04 Polynomial Multiplication

Thursday, January 16, 2025 13:50

$f(x) = \sum_{i=0}^{d} f_i \cdot x^i$ polynomial of degree d

$[5, 2, 3, 1, 2]$

$(5 + 2x + 3x^2 + 1x^3 + 2x^4) \cdot (1 + 3x)$

$= (5 \cdot 1) + x(5 \cdot 3 + 2 \cdot 1) + x^2(2 \cdot 3 + 3 \cdot 1) + \dots$

$$\left(\sum_{i=0}^{d} f_i x^i\right) \cdot \left(\sum_{i=0}^{d} g_i x^i\right) = \sum_{i=0}^{2d} x^i \left(\sum_{k=0}^{i} g_k \cdot f_{i-k}\right) = \sum_{i=0}^{2d} x^i \cdot \left(\sum_{k,j} g_k \cdot f_j\right)$$

where $k + j = i$

Input: $A[0 \dots d]$, $B[0 \dots d]$

Output: $C[0 \dots 2d]$

$$C[i] = \sum_{k=0}^{i} A[k] \cdot B[i-k]$$

Naive Algo

for $i = 0 \dots 2d$
  for $k = 0 \dots i$
    ...

$O(d^2)$

Theorem: There exists an algorithm that computes poly. multiplication in time $O(d \log d)$ where the degrees $\leq d$

Proof: Next week (including pseudo code)

Today: Applications!

Polynomial Multiplication = Convolution

3SUM

Input: 3 sets A, B, C where $|A|, |B|, |C| \leq n$

Output: Decide if there is $a \in A$, $b \in B$ with $a + b \in C$

Naive:
```
for a ∈ A
  for b ∈ B
    if a+b ∈ C      // C should be hash map  ->  O(n^2)
      return true
return false
```

---

return false

Input $A \subseteq \{1 \ldots N\}$, $B \subseteq \{1 \ldots N\}$ $C \subseteq \{1 \ldots N\}$

Out: $\exists\, a \in A, b \in B$ $a+b \in C$

Prev $n = \#$ of entries

Now $N =$ bounds the largest entry

3Sum$(A[0 \ldots n-1], B[0 \ldots n-1], C[0 \ldots n-1])$

$f = [001110001]$ $f_k = \begin{cases} 1 & k \in A \\ 0 & k \notin A \end{cases}$

$f = \sum_{i=0}^{n} x^{A[i]}$ // degree $\in N$ $O(n)$

$g = \sum_{i=0}^{n} x^{B[i]}$

$h = f \cdot g$ // $O(N \log N)$ $\Rightarrow$ total time $O(N \log N)$

for $i = 0 \ldots n-1$ // $O(n)$ $n \le N$ if no repetitions

$k = C[i]$

if $h_k \neq 0$ // h_k is coefficient of x^k in poly. h

return true

$h(x) = \sum_{i=0}^{d} h_i\, x^i$

return false

Proof: $h = f \cdot g$ $h_k = \sum_{j=0}^{k} f_j \cdot g_{k-j} = \#$ pairs $j \in A$ $k-j \in B$ $= \#$ pairs $a \in A, b \in B$, $a+b=k$

$f_j = \begin{cases} 0 & \text{if } j \notin A \\ 1 & \text{if } j \in A \end{cases}$ $\Rightarrow f_j \cdot g_{k-j} = \begin{cases} 1 & \text{if } j \in A \text{ and } k-j \in B \\ 0 & \text{else} \end{cases}$

$g_{k-j} = \begin{cases} 0 & \text{if } k-j \notin B \\ 1 & \text{if } k-j \in B \end{cases}$

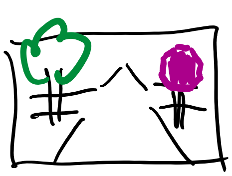
$A = \{1, 2\}$ $f = x^1 + x^2$ $f \cdot g = 1 \cdot x^3 + x^4 \cdot 2 + \underline{x^5 \cdot 1}$

$B = \{2, 3\}$ $g = x^2 + x^3$

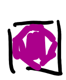
$C = \underline{\{5\}}$

\# of pairs $a \in A$, $b \in B$ with $a+b = \underline{4}$

2:47

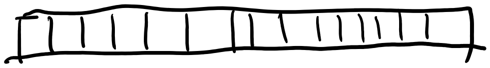


A



B

Find B inside A

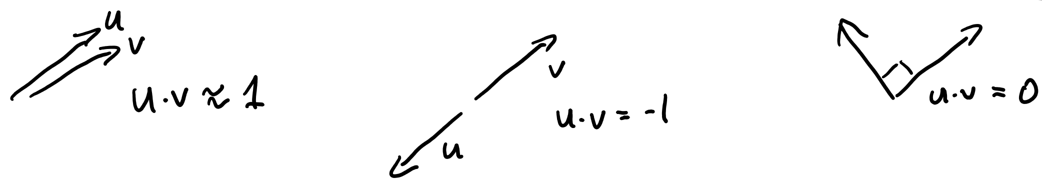
Array $A =$  $\in \mathbb{R}^n$ array of grayscale values

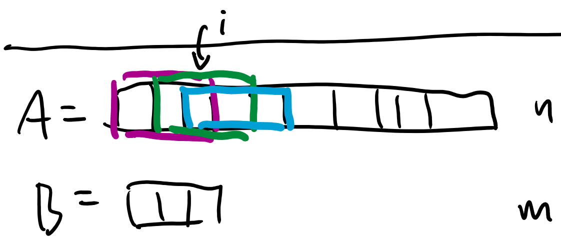
$B =$  $\in \mathbb{R}^m$ $\quad m \le n$

Similarity for vectors: $u, v \in \mathbb{R}^d$

- angle $\arccos\left(\frac{u \cdot v}{\|u\|\|v\|}\right)$
- distance $\|u - v\|$ $\leftarrow$ homework PS 2
- dot product $u \cdot v$ $\leftarrow$ today

Assume $\|u\| = \|v\| = 1$

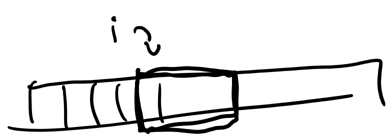




for $i = 0 \dots n-m$

compute $B \cdot A[i, i+1 \dots i+m-1]$ $\quad O(n \cdot m)$

Via poly. multiplication we can do $O(n \log n)$



Input: $A[0 \dots n-1]$ $\quad B[0 \dots m-1]$

Out: $C[0 \dots n-m]$

$$C[i] = \sum_{k=0}^{m-1} A[i+k] \cdot B[k]$$ = dot product $A[i, i+1, \dots i+m-1]$ and B

"Cross-Correlation"

convolution / poly. mult. $\quad k = 0, 1, \dots m-1 \quad\quad -m+1+k = m-1, m-2, \dots 1, 0$

$$C[i] = \sum_{k=0}^{m-1} A[i-k] \cdot B[k] = \sum_{k=0}^{m-1} A[i-m+1+k] \cdot B[m-1-k]$$

$$C[i+m-1] = \sum_{k=0}^{m-1} A[i+k]\, B[m-1-k] = \sum_{k=0}^{m-1} A[i+k] \cdot \overline{B}[k]$$

$\overline{B}$ is array B reverted

Cross Correlation $(A[0 \dots n-1], B[0 \dots m-1])$

B is array B reversed

Cross Correlation (A [0...n-1], B [0...m-1])

$\tilde{B}$ = B reverted

C = $A \cdot \tilde{B}$ // convolution

C = C [m:..] // drop first m-1 entries

return C

$O(n \log n)$