ACC^0 and Multiparty Communication

Fighting the $\log n$ barrier

Yassine Hamoudi

December 6, 2017

IRIF, Université Paris Diderot

arXiv:1710.01969

Two player model

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

Alice

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

$F(x,y) =?$

$$\xleftrightarrow[\text{channel}]{0,1}$$

Bob

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

$F(x,y) =?$

Two player model

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

Alice

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

$F(x,y) = ?$

$0, 1$

channel

Bob

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

$F(x,y) = ?$

Number of bits communicated?

- $\mathrm{D}_2(F)$: cost of the most efficient deterministic protocol
- $\mathrm{R}_2(F)$: cost of the most efficient randomized protocol with error 1/3

Two player simultaneous model

Alice

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

Bob

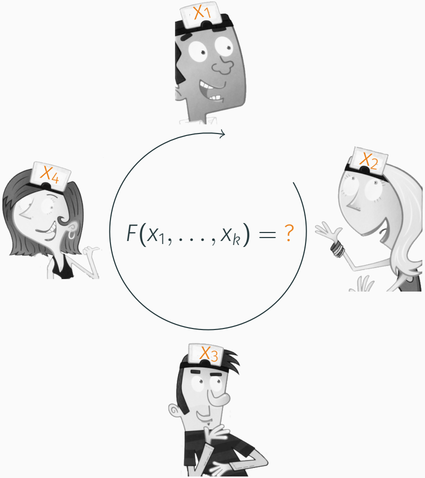
$y \in \{0,1\}^n$

Referee

$F(x,y) = ?$

Simultaneous communication complexity: $\mathrm{D}_2^{||}(F)$ and $\mathrm{R}_2^{||}(F)$

Number On the Forehead model



Number On the Forehead (NOF) model:

- Player i does not see x_i. Communicate by broadcasting
- Communication cost: $\mathrm{D}_k(F)$, $\mathrm{R}_k(F)$, $\mathrm{D}_k^{||}(F)$ and $\mathrm{R}_k^{||}(F)$

A protocol is efficient if it has cost $\operatorname{polylog} n$

Two lines of research:

- Efficient protocols for ”interesting” functions $\leftarrow$ this talk
- Strong lower bounds for some functions $\leftarrow$ harder as k grows up

Outline

The $\log n$ barrier problem

Efficient simultaneous protocols for $\textsc{Maj} \circ \textsc{Maj}_t$

(Far) Beyond $\log n$ players

Conclusion

The $\log n$ barrier problem

What are the best lower bounds in the NOF model so far?

The $\log n$ barrier

What are the best lower bounds in the NOF model so far? $\widetilde{\Omega}\left(n/2^k\right)$

$\rightarrow$ no hard function is known for $k \geq \log n$ players

What are the best lower bounds in the NOF model so far? $\widetilde{\Omega}\left(n/2^k\right)$
$\rightarrow$ no hard function is known for $k \geq \log n$ players

The $\log n$ barrier:

Find a function F such that $\mathrm{D}_k^{||}(F) \gg \log n$ when $k \gtrsim \log n$.

What are the best lower bounds in the NOF model so far? $\widetilde{\Omega}\left(n/2^k\right)$
$\rightarrow$ no hard function is known for $k \geq \log n$ players

The $\log n$ barrier:

Find a function F such that $\mathrm{D}_k^{||}(F) \gg \log n$ when $k \gtrsim \log n$.

Why is it interesting?

- A uniformly random function is almost surely hard [BNS92, For06]
- The only general lower bound technique known so far (discrepancy method) seems intrinsically stuck at $\log n$ players
- Connections with ACC^0 lower bounds

P vs NP and circuits lower bounds

- P/poly = languages recognized by polysize circuits
- Conjecture: $NP \not\subseteq P/poly$ (which implies $P \neq NP$) $\leftarrow$ way too hard

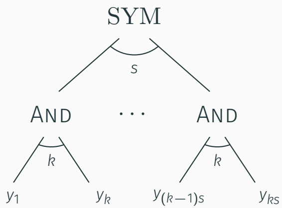
P vs NP and circuits lower bounds

- P/poly = languages recognized by polysize circuits
- Conjecture: $\mathsf{NP} \not\subseteq \mathsf{P/poly}$ (which implies $\mathsf{P} \neq \mathsf{NP}$) $\leftarrow$ way too hard

