The Strength of Equality Oracles in Communication

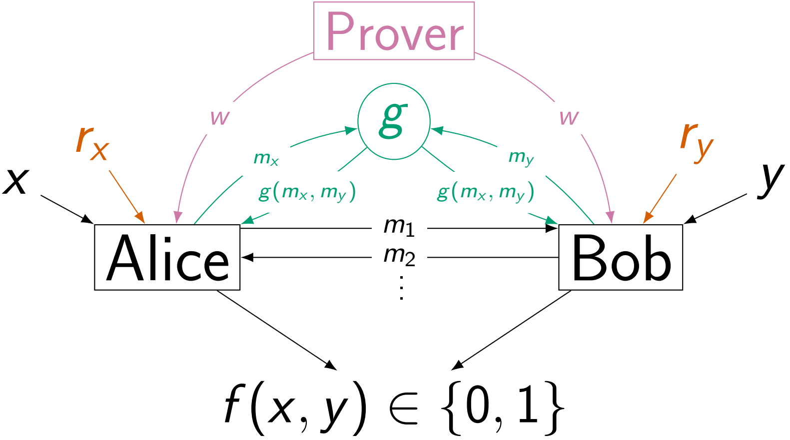
ITCS 2023 (Full Talk)

Toniann Pitassi
Columbia University

Morgan Shirley
University of Toronto

Adi Shraibman
The Academic College of Tel Aviv-Yaffo

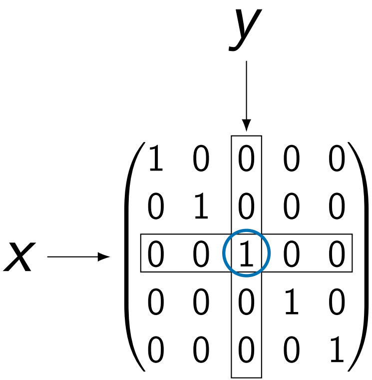
Communication Complexity



“Efficient” means polylogarithmically many bits sent.

Models of interest: Randomness, Nondeterminism, Oracles

Communication Matrices



The EQUALITY Function

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \textsc{Equality}(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Hard for deterministic communication: high rank

Easy for randomized communication: hashing

Example: The GREATER-THAN Function

$$\text{GREATER-THAN}(x, y) = \begin{cases} 1 & \text{if } x > y \\ 0 & \text{if } x \leq y \end{cases}$$

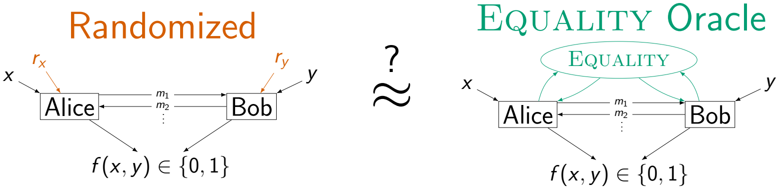
Efficient randomized protocol via reduction to EQUALITY:

- Binary search for first coordinate i where inputs differ:
  - If left half of number is equal, recurse on right
  - Otherwise, recurse on left
- Check whether $x_i > y_i$

0 1 0 0 1 1 0 1

0 1 0 0 0 0 0 1

EQUALITY Oracles vs. Randomness



CLV19 shows that these are *not* the same!

What happens when nondeterminism is added?
What happens when only one oracle call is allowed?

We characterize these models using properties of the **communication matrix**.

Models in Our Paper

	Many calls	One call
Nondeterministic	$\mathsf{NP}^{\mathsf{EQcc}}$	$\exists \cdot \mathsf{EQ}^{\mathsf{cc}}$
Unambiguous Nondeterministic	$\mathsf{UP}^{\mathsf{EQcc}}$	$\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$

Matrix Characterizations: Blocky Matrices

Generalizations of identity matrices, studied in **HHH22**.

