The Discrete Fourier Transform

William Hart

04–July–2010

The Fourier Transform

Given $f : \mathbb{R} \to \mathbb{C}$ continuous, absolutely integrable, the Fourier transform is

- $$\hat{f}(s) = \int_{-\infty}^{\infty} f(x) e^{-2\pi\,\mathrm{i}xs}\,\mathrm{dx} \quad \text{for} \quad s \in \mathbb{R}.$$

The Fourier Transform

Given $f : \mathbb{R} \to \mathbb{C}$ continuous, absolutely integrable, the Fourier transform is

- $$\hat{f}(s) = \int_{-\infty}^{\infty} f(x) e^{-2\pi\,\mathrm{i}xs}\ \mathrm{d}x \quad \text{for} \quad s \in \mathbb{R}.$$

- Can recover f from the Fourier Inversion Formula

$$f(x) = \int_{-\infty}^{\infty} e^{2\pi\,\mathrm{i}xs} \hat{f}(s)\ \mathrm{d}s\,.$$

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups
- Abelian groups for now

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups
- Abelian groups for now

Some standard examples:

- Finite additive groups with the discrete topology, e.g. $\mathbb{Z}/n\mathbb{Z}$

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups
- Abelian groups for now

Some standard examples:

- Finite additive groups with the discrete topology, e.g. $\mathbb{Z}/n\mathbb{Z}$
- Tori, $(\mathbb{R}/\mathbb{Z})^d$ with the standard topology

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups
- Abelian groups for now

Some standard examples:

- Finite additive groups with the discrete topology, e.g. $\mathbb{Z}/n\mathbb{Z}$
- Tori, $(\mathbb{R}/\mathbb{Z})^d$ with the standard topology
- Euclidean space $\mathbb{R}^d$ with standard topology

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups
- Abelian groups for now

Some standard examples:

- Finite additive groups with the discrete topology, e.g. $\mathbb{Z}/n\mathbb{Z}$
- Tori, $(\mathbb{R}/\mathbb{Z})^d$ with the standard topology
- Euclidean space $\mathbb{R}^d$ with standard topology
- Finitely generated additive groups with the discrete topology, e.g. $\mathbb{Z}^d$

Locally Compact Abelian Groups

More generally, allow complex valued functions on group G

- Restrict to locally compact, Hausdorff topological groups
- Abelian groups for now

Some standard examples:

- Finite additive groups with the discrete topology, e.g. $\mathbb{Z}/n\mathbb{Z}$
- Tori, $(\mathbb{R}/\mathbb{Z})^d$ with the standard topology
- Euclidean space $\mathbb{R}^d$ with standard topology
- Finitely generated additive groups with the discrete topology, e.g. $\mathbb{Z}^d$
- Adele ring with the usual restricted topology

Haar Measure

Require:

- Haar measure is translation invariant:

Haar Measure

Require:

- Haar measure is translation invariant:
- $$\mu(U) = \mu(U + g)$$

  for all $g \in G$, subsets $U \subseteq G$ generated from compact subsets by countable unions and complements.

Haar Measure

Require:

- Haar measure is translation invariant:
- $$\mu(U) = \mu(U + g)$$

  for all $g \in G$, subsets $U \subseteq G$ generated from compact subsets by countable unions and complements.
- Haar measure of compact sets is finite

Haar Measure

Require:

- Haar measure is translation invariant:
- $$\mu(U) = \mu(U + g)$$

  for all $g \in G$, subsets $U \subseteq G$ generated from compact subsets by countable unions and complements.
- Haar measure of compact sets is finite

Theorem (Weil) All locally compact abelian (LCA) groups have a non-trivial Haar measure

Haar Measure

Require:

- Haar measure is translation invariant:
-
$$\mu(U) = \mu(U + g)$$
  for all $g \in G$, subsets $U \subseteq G$ generated from compact subsets by countable unions and complements.
- Haar measure of compact sets is finite

Theorem (Weil) All locally compact abelian (LCA) groups have a non-trivial Haar measure

- For the discrete examples, Haar measure is the counting measure

Haar Measure

Require:

- Haar measure is translation invariant:
- $$\mu(U) = \mu(U + g)$$

  for all $g \in G$, subsets $U \subseteq G$ generated from compact subsets by countable unions and complements.
- Haar measure of compact sets is finite

Theorem (Weil) All locally compact abelian (LCA) groups have a non-trivial Haar measure

- For the discrete examples, Haar measure is the counting measure
- For other (non-adele) examples can construct Haar measure from Lebesgue measure

Fourier Transform on an LCA

Haar measure on an LCA unique up to multiplication by scalar.

