November 18, 2022 10:49 AM

Beyond Polylog Speedup

Williams '14: APSP in $O\left(\frac{n^3}{2^{\Theta(\sqrt{\log n})}}\right)$ time (rand.)

Abboud, Williams, Yu '15:

OV in $d = c \log n$ dims

in $O\left(n^{2 - \frac{1}{\Theta(\log c)}}\right)$ time (rand.)

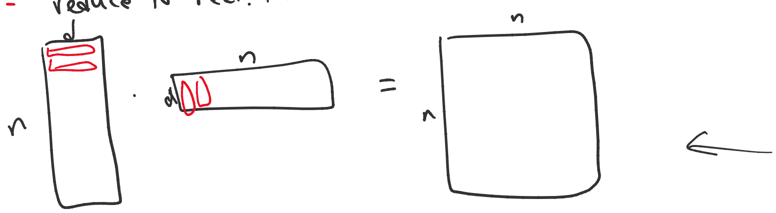
by polynomial method

OV

Given vectors $x^{(1)}, \dots, x^{(n)}, y^{(1)}, \dots, y^{(n)} \in \{0,1\}^d$,

decide $\exists i, j$ s.t. $x^{(i)} \cdot y^{(j)} = 0$.

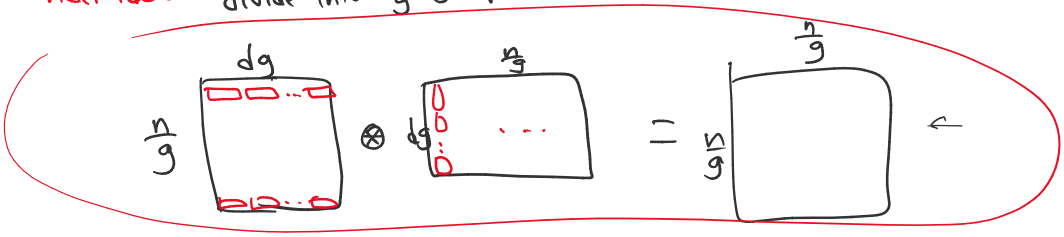
first idea - reduce to rect. MM



$M(n, d, n)$ time

Coppersmith '82: $\tilde{O}(n^2)$ time if $d \le n^{0.172}$

next idea - divide into $\frac{n}{g}$ groups of g vectors



Define new "weird" dot product ⊛:

Given $x = (x_1^{(1)}, \dots, x_d^{(1)}, \dots, x_1^{(g)}, \dots, x_d^{(g)}) \in \{0,1\}^{dg}$

$y = (y_1^{(1)}, \dots, y_d^{(1)}, \dots, y_1^{(g)}, \dots, y_d^{(g)})$

let $$x \circledast y = \bigwedge_{i,j \in [g]} [x^{(i)} \cdot y^{(j)} \neq 0]$$

$$= \boxed{\bigwedge_{i,j \in [g]} \bigvee_{k \in [d]} (x_k^{(i)} \wedge y_k^{(j)})}$$

("AND-of-OR" dot product)

Obs Suppose $x \circledast y$ can be rewritten as a polynomial with D terms called monomials

Then $x \circledast y = \varphi(x) \cdot \psi(y)$

weird dot prod. standard dot prod.

for some $\varphi : \mathbb{Z}^{dg} \to \mathbb{Z}^D$

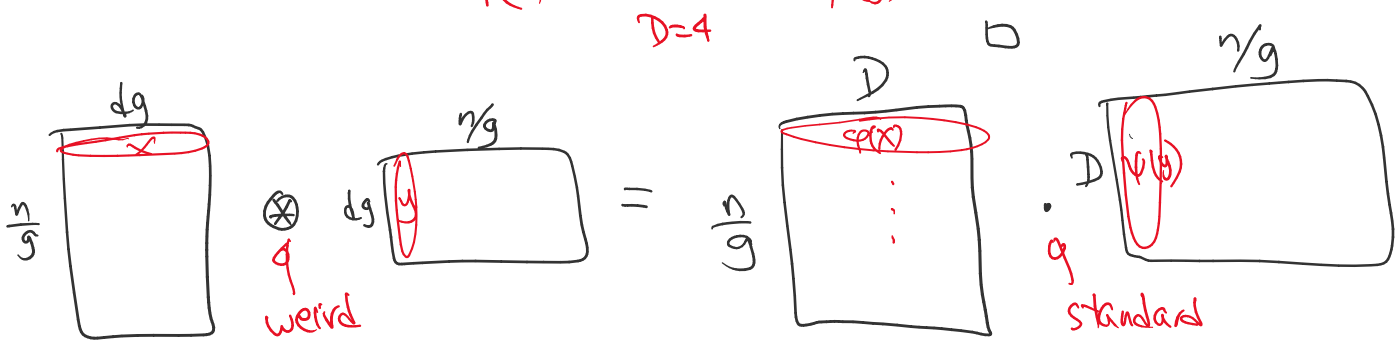
$\psi : \mathbb{Z}^{dg} \to \mathbb{Z}^D$

