Diagonalization of the Discrete Fourier Transform using Weil Representation

Shamgar Gurevich

Madison

August 3, 2014

(0) Motivation - Diagonalizing DFT

- $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ – Hilbert space of digital sequences.

(0) Motivation - Diagonalizing DFT

- $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ – Hilbert space of digital sequences.
  - $\psi(t) = \exp(2\pi i t/p)$.

(0) Motivation - Diagonalizing DFT

- $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ – Hilbert space of digital sequences.
  - $\psi(t) = \exp(2\pi i t/p)$.
- $DFT : \mathcal{H} \to \mathcal{H}$ - Discrete Fourier Transform

$$DFT[f](\omega) = \frac{1}{\sqrt{p}} \sum_{t \in \mathbb{F}_p} \psi(\omega t) f(t).$$

(0) Motivation - Diagonalizing DFT

- $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ – Hilbert space of digital sequences.
  - $\psi(t) = \exp(2\pi i t/p)$.
- $DFT : \mathcal{H} \to \mathcal{H}$ - Discrete Fourier Transform

$$DFT[f](\omega) = \frac{1}{\sqrt{p}} \sum_{t \in \mathbb{F}_p} \psi(\omega t) f(t).$$

- Fact: $DFT^4 = Id \implies \lambda(DFT) \in \{\pm 1, \pm i\}$.

(0) Motivation - Diagonalizing DFT

- $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ – Hilbert space of digital sequences.
  - $\psi(t) = \exp(2\pi i t/p)$.
- $DFT : \mathcal{H} \to \mathcal{H}$ - Discrete Fourier Transform

$$DFT[f](\omega) = \frac{1}{\sqrt{p}} \sum_{t \in \mathbb{F}_p} \psi(\omega t) f(t).$$

- Fact: $DFT^4 = Id \implies \lambda(DFT) \in \{\pm 1, \pm i\}$.

Problem (Diagonalization)

Find natural basis of eigenfunctions for DFT.

Solution - Idea

- Find natural Symmetries

$$DFT \curvearrowright \mathcal{H} \curvearrowleft C$$

Solution - Idea

- Find natural Symmetries

$$DFT \curvearrowright \mathcal{H} \curvearrowleft C$$

  - C commutative group.

Solution - Idea

- Find natural Symmetries

$$DFT \curvearrowright \mathcal{H} \curvearrowleft C$$

  - C commutative group.
  - Take common eigenfunctions!

Solution - Idea

- Find natural Symmetries

$$DFT \curvearrowright \mathcal{H} \curvearrowleft C$$

  - C commutative group.
  - Take common eigenfunctions!

- **Question:** $C =?$.

Solution - Idea

- Find natural Symmetries

$$DFT \curvearrowright \mathcal{H} \curvearrowleft C$$

  - C commutative group.
  - Take common eigenfunctions!

- **Question:** $C =?$.

- **Answer:** Characterization of DFT.

Characterization of DFT

- Basic operations

Characterization of DFT

- Basic operations
  - Time shift: $\tau \in \mathbb{F}_p$,

$$\begin{cases} L_\tau : \mathcal{H} \to \mathcal{H}, \\ L_\tau[f](t) = f(t+\tau), \ t \in \mathbb{Z}_N. \end{cases}$$

Characterization of DFT

- Basic operations
  - Time shift: $\tau \in \mathbb{F}_p$,

$$\begin{cases} L_\tau : \mathcal{H} \to \mathcal{H}, \\ L_\tau[f](t) = f(t+\tau), \ t \in \mathbb{Z}_N. \end{cases}$$

  - Frequency shift: $\omega \in \mathbb{F}_p$,

$$\begin{cases} M_\omega : \mathcal{H} \to \mathcal{H}, \\ M_\omega[f](t) = \psi(\omega t) f(t). \end{cases}$$

Characterization of DFT

- Basic operations
  - Time shift: $\tau \in \mathbb{F}_p$,

$$\begin{cases} L_\tau : \mathcal{H} \to \mathcal{H}, \\ L_\tau[f](t) = f(t+\tau), \ t \in \mathbb{Z}_N. \end{cases}$$

  - Frequency shift: $\omega \in \mathbb{F}_p$,

$$\begin{cases} M_\omega : \mathcal{H} \to \mathcal{H}, \\ M_\omega[f](t) = \psi(\omega t) f(t). \end{cases}$$

- Intertwining relations

$$\begin{cases} DFT \circ L_\tau = M_\tau \circ DFT, \\ DFT \circ M_\omega = L_{-\omega} \circ DFT. \end{cases}$$

Characterization of DFT - Cont.