Fourier Transform on an LCA

Haar measure on an LCA unique up to multiplication by scalar.

- The Fourier Transform for an absolutely integrable function f is:

$$\hat{f}(s) = \int_G f(x) e^{-2\pi \,\mathrm{i} s \cdot x} d\mu(x).$$

Fourier Transform on an LCA

Haar measure on an LCA unique up to multiplication by scalar.

- The Fourier Transform for an absolutely integrable function f is:
$$\hat{f}(s) = \int_G f(x)e^{-2\pi \,\mathrm{i} s \cdot x} d\mu(x).$$
- $\hat{f} : \hat{G} \to \mathbb{C}$ where $\hat{G}$ is the Pontryagin dual of G

Fourier Transform on an LCA

Haar measure on an LCA unique up to multiplication by scalar.

- The Fourier Transform for an absolutely integrable function f is:
$$\hat{f}(s) = \int_G f(x) e^{-2\pi \, \mathrm{i} s \cdot x} d\mu(x).$$
- $\hat{f} : \hat{G} \to \mathbb{C}$ where $\hat{G}$ is the Pontryagin dual of G
- $\hat{G}$ is space of additive characters of G (continuous additive homomorphisms) $s : G \to \mathbb{R}/\mathbb{Z}$

Discrete Fourier Transform

We are interested in G a finite abelian group with discrete topology

- The Discrete Fourier Transform

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

Discrete Fourier Transform

We are interested in G a finite abelian group with discrete topology

- The Discrete Fourier Transform

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

- E.g. $G = \mathbb{Z}/n\mathbb{Z}$, functions f on G are polynomials in $\mathbb{C}[x]/(x^n - 1)$.

Discrete Fourier Transform

We are interested in G a finite abelian group with discrete topology

- The Discrete Fourier Transform

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

- E.g. $G = \mathbb{Z}/n\mathbb{Z}$, functions f on G are polynomials in $\mathbb{C}[x]/(x^n - 1)$.
- let $\zeta_j(g) = \exp\left(\frac{2\pi \, \mathrm{ijg}}{n}\right)$ for $g \in \mathbb{Z}/\,\mathrm{n}\mathbb{Z}$

Discrete Fourier Transform

We are interested in G a finite abelian group with discrete topology

- The Discrete Fourier Transform

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

- E.g. $G = \mathbb{Z}/n\mathbb{Z}$, functions f on G are polynomials in $\mathbb{C}[x]/(x^n - 1)$.
- let $\zeta_j(g) = \exp\left(\frac{2\pi\,\mathrm{ijg}}{n}\right)$ for $g \in \mathbb{Z}/\,\mathrm{n}\mathbb{Z}$
- DFT of $f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ at ζ_j is

$$\hat{f}_j = \hat{f}(\zeta_j) = \sum_{m=0}^{n-1} a_n e^{-2\pi\,\mathrm{ijm}\,/n}.$$

Generalisation

- For finite abelian group G of exponent n ($\mathrm{nG} = 0$) can replace $\mathbb{C}$ with commutative ring K containing primitive n-th root of unity ζ (with some additional conditions).

Generalisation

- For finite abelian group G of exponent n (nG $= 0$) can replace $\mathbb{C}$ with commutative ring K containing primitive n-th root of unity ζ (with some additional conditions).
- DFT is homomorphism $K[G] \to K^{\hat{G}}$ defined by $\hat{a}(\hat{g}) = \sum_{g \in G} a(g) < g, \hat{g} >$ for choice of non-degenerate form $< g, \hat{g} >$: $G \times \hat{G} \to < \zeta >$.

