The Discrete Fourier Transform

Joel Laity

October 3, 2017

1 The space $\ell^2(G)$

We are interested in analysing functions of the form $f : G \to \mathbb{C}$ where G is some finite abelian group. Most people only care about the case where G is the cyclic group $G = \mathbb{Z}_n$ and this is the example the reader should keep in mind when reading the theorems. The following definition gives us some notation to talk about the space of these functions.

Definition 1. *Let G be a finite, abelian group. Define $\ell^2(G)$ to be the set of all functions $f : G \to \mathbb{C}$. In symbols,*

$$\ell^2(G) = \{f : G \to \mathbb{C}\}.$$

The set $\ell^2(G)$ is a vector space over $\mathbb{C}$ with the usual addition and scalar multiplication of functions. It comes with an inner product

$$\langle f, g\rangle = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{g(x)}.$$

In fact, $\ell^2(G)$ is a Hilbert space; i.e., the inner product satisfies the following properties:

1. $\langle f, g\rangle = \overline{\langle g, f\rangle}$,
2. $\langle f, g\rangle$ is linear in f and conjugate linear in g,
3. $\langle f, f\rangle \geq 0$,
4. $\langle f, f\rangle = 0$ if and only if $f = 0$,

and the space is a compete metric space where the metric is given by the norm induced by the inner product

$$\|f\|_2 = \sqrt{\langle f, f\rangle}.$$

Proposition 1. *Let G be a finite, abelian group. Then*

$$\dim \ell^2(G) = |G|.$$

Proof. For all $x \in G$ define $\delta_x : G \to \mathbb{C}$ by $\delta_x(y) = 1$ if $x = y$ and $\delta_x(y) = 0$ if $x \neq y$. Then the δ_x are linearly independent. For any $f \in \ell^2(G)$ we have $f = \sum_{x \in G} f(x)\delta_x$ thus the δ_x span $\ell^2(G)$. It follows that $\dim \ell^2(G) = |G|$. $\square$

We now define a way of multiplying two elements in our space.

Definition 2. *Let G be a finite, abelian group. Let $f, g \in \ell^2(G)$. Then the convolution of f and g is the function $f * g : G \to \mathbb{C}$ defined by*

$$(f * g)(x) = \frac{1}{|G|} \sum_{y \in G} f(y)g(x - y).$$

Proposition 2. *Let G be a finite, abelian group. Let $f, g, h \in \ell^2(G)$. Then*

1. *$f * g = g * f$ for all $f, g \in \ell^2(G)$,*
2. *$f * (g * h) = (f * g) * h$ for all $f, g \in \ell^2(G)$,*
3. *$f * (g + h) = f * g + f * h$ for all $f, g \in \ell^2(G)$,*
4. *$(af) * (bg) = (ab)(f * g)$ for all $f, g \in \ell^2(G)$ and $a, b \in \mathbb{C}$.*

Proposition 2 shows that the vector space $\ell^2(G)$ is an associative algebra where $*$ is the algebra multiplication.

The definition of convolution can seem a little mysterious at first. An alternative way of defining convolution would be to say it is a map $* : \ell^2(G) \times \ell^2(G) \to \ell^2(G)$ with properties 1-4 of Proposition 2 and

$$\delta_x * \delta_y = \delta_{x+y}$$

where $\delta_x : G \to \mathbb{C}$ is the usual delta function

$$\delta_x(z) = \begin{cases} 1 & \text{if } x = z, \\ 0 & \text{otherwise.} \end{cases}$$

This definition of convolution extends linearly to all of $\ell^2(G)$.

Remark 1 (The group algebra of G and $\ell^2(G)$ are isomorphic)**.** *Another way of viewing convolution is that it is multiplication in the group algebra of G.*

Recall the complex group algebra of a finite group G is a vector space with basis G, so an arbitrary element of the group algebra is a formal sum

$$\sum_{x \in G} \alpha_x x$$

where $\alpha_x \in \mathbb{C}$. The notation is confusing since we have been using additive notation for G, bear in mind that the sum here is a formal sum of linearly independent vectors.

The multiplication of the basis vectors in the group algebra is just the usual group operation and this extends linearly to define a multiplication on the group algebra. It's easy to verify that

$$\delta_x \mapsto x.$$

extends linearly to an (algebra) isomorphism between $\ell^2(G)$ and the group algebra of G. We can explicitly write this isomorphism as

$$f \mapsto \sum_{x \in G} f(x) x.$$

2 Characters

So far we have encountered the delta basis for $\ell^(G)$ which consists of all functions of the form

$$\delta_x(y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{otherwise.} \end{cases}$$

We will now define the *Fourier Basis*, $\widehat{G}$, which consists of all the *characters* (defined below) of G. This sections defines the Fourier Basis and proves that it is indeed a basis.

Definition 3. *Let G be a finite, abelian group. The dual of G, denoted $\widehat{G}$, is the set of all group homomorphisms from G to the group of non-zero complex numbers $(\mathbb{C}^*, \cdot)$ under complex multiplication. In symbols,*

$$\widehat{G} = \{\chi : G \to \mathbb{C}^* \mid \chi \text{ is a group homomorphism}\}.$$

The homomorphisms $\chi \in \widehat{G}$ are called characters.

