Finite Fourier Analysis

Bradford Hill

Andrew Gordon

April 26, 2019

1 Introduction

1.1 Motivation

The theory of finite Fourier analysis makes use of several ideas which originated in ordinary Fourier analysis. In the latter, a smooth function $\mathbb{R} \to \mathbb{R}$ can be decomposed into a linear combination of complex exponentials. In the former, we use group characters to span all functions from G to $\mathbb{C}$. We sum up some correspondences in the following table:

	Ordinary Fourier analysis	Finite Fourier analysis
Vector space	Functions, $\mathbb{R} \to \mathbb{R}$	Functions, $G \to \mathbb{C}$
Basis vectors	Complex exponentials	Characters on G

Let's illustrate some definitions so we can understand what these ideas are and why they are connected.

1.2 Characters of Abelian groups

Definition 1.1 (Character)**.** Let G be a finite Abelian group. A *character on* G is a homomorphism from G to the multiplicative group of the unit circle $S^1 \subseteq \mathbb{C}$.

One might wonder if there is any algebraic structure to the collection of all characters on G. In the following we will set up some definitions to illustrate this.

Definition 1.2 (Dual group)**.** The *dual group* of a finite Abelian group G is the set of all characters on G, denoted $\widehat{G}$. The product of two characters e_a, e_b in $\widehat{G}$ is defined $(e_a \cdot e_b)(g) = e_a(g)e_b(g)$, for all $g \in G$.

Because $\widehat{G}$ is a group, it has a unique identity element.

Definition 1.3 (Trivial character)**.** The *trivial character* is the element $e \in \widehat{G}$ where $e(g) = 1$ for every $g \in G$.

Theorem 1.1. The trivial character on G is the identity in $\widehat{G}$.

Proof. Let e_1 be the trivial character on G. If e is another character on G and $g \in G$, we have $e_1(g)e(g) = 1 \cdot e(g) = e(g)$, so $e_1 \cdot e = e$ for any character $e \in \widehat{G}$, i.e. e_1 is the identity in $\widehat{G}$. □

Remark. The definition of a character is such that that all characters $e \in \widehat{G}$ are linearly independent in V. We will examine this in the next section.

Example 1.1 (Characters on $\mathbb{Z}(N)$)**.**

- When $G = \mathbb{Z}(N)$ the additive group of integers modulo N, define a family of functions $e_n : \mathbb{Z}(N) \to S^1$ by

$$e_n(k) = \exp(2\pi ikn/N).$$

  These e_n are characters on $\mathbb{Z}(N)$. The function e_N is referred to as the *trivial character* on $\mathbb{Z}(N)$.

- If e is a character on $\mathbb{Z}(N)$ and $k \in \mathbb{Z}(N)$,

$$e(k) = e_l(k) = \exp(2\pi ilk/N)$$

  for some integer $1 \leq l \leq N - 1$.

A proof of the above is given in Shakarchi.

Several examples have shown that a character of an Abelian group maps elements of G to roots of unity. This turns out to be true for any Abelian group.

Example 1.2. Let G be an Abelian group and $e : G \to \mathbb{C}$ be a function such that $e(xy) = e(x)e(y)$ for all $x, y \in G$. We claim that this is sufficient to say $e(x)$ is a root of unity for all $x \in G$.

- *Claim.* Either e is identically zero, or e never vanishes.

  Proof. 1. If $e \equiv 0$ is the zero function, we have $e(xy) = e(x)e(y)$ trivially.

  2. Suppose there is $v \in G$ so that $e(v) = 0$, and also $w \in G$ so that $e(w) \neq 0$. Because G is a group, there exists $b \in G$ where $vb = w$. Then we have $e(w) = e(vb) = e(v)e(b) = 0$, which contradicts our earlier assumption that $e(w)$ is nonzero.

  □

- *Claim.* For each $x \in G$, $e(x) = e^{2\pi ir}$, where $r \in \mathbb{Q}$.

  Proof. Let $e : G \to \mathbb{C}$ be a group homomorphism. We have either $e \equiv 0$ or $e(x) \neq 0, \forall x \in G$. Suppose the latter case holds. Let x be an element of $G.$, then x has finite order. We will say $o(x) := N$. Then $x^N = 1_G$, the identity element in G. Note: $e(1_G) = 1$. Thus, we have $1 = |e(1_G)| = |e(x^N)| = |e(x)|^N$, and necessarily $|e(x)| = 1$. Then e maps all elements of G to the unit circle. We now have for each $x \in G$, $e(x) = e^{2\pi i\theta}$ for some $\theta \in \mathbb{R}$. It remains to prove that θ is rational. Observe that $e(x^N) = e(x)^N = 1$, so $e^{2\pi ik} = e^{2\pi iN\theta}$. Thus $N\theta$ has to be an integer, so we finally obtain $\theta \in \mathbb{Q}$.

