Tutorial 7

Wednesday, 13 October 2021 2:05 PM

Q1 (i) $A \subseteq [1, M]$

$B \subseteq [1, M]$

Find $S = \{ a+b \mid a \in A,\ b \in B \}$ in $O(M \log M)$ time

$$A(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_M x^M$$
$$B(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_M x^M$$

$a_i = \begin{cases} 1 & \text{if } i \in A \\ 0 & \text{if } i \notin A \end{cases}$

$b_j = \begin{cases} 1 & \text{if } j \in B \\ 0 & \text{if } 0 \end{cases}$

$$C(x) = A(x)B(x)$$

$$C_k = (\underline{a_k b_0} + \underline{a_{k-1} b_1} + \dots + \underline{a_0 b_k})$$

C_k is non zero iff $k \in S$

No of ways of generating the sum "k"

In set you add k iff $C_k \neq 0$.

Q1 (ii) $A = 1\ 1\ 1\ \ 0\ 0\ \ 0\ 0$ | $A^c = 0\ 0\ 0\ \ 1\ 1\ \ 1\ 1$

$B = 1\,1\,1 \quad 1\,1 \quad 0\,0 \quad | \quad B^c = 0\,0\,0 \quad 0\,0 \quad 1\,1$

$(A \cdot B) = 3 \qquad (A^c \cdot B^c) = 2$

$$\text{Ham Dist}(A,B) = \text{len}(A) - (A \cdot B) - (A^c \cdot B^c)$$

$\text{Ham-Dist}(A, B^i) \qquad \boxed{\underline{\underline{(A, B^i)}} \quad \text{Compute this for all indices } i} \qquad \underline{\underline{(A^c, (B^c)^i)}}$

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

$$B(x) = b_1 x + b_2 x^2 + \dots + b_{n-1}x^{n-1} + b_n x^n$$
$$\left.+ b_1 x^{n+1} + b_2 x^{n+2} + \dots + b_{n-1} x^{2n-1} + b_n x^{2n}\right\} \leftarrow$$

$$\text{Co-eff}(x^{n+i}) \text{ in } A(x)B(x) = \text{Dot Prod}\begin{pmatrix} [a_1 \; a_2 \; \dots \; a_n] \\ [b_{i+1} \dots b_n \; b_1 \dots b_i] \end{pmatrix}$$

Find $C(x)$ in $n \log n$ time, generate $(A \cdot B^i)$, $\forall i$.

$\boxed{\text{Exercise : Ternary vectors } A, B, \text{ ham-dist}(A, B^i), \forall i}$

Q2 (i) ω - prim N root

$S = \{1, \omega, \omega^2, \ldots, \omega^{N-1}\}$

Claim 1 : All eles of S are distinct

Proof : Take i, j $(i < j)$ | if $\omega^i = \omega^j$

$\Rightarrow \omega^{j-i} = 1$ $\qquad j - i < N$

This is not possible bcoz ω is N-th prim root.

Claim 2 : ω^i is sol of $x^N - 1 = 0$

$$(\omega^i)^N - 1 = (\omega^N)^i - 1 = 1 - 1 = 0$$

(ii) $1 + \omega^i + \omega^{2i} + \omega^{3i} + \ldots + \omega^{(N-1)i} = \frac{\omega^{iN} - 1}{\ldots} = 0$

(ii) $1 + \omega^i + \omega^{2i} + \omega^{3i} + \dots + \omega^{(N-1)i} = \frac{\omega^{iN} - 1}{\omega^i - 1} = 0$

denom = non zero
bcoz ω is prim root

(iii) If ω is not prim root

$\Rightarrow \exists\, i$ s.t. $1 + \omega^i + \omega^{2i} + \omega^{3i} + \dots + \omega^{(N-1)i}$ is $\neq 0$

<u>Proof</u> If ω is not prim root then by def $\exists\, i < N$ s.t. $\omega^i = 1$

$1 + \omega^i + \omega^{2i} + \dots + \omega^{i(N-1)} = N$

(iv) ω = prim root $\qquad \omega^i$ = ? prim root $\qquad N$ = pow of 2

i = even
$i = 2k$ $\qquad (\omega^i)^{N/2} = \omega^{2k \cdot \frac{N}{2}} = \omega^{kN} = 1$

So ω^i raise to power $\frac{N}{2}$ is 1 $\Rightarrow$ not prim

i = odd
$i = 2k+1$

To show : ω^i is prim root i.e $(\omega^i)^j \neq 1 \quad 1 \leq j \leq N-1$

w^{ij} will be 1 iff $\frac{ij}{N}$ = integer

$\Rightarrow w^{ij} \neq 1.$ common factor

(4) $A(x) = 1 + 2x + x^2 + x^3$ vector = [1 2 1 1]

N = 4

$w = i$ (iota) Matrix

$w^4 = 1$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ i \\ -1 \\ -i \end{bmatrix}$$