We will now prove some basic properties of characters. For the next couple of lemmas G is a finite, abelian group and $\chi \in \widehat{G}$.

Lemma 1. *$\chi(x)$ is a $|G|$-th root of unity and in particular $|\chi(x)| = 1$.*

Proof. For any $\chi \in \widehat{G}$ and any $x \in G$ we have

$$\chi(x)^{|G|} = \chi(|G|x) = \chi(0) = 1.$$

□

Definition 4. *Let $\chi \in \widehat{G}$ be a character of G. Define the conjugate character $\overline{\chi}(x) : G \to \mathbb{C}$ by $\overline{\chi}(x) = \overline{\chi(x)}$.*

Lemma 2. *$\chi(-x) = \overline{\chi}(x)$.*

Proof. Since $\chi \in \widehat{G}$ is a group homomorphism we have

$$\chi(-x) = \chi(x)^{-1} = \frac{\overline{\chi(x)}}{|\chi(x)|^2} = \overline{\chi(x)} = \overline{\chi}(x).$$

□

We aim to show that $\widehat{G}$ forms a basis for $\ell^2(G)$ but first we prove that $\widehat{G}$ is a group.

Proposition 3. *The set $\widehat{G}$ from Definition 3 forms an abelian group where the group operation is pointwise multiplication, i.e. $(\chi\psi)(x) = \chi(x)\psi(x)$ for any $\chi, \psi \in \widehat{G}$ and any $x \in G$.*

Proof. The group operation is clearly associative. Let $\chi, \psi \in \widehat{G}$. Then $(\chi\psi)(x+y) = \chi(x+y)\psi(x+y) = \chi(x)\chi(y)\psi(x)\psi(y) = (\chi\psi)(x)(\chi\psi)(y)$. So $\widehat{G}$ is closed under multiplication. Finally the inverse of a character χ in the group $\widehat{G}$ is the conjugate character $\overline{\chi}$ as defined in Definition 4. The function $\overline{\chi}$ is clearly a homomorphism and it is the inverse of χ since $(\chi\overline{\chi})(x) = \chi(x)\overline{\chi(x)} = |\chi(x)|^2 = 1$, where the last equality follows by Lemma 1. □

So far we have been talking about abelian groups in the abstract. The Fundamental Theorem of Finite Abelian Groups says that any abelian group is a direct product of cyclic groups and for many applications we can just assume we are working with the group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. This allows us to write down explicit formulae for the homomorphisms and there is a very natural way of indexing the elements of $\widehat{G}$ with those of G which makes the notaion more convenient.

Definition 5. *Let* $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. *Then for every* $x = (x_1, x_2, \ldots, x_r) \in G$ *define* $\chi_x : G \to \mathbb{C}^*$ *by*

$$chi_x(y) = \prod_{j=1}^{r} \exp\left(2\pi i \frac{x_j y_j}{m_j}\right),$$

where $i = \sqrt{-1}$.

Remark 2. *Note that* $\chi_x(y) = \chi_y(x)$ *for all* $x, y \in G$.

It is easy to verify that χ_x is a character of G for all $x \in G$. The next proposition shows that all the characters are of this form.

Proposition 4. *Let* $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. *Then* $G \cong \widehat{G}$ *under the isomorphism* $\phi : G \to \widehat{G}$ *defined by* $\phi(x) = \chi_x$.

Proof. The map ϕ is a homomorphism since

$$\begin{aligned}
\chi_{x+y}(z) &= \prod_{j=1}^{r} \exp\left(2\pi i \frac{(x_j + y_j) z_j}{m_j}\right) \\
&= \prod_{j=1}^{r} \exp\left(2\pi i \frac{x_j z_j}{m_j}\right) \exp\left(2\pi i \frac{y_j z_j}{m_j}\right) \\
&= \chi_x(z)\chi_y(z).
\end{aligned}$$

For surjectivity, define $e_j = (0, \ldots, 0, 1, 0 \ldots, 0) \in G$ to be the tuple with 1 in the j-th position and 0 everywhere else. Let $\chi : G \to \mathbb{C}^*$ be a homomorphism. Then $\chi(e_j)$ is an m_j-th root of unity (see Lemma 1) so $\chi(e_j) = \exp(2\pi i x_j / m_j)$ for some $x_j \in \{0, 1, \ldots, m_j - 1\}$. Let $x = (x_1, \ldots, x_{m_j})$ then $\chi_x(e_j) = \chi(e_j)$ for all $1 \leq j \leq r$ and, since the e_j form a generating set for G, it follows that $\chi = \chi_x$. □

The fundamental theorem of finite abelian groups, when combined with the proposition above, tells us that any finite abelian group is isomorphic to its dual.

Proposition 5. *Any finite abelian group* G *is isomorphic to its dual* $\widehat{G}$.

Note that there is no *canonical* isomorphism between G and $\widehat{G}$. For example, when G is cyclic we must first identify it with $\mathbb{Z}_n$ to invoke Proposition 4. To do this we must first choose a generator for G. A change in the choice of generator changes the isomorphism. Despite this, we will find it very useful later on (see Definition 6) to index the elements of $\widehat{G}$ with elements of G using the χ_x notation.

