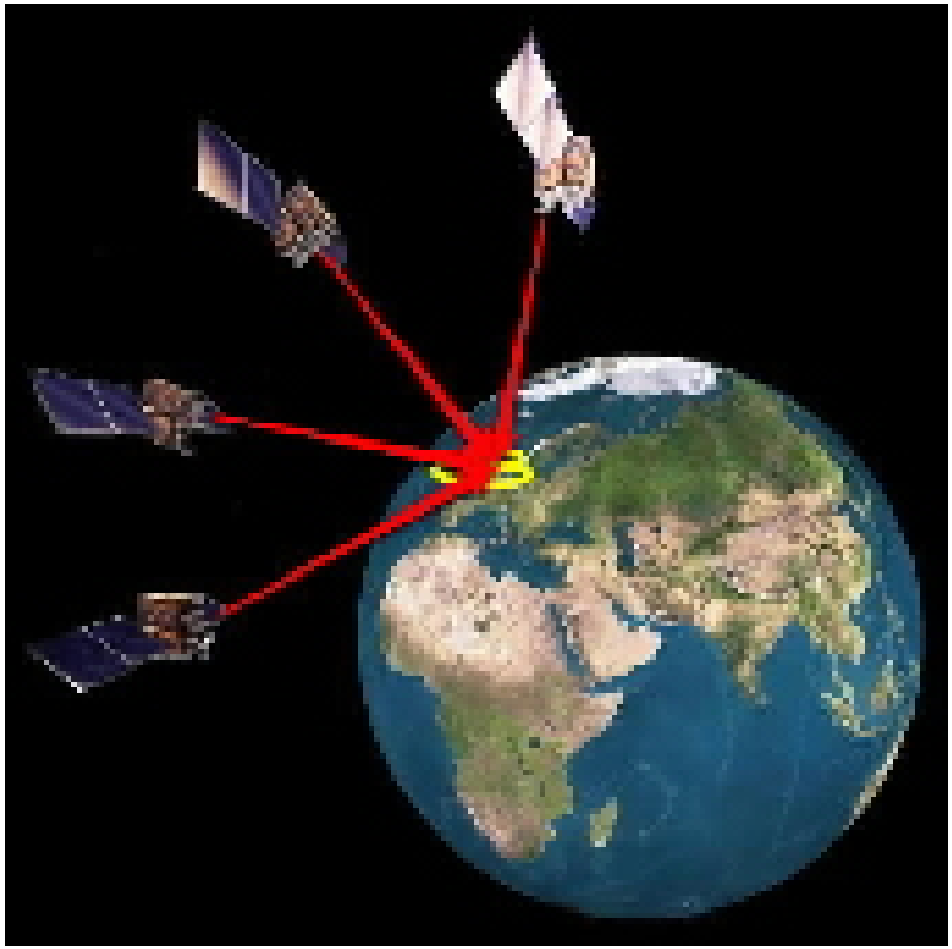
# The Geometric Weil Representation and Pseudo-Random Vectors

Shamgar Gurevich

Madison

August 5, 2014

# (0) MOTIVATION - GPS



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

# Motivation - GPS

- $S$, $R \in \mathcal{H} = \mathbb{C}^p$ – Hilbert space of digital sequences, $p \gg 1000$.

# Motivation - GPS

- $S,\ R \in \mathcal{H} = \mathbb{C}^p$ – Hilbert space of digital sequences, $p \gg 1000$.
  - $S,\ R : \mathbb{F}_p = \{0, ...., p-1\} \to \mathbb{C}$.

# Motivation - GPS

- $S,\ R \in \mathcal{H} = \mathbb{C}^p$ – Hilbert space of digital sequences, $p \gg 1000$.
  - $S,\ R : \mathbb{F}_p = \{0, ...., p-1\} \to \mathbb{C}$.
  - $\psi[n] = e^{\frac{2\pi i}{p} n}$.

# Motivation - GPS

- $S,\ R \in \mathcal{H} = \mathbb{C}^p$ – Hilbert space of digital sequences, $p \gg 1000$.
  - $S,\ R : \mathbb{F}_p = \{0, ...., p-1\} \to \mathbb{C}$.
  - $\psi[n] = e^{\frac{2\pi i}{p} n}$.
- Satellite transmits $b \cdot S,\ b \in \{1, -1\}$ coordinates.

# Motivation - GPS

- $S,\ R \in \mathcal{H} = \mathbb{C}^p$ – Hilbert space of digital sequences, $p \gg 1000$.
  - $S,\ R : \mathbb{F}_p = \{0, ...., p-1\} \to \mathbb{C}$.
  - $\psi[n] = e^{\frac{2\pi i}{p} n}$.
- Satellite transmits $b \cdot S,\ b \in \{1, -1\}$ coordinates.

## Fact

*Client receives*

$$R[n] = b \cdot \alpha_0 \cdot \psi[\omega_0 n] \cdot S[n - \tau_0] + \mathcal{W}[n], \quad n \in \mathbb{F}_p,$$

$\alpha_0 \in \mathbb{C}$ *attenuation,* $\omega_0 \in \mathbb{F}_p$ *Doppler,* $\tau_0 \in \mathbb{F}_p$ *delay,* $\mathcal{W} \in \mathcal{H}$ *random white noise.*

# Motivation - GPS

- $S,\ R \in \mathcal{H} = \mathbb{C}^p$ – Hilbert space of digital sequences, $p \gg 1000$.
  - $S,\ R : \mathbb{F}_p = \{0, ...., p-1\} \to \mathbb{C}$.
  - $\psi[n] = e^{\frac{2\pi i}{p} n}$.
- Satellite transmits $b \cdot S,\ b \in \{1, -1\}$ coordinates.