□

Often, a group turns out to be isomorphic to its dual group. Recall that an isomorphism of groups is a bijective homomorphism.

Theorem 1.2. All cyclic groups are self-dual if and only if $\mathbb{Z}(N)$ is self-dual for all N.

Proof. Every cyclic group of order N is isomorphic to $\mathbb{Z}(N)$. □

Theorem 1.3. $\mathbb{Z}(N)$ is self-dual for all N.

Proof. We will apply some results from the theory of groups. If we can show that there exists a well-defined homomorphism ϕ from $\mathbb{Z}$ to $\widehat{\mathbb{Z}(N)}$ such that ϕ sends all multiples of N to the identity in $\widehat{\mathbb{Z}(N)}$, then we can apply the first isomorphism theorem for groups.

- *Claim.* $\phi_N : \mathbb{Z} \to \widehat{\mathbb{Z}(N)}$ given by $\phi_N(n) = e_n$ is a well-defined homomorphism of Abelian groups.

  Proof. Let $n, m \in \mathbb{Z}$. Then for all $k \in \mathbb{Z}(N)$,

$$\begin{aligned}
\phi_N(n+m)(k) = e_{n+m}(k) &= \exp(2\pi i(n+m)k/N) && (1)\\
&= \exp(2\pi ink/N + 2\pi imk/N) && (2)\\
&= \exp(2\pi ink/N)\exp(2\pi imk/N) && (3)\\
&= e_n(k)e_m(k) = \phi_N(n)(k)\cdot\phi_N(m)(k). && (4)
\end{aligned}$$

  We have $\phi_N(n+m) = \phi_N(n)\cdot\phi_N(m)$, so ϕ_N is a homomorphism.

- *Claim.* $\ker \phi_N = N\mathbb{Z}$.

  Proof. Let $r \in N\mathbb{Z}$, so $r = Nt$ for some $t \in \mathbb{Z}$. Suppose $k \in \mathbb{Z}(N)$.

$$\phi_N(r)(k) = e_r(k) = \exp(2\pi irk/N) \tag{5}$$

$$= \exp(2\pi iNtk/N) = \exp(2\pi itk) = 1 \tag{6}$$

$$= e_N(k). \tag{7}$$

  We now have that e_r is the trivial character e_N, the identity element of $\widehat{\mathbb{Z}(N)}$. Thus we have $N\mathbb{Z} \subseteq \ker \phi_N$. Suppose e_r is trivial. The above steps are reversible, thus we conclude that $\ker \phi_N = N\mathbb{Z}$. By the first group isomorphism theorem, $\mathbb{Z}/N\mathbb{Z} = \mathbb{Z}(N) \simeq \widehat{\mathbb{Z}(N)}$.

□

1.3 Complex-valued functions on G

Given some arbitrary complex-valued function f on G, one may find it useful to describe f with respect to characters on G. This can be done in the setting of linear algebra, where we take V to be the vector space of functions $G \to \mathbb{C}$. One might want to construct a basis for this vector space, and our hope is that the characters on G are such a basis.

Remark. The dimension of V is $|G|$. We can show this by constructing a basis of size $|G|$ for complex-valued functions on G.

Definition 1.4 (Inner Product)**.** If $f, g \in V$, then the *inner product* of f and g is

given by

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

This definition of an inner product is central to the idea of orthogonality and normality.

Definition 1.5. Two vectors v, w in an inner product space V are *orthogonal* if their inner product (v, w) is equal to 0.

Definition 1.6 (Orthonormal)**.** A basis $\mathcal{B}$ of a vector space V is *orthonormal* if all vectors in $\mathcal{B}$ are mutually orthogonal and $(e, e) = 1$ for all $e \in \mathcal{B}$.

Theorem 1.4. The characters of G are an orthonormal basis of V. Equivalently,

1. $(e_i, e_j) = 0$ for all characters $e_i \neq e_j$.
2. $(e, e) = 1$ for all characters $e \in \widehat{G}$.

Proof. See Shakarchi. □

2 The finite Fourier setting

2.1 Motivation

Now that we have that the characters of G form an orthonormal basis of V, we can represent a function $f \in V$ by a linear combination of these basis characters. Note that we can recover our more familiar ordinary Fourier series definitions by defining the Abelian group to be $\mathbb{Z}(N)$, and letting N approach infinity.