Since G is isomorphic to its dual it is obvious that G is isomorphic to its double dual, $G^{\wedge\wedge}$. Even though there is no canonical isomorphism between G and $\widehat{G}$ there *is* a canonical isomorphism between G and $G^{\wedge\wedge}$. The isomorphism is $\phi : G \to G^{\wedge\wedge}$ where, for each $g \in G$ we define $\phi(g) : \widehat{G} \to \mathbb{C}^*$ by $[\phi(g)](\chi) = \chi(g)$.

We can now prove that $\widehat{G}$ forms a basis for $\ell^2(G)$.

Theorem 1. *Let G be a finite, abelian group. The group, $\widehat{G}$, of characters of G satisfies the following orthogonality relations:*

$$\sum_{x\in G}\chi(x) = \begin{cases} |G| & \text{if } \chi \text{ is the identity in } \widehat{G}, \\ 0 & \text{otherwise,} \end{cases} \qquad \sum_{\chi\in\hat{G}}\chi(x) = \begin{cases} |G| & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $S = \sum_{x\in G}\chi(x)$. If χ is the identity in $\widehat{G}$ then clearly $\chi(x) = 1$ for all $x \in G$ so $S = |G|$. If not, then there exists some $y \in G$ such that $\chi(y) \neq 1$. Then

$$\chi(y)S = \sum_{x\in G}\chi(x+y) = S.$$

Hence $S = 0$.

For the second part let $T = \sum_{\chi\in\hat{G}}\chi(x)$. If $x = 0$ then $T = |G|$. If $x \neq 0$ then, by using Definition 5 it is easy to see there exists some $\psi \in \widehat{G}$ such that $\psi(x) \neq 1$. Then

$$\psi(x)T = \sum_{\chi\in\hat{G}}(\psi\chi)(x) = T.$$

Hence $T = 0$. □

Corollary 1. *Let $\chi, \psi \in \widehat{G}$. Then*

$$\langle\chi,\psi\rangle = \begin{cases} 1 & \text{if } \chi = \psi, \\ 0 & \text{if } \chi \neq \psi. \end{cases}$$

Thus the set $\widehat{G}$ forms an orthonormal basis for $\ell^2(G)$ which we call the Fourier Basis.

Proof. By definition

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{x \in G} \chi(x) \overline{\psi(x)} = \frac{1}{|G|} \sum_{x \in G} (\chi \overline{\psi})(x).$$

Recall from the proof of Proposition 3 that $\overline{\psi} = \psi^{-1}$. The corollary now follows by substituting $\chi\psi^{-1}$ for χ in the first equation of the theorem. Since the characters are orthogonal they are linearly independent in $\ell^2(G)$. Using Propositions 4 and 1 we know $|\widehat{G}| = |G| = \dim \ell^2(G)$ hence the characters form a spanning set. □

The Fourier Basis is natural basis $\ell^2(G)$ for a number of reasons. It is orthonormal, which is a good property for any basis of a vector space to have, and since it consists of homomorphisms it "knows" that G is a group and not just some finite set.

3 The Fourier transform

Since the characters form an orthonormal basis for $\ell^2(G)$ we know that any $f \in \ell^2(G)$ can be written as $f = \sum_{x \in G} c_x \chi_x$, where $c_x = \langle f, \chi_x \rangle$. The Fourier transform of a function is the change of basis operator which takes a character as input and outputs the coefficient, c_x, of that character.

Definition 6. *The Fourier transform is a function $\mathscr{F} : \ell^2(G) \to \ell^2(\widehat{G})$ defined by*

$$(\mathscr{F} f)(\chi) = \langle f, \chi \rangle$$

for any $f \in \ell^2(G)$.

Since the inner product on $\ell^2(G)$ is linear in the first slot it follows that $\mathscr{F}$ is a linear map. The kernel of $\mathscr{F}$ is trivial because if $\langle f, \chi \rangle = 0$ for all $\chi \in \widehat{G}$ then $f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \chi = 0$. This means that $\mathscr{F}$ is an injective linear map and, since $\ell^2(G)$ has the same dimension as $\ell^2(\widehat{G})$, we conclude that $\mathscr{F}$ is in fact a bijection. In other words $\mathscr{F}$ is a vector space isomorphism.

Proposition 6. *The map $\mathscr{F} : \ell^2(G) \to \ell^2(\widehat{G})$ is bijective and linear.*

Unfortunately the notation $(\mathscr{F}f)(\chi)$ is a little cumbersome. We will define a different notation which uses the fact that we can index the characters of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ by the elements of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$.

Definition 7. *Let $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. For every $f : G \to \mathbb{C}$ define $\widehat{f} : G \to \mathbb{C}$ by $\widehat{f}(x) = (\mathscr{F}f)(\chi_x) = \langle f, \chi_x \rangle$.*

Note that $\widehat{f}(x)$ is not well defined if the domain of f is an arbitrary abelian group. This is because there is no canonical isomorphism between G and $\widehat{G}$ and therefore no God-given choice for what the character χ_x should be for a given $x \in G$.

The next proposition gives us a formula for writing f as a linear combination of the characters of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$.

Proposition 7. *Let $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. Then*

$$f = \sum_{x \in G} \widehat{f}(x) \chi_x$$

for all $f \in \ell^2(G)$.