- Combine

$$\begin{cases} \pi : \mathbb{F}_p \times \mathbb{F}_p \to U(\mathcal{H}), \\ \pi(\tau, \omega) = \psi(-\frac{1}{2}\tau\omega) \cdot M_\omega \circ L_\tau \end{cases}$$

Characterization of DFT - Cont.

- Combine

$$\begin{cases} \pi : \mathbb{F}_p \times \mathbb{F}_p \to U(\mathcal{H}), \\ \pi(\tau, \omega) = \psi(-\frac{1}{2}\tau\omega) \cdot M_\omega \circ L_\tau \end{cases}$$

- Intertwining relations

$$\Sigma_W : \ DFT \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(\overbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}^{W} \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ DFT.$$

System of p^2 linear equations.

Characterization of DFT - Cont.

- Combine

$$\begin{cases} \pi : \mathbb{F}_p \times \mathbb{F}_p \to U(\mathcal{H}), \\ \pi(\tau, \omega) = \psi(-\frac{1}{2}\tau\omega) \cdot M_\omega \circ L_\tau \end{cases}$$

- Intertwining relations

$$\Sigma_W : \ DFT \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(\overbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}^{W} \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ DFT.$$

System of p^2 linear equations.

Theorem (Stone - von Neumann)

$\dim Sol(\Sigma_W) = 1.$

Characterization of DFT - Cont.

- Combine

$$\begin{cases} \pi : \mathbb{F}_p \times \mathbb{F}_p \to U(\mathcal{H}), \\ \pi(\tau, \omega) = \psi(-\frac{1}{2}\tau\omega) \cdot M_\omega \circ L_\tau \end{cases}$$

- Intertwining relations

$$\Sigma_W : \ DFT \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(\overbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}^{W} \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ DFT.$$

  System of p^2 linear equations.

Theorem (Stone - von Neumann)

$\dim Sol(\Sigma_W) = 1$.

- $\Longrightarrow$ *DFT* is characterized by Σ_W.

(II) The Weil Representation

- Note

$$W \in SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; \ a, b, c, d \in \mathbb{F}_p, \quad ad - bc = 1 \right\}.$$

(II) The Weil Representation

- Note

$$W \in SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; \ a, b, c, d \in \mathbb{F}_p, \quad ad - bc = 1 \right\}.$$

- Generalization: $g \in SL_2(\mathbb{F}_p)$

$$\Sigma_g : \ \rho(g) \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(g \cdot \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ \rho(g).$$

System of p^2 linear equations.

(II) The Weil Representation

- Note

$$W \in SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; \ a, b, c, d \in \mathbb{F}_p, \quad ad - bc = 1 \right\}.$$

- Generalization: $g \in SL_2(\mathbb{F}_p)$

$$\Sigma_g : \ \rho(g) \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(g \cdot \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ \rho(g).$$

System of p^2 linear equations.

Theorem (Stone - von Neumann)

$\dim Sol(\Sigma_g) = 1.$

(II) The Weil Representation

- Note

$$W \in SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; \ a, b, c, d \in \mathbb{F}_p, \quad ad - bc = 1 \right\}.$$

- Generalization: $g \in SL_2(\mathbb{F}_p)$

$$\Sigma_g : \ \rho(g) \circ \pi \begin{pmatrix} \tau \\ \omega \end{pmatrix} = \pi(g \cdot \begin{pmatrix} \tau \\ \omega \end{pmatrix}) \circ \rho(g).$$

System of p^2 linear equations.

Theorem (Stone - von Neumann)

$\dim Sol(\Sigma_g) = 1.$

- $\Longrightarrow \rho(g)$ is characterized by Σ_g.

