Communication Complexity

Yassine Hamoudi

June 20, 2016

Carnegie Mellon University

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

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

$F(x,y) = ?$

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

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

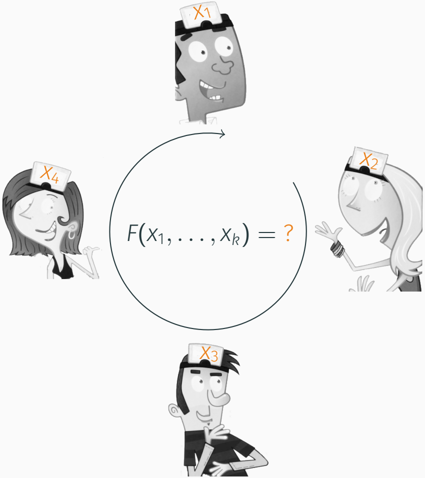
$y \in \{0,1\}^n$

Referee

$F(x,y) = ?$

Simultaneous communication complexity: $D_2^{||}(F)$ and $R_2^{||}(F)$

Number On the Forehead model



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 $\mathrm{R}_k^{||}(F)$

Applications of Communication Complexity

Circuit complexity [HG91, BT94]

Ramsey theory [CFL83]

Branching programs [CFL83]

Proof complexity [BPS07]

Quasirandom graphs [CT93]

Property testing [BBM12]

Streaming algorithms [AMS96]

Game theory [CS04, NS06]

Data structures [MNSW95]

Contents

The $\log n$ barrier and composed functions

The $\log n$ barrier:

Find a function F such that $\mathrm{D}_k^{||}(F) = \omega(\operatorname{polylog} n)$ when $k = \operatorname{polylog} n$.

ACC^0 and the $\log n$ barrier

The $\log n$ barrier:

Find a function F such that $\mathsf{D}_k^{||}(F) = \omega(\text{polylog}\, n)$ when $k = \text{polylog}\, n$.

Motivations:

- ACC^0 = functions computable by polysize constant-depth circuits made of AND, OR, NOT and MOD_m gates
- NEXP $\not\subseteq$ ACC^0 [Wil14]
- Conjecture: NP $\not\subseteq$ ACC^0

ACC^0 and the $\log n$ barrier

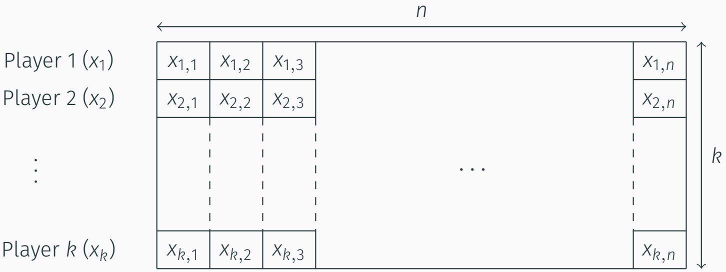
The $\log n$ barrier:

Find a function F such that $\mathrm{D}_k^{||}(F) = \omega(\operatorname{polylog} n)$ when $k = \operatorname{polylog} n$.

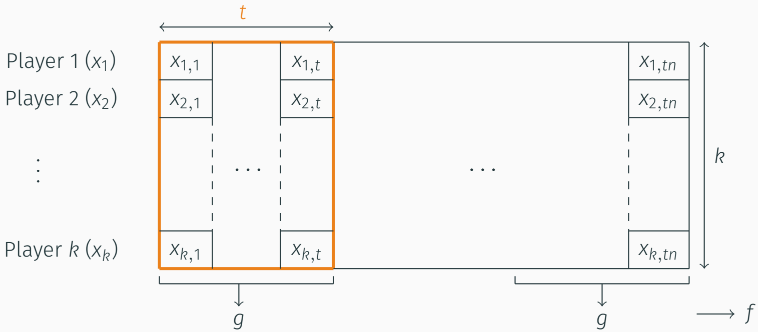
Motivations:

- ACC^0 = functions computable by polysize constant-depth circuits made of AND, OR, NOT and MOD_m gates
- $\mathsf{NEXP} \not\subseteq \mathsf{ACC}^0$ [Wil14]
- Conjecture: $\mathsf{NP} \not\subseteq \mathsf{ACC}^0$

$$F \text{ breaks the } \log n \text{ barrier} \xrightarrow{\text{[HG91]}} F \notin \mathsf{ACC}^0$$


n
Player 1 (x_1)
Player 2 (x_2)
$\vdots$
Player k (x_k)
$x_{1,1}$ $x_{1,2}$ $x_{1,3}$ $x_{1,n}$
$x_{2,1}$ $x_{2,2}$ $x_{2,3}$ $x_{2,n}$
$\cdots$
$x_{k,1}$ $x_{k,2}$ $x_{k,3}$ $x_{k,n}$
k