"Pf by Example:"

$$x \circledast y = x_1^2 y_2 + 5x_1 y_2^2 + 6x_1 y_1^2 y_2 + 3x_1 x_2 y_1 y_2$$

$$= \underbrace{(x_1^2, 5x_1, 6x_1, 3x_1x_2)}_{\varphi(x)} \cdot \underbrace{(y_2, y_2^2, y_1^2 y_2, y_1 y_2)}_{\psi(y)}$$

D=4



$$O\left(M\left(\frac{n}{g}, D, \frac{n}{g}\right)\right) \text{ time}$$

by Coppersmith: $\tilde{O}\left(\left(\frac{n}{g}\right)^2\right)$ if $D \le \left(\frac{n}{g}\right)^{0.172}$

subquadratic!

New Problem

rewrite AND-of-OR dot product as a polynomial

to ~~minimize # of monomials~~

to minimize degree

luckily: studied before ("circuit complexity")

Warm-Up:

polynomial for OR: $z_1 \vee \dots \vee z_d$

Silly attempt: $z_1 + \dots + z_d$

Warm-up: polynomi...

Sol'n: Attempt 1: $z_1 + \dots + z_d$

deg 1 but output is not 0/1.

Attempt 2: $1 - (1-z_1)\cdots(1-z_d)$

but $\underline{\text{deg } d}$: too high

($\#$ monomials $\sim 2^d$)

Randomized Sol'n by Razborov-Smolensky '87:

Take rand $a_1, \dots, a_d \in \{0,1\}$

return $((a_1 z_1 + \dots + a_d z_d))$ mod 2

same as $\mathbb{Z}_2$ (or $\mathbb{F}_2$)

same as XOR

Analysis: deg 1 (work in $\mathbb{Z}_2$)

if OR is false, output is 0 $\Rightarrow$ correct

if OR is true,

then $z_{i_0} = 1$ for some i_0

$$\Pr[\text{output} = 0] = \Pr\left[\sum_{i=1}^{d} a_i z_i = 0 \text{ in } \mathbb{Z}_2\right]$$

$$= \Pr\left(a_{i_0} = -\sum_{i \neq i_0} a_i z_i \text{ in } \mathbb{Z}_2\right)$$

$$= \frac{1}{2}$$

Can lower err prob by repeating $\ell = \underline{\log s}$ times

i.e. return $1 - \left(1 - (a_1^{(1)} z_1 + \dots + a_d^{(1)} z_d)\right) \cdots \left(1 - (a_1^{(\ell)} z_1 + \dots + a_d^{(\ell)} z_d)\right)$

err prob $\left(\frac{1}{2}\right)^{\log s} = \frac{1}{s}$.

$$\overbrace{z_0 z_0 \cdots z_0}^{\log s}$$

deg $= \underline{\log s}$

$\deg = \log s$

$\#$ monomials $\leq \binom{d}{\log s}$

Finally, to rewrite

$$x \circledast y = \underbrace{\bigwedge_{i,j\in[g]}}_{\substack{\text{use de-Morgan}\\ \text{\& then use R-S}\\ \text{with err prob } \frac{1}{4}}} \underbrace{\bigvee_{k\in[d]} x_k^{(i)} y_k^{(j)}}_{\substack{\text{use R-S}\\ \text{with err prob } \frac{1}{s} \sim \frac{1}{8g^2}}}$$