Proof. Note by definition $\widehat{f}(x) = \langle f, \chi_x \rangle$. The proposition now follows since the χ_x form an orthonormal basis. □

Recall we can write $f \in \ell^2(\mathbb{Z}_n)$ as

$$f = \sum_{x \in \mathbb{Z}_n} f(x) \delta_x$$

where $\delta_x(y) = 1$ if $x = y$ and $\delta_x(y) = 0$ otherwise. Hence the vector

$$\begin{pmatrix} f(0) \\ f(1) \\ \vdots \\ f(n-1) \end{pmatrix} \in \mathbb{C}^n$$

is the coordinate column of f with respect to the delta-basis $\{\delta_x \mid x = 0, 1, \ldots, n-1\}$.

Similarly we can write

$$f = \sum_{x \in \mathbb{Z}_n} \widehat{f}(x) \chi_x$$

so the vector

$$\begin{pmatrix} \widehat{f}(0) \\ \widehat{f}(1) \\ \vdots \\ \widehat{f}(n-1) \end{pmatrix} \in \mathbb{C}^n$$

is the coordinate column of f with respect to the Fourier basis $\{\chi_x \mid x = 0, 1, \ldots, n-1\}$.

We defined the Discrete Fourier transform as a mapping from $\mathscr{F} : \ell^2(G) \to \ell^2(\widehat{G})$. This definition is fancier than necessary for most practical purposes. It is often simpler to view the Discrete Fourier Transform for $\mathbb{Z}_n$ as the change of basis matrix $\mathscr{F}_n \in \mathbb{C}^{n \times n}$ defined by

$$\mathscr{F}_n = \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_n & \omega_n^2 & \omega_n^3 & \cdots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \omega_n^6 & \cdots & \omega_n^{2(n-1)} \\ 1 & \omega_n^3 & \omega_n^6 & \omega_n^9 & \cdots & \omega_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2(n-1)} & \omega_n^{3(n-1)} & \cdots & \omega_n^{(n-1)(n-1)} \end{bmatrix}$$

which maps coordinate columns in the delta basis to coordinate columns in the Fourier basis

$$\begin{pmatrix} f(0) \\ f(1) \\ \vdots \\ f(n-1) \end{pmatrix} \overset{\mathscr{F}_n}{\longmapsto} \begin{pmatrix} \widehat{f}(0) \\ \widehat{f}(1) \\ \vdots \\ \widehat{f}(n-1) \end{pmatrix}.$$

Remark 3 (The connection between the Fourier basis and polynomials)**.** *There is a fundamental connection between polynomials and the Fourier Transform.*

Consider the case where the group G is the n-roots of unity under the group operation of complex multiplication. That is, $G = \{\omega_n^j \mid j \in \{0, \ldots, n-1\}\}$ where $\omega_n = \exp(2\pi i/n)$ and $i = \sqrt{-1}$. It is easy to see that all the homomorphisms from G to $\mathbb{C}^*$ are of the from $x \mapsto x^j$ where $j \in \{0, 1, \ldots, n-1\}$. This means that the space $\ell^2(G)$ is equal to $\operatorname{span}_{\mathbb{C}}\{1, x, x^2, \ldots, x^{n-1}\}$. In other words, $\ell^2(G)$ is the set of all polynomials of degree less than n with complex coefficients. The Fourier coefficients are the coefficients of the polynomial.

This has implications for interpolation of polynomials. Given a polynomial of degree less than n

$$f(x) = a_n x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 \in \mathbb{C}[x],$$

if we know the values $f(1), f(\omega_n), f(\omega_n^2), \ldots f(\omega_n^{n-1})$ *then one way of finding the coefficients* $a_0, a_1, \ldots, a_{n-1}$ *of* f *is to solve a system of linear equations over* $\mathbb{C}$*. Another way is to identify the polynomial* f *with a function*

$$f : \{1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}\} \to \mathbb{C}$$

which we then identify with

$$f : \mathbb{Z}_n \to \mathbb{C}$$

and then, from the previous discussion, the Fourier coefficients of $f : \mathbb{Z}_n \to \mathbb{C}$ *are precisely the coefficients of the polynomial* $f \in \mathbb{C}[x]$*, i.e.*

$$\widehat{f}(j) = a_j.$$

Thus interpolating a polynomial is the same as finding the Fourier coefficients of the function $f : \{1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}\} \to \mathbb{C}$ *defined by the polynomial. In Section ?? we will use this equivalence to efficiently compute the Fourier transform of a function.*

Multivariate polynomials can be viewed as functions from $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ *to* $\mathbb{C}$ *and their coefficients are the Fourier coefficients of the function they represent.*

We will now show that the Fourier Basis interacts well with the convolution operator.

Proposition 8. *Let* $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$*. Let* $f : G \to \mathbb{C}$*. Define an operato* $A_f : \ell^2(G) \to \ell^2(G)$ *by*

$$A_f g = f * g.$$

Then the characters $\chi_x \in \widehat{G}$ *diagonalise* A_f*. Each* $\chi_x \in \widehat{G}$ *is an eigenvector of* A_f *and its corresponding eigenvalue is* $\widehat{f}(x)$*.*

Proof. For all $y \in G$ we have

$$\begin{aligned}
(A_f\chi_x)(y) &= (f * \chi_x)(y) \\
&= \frac{1}{|G|}\sum_{z\in G} f(z)\chi_x(y-z) \\
&= \frac{1}{|G|}\sum_{z\in G} f(z)\chi_x(y)\overline{\chi_x(z)} \\
&= \left(\frac{1}{|G|}\sum_{z\in G} f(z)\overline{\chi_x(z)}\right)\chi_x(y) \\
&= \langle f, \chi\rangle\chi_x(y) \\
&= \widehat{f}(x)\chi(y),
\end{aligned}$$

as required. □

We have seen in Proposition 6 that the Fourier transform respects the addition and scalar multiplication in $\ell^2(G)$. Propositions 9 through 12 prove some of the fundamental properties of the Fourier transform. The proofs of these propositions are not that interesting; they are mostly just calculations.