2.2 Finite Fourier series

Definition 2.1 (Fourier Coefficient)**.** The *Fourier coefficient of f with respect to a character e* is defined:

$$\hat{f}(e) = (f, e) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{e(a)}.$$

Definition 2.2 (Fourier Series)**.** We can write f as a linear combination of elements of $\widehat{G}$.

$$\sum_{e \in \hat{G}} \hat{f}(e)e.$$

Example 2.1 (Finite Fourier series over $G \coloneqq \mathbb{Z}(2)$)**.** Let $G \coloneqq \mathbb{Z}(2)$. Note that the order of G is 2. Let f be a function from G to $\mathbb{C}$ given by:

$$f(n + 2\mathbb{Z}) = ne^{2\pi i n/2}$$

where n is the unique smallest representative $0 \leq n \leq 1$ of $n + 2\mathbb{Z}$.

Since all characters of G are of the form $e_l(k) = e^{2\pi i l k/2}$, the finite Fourier coefficients of f with respect to the two $\mathbb{Z}(2)$–characters e_0 and e_1 are given by

$$\hat{f}(e_0) = (f, e_0) = \sum_{a \in G} f(a)\overline{e_0(a)} \tag{8}$$

$$= \sum_{a \in G} ae^{2\pi i a/2}\overline{e^0} \tag{9}$$

$$= \sum_{a \in G} ae^{\pi i a} = 0 + (-1) = -1. \tag{10}$$

$$\hat{f}(e_1) = (f, e_1) = \sum_{a \in G} f(a)\overline{e_1(a)} \tag{11}$$

$$= \sum_{a \in G} a e^{2\pi i a/2} e^{-2\pi i (1) a/2} \tag{12}$$

$$= \sum_{a \in G} a e^{2\pi i a/2 - 2\pi i a/2} \tag{13}$$

$$= \sum_{a \in G} a = 0 + 1 = 1. \tag{14}$$

We obtain a finite Fourier series for f:

$$f = -e_0 + e_1.$$

Remark. The fundamental theorem of finite Abelian groups states that every finite Abelian group is isomorphic to a direct product of cyclic groups. This implies that the dual group of G is isomorphic to the dual group of $\mathbb{Z}_{q_1} \oplus \ldots \oplus \mathbb{Z}_{q_n}$. Thus, a finite Fourier series over *any* Abelian group G is the same as a finite Fourier series over a direct product of cyclic groups.

We will demonstrate an example of a finite Fourier series of a function on a non-cyclic Abelian group.

Example 2.2 (Finite Fourier series over $G := \mathbb{Z}(2) \oplus \mathbb{Z}(2)$)**.** G has order 4, so $\chi(a)^4 = 1$ for any $a \in G$. Thus $\chi(a)$ will only take on values $\{\pm 1, \pm i\}$. So we have a character table for the dual group of G:

Let $f : G \to \mathbb{C}$ given by $f(a, b) = a + bi$. We will compute each Fourier coefficient,

	(0,0)	(1,0)	(0,1)	(1,1)
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	-1	$-i$	i
χ_3	1	i	-1	$-i$

using values from the above table.

$$\hat{f}(\chi_0) = 2 + 2i \tag{15}$$

$$\hat{f}(\chi_1) = -2 \tag{16}$$

$$\hat{f}(\chi_2) = -1 - i \tag{17}$$

$$\hat{f}(\chi_3) = -1 - i \tag{18}$$

Therefore we have a finite Fourier series for f:

$$f = (2 + 2i)\chi_0 - 2\chi_1 + (-1 - i)\chi_2 + (-1 - i)\chi_3.$$

3 Applications

Definition 3.1 (Convolution)**.** If f, g are complex-valued functions on G, the *convolution* of f and g is another function $G \to \mathbb{C}$ defined, for all $a \in G$:

$$(f * g)(a) = \frac{1}{|G|} \sum_{b \in G} f(b) g(a \cdot b^{-1})$$

Example 3.1 (Fourier coefficients of convolutions)**.** In ordinary Fourier analysis, convolution and multiplication are intertwined. We have a similar situation in finite

Fourier analysis.

For all $e \in \widehat{G}$, we claim

$$\widehat{(f * g)}(e) = \hat{f}(e)\hat{g}(e).$$

Proof. Consider the finite Fourier coefficient of the convolution $f * g$ with respect to e.

$$\widehat{(f * g)}(e) = (f * g, e) = \frac{1}{|G|} \sum_{a \in G} (f * g)(a)\overline{e(a)} \tag{19}$$

$$= \frac{1}{|G|} \sum_{a \in G} \left(\frac{1}{|G|} \sum_{b \in G} f(b)g(a \cdot b^{-1}) \right) \overline{e(a)} \tag{20}$$

$$= \frac{1}{|G|^2} \sum_{a \in G} \sum_{b \in G} f(b)g(ab^{-1})\overline{e(a)}. \tag{21}$$

