Matrix Rigidity

Rigidity and communication complexity

weak LB on rigidity ⇒ CC lower bound

$E^{NP} \notin PH^{cc}$

$P \; ? \; PH^{cc}$

Sasha Golovnev

December 7, 2020

PH

$$\Sigma_0^p = \Pi_0^p = \mathsf{P}$$

$$
\begin{tikzcd}[column sep=small]
 & \Sigma_0^P = \Pi_0^P = P = \Delta_1^P = \Sigma_1^P \cap \Pi_1^P \arrow[dl] \arrow[dr] & \\
\Sigma_1^P = NP \arrow[dr] \arrow[dd] & & \underline{\Pi_1}^P = coNP \arrow[dl] \arrow[dd] \\
 & \underline{\Delta_2}^P = \Sigma_2^P \cap \Pi_2^P = P^{NP} \arrow[dl] \arrow[dr] & \\
\underline{\Sigma_2}^P = NP^{NP} \arrow[d] & & \underline{\Pi_2}^P = coNP^{coNP} \arrow[d] \\
\underline{\Sigma_3}^P = NP^{\Sigma_2^P} \arrow[d] & & \Pi_3^P = coNP^{\Pi_2^P} \arrow[d] \\
\vdots & & \vdots
\end{tikzcd}
$$

PH

$$\Sigma_0^p = \Pi_0^p = \mathsf{P}$$

$$\Sigma_i^p = (\mathsf{NP})^{\Sigma_{i-1}^p} \qquad \Pi_i^p = (\mathsf{coNP})^{\Pi_{i-1}^p}$$

PH

Polynomial Hierarchy

$$\Sigma_0^p = \Pi_0^p = \mathsf{P}$$

$$\Sigma_i^p = (\mathsf{NP})^{\Sigma_{i-1}^p} \qquad \Pi_i^p = (\mathsf{coNP})^{\Pi_{i-1}^p}$$

$$\boxed{\mathsf{PH}} = \cup_{i=1}^{\infty} \Sigma_i^p = \bigcup_{i=1} \Pi_i^p ?$$

$$= \bigcup_{i=1} (\Sigma_i^p \cup \Pi_i^p) ? \ldots$$

$L \in \Sigma_1^P = NP$ poly-time alg M

$x \in \{0,1\}^n$

$x \in L \iff \exists v_1 \in \{0,1\}^{poly(n)}$

$M(x, v_1) = \text{True}$

$L \in \Sigma_2^P$ poly-time alg M

$x \in \{0,1\}^n$

$x \in L \iff \exists v_1 \in \{0,1\}^{poly(n)}$

$\forall v_2 \in \{0,1\}^{poly(n)}$

$M(x, v_1, v_2) = \text{True}$

$L \in \Sigma_k^P$ poly time alg M

$x \in \{0,1\}^n$ $Q \in \{\exists, \forall\}$

$x \in L \iff \exists v_1 \in \{0,1\}^{poly(n)}$

$\forall v_2 \in \{0,1\}^{poly(n)}$

$----$

$Q\, v_k \in \{0,1\}^{poly(n)}$

$M(x, v_1, \ldots, v_k) = \text{True}$

PH^{cc}

P^{cc} = problems with $O(\text{poly} \log n)$ communication

$F : \{0,1\}^{2n} \to \{0,1\}$

Alice $x \in \{0,1\}^n$ $\xleftrightarrow{\text{communicate}}$ Bob $y \in \{0,1\}^n$

$F(x,y)$

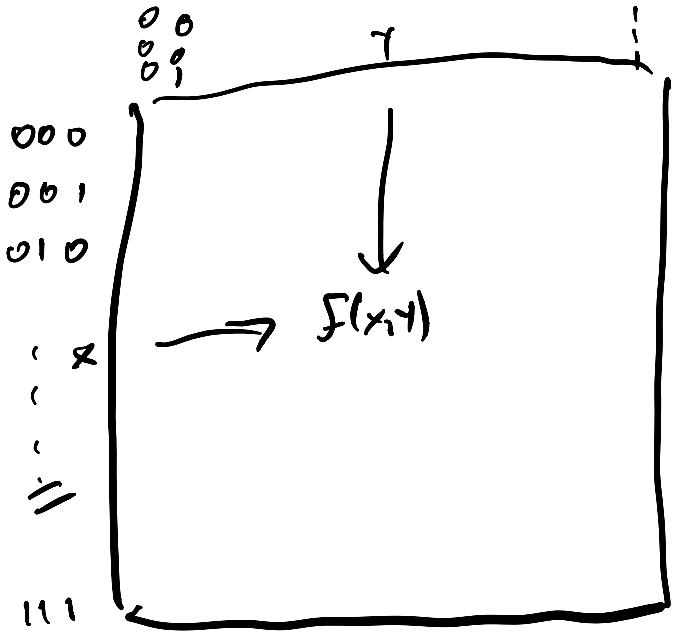
Goal: minimize communication

$CC(F) \leq n+1$

Alice $\xrightarrow{x}$ Bob

Bob $\xrightarrow{F(x,y)}$ Alice

Values of x (Alice's input)