## Fact

*Client receives*

$$R[n] = b \cdot \alpha_0 \cdot \psi[\omega_0 n] \cdot S[n - \tau_0] + \mathcal{W}[n], \quad n \in \mathbb{F}_p,$$

$\alpha_0 \in \mathbb{C}$ *attenuation,* $\omega_0 \in \mathbb{F}_p$ *Doppler,* $\tau_0 \in \mathbb{F}_p$ *delay,* $\mathcal{W} \in \mathcal{H}$ *random white noise.*

## Problem (The GPS Problem)

*Design* $S \in \mathcal{H}$*, and effective method to extract* $(b, \tau_0)$*, using* $R$ *and* $S$*.*

# SOLUTION - Matched Filter

## Definition

Matched filter

$$\begin{cases} \mathcal{M}(R,S): \overbrace{\mathbb{F}_p \times \mathbb{F}_p}^{\text{Time-Frequency}} \to \mathbb{C}, \\ \mathcal{M}(R,S)[\tau,\omega] = \langle R[n] \ , \ \psi[\omega n] \cdot S[n-\tau] \rangle \ . \end{cases}$$

# SOLUTION - Matched Filter

## Definition

Matched filter

$$\begin{cases} \mathcal{M}(R,S): \overbrace{\mathbb{F}_p \times \mathbb{F}_p}^{\text{Time-Frequency}} \to \mathbb{C}, \\ \mathcal{M}(R,S)[\tau,\omega] = \langle R[n] \ , \ \psi[\omega n] \cdot S[n-\tau] \rangle \ . \end{cases}$$

- **Question:** What $S$ to use for extracting $(\tau_0, \omega_0)$ from $\mathcal{M}(R,S)$ ?

# Solution - MATCHED FILTER

- Typical solution: $S$ = pseudo-random (PR)

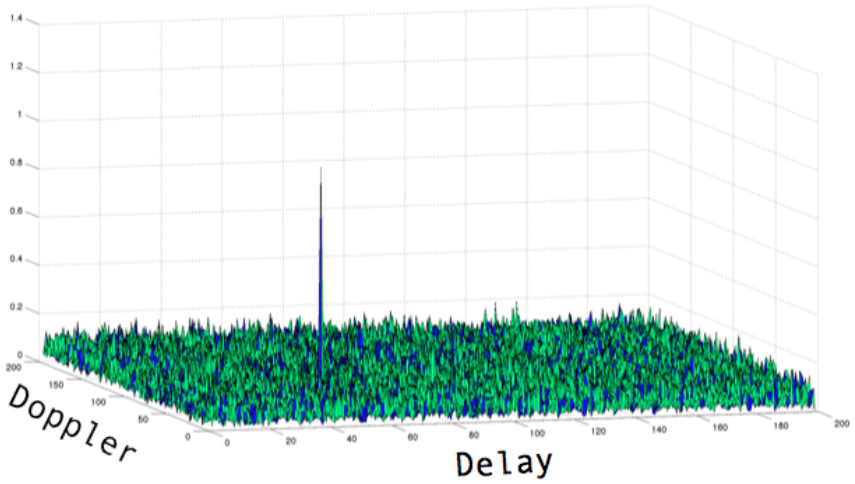



Figure: $|\mathcal{M}(R,S)|$, $(\tau_0,\omega_0)=(50,50)$.

# Solution - MATCHED FILTER

- Typical solution: $S$ = pseudo-random (PR)

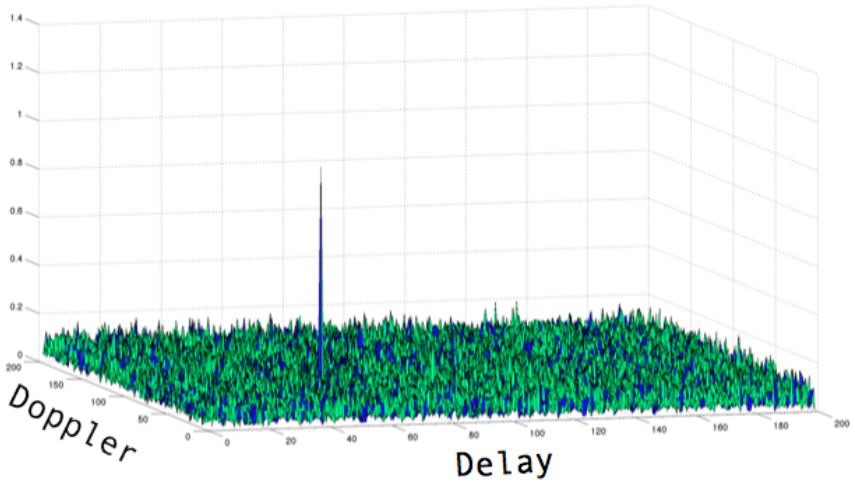



Figure: $|\mathcal{M}(R,S)|$, $(\tau_0,\omega_0)=(50,50)$.