We perform a change of variables $(a, b) \mapsto (b, a)$, then $(a, b) \mapsto (a, ab)$to obtain:

$$\widehat{(f * g)}(e) = \frac{1}{|G|^2} \sum_{a \in G} \sum_{b \in G} f(a)g(b)\overline{e(ab)} \tag{22}$$

Now consider the product of the finite Fourier coefficients of$f$ and g with respect to the same e:

$$\hat{f}(e)\hat{g}(e) = (f, e)(g, e) = \left(\frac{1}{|G|} \sum_{a \in G} f(a)\overline{e(a)} \right) \left(\frac{1}{|G|} \sum_{b \in G} f(b)\overline{e(b)} \right). \tag{23}$$

Because characters are group homomorphisms, we can write $e(a)e(b)$ as $e(ab)$. Thus, we have:

$$\hat{f}(e)\hat{g}(e) = \frac{1}{|G|^2} \sum_{a \in G} \sum_{b \in G} f(a)g(b)\overline{e(ab)}. \tag{24}$$

QED. □

4 The Discrete Fourier Transform, a Fast Algorithm for its Computation, and some Applications

4.1 The Discrete Fourier Transform

We begin by introducing the discrete Fourier transform. Suppose we have some finite sequence of complex numbers $\{c_i\}_{0 \leq i \leq N-1}$ (or perhaps we have a sequence of real numbers $\{r_i\}_{i \leq N}$, in which case we consider it to be the complex sequence $\{r_i + 0i\}_{i \leq N} = \{c_i\}_{0 \leq i \leq N-1}$), and we are interested in analyzing this sequence in terms of the *frequencies* that make it up rather than the *samples* (value at index j) that make it up. We index the values starting at zero and going up to $N - 1$ to each the implementation of this algorithm using arrays (as arrays start their indexing at the "0th" index, not the "1st"). Thus we wish to create some function such that when evaluated on the samples, becomes a sum in terms of combinations of sin and/or cos and an inverse function that transforms these combinations of sin and cos back into

the samples. Consider the following:

$$\{F_k\} = \{\sum_{j=0}^{N-1} c_j e^{-\frac{2\pi ijk}{N}}\}_{0\leq k\leq N-1}$$

Then our equation transforms each our sequence $\{c_j\}_{0\leq j\leq N-1}$ of length N into a new sequence $\{F_k\}_{0\leq k\leq N-1}$ of length N, whose use shall soon be made clear. Observe that since each F_k is a sum of products, if consider our $\{c_i\}_{0\leq i\leq N-1}$ to be an N-dimensional column vector, we can represent the function that transforms $\{c_i\}_{0\leq i\leq N-1}$ to $\{F_k\}_{0\leq k\leq N-1}$ with the following matrix:

$$\begin{bmatrix} e^{-\frac{2\pi i(0)(0)}{N}} & e^{-\frac{2\pi i(1)(0)}{N}} & \cdots & e^{-\frac{2\pi i(j)(0)}{N}} & \cdots & e^{-\frac{2\pi i(N-1)(0)}{N}} \\ e^{-\frac{2\pi i(0)(1)}{N}} & e^{-\frac{2\pi i(1)(1)}{N}} & \cdots & e^{-\frac{2\pi i(j)(1)}{N}} & \cdots & e^{-\frac{2\pi i(N-1)(1)}{N}} \\ \vdots & \vdots & \ddots & & & \vdots \\ e^{-\frac{2\pi i(0)(k)}{N}} & e^{-\frac{2\pi i(1)(k)}{N}} & & e^{-\frac{2\pi i(j)(k)}{N}} & & e^{-\frac{2\pi i(N-1)(k)}{N}} \\ \vdots & \vdots & & & \ddots & \vdots \\ e^{-\frac{2\pi i(0)(N-1)}{N}} & e^{-\frac{2\pi i(1)(N-1)}{N}} & \cdots & e^{-\frac{2\pi i(j)(N-1)}{N}} & \cdots & e^{-\frac{2\pi i(N-1)(N-1)}{N}} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_j \\ \vdots \\ c_{N-1} \end{bmatrix} = \begin{bmatrix} F_0 \\ F_1 \\ \vdots \\ F_k \\ \vdots \\ F_{N-1} \end{bmatrix}$$

Thus it should now be clear that the function which transforms a sequence of N many complex numbers to their F-coefficients is linear, due to it having a well-behaved matrix representation. Henceforth, we will call the function which transforms a sequence of N many complex numbers to their F-coefficients D_N, and will generally use its matrix representation. Now that we have a matrix, a natural question to ask of it is: is it invertible? We use the following theorem:

Theorem 4.1. Vectors of the form $\begin{bmatrix} e^{-\frac{2\pi i(h)(0)}{N}} & e^{-\frac{2\pi i(h)(1)}{N}} & \cdots & e^{-\frac{2\pi i(h)(j)}{N}} & \cdots & e^{-\frac{2\pi i(h)(N-1)}{N}} \end{bmatrix}$

are orthogonal.

