Fast Fourier Transform II

Recall

Assume that $P(x) = \sum_{i=0}^{n-1} a_i x^i$
$= a_0 + a_1 x + a_2 x^2 + \ldots a_{n-1} x^{n-1}$

$\omega \equiv e^{\frac{2\pi i}{n}}$

$FFT(P(x)) \equiv (P(\omega^{n-1}), P(\omega^{n-2}), \ldots, P(\omega), P(1))$
$= \left(P(e^{\frac{2\pi i(n-1)}{n}}), \ldots, P(e^{\frac{2\pi i 2}{n}}), P(e^{\frac{2\pi i 1}{n}}), P(e^{\frac{2\pi i 0}{n}})\right)$

Define the following two polynomials.
$P^{(0)}(x) \equiv \sum_{i=0}^{\frac{n}{2}-1} a_{2i} x^i$
$= a_0 + a_2 x + a_4 x^2 + \ldots + a_{n-2} x^{\frac{n}{2}-1}$
$P^{(1)}(x) \equiv \sum_{i=0}^{\frac{n}{2}-1} a_{2i+1} x^i$
$= a_1 + a_3 x + a_5 x^2 + \ldots + a_{n-1} x^{\frac{n}{2}-1}$

Time Analysis

$FFT(P(x))$

- If $n = 1$ return $P(x)$.
- Compute $FFT(P^{(0)}(x))$.
- Compute $FFT(P^{(1)}(x))$.
- $\omega \equiv e^{\frac{2\pi i}{n}}$
  $\Omega \equiv (\omega^{\frac{n}{2}-1}, \omega^{\frac{n}{2}-2}, \ldots, \omega, 1)$
  Return the following expression:
  $[FFT(P^{(0)}(x)) - \Omega * FFT(P^{(1)}(x))].[FFT(P^{(0)}(x)) + \Omega * FFT(P^{(1)}(x))]$

Let $T(n) \equiv$ operations needed if $|P(x)| = n$.

$T(n) = 2T(\frac{n}{2}) + \Theta(n) \Rightarrow T(n) = \Theta(n \log n)$

Why does it work?

$$P(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_{n-1} x^{n-1}$$
$$P^{(0)}(x) = a_0 + a_2 x + a_4 x^2 + \ldots + a_{n-2} x^{\frac{n}{2}-1}$$
$$P^{(1)}(x) = a_1 + a_3 x + a_5 x^2 + \ldots + a_{n-1} x^{\frac{n}{2}-1}$$

The Key Math Fact: $P(x) = P^{(0)}(x^2) + xP^{(1)}(x^2)$

Notation: For any vector v, let v_k be the kth term of the vector starting from the right and counting up to the left.

Example: $(1,2,3)_0 = 3$ and $(1,2,3)_2 = 1$

The Lower Order Terms

$[FFT(P^{(0)}(x)) - \Omega * FFT(P^{(1)}(x))].[FFT(P^{(0)}(x)) + \Omega * FFT(P^{(1)}(x))]$

The Key Math Fact: $P(x) = P^{(0)}(x^2) + xP^{(1)}(x^2)$

For any $0 \leq k < n$, by the Key Math Fact,
$FFT(P(x))_k = P(\omega^k) = P^{(0)}(\omega^{2k}) + \omega^k P^{(1)}(\omega^{2k})$

<table>
<tr><td>$\omega = i$</td><td colspan="4">$0x^3 + 0x^2 - x + 1$</td></tr>
<tr><td>$\omega = -1$</td><td colspan="2">$0x - 1$</td><td colspan="2">$0x + 1$</td></tr>
<tr><td>$\omega = 1$</td><td>0</td><td>-1</td><td>0</td><td>1</td></tr>
</table>

Notice that when $n \to \frac{n}{2}, \omega \to \omega^2$.
If $0 \leq k < \frac{n}{2}$, then (i.e. *for the low order values*)
$FFT(P(x))_k = FFT(P^{(0)}(x))_k + \omega^k FFT(P^{(1)}(x))_k$

The Higher Order Terms

$[FFT(P^{(0)}(x)) - \Omega * FFT(P^{(1)}(x))].[FFT(P^{(0)}(x)) + \Omega * FFT(P^{(1)}(x))]$

The Key Math Fact: $P(x) = P^{(0)}(x^2) + xP^{(1)}(x^2)$

For any $0 \leq k < n$, by the Key Math Fact,

$$FFT(P(x))_k = P(\omega^k) = P^{(0)}(\omega^{2k}) + \omega^k P^{(1)}(\omega^{2k})$$

$$\omega \equiv e^{\frac{2\pi i}{n}}$$

$\omega^n = 1 \Rightarrow \omega^{\frac{n}{2}} = -1$ and $\omega^{2k} = \omega^{2k-n} = \omega^{2(k-\frac{n}{2})}$

If $\frac{n}{2} \leq k < n$ (i.e. *for the high order values*)

$$FFT(P(x))_k = P^{(0)}(\omega^{2k}) + \omega^k P^{(1)}(\omega^{2k}) =$$

$$P^{(0)}(\omega^{2(k-\frac{n}{2})}) + \omega^k P^{(1)}(\omega^{2(k-\frac{n}{2})}) =$$

$$FFT(P^{(0)}(x))_{k-\frac{n}{2}} + \omega^k FFT(P^{(1)}(x))_{k-\frac{n}{2}} =$$

$$FFT(P^{(0)}(x))_{k-\frac{n}{2}} - \omega^{k-\frac{n}{2}} FFT(P^{(1)}(x))_{k-\frac{n}{2}}$$

Inversion

The FFT is really a faster way of performing a matrix multiplication. To transform $3x - 4$ when $n = 4$,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} -4 \\ 3 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ -4+3i \\ -7 \\ -4-3i \end{bmatrix}$$

Consider what happens when you multiply the FFT matrix by its conjugate.

