Discussion 2 Dec. 19. 2020

1. Squaring vs Multiplying Matrices

a) show that five multiplications are sufficient to compute the square of 2x2 matrix.

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1^2 + a_2 a_3 & a_1 a_2 + a_2 a_4 \\ a_1 a_3 + a_3 a_4 & a_2 a_3 + a_4^2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1^2 + a_2 a_3 & a_2(a_1 + a_4) \\ a_3(a_1 + a_4) & a_2 a_3 + a_4^2 \end{pmatrix}$$

five multiplications : a_1^2. a_4^2. $a_2 a_3$. $(a_1+a_4)a_3$. $(a_1+a_4)a_2$

(b) What's wrong with the following algorithm for computing square of nxn matrix?

divide and conquer get 5 subproblems of size $n/2$ (part a),

$T(n) = O(n^{\log_2 5})$

Solution: $\begin{pmatrix} A & B \\ C & D \end{pmatrix}^2 = \begin{pmatrix} A^2+BC & AB+BD \\ CA+DC & CB+D^2 \end{pmatrix} \neq \begin{pmatrix} A^2+BC & B(A+D) \\ C(A+D) & BC+D^2 \end{pmatrix}$

wrong: ① five subproblems are multiplying $\frac{n}{2} \times \frac{n}{2}$, not squaring $\frac{n}{2}$ matrix (not the same type)

② matrix don't commute, $BC \neq CB$

c) In fact, square matrices is no easier than multiplying.

Show that if nxn matrices can be squared in $O(n^c)$ time,

then any nxn matrices can be multiplied in $O(n^c)$ time.

Solution: use square to calculate multiplication.

Goal: XY

$$A = \begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix} \quad A^2 = \begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}\begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix} = \begin{pmatrix} \cancel{X}Y & \cancel{XY}\ 0 \\ 0 & YX \end{pmatrix}$$

if we can compute A^2 in $\theta(n^c)$ time, XY is solved.

$$\theta(n^c) = \theta\left(\left(\frac{n}{2}\right)^c \cdot 2^c\right) = \theta\left(\left(\frac{n}{2}\right)^c\right).$$

An example of $\boxed{\text{reduction}}$: we can trick any program for squaring to actually solve the more general problem of multiplication,

$$\begin{tikzcd} \text{Squaring} \arrow[r, bend left, "\text{reduction}"] & \text{Multiplication} \arrow[l, bend left, "\text{reduction}"] \end{tikzcd}$$

the same level.

2. Complex numbers review

(a) $x = e^{\frac{2\pi i 3}{10}}$ $y = e^{\frac{2\pi i 5}{10}}$ compute $x \cdot y$. Is this an n-th root of unity? Is it a 10-th root? What if $x = e^{\frac{2\pi i 6}{10}}$ $y = e^{\frac{2\pi i 7}{10}}$.

① $x \cdot y = e^{\frac{2\pi i 8}{10}}$, a 5th and 10-th root

② $x \cdot y = e^{\frac{2\pi i 13}{10}} = e^{\frac{2\pi i 3}{10}}$ a 10th root

(b) show that for any n-th root of unity $w \neq 1$, $\sum_{k=0}^{n-1} w^k = 0$, when $n > 1$

$$\sum_{k=0}^{n-1} w^k = \frac{w^{n+1} - 1}{w - 1} - w^n$$

$$= \frac{w^{n+1} - 1 - w^{n+1} + w^n}{w - 1}$$

$$= \frac{w^n - 1}{w - 1} = 0$$

(c) (i) Find all w such that $w^2 = -1$.

$\cancel{w^2 = e^{2\pi i}}$ $\quad w^2 = e^{i(2k\pi + \pi)}$

$$w = e^{i \pm \frac{\pi}{2}} = \pm i$$

(ii) Find all w such that $w^4 = -1$

$w^4 = e^{i(\pi + 2k\pi)}$ $\quad w = e^{i\left(\frac{\pi}{4} + \frac{k\pi}{2}\right)}$

$w = e^{\frac{2\pi i \cdot 1}{8}}$ $\quad w = e^{\frac{2\pi i \cdot 3}{8}}$ $\quad w = e^{\frac{2\pi i \cdot 5}{8}}$ $\quad w = e^{\frac{2\pi i \cdot 7}{8}}$

3. FFT Intro

(a) Let $p = (p_0)$, what is $FFT(p, 1)$

$FFT(p,1) = (1)(p_0) = (p_0)$

(b) use FFT to compute $FFT((1,4),2)$ and $FFT((3,2),2)$

$\boxed{\begin{array}{l} \text{① compute } FFT(Even, n/2) \text{ and } FFT(Odd, n/2) \\ \text{② } p(\omega_n^i) = E((\omega_n^i)^2) + \omega_n^i \cdot O((\omega_n^i)^2) \end{array}}$

$p(x) = P_{even}(x^2) + P_{odd}(x^2) \cdot x$

1) $FFT((1,4),2)$

$E = FFT(1,1) = (1)$

$O = FFT(4,1) = (4)$

$$FFT((1,4),2) = \begin{pmatrix} 1+4 \\ 1+\omega_2 \cdot 4 \end{pmatrix} = \begin{pmatrix} 5 \\ -3 \end{pmatrix}$$

2) $FFT((3,2),2)$

$E = FFT(3,1) = (3)$

$O = FFT(2,1) = (2)$

$$FFT((3,2),2) = \begin{pmatrix} 3+2 \\ 3+\omega_2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$$

(c) compute $FFT((1,3,4,2),4)$

$$\text{Even} = FFT((1,4),2) = \begin{pmatrix} 5 \\ -3 \end{pmatrix} \begin{matrix} 1 \\ -1 \end{matrix}$$

$$\text{Odd} = FFT((3,2),2) = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \begin{matrix} 1 \\ -1 \end{matrix}$$

~~$FFT((1,3,4,2),4)$~~

$i=0$: $5+5=10$

$i=1$: $-3+i \cdot 1 = -3+i$

$i=2$: $5-5=0$

$i=3$: $-3+i^3 \cdot 1 = -3-i$

$$FFT((1,3,4,2),4) = \begin{pmatrix} 10 \\ -3+i \\ 0 \\ -3-i \end{pmatrix}$$

(d) Describe how to multiply two polynomials $p(x), q(x)$ in coefficient form of degree at most d.

Take $FFT(p)$ and $FFT(q)$, then get $p \cdot q$ (which is at most $2d$), Then $M = FFT(p, 2^k) \cdot FFT(q, 2^k)$, computes $pq(\omega_{2^k}^i)$ take inverse FFT of M to get back in coefficient form.

4. Practice with FFT

When is the FFT of (1, 0, 0, 0)? What is the value of w?
Of which sequence is (1, 0, 0, 0) the FFT?

$$FFT\big((1,0,0,0)\big) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$w = 1, i, -1, -i$. actually ~~FFT(~~
(1, 0, 0, 0) means $y = x^0 = 1$

---

if $FFT(x) = (1, 0, 0, 0)$

$$F \cdot X = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad X = F^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/4 \\ 1/4 \\ 1/4 \\ 1/4 \end{pmatrix}$$

$$\begin{array}{l} 1 \\ \text{or } i \\ -1 \\ -i \end{array} \begin{cases} a_1 + a_2 + a_3 + a_4 = 1 \\ a_1 + a_2 i - a_3 - a_4 i = 0 \\ a_1 - a_2 + a_3 - a_4 = 0 \\ a_1 - a_2 i - a_3 + a_4 i = 0 \end{cases}$$