Proof. Suppose we have vectors: $\begin{bmatrix} e^{-\frac{2\pi i(h)(0)}{N}} & e^{-\frac{2\pi i(h)(1)}{N}} & \cdots & e^{-\frac{2\pi i(h)(j)}{N}} & \cdots & e^{-\frac{2\pi i(h)(N-1)}{N}} \end{bmatrix}$, $\begin{bmatrix} e^{-\frac{2\pi i(h')(0)}{N}} & e^{-\frac{2\pi i(h')(1)}{N}} & \cdots & e^{-\frac{2\pi i(h')(j)}{N}} & \cdots & e^{-\frac{2\pi i(h')(N-1)}{N}} \end{bmatrix}$. Then:

$$\begin{bmatrix} e^{-\frac{2\pi i(h)(0)}{N}} & e^{-\frac{2\pi i(h)(1)}{N}} & \cdots & e^{-\frac{2\pi i(h)(j)}{N}} & \cdots & e^{-\frac{2\pi i(h)(N-1)}{N}} \end{bmatrix}^T * \begin{bmatrix} e^{-\frac{2\pi i(h')(0)}{N}} & e^{-\frac{2\pi i(h')(1)}{N}} & \cdots & e^{-\frac{2\pi i(h')(j)}{N}} & \cdots & e^{-\frac{2\pi i(h')(N-1)}{N}} \end{bmatrix}$$

$$=$$

$$\sum_{n=0}^{N-1} e^{-\frac{2\pi in}{N}(h-h')}$$

If $h = h'$, then

$$\sum_{n=0}^{N-1} e^{-\frac{2\pi in}{N}(h-h')} = \sum_{n=0}^{N-1} e^{-\frac{2\pi in}{N}(0)} = \sum_{n=0}^{N-1} 1 = N$$

Suppose $h \neq h'$. Observe that $h - h'$ is an integer, thus $\sum_{n=0}^{N-1} e^{-\frac{2\pi in}{N}(h-h')}$ is a sum of the N-th primitive roots of unity, thus are the sum of the solutions of the following equation: $x^N - 1 = 0$. This can be expresses as the equivalent system of equations:

$$\begin{cases} a_N x^N + a_{N-1} x^{N-1} + 1 & = 0 \\ a_N & = 1 \\ a_{N-1} & = 0 \end{cases}$$

. We cite Viète's theorem (Encyclopedia of Mathematics) to conclude that

$$\sum_{n=0}^{N-1} e^{-\frac{2\pi in}{N}(h-h')} = \frac{a_{N-1}}{a_N} = \frac{0}{1} = 0$$

□

Thus each of the row vectors of D_N's matrix representation is orthogonal to each other row vector, thus the rows are independent, thus D_N is invertible. Moreover, from this orthogonality condition, we can easily derive the inverse matrix by guess-and-check. Try:

$$D'_N := \begin{bmatrix} e^{\frac{2\pi i(0)(0)}{N}} & e^{\frac{2\pi i(1)(0)}{N}} & \cdots & e^{\frac{2\pi i(j)(0)}{N}} & \cdots & e^{\frac{2\pi i(N-1)(0)}{N}} \\ e^{\frac{2\pi i(0)(1)}{N}} & e^{\frac{2\pi i(1)(1)}{N}} & \cdots & e^{\frac{2\pi i(j)(1)}{N}} & \cdots & e^{\frac{2\pi i(N-1)(1)}{N}} \\ \vdots & \vdots & \ddots & & & \vdots \\ e^{\frac{2\pi i(0)(k)}{N}} & e^{\frac{2\pi i(1)(k)}{N}} & & e^{\frac{2\pi i(j)(k)}{N}} & & e^{\frac{2\pi i(N-1)(k)}{N}} \\ \vdots & \vdots & & & \ddots & \vdots \\ e^{\frac{2\pi i(0)(N-1)}{N}} & e^{\frac{2\pi i(1)(N-1)}{N}} & \cdots & e^{\frac{2\pi i(j)(N-1)}{N}} & \cdots & e^{\frac{2\pi i(N-1)(N-1)}{N}} \end{bmatrix}$$

