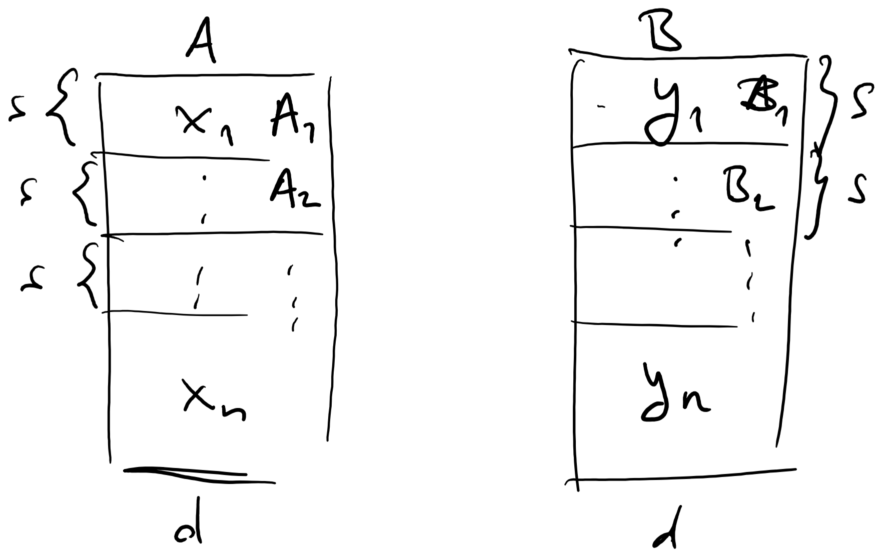
Alg. for OVP

12 November, 2020 16:43

- for $d = c \lg n$ we will describe an algorithm for OVP that runs in time $n^{2-\varepsilon_c}$, where $\varepsilon_c > 0$ depends only on $\underline{c}$.

  $\left(\varepsilon_c \approx \frac{1}{\lg c} \right)$

<u>Approach:</u>



$|A| = |B| = n$

$A, B \subseteq \{0,1\}^d$

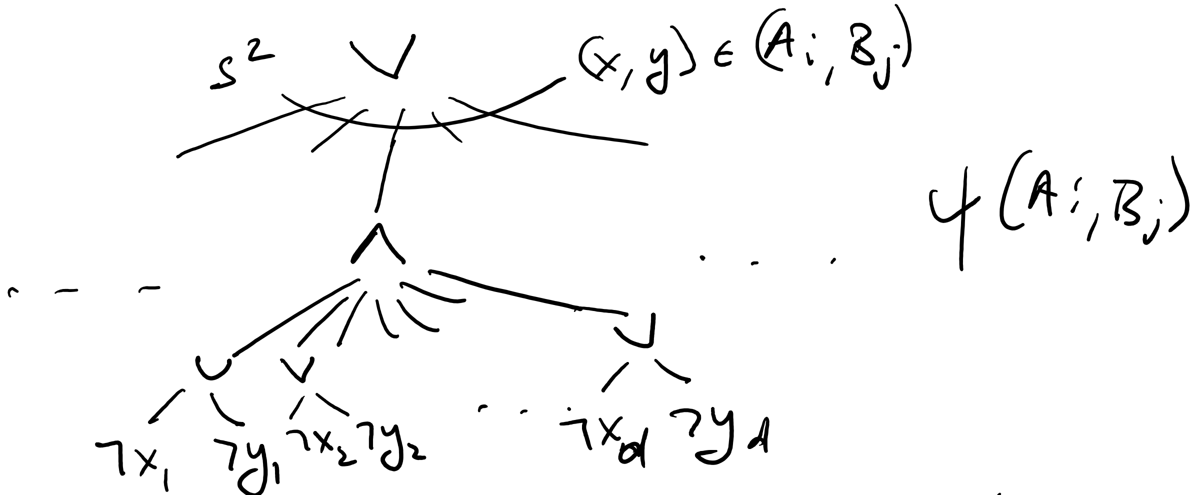
$s \approx n^{\varepsilon'}$ for some small $\varepsilon' < \frac{1}{100}$

- divide A into blocks of vectors $A_1, \dots A_{\frac{n}{s}}$
  & B into $B_1, \dots B_{\frac{n}{s}}$
- $\forall x \in A \ \forall y \in B \ \langle x, y \rangle \neq 0 \iff \forall i, j \in [\frac{n}{s}]$ no two vectors in A_i & B_j are orthogonal
- Solving OVP on A, B can be reduced

to solving $\left(\frac{n}{s}\right)^2$ OVPs on A_i, B_j for various i & j.

