Fast Fourier Transform: Why? How?

Shamgar Gurevich

UW Madison

May 13, 2012

Joint work with:

Ronny Hadani (Math, Austin)

Motivation:

- Discrete Fourier Transform

$$DFT = \frac{1}{\sqrt{N}} \left(e^{\frac{2\pi i}{N} \tau \cdot \omega} \right)_{0 \leq \tau, \omega \leq N-1}$$

Motivation:

- Discrete Fourier Transform

$$DFT = \frac{1}{\sqrt{N}} \left(e^{\frac{2\pi i}{N} \tau \cdot \omega} \right)_{0 \leq \tau, \omega \leq N-1}$$

- Compute:

$$\widehat{f} = DFT[f]; \qquad f = \begin{pmatrix} f(0) \\ . \\ . \\ . \\ f(N-1) \end{pmatrix}; \qquad \text{Fast!!}$$

Motivation:

- Discrete Fourier Transform

$$DFT = \frac{1}{\sqrt{N}} \left(e^{\frac{2\pi i}{N} \tau \cdot \omega} \right)_{0 \leq \tau, \omega \leq N-1}$$

- Compute:

$$\widehat{f} = DFT[f]; \qquad f = \begin{pmatrix} f(0) \\ . \\ . \\ . \\ f(N-1) \end{pmatrix}; \qquad \text{Fast!!}$$

- Cooley–Tukey (1965): $O(N \cdot \log(N))$ operations!

Solution:

(I) Heisenberg Group Representation

- $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ — Hilbert space of digital signals.

Solution:

(I) Heisenberg Group Representation

- $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ — Hilbert space of digital signals.
  - $f : \{0, ..., N-1\} \to \mathbb{C}$.

Solution:

(I) Heisenberg Group Representation

- $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ — Hilbert space of digital signals.
  - $f : \{0, ..., N - 1\} \to \mathbb{C}$.
- Basic operations

Solution:

(I) Heisenberg Group Representation

- $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ — Hilbert space of digital signals.
  - $f : \{0, ..., N-1\} \to \mathbb{C}$.
- Basic operations
  - Time shift: $\tau \in \mathbb{Z}_N$,

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

- $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ — Hilbert space of digital signals.
  - $f : \{0, ..., N-1\} \to \mathbb{C}$.
- Basic operations
  - Time shift: $\tau \in \mathbb{Z}_N$,

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

  - Frequency shift: $\omega \in \mathbb{Z}_N$,

$$M_\omega : \mathcal{H} \to \mathcal{H},$$
$$M_\omega[f](t) = e^{\frac{2\pi i}{N}\omega t} f(t).$$

Solution:

(I) Heisenberg Group Representation

- $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ — Hilbert space of digital signals.
  - $f : \{0, ..., N-1\} \to \mathbb{C}$.
- Basic operations
  - Time shift: $\tau \in \mathbb{Z}_N$,

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

  - Frequency shift: $\omega \in \mathbb{Z}_N$,

$$M_\omega : \mathcal{H} \to \mathcal{H},$$
$$M_\omega[f](t) = e^{\frac{2\pi i}{N}\omega t} f(t).$$

- Note:

$$M_\omega \circ L_\tau = e^{\frac{2\pi i}{N}\omega\tau} \cdot L_\tau \circ M_\omega \quad \text{—} \quad \textit{Heisenberg commutation relations}$$

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$

$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$

$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$

- Identity:

$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$

$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$

- Identity:

$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$

- Question. How to think on this?

