Matrix Rigidity

Rigidity in P^{NP}

Sasha Golovnev

October 26, 2020

Overview

- Recall that we want $M \in \mathbb{F}_2^{n \times n}$, $\underline{M \in \mathsf{E}^{\mathsf{NP}}}$
$$\mathcal{R}_M^{\mathbb{F}_2}(\varepsilon n) \geq \Omega(n^{1+\delta}) .$$
- We'll prove that there is $M \in \mathbb{F}_2^{n \times n}$, $\underline{M \in \mathsf{P}^{\mathsf{NP}}}$
$$\mathcal{R}_M^{\mathbb{F}_2}(2^{\underline{\log n / \log \log n}}) \geq \Omega(n^2) .$$
- We'll use
  - Orthogonal Vectors
  - Non-deterministic Hierarchy Theorem
  - Rectangular PCPs

Orthogonal Vectors

Theorem

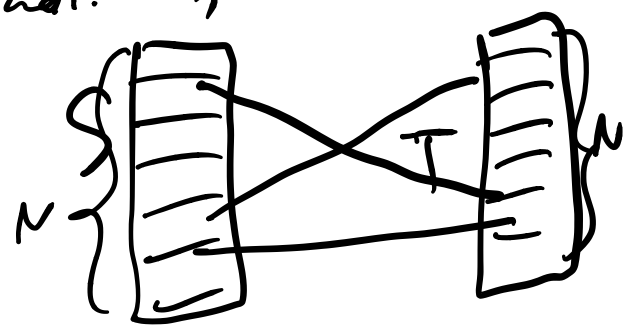
There is a deterministic algorithm that solves #OV over $\mathbb{F}_2$ in time $\boxed{O(N^{2-1/\log(d/\log n)})}$ for any $d = \cancel{n}N^{o(1)}$.

S - sets of N vectors from $\mathbb{F}_2^d$

T

Count # of (s,t) orthogonal: $\langle s,t \rangle = 0$

$s \in S$, $t \in T$



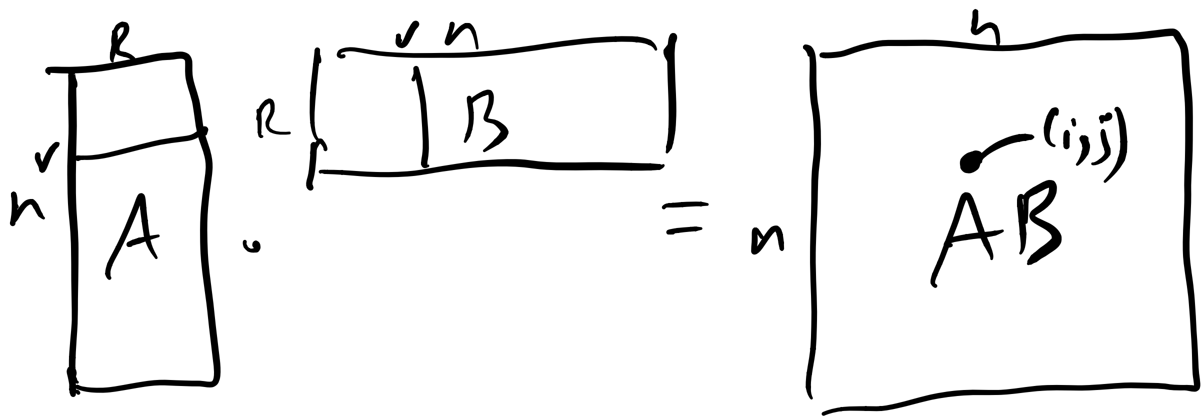
Orthogonal Vectors

Theorem

There is a deterministic algorithm that solves #OV over $\mathbb{F}_2$ in time $O(N^{2-1/\log(d/\log n)})$ for any $d = N^{o(1)}$.

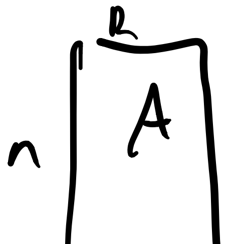
Corollary

There is a deterministic algorithm that, given $A \in \mathbb{F}_2^{n\times r}$ and $B \in \mathbb{F}_2^{r\times n}$, computes the number of ones in AB in time $n^{2-1/\log(r/\log n)}$ for any $r = n^{o(1)}$.

