The Fast Fourier Transform

1 Complex Numbers

A *complex number*, or *Gaussian number*, is an ordered pair of real numbers (a, b), together with the following operations.

1. (Addition) $(a, b) + (c, d) = (a + c, b + d)$.
2. (Multiplication) $(a, b)(c, d) = (ac - bd, ad + bc)$.

Write $\mathbb{C}$ for the system of all complex numbers, together with the two operations of addition and multiplication.

Lemma 1.1

(a) *$\mathbb{C}$ is a field. More specifically:*

1. *The additive identity is $(0, 0)$.*
2. *The additive inverse of (a, b) is $(-a, -b)$.*
3. *The multiplicative identity is $(1, 0)$.*
4. *If $(a, b) \neq (0, 0)$, the multiplicative inverse of (a, b) is $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2,b^2}\right)$.*
5. *$\mathbb{C}$ satisfies the field axioms.*

(b) *The field of real numbers, $\mathbb{R}$, embeds in $\mathbb{C}$ by $x \mapsto (x, 0)$.*

By a slight abuse of notation, we will consider $\mathbb{R}$ to be a subfield of $\mathbb{C}$, by identifying the real number x with the complex number $(x, 0)$. We assign the special name $\mathbf{i} = (0, 1)$. Thus, we can write the complex number (a, b) as $a + b\mathbf{i}$; we call this *standard form*.

If $z = a + b\mathbf{i}$ is any complex number, we write

1. $|z| = \sqrt{a^2 + b^2}$, the *absolute value* of z.
2. $\bar{z} = a - b\mathbf{i}$, the *conjugate* of z.

Lemma 1.2 *For any $z \in \mathbb{C}$, $z\bar{z} = |z|^2$*

For any integer $n > 0$ and any integer i, define $\omega_n^i = \cos\left(\frac{2\pi i}{n}\right) + \mathbf{i}\sin\left(\frac{2\pi i}{n}\right)$.

Lemma 1.3 *For any $n \geq 1$ and any integer i:*

(a) $|\omega_n^i| = 1$.

(b) $\overline{\omega_n^i} = \omega_n^{-i}$.

(c) $\omega_n^i = \omega_n^j$ *if and only if $j - i$ is a multiple of n.*

(d) *There are exactly n solutions to the equation $z^n = 1$, namely ω_n^i for all $0 \leq i < n$. We call these the n^{th}* roots of unity*, and $\omega_n = \omega_n^1$ is called the* principle n^{th} root of unity*.*

(e) $(\omega_n^i)^j = \omega_n^{ij}$.

(f) *For any positive integer p, $\omega_{np}^{ip} = \omega_n^i$.*

2 The Polynomial Ring $\mathbb{C}[x]$

Let $\mathbb{C}[x]$ be the set of polynomial in one formal variable, x, with coefficients in the complex numbers $\mathbb{C}$. It is important to note that x is not a number, but rather, is what we call a *formal variable.*

The objects of $\mathbb{C}[x]$ are polynomials of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $n \geq 0$ is an integer and each a_i is a complex number. If $f(x) \in \mathbb{C}[x]$, we can also think of f as being a function from $\mathbb{C}$ to $\mathbb{C}$.

$\mathbb{C}[x]$ admits addition and multiplication, both defined in the usual "high school algebra" way, but not division. We define the *degree* of a polynomial f to be the index of the largest non-zero coefficient of x; thus, we would say that $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ has degree n if $a_n \neq 0$.

Remark 2.1 *If $f(x), g(x) \in \mathbb{C}[x]$, then the degree of $f(x)g(x)$ is the sum of the degrees of $f(x)$ and $g(x)$.*

2.1 Point-Value Representation of Polynomials

We will use the following well-known lemma:

Lemma 2.2 *If f is a polynomial function and $f(u) = 0$, then $f(x) = (x - u)g(x)$ for some polynomial function g.*

Define $\mathbb{C}^n[x]$ to be the set of all polynomials of degree *less* then n over $\mathbb{C}$. If $f(x) \in \mathbb{C}^n[x]$, then $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$. The *coefficient* representation of $f(x)$ is the vector $(a_0, a_1, a_2, \ldots a_{n-1})$.