Note that the signs have been swapped (and thus we are taking the multiplicative inverses of each entry), and since D_N is symmetric along the $(1,1) \to (N,N)$ axis the j-th row of D_N is equal to the j-th column of D'_N. Thus the q,p-th entry of the matrix $D_N D'_N$ is: $\sum_{n=0}^{N-1} e^{-\frac{2\pi inq}{N}} e^{\frac{2\pi inp}{N}} = \sum_{n=0}^{N-1} e^{\frac{2\pi in}{N}(p-q)} = \begin{cases} N & p = q \\ 0 & p \neq q \end{cases}$ by the above orthogonality proof. Thus:

$$D_N D'_N = \begin{bmatrix} N & 0 & \cdots & 0 \\ 0 & N & & \\ \vdots & & \ddots & \\ 0 & & & N \end{bmatrix} = NI_N$$

with I_N being the $N \times N$ identity matrix. Thus it is now clear that $\frac{1}{N} D'_N$ is the inverse matrix of D_N. Citing the Euler identity:

$$e^{\frac{2k}{N}\pi i} = \cos(\frac{2k}{N}\pi) + i\sin(\frac{2k}{N}\pi)$$

We can now finally understand what $\{F_k\}$ is in relation to $\{c_j\}$: since

$$\frac{1}{N} D_N D'_N = I_N$$

and

$$D_N \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_j \\ \vdots \\ c_{N-1} \end{bmatrix} = \begin{bmatrix} F_0 \\ F_1 \\ \vdots \\ F_k \\ \vdots \\ F_{N-1} \end{bmatrix}$$

holds, we can now derive:

$$\frac{1}{N} D'_N D_N \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_j \\ \vdots \\ c_{N-1} \end{bmatrix} = \frac{1}{N} D'_N \begin{bmatrix} F_0 \\ F_1 \\ \vdots \\ F_k \\ \vdots \\ F_{N-1} \end{bmatrix} \Longrightarrow \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_j \\ \vdots \\ c_{N-1} \end{bmatrix} = \frac{1}{N} D'_N \begin{bmatrix} F_0 \\ F_1 \\ \vdots \\ F_k \\ \vdots \\ F_{N-1} \end{bmatrix}$$

Thus finally we know that:

$$c_j = \frac{\sum_{k=0}^{N-1} F_k e^{\frac{2\pi ijk}{N}}}{N} = \frac{\sum_{k=0}^{N-1} F_k \left(\cos(\frac{2\pi jk}{N}) + i\sin(\frac{2\pi jk}{N})\right)}{N}$$

That is to say, we have decomposed every c_j into a sum of trigonometric functions whose amplitude at the k-th summand is specified by F_K and whose frequency at each summand is specified by jk. Now we can finally investigate $\{c_j\}$ in terms of its constituent *frequencies* and their *amplitudes* instead of its constituent *samples*.

4.1.1 Computing an example DFT and inverse matrix

Suppose we wish to compute the DFT of the following sequence of complex numbers: $\{1+4i, 6+12i, 4-8i\}$. Then we use the matrix product:

$$\begin{bmatrix} e^{-\frac{2\pi i(0)(0)}{3}} & e^{-\frac{2\pi i(0)(1)}{3}} & e^{-\frac{2\pi i(0)(2)}{3}} \\ e^{-\frac{2\pi i(1)(0)}{3}} & e^{-\frac{2\pi i(1)(1)}{3}} & e^{-\frac{2\pi i(1)(2)}{3}} \\ e^{-\frac{2\pi i(2)(0)}{3}} & e^{-\frac{2\pi i(2)(1)}{3}} & e^{-\frac{2\pi i(2)(2)}{3}} \end{bmatrix} \begin{bmatrix} 1+4i \\ 6+12i \\ 4-8i \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{-\frac{2\pi i}{3}} & e^{-\frac{4\pi i}{3}} \\ 1 & e^{-\frac{4\pi i}{3}} & e^{-\frac{8\pi i}{3}} \end{bmatrix} \begin{bmatrix} 1+4i \\ 6+12i \\ 4-8i \end{bmatrix} =$$

$$= \begin{bmatrix} 1+4i+6+12i+4-8i \\ 1+4i+(6+12i)\,e^{-\frac{2\pi i}{3}}+(4-8i)\,e^{-\frac{4\pi i}{3}} \\ 1+4i+(6+12i)\,e^{-\frac{4\pi i}{3}}+(4-8i)\,e^{-\frac{8\pi i}{3}} \end{bmatrix}$$

$$= \begin{bmatrix} 11-8i \\ -4+10\sqrt{3}+i(2-\sqrt{3}) \\ -4+10\sqrt{3}+i(2+\sqrt{3}) \end{bmatrix}$$