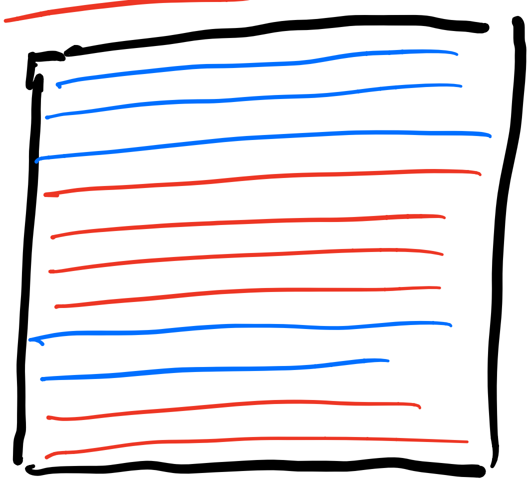


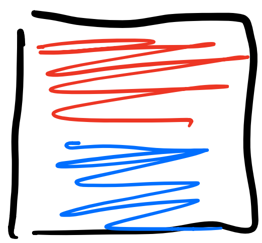
Values of y (Bob's input)

$M =$

$M \in \{0,1\}^{2^n \times 2^n}$

Imagine $CC(f) = 1$



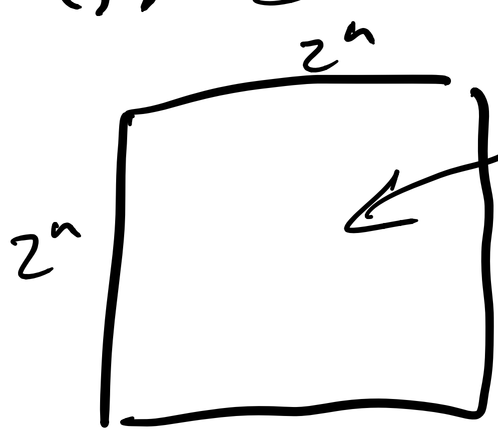


Rank-1 matrix

$CC(f)=2$

0	0
1	1

$CC(f) = \underline{k}$



can be partitioned into $\underline{2^k}$ submatrices, each submatrix is "monochromatic"

Functions f whose matrices can be partitioned into poly(n) monochromatic matrices form P^{cc}

$\mathsf{PH}^{\mathsf{cc}}$

$\mathsf{P}^{\mathsf{cc}} =$ problems with $O(\text{poly}\log n)$ communication

$\mathsf{NP}^{\mathsf{cc}} =$ problems with $O(\text{poly}\log n)$ non-deterministic communication

$\mathsf{coNP}^{\mathsf{cc}}$

$\mathsf{PH}^{\mathsf{cc}}$

$\mathsf{P}^{\mathsf{cc}} =$ problems with $O(\operatorname{poly}\log n)$ communication

$\mathsf{NP}^{\mathsf{cc}} =$ problems with $O(\operatorname{poly}\log n)$
non-deterministic communication

$\cdots$

PH^{cc}

$\mathrm{P}^{cc} =$ problems with $O(\text{poly}\log n)$ communication

$\mathrm{NP}^{cc} =$ problems with $O(\text{poly}\log n)$ non-deterministic communication

