Beyond Polylog Speedups

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

bigger than $\log^{100000} n$ (but not bigger than n^{δ}).

Abboud, Williams, Yu '15 :

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

e.g. set $c = 2^{\Theta(\sqrt{\log n})}$

$\Rightarrow$ in $2^{\Theta(\sqrt{\log n})}$ dims,

$$O\left(n^{2-\frac{1}{\Theta(\sqrt{\log n})}}\right) = O\left(\frac{n^2}{(2^{\log n})^{\frac{1}{\Theta(\sqrt{\log n})}}}\right)$$

$$= O\left(\frac{n^2}{2^{\Theta(\sqrt{\log n})}}\right).$$

by polynomial method

OV

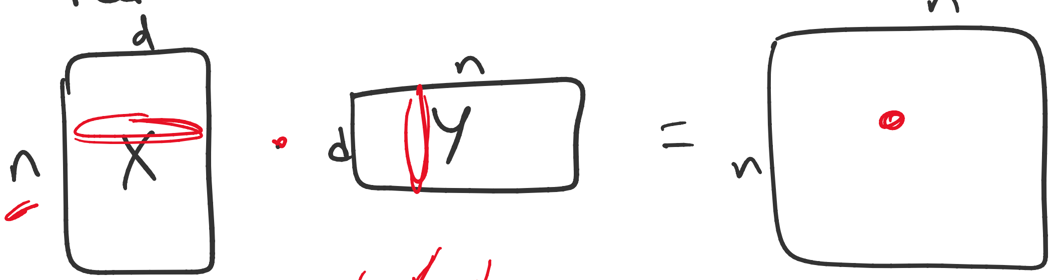
Given vectors $x^{(1)}, \ldots, x^{(n)}, y^{(1)}, \ldots, y^{(n)} \in \{0,1\}^d$,

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

i.e. $\bigvee_{k \in [d]} (x^{(i)}_k \wedge y^{(j)}_k) = 0$.

(brute force $O(dn^2)$)

first idea - reduce to rect. MM

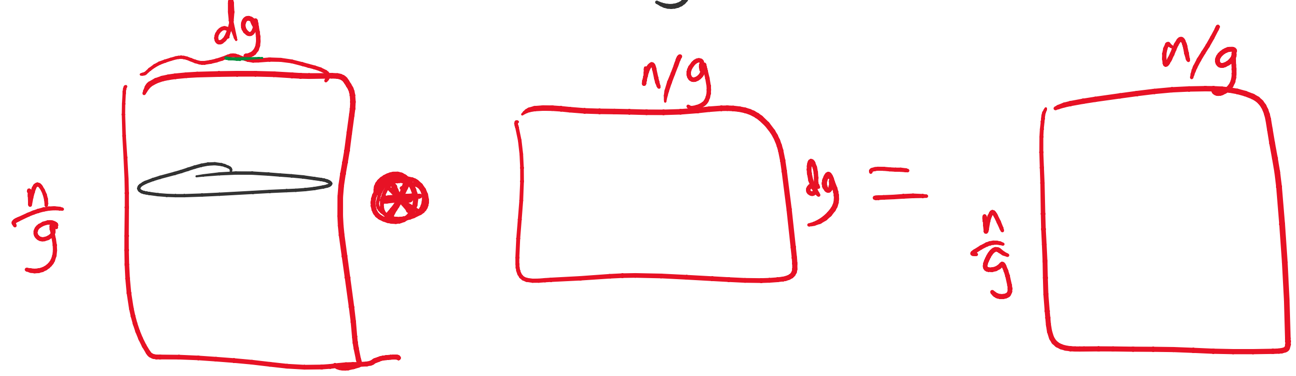


$O(MM(n, d, n))$ time

$O(M(n, d, n))$ 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



unfortunately, $\circledast$ is "funny"
not standard dot product!

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

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

want to compute

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

← "AND-of-ORs dot product"

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

Then given $x^{(1)}, \dots, x^{(n/g)}, y^{(1)}, \dots, y^{(n/g)}$,

can compute $x^{(i)} \circledast y^{(j)}$ for all i,j

in $O(M(\frac{n}{g}, D, \frac{n}{g}))$ time

$\Rightarrow \tilde{O}(\frac{n^2}{g^2})$ time if $D \le (\frac{n}{g})^{0.172}$

Pf: by Example. # monomials $= 4$

$\dots x_1 y_1 + 8 x_2 y_1^2 y_2 + 5 x_1^3 x_2 y_1$

4. by example.

Say $x \circledast y = x_1 y_2 + 8 x_2 y_1^2 y_2 + 5 x_1^3 x_2 y_1 + 6 x_1 x_2 y_1 y_2$.

$(\underline{x_1, x_2}) \circledast (\underline{y_1, y_2})$

$$= (x_1, 8x_2, 5x_1^3 x_2, 6x_1x_2) \cdot (y_2, y_1^2 y_2, y_1, y_1 y_2)$$

standard dot prod in D dims. $\square$

New Problem

how to rewrite AND-of-ORs fn as polynomial

to minimize $\underline{\#}$ monomials

aim for low $\underline{\text{degree}}$

luckily, studied in circuit complexity theory!

Warm-Up Problem

design polynomial for OR: $z_1 \vee \cdots \vee z_d$.

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

but output is not 0/1.

Sol'n Attempt 2: $1 - (1-z_1)\cdots(1-z_d)$ — (by De Morgan law)

but deg is $\underline{d}$. too big!

monomials is $\sim 2^d$.

Very Simple Rand. Sol'n by Razborov-Smolensky '87:

Take random $a_1, \ldots, a_d \in \{0,1\}$.

Return $(a_1 z_1 + \cdots + a_d z_d) \bmod 2$ (i.e. XOR) (working in $\mathbb{F}_2$)

Analysis: deg 1. (can do MM in $\mathbb{F}_2$)

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

If OR is true,

then say $z_{i_0} = 1$.

$$\Pr[\text{output} = 0] = \Pr\left[\sum_i a_i z_i \equiv 0 \pmod 2\right]$$

$$= \Pr\left(a_{i_0} \equiv -\sum_{i \neq i_0} a_i z_i \pmod 2\right)$$

random!

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

err prob $\frac{1}{2}$ $\leftarrow$ terrible?

Can lower err prob by repeating $\log s$ times

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

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

$\deg = \boxed{\log s}$

$(z_i^2 = z_i)$

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

Finally, to rewrite

$$x \circledast y = \underbrace{\bigwedge_{i,j \in [g]}}_{} \underbrace{\bigvee_{k \in [d]} \overbrace{(x_k^{(i)} y_k^{(j)})}^{z_k^{(i,j)}}}_{}$$

use De Morgan & then R-S with err prob $\frac{1}{4}$

use R-S with err prob $\frac{1}{s} = \frac{1}{8g^2}$

$\Rightarrow$ err prob. $\leq g^2 \cdot \frac{1}{8g^2} + \frac{1}{4} = \frac{3}{8}$

(can reduce err prob by repeating alg'm 100 log n times

(can reduce err prob by repeating algm 100 or log n times
& return majority per entry)

deg $O(\log s) = O(\log g)$

D = # monomials

⋮

final bd? next time!

Presentation schedule: Dec 4, 9   11am - 1:30pm