Composed functions



Given $f : \{0,1\}^{n/t} \to \{0,1\}$ and $g : \{0,1\}^{t \cdot k} \to \{0,1\}$:

$$f \circ g(x_1, \ldots, x_k)$$

Prior work

Symmetric function = invariant under any permutation of the input

Symmetric function = invariant under any permutation of the input

When $k = \mathrm{polylog}\, n$:

- $\mathrm{D}_k(\textsc{Sym} \circ \mathrm{AND}_1) = \mathcal{O}\left(\log^2 n\right)$ [Gro94]
- $\mathrm{D}_k^{||}(\textsc{Sym} \circ \textsc{Sym}_1) = \mathcal{O}\left(\log^3 n\right)$ [BGKL04]
- $\mathrm{D}_k^{||}(\textsc{Sym} \circ \textsc{Any}_1) = \mathcal{O}\left(\log^3 n\right)$ [ACFN15]
- $\mathrm{D}_k(\textsc{Sym} \circ \textsc{Any}_t) = \mathcal{O}\left(polylogn\right)$ for $t \leq \log\log n$ [CS14]

Prior work

Symmetric function = invariant under any permutation of the input

When $k = \text{polylog}\, n$:

- $D_k(\textsc{Sym} \circ \text{AND}_1) = \mathcal{O}\left(\log^2 n\right)$ [Gro94]
- $D_k^{||}(\textsc{Sym} \circ \textsc{Sym}_1) = \mathcal{O}\left(\log^3 n\right)$ [BGKL04]
- $D_k^{||}(\textsc{Sym} \circ \textsc{Any}_1) = \mathcal{O}\left(\log^3 n\right)$ [ACFN15]
- $D_k(\textsc{Sym} \circ \textsc{Any}_t) = \mathcal{O}\left(polylogn\right)$ for $t \leq \log\log n$ [CS14]

Our result:

- $D_k^{||}(\textsc{Sym} \circ \textsc{Sym}_t) = \mathcal{O}\left(polylogn\right)$ for constant t

Proof sketch

Symmetric f and g with $t = 2$:

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

g g $\cdots$ g $\longrightarrow f$

Proof sketch

Symmetric f and g with $t = 2$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

Proof sketch

Symmetric f and g with $t = 2$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

y_{i_1,i_2,i_3} = # columns with exactly i_1 occurrences of 1, i_2 of 2 and i_3 of 3

Proof sketch

Symmetric f and g with $t = 2$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

y_{i_1,i_2,i_3} = # columns with exactly i_1 occurrences of 1, i_2 of 2 and i_3 of 3

$\rightarrow y_{0,0,0} = 1$

Proof sketch

Symmetric f and g with $t = 2$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \ldots \quad g \longrightarrow f$

y_{i_1,i_2,i_3} = # columns with exactly i_1 occurrences of 1, i_2 of 2 and i_3 of 3

$\rightarrow y_{0,0,0} = 1, y_{1,0,0} = 2$

Proof sketch

Symmetric f and g with $t = 2$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \dots \quad g \longrightarrow f$

y_{i_1,i_2,i_3} = # columns with exactly i_1 occurrences of 1, i_2 of 2 and i_3 of 3

$\rightarrow y_{0,0,0} = 1, y_{1,0,0} = 2, y_{0,4,1} = 0, \dots$

Proof sketch

Symmetric f and g with $t = 2$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \dots \quad g \longrightarrow f$

y_{i_1,i_2,i_3} = # columns with exactly i_1 occurrences of 1, i_2 of 2 and i_3 of 3

$\rightarrow y_{0,0,0} = 1, y_{1,0,0} = 2, y_{0,4,1} = 0, \dots$

$\boxed{\text{Recovering the } y_{i_1,i_2,i_3}\text{'s is enough since } f \text{ and } g \text{ are symmetric}}$

Proof sketch

~~0~~	~~0~~	~~1~~	~~2~~	~~0~~	~~2~~	~~3~~	~~2~~	~~1~~	~~1~~
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

- Player 1 sends to the referee:

  $a^1_{i_1,i_2,i_3}$ = # columns he sees with i_1 occurrences of 1, i_2 of 2 and i_3 of 3