$\dots$

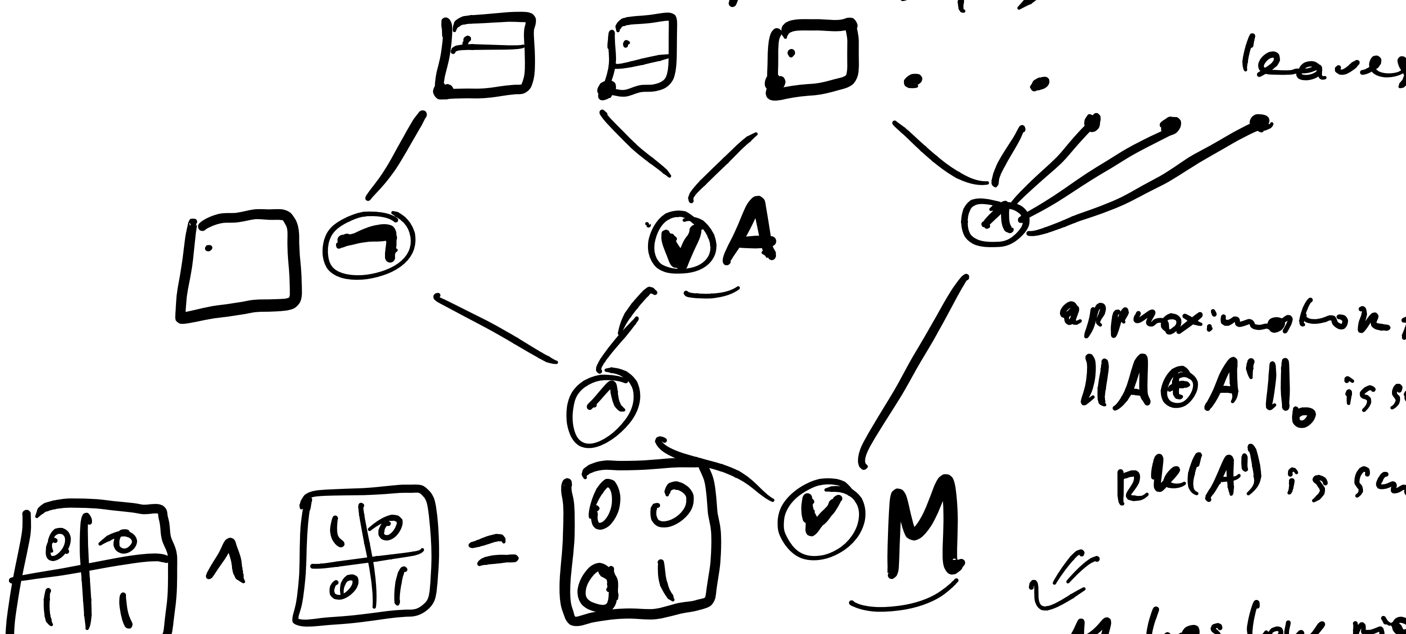
$$\boxed{\mathrm{PH}^{cc}} = \cup_{i=1}^{\infty} \Sigma_i^{cc}$$

Find a language $\notin PH^{cc}$

Characterization of $\boxed{\mathrm{PH}^{cc}}$

Leaves are rank-1 matrices, gates are bitwise $\wedge$, $\vee \neg$.

$M \in \{0,1\}^{n \times n}$



approximation A'

$\|A \oplus A'\|_0$ is small

$\mathrm{rk}(A')$ is small

$\Rightarrow$ M has low rigidity

Characterization of $\mathbf{PH}^{cc}$

Leaves are rank-1 matrices, gates are bitwise $\wedge, \vee \neg$.

Theorem (BFS86)

Every matrix $M \in \mathbb{F}_2^{n \times n}$ from $M \in \mathbf{PH}^{cc}$ can be computed by a constant-depth circuit of size $2^{\log \log n^{O(1)}}$ over the basis $\{\wedge, \vee\}$.

"weak" rigidity LB for M implies M cannot be computed by

Approximation of OR

Lemma (Raz89)

Let $A_1, \ldots, A_k \in \mathbb{F}_2^{n \times n}$ *be matrices of rank* $\leq r$, *and*

$$A = \bigvee_{i=1}^{k} A_i \,.$$

non-rigidity of A

For every $s \geq 1$, *there exists a matrix* L *s.t.* $\|A + L\|_0 \leq n^2/2^s$ *and*

$$\mathrm{rk}(L) \leq 1 + (1 + rk)^s \,.$$

$A_1, \dots, A_k$

$\mathrm{rk}(A_1), \dots, \mathrm{rk}(A_k) \le R$

Want to approximate A

$$\boxed{A} = \bigvee_{i=1}^{k} A_i$$

$B \in \mathbb{F}_2^{n \times n}$ random : $\mathrm{rk}(B) \le k \cdot R$ ✓

$$B = A_1 \cdot \lambda_1 \oplus A_2 \cdot \lambda_2 \oplus \dots \oplus A_k \cdot \lambda_k$$

$\lambda_1, \dots, \lambda_k \in \{0,1\}$ are ind. uniformly random

If $A_{ij} = 0 \Rightarrow$
$(A_1)_{ij} = (A_2)_{ij} = \dots = (A_k)_{ij} = 0$
$\Rightarrow B_{ij} = 0$

If $A_{ij} = 1 \Rightarrow (A_t)_{ij} = 1$ for some $t \in \{1, \dots, k\}$

$B_{ij} = 1$ w.p. $\frac{1}{2}$

$$C = \bigvee_{t=1}^{s} B_t$$

C approximates A much better.

