II. Topics / A. Fast Fourier transform

- Intoduction to premise and problem (**Today**)
- The complex roots of unity (Friday)
- FFT algorithm details (next week Friday, Oct 25)

Today:

- Problem statement
- Terms and indices
- Representing polynomials: Coefficient form
- Representing polynomials: Point-value form

A *field* is a set together with two binary operations satisfying certain properties, known as the *field axioms*. The real numbers with addition and multiplication is the canonical example, but everything in the FFT works for other fields (such as rational numbers and complex numbers).

A *polynomial* is a function of x in the form

$$A(x) = \sum_{j=0}^{n-1} a_j x^j$$

A polynomial with *degree* k has $k+1$ coefficients and least *degree bound* $k+1$.

A polynomial with degree bound n has degree no greater than $n-1$ and has (at most) n coefficients.

The product of two polynomials with (least common) degree bound n, has degree bound $2n-1$.

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + c_nx^n &= (q_0 + q_1x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0x + q_1x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0x_0 - q_1x_0x - \cdots - q_{n-1}x_0x^{n-1} + r \\
&= (r - q_0x_0) + (q_0 - q_1x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1x_0 \\
r &= c_0 + q_0x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad - q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad + (q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}$$

$$\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad - q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad + (q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}$$

$$\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}$$

$$\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}$$

$$\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad - q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad + (q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$
\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}
$$

$$
\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}
$$

Ex 30.1-2. To compute $A(x_0)$, first find $q(x)$ and r such that $A(x) = q(x)(x - x_0) + r$. Then $A(x_0) = r$.

$$\begin{aligned}
c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + c_n x^n &= (q_0 + q_1 x + \cdots + q_{n-1}x^{n-1})(x - x_0) + r \\
&= q_0 x + q_1 x^2 + \cdots + q_{n-2}x^{n-1} + q_{n-1}x^n \\
&\quad -q_0 x_0 - q_1 x_0 x - \cdots - q_{n-1}x_0 x^{n-1} + r \\
&= (r - q_0 x_0) + (q_0 - q_1 x_0)x + \cdots \\
&\quad +(q_{n-2} - q_{n-1}x_0)x^{n-1} + q_{n-1}x^n
\end{aligned}$$

$$\begin{aligned}
q_{n-1} &= c_n \\
q_{n-2} &= c_{n-1} + q_{n-1}x_0 \\
&\vdots \\
q_0 &= c_1 + q_1 x_0 \\
r &= c_0 + q_0 x_0
\end{aligned}$$

Ex 30.1-4. Prove that n distinct point-value pairs are necessary to uniquely specify a polynomial of degree-bound n. (Fewer than n distinct pairs fail to specify a unique polynomial.)

Proof. *Let* $\{(x_0, y_0), \ldots (x_{n-2}, y_{n-2})\}$ *be the set of points. WOLOG, assume no* $x_i = 0$.

Add the point $(0, 0)$ *to the set. By Theorem 30.1, this set specifies a unique n-degree-bound function* $A(x)$.

Alternately, add the point $(0, 1)$ *to the set. By Theorem 30.1, this set specifies a unique n-degree-bound function* $B(x)$.

Since $A(0) = 0 \neq 1 = B(0)$, *it must be that* $A \neq B$. *Therefore n points are necessary.* $\square$.

Given n points, $(x_0, y_0), \ldots (x_{n-1}, y_{n-1})$,

$$A(x) = \sum_{k=0}^{n-1} y_k \frac{\prod_{j \neq k}(x - x_j)}{\prod_{j \neq k}(x_k - x_j)}$$

For next time:

Read Sec 30.2

Do Ex 30.2-1