENBERG+WEIL (FLAG) SYSTEM

Theorem ([Fish–G–Hadani–Sayeed–Schwartz])

Take $S_L = \underbrace{f_L}_{\in \mathcal{B}_L} + \underbrace{\varphi_\chi}_{\in \mathcal{B}_T}$. *Then*

1. **Flag.** *We have* $|\mathcal{M}(S_L, S_L)[\tau, \omega]| = \begin{cases} \approx 2, \text{ if } (\tau, \omega) = (0,0); \\ \approx 1, \text{ if } (\tau, \omega) \in L \smallsetminus (0,0); \\ \leq \frac{7}{\sqrt{N}}, \text{ otherwise.} \end{cases}$

HEISENBERG+WEIL (FLAG) SYSTEM

Theorem ([Fish–G–Hadani–Sayeed–Schwartz])

Take $S_L = \underbrace{f_L}_{\in \mathcal{B}_L} + \underbrace{\varphi_\chi}_{\in \mathcal{B}_T}$. *Then*

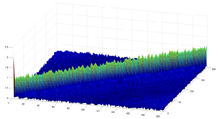
1. **Flag.** *We have* $|\mathcal{M}(S_L, S_L)[\tau, \omega]| = \begin{cases} \approx 2, \text{ if } (\tau, \omega) = (0, 0); \\ \approx 1, \text{ if } (\tau, \omega) \in L \smallsetminus (0, 0); \\ \leq \frac{7}{\sqrt{N}}, \text{ otherwise.} \end{cases}$

2. **Almost orthogonality.** *For* $L \neq M$ *we have* $|\mathcal{M}(S_L, S_M)[\tau, \omega]| \leq \frac{7}{\sqrt{N}}$, *for every* $(\tau, \omega) \in \mathbb{Z}_N \times \mathbb{Z}_N$.

Theorem ([Fish–G–Hadani–Sayeed–Schwartz])

Take $S_L = \underbrace{f_L}_{\in \mathcal{B}_L} + \underbrace{\varphi_\chi}_{\in \mathcal{B}_T}$. *Then*

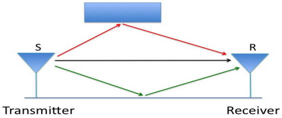
1. **Flag.** *We have* $|\mathcal{M}(S_L, S_L)[\tau,\omega]| = \begin{cases} \approx 2, \text{ if } (\tau,\omega) = (0,0); \\ \approx 1, \text{ if } (\tau,\omega) \in L \smallsetminus (0,0); \\ \leq \frac{7}{\sqrt{N}}, \text{ otherwise.} \end{cases}$
2. **Almost orthogonality.** *For* $L \neq M$ *we have* $|\mathcal{M}(S_L, S_M)[\tau,\omega]| \leq \frac{7}{\sqrt{N}}$, *for every* $(\tau,\omega) \in \mathbb{Z}_N \times \mathbb{Z}_N$.



- $|\mathcal{M}(S_L, S_L)|$, $L = \{(\tau,\tau)\}$

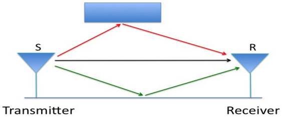
(A) Channel Estimation

- **Transmit** flag waveform $S = S_L$



(A) Channel Estimation

- **Transmit** flag waveform $S = S_L$



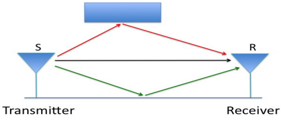
- **Receive**

$$R[n] = \sum_{k=1}^{m} \alpha_k \cdot \underbrace{e^{\frac{2\pi i}{N}\omega_k \cdot n}}_{\text{Doppler}} \cdot S_L[n + \underbrace{\tau_k}_{\text{delay}}] + \mathcal{W}[n],$$

$\mathcal{W}$ = noise, τ_k = delay along path k, ω_k = Doppler along path k,
α_k = intensity coefficient, $|\alpha_1|^2 + ... + |\alpha_m|^2 \leq 1$.

(A) Channel Estimation

- **Transmit** flag waveform $S = S_L$



- **Receive**

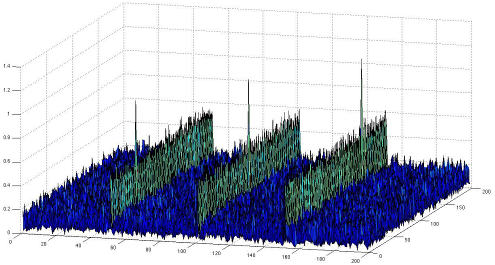
$$R[n] = \sum_{k=1}^{m} \alpha_k \cdot \underbrace{e^{\frac{2\pi i}{N}\omega_k \cdot n}}_{\text{Doppler}} \cdot S_L[n + \underbrace{\tau_k}_{\text{delay}}] + \mathcal{W}[n],$$

$\mathcal{W}$ = noise, τ_k = delay along path k, ω_k = Doppler along path k, α_k = intensity coefficient, $|\alpha_1|^2 + ... + |\alpha_m|^2 \leq 1$.

- **Goal** Extract $(\alpha_k, \tau_k, \omega_k)$'s, using R and S_L.