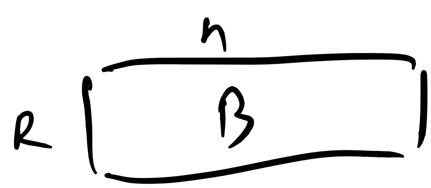


Assume $A \cdot B$ in $O(n^2)$,
compute # ones in $A \cdot B$ $\underline{O(n^2)}$
at best

Actually, compute # ones in time
$n^{2 - \frac{1}{\log(k/\log n)}}$



$\longrightarrow$ n vectors from $\mathbb{F}_2^k$



$\longrightarrow$ n vectors from $\mathbb{F}_2^k$

orthogonal pairs = # zeros in $A \cdot B$

Non-deterministic Hierarchy Theorem

Theorem

If f, g are time constructible and $f(n+1) = o(g(n))$, then

$$\mathbf{NTIME}[f(n)] \subsetneq \mathbf{NTIME}[g(n)]\,.$$

Moreover, $\exists$ unary language $L \subseteq \{1\}^*$

$f(n) = 2^n$, $g(n) = 2^n/n$

Corollary

There exists a unary language $L \subseteq \{1\}^*$, $L \in \mathbf{NTime}[2^n] \setminus \mathbf{NTime}[2^n/n]$.

PCP

randomness

queries

Let $r, q : \mathbb{N} \to \mathbb{N}$, then **PCP**$(r, q)$ is the class of languages L s.t. there exists a poly-time probabilistic V:

- Efficient: For $x \in \{0,1\}^n$ and a proof π, V has $O(r(n))$ random bits, makes $O(q(n))$ queries to π
- Completeness: If $x \in L$, then V accepts with probability 1
- Soundness: if $x \notin L$, then V accepts with probability $< s$

Smooth PCPs

Definition

A PCP is smooth if V queries every variable with equal probability (queries every bit of the proof with equal probability).

Smooth PCPs

Definition

A PCP is smooth if V queries every variable with equal probability (queries every bit of the proof with equal probability).

If your proof is not correct, but differs from it in a few positions, chances are your proof will be accepted by a smooth verifier!

Rectangular PCPs

Example: $\boxed{\text{Max-2LIN}}$ ✓ $\qquad x \oplus y$

PCP: $L \subseteq \{1\}^*$

$\boxed{x = 1^n} \longrightarrow$ formula $\quad x_1, \ldots, x_{N^2}$ ✓

clauses $\quad C_1, \ldots, C_{M^2}$

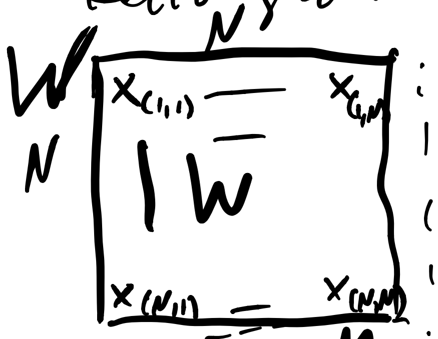
$$C_i = (x_j \oplus x_k)$$

$$(x_1 \oplus x_3)\,(x_j \oplus x_k)\ \ldots\ (x_N \oplus x_{N^2})$$

If $x \in L \Rightarrow \exists\, \pi \in \{0,1\}^{N^2}$ s.t. all clauses are SAT.

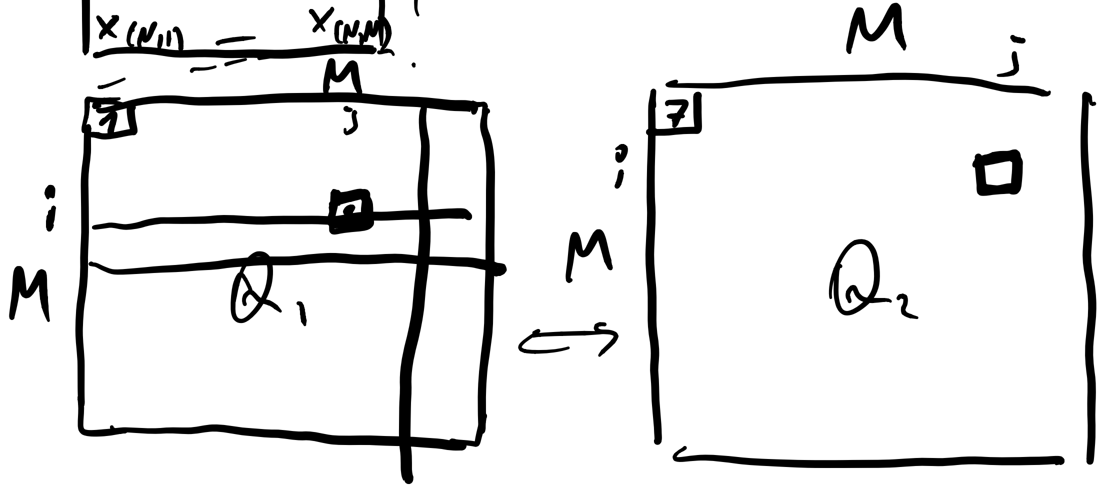
If $x \notin L \Rightarrow \forall\, \pi \in \{0,1\}^{N^2} \Rightarrow \leq 0.9 M^2$ clauses are SAT

