FOURIER TRANSFORM NOTES

APRIL 4, 2019

1. The Discrete Fourier Transform

Suppose $1 \leq N \in \mathbb{Z}$. Let $G = \{0, 1, \ldots, N-1\}$ and suppose $f : G \to \mathbb{C}$ is a function. We will always extend such f to functions on $\mathbb{Z}$ by setting $f(j) = f(j + mN)$ for all integers j and m. Let $w = \exp(2\pi\sqrt{-1}/N)$. Then w is a root of unity of order N in the sense that N is the smallest integer such that $w^N = 1$.

For $j \in G$, define $e_j : G \to \{0, 1, \ldots, N-1\}$ by

$$e_j(m) = w^{jm} \tag{1.1}$$

for all m. We define an inner product $\langle\ ,\ \rangle$ on the complex vector space $C(G) = \{f : G \to \mathbb{C}\}$ of all complex functions on G by

$$\langle f, g\rangle = \frac{1}{N}\sum_{m=0}^{N-1} f(m)\overline{g(m)} \tag{1.2}$$

Then $\{e_j\}_{j=0}^{N-1}$ forms an orthonormal basis of $C(G)$.

Every $f \in C(G)$ has a unique expansion as

$$f = \sum_{j=0}^{N-1} \hat{f}(j) e_j \tag{1.3}$$

where $\hat{f} : G \to \mathbb{C}$ is the Fourier transform of f defined by

$$\hat{f}(j) = \langle f, e_j\rangle = \frac{1}{N}\sum_{m=0}^{N-1} f(m) w^{-jm} \tag{1.4}$$

2. Fourier Inversion

Theorem 2.1. *For all $f : G \to \mathbb{C}$ and $j \in \mathbb{Z}$ one has*

$$\hat{\hat{f}}(j) = \frac{1}{N} f(-j) \tag{2.5}$$

Proof. Recall that we extend f to a periodic function on Z by $f(j + mN) = f(j)$ for all $j, m \in \mathbb{Z}$. We now compute

$$\begin{aligned}
\hat{\hat{f}}(j) &= \frac{1}{N}\sum_{m=0}^{N-1} \hat{f}(m) w^{-jm} \\
&= \frac{1}{N}\sum_{m=0}^{N-1} \left(\frac{1}{N}\sum_{k=0}^{N-1} f(k) w^{-mk}\right) w^{-jm} \\
&= \frac{1}{N^2}\sum_{k=0}^{N-1} f(k) \left(\sum_{m=0}^{N-1} w^{-m(k+j)}\right) \\
&= \frac{1}{N^2} f(-j) N \qquad (2.6)
\end{aligned}$$

as claimed. ∎

One consequence of this is that one can recover each of f and $\hat{f}$ from the other in $O(N\log(N))$ steps using the fast Fourier transform discussed in class.

3. Convolution and Fourier Transforms

The convolution $f \star g : G \to \mathbb{C}$ of two functions $f, g \in \mathbb{C}(G)$ is defined by

$$f \star g(j) = \sum_{m=0}^{N-1} f(m)g(j-m) \tag{3.7}$$

where as usual, we extend f, g and $f \star g$ to periodic functions on all of $\mathbb{Z}$.

Theorem 3.1.

$$\widehat{f \star g} = N \cdot \hat{f} \cdot \hat{g}$$

Proof. We compute

$$\begin{aligned}
\widehat{f \star g}(\ell) &= \frac{1}{N}\sum_{j=0}^{N-1} f \star g(j) w^{-j\ell} \\
&= \frac{1}{N}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} f(m)g(j-m)w^{-j\ell} \\
&= \frac{1}{N}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} f(m)g(j-m)w^{-m\ell}w^{-(j-m)\ell} \\
&= \frac{1}{N}\sum_{m=0}^{N-1}\sum_{m'=0}^{N-1} f(m)g(m')w^{-m\ell}w^{-m'\ell} \\
&= N \cdot \left(\frac{1}{N}\sum_{m=0}^{N-1} f(m)w^{-m\ell}\right) \cdot \left(\frac{1}{N}\sum_{m'=0}^{N-1} g(m')w^{-m'\ell}\right) \\
&= N \cdot \hat{f}(\ell) \cdot \hat{g}(\ell) \qquad (3.8)
\end{aligned}$$

□

4. Computing products of polymomials and of integers using the Fourier transform

Suppose

$$F(t) = \sum_{r=0}^{p} a_r t^r \quad \text{and} \quad G(t) = \sum_{s=0}^{q} b_s t^s$$

are two polynomials in the indeterminate t with complex coefficients. Computing the product polynomial

$$F(t) \cdot G(t) = \sum_{u=0}^{p+q} c_u t^u \tag{4.9}$$

the naive way takes at least pq operations. Let's see how to do this in $O((p+q)\cdot \ln(p+q))$ operations using the fast Fourier transform.

