2021. szeptember 28.

Hogyan számolhatók ki a $C_{11}, C_{12}, C_{21}, C_{22}$ részmátrixok két $n/2 \times n/2$-es mátrixszorzással?

$$P_1 = A_{11} (B_{12} - B_{22})$$

$$P_2 = (A_{11} + A_{12}) B_{22}$$

$$P_3 = (A_{21} + A_{22}) B_{11}$$

$$P_4 = A_{22}(B_{21} - B_{11})$$

$$P_5 = (A_{11} + A_{22})(B_{11} + B_{22})$$

$$P_6 = (A_{12} - A_{22})(B_{21} + B_{22})$$

$$P_7 = (A_{11} - A_{21})(B_{11} + B_{12})$$

$$C_{11} = P_5 + P_4 - P_2 + P_6$$

$$C_{12} = P_1 + P_2$$

$$C_{21} = P_3 + P_4$$

$$C_{22} = P_5 + P_1 - P_3 - P_7$$

Ellenőrizhető!

Például

$$C_{12} = P_1 + P_2 = A_{11}(B_{12} - B_{22}) + (A_{11} + A_{12})B_{22} =$$

$$A_{11}B_{12} - A_{11}B_{22} + A_{11}B_{22} + A_{12}B_{22} = A_{11}B_{12} + A_{12}B_{22}$$

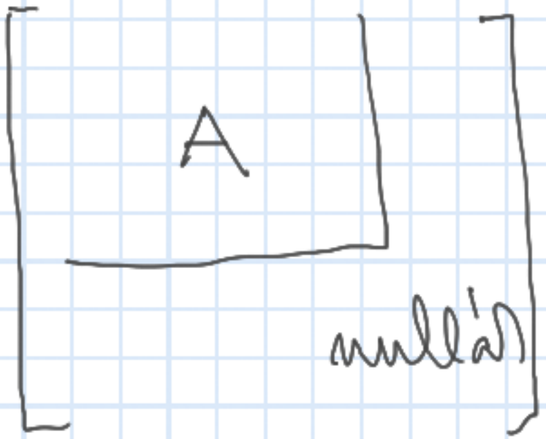
Mester módszerből

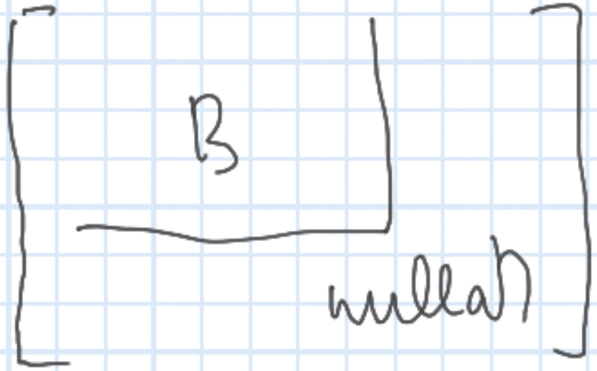
$S(n) = \Theta(n^{\log_2 7})$ elemi összeadások

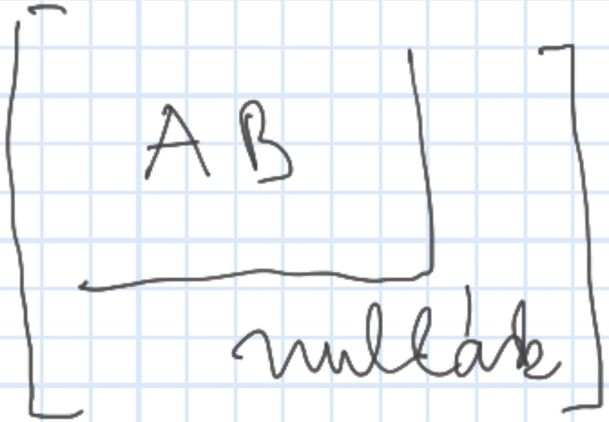
$M(n) = \Theta(n^{\log_2 7})$ elemi szorzások

Adósság: n nem kettőhatvány

Ez nem nehéz

$A \rightarrow A^* =$ 

$B \rightarrow B^* =$ 

$C \rightarrow C^* =$ 

leghosszabbi kettő-hatvány méret

Kapcsolódó kérdés

$A, B, C \in \mathbb{R}^{n \times n}$

A számolás elvégzése nélkül eldönthető-e, hogy $AB = C$?

Randomizált algoritmusok

- Las Vegas algoritmusok
  - → quicksort
  - Sose téved, de lehet lassú

- Monte Carlo algoritmusok
  → ilyet nézünk most
  gyors, de néha téved

Algoritmus (Freivalds)

Véletlenszerűen választunk egy $\alpha \in \{0,1\}^n$ bitvektort, és kiszámoljuk

$$\beta = (AB)\alpha = A(B\alpha)$$
$$\gamma = C\alpha$$

} kvadratikus költség

Ha $\beta \neq \gamma$, akkor térjünk rá arra, hogy $AB \neq C$ (ez biztos nem tévedünk)

Ha $\beta = \gamma$, akkor térjünk rá arra, hogy $AB = C$ (itt tévedhetünk)

Mit mondhatunk abban az esetben ha $\beta = \gamma$ miközben $AB \neq C$?

Kiderül, hogy ez legfeljebb az n-di-

menzión bitvektorok fölé teljesülhet.