If $A_{ij} = 0 \Rightarrow (B_t)_{ij} = 0$

$\Rightarrow C_{ij} = 0$

If $A_{ij} = 1 \Rightarrow (B_t)_{ij} = 0$ w.p. $1/2$

$(C_{ij} = 0)$ only w.p $\left(\frac{1}{2}\right)^s$

$A_{ij} = C_{ij}$ w.p. $1 - \left(\frac{1}{2}\right)^s$

$E\|A \oplus C\|_0 \leq \left(\frac{1}{2}\right)^s \cdot n^2$

C - approximation of A

$\exists$ a matrix C s.t.

(1) $\|A \oplus C\|_0 \leq \frac{n^2}{2^s}$

(2) $rk(C) \lessapprox rk(B)^s = (rk)^s$ $\square$

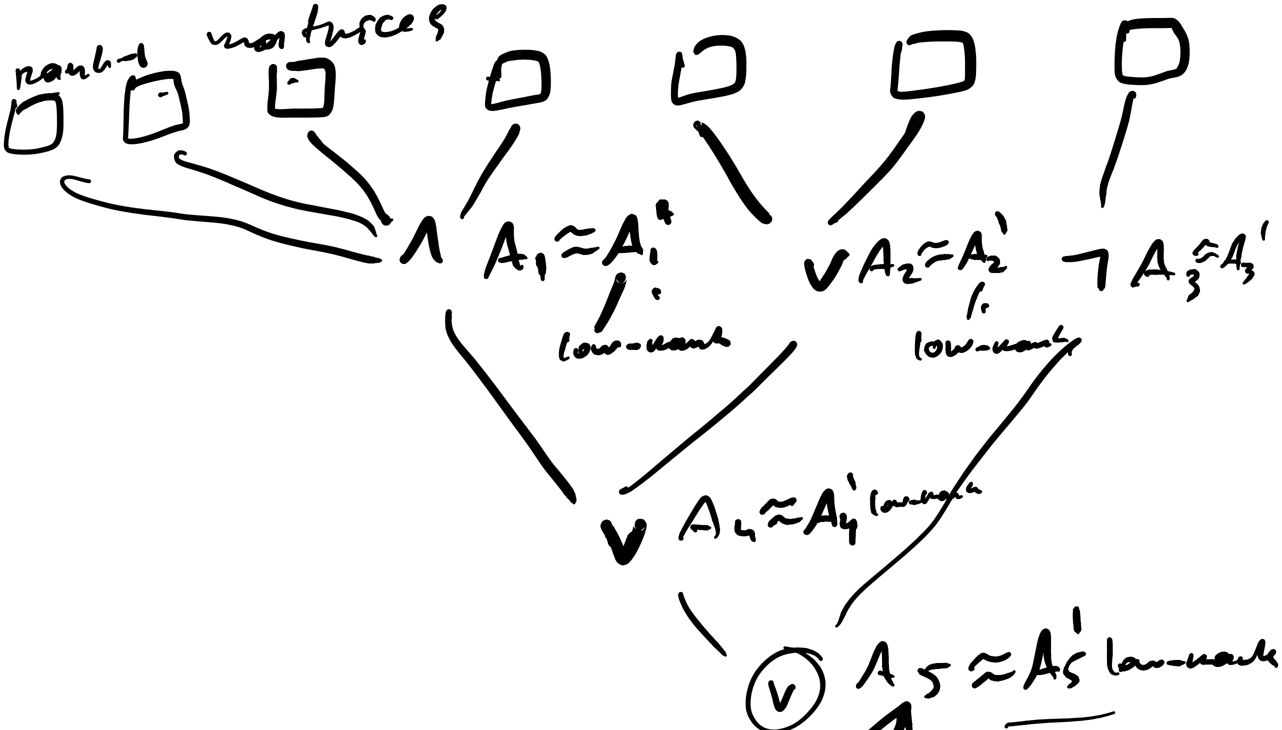
Circuit Lower Bound

Theorem (Raz89)

Let $f(r) = (\log r)^{1/(d+1)}$. *If* $M \in \mathbb{F}_2^{n \times n}$ *has rigidity*

$$\boxed{\mathcal{R}_M^{\mathbb{F}_2}(r) \geq n^2/2^{f(r)}},$$

then every depth-d circuit computing M *has size at least* $2^{\Omega(f(r))}$.



I compute a matrix that is close in ham distance, but has low rank.

Thus, A_5 is not rigid

Rigidity and Communication Complexity

Corollary

If $M \in \mathbb{F}_2^{n \times n}$ has rigidity

$$\mathcal{R}_M^{\mathbb{F}_2}(r) \geq \frac{n^2}{2^{\log r^{o(1)}}} \text{ for } r \geq 2^{\log\log n^{\omega(1)}}$$

then $M \notin \mathsf{PH}^{\mathsf{cc}}$.

We know such matrices M in E^{NP}.