Discrete Fourier Transform

Tristan Shin

2 May 2020

Disclaimer

The following slides are live-TeX'ed, so there may be typos and errors. Sorry in advance.

Fourier

- Helps with signal processing
- Not talking about general Fourier transform
- Talking about finite sets today
- Talking about the integers mod m
- $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$

Discrete Fourier Transform

Define the **discrete Fourier Transform** of $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ is $\hat{f}\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ satisfying

$$\begin{aligned}\hat{f}(r) &= \frac{1}{m}\sum_{x\in\mathbb{Z}/m\mathbb{Z}} f(x)\omega^{-rx} = \mathbb{E}_x\, f(x)\omega^{-rx} \\ &= \frac{1}{m}\left(f(0) + f(1)\omega^{-r} + f(2)\omega^{-2r} + \cdots + f(m-1)\omega^{-r(m-1)}\right)\end{aligned}$$

where $\omega = e^{i\cdot\frac{2\pi}{m}}$ (so $\omega^m = 1$, so $\omega^{2m+7} = \omega^7$)

Roots of Unity Filter

Problem

Compute

$$\binom{100}{1} + \binom{100}{4} + \binom{100}{7} + \cdots + \binom{100}{100}$$

Consider $(1+X)^{100}$, want coefficients of X^k for $k \equiv 1 \pmod 3$

Plug in $1, \omega, \omega^2$ where $\omega = -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}$

Roots of Unity Filter

$m = 3$

$$\hat{f}(0) = \frac{1}{3}(f(0) + f(1) + f(2))$$
$$\hat{f}(1) = \frac{1}{3}(f(0) + f(1)\omega^{-1} + f(2)\omega^{-2})$$
$$\hat{f}(2) = \frac{1}{3}(f(0) + f(1)\omega^{-2} + f(2)\omega^{-4})$$

If we have a polynomial

$$P(X) = f(0) + f(1)X + f(2)X^2,$$

then $\hat{f}(r) = \frac{1}{3}P(\omega^{-r})$

Roots of Unity Filter

$$\begin{aligned}\hat{f}(0)+\hat{f}(1)+\hat{f}(2) &= \frac{1}{3}(3f(0)+(1+\omega^{-1}+\omega^{-2})f(1) \\ &\quad +(1+\omega^{-2}+\omega^{-4})f(2)) \\ &= f(0)\end{aligned}$$

$\omega^3 = 1$

$$1+\omega^{-2}+\omega^{-4} = \frac{(\omega^{-2})^3-1}{\omega^{-2}-1} = 0$$

Roots of Unity Filter

$$\begin{aligned}
\hat{f}(0) + \hat{f}(1) + \hat{f}(2) &= f(0) \\
\hat{f}(0) + \hat{f}(1)\omega + \hat{f}(2)\omega^2 &= \frac{1}{3}((1 + \omega + \omega^2)f(0) + 3f(1) \\
&\quad + (1 + \omega^{-1} + \omega^{-2})f(2)) \\
&= f(1) \\
\hat{f}(0) + \hat{f}(1)\omega^2 + \hat{f}(2)\omega^4 &= f(2)
\end{aligned}$$

Define

$$Q(X) = \hat{f}(0) + \hat{f}(1)X + \hat{f}(2)X^2,$$

$f(x) = Q(\omega^x)$

$\hat{f}(0)$

$$\hat{f}(0) = \mathbb{E}_x \, f(x)\omega^{-0 \cdot x} = \mathbb{E}_x \, f(x)$$

Inversion

$$
\begin{aligned}
\sum_r \hat{f}(r)\omega^{ry} &= \sum_r \left(\mathbb{E}_x\, f(x)\omega^{-rx}\right)\omega^{ry} \\
&= \mathbb{E}_x \sum_r f(x)\omega^{-rx+ry} \\
&= \mathbb{E}_x\, f(x) \sum_r \omega^{r(y-x)} \\
&= \frac{1}{m}\sum_x f(x)[m \text{ if } y = x\text{, otherwise } 0] \\
&= \frac{1}{m} f(y)\cdot m \\
&= f(y)
\end{aligned}
$$

$$
\boxed{f(x) = \sum_r \hat{f}(x)\omega^{rx}}
$$

Inversion

If $t \not\equiv 0 \pmod{m}$

$$\sum_r \omega^{rt} = 1 + \omega^t + \omega^{2t} + \cdots + \omega^{(m-1)t}$$

$$= \frac{(\omega^t)^m - 1}{\omega^t - 1} = 0$$

It $t \equiv 0 \pmod{m}$

$$\sum_r \omega^{rt} = \sum_r 1 = m$$

Convolution

$$(f * g)(x) = \mathbb{E}_y\, f(y)g(x-y)$$

$$\begin{aligned}
\widehat{f * g}(r) &= \mathbb{E}_x (f*g)(x)\omega^{-rx} \\
&= \mathbb{E}_x \left(\mathbb{E}_y\, f(y)g(x-y)\right)\omega^{-rx} \\
&= \mathbb{E}_y\, \mathbb{E}_x\, f(y)\omega^{-ry} g(x-y)\omega^{-r(x-y)} \\
&= \mathbb{E}_y\, f(y)\omega^{-ry}\, \mathbb{E}_x\, g(x-y)\omega^{-r(x-y)} \\
&= \mathbb{E}_y\, f(y)\omega^{-ry}\, \mathbb{E}_z\, g(z)\omega^{-rz} \\
&= \hat{f}(r)\hat{g}(r)
\end{aligned}$$