- Using FFT compute $\mathcal{M}(R,S)$ in $O(p^2\cdot\log p)$ operations.

# Solution - MATCHED FILTER

- Typical solution: $S$ = pseudo-random (PR)

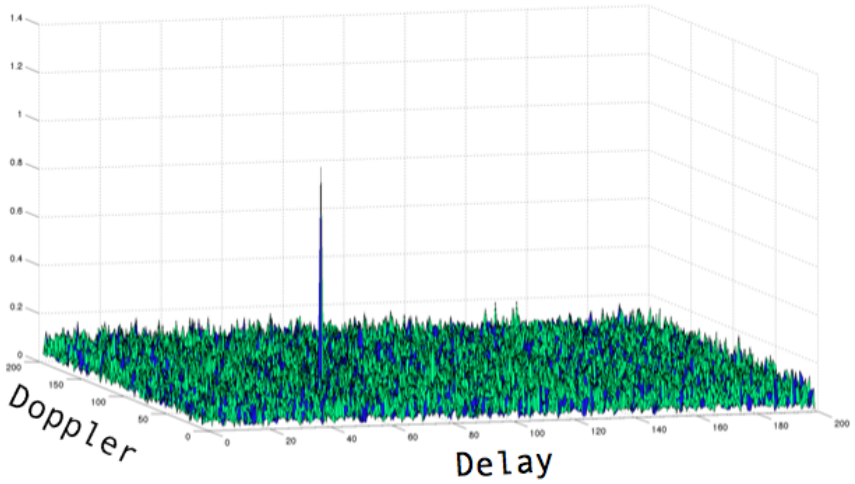



Figure: $|\mathcal{M}(R,S)|$, $(\tau_0,\omega_0)=(50,50)$.

- Using FFT compute $\mathcal{M}(R,S)$ in $O(p^2\cdot\log p)$ operations.

- **Task:** Find method to construct explicit PR sequences.

# WEIL REP'N SEQUENCES - Idea

- Weil rep'n (**Weil** 64)

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to GL(\mathbb{C}(\mathbb{F}_p)), \\ \rho \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = DFT. \end{cases}$$

# WEIL REP'N SEQUENCES - Idea

- Weil rep'n (**Weil** 64)

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to GL(\mathbb{C}(\mathbb{F}_p)), \\ \rho \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = DFT. \end{cases}$$

- **Mechanism for sequences construction**

# WEIL REP'N SEQUENCES - Idea

- Weil rep'n (**Weil** 64)

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to GL(\mathbb{C}(\mathbb{F}_p)), \\ \rho \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = DFT. \end{cases}$$

- **Mechanism for sequences construction**
  - $T \subset SL_2(\mathbb{F}_p)$ torus

$$\rho : T \curvearrowright \mathcal{H} = \bigoplus_{\chi : T \to \mathbb{C}^*} \mathcal{H}_\chi.$$

# WEIL REP'N SEQUENCES - Idea

- Weil rep'n (**Weil** 64)

$$\begin{cases} \rho : SL_2(\mathbb{F}_p) \to GL(\mathbb{C}(\mathbb{F}_p)), \\ \rho \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = DFT. \end{cases}$$

- **Mechanism for sequences construction**
  - $T \subset SL_2(\mathbb{F}_p)$ torus

$$\rho : T \curvearrowright \mathcal{H} = \bigoplus_{\chi : T \to \mathbb{C}^*} \mathcal{H}_\chi.$$

  - $\dim \mathcal{H}_\chi = 1, \quad \varphi_\chi \in \mathcal{H}_\chi, \quad \left\| \varphi_\chi \right\| = 1.$

# Weil Rep'n Sequences - IDEA

## Theorem (Pseudo Randomness)

*For* $(\tau, \omega) \neq (0, 0)$

$$\left|\mathcal{M}(\varphi_\chi\ ,\ \varphi_\chi)[\tau, \omega]\right| \leq \frac{2}{\sqrt{p}}.$$

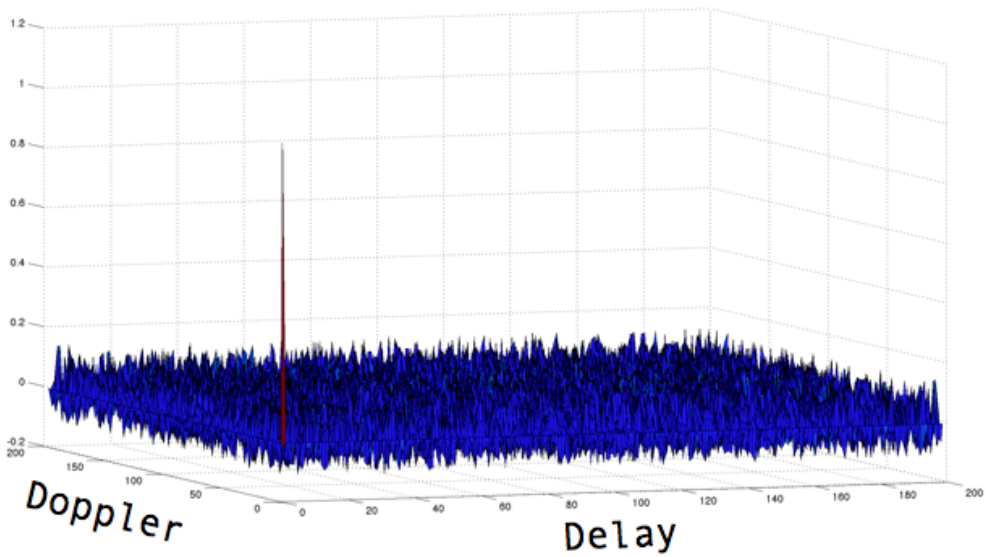



Figure: $\mathcal{M}(\varphi_\chi, \varphi_\chi)$, $q = 199$.