$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix} \quad \begin{pmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1 \end{pmatrix} \quad \begin{pmatrix} 1&1&1&0&0\\ 1&1&1&0&0\\ 0&0&0&1&1\\ 0&0&0&1&1\\ 0&0&0&1&1 \end{pmatrix} \quad \begin{pmatrix} 1&0&1&0&1\\ 0&1&0&1&0\\ 0&1&0&1&0\\ 1&0&1&0&1\\ 0&1&0&1&0 \end{pmatrix}$$

These characterize EQUALITY oracle calls.

Blocky covering number of M: Number of blocky matrices needed to *entrywise or* to M. Denoted $C_1^B(M)$.
Blocky partition number of M: Number of blocky matrices needed to *entrywise sum* to M. Denoted $\chi_1^B(M)$.

Blocky Covering Number Example

0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0
0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0
0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0
1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0
1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0
1	1	1	1	1	1	0	1	1	1	1	1	1	0	0	0
1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	0
1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	0

Matrix Characterizations: Binary Factorization Norm

$$\gamma_2(A) = \min_{\substack{X,Y \\ XY^\top = A}} r(X)r(Y)$$

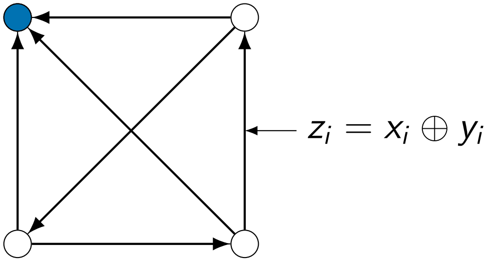
$$\gamma_{2,B}(A) = \min_{\substack{\{0,1\}\text{-matrices } X,Y \\ XY^\top = A}} r(X)r(Y)$$

Matrix Characterizations: Summary

	Many calls	One call	
Nondeterministic	$\mathsf{NP}^{\mathsf{EQ^{cc}}}$	$\exists \cdot \mathsf{EQ}^{\mathsf{cc}}$	$\log C_1^B$ $\log \gamma_{2,B}^{\infty}$
Unambiguous Nondeterministic	$\mathsf{UP}^{\mathsf{EQ^{cc}}}$	$\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$	$\log \chi_1^B$ $\log \gamma_{2,B}$

Application: Upper Bounds

CMS20: The function SINK∘XOR has high randomized complexity, but low approximate rank (disproving LARC).



Application: Upper Bounds

$\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ Protocol:

- Prover announces *unique* vertex v that is a sink.
- Alice computes w such that v is a sink iff $y[v] = w$.
- Check if $y[v] = w$ using $\textsc{Equality}$ oracle.

Application: Upper Bounds

New proof of the upper bound:

- $\textsc{Sink} \circ \mathrm{XOR}$ has an efficient $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ protocol.
- $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ is tightly bounded by $\gamma_{2,B}$.
- $\gamma_{2,B}$ is lower-bounded by γ_2.
- γ_2 is lower-bounded by approximate rank.

So low $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ complexity implies low approximate rank!

Corollary: $\mathsf{P}^{\mathsf{EQcc}} \subsetneq \mathsf{UP}^{\mathsf{EQcc}}$ (contrast with $\mathsf{P}^{\mathsf{cc}} = \mathsf{UP}^{\mathsf{cc}}$).

Application: Lower Bounds

CLV19 separates $\mathsf{P}^{\mathsf{EQcc}}$ from randomized communication .

What about $\mathsf{NP}^{\mathsf{EQcc}}$ and $\mathsf{MA}^{\mathsf{cc}}$?

Our techniques help strengthen the proof from **CLV19** to separate $\mathsf{NP}^{\mathsf{EQcc}}$ from $\mathsf{MA}^{\mathsf{cc}}$.

