

Kelsey Neis -neis@umn.edu

CSCI 5421 - Advanced Algorithms - HW1

30.1 - 2

known: $[a_0, a_1, \dots, a_{n-1}]$, x_0 - some scalar $\underline{a(x_0) = r}$

find: coefficients of $q(x)$ and remainder r

$$a(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots + a_{n-1}x^{n-1}$$

$$\begin{array}{r} \quad \quad \quad \begin{array}{c} q \\ | \end{array} \\ \hline \begin{array}{l} \boxed{a_{n-1}}x^{n-2} + \boxed{(a_{n-2} + x_0a_{n-1})}x^{n-3} + \boxed{(a_{n-3} + x_0a_{n-2} + x_0^2a_{n-1})}x^{n-4} \dots \\ a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_2x^2 + a_1x + a_0 \end{array} \\ \hline - a_{n-1}x^{n-1} + x a_{n-1}x^{n-2} \\ \quad \quad \quad 0 + (a_{n-2} + x_0a_{n-1})x^{n-2} \dots \\ - \quad \quad \quad (a_{n-2} + x_0a_{n-1})x^{n-2} + (x_0a_{n-2} + x_0^2a_{n-1})x^{n-3} \dots \\ \quad \quad \quad \vdots \\ \quad \quad \quad r \end{array}$$

Since the divisor $(x - x_0)$ does not have coefficients, we can assume $q(x)$ will follow a certain pattern. It appears that the first coefficient q_0 (not shown above, because I reversed $A(x)$) will be the sum of all of A above it, multiplied by x_0^* . I think the simplest way would be to go backwards to get the coefficients. Starting at $A(n-1)$ for the value of the $q(n-1)$ coefficient, then for subsequent values, multiply the previous coefficient by x_0 and then add $A(i)$. Then the remainder r should equal $q_0 * x_0 + a_0$.

This should take $\theta(n)$ time, as the coefficient calculated for $q(n-1)$ is reused to get the next one $q(n-2)$, so it only requires iterating once through A .

$$A(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots + a_{n-1} x^{n-1}$$

$$A^{rev}(x) = a_{n-1} x^0 + a_{n-2} x^1 + a_{n-3} x^2 + \dots + a_0 x^{n-1}$$

$$\text{point-value of } A(x) : (x_0, y_0), (x_1, y_1), (x_2, y_2), \dots, (x_{n-1}, y_{n-1})$$

$$\text{where } y_0 = a_0 x_0^0 + a_1 x_0^1 + a_2 x_0^2 + \dots + a_{n-1} x_0^{n-1}$$

$$y_0^{rev} = a_0 x_0^{n-1} + a_1 x_0^{n-2} + a_2 x_0^{n-3} + \dots + a_{n-1} x_0^0$$

$$\begin{array}{ccccccc} x_0^{n-1} & x_0^{n-2} & x_0^{n-3} & \dots & x_0^0 \\ i: 0 & 1 & 2 & \dots & n-1 \end{array}$$

$$n-1-2i$$

$$n-1-2 \cdot 0 \quad n-1-2 \cdot 1 \quad n-1-2 \cdot 2$$

$$a_i^{rev}(x) = (x_i, x_i^{n-1-2i} \cdot a_i(x^{-2}))$$

4

Theorem: for any set of distinct n point-value pairs there is a unique polynomial $A(x)$ such that $y_k = A(x_k)$ $k=0 \rightarrow n-1$

Vandermonde with $n-1$ points: $m \times n$

$$V = \begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix}$$

The above evaluation works correctly to get the values for $(n-1)$ points. However, V is not square, and is therefore not invertible. To find the unique polynomial, we need all n coefficients, but we cannot get those with only $n-1$ point value pairs.

$$a = V(X_0, X_1, \dots, X_{n-2})^{-1} y$$

This equation can't be solved if V is not $n \times n$

Further, if we were to add another point value pair, a would change, and if we assumed from the beginning that a was the unique polynomial of degree bound n , this would lead to a contradiction.