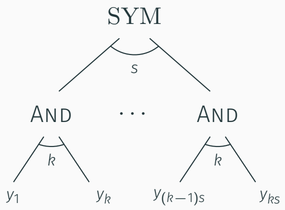
A weaker class: ACC^0

- ACC^0 = languages recognized by polysize constant-depth circuits made of AND, OR, NOT and $\textsc{Mod}_m$ gates
- Conjectures:
  - $\textsc{Maj} \notin \mathsf{ACC}^0$
  - $\mathsf{NP} \not\subseteq \mathsf{ACC}^0$
- Current (breakthrough) result: $\mathsf{NEXP} \not\subseteq \mathsf{ACC}^0$ [Wil14]

$SYM^+(s, k)$ = depth-2 circuits whose top gate are any symmetric function (i.e. only depends on the number of 1), and bottom gates are AND functions

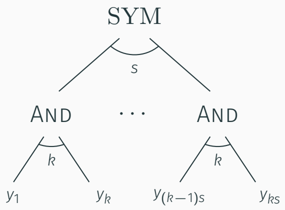


$\mathrm{SYM}^+(s, k)$ = depth-2 circuits whose top gate are any symmetric function (i.e. only depends on the number of 1), and bottom gates are AND functions



For any partition of $y_1, \ldots, y_{ks}$ between $k+1$ players in the NOF model, each AND gate can be computed by at least one player.

$\mathrm{SYM}^+(s, k)$ = depth-2 circuits whose top gate are any symmetric function (i.e. only depends on the number of 1), and bottom gates are AND functions



For any partition of $y_1, \ldots, y_{ks}$ between $k+1$ players in the NOF model, each AND gate can be computed by at least one player.

$\longrightarrow$ simultaneous protocol of cost $\mathcal{O}(k \log s)$ for computing the whole circuit

ACC^0 and the $\log n$ barrier

f is computed by a $\mathsf{SYM}^+(s, k)$ circuit

$\Downarrow$

For any partition of the input between $k+1$ players, there is a simultaneous NOF protocol of cost $\mathcal{O}(k \log s)$ computing f

f is computed by a $\mathsf{SYM}^+(s, k)$ circuit

$\Downarrow$

For any partition of the input between $k+1$ players, there is a simultaneous NOF protocol of cost $\mathcal{O}(k \log s)$ computing f

Theorem ([Yao90, BT94])

$\mathsf{ACC}^0 \subset \mathsf{SYM}^+(2^{\operatorname{polylog} n}, \operatorname{polylog} n)$

ACC^0 and the $\log n$ barrier

f is computed by a $\mathsf{SYM}^+(s, k)$ circuit

$\Downarrow$

For any partition of the input between $k+1$ players, there is a simultaneous NOF protocol of cost $\mathcal{O}(k \log s)$ computing f

Theorem ([Yao90, BT94])

$\mathsf{ACC}^0 \subset \mathsf{SYM}^+(2^{\text{polylog}\, n}, \text{polylog}\, n)$

$\rightarrow$ $\forall$ function $f \in \mathsf{ACC}^0$ and $\forall$ partition of the input between $\sim$ polylog n players, there is a simultaneous NOF protocol for f of cost $\mathcal{O}(\text{polylog}\, n)$.

f is computed by a $\mathrm{SYM}^+(s, k)$ circuit

$\Downarrow$

For any partition of the input between $k+1$ players, there is a simultaneous NOF protocol of cost $\mathcal{O}(k \log s)$ computing f

Theorem ([Yao90, BT94])

$\mathrm{ACC}^0 \subset \mathrm{SYM}^+(2^{\mathrm{polylog}\, n}, \mathrm{polylog}\, n)$

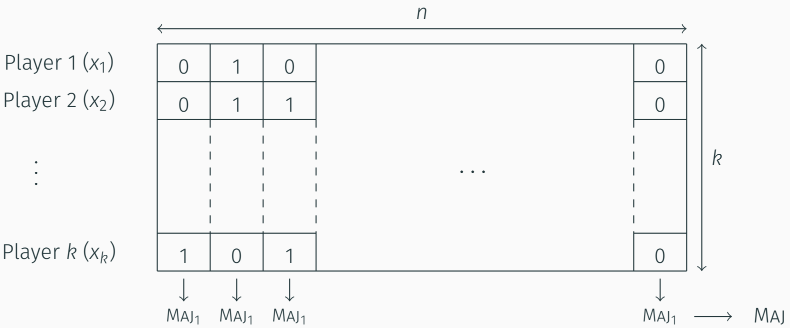
$\rightarrow \forall$ function $f \in \mathrm{ACC}^0$ and $\forall$ partition of the input between $\sim \mathrm{polylog}\, n$ players, there is a simultaneous NOF protocol for f of cost $\mathcal{O}(\mathrm{polylog}\, n)$.