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4I$$

Note that multiplying by the conjugate is the same as performing the same operation with $\omega \to \overline{\omega}$.

Does this result hold in general?

Inversion

Inversion Math Fact: $\forall j \not\equiv 0(\text{mod n})$,
$\sum_{k=0}^{n-1} e^{\frac{2\pi ijk}{n}} = \sum_{k=0}^{n-1} \omega^{jk} = 0$
If $j \equiv 0(\text{mod n})$, the sum is equal to n.

[rth row, FFT][cth column, *inverse* FFT] is...

$$\begin{bmatrix} \omega^{r(0)} & \omega^{r(1)} & \omega^{r(2)} & \dots & \omega^{r(n-1)} \end{bmatrix} \begin{bmatrix} \omega^{-c(0)} \\ \omega^{-c(1)} \\ \omega^{-c(2)} \\ \dots \\ \omega^{-c(n-1)} \end{bmatrix}$$

$= \sum_{k=0}^{n-1} \omega^{(r-c)k}$
So if $r = c$, the sum is n and 0 otherwise!

String Matching

Problem: Assume that you are given a pattern $p = p_0 p_1 \ldots p_{m-1}$ that you want to match within a string $s = s_0 s_1 \ldots s_{n-1}$. The goal is to find every spot k in the string where the pattern matches. In other words, the goal is to find every k so that $\forall 0 \leq j \leq m-1, s_{k+j} = p_j$.

Example: $p = CT$ and $s = GTAACTCCTG$
Answer: k=4,7

Application: Genetic marker location

String Matching

Let $s = s_0 s_1 \ldots s_{n-1}$ (with alphabet A) be

$s(x) \equiv \sigma_0 x^0 + \sigma_1 x^1 + \ldots + \sigma_{n-1} x^{n-1}$ where $\sigma_i \equiv e^{\frac{2\pi i s_i}{|A|}}$

Let $p = p_0 p_1 \ldots p_{m-1}$ (with alphabet A) be

$p(x) \equiv \rho_0 x^0 + \rho_1 x^1 + \ldots + \rho_{m-1} x^{m-1}$ where $\rho_i \equiv e^{-\frac{2\pi i p_{m-1-i}}{|A|}}$

What is the coefficient of x^{m-1+i} of the product $s(x)p(x)$?
$s(x)p(x) = \sum_{k=0}^{n+m-2} c_k x^k \Rightarrow c_{m-1+i} = \sum_{j=0}^{m-1} \sigma_{j+i} \rho_{m-1-j}$

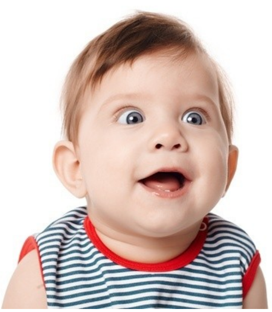
Notice that this coefficient is the sum of m terms, each of which is a complex number with unit magnitude. What would it take for the sum to reach m?

String Matching

$c_{m-1+i} \equiv \sum_{j=0}^{m-1} \sigma_{j+i}\rho_{m-1-j}$

In order for this sum to reach m, we must have
$\forall 0 \leq j \leq m-1, \sigma_{j+i} = \overline{\rho_{m-1-j}} \Leftrightarrow$

$$\forall 0 \leq j \leq m-1, e^{\frac{2\pi i s_{j+i}}{|A|}} = \overline{e^{-\frac{2\pi i p_{m-1-(m-1-j)}}{|A|}}} \Leftrightarrow$$



$\forall 0 \leq j \leq m-1, s_{j+i} = p_j$

So there is a match for the pattern at position i in the string s if and only if the coefficient $c_{m-1+i} = m$!

Wildcards

Problem: What if there is a wildcard in the pattern? For example, what if $p = p_0 * p_2 \ldots p_{m-1}$?

$p(x) \equiv \rho_0 x^0 + \rho_1 x^1 + \ldots + \rho_{m-1} x^{m-1}$ where $\rho_i \equiv e^{-\frac{2\pi i p_{m-1-i}}{|A|}}$

Let the coefficient for p_1 be $0 \Rightarrow \rho_1 = 0$

$c_{m-1+i} \equiv \sum_{j=0}^{m-1} \sigma_{j+i} \rho_{m-1-j}$

Anywhere in the sum that the term appears, it will contribute 0 (as opposed to combining with another term to create 1). Thus if there is a wildcard, we no longer look for the sum to reach m; instead, we want the sum of the corresponding coefficient to reach only $m-1$. If there are w wildcards in the pattern, then we want the sum to reach $m - w$.