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$

$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$

- Identity:

$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$

- Question. How to think on this?
- Answer. Heisenberg group:

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$

$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$

- Identity:

$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$

- Question. How to think on this?
- Answer. Heisenberg group:
  - $H = \underbrace{\mathbb{Z}_N \times \mathbb{Z}_N}_{V} \times \underbrace{\mathbb{Z}_N}_{Z};$

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$
$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$
- Identity:
$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$
- Question. How to think on this?
- Answer. Heisenberg group:
    - $H = \underbrace{\mathbb{Z}_N \times \mathbb{Z}_N}_{V} \times \underbrace{\mathbb{Z}_N}_{Z}$;
    - $(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\begin{vmatrix} v \\ v' \end{vmatrix})$;

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$
$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$
- Identity:
$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$
- Question. How to think on this?
- Answer. Heisenberg group:
  - $H = \underbrace{\mathbb{Z}_N \times \mathbb{Z}_N}_{V} \times \underbrace{\mathbb{Z}_N}_{Z}$;
  - $(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\begin{vmatrix} v \\ v' \end{vmatrix})$;
  - $(0, 0) \cdot (v, z) = (v, z) \cdot (0, 0) = (v, z)$;

Heisenberg Rep'n, cont.

- Combine: $\tau, \omega, z \in \mathbb{Z}_N$
$$\pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau.$$
- Identity:
$$\pi(\tau, \omega, z) \circ \pi(\tau', \omega', z') = \pi(\tau + \tau', \omega + \omega', z + z' + \frac{1}{2}\begin{vmatrix} \tau & \omega \\ \tau' & \omega' \end{vmatrix}).$$
- Question. How to think on this?
- Answer. Heisenberg group:
  - $H = \underbrace{\mathbb{Z}_N \times \mathbb{Z}_N}_{V} \times \underbrace{\mathbb{Z}_N}_{Z}$;
  - $(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\begin{vmatrix} v \\ v' \end{vmatrix})$;
  - $(0, 0) \cdot (v, z) = (v, z) \cdot (0, 0) = (v, z)$;
  - $(v, z) \cdot (-v, -z) = (-v, -z) \cdot (v, z) = (0, 0)$.

Heisenberg Rep'n, cont.

- Summary: Heisenberg Rep'n

$$\left\{ \begin{array}{c} \pi : H \longrightarrow GL(\mathcal{H}); \\ \pi(\tau,\omega,z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau+z\}}\cdot M_{\omega}\circ L_{\tau}; \\ \pi(h\cdot h') = \pi(h)\circ\pi(h') \text{ — homomorphism.} \end{array} \right.$$

Heisenberg Rep'n, cont.

- Summary: Heisenberg Rep'n

$$\begin{cases} \pi : H \longrightarrow GL(\mathcal{H}); \\ \pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau; \\ \pi(h \cdot h') = \pi(h) \circ \pi(h') \text{ — homomorphism.} \end{cases}$$

Definition

A representation of a group H on a complex vector space $\mathcal{H}$ is a homomorphism

$$\begin{aligned} \pi &: H \rightarrow GL(\mathcal{H}), \\ \pi(h \cdot h') &= \pi(h) \circ \pi(h'). \end{aligned}$$

Heisenberg Rep'n, cont.

- Summary: Heisenberg Rep'n

$$\begin{cases} \pi : H \longrightarrow GL(\mathcal{H}); \\ \pi(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau; \\ \pi(h \cdot h') = \pi(h) \circ \pi(h') \text{ — homomorphism.} \end{cases}$$

Definition

A representation of a group H on a complex vector space $\mathcal{H}$ is a homomorphism

$$\begin{aligned} \pi \quad &: \quad H \longrightarrow GL(\mathcal{H}), \\ \pi(h \cdot h') \quad &= \quad \pi(h) \circ \pi(h'). \end{aligned}$$

- Question. DFT ?