Weil Representation

Theorem

$\exists!$ *collection of operators* $\rho(g) \in Sol(\Sigma_g)$, $g \in SL_2(\mathbb{F}_p)$, *such that*

$$\rho(gh) = \rho(g) \circ \rho(h).$$

Weil Representation

Theorem

$\exists!$ *collection of operators* $\rho(g) \in Sol(\Sigma_g)$, $g \in SL_2(\mathbb{F}_p)$, *such that*

$$\rho(gh) = \rho(g) \circ \rho(h).$$

- The homomorphism

$$\rho : SL_2(\mathbb{F}_p) \to U(\mathcal{H}), \quad \mathcal{H} = \mathbb{C}(\mathbb{F}_p),$$

is called the **Weil Representation.**

(III) Diagonalizing the DFT

- We have

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to U(\mathcal{H}) \supset C = ? \\ W \mapsto \rho(W) = DFT; \end{cases}$$

(III) Diagonalizing the DFT

- We have

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to U(\mathcal{H}) \supset C = ? \\ W \mapsto \rho(W) = DFT; \end{cases}$$

- Consider symmetries of W :

$$\begin{aligned} T_W &= \{g \in SL_2(\mathbb{F}_p);\ gW = Wg\} \\ &= \left\{g \in SL_2(\mathbb{F}_p);\ gg^t = I\right\} \\ &= SO_2(\mathbb{F}_p) \ \text{ - finite rotations.} \end{aligned}$$

(III) Diagonalizing the DFT

- We have

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to U(\mathcal{H}) \supset C = ? \\ W \mapsto \rho(W) = DFT; \end{cases}$$

- Consider symmetries of W :

$$\begin{aligned} T_W &= \{g \in SL_2(\mathbb{F}_p);\ gW = Wg\} \\ &= \left\{g \in SL_2(\mathbb{F}_p);\ gg^t = I\right\} \\ &= SO_2(\mathbb{F}_p) \ \text{ - finite rotations.} \end{aligned}$$

Lemma

T_W is a maximal commutative subgroup (torus) of $SL_2(\mathbb{F}_p)$.

(III) Diagonalizing the DFT

- We have
$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to U(\mathcal{H}) \supset C = ? \\ W \mapsto \rho(W) = DFT; \end{cases}$$
- Consider symmetries of W :

$$\begin{aligned} T_W &= \{g \in SL_2(\mathbb{F}_p);\ gW = Wg\} \\ &= \left\{g \in SL_2(\mathbb{F}_p);\ gg^t = I\right\} \\ &= SO_2(\mathbb{F}_p) \ \text{ - finite rotations.} \end{aligned}$$

Lemma

T_W is a maximal commutative subgroup (torus) of $SL_2(\mathbb{F}_p)$.

Proof.

$P_W(x) = \det(xI - W) = x^2 + 1$. Hence $\lambda(W) = \pm\sqrt{-1}$. □

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g)\ ;\quad g \in T_W\}\,.$$

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g)\ ;\quad g \in T_W\}\,.$$

  - C commutative group of unitary operators commuting with DFT.

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g)\ ;\quad g \in T_W\}\,.$$

  - C commutative group of unitary operators commuting with DFT.
  - Can diagonalize C simultaneously.

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g) \; ; \quad g \in T_W\}.$$

  - C commutative group of unitary operators commuting with DFT.
  - Can diagonalize C simultaneously.
- We have orthogonal decomposition

$$\mathcal{H} = \bigoplus_{\chi : T_W \to \mathbb{C}^*} \mathcal{H}_\chi,$$

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g)\ ;\ \ g \in T_W\}\,.$$

  - C commutative group of unitary operators commuting with DFT.
  - Can diagonalize C simultaneously.
- We have orthogonal decomposition

$$\mathcal{H} = \bigoplus_{\chi: T_W \to \mathbb{C}^*} \mathcal{H}_\chi,$$

  - $\varphi_\chi \in \mathcal{H}_\chi$ iff $\rho(g)\varphi_\chi = \chi(g)\varphi_\chi$ for every $g \in T_W$.

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g)\ ;\ \ g \in T_W\}\,.$$

  - C commutative group of unitary operators commuting with DFT.
  - Can diagonalize C simultaneously.
- We have orthogonal decomposition

$$\mathcal{H} = \bigoplus_{\chi: T_W \to \mathbb{C}^*} \mathcal{H}_\chi,$$

  - $\varphi_\chi \in \mathcal{H}_\chi$ iff $\rho(g)\varphi_\chi = \chi(g)\varphi_\chi$ for every $g \in T_W$.