- a naive way to solve OVP on (A_i, B_j) takes time $O(s^2)$, so we need something better.

- consider a Boolean fla describing OVP on A_i, B_j



this is a formula in $2ds$ variables (bits of vectors from A_i, B_j)

- we will represent this $\psi(A_i, B_j)$ by a polynomial

$$F(A_i, B_j) \text{ over } GF_2$$

e.g. if $A_i = \{x^1, x^2, \dots x^s\}$ $B = \{y^1, y^2, \dots y^s\}$

then $F(A_i, B_j) = \underbrace{x_7^1 \cdot x_5^2 \cdot y_1^3}_{} + \dots + \dots$

monomials, each variable has degree ≤ 1 since we are over GF_2

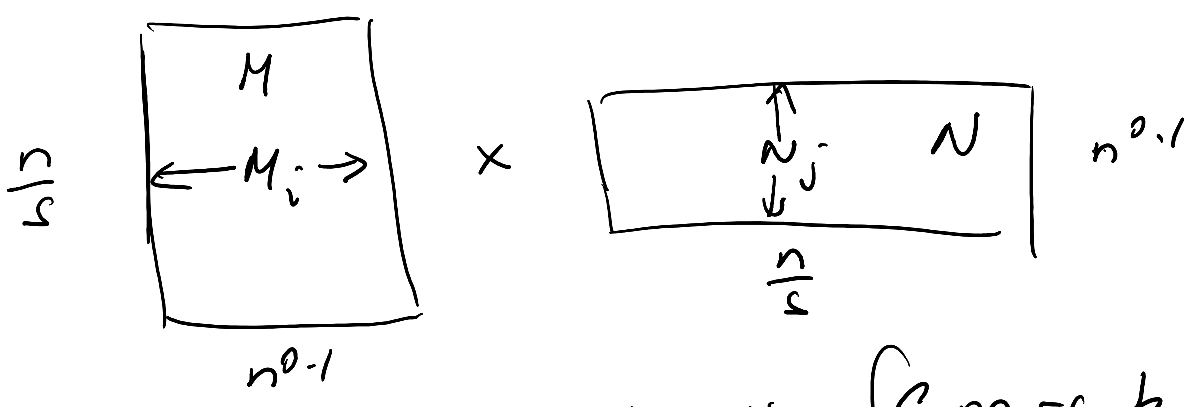
- the polynomial F will have at most $n^{0.1}$ monomials
- For each A_i, we will precompute the contribution of vectors from A_i to each monomial of F $\rightarrow$ M_i vector of contributions

  For each B_j, we will precompute the contribution of vectors from B_j to each monomial of F $\rightarrow$ N_j

  ℓ^{th} entry is the product of vars from A_i that appear in ℓ^{th} monomial

$$\longrightarrow \langle M_i, N_j \rangle = F(A_i, B_j) \quad (\text{mod } 2)$$

- Build two matrices



and compute their product using [Coppersmith] alg. for rectangular matrices.

Needs time $O\left(\left(\frac{n}{s}\right)^2\right)$.

- Computing M & N takes time $O(n^{1.1} \cdot ds)$
$= O(n^{1.2})$.

(curiously, # monomials in $F \gg s^2$)

- If the product of the matrices is not all zero matrix, then A & B contain an orthogonal pair of vectors.

<u>Glitch</u>: F with few monomials might not exist.

→ Instead of F agreeing with ψ on all inputs we will pick an approximate F, that agrees with ψ on $\geq \frac{3}{4}$ inputs.

- F will be picked at random so that on any fixed input A_i, B_j to ψ, $F(A_i, B_j) = \psi(A_i, B_j)$ w.p. at least $\frac{3}{4}$.

→ We will pick $O(\log n)$ of such F at random, independently, compute the matrices M & N and the product matrix $M \times N$. For each entry of the product we output the majority value appearing for different F's.

- By chernoff bound, this will give a correct answer for all entries of the product w.h.p.