  $\rightarrow a^1_{0,0,0} = 2, a^1_{1,0,0} = 1, a^1_{2,1,1} = 1, \ldots$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

- Player 1 sends to the referee:

  $a^1_{i_1,i_2,i_3}$ = # columns he sees with i_1 occurrences of 1, i_2 of 2 and i_3 of 3

  $\rightarrow a^1_{0,0,0} = 2, a^1_{1,0,0} = 1, a^1_{2,1,1} = 1, \ldots$
- Players 2 to 5 do the same

Proof sketch

The referee computes:

$$b_{i_1,i_2,i_3} = a^1_{i_1,i_2,i_3} + \cdots + a^5_{i_1,i_2,i_3}$$

Proof sketch

The referee computes:

$$b_{i_1,i_2,i_3} = a^1_{i_1,i_2,i_3} + \cdots + a^5_{i_1,i_2,i_3}$$

It verifies:

$$\begin{cases} y_{i_1,i_2,i_3} \geq 0 \\ \\ \\ \\ \end{cases}$$

Proof sketch

The referee computes:

$$b_{i_1,i_2,i_3} = a^1_{i_1,i_2,i_3} + \cdots + a^5_{i_1,i_2,i_3}$$

It verifies:

$$\begin{cases} y_{i_1,i_2,i_3} \geq 0 \\ \sum y_{i_1,i_2,i_3} = n \\ \\ \\ \end{cases}$$

Proof sketch

The referee computes:

$$b_{i_1,i_2,i_3} = a^1_{i_1,i_2,i_3} + \cdots + a^5_{i_1,i_2,i_3}$$

It verifies:

$$\begin{cases} y_{i_1,i_2,i_3} \geq 0 \\ \sum y_{i_1,i_2,i_3} = n \\ (k - (i_1 + i_2 + i_3))y_{i_1,i_2,i_3} + (i_1 + 1)y_{i_1+1,i_2,i_3} \\ \qquad + (i_2 + 1)y_{i_1,i_2+1,i_3} + (i_3 + 1)y_{i_1,i_2,i_3+1} = b_{i_1,i_2,i_3} \end{cases}$$

Proof sketch

The referee computes:

$$b_{i_1,i_2,i_3} = a^1_{i_1,i_2,i_3} + \cdots + a^5_{i_1,i_2,i_3}$$

It verifies:

$$\begin{cases} y_{i_1,i_2,i_3} \geq 0 \\ \sum y_{i_1,i_2,i_3} = n \\ (k - (i_1 + i_2 + i_3)) y_{i_1,i_2,i_3} + (i_1 + 1) y_{i_1+1,i_2,i_3} \\ \qquad + (i_2 + 1) y_{i_1,i_2+1,i_3} + (i_3 + 1) y_{i_1,i_2,i_3+1} = b_{i_1,i_2,i_3} \end{cases}$$

Theorem

If $k \geq 5^{2^t} \log n$ then it admits exactly one integral solution.

$\rightarrow$ the referee recovers the y_{i_1,i_2,i_3}'s and computes the output

Decision tree complexity and log-rank conjecture

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

Proposition ([MS82])

Let $M_F \in \{0,1\}^{n \times n}$ be the communication matrix: $M_F(x,y) = F(x,y)$.

$$\log \operatorname{rank} M_F \leq D_2(F)$$

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

Proposition ([MS82])

Let $M_F \in \{0,1\}^{n \times n}$ be the communication matrix: $M_F(x,y) = F(x,y)$.

$$\log \operatorname{rank} M_F \leq D_2(F)$$

Conjecture

For some absolute constant c:

$$\log \operatorname{rank} M_F \leq D_2(F) \leq \log^c \operatorname{rank} M_F$$

XOR and AND functions

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an XOR function if:

$$F(x, y) = f(x \oplus y)$$

  for some $f : \{0,1\}^n \to \{0,1\}$

XOR and AND functions

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an XOR function if:

$$F(x,y) = f(x \oplus y)$$

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an AND function if:

$$F(x,y) = f(x \wedge y)$$

XOR and AND functions

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an XOR function if:

$$F(x,y) = f(x \oplus y)$$

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an AND function if:

$$F(x,y) = f(x \wedge y)$$

Examples: $\textsc{Equality}(x,y) = \mathrm{NOR}(x \oplus y)$, $\textsc{Hamming}_d(x,y) = \mathrm{GAP}_d(x \oplus y)$, $\textsc{Disjointness}(x,y) = \mathrm{NOR}(x \wedge y)$, $\textsc{InnerProduct}(x,y) = \mathrm{MOD}_2(x \wedge y)$, etc.