A polynomial can be characterized by its values at a list of points of $\mathbb{C}$, provided the number of those points is at least one larger than the degree of the polynomial.

Let $U = (u_0, u_1, \ldots, u_{n-1})$ be a list of distinct points of length n. If f is any function, write $f(U) = (f(u_0), f(u_1), \ldots, f(u_{n-1}))$.

Lemma 2.3 *If $U = (u_0, u_1, \ldots, u_{n-1})$ is a list of distinct points of $\mathbb{C}$ of length n, and Let $V = (v_0, v_1, \ldots, v_{n-1})$ be a list of points of $\mathbb{C}$ of length n. Then there is exactly one polynomial f of degree less than n such that $f(U) = V$.*

Proof: Let

$$f(x) = \sum_{j=0}^{n-1} \left(\frac{v_j \prod_{k \neq j}(x - u_k)}{\prod_{k \neq j}(u_j - u_k)} \right)$$

Trivially, $f(U) = V$.

To prove uniqueness, assume that g is another polynomial function of degree less than n, such that $g(U) = V$. Let $h(x) = f(x) - g(x)$. Thus, $h(u_j) = 0$ for all j. By Lemma 2.2, $h(x)$ is divisible by the polynomial $\prod_{j=0}^{n-1}(x - u_j)$, which has degree n. But the degree of h must be less than n. The only possibility is that $h(x) = 0$, and we are done. $\square$

If U is a fixed list of distinct points of length n, then a polynomial $f \in \mathbb{C}^n$ can be characterized either by the list of its coefficients or its point-value list $f(U)$. Henceforth, we will always let $U = \Omega_n = (1, \omega_n, \omega_n^2, \ldots \omega_n^{n-1})$, the list consisting of the n^{th} roots of unity.

If $f(U) = V$, the process of computing V from the list of coefficients of f is called *evaluation*, while the process of computing the list of coefficients of f from V is called *interpolation*.

2.2 Preliminaries

We will always assume that n is a power of 2, since we can pad a polynomial with zero terms if necessary.

Divide and Conquer. If $f = \sum_{j=0}^{n-1} a_j x^j$ is a polynomial, for $n > 1$ a power of 2, we define polynomials ${}^0f$ and ${}^1f$ as follows:

$$\begin{aligned} {}^0f(x) &= \sum_{j=0}^{n/2-1} a_{2j} x^j \\ {}^1f(x) &= \sum_{j=0}^{n/2-1} a_{2j+1} x^j \end{aligned}$$

We can characterize these two polynomials by the conditions that each has degree less than $n/2$, and that $f(x) = {}^0f(x^2) + x\ {}^1f(x^2)$.

Let $f \in \mathbb{C}^n$. We can recursively compute $f(\Omega_n)$ as follows.

- If $n = 1$, then $f(x) = a_0$, a constant function, $\Omega_1 = (1)$ and $f(\Omega_1) = (a_0)$.
- If $n > 1$, recursively compute ${}^0f(\Omega_{n/2}) = {}^0V = ({}^0v_0,\ {}^0v_1 \ldots,\ {}^0v_{n/2-1})$ and ${}^1f(\Omega_{n/2}) = {}^1V = ({}^1v_0,\ {}^1v_1 \ldots,\ {}^1v_{n/2-1})$. Then $f(\Omega_n) = V = (v_0, v_1, \ldots v_{n-1})$ where

$$v_j = \begin{cases} {}^0v_j + \omega_n^j\ {}^1v_j & \text{if } 0 \leq j < n/2 \\ {}^0v_{j-n/2} + \omega_n^j\ {}^1v_{j-n/2} = {}^0v_{j-n/2} - \omega_n^{j-n/2}\ {}^1v_{j-n/2} & \text{if } n/2 \leq j < n \end{cases}$$

Note that we are actually solving $n/2$ sets of two equations in two unknowns. Reversing the process, we can compute both ${}^0f(\Omega_{n/2})$ and ${}^1f(\Omega_{n/2})$ from $f(\Omega_n)$ as follows. For any $0 \le j < n/2$:

$$ {}^0v_j = \frac{v_j + v_{j+n/2}}{2} $$

$$ {}^1v_j = \frac{v_j - v_{j+n/2}}{2\omega_n^j} $$

also by solving $n/2$ sets of two equations in two unknowns. This gives us a recursive procedure for computing the coefficients of f from $f(\Omega_n)$.