Application: Lower Bounds (Proof Sketch)

$$\frac{\alpha}{c\sqrt{\beta}}$$

Number of ones

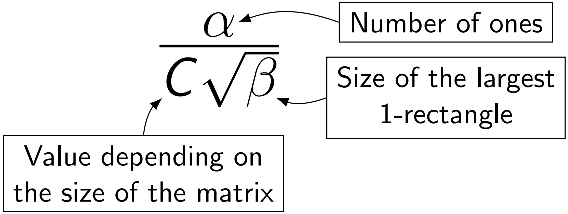
Size of the largest 1-rectangle

Value depending on the size of the matrix

Application: Lower Bounds (Proof Sketch)

0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0
0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0
0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0
1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0
1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0
1	1	1	1	1	1	0	1	1	1	1	1	1	0	0	0
1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	0
1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	0

Application: Lower Bounds (Proof Sketch)



$E_x(i)$: event that $R_i \in \mathcal{R}$ contains row x
$E_y(i)$: event that $R_i \in \mathcal{R}$ contains row y
m, n: dimensions of matrix M

$$\begin{aligned}(m+n)C_1^B(M) &\geq \sum_x \sum_i E_x(i) + \sum_y \sum_i E_y(i) = \sum_i \left(\sum_x E_x(i) + \sum_y E_y(i) \right) \\ &\geq 2 \sum_i \sqrt{\left(\sum_x E_x(i) \right) \left(\sum_y E_y(i) \right)} = 2 \sum_i \sqrt{\sum_{x,y} (E_x(i) E_y(i))} \\ &= 2 \sum_i \sqrt{|R_i|}.\end{aligned}$$

Application: Lower Bounds (Proof Sketch)

$$\frac{\alpha}{C\sqrt{\beta}}$$

Number of ones

Size of the largest 1-rectangle

Value depending on the size of the matrix

$$C \cdot C_1^B(M) \geq \sum_i \sqrt{|R_i|} \qquad |R_i| \leq \beta \qquad \sum_i |R_i| \geq \alpha$$

$$C_1^B(M) \geq \Omega\left(\frac{\alpha}{C\sqrt{\beta}}\right)$$

Open Problems

1. HARD — One-sided vs. Two-sided error

2. SOLVED — One-sided error vs. Unambiguous EQUALITY

3. SOLVED — γ_2 vs. γ_2^α

4. γ_2 vs. $\gamma_{2,B}$

5. P^{cc} vs. $\mathsf{NP}^{\mathsf{EQcc}} \cap \mathsf{coNP}^{\mathsf{EQcc}}$

6. P^{cc} vs. $\mathsf{UP}^{\mathsf{EQcc}} \cap \mathsf{coUP}^{\mathsf{EQcc}}$

Open Problems: Intersection Classes

Recall: $\mathsf{P}^{\mathsf{EQcc}} \subsetneq \mathsf{UP}^{\mathsf{EQcc}}$ but $\mathsf{P}^{\mathsf{cc}} = \mathsf{UP}^{\mathsf{cc}}$

AUY83: $\mathsf{P}^{\mathsf{cc}} = \mathsf{NP}^{\mathsf{cc}} \cap \mathsf{coNP}^{\mathsf{cc}}$

What happens if we add Equality oracles here?

$$\mathsf{P}^{\mathsf{cc}} \text{ vs. } \mathsf{NP}^{\mathsf{EQcc}} \cap \mathsf{coNP}^{\mathsf{EQcc}}$$
$$\mathsf{P}^{\mathsf{cc}} \text{ vs. } \mathsf{UP}^{\mathsf{EQcc}} \cap \mathsf{coUP}^{\mathsf{EQcc}}$$

Open Problems: Intersection Classes (Ideas)

Recall: $C_1^B \geq \Omega\left(\frac{\alpha}{C\sqrt{\beta}}\right)$
α is the number of ones in the matrix
β is the size of the largest 1-rectangle of the matrix
C is a value depending on the size of the matrix

If a function is in $\mathrm{NP}^{\mathrm{EQcc}} \cap \mathrm{coNP}^{\mathrm{EQcc}}$:

- If it has a lot of 1s, it has a large 1-rectangle.
- If it has a lot of 0s, it has a large 0-rectangle.
- Therefore, it has a large 1-rectangle or a large 0-rectangle!

Thanks!