# BOUNDS VIA GEOMETRIC WEIL REP'N - Idea

- $\ell$-adic sheaves (**Grothendieck** 60s)

$$D_c^b(\mathbb{A}^1) \quad \rightsquigarrow \quad \mathbb{C}(\mathbb{F}_q).$$

# BOUNDS VIA GEOMETRIC WEIL REP'N - Idea

- $\ell$-adic sheaves (**Grothendieck** 60s)

$$D_c^b(\mathbb{A}^1) \quad \rightsquigarrow \quad \mathbb{C}(\mathbb{F}_q).$$

- Want

$$\text{Geometric Weil Rep'n} \quad \rightsquigarrow \quad \rho.$$

# BOUNDS VIA GEOMETRIC WEIL REP'N - Idea

- $\ell$-adic sheaves (**Grothendieck** 60s)

$$D_c^b(\mathbb{A}^1) \quad \rightsquigarrow \quad \mathbb{C}(\mathbb{F}_q).$$

- Want

$$\text{Geometric Weil Rep'n} \quad \rightsquigarrow \quad \rho.$$

- Application: Geometrizing $\mathcal{M}(\varphi_\chi, \varphi_\chi)$ and obtain the bound.

# (I) WEIL REPRESENTATION

- Heisenberg Representation

# (I) WEIL REPRESENTATION

- Heisenberg Representation
  - $(V, \Omega)$ – $2n$-dimensional symplectic vector space over $k = \mathbb{F}_q$, char$\neq 2$.

# (I) WEIL REPRESENTATION

- Heisenberg Representation
  - $(V, \Omega)$ – $2n$-dimensional symplectic vector space over $k = \mathbb{F}_q$, char$\neq 2$.
  - $H = H(V)$ – Heisenberg group

# (I) WEIL REPRESENTATION

- Heisenberg Representation
  - $(V, \Omega)$ – $2n$-dimensional symplectic vector space over $k = \mathbb{F}_q$, char$\neq 2$.
  - $H = H(V)$ – Heisenberg group
    - $H = V \times k$;

# (I) WEIL REPRESENTATION

- Heisenberg Representation
  - $(V, \Omega)$ – $2n$-dimensional symplectic vector space over $k = \mathbb{F}_q$, char$\neq 2$.
  - $H = H(V)$ – Heisenberg group
    - $H = V \times k$;
    - $(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\Omega(v, v'))$.

# (I) WEIL REPRESENTATION

- Heisenberg Representation
  - $(V, \Omega)$ – $2n$-dimensional symplectic vector space over $k = \mathbb{F}_q$, char$\neq 2$.
  - $H = H(V)$ – Heisenberg group
    - $H = V \times k$;
    - $(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\Omega(v, v'))$.
  - $1 \neq \psi : k \to \mathbb{C}^*$ – additive character.

# (I) WEIL REPRESENTATION

- Heisenberg Representation
  - $(V, \Omega)$ – $2n$-dimensional symplectic vector space over $k = \mathbb{F}_q$, char$\neq 2$.
  - $H = H(V)$ – Heisenberg group
    - $H = V \times k$;
    - $(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\Omega(v, v'))$.
  - $1 \neq \psi : k \to \mathbb{C}^*$ – additive character.

**Theorem (Stone–von Neumann)**

*There exists a unique (up to $\simeq$) irreducible representation* $\underbrace{\pi : H \to GL(\mathcal{H})}_{\text{Heisenberg rep'n}}$ *s.t.* $\pi(z) = \psi(z) \cdot Id_{\mathcal{H}}$, $z \in Z(H) = k$.

# WEIL REPRESENTATION

## Example

$n = 1$, $V = k \times k$, $\mathcal{H} = \mathbb{C}(k)$,

# WEIL REPRESENTATION

## Example

$n = 1$, $V = k \times k$, $\mathcal{H} = \mathbb{C}(k)$,

- $[\pi(\tau, 0, 0)f](t) = f(t + \tau)$;

# WEIL REPRESENTATION

## Example

$n = 1,\ V = k \times k,\ \ \mathcal{H} = \mathbb{C}(k),$

- $[\pi(\tau, 0, 0)f](t) = f(t + \tau);$
- $[\pi(0, \omega, 0)f](t) = \psi(\omega t)f(t);$

# WEIL REPRESENTATION

## Example

$n = 1,\ V = k \times k,\ \ \mathcal{H} = \mathbb{C}(k),$

- $[\pi(\tau, 0, 0)f](t) = f(t + \tau);$
- $[\pi(0, \omega, 0)f](t) = \psi(\omega t)f(t);$
- $[\pi(0, 0, z)f](t) = \psi(z)f(t).$

# WEIL REPRESENTATION

## Example

$n = 1$, $V = k \times k$, $\mathcal{H} = \mathbb{C}(k)$,

- $[\pi(\tau, 0, 0)f](t) = f(t + \tau)$;
- $[\pi(0, \omega, 0)f](t) = \psi(\omega t)f(t)$;
- $[\pi(0, 0, z)f](t) = \psi(z)f(t)$.