Pick $N > p+q$ and define functions $f, g : G = \{0, \ldots, N-1\} \to \mathbb{C}$ by

$$f(r) = a_r \quad \text{if} \quad 0 \le r \le p, \quad f(r) = 0 \quad \text{if} \quad p < r < N$$

and

$$g(s) = b_s \quad \text{if} \quad 0 \le s \le q, \quad g(s) = 0 \quad \text{if} \quad q < s < N. \tag{4.10}$$

We extend f and g to all of $\mathbb{Z}$ in the usual way by making them periodic mod N.

Lemma 4.1. *The coefficient c_u in (4.9) is*

$$c_u = f \star g(u)$$

for $0 \leq u \leq p+q$.

Proof. Define $a_r = 0$ if $p < r$ and let $b_s = 0$ if $q < s$. It's clear that for $0 \leq u \leq p+q$ we have

$$c_u = \sum_{r+s=u,\ r\geq 0,\ s\geq 0} a_r b_s. \tag{4.11}$$

For such u we have

$$f \star g(u) = \sum_{r=0}^{N-1} f(r)g(u-r) = \sum_{r=0}^{p} a_r\ g(u-r) \tag{4.12}$$

since $f(r) = 0$ if $p < r < N$ and $f(r) = a_r$ for $0 \leq r \leq p$.

We claim that to prove the Lemma, it will be enough to show

$$g(u-r) = 0 \quad \text{if} \quad 0 \leq r \leq p < N, \quad 0 \leq u \leq p+q \quad \text{and} \quad u-r < 0. \tag{4.13}$$

If we can show this, then all the terms on the far right side of (4.12) with $s = u - r < 0$ are 0. The non-negative values of $s = u - r$ are exactly those which occur on the right side of (4.11) since for such s, $g(u-r) = g(s) = b_s$ because $0 \leq s = u - r < N$. So we will have shown (4.11) and (4.12) are equal provided we check (4.13).

To show (4.13) note that

$$0 < u - r + N < N \tag{4.14}$$

and by our extension of g to a periodic function mod N we have

$$g(u-r) = g(u-r+N). \tag{4.15}$$

Here

$$u - r + N = N - (r-u) \geq N - p > q \tag{4.16}$$

since $0 \leq r \leq p$ and $u \geq 0$ give $r - u \leq p$ and we have assumed $p + q < N$. So combining (4.14) and (4.16) gives

$$q < u - r + N < N \tag{4.17}$$

We can now apply the definition of the function g in (4.10)to conclude

$$g(u-r) = g(u-r+N) = b_{u-r+N} = 0$$

since $b_s = 0$ for $s > q$. This proves (4.13) and the Lemma. □

Corollary 4.2. *One can compute the product in (4.9) in $O((p+q)\ln(p+q))$ steps.*

Proof. Taking $N = p+q+1$, Lemma 4.1 shows it is enough to find $f \star g$ quickly. We can find $f \star g$ quickly from $\widehat{f \star g} = n \cdot \hat{f} \cdot \hat{g}$. Since $\hat{f}$ and $\hat{g}$ can be computed quickly, this implies the Corollary. □

This result implies one can compute the decimal expansions of product of integers quickly. Namely, suppose we are given integers

$$M = \sum_{r=0}^{p} a_r 10^r \quad \text{and} \quad L = \sum_{s=0}^{q} b_s 10^s$$

with the a_r and b_s in $\{0, \ldots, 9\}$. We write down the corresponding polyomials $F(T)$ and $G(T)$ and compute

$$F(T) \cdot G(T) = \sum_{u=0}^{p+q} c_u t^u = H(T)$$

quickly. Then

$$M \cdot L = H(10) = \sum_{u=0}^{p+q} c_u 10^u. \tag{4.18}$$

Here the c_u are between 0 and $(p+q+1)\cdot 81$ so each c_q has $O(\ln(p+q))$ decimal digits. By induction on n, we see that the decimal expansion of

$$\sum_{u=0}^{n} c_u 10^u$$

can be computed in less than a constant times $n \cdot (p+q+1) \cdot 81$ steps for $0 \leq n \leq p+q$. So the number of operations needed to reduce the right hand side of (4.18) to decimal form is bounded by $O((p+q)\ln(p+q))$.