Theorem

$\dim \mathcal{H}_\chi = 1$.

Diagonalizing the DFT

- Symmetries of DFT

$$C = \mathrm{Im}(T_W) = \{\rho(g)\ ;\ \ g \in T_W\}\,.$$

  - C commutative group of unitary operators commuting with DFT.
  - Can diagonalize C simultaneously.
- We have orthogonal decomposition

$$\mathcal{H} = \bigoplus_{\chi: T_W \to \mathbb{C}^*} \mathcal{H}_\chi,$$

  - $\varphi_\chi \in \mathcal{H}_\chi$ iff $\rho(g)\varphi_\chi = \chi(g)\varphi_\chi$ for every $g \in T_W$.

Theorem

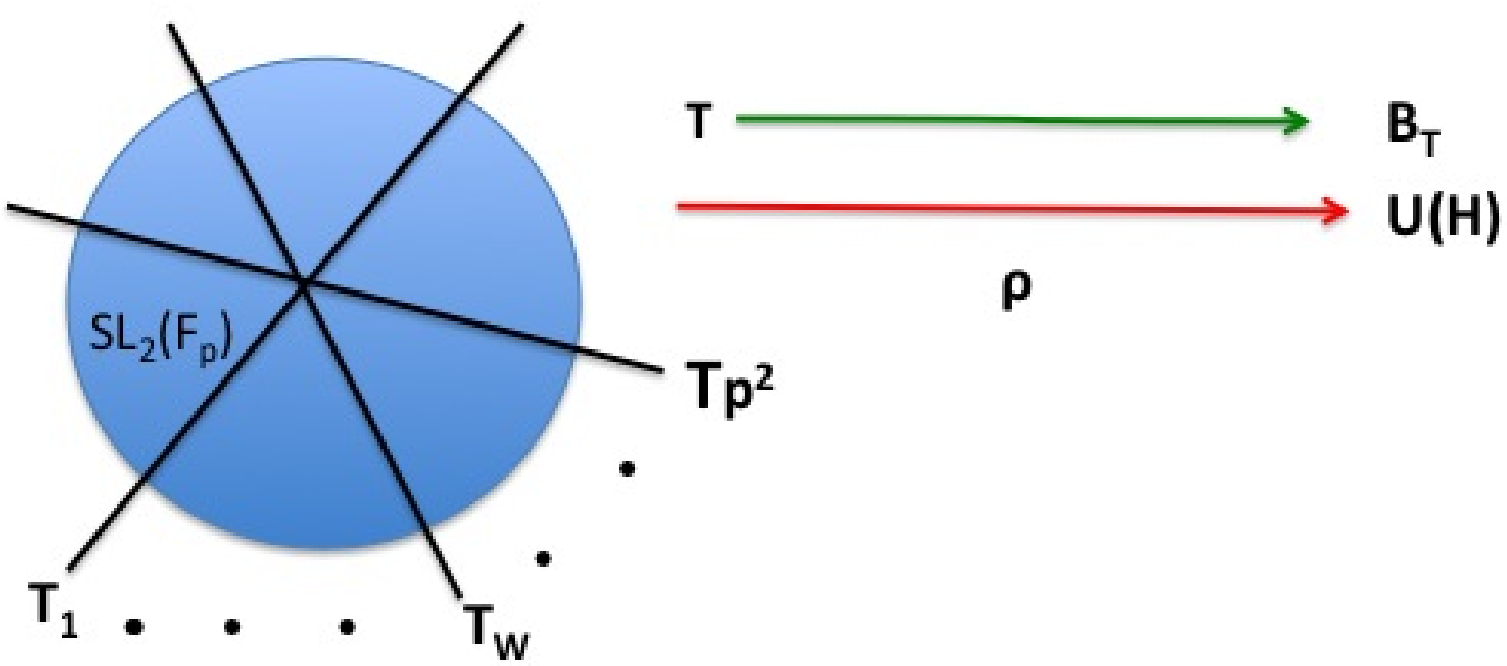
$\dim \mathcal{H}_\chi = 1$.