Application - CHANNEL ESTIMATION

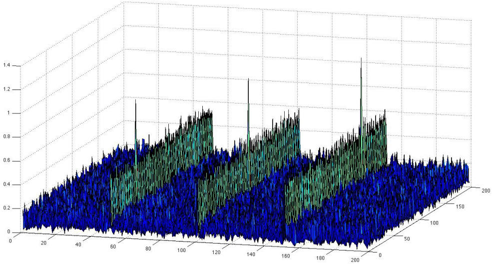
- We have $|\mathcal{M}(R,S_L)[\tau,\omega]| \approx$
$$\begin{cases} 2\cdot\alpha_k, \text{ if } (\tau,\omega)=(\tau_k,\omega_k); \\ 1\cdot\alpha_k, \text{ if } (\tau,\omega)\in L+(\tau_k,\omega_k)\smallsetminus(\tau_k,\omega_k); \\ \le O(\frac{m}{\sqrt{N}}), \text{ otherwise.} \end{cases}$$



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

Application - CHANNEL ESTIMATION

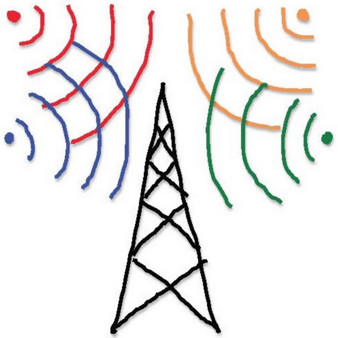
- We have $|\mathcal{M}(R,S_L)[\tau,\omega]| \approx$
$$\begin{cases} 2\cdot\alpha_k, \text{ if } (\tau,\omega) = (\tau_k,\omega_k); \\ 1\cdot\alpha_k, \text{ if } (\tau,\omega) \in L + (\tau_k,\omega_k) \setminus (\tau_k,\omega_k); \\ \leq O(\frac{m}{\sqrt{N}}), \text{ otherwise.} \end{cases}$$



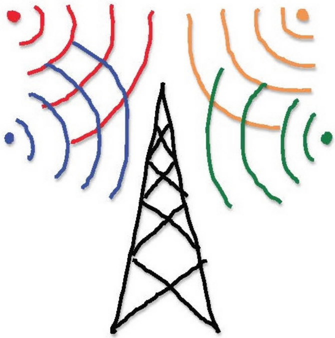
$|\mathcal{M}(R,S_L)|$, $L = \{(\tau,0)\}$, $(\alpha_k,\tau_k,\omega_k) = (\frac{1}{\sqrt{3}}, 50k, 50k)$, $k = 1,2,3$.

- Flag method computes channel parameters in $O(m \cdot N\log(N))$.

- **(B) Mobile Communication: CDMA, GSM...**



- **(B) Mobile Communication: CDMA, GSM...**



- User transmits message

$$\overbrace{b}^{+1 \text{ or } -1} \cdot S_L$$

using his private flag waveform S_L.

Application - MOBILE COMMUNICATION

- Antenna receives:

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

- Antenna receives:

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

- Assumption (slow varying channel): Antenna knows, using our $O(m \cdot N \log(N))$ channel estimation, the $(\alpha_k, \omega_k, \tau_k)$'s.

Application - MOBILE COMMUNICATION

- Antenna receives:

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

- Assumption (slow varying channel): Antenna knows, using our $O(m \cdot N \log(N))$ channel estimation, the $(\alpha_k, \omega_k, \tau_k)$'s.
- **Goal:** Extract b using R and S_L.

Application - MOBILE COMMUNICATION

- Antenna receives:

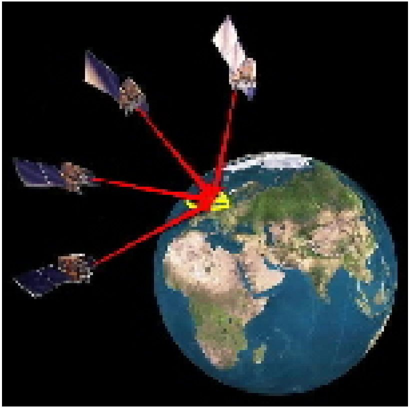
$$R[n] = b \cdot \sum_{k=1}^{m} \alpha_k \cdot e^{\frac{2\pi i}{N}\omega_k \cdot n} \cdot S_L[n+\tau_k] + \mathcal{W}[n],$$

- Assumption (slow varying channel): Antenna knows, using our $O(m \cdot N \log(N))$ channel estimation, the $(\alpha_k, \omega_k, \tau_k)$'s.
- **Goal:** Extract b using R and S_L.
- Method:

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

Application - GPS

- **(C) GPS**



CLIENT WANT: Coordinates of satellite and time delay (enables to calculate distance to a satellite)?

Application - GPS

- S_L, $R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$, $N >> 1000$.

Application - GPS

- S_L, $R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$, $N >> 1000$.

Fact

GPS System

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

τ_k =*delay*, ω_k =*Doppler*, b =*coordinates of satellite*, α_k = *intensity coefficient*, $|\alpha_1|^2 + ... + |\alpha_m|^2 \leq 1$.

Application - GPS

- $S_L,\ R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N),\ N >> 1000.$

Fact

GPS System

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

τ_k =*delay*, ω_k =*Doppler*, b =*coordinates of satellite*, α_k = *intensity coefficient*, $|\alpha_1|^2 + ... + |\alpha_m|^2 \leq 1$.

Problem

Extract (b, τ), $\tau = \min\{\tau_k\text{'s}\}$ *using* R *and* S_L.

Application - GPS

- S_L, $R \in \mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$, $N >> 1000$.

Fact

GPS System

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

τ_k =*delay*, ω_k =*Doppler*, b =*coordinates of satellite*, α_k = *intensity coefficient*, $|\alpha_1|^2 + ... + |\alpha_m|^2 \leq 1$.

Problem

Extract (b, τ), $\tau = \min\{\tau_k\text{'s}\}$ *using* R *and* S_L.

Solution

Flag method solves in $O(m \cdot N \log(N))$.

THANK YOU

Sasha

Ronny

Akbar

Oded