Generalisation

- For finite abelian group G of exponent n (nG $= 0$) can replace $\mathbb{C}$ with commutative ring K containing primitive n-th root of unity ζ (with some additional conditions).
- DFT is homomorphism $K[G] \to K^{\hat{G}}$ defined by $\hat{a}(\hat{g}) = \sum_{g \in G} a(g) < g, \hat{g} >$ for choice of non-degenerate form $< g, \hat{g} >$: $G \times \hat{G} \to < \zeta >$.
- Fourier inversion theorem (conditions)

$$(\#G)^{-1}\widehat{\hat{a}}(-g) = a(g) \quad \text{for} \quad a \in K[G].$$

Examples

- (Number Theoretic Transform)
  $K = \mathbb{Z}/p\mathbb{Z}$ for prime p, ζ primitive n-th root of unity in K

Examples

- (Number Theoretic Transform)
  $K = \mathbb{Z}/p\mathbb{Z}$ for prime p, ζ primitive n-th root of unity in K
- (Fermat Ring)
  $R = \mathbb{Z}/p\mathbb{Z}$ for $p = 2^{a2^K} + 1$ (not necessarily prime), $a, K \in \mathbb{N}$.
  2^a is a primitive 2^{K+1}-th root of unity in R.

Examples

- (Number Theoretic Transform)
  $K = \mathbb{Z}/p\mathbb{Z}$ for prime p, ζ primitive n-th root of unity in K
- (Fermat Ring)
  $R = \mathbb{Z}/p\mathbb{Z}$ for $p = 2^{a2^K} + 1$ (not necessarily prime), $a, K \in \mathbb{N}$.
  2^a is a primitive 2^{K+1}-th root of unity in R.
- $S = \mathbb{Z}[x]/(x^{2^n} + 1)$

Examples

- (Number Theoretic Transform)
  $K = \mathbb{Z}/p\mathbb{Z}$ for prime p, ζ primitive n-th root of unity in K
- (Fermat Ring)
  $R = \mathbb{Z}/p\mathbb{Z}$ for $p = 2^{a2^K} + 1$ (not necessarily prime), $a, K \in \mathbb{N}$.
  2^a is a primitive 2^{K+1}-th root of unity in R.
- $S = \mathbb{Z}[x]/(x^{2^n} + 1)$
- (non-example) Mersenne Ring
  $R = \mathbb{Z}/p\mathbb{Z}$ for $p = 2^{2^K} - 1$

Convolution

- G an LCA with non-trivial Haar measure μ
  convolution of two absolutely integrable functions $f, g : G \to \mathbb{C}$ is defined by

$$f \star g(x) = \int_G f(y)g(x-y)d\mu(y).$$

Convolution

- G an LCA with non-trivial Haar measure μ
  convolution of two absolutely integrable functions $f, g : G \to \mathbb{C}$ is defined by
  $$f \star g(x) = \int_G f(y)g(x-y)d\mu(y).$$
- $$\widehat{f \star g}(s) = \hat{f}(s)\hat{g}(s),$$
  "Fourier Transform converts convolution into "pointwise" multiplication"

Convolution

- G an LCA with non-trivial Haar measure μ
  convolution of two absolutely integrable functions $f, g : G \to \mathbb{C}$ is defined by
  $$f \star g(x) = \int_G f(y)g(x-y)d\mu(y).$$
- $$\widehat{f \star g}(s) = \hat{f}(s)\hat{g}(s),$$
  "Fourier Transform converts convolution into "pointwise" multiplication"
- Retrieve convolution of f, g using inverse Fourier transform

Example

- $G = \mathbb{Z}/n\mathbb{Z}$, for $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ and $g = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in \mathbb{C}[x]/(x^n - 1)$, have

$$(f \star g)_j = \sum_{m=0}^{n-1} a_m b_{j-m \pmod{n}}.$$

Example

- $G = \mathbb{Z}/n\mathbb{Z}$, for $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ and $g = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in \mathbb{C}[x]/(x^n - 1)$, have

$$(f \star g)_j = \sum_{m=0}^{n-1} a_m b_{j-m \pmod{n}}.$$

- Here convolution is multiplication of polynomials modulo $x^n - 1$.