Így a-t véletlenszerűen választva, a tévesztés valószínűsége nem nagyobb, mint 1/2

"Igazi" algoritmus

Ismételjük meg százszor a számolást. Annak valószínűsége, hogy mindig tévedünk legfeljebb $\frac{1}{2^{100}}$

"Bebizonyítjuk ezt az 1/2-es valószínűségre"

Tegyük fel, hogy $AB \neq C$ miközben

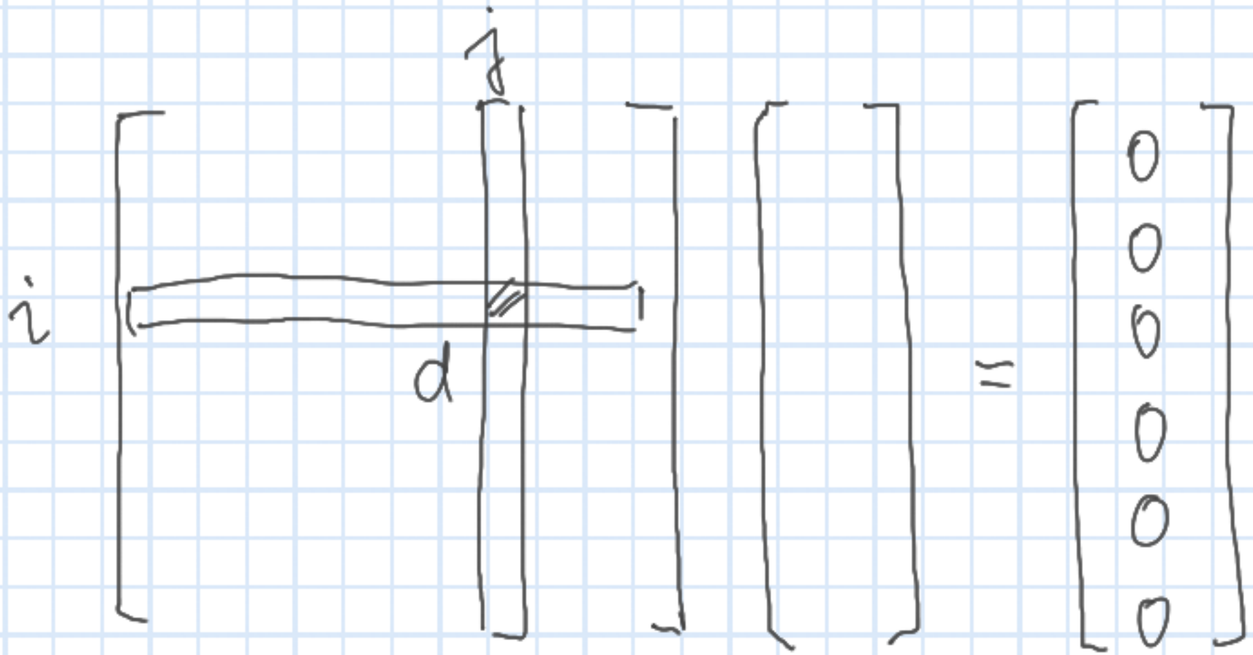
$ABx = Cx$ valamely $x \in \{0,1\}^n$ esetén

$AB \neq C \Rightarrow AB - C \neq 0 \Rightarrow AB - C$-nek

van 0-tól különböző eleme, legyen $d \neq 0$

ilyen mondjuk a i-edik sor és a j-edik

oszlop metszéspontjában



$AB - C \qquad \alpha \qquad \underline{0}$

Változtassunk meg α j-edik koordinátáját

$0 \to 1$, $1 \to 0$

Ekkor az eredmény i-edik koordinátája

d-vel nő vagy csökken, így az eredmény $\neq \underline{0}$

Vegyük észre, hogy különbözö olyan α bitvektorokra, amelyekre $AB\alpha = C\alpha$, a j-edik koordináta megváltoztatásával különbözö olyan α^* bitvektorokat kapunk, amelyekre $AB\alpha^* \neq C\alpha^*$

Így az előbbiek száma nem lehet nagyobb, mint az előbbiaké.

Polinomok szorzása

Adottak

$$A(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{m-1} x^{m-1}$$

$$B(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_{n-1} x^{n-1}$$

Szeretnénk meghatározni a szorzatukat

$$C(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{m+n-2} x^{m+n-2}$$

Egészen pontosan a $c_0, c_1, \dots, c_{m+n-2}$ együtthatókra vagyunk kíváncsiak.

Általános módon

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_{k-1} b_1 + a_k b_0$$

Ez egy $\Theta(mn)$ költségű algoritmus

létezik ennél hatékonyabb? IGEN!

Az egyszerűség kedvéért tfh $n = m$. Ekkor

az előző módszer költsége $\Theta(n^2)$, a most

ismertetendőé $\Theta(n \log n)$

Fő ötlet:

lecsszük az algebra nemüveget és felvesszük

az analízis szemüveget:

① Határozzuk meg $A(x)$ és $B(x)$ helyettesítési értékeit valamilyen $x_1, x_2, \dots$ helyeken

② Határozzuk meg a $C(x_i) = A(x_i)B(x_i)$ értékeit $C(x)$-nek $i = 1, 2, \dots$

③ Ezekből rekonstruáljuk $C(x)$ együtthatóit

Super cool ötlet

Legyenek $x_1, x_2, \ldots$ a $2n$-edik komplex egységgyökök!