Rectangular PCP



$$\underbrace{\overline{(x_1 \oplus x_7)} + \dots \oplus \overline{(x_N \oplus x_{N^2})}}_{M^2}$$

(1,1) (i,j)



$Q_1(i,j)$ = index of first var of clause # (i,j)

$Q_2(i,j)$ = index of second var of clause # (i,j)

N^2 var $x_{(i,j)}$ $1 \le i,j \le N$

$$Q_1(i,j) = (\overset{\in[N]}{a_1(i,j)}, \overset{\in[N]}{a_2(i,j)})$$

$\Rightarrow$ 1st var in clause (i,j) is

$$x_{a_1(i,j),\, a_2(i,j)}$$

$$Q_2(i,j) = (b_1(i,j), b_2(i,j))$$

Rectangular PCP:

$$Q_1(i,j) = (a_1(i,j), a_2(i,j))$$

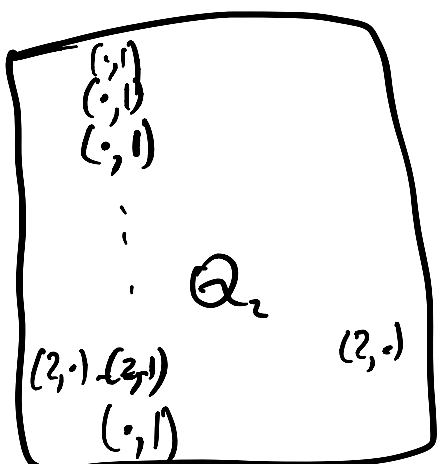
<u>BUT</u> $a_1(i,j) = a_1(i)$

$$a_2(i,j) = a_2(j)$$

$$Q_2(i,j) = (b_1(i,j), b_2(i,j))$$

$$b_1(i,j) = b_1(i)$$

$$b_2(i,j) = b_2(j)$$



matrices describing clauses

matrix w variables

$$Q_2 = \underline{B_1} \cdot \underline{W} \cdot \underline{B_2}$$

$$Q_1 = \underline{A_1} \cdot \underline{W} \cdot \underline{A_2}$$

Rectangular

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[2^n]$, there exists a PCP verifier V that

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[\underbrace{2^n}]$, there exists a PCP verifier V that

- *# of random bits is $n + o(n)$*

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[2^n]$, there exists a PCP verifier V that

- *# of random bits is $n + o(n)$*
- *query complexity is $O(1)$*

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[2^n]$, there exists a PCP verifier V that

- *# of random bits is $n + o(n)$*
- *query complexity is $O(1)$*
- *proof of length $2^n \operatorname{poly}(n)$* = # of clauses

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[2^n]$, there exists a PCP verifier V that

- *# of random bits is $n + o(n)$*
- *query complexity is $O(1)$*
- *proof of length $2^n \operatorname{poly}(n)$*
- *V runs in time $2^{(1-\varepsilon)n}$*

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[2^n]$, there exists a PCP verifier V that

- *# of random bits is $n + o(n)$*
- *query complexity is $O(1)$*
- *proof of length $2^n \operatorname{poly}(n)$*
- *V runs in time $2^{(1-\varepsilon)n}$*
- *V is smooth*

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathsf{NTIME}[2^n]$, there exists a PCP verifier V that

- *# of random bits is $n + o(n)$*
- *query complexity is $O(1)$*
- *proof of length $2^n \operatorname{poly}(n)$*
- *V runs in time $2^{(1-\varepsilon)n}$*
- *V is smooth*
- *V is almost rectangular*

Efficient Rectangular PCPs

Theorem (BHPT20)

