FINITE FOURIER ANALYSIS

NEIL LYALL

1. The group $\mathbb{Z}_N$

Let N be a positive integer. A complex number z is an N^{th} root of unity if $z^N = 1$. It is then easy to verify that the set of N^{th} roots of unity is precisely

$$\left\{1, e^{2\pi i/N}, e^{2\pi i 2/N}, \ldots, e^{2\pi i(N-1)/N}\right\}.$$

In fact, if we let $\omega = e^{2\pi i/N}$ we find that ω^n exhausts all the N^{th} roots of unity and

$$\omega^n = \omega^m \Leftrightarrow n - m \text{ is divisible by } N.$$

We denote the set of all N^{th} roots of unity by $\mathbb{Z}_N$. It is an easy exercise (do it!) to see that $\mathbb{Z}_N$ is an abelian group under complex multiplication.

It turns out that there is another natural way to visualize the group $\mathbb{Z}_N$. We can associate to each root of unity ζ the integer n so that $\omega^n = \zeta$. We observed above that this integer is not unique, in fact we saw that there is a whole class of such integer with the property that any two members of the class must differ by an integer multiple of N.

Two integers x and y whose difference $x - y$ is divisible by N are said to be congruent modulo N, usually denoted $x \equiv y \mod N$. It is an easy exercise to see that this defines an equivalence relation on $\mathbb{Z}$. Let $R(x)$ denote the equivalence class of an integer x. There are precisely N equivalence classes, and each class has a unique representative (element) between 0 and $N - 1$. We may add equivalence classes by defining

$$R(x) + R(y) = R(x + y).$$

This definition is independent of the representatives x and y (check!) and turns the set of equivalence classes into an abelian group called the group of integers modulo N, sometimes denoted by $\mathbb{Z}/N\mathbb{Z}$.

The association

$$R(k) \leftrightarrow e^{2\pi ik/N}$$

gives a correspondence between the two groups, $\mathbb{Z}/N\mathbb{Z}$ and $\mathbb{Z}_N$. Since the operations are respected, in the sense that addition of integers modulo n becomes multiplication of complex numbers, we shall also denote the group of integers modulo N by $\mathbb{Z}_N$. Observe that 0 (or N) $\in \mathbb{Z}/N\mathbb{Z}$ corresponds to 1 on the unit circle.

Let V and W denote the vector spaces of complex-valued functions on the group of integers modulo N and the N^{th} roots of unity, respectively. Then, the identification given above carries over to V and W as follows

$$F(k) \leftrightarrow f(e^{2\pi ik/N}),$$

where F is a function on the group of integers modulo N and f is a function on the N^{th} roots of unity.

From now on, we write $\mathbb{Z}_N$ but think of either the group of N^{th} roots of unity or the group of integers modulo N, which can of course be identified with the set $\{1, \dots, N\}$.

2. Functions on $\mathbb{Z}_N$

The vector space V of all complex-valued functions $f : \mathbb{Z}_N \to \mathbb{C}$ can be identified with the n-dimensional complex Euclidean space by assigning the vector: $v_f = (f(1), \dots, f(n))$ to the function f. V is therefore endowed with the (Hermitian) inner product

$$(f, g) = \sum_{n=1}^{N} f(n)\overline{g(n)} \tag{1}$$

(where $\overline{z}$ stands for the complex conjugate of z) and associated ℓ^2-norm

$$\|f\|_2 = (f, f)^{1/2}. \tag{2}$$

This inner product and associated norm satisfies the following usual properties.

Proposition 2.1. *If $f, g, h \in V$ and λ, μ are complex numbers then*

(i) $(f, g) = \overline{(g, f)}$
(ii) $(f, f) \geq 0$ *and* $(f, f) = 0$ *if and only if* $f = 0$.
(iii) $(\lambda f + \mu g, h) = \lambda(f, h) + \mu(g, h)$.

Proposition 2.2. *For $f, g, \in V$ and $\lambda \in \mathbb{C}$ one has*

(i) $\|\lambda f\|_2 = |\lambda| \|f\|_2$
(ii) $\|f + g\|_2 \leq \|f\|_2 + \|g\|_2$ *(triangle inequality)*

where equality holds in (ii) if and only if f and g are linearly dependent.

The proofs of all these properties except the triangle inequality are immediate. In order to establish the triangle inequality we need the following important inequality.

Proposition 2.3. Cauchy-Schwarz Inequality. *If $f, g \in V$ then one has*

$$|(f, g)| \leq \|f\|_2 \|g\|_2, \tag{3}$$

where equality holds if and only if f and g are linearly dependent.