- Weil Representation (Weil '64): Take $g \in Sp(V) = Sp$, then

# WEIL REPRESENTATION

## Example

$n = 1$, $V = k \times k$, $\mathcal{H} = \mathbb{C}(k)$,

- $[\pi(\tau, 0, 0)f](t) = f(t + \tau)$;
- $[\pi(0, \omega, 0)f](t) = \psi(\omega t)f(t)$;
- $[\pi(0, 0, z)f](t) = \psi(z)f(t)$.

- Weil Representation (Weil '64): Take $g \in Sp(V) = Sp$, then

  $$\pi \overset{\rho(g)}{\widetilde{\longrightarrow}} \pi^g(v, z) = \pi(gv, z),$$

  i.e.,

  $$\rho(g)\pi(h)\rho(g)^{-1} = \pi(g[h]), \quad \text{for every } h \in H. \tag{1}$$

# WEIL REPRESENTATION

**Theorem**

*There exists a unique representation*

$$\rho : Sp \to GL(\mathcal{H}) \quad — \quad \textit{Weil representation},$$

*that satisfies (1).*

# WEIL REPRESENTATION

**Theorem**

*There exists a unique representation*

$$\rho : Sp \to GL(\mathcal{H}) \quad — \quad \textit{Weil representation},$$

*that satisfies (1).*

**Problem**

*Formula for $\rho$ ?*

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;
  - $W(A)[h] = \frac{1}{\dim \mathcal{H}} Tr(A\pi[h^{-1}])$.

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;
  - $W(A)[h] = \frac{1}{\dim \mathcal{H}} Tr(A\pi[h^{-1}])$.
- Kernel of Weil Rep'n

$$\begin{cases} K : Sp \times V \to \mathbb{C}, \\ K(g, v) = W(\rho(g))[v]. \end{cases}$$

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;
  - $W(A)[h] = \frac{1}{\dim \mathcal{H}} Tr(A\pi[h^{-1}])$.
- Kernel of Weil Rep'n

$$\begin{cases} K : Sp \times V \to \mathbb{C}, \\ K(g, v) = W(\rho(g))[v]. \end{cases}$$

1. $\pi[K(g, \cdot)] := \sum_{v \in V} K(g, v)\pi(v) = \rho(g)$.

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;
  - $W(A)[h] = \frac{1}{\dim \mathcal{H}} Tr(A\pi[h^{-1}])$.
- Kernel of Weil Rep'n

$$\begin{cases} K : Sp \times V \to \mathbb{C}, \\ K(g, v) = W(\rho(g))[v]. \end{cases}$$

1. $\pi[K(g, \cdot)] := \sum_{v \in V} K(g, v)\pi(v) = \rho(g)$.
2. $K(g_1, \cdot) * K(g_2, \cdot) = K(g_1 g_2, \cdot)$.

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;
  - $W(A)[h] = \frac{1}{\dim \mathcal{H}} Tr(A\pi[h^{-1}])$.
- Kernel of Weil Rep'n

$$\begin{cases} K : Sp \times V \to \mathbb{C}, \\ K(g, v) = W(\rho(g))[v]. \end{cases}$$

1. $\pi[K(g, \cdot)] := \sum_{v \in V} K(g, v)\pi(v) = \rho(g)$.
2. $K(g_1, \cdot) * K(g_2, \cdot) = K(g_1 g_2, \cdot)$.
3. **Formula**: On $U = \{g \in Sp;\ \det(g - I) \neq 0\}$

$$K(g, v) = \frac{1}{q^n} \cdot \sigma[(-1)^n \det(g - I)] \cdot \psi[\Omega(\frac{g + I}{g - I} v, v)].$$

# Weil Rep'n - FORMULA

- Formula for $A \in End(\mathcal{H})$?
- Weyl Transform
  - $\mathbb{C}(H, \overset{*}{\psi}^{-1}) \underset{W}{\overset{\pi}{\rightleftarrows}} \overset{\circ}{End}(\mathcal{H})$;
  - $W(A)[h] = \frac{1}{\dim \mathcal{H}} Tr(A\pi[h^{-1}])$.
- Kernel of Weil Rep'n

$$\begin{cases} K : Sp \times V \to \mathbb{C}, \\ K(g, v) = W(\rho(g))[v]. \end{cases}$$

1. $\pi[K(g, \cdot)] := \sum_{v \in V} K(g, v)\pi(v) = \rho(g)$.
2. $K(g_1, \cdot) * K(g_2, \cdot) = K(g_1 g_2, \cdot)$.
3. **Formula**: On $U = \{g \in Sp;\ \det(g - I) \neq 0\}$

$$K(g, v) = \frac{1}{q^n} \cdot \sigma[(-1)^n \det(g - I)] \cdot \psi[\Omega(\frac{g + I}{g - I} v, v)].$$

- *Proof.* Geometric Weil Rep'n.

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - **X** – Algebraic variety over $k = \mathbb{F}_q$.

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - $\mathbf{X}$ – Algebraic variety over $k = \mathbb{F}_q$.
    - $Fr \curvearrowright \mathbf{X}$.