2.3 Implementation Matrix

In matrix shown below, we take $n = 8$, and we let ω denote $\omega_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\mathbf{i}$, the principle eighth root of unity. Then,

$$ \Omega_8 = (\omega^0, \omega^1, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7) = (1, \tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}\mathbf{i}, \mathbf{i}, -\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}\mathbf{i}, -1, -\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}\mathbf{i}, -\mathbf{i}, \tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}\mathbf{i}) $$

${}^{000}f(1)$	${}^{001}f(1)$	${}^{010}f(1)$	${}^{011}f(1)$	${}^{100}f(1)$	${}^{101}f(1)$	${}^{110}f(1)$	${}^{111}f(1)$
${}^{00}f(1)$	${}^{01}f(1)$	${}^{10}f(1)$	${}^{11}f(1)$	${}^{00}f(-1)$	${}^{01}f(-1)$	${}^{10}f(-1)$	${}^{11}f(-1)$
${}^{0}f(1)$	${}^{1}f(1)$	${}^{0}f(\mathbf{i})$	${}^{1}f(\mathbf{i})$	${}^{0}f(-1)$	${}^{1}f(-1)$	${}^{0}f(-\mathbf{i})$	${}^{1}f(-\mathbf{i})$
$f(1)$	$f(\omega)$	$f(\mathbf{i})$	$f(\omega^3)$	$f(-1)$	$f(\omega^5)$	$f(-\mathbf{i})$	$f(\omega^7)$

Let us square $6561 = 1 + 6(10) + 5(10)^2 + 6(10)^3$. We first write the matrix for 6561, starting at the top row.

1	6	5	6	0	0	0	0
1	6	5	6	1	6	5	6
6	12	$1+5\mathbf{i}$	$6+6\mathbf{i}$	-4	0	$1-5\mathbf{i}$	$6-6\mathbf{i}$
18	$1+\left(5+6\sqrt{2}\right)\mathbf{i}$	-4	$1+\left(-5+6\sqrt{2}\right)\mathbf{i}$	-6	$1+\left(5-6\sqrt{2}\right)\mathbf{i}$	-4	$1-\left(5+6\sqrt{2}\right)\mathbf{i}$

We now construct the interpolation matrix. We square each entry in the bottom row of the evaluation matrix to obtain the bottom row of the interpolation matrix. We then fill in the remaining rows, in bottom-up order.

1	12	46	72	97	60	36	0
98	72	82	72	-96	-48	10	72
180	144	$-96+10\mathbf{i}$	$-48+72\mathbf{i}$	16	0	$-96-10\mathbf{i}$	$-48-72\mathbf{i}$
324	$-96-60\sqrt{2}$ $+\left(10+12\sqrt{2}\right)\mathbf{i}$	16	$-96+60\sqrt{2}$ $+\left(-10+12\sqrt{2}\right)\mathbf{i}$	36	$-96+60\sqrt{2}$ $+\left(10-12\sqrt{2}\right)\mathbf{i}$	16	$-96-60\sqrt{2}$ $-\left(10+12\sqrt{2}\right)\mathbf{i}$

We now complete the calculation:

$$\begin{aligned}
6561^2 &= \left(1 + 6(10) + 5(10)^2 + 6(10)^3\right)^2 \\
&= 1 + 12(10) + 46(10)^2 + 72(10)^3 + 97(10)^4 + 60(10)^5 + 36(10)^6 \\
&= 1 + 120 + 4600 + 72000 + 970000 + 6000000 + 36000000 \\
&= 43046721
\end{aligned}$$