Fast Fourier Transforms

- DFT can be computed naively in $O(n^2)$ steps

Fast Fourier Transforms

- DFT can be computed naively in $O(n^2)$ steps
- Convolution can be computed naively in $O(n^2)$ steps

Fast Fourier Transforms

- DFT can be computed naively in $O(n^2)$ steps
- Convolution can be computed naively in $O(n^2)$ steps
- Suppose G has a increasing subgroup series

$$0 = G_0 \subset G_1 \subset \ldots \subset G_K = G$$

Fast Fourier Transforms

- DFT can be computed naively in $O(n^2)$ steps
- Convolution can be computed naively in $O(n^2)$ steps
- Suppose G has a increasing subgroup series

$$0 = G_0 \subset G_1 \subset \ldots \subset G_K = G$$

- Recall that

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

Fast Fourier Transforms

- DFT can be computed naively in $O(n^2)$ steps
- Convolution can be computed naively in $O(n^2)$ steps
- Suppose G has a increasing subgroup series

$$0 = G_0 \subset G_1 \subset \ldots \subset G_K = G$$

- Recall that

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

- Write every $g \in G$ as sum of element in G_{K-1} and element from fixed set of representatives for G_K / G_{K-1}.

Fast Fourier Transforms

- DFT can be computed naively in $O(n^2)$ steps
- Convolution can be computed naively in $O(n^2)$ steps
- Suppose G has a increasing subgroup series

$$0 = G_0 \subset G_1 \subset \ldots \subset G_K = G$$

- Recall that

$$\hat{f}(\zeta) = \sum_{g \in G} \zeta(g) f(g).$$

- Write every $g \in G$ as sum of element in G_{K-1} and element from fixed set of representatives for G_K / G_{K-1}.
- For $\mathbb{Z}/2^n\mathbb{Z}$ get Cooley-Tukey FFT, complexity $O(n \log n)$

Rader/Winograd FFT

- G of prime order, work with the multiplicative group of invertible elements modulo p, order $p - 1$.

Rader/Winograd FFT

- G of prime order, work with the multiplicative group of invertible elements modulo p, order $p-1$.
- g primitive root mod p, compute

$$\hat{f}_0 = \sum_{m=0}^{p-1} a_m \quad \text{and} \quad \hat{f}_{g^{-j}} = a_0 + \sum_{m=0}^{p-2} a_{g^m} e^{-\frac{2\pi i}{p} g^{-(j-m)}}.$$

Rader/Winograd FFT

- G of prime order, work with the multiplicative group of invertible elements modulo p, order $p-1$.
- g primitive root mod p, compute

$$\hat{f}_0 = \sum_{m=0}^{p-1} a_m \quad \text{and} \quad \hat{f}_{g^{-j}} = a_0 + \sum_{m=0}^{p-2} a_{g^m} e^{-\frac{2\pi i}{p} g^{-(j-m)}}.$$

- Sum is cyclic convolution of two length $p-1$ vectors

Rader/Winograd FFT

- G of prime order, work with the multiplicative group of invertible elements modulo p, order $p-1$.
- g primitive root mod p, compute

$$\hat{f}_0 = \sum_{m=0}^{p-1} a_m \quad \text{and} \quad \hat{f}_{g^{-j}} = a_0 + \sum_{m=0}^{p-2} a_{g^m} e^{-\frac{2\pi i}{p} g^{-(j-m)}}.$$

- Sum is cyclic convolution of two length $p-1$ vectors
- Compute using zero padded FFTs or recurse on Rader's FFT

Rader/Winograd FFT

- G of prime order, work with the multiplicative group of invertible elements modulo p, order $p-1$.
- g primitive root mod p, compute

$$\hat{f}_0 = \sum_{m=0}^{p-1} a_m \quad \text{and} \quad \hat{f}_{g^{-j}} = a_0 + \sum_{m=0}^{p-2} a_{g^m} e^{-\frac{2\pi i}{p} g^{-(j-m)}}.$$