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - $\mathbf{X}$ – Algebraic variety over $k = \mathbb{F}_q$.
    - $Fr \curvearrowright \mathbf{X}$.
    - $X = \mathbf{X}^{Fr} = \mathbf{X}(k)$.

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - $\mathbf{X}$ – Algebraic variety over $k = \mathbb{F}_q$.
    - $Fr \curvearrowright \mathbf{X}$.
    - $X = \mathbf{X}^{Fr} = \mathbf{X}(k)$.
  - Nice function

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - $\mathbf{X}$ – Algebraic variety over $k = \mathbb{F}_q$.
    - $Fr \curvearrowright \mathbf{X}$.
    - $X = \mathbf{X}^{Fr} = \mathbf{X}(k)$.
  - Nice function
    -

$$Fr \curvearrowright \overset{\ell\text{-adic Weil sheaf}}{\underset{\mathbf{X}}{\overset{\mathcal{F}}{\downarrow}}} \quad \underset{\text{sheaf-to-function}}{- - - - - - - >} \quad f^{\mathcal{F}} : X \to \mathbb{C}.$$

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - $\mathbf{X}$ – Algebraic variety over $k = \mathbb{F}_q$.
    - $Fr \curvearrowright \mathbf{X}$.
    - $X = \mathbf{X}^{Fr} = \mathbf{X}(k)$.
  - Nice function
    - $$Fr \curvearrowright \begin{array}{c} \overset{\ell\text{-adic Weil sheaf}}{\mathcal{F}} \\ \downarrow \\ \mathbf{X} \end{array} \quad \underset{\text{sheaf-to-function}}{- - - - - - - >} \quad f^{\mathcal{F}} : X \to \mathbb{C}.$$
    - $Fr : \mathcal{F}_x \widetilde{\to} \mathcal{F}_{Fr(x)}$.

# (II) Geometric Weil Rep'n - GEOMETRIZATION

- Geometrization (**Grothendieck**)
  - Nice set
    - $\mathbf{X}$ – Algebraic variety over $k = \mathbb{F}_q$.
    - $Fr \curvearrowright \mathbf{X}$.
    - $X = \mathbf{X}^{Fr} = \mathbf{X}(k)$.
  - Nice function
    - $$Fr \curvearrowright \begin{array}{c} \overset{\ell\text{-adic Weil sheaf}}{\mathcal{F}} \\ \downarrow \\ \mathbf{X} \end{array} \quad \underset{\text{sheaf-to-function}}{- - - - - - - >} \quad f^{\mathcal{F}} : X \to \mathbb{C}.$$
    - $Fr : \mathcal{F}_x \widetilde{\to} \mathcal{F}_{Fr(x)}$.
    - $f^{\mathcal{F}}(x) = Tr(Fr \curvearrowright \mathcal{F}_x)$, $x \in X$.

# Geometrization - EXAMPLES

- Examples

# Geometrization - EXAMPLES

- Examples
  1. $\mathbf{X} = \mathbb{A}^1$, $Fr(x) = x^q$, $\mathbb{A}^1(k) = k$, $\psi : k \to \mathbb{C}^*$ – additive character,

$$Fr \curvearrowright \overset{\text{Artin–Schreier sheaf}}{\underset{\mathbb{A}^1}{\mathcal{L}_\psi \downarrow}} \quad \underset{\text{sheaf-to-function}}{- - - - - - - >} \quad f^{\mathcal{L}_\psi} = \psi.$$

# Geometrization - EXAMPLES

- Examples
  1. $\mathbf{X} = \mathbb{A}^1$, $Fr(x) = x^q$, $\mathbb{A}^1(k) = k$, $\psi : k \to \mathbb{C}^*$ – additive character,

$$Fr \curvearrowright \begin{array}{c} \overset{\text{Artin–Schreier sheaf}}{\mathcal{L}_\psi} \\ \downarrow \\ \mathbb{A}^1 \end{array} \quad \underset{\text{sheaf-to-function}}{- - - - - - - >} \quad f^{\mathcal{L}_\psi} = \psi.$$

  2. $\mathbf{X} = \mathbb{G}_m$, $Fr(x) = x^q$, $\mathbb{G}_m(k) = k^*$, $\chi : k^* \to \mathbb{C}^*$ – multiplicative character,

$$Fr \curvearrowright \begin{array}{c} \overset{\text{Kummer sheaf}}{\mathcal{L}_\chi} \\ \downarrow \\ \mathbb{G}_m \end{array} \quad \underset{\text{sheaf-to-function}}{- - - - - - - >} \quad f^{\mathcal{L}_\chi} = \chi.$$

# GEOMETRIC WEIL REP'N

- Weil rep'n kernel

$$K : \overbrace{Sp \times V}^{\mathbf{Sp} \times \mathbf{V}(k)} \to \mathbb{C}.$$

# GEOMETRIC WEIL REP'N

- Weil rep'n kernel

$$K : \overbrace{Sp \times V}^{\mathbf{Sp} \times \mathbf{V}(k)} \to \mathbb{C}.$$

## Theorem (Geometri Weil Repn)

$\exists$ *geometrically irreducible* $[\dim \mathbf{Sp}]$*-perverse Weil sheaf* $\mathcal{K}$ *on* $\mathbf{Sp} \times \mathbf{V}$ *of pure weight zero with*

# GEOMETRIC WEIL REP'N

- Weil rep'n kernel

$$K : \overbrace{Sp \times V}^{\mathbf{Sp} \times \mathbf{V}(k)} \to \mathbb{C}.$$

## Theorem (Geometri Weil Repn)

$\exists$ *geometrically irreducible* $[\dim \mathbf{Sp}]$*-perverse Weil sheaf* $\mathcal{K}$ *on* $\mathbf{Sp} \times \mathbf{V}$ *of pure weight zero with*

1. *Multiplicativity. Canonical isomorphism* $\theta : \mathcal{K}(g_1, \cdot) * \mathcal{K}(g_2, \cdot) \widetilde{\to} \mathcal{K}(g_1 g_2, \cdot)$.