Consequences:

- Contraposition: if a function breaks the $\log n$ barrier then we could obtain "something" that is not in ACC^0
- Conjecture: Majority $\notin$ ACC^0 $\rightarrow$ good candidates for breaking the $\log n$ barrier are the "Majority-like" functions

Efficient simultaneous protocols for $\textsc{Maj} \circ \textsc{Maj}_t$

The Majority of Majority ($\textsc{Maj} \circ \textsc{Maj}_1$) function:



Conjecture ([BKL95]): $\textsc{Maj} \circ \textsc{Maj}_1$ breaks the $\log n$ barrier

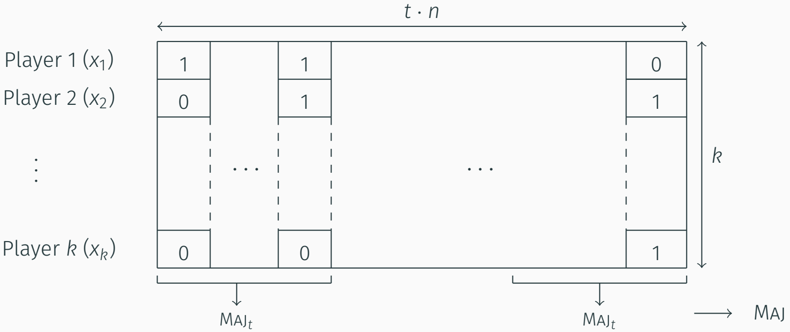
~~Conjecture ([BKL95]): $\textsc{Maj} \circ \textsc{Maj}_1$ breaks the $\log n$ barrier~~

- [BGKL04] $D_k^{||}(\textsc{Maj} \circ \textsc{Maj}_1) = \mathcal{O}\left(\log^3 n\right)$ when $k > 1 + \log n$
- [ACFN15] $D_k^{||}(f \circ g) = \mathcal{O}\left(\log^3 n\right)$ when $k > 1 + 2\log n$ and f is symmetric

A function h : is symmetric if it is invariant under any permutation of its input variables.

$$h(z_1, \dots, z_m) = h(z_{\pi(1)}, \dots, z_{\pi(m)}) \text{ for all permutations } \pi$$

Majority of Majority ($\textsc{Maj} \circ \textsc{Maj}_t$) with larger block-width t:



Conjecture ([BGKL04]): $\textsc{Maj} \circ \textsc{Maj}_{\sqrt{n}}$ breaks the $\log n$ barrier

$\text{MAJ} \circ \text{MAJ}_t$

Conjecture ([BGKL04]): $\text{MAJ} \circ \text{MAJ}_{\sqrt{n}}$ breaks the $\log n$ barrier

Previous result ([CS14]) for $t = \mathcal{O}(\log \log n)$:

- $D_k(\text{MAJ} \circ \text{MAJ}_t) = \mathcal{O}\left(\log^3 n\right)$ when $k > log^{\mathcal{O}(1)} n$
- $R_k^{||}(\text{MAJ} \circ \text{MAJ}_t) = \mathcal{O}\left(\log^3 n\right)$ when $k > log^{\mathcal{O}(1)} n$

Conjecture ([BGKL04]): $\textsc{Maj} \circ \textsc{Maj}_{\sqrt{n}}$ breaks the $\log n$ barrier

Previous result ([CS14]) for $t = \mathcal{O}(\log \log n)$:

- $\mathrm{D}_k(\textsc{Maj} \circ \textsc{Maj}_t) = \mathcal{O}\left(\log^3 n\right)$ when $k > log^{\mathcal{O}(1)} n$
- $\mathrm{R}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_t) = \mathcal{O}\left(\log^3 n\right)$ when $k > log^{\mathcal{O}(1)} n$

Our result: first efficient deterministic simultaneous protocol for some $t > 1$

Theorem

If $k \geq 5^{2^{t-1}} \log n$, then $\mathrm{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_t) = \mathcal{O}\left(k^{2^t} \log n\right)$.