The first of these propositions shows us how the Fourier transform interacts with the convolution operator.

Proposition 9. *Let $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. Then*

$$\widehat{(f * g)}(x) = \widehat{f}(x)\widehat{g}(x)$$

for every $f, g \in \ell^2(G)$ and every $x \in G$.

Proof. Let $f, g \in \ell^2(G)$. Let $x \in G$. Then

$$\begin{aligned}
\widehat{(f * g)}(x) &= \langle f * g, \chi_x\rangle \\
&= \frac{1}{|G|}\sum_{y\in G}(f * g)(y)\overline{\chi_x(y)} \\
&= \frac{1}{|G|}\sum_{y\in G}\left(\frac{1}{|G|}\sum_{z\in G} f(z)g(y-z)\right)\overline{\chi_x(y)} \\
&= \frac{1}{|G|^2}\sum_{y,z\in G} f(z)g(y-z)\overline{\chi_x(y)}
\end{aligned}$$

using the change of variables $w = y - z$ we get

$$\begin{aligned}
&= \frac{1}{|G|^2} \sum_{w,z \in G} f(z) g(w) \overline{\chi_x(w+z)} \\
&= \frac{1}{|G|^2} \sum_{w,z \in G} f(z) g(w) \overline{\chi_x(w)\chi_x(z)} \\
&= \frac{1}{|G|} \sum_{z \in G} f(z) \overline{\chi_x(z)} \frac{1}{|G|} \sum_{w \in G} g(w) \overline{\chi_x(w)} \\
&= \langle f, \chi_x \rangle \langle g, \chi_x \rangle \\
&= \widehat{f}(x) \widehat{g}(x).
\end{aligned}$$

□

Parsevals identity gives a relationship between the functions value and the Fourier coefficients.

Proposition 10 (Parseval's Identity)**.** *Let $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. Let $f \in \ell^2(G)$. Then*

$$\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 = \sum_{x \in G} |\widehat{f}(x)|^2.$$

Proof. We have

$$\begin{aligned}
\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 &= \langle f, f \rangle \\
&= \langle \sum_{x \in G} \widehat{f}(x) \chi_x, f \rangle \\
&= \sum_{x \in G} \widehat{f}(x) \langle \chi_x, f \rangle \\
&= \sum_{x \in G} \widehat{f}(x) \overline{\langle f, \chi_x \rangle} \\
&= \sum_{x \in G} \widehat{f}(x) \overline{\widehat{f}(x)} \\
&= \sum_{x \in G} |\widehat{f}(x)|^2.
\end{aligned}$$

□

There are two other useful forms of Parseval's theorem which we state in the corollaries below for easy reference later.

Corollary 2. *Let G and f be as above. Then $\frac{1}{|G|}\langle f, f\rangle = \left\langle \widehat{f}, \widehat{f} \right\rangle$.*

Corollary 3. *Let G and f be as above. Then $\frac{1}{|G|}\|f\|_2^2 = \|\widehat{f}\|_2^2$.*

Proposition 11. *Let $s \in G$. Let $f \in \ell^2(G)$. Define $g : G \to \mathbb{C}$ by $g(x) = f(s+x)$. Then $\widehat{g}(x) = \chi_x(s)\widehat{f}(x)$.*

Proof. We have

$$\begin{aligned}
\widehat{g}(x) &= \langle g, \chi_x \rangle \\
&= \frac{1}{|G|} \sum_{y \in G} g(y)\overline{\chi_x(y)} \\
&= \frac{1}{|G|} \sum_{y \in G} f(s+y)\overline{\chi_x(y)} \\
&= \frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi_x(w-s)}
\end{aligned}$$

substituting $w = y + s$

$$\begin{aligned}
&= \frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi_x(w)\chi_x(-s)} \\
&= \frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi_x(w)\chi_{-s}(x)} \\
&= \frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi_x(w)}\chi_x(s) \\
&= \chi_x(s)\frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi_x(w)}.
\end{aligned}$$

□

Proposition 12. *Let $s \in \mathbb{Z}_n^*$. Let $f \in \ell^2(\mathbb{Z}_n)$. Define $g : \mathbb{Z}_n \to \mathbb{C}$ by $g(x) = f(sx)$. Then $\widehat{g}(x) = \widehat{f}(s^{-1}x)$.*

Proof. We have

$$\begin{aligned}\widehat{g}(x) &= \langle g, \chi_x \rangle \\ &= \frac{1}{n} \sum_{y \in \mathbb{Z}_n} g(y) \overline{\chi_x(y)} \\ &= \frac{1}{n} \sum_{y \in \mathbb{Z}_n} f(sy) \overline{\chi_x(y)}\end{aligned}$$