# GEOMETRIC WEIL REP'N

- Weil rep'n kernel

$$K : \overbrace{Sp \times V}^{\mathbf{Sp} \times \mathbf{V}(k)} \to \mathbb{C}.$$

## Theorem (Geometri Weil Repn)

$\exists$ *geometrically irreducible* $[\dim \mathbf{Sp}]$*-perverse Weil sheaf* $\mathcal{K}$ *on* $\mathbf{Sp} \times \mathbf{V}$ *of pure weight zero with*

1. *Multiplicativity. Canonical isomorphism* $\theta : \mathcal{K}(g_1, \cdot) * \mathcal{K}(g_2, \cdot) \widetilde{\to} \mathcal{K}(g_1 g_2, \cdot)$.
2. *Function.* $f^{\mathcal{K}} = K$.

# GEOMETRIC WEIL REP'N

- Weil rep'n kernel

$$K : \overbrace{Sp \times V}^{\mathbf{Sp} \times \mathbf{V}(k)} \to \mathbb{C}.$$

## Theorem (Geometri Weil Repn)

$\exists$ *geometrically irreducible* $[\dim \mathbf{Sp}]$*-perverse Weil sheaf* $\mathcal{K}$ *on* $\mathbf{Sp} \times \mathbf{V}$ *of pure weight zero with*

1. *Multiplicativity. Canonical isomorphism* $\theta : \mathcal{K}(g_1, \cdot) * \mathcal{K}(g_2, \cdot) \widetilde{\to} \mathcal{K}(g_1 g_2, \cdot)$.
2. *Function.* $f^{\mathcal{K}} = K$.
3. *Formula. On* $\mathbf{U} \times \mathbf{V}$

$$\mathcal{K}(g, v) = \mathcal{L}_{\sigma[(-1)^n \det(g-I))]} \otimes \mathcal{L}_{\psi[\Omega(\frac{g+I}{g-I} v, v)]}[2n](n).$$

# (III) APPLICATION – Pseudo-Randomness of Weil Sequences

- $\rho : SL_2(k) \to GL(\mathcal{H})$, $\mathcal{H} = \mathbb{C}(k)$.

# (III) APPLICATION – Pseudo-Randomness of Weil Sequences

- $\rho : SL_2(k) \to GL(\mathcal{H})$, $\mathcal{H} = \mathbb{C}(k)$.
- $T \subset SL_2(k)$ torus

$$\rho : T \curvearrowright \mathcal{H} = \bigoplus_{\chi : T \to \mathbb{C}^*} \mathcal{H}_\chi.$$

# (III) APPLICATION – Pseudo-Randomness of Weil Sequences

- $\rho : SL_2(k) \to GL(\mathcal{H})$, $\mathcal{H} = \mathbb{C}(k)$.
- $T \subset SL_2(k)$ torus

$$\rho : T \curvearrowright \mathcal{H} = \bigoplus_{\chi : T \to \mathbb{C}^*} \mathcal{H}_\chi.$$

- $\dim \mathcal{H}_\chi = 1$, $\varphi_\chi \in \mathcal{H}_\chi$, $\left\| \varphi_\chi \right\| = 1$.

# (III) APPLICATION – Pseudo-Randomness of Weil Sequences

- $\rho : SL_2(k) \to GL(\mathcal{H})$, $\mathcal{H} = \mathbb{C}(k)$.
- $T \subset SL_2(k)$ torus

$$\rho : T \curvearrowright \mathcal{H} = \bigoplus_{\chi : T \to \mathbb{C}^*} \mathcal{H}_\chi.$$

- $\dim \mathcal{H}_\chi = 1, \varphi_\chi \in \mathcal{H}_\chi, \left\|\varphi_\chi\right\| = 1.$

**Theorem (Pseudo-randomness)**

*For $v \neq 0$ we have*

$$\left|\left\langle \varphi_\chi, \pi(v)\varphi_\chi \right\rangle\right| \leq \frac{2}{\sqrt{q}}.$$

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.
  - $\left\langle \varphi_\chi, \pi(v)\varphi_\chi \right\rangle = Tr(P_\chi \pi(v)) = \frac{1}{q \pm 1} \sum_{g \in T} \chi(g^{-1})\, Tr(\rho(g)\pi(v))$.

