Ass2 讲解

登登 Queenie

Q1

Divide and conquer

e.g. M^8

$\log_2 8 = 3$

M -> 3 次乘法 -> M^8

第一次：$M \times M = M^2$

第二次：$M^2 \times M^2 = M^4$

第三次：$M^4 \times M^4 = M^8$

$\log_2 n$

M^{10}

第一次：$M \times M = M^2$

第二次：$M^2 \times M^2 = M^4$

第三次：$M^4 \times M^4 = M^8$

第四次：$M^8 \times M^2 = M^{10}$

$ceiling(\log_2 n)$

-> O(logn)

指数都会翻倍

Q2

$P(x)^2 = (A_0 + A_1 x^{100} + A_2 x^{200})^2$

Let y = x^{100}

$P(x)^2 = (A_0 + A_1 y + A_2 y^2)^2$

${A_0}^2, {A_1}^2, {A_2}^2, 2A_0A_1, 2A_0A_2, 2A_1A_2$

$= {A_0}^2 + (A_1 y + A_2 y^2)^2 + 2A_0(A_1 y + A_2 y^2)$

$= {A_0}^2 + {A_1}^2 y^2 + {A_2}^2 y^4 + 2A_1 A_2 y^3 + 2A_0 A_1 y + 2A_0 A_2 y^2$

Result:

$R(y) = {A_2}^2 y^4 + 2A_1 A_2 y^3 + ({A_1}^2 + 2A_0 A_2) y^2 + A_0 A_1 y + {A_0}^2$

五个点可以确定R

{-2, -1, 0, 1, 2}, 5th root of unity

7. Multiply the following pairs of polynomials using at most the prescribed number of multiplications where both numbers multiplied are large (large numbers are those which depend on the coefficients and thus can be arbitrarily large).

   (a) $P(x) = a_0 + a_2 x^2 + a_4 x^4 + a_6 x^6$ and $Q(x) = b_0 + b_2 x^2 + b_4 x^4 + b_6 x^6 + b_8 x^8$ using at most 8 multiplications of large numbers;

   (b) $P(x) = a_0 + a_{100} x^{100}$ and $Q(x) = b_0 + b_{100} x^{100}$ with at most 3 multiplications of large numbers.

   Solution:

   (a) First, observe that it is enough to be able to multiply any degree 3 polynomial by a degree 4 polynomial using 8 such multiplications: both P and Q are really polynomials with those respective degrees in x^2.

   Since the result is a polynomial of degree 7, we can uniquely determine it by determining its values at 8 points. For this we can choose $\{-4, -3, \ldots, 3\}$ or alternatively, the 8th roots of unity. We evaluate P at these 8 points and Q at these 8 points: these are only multiplications of a large number my a (constant size) scalar, so these operations are cheap.

   We then multiply the results pointwise: these require precisely 8 large number multiplications. We can then determine the coefficients from these values by setting up a system of linear equations. Solving this is done by inverting a constant matrix (as described in the course), so this inversion can even be done by hand, offline and requires no computation. We then multiply the matrix by the vector formed by the pointwise multiplications, which again only multiplies these results by scalars, to give the final polynomial.

   (b) We have that $PQ(x) = a_0 b_0 + (a_0 b_{100} + a_{100} b_0) x^{101} + (a_{100} b_{100}) x^{200}$. Remember that addition is cheap, but multiplication is expensive. By observing that $(a_0 + a_{100})(b_0 + b_{100}) = a_0 b_0 + a_0 b_{100} + a_{100} b_0 + a_{100} b_{100}$, we can perform this multiplication, as well as $a_0 b_0$ and $a_{100} b_{100}$. The latter two give the coefficients of x^0 and x^{200}, and subtracting these from the first gives the coefficient of x^{101}. Thus, we only use 3 multiplications.

Q3

Lecture slides p29 -30

Q4

A = <1, (k 0s), 1> length = k + 2

$P_A = 1 + x^{k+1}$

Tutorial question 10.(a)

$P_A(x)^2 = (1 + x^{k+1})^2 = 1 + 2x^{k+1} + 1x^{k+1^2}$

$\widehat{A} =< 1, (k0s), 2, (k0s), 1 >$

2(k+1)+1 = 2k + 3

b) = Tutorial q15, slides p29

Solution: Since $B = \langle 1, \underbrace{0, \ldots, 0}_{k}, 1\rangle$, the corresponding polynomial is $P_B(x) = 1 + x^{k+1}$ and

$$\begin{aligned} DFT(B) &= \langle P_B(\omega_{k+2}^0), P_B(\omega_{k+2}^1), \ldots, P_B(\omega_{k+2}^{k+1})\rangle \\ &= \langle 1 + \omega_{k+2}^{0\cdot(k+1)}, 1 + \omega_{k+2}^{1\cdot(k+1)}, \ldots, 1 + \omega_{k+2}^{(k+1)\cdot(k+1)}\rangle \\ &= \langle 0, 1 + \omega_{k+2}^{k+1}, 1 + \omega_{k+2}^{2(k+1)}, \ldots, 1 + \omega_{k+2}^{(k+1)^2}\rangle \end{aligned}$$

Q5

C = <1, 0 , -1, 2, -1>. degree 4 polynomial

A = < a0, a1, a2> degree 2 polynomial

B = <1, 1, -1> degree 2 polynomial

```
0 0 a0 a1 a2

-1 1 1 (reverse B)
```

$C_0 = a_0 \times 1 = 1$

```
0   0 a0 a1 a2

  -1   1   1
```

$C_1 = a_0 + a_1 = 0$

```
0  0 a0 a1 a2

     -1  1  1
```

$C_2 = -a0 + a1 + a2 = -1$

=>

$a_0 = 1, a_1 = -1, a_2 = 1$

```
0  0 a0 a1 a2 0

        -1  1  1
```

$C_3 = -a_1 + a_2 = 2$

```
0  0 a0 a1 a2 0

           -1  1  1
```

$C_4 = -a2 = -1$

<1, -1, 1>