(II) Representation Theory

Definitions

We say that $(\pi_1, H, \mathcal{H}_1)$, $(\pi_2, H, \mathcal{H}_2)$ are equivalent, $\pi_1 \simeq \pi_2$, if

$$\exists\ \alpha : \mathcal{H}_1 \xrightarrow{\sim} \mathcal{H}_2 \ - \ \text{Intertwiner},$$

such that for every $h \in H$

$$\begin{array}{ccc} \mathcal{H}_1 & \xrightarrow{\pi_1(h)} & \mathcal{H}_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\ \mathcal{H}_2 & \xrightarrow{\pi_2(h)} & \mathcal{H}_2 \end{array}$$

i.e., $\alpha \circ \pi_1(h) = \pi_2(h) \circ \alpha$.

(II) Representation Theory

Definitions

We say that $(\pi_1, H, \mathcal{H}_1)$, $(\pi_2, H, \mathcal{H}_2)$ are equivalent, $\pi_1 \simeq \pi_2$, if

$$\exists\ \alpha : \mathcal{H}_1 \widetilde{\rightarrow} \mathcal{H}_2 \ - \ \text{Intertwiner},$$

such that for every $h \in H$

$$\begin{array}{ccc} \mathcal{H}_1 & \xrightarrow{\pi_1(h)} & \mathcal{H}_1 \\ \downarrow \alpha & & \downarrow \alpha \\ \mathcal{H}_2 & \xrightarrow{\pi_2(h)} & \mathcal{H}_2 \end{array}$$

i.e., $\alpha \circ \pi_1(h) = \pi_2(h) \circ \alpha$.

- Example: *DFT* is an intertwiner!

Rep'n Theory, cont.

- $H = V \times Z = \underbrace{\mathbb{Z}_N}_{T} \times \underbrace{\mathbb{Z}_N}_{W} \times \underbrace{\mathbb{Z}_N}_{Z}$

Rep'n Theory, cont.

- $H = V \times Z = \underbrace{\mathbb{Z}_N}_{T} \times \underbrace{\mathbb{Z}_N}_{W} \times \underbrace{\mathbb{Z}_N}_{Z}$
- Time representation: $\mathcal{H}_T = \mathbb{C}(T)$

$$\begin{cases} \pi_T : H \to GL(\mathcal{H}_T); \\ \pi_T(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau. \end{cases}$$

Rep'n Theory, cont.

- $H = V \times Z = \underbrace{\mathbb{Z}_N}_{T} \times \underbrace{\mathbb{Z}_N}_{W} \times \underbrace{\mathbb{Z}_N}_{Z}$
- Time representation: $\mathcal{H}_T = \mathbb{C}(T)$

$$\begin{cases} \pi_T : H \to GL(\mathcal{H}_T); \\ \pi_T(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau. \end{cases}$$

- Frequency representation: $\mathcal{H}_W = \mathbb{C}(W)$

$$\begin{cases} \pi_W : H \to GL(\mathcal{H}_W); \\ \pi_W(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{-\frac{1}{2}\omega\tau + z\}} \cdot M_\tau \circ L_{-\omega}. \end{cases}$$

Rep'n Theory, cont.

- $H = V \times Z = \underbrace{\mathbb{Z}_N}_{T} \times \underbrace{\mathbb{Z}_N}_{W} \times \underbrace{\mathbb{Z}_N}_{Z}$
- Time representation: $\mathcal{H}_T = \mathbb{C}(T)$

$$\begin{cases} \pi_T : H \to GL(\mathcal{H}_T); \\ \pi_T(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{\frac{1}{2}\omega\tau + z\}} \cdot M_\omega \circ L_\tau. \end{cases}$$

- Frequency representation: $\mathcal{H}_W = \mathbb{C}(W)$

$$\begin{cases} \pi_W : H \to GL(\mathcal{H}_W); \\ \pi_W(\tau, \omega, z) = e^{\frac{2\pi i}{N}\{-\frac{1}{2}\omega\tau + z\}} \cdot M_\tau \circ L_{-\omega}. \end{cases}$$

- Fact:

$$DFT \circ \pi_T(h) = \pi_W(h) \circ DFT,$$

where

$$DFT[f](w) = \frac{1}{\sqrt{N}} \sum_{t \in \mathbb{Z}_N} f(t) e^{\frac{2\pi i}{N} wt}.$$