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.
  - $\left\langle \varphi_\chi, \pi(v)\varphi_\chi \right\rangle = Tr(P_\chi \pi(v)) = \frac{1}{q \pm 1} \sum_{g \in T} \chi(g^{-1})\, Tr(\rho(g)\pi(v))$.
  - Show

$$\left| \sum_{g \in T} \underbrace{\chi(g^{-1}) K_{|T}(g, v)}_{F,\ |F|=1} \right| \leq 2\sqrt{q}.$$

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.
  - $\left\langle \varphi_\chi,\, \pi(v)\varphi_\chi \right\rangle = Tr(P_\chi \pi(v)) = \frac{1}{q \pm 1} \sum_{g \in T} \chi(g^{-1})\, Tr(\rho(g)\pi(v))$.
  - Show

$$\left| \sum_{g \in T} \underbrace{\chi(g^{-1}) K_{|T}(g, v)}_{F,\ |F|=1} \right| \leq 2\sqrt{q}.$$

- (2) *Geometric Weil rep'n.*

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.
  - $\left\langle \varphi_\chi,\, \pi(v)\varphi_\chi \right\rangle = Tr(P_\chi \pi(v)) = \frac{1}{q \pm 1} \sum_{g \in T} \chi(g^{-1})\, Tr(\rho(g)\pi(v))$.
  - Show

$$\left| \sum_{g \in T} \underbrace{\chi(g^{-1}) K_{|T}(g, v)}_{F,\ |F|=1} \right| \leq 2\sqrt{q}.$$

- (2) *Geometric Weil rep'n.*
  - $F = f^{\mathcal{F}}$, $\mathcal{F} = \mathcal{L}_\chi \otimes \mathcal{K}_{|\mathbf{T}}$ - explicit line bundle on $\mathbf{T}$ with flat connection.

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.
  - $\left\langle \varphi_\chi,\, \pi(v)\varphi_\chi \right\rangle = Tr(P_\chi \pi(v)) = \frac{1}{q \pm 1} \sum_{g \in T} \chi(g^{-1})\, Tr(\rho(g)\pi(v))$.
  - Show

$$\left| \sum_{g \in T} \underbrace{\chi(g^{-1}) K_{|T}(g, v)}_{F,\ |F|=1} \right| \leq 2\sqrt{q}.$$

- (2) *Geometric Weil rep'n.*
  - $F = f^{\mathcal{F}}$, $\mathcal{F} = \mathcal{L}_\chi \otimes \mathcal{K}_{|\mathbf{T}}$ - explicit line bundle on $\mathbf{T}$ with flat connection.
  - $\mathcal{F}$ has weight zero.

# Pseudo-Randomness – PROOF

- (1) *Linear algebra.*
  - $P_\chi = \frac{1}{\#T} \sum_{g \in T} \chi(g^{-1})\rho(g)$ – Projector onto $\mathcal{H}_\chi$.
  - $\left\langle \varphi_\chi, \pi(v)\varphi_\chi \right\rangle = Tr(P_\chi \pi(v)) = \frac{1}{q \pm 1} \sum_{g \in T} \chi(g^{-1})\, Tr(\rho(g)\pi(v))$.
  - Show

$$\left| \sum_{g \in T} \underbrace{\chi(g^{-1}) K_{|T}(g, v)}_{F,\ |F|=1} \right| \leq 2\sqrt{q}.$$

- (2) *Geometric Weil rep'n.*
  - $F = f^{\mathcal{F}}$, $\mathcal{F} = \mathcal{L}_\chi \otimes \mathcal{K}_{|\mathbf{T}}$ - explicit line bundle on $\mathbf{T}$ with flat connection.
  - $\mathcal{F}$ has weight zero.
  - $\mathcal{F}$ has non-trivial monodromy.

# Pseudo-Randomness – PROOF

- (3) *Topology.*

# Pseudo-Randomness – PROOF

- (3) *Topology.*

## Theorem (Deligne, Weil Conjectures II)

$\mathbf{X}/\mathbb{F}_q$, $\dim \mathbf{X} = 1$, $(\mathcal{F}, \bigtriangledown)$ *Weil line bundle with flat connection and weight zero. Then*

$$\left| \sum_{x \in \mathbf{X}} f^{\mathcal{F}}(x) \right| \leq c \cdot \sqrt{q},$$

*iff* $\mathcal{F}$ *has non-trivial monodromy.*

# Pseudo-Randomness – PROOF

- (3) *Topology.*

**Theorem (Deligne, Weil Conjectures II)**

$\mathbf{X}/\mathbb{F}_q$, $\dim \mathbf{X} = 1$, $(\mathcal{F}, \bigtriangledown)$ *Weil line bundle with flat connection and weight zero. Then*

$$\left| \sum_{x \in \mathbf{X}} f^{\mathcal{F}}(x) \right| \leq c \cdot \sqrt{q},$$

*iff* $\mathcal{F}$ *has non-trivial monodromy.*

- In our case $\mathcal{F}$ is explicit. Can compute $c = 2$. Done!

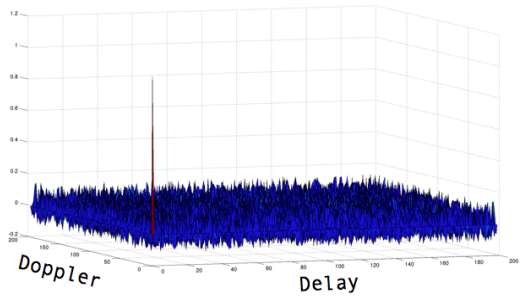



Figure: $\left\langle \varphi_\chi,\ \pi(\tau, \omega)\varphi_\chi \right\rangle$, $q = 199$.

# THANK YOU

Thank You!