We use the change of variables $z = sy$. Since $s \in \mathbb{Z}_n^*$ we know that z ranges over $\mathbb{Z}_n$ as y ranges over $\mathbb{Z}_n$.

$$\begin{aligned}&= \frac{1}{n} \sum_{y \in \mathbb{Z}_n} f(sy) \overline{\chi_x(y)} \\ &= \frac{1}{n} \sum_{z \in \mathbb{Z}_n} f(z) \overline{\chi_x(s^{-1}z)} \\ &= \frac{1}{n} \sum_{z \in \mathbb{Z}_n} f(y) \overline{\chi_{s^{-1}x}(z)} \\ &= \langle f, \chi_{s^{-1}x} \rangle \\ &= \widehat{f}(s^{-1}x).\end{aligned}$$

□

4 Quotient groups and the Poisson summation formula

We now turn our attention to classifying the duals of quotient groups. This will give us the results we need to prove the finite analogue of the Poisson summation formula. It turns out we can identify the duals of all the quotients of G with subgroups of $\widehat{G}$.

Definition 8. *Let G be a finite, abelian group and let $H \leq G$ be a subgroup of G. Define*

$$H^{\#} = \{\chi \in \widehat{G} \mid \chi(h) = 1 \text{ for all } h \in H\}.$$

In the next proposition we use the notation $\overline{\chi}$ to refer to a character defined on a quotient of G. Everywhere else the notation $\overline{\chi}$ refers to the conjugate character defined by $\overline{\chi}(x) = \overline{\chi(x)}$ as in Definition 4.

Proposition 13. *Let G be a finite, abelian group and let $H \leq G$ be a subgroup of G. For each $\chi \in H^{\#}$ define $\overline{\chi} : G/H \to \mathbb{C}^*$ by $\overline{\chi}(g+H) = \chi(g)$. Then $\overline{\chi}$ is well defined and*

$$H^{\#} \cong \widehat{G/H}$$

under the map $\chi \mapsto \overline{\chi}$.

Proof. Define $\phi : H^{\#} \to \widehat{G/H}$ by $\phi(\chi) = \overline{\chi}$. Let $\chi \in H^{\#}$. Since $\chi(h) = 1$ for all $h \in H$ the function $\overline{\chi}$ is well defined. The map ϕ is a homomorphism since $\overline{\chi\psi}(g+H) = \chi\psi(g) = \chi(g)\psi(g) = \overline{\chi}(g+H)\overline{\psi}(g+H)$. Define $\theta : \widehat{G/H} \to H^{\#}$ by $\theta(\psi)(g) = \psi(g+H)$. Then $\theta(\psi)$ is identically 1 on H, so the map is well defined. It is easy to show that θ is the inverse of ϕ, thus ϕ is bijective. This completes the proof. □

Definition 9. *Let $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. Let $H \leq G$. Define*

$$H^{\perp} = \{x \in G \mid \chi_x \in H^{\#}\}.$$

Let $G = \mathbb{Z}_n$. Then any $H \leq G$ is generated by a single element $H = \langle a \rangle$. Without loss of generality we may assume a divides n, hence $H^{\perp} = \langle n/a \rangle$. Moreover, if K is a subgroup of some group J then $(H \times K)^{\perp} = H^{\perp} \times K^{\perp} \leq G \times J$, so given generators for any subgroup of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ it is easy to find $H^{\perp}$.

Now that we have defined $H^{\perp}$ we can prove a generalisation of the orthogonality relations in Proposition 1.

Proposition 14. *Let $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. Let $H \leq G$. Then*

$$\sum_{h \in H} \chi_h(x) = \begin{cases} |H|, & \text{if } x \in H^{\perp}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $x \in H^{\perp}$ then, by definition of $H^{\perp}$, we have $\chi_x(h) = 1$ for all $h \in H$. Hence by Remark 2 we have $\chi_h(x) = 1$ for all $h \in H$. If $x \notin H^{\perp}$ then, by definition of $H^{\perp}$, there exists some $h' \in H$ for which $\chi_x(h') \neq 1$. Then

$$\sum_{h \in H} \chi_h(x) = \sum_{h \in H} \chi_{h+h'}(x) = \chi_{h'}(x) \sum_{h \in H} \chi_h(x) = \chi_x(h') \sum_{h \in H} \chi_h(x)$$

which implies that $\sum_{h \in H} \chi_h(x) = 0$.

□

Proposition 15 (Poisson summation formula)**.** *Let* $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$*. Let* $f : G \to \mathbb{C}$*. Let* $H \leq G$*. Then*

$$\sum_{h \in H} \widehat{f}(h)\chi_h(x) = \frac{1}{|G : H|} \sum_{y \in H^\perp} f(x - y).$$

We will actually prove a slightly more general version of the Poisson summation formula where the sum on the left hand side of the equation is a sum over a coset instead of a subgroup.