(III) FFT Algorithm

- Idea:

$$
\begin{tikzcd}
\mathcal{H}_T \arrow[r, "fast"] \arrow[d, "slow"', "DFT"] & \mathcal{H}^{\Lambda} \arrow[d, equal] \\
\mathcal{H}_W & \mathcal{H}^{\Lambda} \arrow[l, "fast"]
\end{tikzcd}
$$

(III) FFT Algorithm

- Idea:

$$
\begin{tikzcd}
\mathcal{H}_T \arrow[r, "fast"] \arrow[d, "slow"', "DFT"] & \mathcal{H}^{\Lambda} \arrow[d, equal] \\
\mathcal{H}_W & \mathcal{H}^{\Lambda} \arrow[l, "fast"]
\end{tikzcd}
$$

- More representation theory:

(III) FFT Algorithm

- Idea:

$$\begin{tikzcd} \mathcal{H}_T \arrow[r, "fast"] \arrow[d, "slow"', "DFT"] & \mathcal{H}^\Lambda \arrow[d, equal] \\ \mathcal{H}_W & \mathcal{H}^\Lambda \arrow[l, "fast"'] \end{tikzcd}$$

- More representation theory:

Definition

A rep'n $(\pi, H, \mathcal{H})$ is irreducible if

$$\nexists \;\; 0 \neq \mathcal{H}' \subsetneq \mathcal{H}$$

such that

$$\pi(h) \cdot \mathcal{H}' \subset \mathcal{H}', \quad \forall h \in H.$$

FFT Algorithm: more RT

Theorem (Stone–von Neumann)

If $(\pi_j, H, \mathcal{H}_j)$, $j = 1, 2$, are irreducible representations of the Heisenberg group $H = V \times Z$, with

$$\pi_j(z) = e^{\frac{2\pi i}{N} z} \cdot Id_{\mathcal{H}_j}, \ \forall z \in Z,$$

then $\pi_1 \simeq \pi_2$ are equivalent, i.e., $\exists\ \alpha : \mathcal{H}_1 \widetilde{\rightarrow} \mathcal{H}_2$ such that

$$\alpha \circ \pi_1(h) = \pi_2(h) \circ \alpha, \quad \forall h \in H. \tag{1}$$

FFT Algorithm: more RT

Theorem (Stone–von Neumann)

If $(\pi_j, H, \mathcal{H}_j)$, $j = 1, 2$, are irreducible representations of the Heisenberg group $H = V \times Z$, with

$$\pi_j(z) = e^{\frac{2\pi i}{N} z} \cdot Id_{\mathcal{H}_j}, \ \forall z \in Z,$$

then $\pi_1 \simeq \pi_2$ are equivalent, i.e., $\exists\ \alpha : \mathcal{H}_1 \widetilde{\rightarrow} \mathcal{H}_2$ such that

$$\alpha \circ \pi_1(h) = \pi_2(h) \circ \alpha, \quad \forall h \in H. \tag{1}$$

Theorem (Schur's lemma)

If $\pi_1 \simeq \pi_2$ equivalent irreducible representations, and if α, α' satisfy equation (1), then

$$\alpha = c \cdot \alpha', \quad \text{for some scalar } c.$$

FFT Algorithm: Models of Heisenberg Rep'n

Examples

(1) Time model: $V \supset T = \{(t, 0);\ t \in \mathbb{Z}_N\}$

$$\pi_T : H \to GL(\mathcal{H}_T).$$

(2) Frequency model: $V \supset W = \{(0, w);\ w \in \mathbb{Z}_N\}$

$$\pi_W : H \to GL(\mathcal{H}_W).$$

Corollary

$DFT : \mathcal{H}_T \to \mathcal{H}_W$ — unique (up to a scalar) intertwiner between π_T and π_W.