- We build F using the method of Razborov-Smolensky:

gate	polynomial	degree
$\neg X$	$1 - x$	1
$\wedge$ ($x_1 \quad x_n$)	$x_1 \cdot x_2 \cdots x_n$	n
$\vee$ ($x_1 \ x_2 \ \cdots \ x_n$)	$1 - \prod_{i=1}^{n} (1 - x_i)$	n

Want: smaller degree

		deg
$\vee$ ($x_1 \ \cdots \ x_n$)	$p_k(x_1 \dots x_n) = 1 - \prod_{j=1}^{k} \left(1 - \sum_{i=1}^{n} a_{ji} x_i\right)$	k

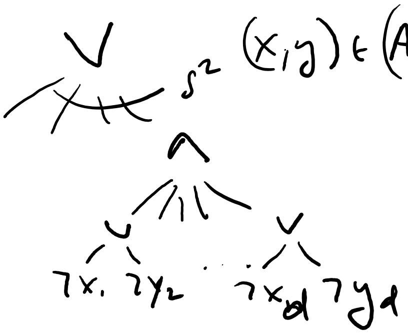
Each $a_{j,i}$ picked at random from $\{0,1\}$.

For given j & x

$$\Pr_{a_{j1}\dots a_{jn} \in \{0,1\}} \left[x_1 \vee x_2 \vee \dots x_n = \sum_{i=1}^{n} a_{ji} x \right] = \begin{cases} 1 & x = 0^n \\ \frac{1}{2} & x \neq 0^n \end{cases}$$

$$\Rightarrow \quad \Pr_{\substack{a_{i,j} \in \{0,1\} \\ j = 1,\dots k \\ i = 1,\dots n}} \left[x_1 \vee x_2 \dots \vee_n = p_k(x_1 \dots x_n) \right] \geq 1 - \frac{1}{2^k}$$

- recall $\psi(A_i, B_j)$



$(x,y) \in (A_i, B_j) \longrightarrow F(A_i, B_j) = p_3\big(F(x,y) \,;\, (x,y) \in A_i, B_j\big)$

$k = 3 + 2\lg s$

$\longrightarrow f(x,y) = 1 - p_k\big(1 - f_1(x,y), 1 - f_2(x,y), \dots 1 - f_d(x,y)\big)$

$\longrightarrow f_i(x,y) = 1 - x_i \cdot y_i$

De Morgan rules $\wedge \to \vee$

all f_i have degree 2 & # monomials 2

all $F(x,y)$ have degree $\leq 2k$ & # monomials $\binom{d+k}{k} + O(1)$ $\quad k = 3 + 2\lg s$

$F(A_i, B_j)$ has degree $\leq 6k$ & # monomials $\left[1 + s^2 \binom{d+k}{k}\right]^3 + 1$

$$\leq 8 \cdot s^6 \binom{d+k}{k}^3$$

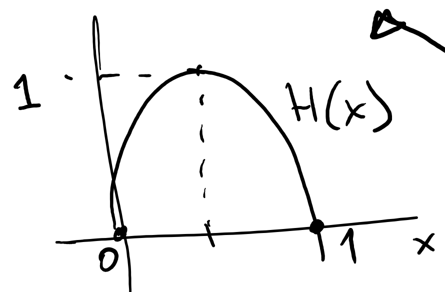
$$\binom{d+k}{k} \leq \binom{c\lg n + 3 + 2\lg s}{3 + 2\lg s} \leq \binom{(c+5)\lg n}{5\lg n^{\varepsilon'}}$$

$s = n^{\varepsilon'}$

$$\leq 2^{H\left(\frac{\varepsilon' 5}{c+5}\right)(c+5)\lg n} \leq 2^{0.01\lg n} = n^{0.01}$$

Fact: $\binom{a}{b} \leq 2^{H\left(\frac{b}{a}\right) \cdot a}$

$H(x) = x\lg\frac{1}{x} + (1-x)\lg\frac{1}{1-x}$



by choosing ε' small enough

- the coefficients $a_{j,i}$ are picked independently for each $p_k(\dots)$.
- given the coefficients we can compute the representation of F in monomials in time $\mathrm{poly}(\#\text{monom.})$
$\leq n^{0.1}$.

Hence computing the M_i, N_j's can be done in time $\leq O(n^{1.1})$.

Correctness of the approx:

For given fixed input A_i, B_j & $x, y \in A_i, B_j$

$f_i(x,y)$ ... always correct

$f(x,y)$ ... prob of error $\leq \frac{1}{2^{3+2\log s}} = \frac{1}{8s^2}$

$F(A_i, B_j)$ ... prob of error $\leq \underbrace{s^2 \cdot \frac{1}{8s^2}}_{\text{On some } x,y \in A_i, B_j \; f(x,y) \text{ incorrect}} + \frac{1}{8} = \frac{1}{4}$

$\frac{1}{8}$ ← $p_3(\dots)$ incorrect

→ for random choice of $a_{j,i}$'s, $\Pr[F(A_i, B_j) \equiv OVP(A_i, B_j)] \geq \frac{3}{4}$