7

We need to convert A and B to coefficient arrays of length $20n$, so the first step is to iterate through each set and represent each value in their corresponding $20n$ -length arrays. If the arrays can be initialized with 20 zeros in constant time, then this step will take time $2n$.

$$A = [4, 1, 6, 8] \quad A[0]=4 \rightarrow A'[4]=1 \dots \Rightarrow A' = [0, 1, 0, 0, 1, 0, 1, 0, 0, \dots, 0]$$

$\underbrace{\quad}_{A[1]} \quad \underbrace{\quad}_{A[0]}$

$$B = [3, 2, 10, 4] \quad B[0]=3 \rightarrow B'[3]=1 \dots \Rightarrow B' = [0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, \dots]$$

$$A'(x) = 0 + 1 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + 1 \cdot x^4 + 0 \cdot x^5 + 1 \cdot x^6 + \dots$$

These will be the coefficient arrays, and using the fact that multiplying 2 powers of x adds together the powers, the power of the resulting $C(x)$ will represent the sums we are trying to compute, and the coefficients will represent the number of times each sum appears in the Cartesian sum.

Now, we need to evaluate the A' and B' coefficients at the 2(th) root of unity by applying the FFT of order $2n$ to get a point-value representation. Evaluation takes $n \log n$ time.

Then pointwise multiply the $A'(x)$ by $B'(x)$ and lastly, apply the FFT on the point value pairs of $C(x)$ to get the coefficients. The resulting vector contains the number of times a given sum is computed from A and B at the index of that sum and from there it is straightforward to present the data.

This will take $n + n \log n$ time, resulting in a total of $\theta(n \log n)$

30.2 -1

$$(\text{from 30.6}): \omega_n = e^{2\pi i/n} \Rightarrow \omega_n^{n/k} = e^{2\pi i/n \cdot n/k} = \underline{e^{\pi i}}$$

$$\omega_2 = e^{2\pi i/2} = \underline{e^{\pi i}}$$

5

If n is a power of 3, it is not as straightforward to divide the problem in to sub problems. We can't rely on the odd-even split, but could use the value of $i \% 3$ to put each coefficient into $a[0]$, $a[1]$, or $a[2]$. If $i \% 3 = 0$, it goes into a $[0]$, if $i \% 3 = 1$, it's part of $a[1]$, otherwise, a $[2]$. Make 3 recursive calls to FFT with $a[0]$,

$a[1]$, and $a[2]$. Iterate $i=0$ to $n/3 - 1$, adding $y[0] + \omega y[1] + \omega^2 y[2]$ to get the top third of the solution vector. To get the middle and bottom thirds, evaluate a at $j+n/3$ and $j+2n/3$:

$$\begin{aligned}
 i &= j + n/3, \\
 a(\omega^{n/3+j}) &= a^{[0]}((\omega^3)^j) + \omega^{(j+n/3)} a^{[1]}((\omega^3)^j) + \omega^{2(n/3+j)} a^{[2]}((\omega^3)^j) \\
 (\omega^3)^i &= (\omega^3)^{n/3+j} = \omega^n \omega^j = \omega^j \\
 \Rightarrow a^{[0]}((\omega^3)^j) + \omega^j a^{[1]}((\omega^3)^j) + \omega^{2j} a^{[2]}((\omega^3)^j) \\
 i &= j + 2n/3: (\omega^3)^i = (\omega^3)^{2n/3+j} = \omega^{2n} \omega^j = \omega^j \\
 a(\omega^{2n/3+j}) &= a^{[0]}((\omega^3)^j) + \omega^j a^{[1]}((\omega^3)^j) + \omega^{2j} a^{[2]}((\omega^3)^j)
 \end{aligned}$$

Runtime:

$$T(n) = 3T\left(\frac{n}{3}\right) + \theta(n)$$

using Master Theorem: $a=3$, $b=3$,
 $f(n)=n$

Matches case 2:

$$f(n) = n^{\log_3 3}$$

Therefore, the runtime is:

$$T(n) = \theta(n \log n)$$

7

Given the polynomial $P(X)$ must be a multiple of $(x-z_j)$, the remainder r of the following equation is 0:

$$\begin{aligned}
 P(x) &= q(x)(x - z_j) + r \\
 &= q(x)(x - z_j)
 \end{aligned}$$

We need to find the quotient that satisfies the above equation for all z .

If $P(x) = 0$ at only $z_0 \dots z_{n-1}$, then it must be composed only of multiples of $x - z_j$, meaning we can roughly represent it as follows:

$$P(x) = (x - z_0)(x - z_1)(x - z_2) \dots (x - z_{n-1})$$

Because the z_0 term contains an x , the above polynomial is $n + 1$ bound. It only remains to get the coefficients now.

From there, we can easily get a point-value representation by choosing n integers not in $z_0 \dots z_n$ and evaluating $P(x)$ at those points.

To then get the coefficients of the polynomial, we need to interpolate, plugging in the point-value representation into the inverse FFT function to get the inverse DFT, which will be the vector of coefficients.