- Obtained the **Canonical basis of eigenfunctions of DFT**

$$B_{T_W} = \{\varphi_\chi \in \mathcal{H}_\chi\}.$$

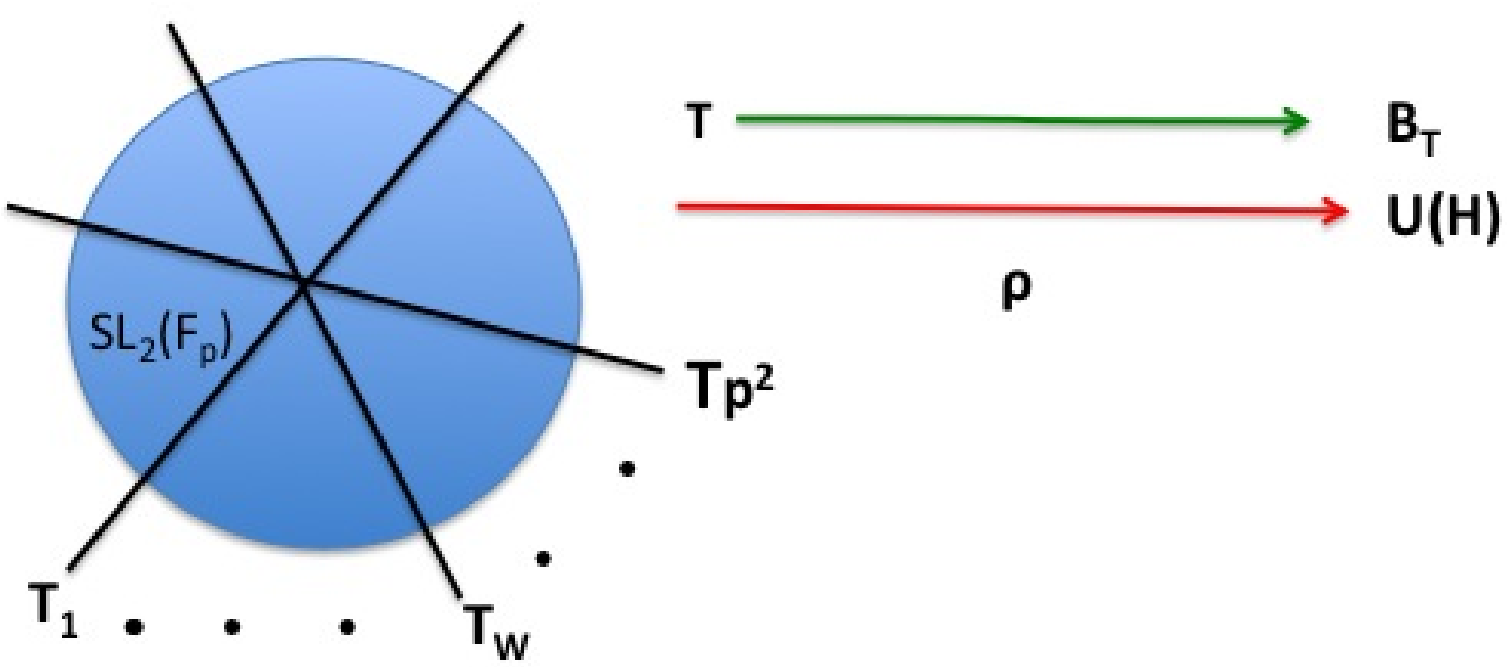
(IV) The Oscillator Dictionary