Examples

(3) W–invariant model:

Space:

$$\mathcal{H}^W = \left\{ \begin{array}{c} f : H \to \mathbb{C}, \\ f(w \cdot h) = f(h), \ \ \forall\ w \in W,\ h \in H, \\ f(z \cdot h) = e^{\frac{2\pi i}{N} z} \cdot f(h), \ \ \forall\ z \in Z,\ h \in H. \end{array} \right.$$

Action:

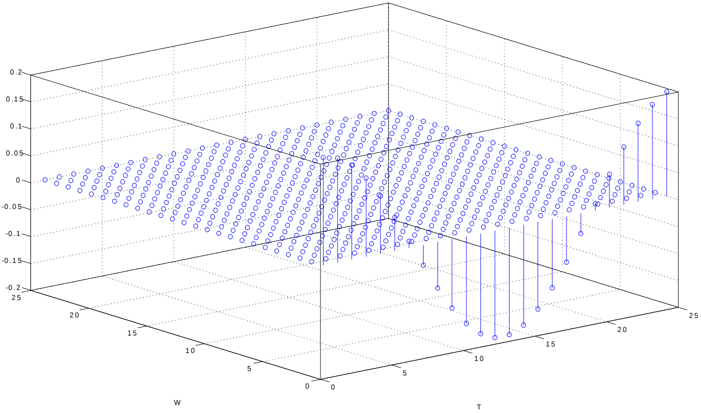
$$\left\{ \begin{array}{c} \pi^W : H \to GL(\mathcal{H}^W), \\ [\pi^W(h')f](h) = f(h \cdot h'). \end{array} \right.$$

- Remark: We have a natural identification $\mathcal{H}_T = \mathcal{H}^W$, given by

$$f \mapsto \widetilde{f}(wtz) = e^{\frac{2\pi i}{N} z} \cdot f(t).$$

Think on W-invariant functions as functions on T

A function $f(t)$ on $T = \{(t, 0, 0);\ t \in \mathbb{Z}/5^2\}$



FFT Algorithm: Models of Heisenberg Rep'n

Examples

(4) T–invariant model:

Space:

$$\mathcal{H}^T = \left\{ \begin{array}{c} g : H \to \mathbb{C}, \\ g(t \cdot h) = g(h), \quad \forall\ t \in T,\ h \in H, \\ g(z \cdot h) = e^{\frac{2\pi i}{N} z} \cdot g(h), \quad \forall\ z \in Z,\ h \in H. \end{array} \right.$$

Action:

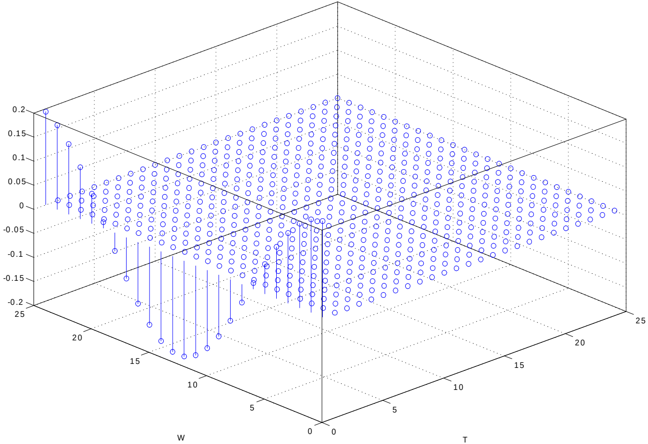
$$\left\{ \begin{array}{c} \pi^T : H \to GL(\mathcal{H}^T), \\ [\pi^T(h')g](h) = g(h \cdot h'). \end{array} \right.$$