XOR and AND functions

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an XOR function if:

$$F(x,y) = f(x \oplus y)$$

- A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an AND function if:

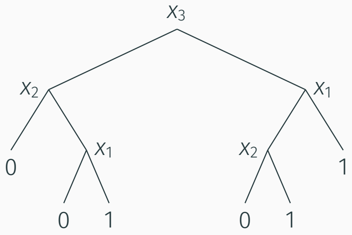
$$F(x,y) = f(x \wedge y)$$

Examples: $\textsc{Equality}(x,y) = \mathrm{NOR}(x \oplus y)$, $\textsc{Hamming}_d(x,y) = \mathrm{GAP}_d(x \oplus y)$, $\textsc{Disjointness}(x,y) = \mathrm{NOR}(x \wedge y)$, $\textsc{InnerProduct}(x,y) = \mathrm{MOD}_2(x \wedge y)$, etc.

Interests:

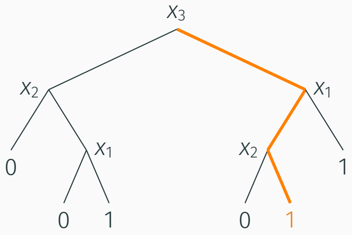
- For XOR functions: $\operatorname{rank} M_F = \operatorname{mon} f$ [BC99]
- For AND functions: $\operatorname{rank} M_F = \operatorname{mon}^\star f$ [BdW01]
- Connections with Decision Tree complexity

A decision tree is an ordered tree where each internal node is labeled with a query, and each leaf is labeled with 0 or 1.



Decision tree complexity

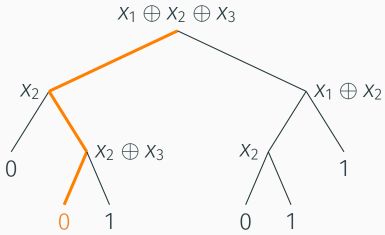
A decision tree is an ordered tree where each internal node is labeled with a query, and each leaf is labeled with 0 or 1.



Input: $x_1x_2x_3 = 011$ on a regular decision tree

$$\mathrm{DT}(f), \mathrm{RDT}(f) \text{ and } \mathrm{QDT}(f)$$

A decision tree is an ordered tree where each internal node is labeled with a query, and each leaf is labeled with 0 or 1.

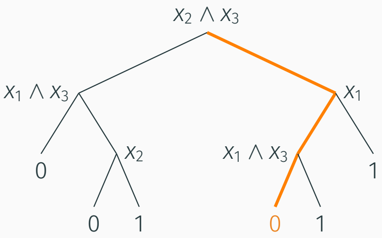


Input: $x_1x_2x_3 = 011$ on a parity decision tree

$$\mathrm{DT}^{\oplus}(f), \mathrm{RDT}^{\oplus}(f) \text{ and } \mathrm{QDT}^{\oplus}(f)$$

Decision tree complexity

A decision tree is an ordered tree where each internal node is labeled with a query, and each leaf is labeled with 0 or 1.



Input: $x_1x_2x_3 = 011$ on a conjunctive decision tree

$$\mathrm{DT}^{\wedge}(f), \mathrm{RDT}^{\wedge}(f) \text{ and } \mathrm{QDT}^{\wedge}(f)$$

Connections

Proposition ([ZS10])

For any XOR function $F(x, y) = f(x \oplus y)$:

$$D_2(F) \leq 2 \cdot DT^{\oplus}(f)$$

For any AND function $F(x, y) = f(x \wedge y)$:

$$D_2(F) \leq 2 \cdot DT^{\wedge}(f)$$

Connections

Proposition ([ZS10])

For any XOR function $F(x, y) = f(x \oplus y)$*:*

$$D_2(F) \leq 2 \cdot DT^{\oplus}(f)$$

For any AND function $F(x, y) = f(x \wedge y)$*:*

$$D_2(F) \leq 2 \cdot DT^{\wedge}(f)$$

Conjecture

- *Communication and Decision Tree complexities are polynomially related*

Proposition ([ZS10])