- Generalization



(IV) The Oscillator Dictionary

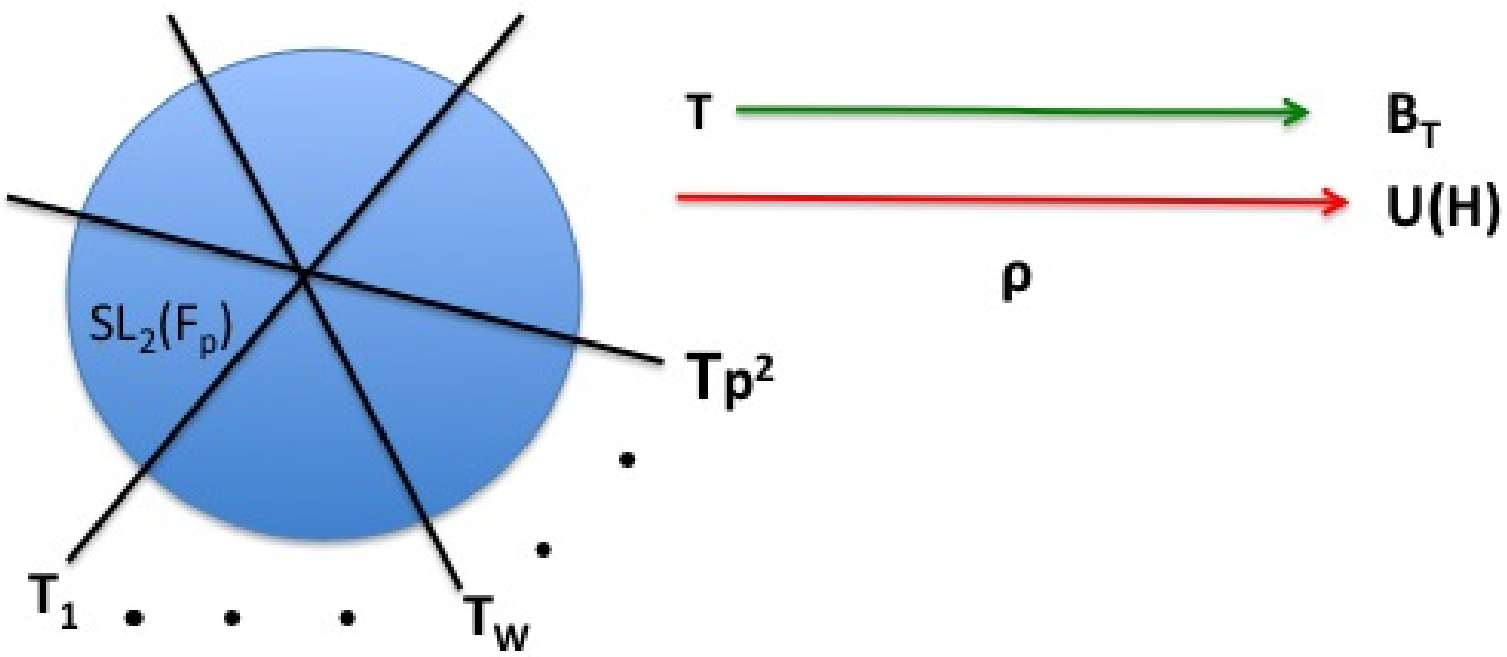
- Generalization



- Each T_i, $i = 1, ..., p^2$, torus in $SL_2(\mathbb{F}_p)$.