- Remark: We have a natural identification $\mathcal{H}_W = \mathcal{H}^T$, given by

$$g \mapsto \widetilde{g}(twz) = e^{\frac{2\pi i}{N} z} \cdot g(w).$$

Think on T-invariant functions as functions on W

A function $g(w)$ on $W = \{(0, w, 0);\ \ w \in \mathbb{Z}/5^2\}$



FFT Algorithm: The Arithmetic Model

Examples

(5) Arithmetic model: $N = p^2$

Lagrangian: $V = \mathbb{Z}/p^2 \times \mathbb{Z}/p^2 \supset \Lambda = \{(p \cdot a,\ p \cdot b)\}$

Space:

$$\mathcal{H}^\Lambda = \left\{ \begin{array}{c} F : H \to \mathbb{C}, \\ F(\lambda \cdot h) = F(h), \ \ \forall\ \lambda \in \Lambda,\ \ h \in H, \\ F(z \cdot h) = e^{\frac{2\pi i}{N} z} \cdot F(h), \ \ \forall\ z \in Z,\ \ h \in H. \end{array} \right.$$

Action:

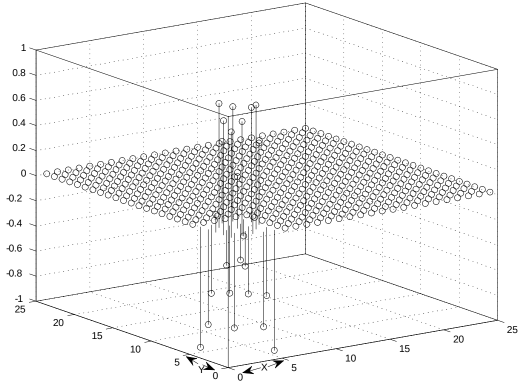
$$\pi^\Lambda : H \to GL(\mathcal{H}^\Lambda), \quad [\pi^\Lambda(h')F](h) = F(h \cdot h').$$

- Remark: We have a natural identification of $\mathcal{H}^\Lambda$ with functions $F(x, y)$ on $\{0, ..., p-1\} \times \{0, ..., p-1\}$

$$F \mapsto \widetilde{F}(\lambda \cdot (x, y, 0) \cdot z) = e^{\frac{2\pi i}{N} z} \cdot F(x, y),\ \lambda \in \Lambda.$$

Think on Lambda-invariant functions as functions on {0,...,p-1} x {0,...,p-1}

A function $F(x, y)$ on $(x, y) \in \{0, ..., 4\} \times \{0, ..., 4\}$, $p = 5$,



FFT: The Algorithm

- Algorithm: Case $N = p^2$

$$\begin{tikzcd} \mathcal{H}_T \arrow[r, "DFT", "p^4"'] \arrow[d, "saw"'] & \mathcal{H}_W \\ \mathcal{H}^W \arrow[d, "\sum_{\lambda \in \Lambda} f(\lambda h)"', "?"] & \mathcal{H}^T \arrow[u, "saw"'] \\ \mathcal{H}^\Lambda \arrow[r, equal] & \mathcal{H}^\Lambda \arrow[u, "?", "\sum_{t \in T} F(tw)"'] \end{tikzcd}$$

- Algorithm: Case $N = p^2$

$$\begin{tikzcd}
\mathcal{H}_T \arrow[r, "DFT"', "p^4"] \arrow[d, "saw"'] & \mathcal{H}_W \\
\mathcal{H}^W \arrow[d, "\sum_{\lambda\in\Lambda} f(\lambda h)"', "?"] & \mathcal{H}^T \arrow[u, "saw"'] \\
\mathcal{H}^\Lambda \arrow[r, equal] & \mathcal{H}^\Lambda \arrow[u, "?", "\sum_{t\in T} F(tw)"']
\end{tikzcd}$$