For any $L \in \mathbf{NTIME}[2^n]$, there exists a PCP verifier V that

- *# of random bits is* $\boxed{n + o(n)}$
- *query complexity is* $O(1)$
- *proof of length* $\boxed{2^n \operatorname{poly}(n)}$
- *V runs in time* $2^{(1-\varepsilon)n}$
- *V is smooth*
- *V is almost* $\boxed{\textit{rectangular}}$
- *the CSP problem is almost* $\boxed{\textit{MAX-2LIN}}$

$2^{n + \text{dual vars}}$

$x \in L \Rightarrow f_L$ with $2^n \operatorname{poly}(n)$ clauses and 2^n variables

Rigidity in P^{NP}

Theorem ([AC19,BHPT20])

There is a P^{NP} machine that for infinitely many n, on input 1^n, outputs a matrix $M_n \in \mathbb{F}_2^{n\times n}$ that has rigidity

$$\mathcal{R}_{M_n}^{\mathbb{F}_2}(r) \geq \Omega(n^2)$$

for $r = 2^{\Omega(\log n/\log\log n)}$.

Theorem ([AC19,BHPT20])

There is a P^{NP} *machine that for infinitely many n, on input* 1^n*, outputs a matrix* $M_n \in \mathbb{F}_2^{n\times n}$ *that has rigidity*

$$\mathcal{R}_{M_n}^{\mathbb{F}_2}(r) \geq \Omega(n^2)$$

for $r = 2^{\Omega(\log n/\log\log n)}$.

NDT Hierarchy thm:

$L \subseteq \{1\}^n$, $L \in \mathrm{NTime}[2^n]$.

$L \notin \mathrm{NTime}[2^n/n]$.

PCP for L:

we have a MAX-2-Lin fla φ

s.t.

if $x \in L \Rightarrow \boxed{\varphi}$ is SAT

if $x \notin L \Rightarrow \leq 0.9$ fraction of clauses is SAT

$x \in L \quad \exists\, W \in \{0,1\}^{2^{n/2} \times 2^{n/2}} =$

$= \boxed{\{0,1\}^{N\times N}}$

$N = 2^{n/2}$

$\boxed{W \text{ is rigid}}$

Assume W is not rigid $\Rightarrow$ L is $NT[2^n/n]$

$\exists\ W' \in \{0,1\}^{N \times N}$ s.t.

$\|W - W'\| \le 0.1 \cdot N^2$

and $\operatorname{rank}(W') < R = 2^{\log n/\log\log n}$

PCP is smooth $\Rightarrow$

V accepts $\boxed{W}$ w.p 1.

V accepts $\boxed{W'}$ w.p 0.9

$\checkmark\ \boxed{x \in L} \Rightarrow \boxed{V}$ accepts $\boxed{W'}$ w.p. 0.9

$\checkmark\ \boxed{x \notin L} \Rightarrow V$ accepts Π w.p. $\le s = 0.7$.

V accepts W' w.p ≥ 0.9 or ≤ 0.7.

I can distinguish

in $NTime[2^n/n] \Rightarrow$

$L \in NTime[2^n/n]$ —

contradicts assumption

$L \in NTime[2^n] \setminus NTime[2^n/n]$

Remains to show $NTime[2^n/n]$

whether V accepts w' w.p. ≥ 0.9

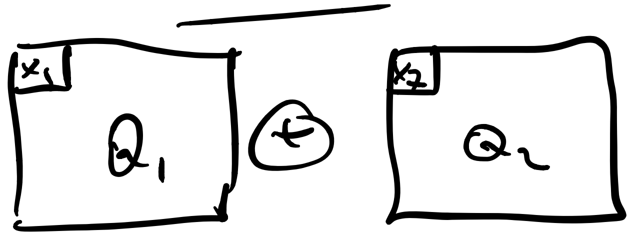
w.p ≤ 0.7.