Proposition 16. *Let* $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$*. Let* $f : G \to \mathbb{C}$*. Let* $H \leq G$*. Let* $\alpha \in G$*. Then*

$$\sum_{h \in H} \widehat{f}(\alpha + h)\chi_{\alpha+h}(x) = \frac{1}{|G : H|} \sum_{y \in H^\perp} f(x - y)\chi_\alpha(y).$$

Proof. Define $g : G \to \mathbb{C}$ by $g(x) = \sum_{h \in H} \chi_{\alpha+h}(x)$. Then Proposition 9 tells us that $\widehat{(f * g)}(\alpha) = \widehat{f}(\alpha)\widehat{g}(\alpha)$ so

$$\sum_{h \in H} \widehat{f}(\alpha + h)\chi_{\alpha+h}(x) = (f * g)(x).$$

Now since the mapping $x \mapsto \chi_x$ is an isomorphism we know $\chi_{\alpha+h}(x) = \chi_\alpha(x)\chi_h(x)$. Hence $g(x) = \chi_\alpha(x) \sum_{h \in H} \chi_h(x)$. It follows from Proposition 14 that

$$g(x) = \begin{cases} \chi_\alpha(x) \cdot |H|, & \text{if } x \in H^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

Putting this all together we get

$$(f * g)(x) = (g * f)(x) = \frac{1}{|G|} \sum_{y \in G} g(y)f(x - y) = \frac{|H|}{|G|} \sum_{y \in H^\perp} \chi_\alpha(y)f(x - y)$$

which is the right hand side of the equation. □

The Poisson summation formula is now an immediate consequence of Proposition 16 by substituting $\alpha = 0$.

5 Computing the Fourier Transform

For the section we will assume the finite, abelian group G is $\mathbb{Z}_n$, where n is an integer power of 2. We assume this for simplicity, not because the Fourier transform can not be efficiently computed for other finite, abelian groups. The algorithms presented in this section can be generalised to non-cyclic abelian groups without too much difficulty, provided the order of the group is smooth (only small primes divide it).

We want an algorithm which given the complex numbers $f(0), f(1), \ldots, f(n-1)$ as input, outputs $\widehat{f}(0), \widehat{f}(1), \ldots, \widehat{f}(n-1)$.

Recall that, by definition

$$\widehat{f}(x) = \langle f, \chi_x \rangle = \frac{1}{|G|} \sum_{z=0}^{n-1} f(z)\overline{\chi_x(z)} = \frac{1}{|G|} \sum_{z=0}^{n-1} f(z)\omega_n^{-xz},$$

where $\omega_n = \exp(2\pi i/n)$ and $i = \sqrt{-1}$. We will ignore the factor of $1/|G|$ and simply state our the computational problem we are trying to solve like this:

Fourier Transform Algorithm: Given an array of complex numbers $x = [x_0, x_1, x_2, \ldots, x_{n-1}]$ as input, output the array $X = [X_0, X_1, \ldots, X_{n-1}]$ where

$$X_k = \sum_{j=0}^{n-1} x_j \omega_n^{-jk}. \tag{1}$$

We will assume that adding or multiplying two complex numbers and computing ω_n^{-jk} takes $O(1)$ time. We will not worry about numerical precision in our analysis.

5.1 The Fast Fourier Transform

If we just directly compute each X_k using Equation (1) this will take $O(n^2)$ time since each X_k requires n multiplications and additions to compute and k ranges from 0 to $n-1$.

To achieve $O(n \log n)$ time algorithm we first reduce the problem of calculating the Fourier Tranform to evaluating a polynomial at the n-th roots of unity. Given some array of complex numbers $x = [x_0, x_1, \ldots, x_{n-1}]$ define

the polynomial

$$p(t) = \sum_{j=0}^{n-1} x_j t^j.$$

Then the Fourier tranform of x is the array X where

$$X_k = \sum_{j=0}^{n-1} x_j \omega_n^{-jk} = \sum_{j=0}^{n-1} x_j \omega_n^{j(n-k)} = \sum_{j=0}^{n-1} x_j (\omega_n^{n-k})^j = p(\omega_n^{n-k}),$$

so

$$X = [X_0, X_1, \ldots, X_{n-1}] = [p(\omega_n^0), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \ldots, p(\omega_n^1)].$$

Thus calculating X is the same as evaluating the polynomial p at all the n-th roots of unity. We can now restate the problem we are trying to solve.

Evaluate Polynomial Problem:

Input: An array of complex numbers $[p_0, p_1, \ldots, p_{n-1}]$ where $n = 2^k$ is an integer power of two.

Output: The array of complex numbers $[p(\omega_n^0), p(\omega_n^{n-1}), \ldots, p(\omega_n^1)]$ where $p(t) \in \mathbb{C}[x]$ is the polynomial defined by

$$p(t) = \sum_{j=0}^{n-1} p_j t^j.$$

That is, evaluate $p(t)$ at all the n-th roots of unity.

The evaluate polynomial problem can be done as follows:

- Define the polynomials p_{even} and p_{odd} to be the polynomials containing only the even or odd terms if p respectively, i.e.

  $$p_{even}(t) = \sum_{j=0,2,4,\ldots,n-2} p_j t^j$$

  and

  $$p_{odd}(t) = \sum_{j=1,3,5,\ldots,n-1} p_j t^j.$$

  Then

  $$p(t) = p_{even}(t^2) + t p_{odd}(t^2).$$

  so

  $$p(\omega_n^k) = p_{even}(\omega_n^{2k}) + \omega_n^k p_{odd}(\omega_n^{2k}) \tag{2}$$

- Recursively evaluate $p_{even}(t)$ at the $n/2$-th roots of unity, i.e. compute the
$$[p_{even}(\omega_{n/2}^0), \ldots, p_{even}(\omega_{n/2}^{n/2-1})].$$
- Recursively evaluate $p_{odd}(t)$ at the $n/2$-th roots of unity, i.e. compute the array
$$[p_{odd}(\omega_{n/2}^0), \ldots, p_{odd}(\omega_{n/2}^{n/2-1})].$$
- Evaluate p at each root of unity using the formula
$$p(\omega_n^k) = p_{even}(\omega_{n/2}^{2k \bmod n/2}) + \omega_n^k p_{odd}(\omega_{n/2}^{2k \bmod n/2}).$$
which holds because of equation (2).