Proof. If f and g are linearly dependent - say $f = \lambda g$ where $\lambda \in \mathbb{C}$, then we clearly have equality. Suppose now that f and g are linear independent: we must show that (3) hold with strict inequality. For any $\lambda \in \mathbb{C}$, $f + \lambda g \neq 0$ and therefore

$$\begin{aligned} 0, (f = \lambda g, f + \lambda g) \\ &= (f, f) + (f, \lambda g) + (\lambda g, f) + (\lambda g, \lambda g) \\ &= \|f\|_2^2 + \overline{\lambda}(f, g) + \lambda\overline{(f, g)} + |\lambda|^2\|g\|_2^2 \\ &= \|f\|_2^2 + 2\,\mathrm{Re}\{\overline{\lambda}(f, g)\} + |\lambda|^2\|g\|_2^2 \end{aligned}$$

We now pick a complex number u of unit modulus such that $\overline{u}(f, g) = |(f, g)|$. On putting $\lambda = tu$ we deduce that for any $t \in \mathbb{R}$,

$$0 < \|f\|_2^2 + 2t|(f, g)| + t^2\|g\|_2^2.$$

This can only happen if the real quadratic on the right has negative discriminant: that is

$$4|(f, g)|^2 - 4\|f\|_2^2\|g\|_2^2 < 0,$$

which yields the desired conclusion. □

Next, we introduce a special basis for the space V consisting of the so-called characters of the group $\mathbb{Z}_N$. For $1 \leq j \leq N$, let $e_j : \mathbb{Z}_N \to \mathbb{C}$ be defined by $e_j(k) = e^{2\pi ijk/N} = \omega^{jk}$.

Proposition 2.4.

(i) $e_j(0) = 1$ *and* $|e_j(k)| = 1$ *for all* j *and* k
(ii) $e_j(k + l) = e_j(k) \cdot e_j(l)$
(iii) *The functions* e_j $(1 \leq j \leq N)$ *form an orthogonal basis of the space* V*, more precisely one has*

$$(e_j, e_k) = \begin{cases} N & \text{if } j = k \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

Proof. Parts (i) and (ii) are obvious from the definition and so is part (iii) when $j = k$. Note, that if $j \neq k$ then $e^{2\pi i(j-k)/N} \neq 1$, and the inner product is the geometric series:

$$(e_j, e_k) = \sum_{\ell=1}^{N} e^{2\pi i(j-k)\ell/N} = \frac{e^{2\pi i(j-k)} - 1}{e^{2\pi i(j-k)/N} - 1} = 0. \tag{5}$$

It follows that the functions e_j are linearly independent, indeed if $\sum_{j=1}^{N} \lambda_j e_j = 0$ then taking the inner product of this sum with e_k one gets $N\lambda_k = 0$. They form a basis since the space V has dimension N. □

Note that if the δ_0 denotes the Delta function, that is $\delta_0(0) = 1$ and $\delta_0(k) = 0$ if $k \neq 0$, then (4) can be written in the more compact form: $(e_j, e_k) = N\delta_0(j - k)$.

3. Fourier analysis on $\mathbb{Z}_N$

Definition 3.1. The (discrete) **Fourier transform** $\hat{f}$, of a function $f : \mathbb{Z}_N \to \mathbb{C}$ is defined by

$$\hat{f}(k) = (f, e_k) = \sum_{x=1}^{N} f(x) e^{-2\pi i x k/N} \tag{6}$$

Of fundamental importance are the following.

Theorem 3.2. *Let $f, g \in V$. Then one has*

(i) **Fourier inversion formula**

$$f(x) = \frac{1}{N} \sum_{k} \hat{f}(k) e^{2\pi i x k/N} \tag{7}$$

(ii) **Parseval's formula**

$$\sum_{x} f(x)\overline{g(x)} = \frac{1}{N} \sum_{k} \hat{f}(k)\overline{\hat{g}(k)} \tag{8}$$

(iii) **Plancherel's formula**

$$\sum_{x} |f(x)|^2 = \frac{1}{N} \sum_{k} |\hat{f}(k)|^2 \tag{9}$$

Proof. All three formulae follows from (6) □

One of the reasons that the Fourier transform: $\mathcal{F} : f \to \hat{f}$ has wide range of applications is that it has many algebraic properties. Among them is the fact that it takes convolutions into pointwise multiplication.