$O(N^2)$ time

DFT (1, $\cancel{2}$, $\cancel{1}$, 1)

$S = \{1, w^1 = i, w^2 = -1, w^3 = -i\}$

$S^2 = \{1 \quad -1 \quad 1 \quad -1\}$

$A(x) = 1 + 2x + x^2 + x^3$

$= \underbrace{(1 + x^2)} + x\underbrace{(2 + x^2)}$

$$= A_{odd}(x^2) + x\, A_{even}(x^2)$$

$$= \underline{(1+y)} + x\,\underline{(2+y)} \qquad y = x^2$$

deg = 1

$y \in S^2$	$1+x^2$ $1+y$	$2+x^2$ $2+y$
1	2	3
−1	0	1

$y=x^2$

deg ≤ 1

deg ≤ 3

$x \in S$	S^2	$\boxed{1+x^2}$	$\boxed{2+x^2}$	$(1+x^2)+x(2+x^2)$
1 ✓	1	2 ✓	3 ✓	5
i ✓	−1	0 ✓	1 ✓	i
−1	1	2	3	−1
−i	−1	0	1	−i

O(N log N) time

Q5 Find count of pairs

collection of binary nos.

$A \in \mathcal{A}$ $B \in \mathcal{B}$

eles are subsets of U   eles are subset of U

$A \cup B = \mathcal{U}$

$A \cap B = \emptyset$

Mapping set to binary vectors.

$U = \{u_1\ u_2\ \dots\ u_n\}$ is universe

If S is set,

$$\boxed{b_S = (b_n \; b_{n-1} \; \cdots \; b_1)}$$

val(S) = decimal equivalent of b_S

where $b_i = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{o/w} \end{cases}$

Eg. $U = \{1, 2, 3, 4, 5\}$

$S = \{1, 3\}$ $\quad b_S = 0\;0\;1\;0\;1$ $\quad$ va

$S' = \{2, 4, 5\}$ $\quad b_{S'} = 1\;1\;0\;1\;0$ $\quad$ val

$S \cup S' =$ univers
$S \cap S' = \phi$
iff b_S and $b_{S'}$ are having 1 at complementary posn?

Find $\mathcal{A}(x) = \sum_{S \in \mathcal{A}} x^{val(S)}$ take $O(|\mathcal{A}| n)$ time

$\mathcal{A} = \{ \{1, 3\}, \{1, 4\} \}$

$00101 \quad 01001$

val = 5 $\quad$ val = 9

$\mathcal{A}(x) = x^5 + x^9$

$\{\underline{1\,1\,1\,1}\}$
$\downarrow$
$2^n - 1$
$\Rightarrow \deg \leq 2^n$

$$\begin{array}{r|l} 1 & \\ 10 & \\ 100 & 4 \end{array}$$

100018

Find $B(x) = \sum_{S \in B} x^{val(S)}$ takes $O(|B| n)$ time

Compute $C(x) = A(x)\, B(x)$ in $O(\deg(A) \log \deg(A))$ time

$O(2^n n)$ time

$\boxed{\text{OUTPUT coeff of } x^{val(U)} = x^{2^n - 1}}$

Lemma: For any $S_1, S_2 \subseteq U$ we have

$\begin{pmatrix} S_1 \cap S_2 = \emptyset \\ S_1 \cup S_2 = U \end{pmatrix}$ iff $val(S_1) + val(S_2) = 2^n - 1$

Proof

(*) If $S_1 \cap S_2 = \phi$ and $(S_1 \cup S_2) = \mathcal{U}$ then
b_{S_1} and b_{S_2} have ones at complementary positions.

So, $b_{S_1} + b_{S_2}$ = binary vector of all 1s.
$\Rightarrow \text{val}(S_1) + \text{val}(S_2) = 2^n - 1.$

(*) Now suppose $\text{val}(S_1) + \text{val}(S_2) = 2^n - 1$. Then $b_{S_1} + b_{S_2}$ = binary vector of all 1s.

<u>Claim</u>: For each $i \in [1, n]$,
$(b_{S_1})_i = 1$ iff $(b_{S_2})_i = 0$
and,
$(b_{S_2})_i = 1$ iff $(b_{S_1})_i = 0$.

<u>Proof of claim</u>:
Suppose i_0 is smallest index where claim is violated
Then,
either $(b_{S_1})_{i_0} = (b_{S_2})_{i_0} = 1$ or $(b_{S_1})_{i_0} = (b_{S_2})_{i_0} = 0$

In $(b_{S_1} + b_{S_2})$ at last $(i_0 - 1)$ indices we will have all 1.

But at index i we will have 0.

This violates the fact $b_{S_1} + b_{S_2}$ is binary vector of all 1's thus our claim holds.

It is straightforward to see that claim implies $S_1 \cap S_2 = \emptyset$ & $S_1 \cup S_2 = \mathcal{U}$.