The pseudocode for this is given below.

Algorithm 1: RecEvaluate

Input: An array of complex numbers $[p_0, p_1, \ldots, p_{n-1}]$ which are the coefficients of the polynomial $p(t) \in \mathbb{C}[x]$.
Output: The array $[p(\omega_n^0), p(\omega_n^{n-1}), \ldots, p(\omega_n^1)]$.
if *p is a constant polynomial* **then**
  return *The array* $[p_0]$
else
  Construct the coefficient array for p_{even} and p_{odd} `/* O(n) time */`

  Calculate $[p_{even}(\omega_{n/2}^0), \ldots, p_{even}(\omega_{n/2}^{n/2-1})]$ by recursively calling RecEvaluate($[p_0, p_2, \ldots, p_{n-2}]$)
  Calculate $[p_{odd}(\omega_{n/2}^0), \ldots, p_{odd}(\omega_{n/2}^{n/2-1})]$ by recursively calling RecEvaluate($[p_1, p_3, \ldots, p_{n-1}]$)

  for *each root of unity* ω_n^k **do**
    Calculate $p(\omega_n^k) = p_{even}\left(\omega_{n/2}^{2k \pmod{n/2}}\right) + \omega_n^k p_{odd}\left(\omega_{n/2}^{2k \pmod{n/2}}\right)$
    `/* O(n) time */`
  return *The array* $[p(\omega_n^0), p(\omega_n^{n-1}), \ldots, p(\omega_n^1)]$

We will now anlyse the running time if this algorithm. Let $T(n)$ be the running time of the algorithm when the input array has length n. That is, $T(n)$ is the time it takes to compute RecEvaluate($[p_0, p_1, \ldots, p_{n-1}]$.

- Constructing the arrays $[p_0, p_2, \ldots, p_{n-2}]$ and $[p_1, p_3, \ldots, p_{n-1}]$ takes $O(n)$ time.
- Calculating $[p_{even}(\omega_{n/2}^0), \ldots, p_{even}(\omega_{n/2}^{n/2-1})] = \text{RecEvaluate}([p_0, p_2, \ldots, p_{n-2}])$ and $[p_{odd}(\omega_{n/2}^0), \ldots, p_{odd}(\omega_{n/2}^{n/2-1})] = \text{RecEvaluate}([p_1, p_3, \ldots, p_{n-1}])$ each take $T(n/2)$ time since their input arrays have size $n/2$.
- Constructing array $[p(\omega_n^0), p(\omega_n^{n-1}), \ldots, p(\omega_n^1)]$ using the formula

$$p(\omega_n^k) = p_{even}\left(\omega_{n/2}^{2k \pmod{n/2}}\right) + \omega_n^k p_{odd}\left(\omega_{n/2}^{2k \pmod{n/2}}\right)$$

  takes $O(n)$ time.
- So we have the recurrence $T(n) = 2T(n/2) + O(n)$.
- Using case 2 of the Master Theorem below this means $T(n) = O(n \log n)$.

Theorem 2 (Master Theorem)**.** *Let $a \geq 1$. Let $b \geq 1$. Let $f : \mathbb{N} \to \mathbb{R}$. Suppose $T : \mathbb{N} \to \mathbb{R}$ satisfies the recurrence*

$$T(n) = aT(n/b) + f(n),$$

where we interpret n/b to mean $\lfloor n/b \rfloor$ or $\lceil n/b \rceil$. Then $T(n)$ has the following asymptotic bounds:

1. *If $f(n) = O(n^{\log_b a - \epsilon})$ for some constant $\epsilon > 0$, then $T(n) = \Theta(n^{\log_b a})$.*
2. *If $f(n) = \Theta(n^{\log_b a})$, then $T(n) = \Theta(n^{\log_b a} \log n)$.*
3. *If $f(n) = \Omega(n^{\log_b a + \epsilon})$ for some constant $\epsilon > 0$, and if $af(n/b) \leq cf(n)$ for some constant $c < 1$ and all sufficiently large n then $T(n) = \Theta(f(n))$.*

Now that we know how to evaluate any degree $n-1$ polynomial at the n-th roots of unity the algorithm for calculating the discrete Fourier transform is easy.

Algorithm 2: FFT

Input: An array of complex numbers $x = [x_0, x_1, \ldots, x_{n-1}]$.
Output: The array $X = [X_0, X_1, \ldots, X_{n-1}]$ where $X_k = \sum_{j=0}^{n-1} x_j \omega_n^{-jk}$.
return *The array* RecEvaluate$([x_0, x_1, \ldots, x_{n-1}])$

This algorithm is known as the Fast Fourier Transform.