For any XOR function $F(x, y) = f(x \oplus y)$*:*

$$D_2(F) \leq 2 \cdot DT^{\oplus}(f)$$

For any AND function $F(x, y) = f(x \wedge y)$*:*

$$D_2(F) \leq 2 \cdot DT^{\wedge}(f)$$

Conjecture

- *Communication and Decision Tree complexities are polynomially related*
- *Log-rank conjecture for decision trees:*
  - *XOR function:* $\log \mathrm{mon}(f) \leq D_2(F) \leq 2 \cdot DT^{\oplus}(f) \leq \log^c \mathrm{mon}(f)$
  - *AND function:* $\log \mathrm{mon}^{\star}(f) \leq D_2(F) \leq 2 \cdot DT^{\wedge}(f) \leq \log^c \mathrm{mon}^{\star}(f)$

Communication complexity[1] of (nontrivial) XOR and AND functions, for symmetric f:

	XOR functions	AND functions
Deterministic	$\Theta(n)$	$\Theta\left((n-t(f))\left(1+\log\frac{n}{n-t(f)}\right)\right)$
Randomized	$\Theta(r(f))$	$\Theta^{\dagger}\left((n-t(f))\left(1+\log\frac{n}{n-t(f)}\right)\right)$
Quantum	$\Theta(r(f))$	$\Theta^{\star}\left(\sqrt{n\cdot\ell_0(f)}+\ell_1(f)\right)$

[1] [ZS09, BdW01, Raz03]

Symmetric functions

Decision tree complexities[2] of (nontrivial) symmetric functions:

	Regular	Parity	Conjunctive
Deterministic	$\Theta(n)$	$\Theta(n)$	$\Theta\left((n-t(f))\left(1+\log\frac{n}{n-t(f)}\right)\right)$
Randomized	$\Theta(n)$	$\Theta(r(f))$	$\Theta^{\dagger}\left((n-t(f))\left(1+\log\frac{n}{n-t(f)}\right)\right)$
Quantum	$\Theta\left(\sqrt{n\cdot\ell(f)}\right)$	$\Theta(r(f))$	$\Theta^{\star}\left(\sqrt{n\cdot\ell_0(f)}+\ell_1(f)\right)$

[2] [ZS09, BdW01, Raz03, BBC$^+$01]

Decision tree complexities[2] of (nontrivial) symmetric functions:

	Regular	Parity	Conjunctive
Deterministic	$\Theta(n)$	$\Theta(n)$	$\Theta\left((n-t(f))\left(1+\log\frac{n}{n-t(f)}\right)\right)$
Randomized	$\Theta(n)$	$\Theta(r(f))$	$\Theta^{\dagger}\left((n-t(f))\left(1+\log\frac{n}{n-t(f)}\right)\right)$
Quantum	$\Theta\left(\sqrt{n\cdot\ell(f)}\right)$	$\Theta(r(f))$	$\Theta^{\star}\left(\sqrt{n\cdot\ell_0(f)}+\ell_1(f)\right)$

Result: Communication and Decision Tree complexities are polynomially related for symmetric functions.

[2] [ZS09, BdW01, Raz03, BBC$^+$01]

Conclusion

Our contributions:

- first efficient simultaneous protocol for $\textsc{Sym} \circ \textsc{Sym}_t$
- full characterization of the decision tree complexities of symmetric functions
- efficient construction for Ramsey numbers over $\mathbb{F}_p^n$

Our contributions:

- first efficient simultaneous protocol for $\textsc{Sym} \circ \textsc{Sym}_t$
- full characterization of the decision tree complexities of symmetric functions
- efficient construction for Ramsey numbers over $\mathbb{F}_p^n$

Future work:

- other protocols for larger families of composed functions
- breaking the log n barrier
- log-rank conjecture for XOR and AND functions (using decision tree complexity?)

References I

Anil Ada, Arkadev Chattopadhyay, Omar Fawzi, and Phuong Nguyen.
The NOF multiparty communication complexity of composed functions.
Computational Complexity, 24(3):645–694, 2015.

Noga Alon, Yossi Matias, and Mario Szegedy.
The space complexity of approximating the frequency moments.
In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 20–29, New York, NY, USA, 1996. ACM.

Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf.
Quantum lower bounds by polynomials.
J. ACM, 48(4):778–797, July 2001.

Eric Blais, Joshua Brody, and Kevin Matulef.
Property testing lower bounds via communication complexity.
computational complexity, 21(2):311–358, 2012.

Anna Bernasconi and Bruno Codenotti.
Spectral analysis of boolean functions as a graph eigenvalue problem.
IEEE Transactions on Computers, 48(3):345–351, 1999.