(IV) The Oscillator Dictionary

- Generalization

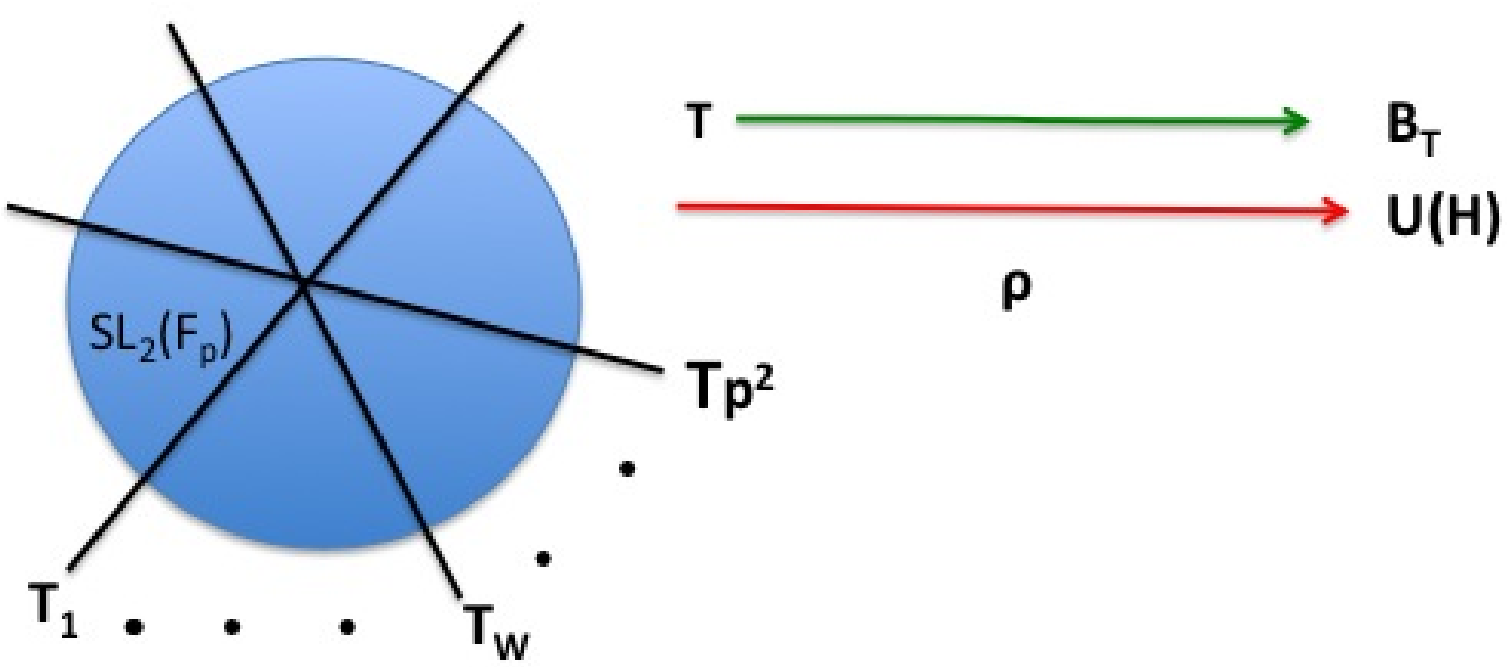


- Each T_i, $i = 1, ..., p^2$, torus in $SL_2(\mathbb{F}_p)$.
- Oscillator Dictionary

$$D = \coprod_{T \subset SL_2(\mathbb{F}_p)} B_T.$$

(IV) The Oscillator Dictionary

- Generalization



- Each T_i, $i = 1, ..., p^2$, torus in $SL_2(\mathbb{F}_p)$.
- Oscillator Dictionary

$$D = \coprod_{T \subset SL_2(\mathbb{F}_p)} B_T.$$

  - $\#D \approx p^3$.

Oscillator Dictionary - Properties

Theorem (Pseudo-Randomness)

We have

Oscillator Dictionary - Properties

Theorem (Pseudo-Randomness)

We have

1. **Auto-correlations.** *For every* $\varphi \in D$

$$|\langle\ \varphi, \pi(\tau,\omega)\varphi\rangle| = \begin{cases} 1 & \text{if } (\tau,\omega) = (0,0), \\ \leq 2/\sqrt{p} & \text{other.} \end{cases}$$

Oscillator Dictionary - Properties

Theorem (Pseudo-Randomness)

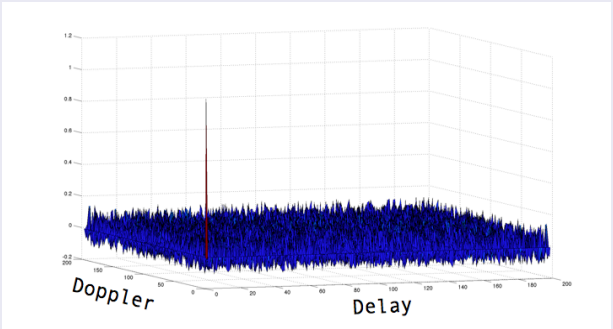
We have

1. **Auto-correlations.** *For every* $\varphi \in D$

$$|\langle\, \varphi, \pi(\tau,\omega)\varphi\rangle| = \begin{cases} 1 & \text{if } (\tau,\omega) = (0,0), \\ \leq 2/\sqrt{p} & \text{other.} \end{cases}$$

2. **Cross-correlation.** *For every* $\varphi \neq \phi \in D$

$$|\langle\, \varphi, \pi(\tau,\omega)\phi\rangle| \leq 4/\sqrt{p}.$$



THANK YOU

Thank You!