Our protocol : generalization of [BGKL04] to $t > 1$

The Equation Solving protocol of [BGKL04]

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

$\downarrow$ $\downarrow$ $\dots$ $\downarrow$

MAJ_1 MAJ_1 $\text{MAJ}_1 \longrightarrow \text{MAJ}$

y_i = # columns with i one's

The Equation Solving protocol of [BGKL04]

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

$\textsc{Maj}_1 \quad \textsc{Maj}_1 \quad \cdots \quad \textsc{Maj}_1 \longrightarrow \textsc{Maj}$

$y_i = \#$ columns with i one's

$\rightarrow y_0 = 1$

The Equation Solving protocol of [BGKL04]

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

$\textsc{Maj}_1 \quad \textsc{Maj}_1 \quad \cdots \quad \textsc{Maj}_1 \longrightarrow \textsc{Maj}$

$y_i = \#$ columns with i one's

$\rightarrow y_0 = 1, y_1 = 2$

The Equation Solving protocol of [BGKL04]

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

MAJ_1 MAJ_1 $\cdots$ $\mathrm{MAJ}_1 \longrightarrow \mathrm{MAJ}$

$y_i = \#$ columns with i one's

$\rightarrow y_0 = 1, y_1 = 2, y_2 = 1$

The Equation Solving protocol of [BGKL04]

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

$\downarrow$ $\textsc{Maj}_1$ $\quad \downarrow$ $\textsc{Maj}_1$ $\quad \dots \quad \downarrow$ $\textsc{Maj}_1 \longrightarrow \textsc{Maj}$

y_i = # columns with i one's

$\rightarrow y_0 = 1, y_1 = 2, y_2 = 1, \dots$

$$\boxed{\text{Recovering the } y_i\text{'s is enough to compute } \textsc{Maj} \circ \textsc{Maj}_1}$$

The Equation Solving protocol of [BGKL04]

~~0~~	~~0~~	~~1~~	~~1~~	~~0~~	~~1~~	~~1~~	~~1~~	~~1~~	~~1~~
1	0	1	1	0	1	1	0	1	0
0	0	1	1	0	0	1	1	1	0
0	0	1	1	0	1	1	1	1	0
1	0	0	1	1	0	1	0	1	0

- Player 1 sends to the referee:

$$a_i^1 = \#\text{ columns she sees with } i \text{ one's}$$

$\rightarrow a_0^1 = 2, a_1^1 = 1, a_2^1 = 3, \ldots$

The Equation Solving protocol of [BGKL04]

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

- Player 1 sends to the referee:

$$a_i^1 = \#\text{ columns she sees with } i \text{ one's}$$

$\rightarrow a_0^1 = 2, a_1^1 = 1, a_2^1 = 3, \ldots$

- Players 2 to 5 do the same

The Equation Solving protocol of [BGKL04]

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

Note that:

- $b_0 =$

The Equation Solving protocol of [BGKL04]

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

Note that:

- $b_0 = 5y_0$

The Equation Solving protocol of [BGKL04]

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

Note that:

- $b_0 = 5y_0 + y_1$

The Equation Solving protocol of [BGKL04]

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

Note that:

- $b_0 = 5y_0 + y_1$
- $b_1 = 4y_1$

The Equation Solving protocol of [BGKL04]

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

Note that:

- $b_0 = 5y_0 + y_1$
- $b_1 = 4y_1 + 2y_2$

The Equation Solving protocol of [BGKL04]

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

The referee computes:

$$b_i = a_i^1 + \cdots + a_i^5$$

Note that:

- $b_0 = 5y_0 + y_1$
- $b_1 = 4y_1 + 2y_2$
- ...

$$b_i = (k - i)y_i + (i + 1)y_{i+1}$$

The Equation Solving protocol of [BGKL04]

Let $(b_i)_{0 \leq i \leq k-1}$ be integers. Consider the system of equations:

$$\begin{cases} (k-i)y_i + (i+1)y_{i+1} = b_i \\ 0 \leq i \leq k-1 \end{cases}$$

Assume further that

$$y_i \geq 0,\ 0 \leq i \leq k \quad and \quad \sum_i y_i = n$$

The Equation Solving protocol of [BGKL04]

Let $(b_i)_{0 \leq i \leq k-1}$ be integers. Consider the system of equations:

$$\begin{cases} (k-i)y_i + (i+1)y_{i+1} = b_i \\ 0 \leq i \leq k-1 \end{cases}$$

Assume further that

$$y_i \geq 0,\ 0 \leq i \leq k \quad \mathit{and} \quad \sum_i y_i = n$$

Theorem ([BGKL04])
If $k > 1 + \log n$ then it admits at most one integral solution.