And apply our inverse formula:

$$\frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \\ 1 & e^{\frac{4\pi i}{3}} & e^{\frac{8\pi i}{3}} \end{bmatrix} \begin{bmatrix} 11-8i \\ -4+10\sqrt{3}+i(2-\sqrt{3}) \\ -4+10\sqrt{3}+i(2+\sqrt{3}) \end{bmatrix} =$$

$$
\begin{aligned}
&= \frac{1}{3}\begin{bmatrix} 11-8i+\left(-4+10\sqrt{3}+i(2-\sqrt{3})\right)+\left(-4+10\sqrt{3}+i(2+\sqrt{3})\right) \\ 11-8i+\left(-4+10\sqrt{3}+i(2-\sqrt{3})\right)e^{\frac{2\pi i}{3}}+\left(-4+10\sqrt{3}+i(2+\sqrt{3})\right)e^{\frac{4\pi i}{3}} \\ 11-8i+\left(-4+10\sqrt{3}+i(2-\sqrt{3})\right)e^{\frac{4\pi i}{3}}+\left(-4+10\sqrt{3}+i(2+\sqrt{3})\right)e^{\frac{8\pi i}{3}} \end{bmatrix} \\
&= \frac{1}{3}\begin{bmatrix} 3+12i \\ 18+36i \\ 12-24i \end{bmatrix}
\end{aligned}
$$

As desired.

4.2 A fast algorithm for the Computation of the DFT (aka an FFT)

Now that we know that the Discrete Fourier Transform is powerful and useful, we may wish to compute the DFT of some specific sequence of real or complex numbers with length N. If we do this naïvely by simply following the above equation, we perform N^2-many computations of roots of unity, N^2-many products of elements in our sequence by roots of unity, and $(N-1)^2$ many sums of the resulting products. This gives us a computational complexity (number of required operations to follow the naïve procedure) of $O(3N^2-2N+1)$. Anyone who is concerned about writing fast, efficient code knows that $O(n^2)$-time is generally considered very bad. Thus, we wish to find a way to compute the Discrete Fourier Transform in a faster manner - enter the Fast Fourier Transform. Recall that we defined the Fourier coefficients in the following manner:

$$F_k = \sum_{j=0}^{N-1} c_j e^{-\frac{2\pi i j k}{N}}$$

Suppose $N = 2^w$ for some $w \in \mathbb{N}$. Now we can perform the following trick:

$$F_k = \sum_{j=0}^{\frac{N}{2}-1} c_{2j} e^{-\frac{2\pi i (2j) k}{N}} + \sum_{j=0}^{\frac{N}{2}-1} c_{2j+1} e^{-\frac{2\pi i (2j+1) k}{N}}$$

By reindexing. Then we can pull out a factor on the rightmost term and:

$$F_k = \sum_{j=0}^{\frac{N}{2}-1} c_{2j} e^{-\frac{2\pi i (j) k}{\frac{N}{2}}} + e^{-\frac{2\pi i k}{N}} \sum_{j=0}^{\frac{N}{2}-1} c_{2j+1} e^{-\frac{2\pi i (j) k}{\frac{N}{2}}}$$

Now we've reexpressed F_k, which used to take N many operations to produce roots of unity, N many products, and $N-1$ many sums as instead a product and a sum over two DFTs of size $\frac{N}{2}$. Repeating this trick recursively on $\sum_{j=0}^{\frac{N}{2}-1} c_{2j} e^{-\frac{2\pi i (j) k}{\frac{N}{2}}}$ and $\sum_{j=0}^{\frac{N}{2}-1} c_{2j+1} e^{-\frac{2\pi i (j) k}{\frac{N}{2}}}$ splits computing F_k into $\log_2(N)$ many summands, with each summand being a Fourier transform of 2 elements. Thus, now we instead have reduced the complexity to $\log_2(N)-1$ many computations of roots of unity plus $\log_2(N)-1$ many products plus $\log_2(N)-1$ many sums times the cost of computing a Fourier transform of 2 elements. Thus our new cost is: $O(3(\log_2(N)-1)(2(2^2)-2(2)+1)) = O(15\log_2(N)-15)$. This is significantly smaller, especially for large inputs. If we want to, for example, compute the Fourier transform of a sequence with $1,048,576$ entries, computing it in the naïve way costs $\frac{3(1,048,576)^2-2(1,048,576)+1}{15\log_2(1,048,576)-15} \approx 1,150,000,000,000$ times many more computations to perform than in this "fast" way.