- Sum is cyclic convolution of two length $p-1$ vectors
- Compute using zero padded FFTs or recurse on Rader's FFT
- Winograd generalised to prime powers

Rader/Winograd FFT

- G of prime order, work with the multiplicative group of invertible elements modulo p, order $p-1$.
- g primitive root mod p, compute

$$\hat{f}_0 = \sum_{m=0}^{p-1} a_m \quad \text{and} \quad \hat{f}_{g^{-j}} = a_0 + \sum_{m=0}^{p-2} a_{g^m} e^{-\frac{2\pi i}{p} g^{-(j-m)}}.$$

- Sum is cyclic convolution of two length $p-1$ vectors
- Compute using zero padded FFTs or recurse on Rader's FFT
- Winograd generalised to prime powers
- Cost somewhere between $O(n^2)$ and $O(n \log n)$ for recursive Rader FFT

Non-abelian DFTs

Can do DFTs for non-abelian finite groups G

- Replace characters with group representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$

Non-abelian DFTs

Can do DFTs for non-abelian finite groups G

- Replace characters with group representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$
- Two reps. equivalent if same up to change of basis

Non-abelian DFTs

Can do DFTs for non-abelian finite groups G

- Replace characters with group representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$
- Two reps. equivalent if same up to change of basis
- Complex reps. irreducible if not the direct sum of smaller reps

Non-abelian DFTs

Can do DFTs for non-abelian finite groups G

- Replace characters with group representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$
- Two reps. equivalent if same up to change of basis
- Complex reps. irreducible if not the direct sum of smaller reps
- As many inequiv. irred. reps. as conjugacy classes in G

Non-abelian DFTs

Can do DFTs for non-abelian finite groups G

- Replace characters with group representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$
- Two reps. equivalent if same up to change of basis
- Complex reps. irreducible if not the direct sum of smaller reps
- As many inequiv. irred. reps. as conjugacy classes in G
- If f is a $\mathbb{C}$-valued fn. on a finite group G then a Fourier transform of f is a set of matrix sums

$$\hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g),$$

one for each ρ in a complete set $\mathcal{R}$ of inequiv. irred. reps.

Wedderburn's isomorphism

One can also use Wedderburn's Theorem for the group algebra $\mathbb{C}[G]$.

- Fourier transform is an isomorphism

$$B = \oplus_{m=1}^{r} B_m : \mathbb{C}[G] \to \oplus_{m=1}^{r} \mathbb{C}^{b_m \times b_m}$$

  to algebra of block diagonal matrices, with r the number of classes of inequiv. irred. reps. of $\mathbb{C}[G]$

Wedderburn's isomorphism

One can also use Wedderburn's Theorem for the group algebra $\mathbb{C}[G]$.

- Fourier transform is an isomorphism

  $$B = \oplus_{m=1}^{r} B_m : \mathbb{C}[G] \to \oplus_{m=1}^{r} \mathbb{C}^{b_m \times b_m}$$

  to algebra of block diagonal matrices, with r the number of classes of inequiv. irred. reps. of $\mathbb{C}[G]$
- Fourier inversion formula, for $\mathcal{R}$ is

  $$f(g) = \frac{1}{\#G} \sum_{\rho \in \mathcal{R}} \dim(\rho)\, \mathrm{Tr}(\hat{f}(\rho)\rho(g^{-1})),$$

  where $\mathrm{Tr}(M)$ is trace of M

Wedderburn's isomorphism

One can also use Wedderburn's Theorem for the group algebra $\mathbb{C}[G]$.

- Fourier transform is an isomorphism

$$B = \oplus_{m=1}^{r} B_m : \mathbb{C}[G] \to \oplus_{m=1}^{r} \mathbb{C}^{b_m \times b_m}$$

  to algebra of block diagonal matrices, with r the number of classes of inequiv. irred. reps. of $\mathbb{C}[G]$
- Fourier inversion formula, for $\mathcal{R}$ is

$$f(g) = \frac{1}{\#G} \sum_{\rho \in \mathcal{R}} \dim(\rho) \operatorname{Tr}(\hat{f}(\rho)\rho(g^{-1})),$$

  where $\operatorname{Tr}(M)$ is trace of M
- FFT for G requires subgroup series and notion of H-adapted reps. for subgroup H of G, etc.

