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

random!

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

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

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

$\#$ monomials $\leq \binom{d}{\log s}$. $\quad (z_i^2 = z_i)$

Finally, to rewrite

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

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 & return majority per entry)

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

$D = \#$ monomials

$\leq O\left((g^2)^2 \binom{d}{O(\log s)}^2 \right)$

$$\le \quad O\left(\binom{\ }{g} \binom{\ }{o(\log s)} \right)$$

$$\approx \quad O\left(\frac{d}{\log s} \right)^{O(\log s)} \qquad d = c\log n$$

$$\binom{a}{b} \le \left(\frac{ea}{b}\right)^{b}$$

$$= \quad O\left(\frac{c\log n}{\log g} \right)^{O(\log g)}$$

Set $g = n^{\frac{1}{k}}$

$$= \quad O(\ ck\ )^{O(\frac{1}{k}\log n)}$$

$$a^{b\log n} = n^{b\log a}$$

$$= \quad n^{O(\frac{1}{k}\log(ck))}$$

Set $k = 100\log c$

$$\le \quad n^{0.1} \quad \le \quad \left(\frac{n}{g}\right)^{0.172}$$

$\Rightarrow$ total time $\tilde{O}\left(\frac{n^2}{g^2}\right) = \tilde{O}\left(n^{2-\theta(\frac{1}{k})}\right)$

$$= \boxed{O\left(n^{2-\theta(\frac{1}{\log c})}\right)}$$

APSP

Suffice to solve $(\min,+)$-MM of $n\times d$ & $d\times n$ matrices A, B. (reals)

i.e. want $k_{ij}^{*} = \arg\min\limits_{k\in[d]} (a_{ik} + b_{kj}) \quad \forall i,j \in [n]$

Fix set $K_0 \subseteq [d]$.

Subproblem decide $\underline{\text{if } k_{ij}^{*} \in K_0}$ $\quad \forall i,j\in(n)$.

(e.g. $K_0 = \{0,\dots,d/2\} \Rightarrow$ leading bit of k_{ij}^{*}

$K_0 =$ all even #s $\Rightarrow$ last bit of k_{ij}^{*}) $\log n$ calls suffice equiv to computing

$$f_{ij} = \bigwedge_{k \notin K_0} \bigvee_{k' \in [d]} [a_{ik} + b_{kj} > a_{ik'} + b_{k'j}]$$

$$\parallel\!\!|$$

$$[a_{ik} - a_{ik'} > b_{k'j} - b_{kj}]$$

FREDMAN'S TRICK!!

For each $k, k' \in [d]$,

sort $L_{kk'} = \{ a_{ik} - a_{ik'} \mid i \in [n] \} \cup \{ b_{k'j} - b_{kj} \mid j \in [n] \}$

(total time $\tilde{O}(d^2 n)$)

Let $r^{(i)}_{kk'}$ = rank of $a_{ik} - a_{ik'}$ in $L_{kk'}$, $s^{(j)}_{kk'}$ = rank of $b_{k'j} - b_{kj}$ in $L_{kk'}$ $\in [2n]$.

$$\Rightarrow \boxed{f_{ij} = \bigwedge_{k \notin K_0} \bigvee_{k' \in [d]} [r^{(i)}_{kk'} > s^{(j)}_{kk'}]}$$

("dominance string match")

next idea - like HW1P2
divide $[2n]$ into h subintervals of length $\frac{n}{h}$.

Near Case: $r^{(i)}_{kk'}$ & $s^{(j)}_{kk'}$ in same subinterval for some k, k'.

for each $i \in [n]$, $k, k' \in [d]$,
find all j s.t. $s^{(j)}_{kk'}$ is in interval of $r^{(i)}_{kk'}$ ← $\frac{n}{h}$ choices
compute f_{ij} by brute force

$\Rightarrow$ time $O(d^2 n \cdot \frac{n}{h} \cdot d^2) = O(n^2)$

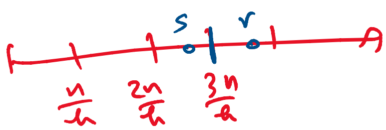
by setting $h = d^4$.

by setting $h = d^4$.

Far Case: $r^{(i)}_{kk'}$ & $s^{(j)}_{kk'}$ in diff subintervals for all k, k'.

$$f_{ij} = \bigwedge_{k\notin K_0} \bigvee_{k'\in[d]} \left[r^{(i)}_{kk'} > s^{(j)}_{kk'} \right]$$

$$= \bigwedge_{k\notin K_0} \bigvee_{k'\in[d],\, \ell\in[h]} \underbrace{\left[r^{(i)}_{kk'} \geq \frac{\ell n}{h} \right]}_{\equiv\, x^{(i)}_{kk'\ell}} \cdot \underbrace{\left[s^{(j)}_{kk'} < \frac{\ell n}{h} \right]}_{\equiv\, y^{(j)}_{kk'\ell}}$$



Given vectors $x, y \in \{0,1\}^{d^2 h}$, define funny dot product

$$\boxed{x \circledast y = \bigwedge_{k\notin K_0} \bigvee_{k'\in[d],\, \ell\in[h]} \left(x_{kk'\ell} \wedge y_{kk'\ell} \right)}$$

d factors AND-of-ORs again! dh

By R-S, get a polynomial with degree $O(\log d)$

err prob $< \frac{3}{8}$

monomials $O\left(d^2 \cdot \binom{dh}{O(\log d)}^2 \right)$

$$\leq (dh)^{O(\log d)}$$

$$= d^{O(\log d)} = 2^{O(\log^2 d)}$$

$$\ll n^{0.172}$$

$\binom{a}{b} \leq a^b$

$h = d^4$

$8\sqrt{\log n}$

Set $\boxed{d = 2^{\delta\sqrt{\log n}}}$

$\Rightarrow$ can compute (min,+)-MM of $n \times d$ & $d \times n$ in $\tilde{O}(n^2)$ time.

$\Rightarrow$ can compute (min,+)-MM of $n \times n$ in $\tilde{O}\left(\frac{n}{d} \cdot n^2\right) = \boxed{O\left(\frac{n^3}{2^{\Theta(\sqrt{\log n})}}\right)}$

Rmks - Still current best ...

- can be derandomized (C.-Williams '16)

idea - reduce # of rand. bits by ε-biased spaces

- then try all rand choices & add up counts

issue - can't count in $\mathbb{F}_2$

fix - "modulus-amplifying polynomial"

e.g. $P(x) = 3x^2 - 2x^3$

$x \equiv 0 \bmod 2^m \Rightarrow P(x) \equiv 0 \bmod 4^{m^2}$

$x \equiv 1 \bmod 2^m \Rightarrow P(x) \equiv 1 \bmod 4^{m^2}$

- appl'ns to #k-SAT,

closest pair in $\{0,1\}^d$ (AND-of-MAJs)

MAX-3-SAT, etc.