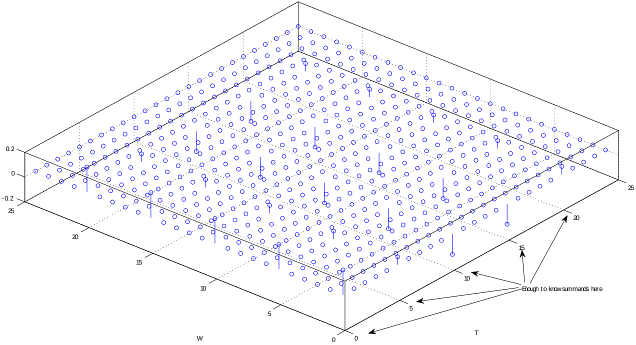
- Observation **(the saving!)**: For $f \in \mathcal{H}^W$, if $\lambda, \lambda' \in \Lambda$ differ by an element of W, i.e., $\lambda = w\lambda'$, then

$$f(\lambda h) = f(w\lambda' h) = f(\lambda' h), \quad \forall h \in H.$$

FFT Algorithms: The Summands

So for a fixed h it is enough to know the summands $f(\lambda h)$, in the transform, only for $\lambda \in \Lambda/[\Lambda \cap W] = \{(0,0), (p,0), ..., ((p-1)p, 0)\}$.

- Example for $p = 5$



FFT Algorithm: The Saving

- So we have

$$\sum_{\lambda \in \Lambda} f(\lambda h) = \sum_{\lambda \in \Lambda / [\Lambda \cap W]} f(\lambda h) \cdot \#(\Lambda \cap W).$$

Only $p = p^2/p = \#(\Lambda / [\Lambda \cap W])$ summands !!!.

FFT Algorithm: The Saving

- So we have

$$\sum_{\lambda\in\Lambda} f(\lambda h) = \sum_{\lambda\in\Lambda/[\Lambda\cap W]} f(\lambda h)\cdot\#(\Lambda\cap W).$$

  Only $p = p^2/p = \#(\Lambda/[\Lambda\cap W])$ summands !!!.
- Complexity of the algorithm

$$\underbrace{p^2}_{\text{values of h}} \cdot \underbrace{p}_{\text{summands}} + \underbrace{p^2\cdot p}_{\text{second operator}} = p\cdot p^2\cdot(1+1) = \underbrace{p}_{\text{constant}} \cdot N\cdot\log(N).$$

FFT Algorithm: Schur's lemma

Denote the intertwiners by

$$FFT^{\Lambda,W} : \mathcal{H}^{W} \rightarrow \mathcal{H}^{\Lambda}, \text{ and } FFT^{T,\Lambda} : \mathcal{H}^{\Lambda} \rightarrow \mathcal{H}^{T}.$$

- Why

$$DFT = FFT^{T,\Lambda} \circ FFT^{\Lambda,W} \ ? \tag{2}$$

FFT Algorithm: Schur's lemma

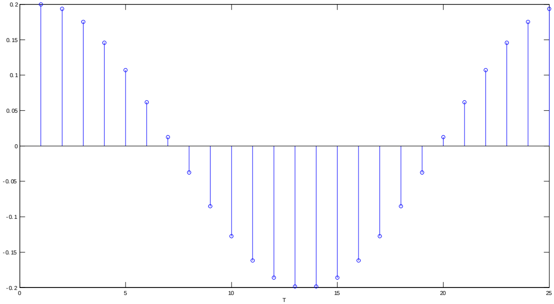
Denote the intertwiners by

$$FFT^{\Lambda,W} : \mathcal{H}^W \rightarrow \mathcal{H}^\Lambda, \text{ and } FFT^{T,\Lambda} : \mathcal{H}^\Lambda \rightarrow \mathcal{H}^T.$$

- Why
$$DFT = FFT^{T,\Lambda} \circ FFT^{\Lambda,W} \text{ ?} \tag{2}$$
- In fact by Schur's lemma: Both sides of (2) intertwine π^W and π^T, so
$$DFT = c \cdot FFT^{T,\Lambda} \circ FFT^{\Lambda,W}$$
for some scalar c. Easy to compute $c = \frac{1}{p}$.