The Equation Solving protocol of [BGKL04]

Let $(b_i)_{0 \leq i \leq k-1}$ be integers. Consider the system of equations:

$$\begin{cases} (k-i)y_i + (i+1)y_{i+1} = b_i \\ 0 \leq i \leq k-1 \end{cases}$$

Assume further that

$$y_i \geq 0,\ 0 \leq i \leq k \quad \textit{and} \quad \sum_i y_i = n$$

Theorem ([BGKL04])
If $k > 1 + \log n$ then it admits at most one integral solution.

$\rightarrow$ the referee recovers the y_i's and computes $\textsc{Maj} \circ \textsc{Maj}_1$

Theorem ([BGKL04])

If $k \geq 1 + \log n$, then $\mathsf{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_1) = \mathcal{O}\left(k^2 \log n\right)$.

Theorem ([BGKL04])

If $k \geq 1 + \log n$, then $\mathrm{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_1) = \mathcal{O}\left(k^2 \log n\right)$.

We generalize the equation of [BGKL04] to block-width $t > 1$ and show that it admits at most one integral solution when $k \geq 5^{2^{t-1}} \log n$:

Theorem

If $k \geq 5^{2^{t-1}} \log n$, then $\mathrm{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_t) = \mathcal{O}\left(k^{2^t} \log n\right)$.

Theorem ([BGKL04])

If $k \geq 1 + \log n$, *then* $\mathrm{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_1) = \mathcal{O}\left(k^2 \log n\right)$.

We generalize the equation of [BGKL04] to block-width $t > 1$ and show that it admits at most one integral solution when $k \geq 5^{2^{t-1}} \log n$:

Theorem

If $k \geq 5^{2^{t-1}} \log n$, *then* $\mathrm{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_t) = \mathcal{O}\left(k^{2^t} \log n\right)$.

$\rightarrow$ The protocol is efficient for all constant t and $k = \operatorname{polylog} n$

$\rightarrow$ $\textsc{Maj} \circ \textsc{Maj}_t$ cannot break the $\log n$ barrier for constant t

(Far) Beyond $\log n$ players

(Far) Beyond $\log n$ players

Theorem

If $k \geq 5^{2^{t-1}} \log n$, *then* $\mathrm{D}_k^{||}(\textsc{Maj} \circ \textsc{Maj}_t) = \mathcal{O}\left(k^{2^t} \log n\right)$.

What if $k \gg \log n$?

- The protocol is not efficient (cost $\gg \operatorname{polylog} n$)
- We don't want all players to speak!

Theorem

If $k \geq 5^{2^{t-1}} \log n$*, then* $\mathsf{D}_k^{||}(\mathit{MAJ} \circ \mathit{MAJ}_t) = \mathcal{O}\left(k^{2^t} \log n\right)$.

What if $k \gg \log n$?

- The protocol is not efficient (cost $\gg \operatorname{polylog} n$)
- We don't want all players to speak!

Let's generalize our previous protocol first:

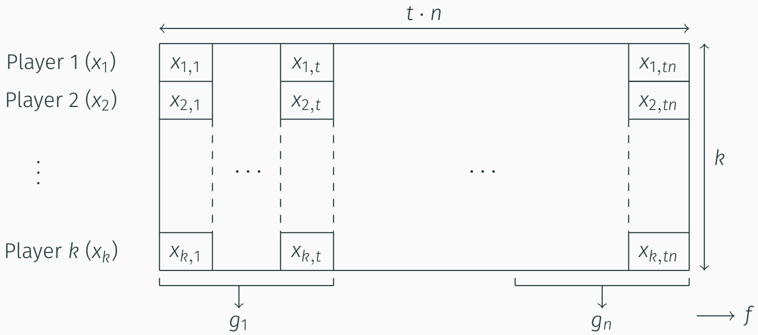
Theorem

If $k \geq 5^{2^t} \log n$*, then* $\mathsf{D}_k^{||}(f \circ (g_1, \ldots, g_n)) = \mathcal{O}\left(k^{2^{t+1}} \log n\right)$ *for any symmetric functions* $f, g_1, \ldots, g_n$.

