January 16, 2023 4:29 PM

Appl'n 1: Multiplying large integers

(n-bit)

Set $x=2$ $\Rightarrow$ $O(n \log n)$ ops on $(\log n)$-bit #s

$\Rightarrow \sim O(n \log^2 n)$ bit ops

(Schönhage-Strassen '71: $O(n \log n \log\log n)$
Fürer '07: $O(n \log n \cdot c^{\log^* n})$.
Harvey-van der Hoeven '21: $O(n \log n)$ bit ops)

Appl'n 2: 3SUM for Bounded Integers

Given $A, B, C \subseteq \{0, \ldots, U-1\} = [U]$

decide $\exists\, a \in A, b \in B, c \in C$ s.t. $a+b=c$

Let $f_a = \begin{cases} 1 & \text{if } a \in A \\ 0 & \text{else} \end{cases}$ $\quad g_b = \begin{cases} 1 & \text{if } b \in B \\ 0 & \text{else} \end{cases}$

For each $c \in C$,

check iff $\exists a$ s.t. $a \in A$ & $c-a \in B$

iff $\exists a$ s.t. $f_a = 1$ & $g_{c-a} = 1$.

iff $h_c = \underbrace{\sum_{a=0}^{U-1} f_a g_{c-a}}_{\text{convolution!}} > 0$

$\Rightarrow$ $O(U \log U)$ time (good if $U \ll n^2$)

(alternative: multiply polynomial $\sum_{a \in A} x^a$ and $\sum_{b \in B} x^b$)

Appl'n 3: String matching with "don't cares"

Given "pattern" string $p_1 p_2 \cdots p_m \in (\Sigma \cup \{'?'\})^*$
"text" string $t_1 t_2 \cdots t_n \in (\Sigma \cup \{'?'\})^*$ $(m < n)$

decide if pattern occurs in text

i.e. $\exists i,\ \forall j,\ p_j = t_{i+j}$ or $p_j = '?'$ or $t_{i+j} = '?'$

e.g. text: "algorithmisfun"
pattern: "th??s"

trivial: $O(mn)$ time

without "don't care": $O(n)$ time by standard string matching
(Knuth-Morris-Pratt, Rabin-Karp, ...)

with "don't care":

Fischer-Paterson '74: $O(n \log n \log |\Sigma|)$

Indyk '98: $O(n \log n)$ rand.
Kalai '02: $O(n \log n)$ rand.
Cole-Hariharan '02:

Simple Deterministic Alg'm by Clifford & Clifford '07:

let $\alpha_i = \begin{cases} 1 & \text{if } p_i \neq '?' \\ 0 & \text{else} \end{cases}$ $\beta_i = \begin{cases} 1 & \text{if } t_i \neq '?' \\ 0 & \text{else} \end{cases}$

match at position i

$$\iff \sum_{j=1}^{m} \alpha_j \beta_{i+j} (p_j - t_{i+j})^2 = 0$$

$$\Leftrightarrow \quad \sum_{j=1} \alpha_j \beta_{i+j} (p_j - \tau_{i+j}) = 0$$

$$\Leftrightarrow \quad \sum_{j=1}^{m} \alpha_j p_j^2 \beta_{i+j} - 2 \sum_{j=1}^{m} \alpha_j p_j \beta_{i+j} t_{i+j}$$

(α_j: A_j, β_{i+j}: B_{i+j}; $\alpha_j p_j$: A'_j, $\beta_{i+j} t_{i+j}$: B'_{i+j})

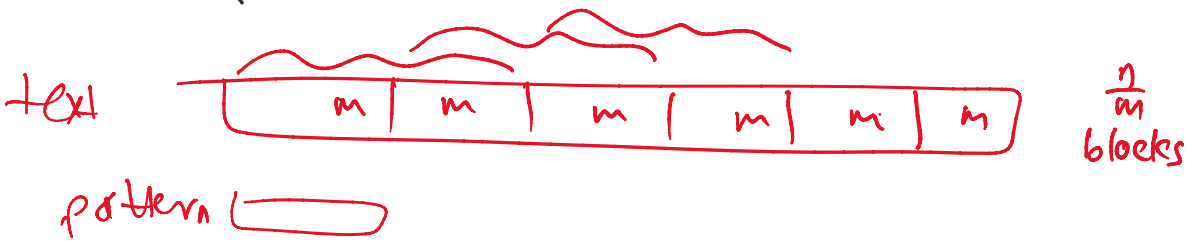
$$= C_i + \sum_{j=1}^{m} \alpha_j \beta_{i+j} t_{i+j}^2 = 0$$

(C_i: convolution!; α_j: A''_j, $\beta_{i+j} t_{i+j}^2$: B''_{i+j})

3 convolutions!

$\Rightarrow$ $O(n \log n)$ time

(improved to $O(n \log m)$)



$\frac{n}{m}$ blocks