Wedderburn's isomorphism

One can also use Wedderburn's Theorem for the group algebra $\mathbb{C}[G]$.

- Fourier transform is an isomorphism

$$B = \oplus_{m=1}^{r} B_m : \mathbb{C}[G] \to \oplus_{m=1}^{r} \mathbb{C}^{b_m \times b_m}$$

  to algebra of block diagonal matrices, with r the number of classes of inequiv. irred. reps. of $\mathbb{C}[G]$
- Fourier inversion formula, for $\mathcal{R}$ is

$$f(g) = \frac{1}{\#G} \sum_{\rho \in \mathcal{R}} \dim(\rho) \operatorname{Tr}(\hat{f}(\rho)\rho(g^{-1})),$$

  where $\operatorname{Tr}(M)$ is trace of M
- FFT for G requires subgroup series and notion of H-adapted reps. for subgroup H of G, etc.
- Set $\mathcal{R}$ of reps. of G is H-adapted if when restricted to H they can be constructed as direct products of fixed set of inequiv. irred. reps. of H

Applications of DFT

- Fast Fourier Transform $G = \mathbb{Z}/2^n\mathbb{Z}$, used in fast polynomial and large integer multiplication

Applications of DFT

- Fast Fourier Transform $G = \mathbb{Z}/2^n\mathbb{Z}$, used in fast polynomial and large integer multiplication
- Middle product for use in division algorithms

Applications of DFT

- Fast Fourier Transform $G = \mathbb{Z}/2^n\mathbb{Z}$, used in fast polynomial and large integer multiplication
- Middle product for use in division algorithms
- Number Theoretic Transform $G = \mathbb{Z}/p\mathbb{Z}$, p odd prime

Applications of DFT

- Fast Fourier Transform $G = \mathbb{Z}/2^n\mathbb{Z}$, used in fast polynomial and large integer multiplication
- Middle product for use in division algorithms
- Number Theoretic Transform $G = \mathbb{Z}/p\mathbb{Z}$, p odd prime
- Multidimensional FFTs, $G = (\mathbb{Z}/2^n\mathbb{Z})^r$ for multivariate polynomial arithmetic

Applications of DFT

- Fast Fourier Transform $G = \mathbb{Z}/2^n\mathbb{Z}$, used in fast polynomial and large integer multiplication
- Middle product for use in division algorithms
- Number Theoretic Transform $G = \mathbb{Z}/p\mathbb{Z}$, p odd prime
- Multidimensional FFTs, $G = (\mathbb{Z}/2^n\mathbb{Z})^r$ for multivariate polynomial arithmetic
- Gauss Sum

$$G(a;p) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) e^{2\pi \,\mathrm{iaj}\,/p}$$

for p an odd prime, is a DFT

Applications of DFT

- Fast Fourier Transform $G = \mathbb{Z}/2^n\mathbb{Z}$, used in fast polynomial and large integer multiplication
- Middle product for use in division algorithms
- Number Theoretic Transform $G = \mathbb{Z}/p\mathbb{Z}$, p odd prime
- Multidimensional FFTs, $G = (\mathbb{Z}/2^n\mathbb{Z})^r$ for multivariate polynomial arithmetic
- Gauss Sum
$$G(a;p) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) e^{2\pi\,\mathrm{iaj}\,/p}$$
for p an odd prime, is a DFT
- $G(a;p) = \left(\frac{a}{p}\right) i^{(p-1)/2}\sqrt{p}$, so Legendre symbol is essentially its own DFT

Questions

- What other applications exist for DFT for abelian and non-abelian groups?

Questions

- What other applications exist for DFT for abelian and non-abelian groups?
- What does Sage implement in the way of DFTs for abelian LCAs?

Questions

- What other applications exist for DFT for abelian and non-abelian groups?
- What does Sage implement in the way of DFTs for abelian LCAs?
- What does Sage implement in the way of DFTs for nonabelian LCHTGs?