Definition 3.3. Let $f, g \in V$. The convolution $f * g$ is defined by

$$f * g(x) = \sum_{y} f(y) g(x - y) \tag{10}$$

The summation, as always in this section is taken over elements of $\mathbb{Z}_N$, unless specified otherwise. Note that $f * g = g * f$ as can be seen by making the substitution: $y := x - y$ in the sum.

Proposition 3.4. *One has*

$$\widehat{f * g}(k) = \hat{f}(k)\hat{g}(k) \tag{11}$$

Proof. The left side of (11) is of the form

$$\sum_x \sum_y f(y)g(x-y)e^{-2\pi iyk/N}e^{-2\pi i(x-y)k/N} = \sum_x f(x)e^{-2\pi ixk/N} \cdot \sum_y g(y)e^{-2\pi iyk/N} = \hat{f}(k)\hat{g}(k)$$

□

4. Execises

1. Prove all three parts of Theorem 3.2.
2. Again let $\omega = e^{2\pi i/N}$, we now use this to define the following $N \times N$ matrix;

$$M = N^{-1/2}(a_{jk})_{1\leq j,k\leq N} \quad \text{where } a_{jk} = \omega^{jk}.$$

   Show that M is unitary and hence
   (i) $(Mu, Mu) = (u, u)$
   (ii) $(Mu, Mv) = (u, v)$
   (iii) $M^* = M^{-1}$, where M^* denote the conjugate transpose of M.

   Interpret these observations in terms of the Fourier transform.
3. For $f, g \in V$ one could define the following "twisted" version of convolution, namely

$$f \star g(x) = \sum_y f(y)\overline{g(y-x)}.$$

   Verify that

$$\widehat{f \star g}(k) = \hat{f}(k)\overline{\hat{g}(k)}$$

4. Use Exercise 3 above and Parseval's formula to show

$$\sum_k |\hat{f}(k)|^2|\overline{\hat{g}(k)}|^2 = N\sum_x \left|\sum_y f(y)\overline{g(y-x)}\right|^2$$

   and consequently

$$\sum_k |\hat{f}(k)|^4 = N \sum_{a-b=c-d} f(a)\overline{f(b)f(c)}f(d).$$

5. Show that if $A \subset \mathbb{Z}_n$ and $f = \chi_A$ (the indicator function of A), then

$$\#\{(x, x+s, x+t, x+s+t) \in A^4\} = \frac{1}{N}\sum_k |\hat{f}(k)|^4$$

6. Quadruples of the form $(x, x+s, x+t, x+s+t)$ are called *squares*. Show that if $A \subset \mathbb{Z}_N$ of cardinality δN, then it contains at least $\delta^4 N^3$ squares. If A were a random set of size δN, then how many squares would you expect A to contain?

7. Can you establish the lower bound for the number of square stated in exercise 6 without resorting to Fourier analysis?

   Hint: Consider the relationship between the number of square and the size of the set $|A \cap (A+k)|$.

8. Given a set A with cardinality δN, let us define the *balanced* function of A to be $f_A : \mathbb{Z}_N \to [-1,1]$ where

$$f_A(s) = \begin{cases} 1-\delta & s \in A \\ -\delta & s \notin A. \end{cases}$$

   How does this function relate to χ_A? Show that

   (i) $\sum_s f_A(s) = 0$, we say that f_A has mean value zero (hence the term *balanced*).

   (ii) $\widehat{f_A}(r) = \widehat{\chi_A}(r)$ for $r \neq 0$.

9. Use the Fourier transform to express the number of solutions to the equations

$$\text{(i) } x+y=z \quad \text{and} \quad \text{(ii) } x+y=2z$$

   in $\mathbb{Z}_N$ and in any subset A of $\mathbb{Z}_N$.

10. Verify that if f is a function from $\mathbb{Z}_N$ to the closed unit disc in $\mathbb{C}$, then the following are equivalent

    (i) $\sum_k \left|\sum_s f(s)\overline{f(s-k)}\right|^2 \leq c_1 N^3$

    (ii) $\sum_{a-b=c-d} f(a)\overline{f(b)f(c)}f(d) \leq c_1 N^3$

    (iii) $\sum_r |\hat{f}(r)|^4 \leq c_1 N^4$

    (iv) $\max_r |\hat{f}(r)| \leq c_2 N$

    (v) $\sum_k \left|\sum_s f(s)\overline{g(s-k)}\right|^2 \leq c_3 N^2 \|g\|_2^2$ for every function $g : \mathbb{Z}_N \to \mathbb{C}$

    where when we say that one property involving c_i implies another involving c_j we mean that whenever the first holds, then then second holds for a constant c_j that tends to zero as c_i tends to zero.