4.3 A cute application for finding "new" primes computationally

Consider the following very important sequence:

$$\{a_n \in \{0,1\} : \begin{cases} a = 1 & a \text{ is prime} \\ a = 0 & a \text{ isn't prime} \end{cases} \}_{n \in \mathbb{N}}$$

Obviously, if this sequence were known, the distribution of primes would be known, and the general distribution of primes is not known. However, the general scientific community does know the first $2^{43,112,609} - 1$-many primes, which is very many indeed. If we take the Discrete Fourier Transform of the first $m < 2^{43,112,609} - 1$ many elements of this sequence, we get a number of Fourier coefficients, and their evaluation at indices higher than $2^{43,112,609} - 1$ won't predict for sure whether or not that number is prime but if their evaluation at point q is very close to 1, then *it is likely* q is prime or very close to a prime. Likewise, if their evaluation at point q is very close to 0, the it is likely that q isn't prime or very close to a prime. Likewise, one could also take the Fourier transform of the sequence:

$$\{\phi_n = \sum_{i=1}^{n} a_i\}_{n \in \mathbb{N}}$$

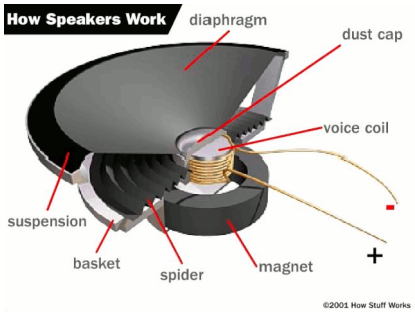
which counts how many primes are below or equal to n, which is of importance in cryptography as well as understanding the distribution of primes. Modifications of both of these ideas that use a slightly more complicated version of the Fourier

transform and that take into account some other known properties of the primes are used both to find patterns in the distribution of primes and to find likely candidates for brute-force computational methods of finding new primes (Tao).

4.4 An informal discussion of the use of the Fourier transform in encoding music

Digital music and sound reproduction is an important part of many people's everyday lives and a large industry. Digital music is reproduced by speakers and headphones, both of which work off of the same basic pattern: electricity is pipped at a certain strength through a wire in one direction or another. This causes an electromagnet mounted on the skin of a drumskin (called the "diaphragm") to be either attracted towards or repulsed away from a magnet nearby. This drumskin moving back and forth causes to air vibrate, recreating the desired sounds. The following diagram illustrates this nicely (PGS Physics):

Figure 1:



Thus, the actual underlying information that is somehow encoded in a music file is literally just instructions on how strong the electrical current going through the

wires should be and if the current should be going one way or the other. Thus, music can be (and in "plain" formats, is) encoded as just long finite sequences of integers, with the absolute values of these integers dictating the strength of the current and the sign of the number dictating the direction of the current. In fact, this is exactly how CDs encode music - they have some metadata fluff containers around just sequences of 44100/second 32-bit integers. However, this takes up a lot of space. Thus, it is desirable to be able to cheaply compress music in a way that is generally "transparent" (i.e. one cannot tell the difference from the uncompressed version) and cheap. Enter the MP3 format, a format that is so pervasive most people think it is a synonym for "digital music" rather than a manner of encoding digital music. There are several technical details of how mp3's work that are not related to how they encode music data that will be mostly ignored in this treatment. We begin with a CD "song" that is 5 minutes long. Thus the actual information is (5)(60)44100 = 13230000 many integers in a sequence $\{a_i\}_{0\leq i\leq 13230000-1}$. For the first 576 many samples $\{a_i\}_{o\leq i\leq 575}$, we compute a DFT of those samples and obtain a new sequence $\{F_i\}_{0\leq i\leq 576}$. We then use psychoacoustics to combine elements with similar frequencies (that is, near indices) into new frequencies that are largely indistinguishable to the human ear and delete frequencies that have very low amplitude (that is, their F_i is a relatively small integer) and obtain a new sequence $\{F'_j\}_{0\leq j<<<576}$. Now the new encoding doesn't *exactly* decode to $\{a_i\}_{0\leq i\leq 575}$, but it decodes to something very close. Once we're done with the first 576 samples, we write a new header file and do the same to the $577th - 1152th$ samples etc. MP3 files generally encode to having $\frac{1}{5}$th to $\frac{1}{7}$th the size of the original CD format, with most people being unable to tell the difference

between the two.

5 References

- Tao, Terrence. "Structure and Randomness in the Prime numbers". https://terrytao.files.wordpress.com/2009/09/structure-and-randomness-in-the-prime-numbers.ppt
- Shakarchi, Rami & Stein, Elias. "Fourier Analysis: an Introduction". 2003.
- Viète theorem. Encyclopedia of Mathematics. http://www.encyclopediaofmath.org/index.php?title=Vi%C3%A8te_theorem&oldid=23172
- PGS Physicis. Retrived 25th April 2019. https://sites.google.com/a/perthgrammar.co.uk/physics/courses/s3-physics/12-how-is-sound-made