$\rightarrow$ the proof needs some work (Fourier analysis of boolean functions)

(Far) Beyond $\log n$ players

Different (symmetric) inner functions on each block:



Lemma

If $g : X_1 \times \cdots \times X_k \to \{0,1\}$ is symmetric, then for any $\ell \leq k$ and $(x_{\ell+1}, \ldots, x_k) \in X_{\ell+1} \times \cdots \times X_k$

$$\begin{aligned} g' : \quad X_1 \times \cdots \times X_\ell &\longrightarrow \{0,1\} \\ (x_1, \ldots, x_\ell) &\longmapsto g(x_1, \ldots, x_\ell, x_{\ell+1}, \ldots, x_k) \end{aligned}$$

is also symmetric.

(Far) Beyond $\log n$ players

Lemma

If $g : X_1 \times \cdots \times X_k \to \{0,1\}$ is symmetric, then for any $\ell \leq k$ and $(x_{\ell+1}, \ldots, x_k) \in X_{\ell+1} \times \cdots \times X_k$

$$\begin{array}{rccl} g' : & X_1 \times \cdots \times X_\ell & \longrightarrow & \{0,1\} \\ & (x_1, \ldots, x_\ell) & \longmapsto & g(x_1, \ldots, x_\ell, x_{\ell+1}, \ldots, x_k) \end{array}$$

is also symmetric.

If $k \gg \log n$, set $\ell = 5^{2^t} \log n$ and let the first ℓ players apply the previous protocol on $f \circ (g'_1, \ldots, g'_n)$.

Lemma

If $g : X_1 \times \cdots \times X_k \to \{0,1\}$ is symmetric, then for any $\ell \leq k$ and $(x_{\ell+1}, \ldots, x_k) \in X_{\ell+1} \times \cdots \times X_k$

$$\begin{array}{rccl} g' : & X_1 \times \cdots \times X_\ell & \longrightarrow & \{0,1\} \\ & (x_1, \ldots, x_\ell) & \longmapsto & g(x_1, \ldots, x_\ell, x_{\ell+1}, \ldots, x_k) \end{array}$$

is also symmetric.

If $k \gg \log n$, set $\ell = 5^{2^t} \log n$ and let the first ℓ players apply the previous protocol on $f \circ (g'_1, \ldots, g'_n)$.

Theorem

If $k \geq 5^{2^t} \log n$, then $\mathrm{D}_k^{||}(f \circ (g_1, \ldots, g_n)) = \mathcal{O}\left(\log^{2^{t+1}} n\right)$ for any symmetric functions $f, g_1, \ldots, g_n$.

Conclusion

Conclusion

Our results (for all constant t):

- $\textsc{Maj} \circ \textsc{Maj}_t$ cannot break the $\log n$ barrier
- Efficient protocols for all $f \circ (g_1, \ldots, g_n)$ when $k \geq \operatorname{polylog} n$

Future work : extend to non-constant t

arXiv:1710.01969

Major open problem: stronger lower bounds techniques in the NOF model

→ $\textsc{Maj} \circ \textsc{Maj}_{\sqrt{n}}$ is conjectured to break the $\log n$ barrier

→ The discrepancy method is stuck at $\log n$ players

→ Last week on ECCC (Podolskii, Sherstov): first superconstant ($\Omega(\log n)$) lower-bound for $k \gg \log n$ players

A. Ada, A. Chattopadhyay, O. Fawzi, and P. Nguyen.
The NOF multiparty communication complexity of composed functions.
Computational Complexity, 24(3):645–694, 2015.

L. Babai, A. Gál, P. G. Kimmel, and S. V. Lokam.
Communication complexity of simultaneous messages.
SIAM J. Comput., 33(1):137–166, 2004.

L. Babai, P. G. Kimmel, and S. V. Lokam.
Simultaneous messages vs. communication.
In *12th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 361–372. Springer, 1995.

L. Babai, N. Nisan, and M. Szegedy.
Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs.
J. Comput. Syst. Sci., 45(2):204–232, 1992.

R. Beigel and J. Tarui.
On ACC.
Computational Complexity, 4(4):350–366, 1994.

A. Chattopadhyay and M. E. Saks.
The power of super-logarithmic number of players.
In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, 2014.

J. S. Ford.
Lower Bound Methods for Multiparty Communication Complexity.
PhD thesis, 2006.

R. Williams.
Nonuniform ACC circuit lower bounds.
J. ACM, 61(1):2:1–2:32, 2014.

A. Yao.
On ACC and threshold circuits.
In *Proceedings 31st Annual Symposium on Foundations of Computer Science*, pages 619–627 vol.2, 1990.