$\#$ of SAT clauses, where clauses are specified by matrices Q_1, Q_2

$(x_1 \oplus x_7)(\_\_\_\ )$

$Q_1 \oplus Q_2$

$\Downarrow$



$\#$ of ones in the matrix $Q_1 \oplus Q_2$

$= \#$ of sat clauses $\geq 0.9\, M^2$

$\leq 0.7\, M^2$

PCP is Rectangular:

$Q_1 = A_1 \cdot \boxed{W'} \cdot A_2$ $\qquad rk(W') \le R$

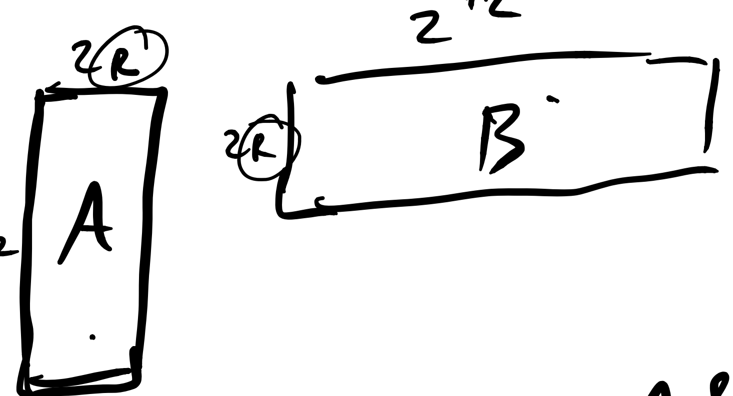
$Q_2 = B_1 \cdot W' \cdot B_2$ $\qquad rk(W') \le R$

$\Rightarrow rk(Q_1), rk(Q_2) \le R$

~~$Q \le$~~ $\Rightarrow rk(Q_1 + Q_2) \le rk(Q_1) + rk(Q_2) \le$

$\le 2R$

$Q_1 + Q_2 =$



Non-deterministic time: guess $A \& B$.

$\#OV$: deterministic $\ll (2^{n/2})^2$

$= 2^n/n$

Summary of Semi-explicit Constructions

construction	rigidity	run-time

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA

Summary of Semi-explicit Constructions

Goal: E^{NP}

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA
brute force	$\mathcal{R}(\varepsilon n) \geq \frac{n^2}{\log n}$	2^{n^2}

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA
brute force	$\mathcal{R}(\varepsilon n) \geq \frac{n^2}{\log n}$	2^{n^2}
explicit	$\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$	$\mathrm{poly}(n)$

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA
brute force	$\mathcal{R}(\varepsilon n) \geq \frac{n^2}{\log n}$	2^{n^2}
explicit	$\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$	$\text{poly}(n)$
Hankel	$\mathcal{R}(r) \geq \frac{n^3}{r^2 \log n}$	2^n

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA
brute force	$\mathcal{R}(\varepsilon n) \geq \frac{n^2}{\log n}$	2^{n^2}
explicit	$\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$	poly(n)
Hankel	$\mathcal{R}(r) \geq \frac{n^3}{r^2 \log n}$	2^n
sub-exponential	$\mathcal{R}(n^{0.5-\varepsilon}) \geq \frac{n^2}{\log n}$	$\boxed{2^{n^{1-\varepsilon}}}$

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA
brute force	$\mathcal{R}(\varepsilon n) \geq \frac{n^2}{\log n}$	2^{n^2}
explicit	$\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$	$\mathrm{poly}(n)$
Hankel	$\mathcal{R}(r) \geq \frac{n^3}{r^2 \log n}$	2^n
sub-exponential	$\mathcal{R}(n^{0.5-\varepsilon}) \geq \frac{n^2}{\log n}$	$2^{n^{1-\varepsilon}}$
sparse	$\mathcal{R}(\varepsilon n) \geq n^{1+\delta}$	$2^{n^{1+\delta} \log n}$

Summary of Semi-explicit Constructions

construction	rigidity	run-time
Vanderm. alg. ind	$\mathcal{R}(\sqrt{n}) \geq \delta n^2$	NA
$\sqrt{p_i}$	$\mathcal{R}(\varepsilon n) \geq \delta n^2$	NA
brute force	$\mathcal{R}(\varepsilon n) \geq \frac{n^2}{\log n}$	2^{n^2}
explicit	$\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$	$\mathrm{poly}(n)$
Hankel	$\mathcal{R}(r) \geq \frac{n^3}{r^2 \log n}$	2^n
sub-exponential	$\mathcal{R}(n^{0.5-\varepsilon}) \geq \frac{n^2}{\log n}$	$2^{n^{1-\varepsilon}}$
sparse	$\mathcal{R}(\varepsilon n) \geq n^{1+\delta}$	$2^{n^{1+\delta} \log n}$
PCP	$\mathcal{R}(\underline{2^{\log n / \log \log n}}) \geq \delta n^2$	$\boxed{\mathsf{P}^{\mathsf{NP}}}$