$$\boxed{\widehat{f * g} = \hat{f} \cdot \hat{g}}$$

Parseval's Identity

$$\begin{aligned}
\sum_r \hat{f}(r)\overline{\hat{g}}(r) &= \sum_r \left(\mathbb{E}_x\, f(x)\omega^{-rx}\right) \overline{\left(\mathbb{E}_y\, g(y)\omega^{-ry}\right)} \\
&= \sum_r \mathbb{E}_x\, f(x)\omega^{-rx}\, \mathbb{E}_y\, \overline{g}(y)\omega^{ry} \\
&= \mathbb{E}_x\, f(x)\, \mathbb{E}_y\, \overline{g}(y) \sum_r \omega^{r(y-x)} \\
&= \mathbb{E}_x\, f(x)\, \mathbb{E}_y\, \overline{g}(y) [m \text{ if } y = x, \text{ otherwise } 0] \\
&= \mathbb{E}_x\, f(x)\overline{g}(x)
\end{aligned}$$

$$\boxed{\sum_r \hat{f}(r)\overline{\hat{g}}(r) = \mathbb{E}_x\, f(x)\overline{g}(x)}$$

One last property

$$\begin{aligned}
\widehat{\overline{f}}(r) &= \mathbb{E}_x\, \overline{f}(x)\omega^{-rx} \\
&= \overline{\mathbb{E}_x\, f(x)\omega^{rx}} \\
&= \overline{\hat{f}(-r)} = \overline{\hat{f}}(-r)
\end{aligned}$$

$$\hat{f}(r) = \mathbb{E}_x\, f(x)\omega^{-rx}$$

Vectors

Let $f\colon (\mathbb{Z}/m\mathbb{Z})^n \to \mathbb{C}$, for example, we take $(x_1, x_2, \ldots, x_n)$ and output a complex number $f(x_1, x_2, \ldots, x_n)$

Then the DFT is $\hat{f}\colon (\mathbb{Z}/m\mathbb{Z})^n \to \mathbb{C}$ satisfying

$$\hat{f}(\mathbf{r}) = \mathbb{E}_{\mathbf{x}}\, f(\mathbf{x})\omega^{-\mathbf{r}\cdot\mathbf{x}}$$

Here, if $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ and $\vec{x} = (x_1, x_2, \ldots, x_n)$ then

$$\mathbf{r}\cdot\mathbf{x} = r_1x_1 + r_2x_2 + \cdots + r_nx_n$$

All of these identities still hold!

Linearity Testing

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Proposition

For all $\epsilon > 0$, there exists a $\delta > 0$ such that for any function $f\colon \mathbb{F}_p^n \to \mathbb{F}_p$ satsifying

$$\mathbb{P}(f(\mathbf{x}) + f(\mathbf{y}) = f(\mathbf{x} + \mathbf{y})) \geq 1 - \delta,$$

there exists an $\mathbf{a} \in \mathbb{F}_p^n$ such that

$$\mathbb{P}(f(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x}) \geq 1 - \epsilon.$$

If $f(\mathbf{x}) + f(\mathbf{y}) = f(\mathbf{x} + \mathbf{y})$ for all $\mathbf{x}, \mathbf{y}$, then $f(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x}$

Proof combines Fourier tools with complex analysis

Cap Set Problem

Consider a subset A of $\mathbb{F}_3^n$. A "SET" in the card game is a "three term arithmetic progression," namely $\{\mathbf{a}, \mathbf{a}+\mathbf{d}, \mathbf{a}+2\mathbf{d}\}$ where $\mathbf{d} \neq \mathbf{0}$. How big can A be if there are no three term arithmetic progressions?

- $n = 1$, $|A| \leq 2$
- $n = 2$, $|A| \leq 4$
- $n = 3$, $|A| \leq 9$
- $n = 4$, $|A| \leq 20$

$|A| < 3^n$

Fourier analysis, $|A| \leq \frac{2}{n} \cdot 3^n$

Polynomial method, $|A| \leq 2.76^n$

Miniature Arrow

Can prove a smaller version of Arrow's theorem.

In general, DFT helps a lot with combinatorics problems. Surprising because it comes from signal processing.

Feedback

Thank you for coming! Hope you enjoyed!

Slides will be posted at
`www.mit.edu/~shint/handouts/vSDMC/dft.pdf`

For any questions or comments, feel free to contact me at
`shint@mit.edu`.

If you have feedback, please give it to us at

`bit.ly/vsdmc-feedback`

Your feedback is valuable to the continued success of vSDMC!