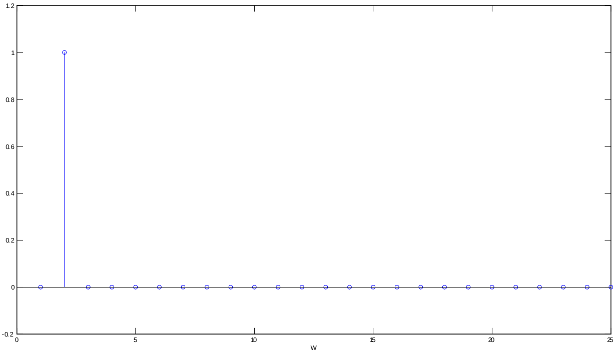
Numerics for n=25

Start with the exponent function $f(t) = e^{\frac{2\pi i}{25}t}/5$ on $T = \mathbb{Z}/25$



Numerics for n=25 : FFT(f)

Apply FFT and get $g(w) = FFT[f](w)$ on $W = \mathbb{Z}/25$



Indeed this is $g(w) = \delta_1(w)$.

FFT Algorithm: General

- $N = p^k$, $k \geq 1$

FFT Algorithm: General

- $N = p^k$, $k \geq 1$
- $V = \mathbb{Z}/p^k \times \mathbb{Z}/p^k$

FFT Algorithm: General

- $N = p^k$, $k \geq 1$
- $V = \mathbb{Z}/p^k \times \mathbb{Z}/p^k$
- Good Lagrangian sequence ("interpolating" W and T)

$$\Lambda_\bullet : \qquad \Lambda_j = \{(p^{k-j} \cdot a, p^j \cdot b)\}, \qquad j = 0, ..., k,$$

with LARGE intersections

$$\# \, \Lambda_j \cap \Lambda_{j+1} = p^{k-1}.$$

FFT Algorithm: General

- $N = p^k$, $k \geq 1$
- $V = \mathbb{Z}/p^k \times \mathbb{Z}/p^k$
- Good Lagrangian sequence ("interpolating" W and T)

$$\Lambda_\bullet : \qquad \Lambda_j = \{(p^{k-j} \cdot a, p^j \cdot b)\}, \qquad j = 0, ..., k,$$

with LARGE intersections

$$\# \Lambda_j \cap \Lambda_{j+1} = p^{k-1}.$$

- FFT Algorithm

$$\mathcal{H}^W \overset{FFT^{\Lambda_1,W}}{\rightarrow} \mathcal{H}^{\Lambda_1} \rightarrow \cdots \rightarrow \mathcal{H}^{\Lambda_{k-1}} \overset{FFT^{T,\Lambda_k}}{\rightarrow} \mathcal{H}^T$$

$$DFT = \frac{1}{\sqrt{p^k}} \cdot FFT^{T,\Lambda_{k-1}} \circ \cdots \circ FFT^{\Lambda_1,W},$$

with complexity

$$\underbrace{p^k}_{\text{values of } h} \cdot \{ \underbrace{k}_{k \text{ operators}} \cdot \underbrace{\# \Lambda_{j+1}/(\Lambda_j \cap \Lambda_{j+1})}_{p \text{ summands}} \} = \underbrace{p}_{\text{constant}} \underbrace{\cdot p^k}_{N} \cdot \underbrace{\log(p^k)}_{\log(N)}.$$

- Conclusion

$$\Lambda_{\bullet} \Longrightarrow \text{Cooley–Tukey } FFT$$

Conclusion and Open Problem

- Conclusion

$$\Lambda_{\bullet} \Longrightarrow \text{Cooley–Tukey } FFT$$

- Open Problem

$$\Lambda_{\text{new}} \Longrightarrow \text{new } \; FFT\text{!!!}$$

THANK YOU

Ronny