Harry Buhrman and Ronald de Wolf.
Communication complexity lower bounds by polynomials.
In *Proceedings of the 16th Annual Conference on Computational Complexity*, CCC '01, pages 120–, Washington, DC, USA, 2001. IEEE Computer Society.

László Babai, Anna Gál, Peter G. Kimmel, and Satyanarayana V. Lokam.
Communication complexity of simultaneous messages.
SIAM J. Comput., 33(1):137–166, January 2004.

László Babai, Peter G. Kimmel, and Satyanarayana V. Lokam.
Simultaneous messages vs. communication, pages 361–372.
Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

Paul Beame, Toniann Pitassi, and Nathan Segerlind.
Lower bounds for Lovász–Schrijver systems and beyond follow from multiparty communication complexity.
SIAM J. Comput., 37(3):845–869, 2007.

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

Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton.
Multi-party protocols.
In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC '83, pages 94–99, New York, NY, USA, 1983. ACM.

Vincent Conitzer and Tuomas Sandholm.
Communication complexity as a lower bound for learning in games.
In *Proceedings of the Twenty-first International Conference on Machine Learning*, ICML '04, pages 24–, New York, NY, USA, 2004. ACM.

References IV

Arkadev Chattopadhyay and Michael E. Saks.
The power of super-logarithmic number of players.
In Klaus Jansen, José D. P. Rolim, Nikhil R. Devanur, and Cristopher Moore, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2014)*, volume 28 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 596–603, Dagstuhl, Germany, 2014. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

Fan R. K. Chung and Prasad Tetali.
Communication complexity and quasi randomness.
SIAMJDiscreteMath, 6(1):110–123, 1993.

Ben Green.
Finite field models in additive combinatorics.
In Bridget S. Webb, editor, *Surveys in Combinatorics 2005*, pages 1–28. Cambridge University Press, 2005.
Cambridge Books Online.

Vince Grolmusz.
The BNS lower bound for multi-party protocols is nearly optimal.
Information and Computation, 112:51–54, 1994.

Johan Håstad and Mikael Goldmann.
On the power of small-depth threshold circuits.
Computational Complexity, 1(2):113–129, 1991.

Michael T. Lacey and William McClain.
On an argument of Shkredov on two-dimensional corners.
Online Journal of Analytic Combinatorics, 2007.

Peter Bro Miltersen, Noam Nisan, Shmuel Safra, and Avi Wigderson.
On data structures and asymmetric communication complexity.
In *Proceedings of the Twenty-seventh Annual ACM Symposium on Theory of Computing*, STOC ’95, pages 103–111, New York, NY, USA, 1995. ACM.

Kurt Mehlhorn and Erik M. Schmidt.
Las Vegas is better than determinism in VLSI and distributed computing.
In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, pages 330–337, New York, NY, USA, 1982. ACM.

Noam Nisan and Ilya Segal.
The communication requirements of efficient allocations and supporting prices.
Journal of Economic Theory, 129:192–224, 2006.

A A Razborov.
Quantum communication complexity of symmetric predicates.
Izvestiya: Mathematics, 67(1):145, 2003.

Ryan Williams.
Nonuniform acc circuit lower bounds.
J. ACM, 61(1):2:1–2:32, January 2014.

Andrew Chi-Chih Yao.
On ACC and threshold circuits.
In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume II*, pages 619–627, 1990.

Zhiqiang Zhang and Yaoyun Shi.
Communication complexities of symmetric XOR functions.
Quantum Info. Comput., 9(3):255–263, March 2009.

Zhiqiang Zhang and Yaoyun Shi.
On the parity complexity measures of boolean functions.
Theor. Comput. Sci., 411(26-28):2612–2618, June 2010.

$\textsc{Equality}$ function

$$\textsc{Equality}(x_1, \ldots, x_k) = 1 \Leftrightarrow x_1 = \cdots = x_k$$

$\mathrm{D}_2(\textsc{Equality}) = \Omega(n)$

- log-rank method

$\mathrm{R}_2^{||}(\textsc{Equality}) = \mathcal{O}(1)$

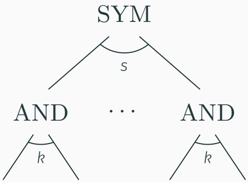
- Alice and Bob test $x \cdot r = y \cdot r \mod 2$ for two random $r \in \{0,1\}^n$

$\mathrm{D}_k^{||}(\textsc{Equality}) = \mathcal{O}(1)$ when $k > 2$

- Player 1 checks $x_2 = \cdots = x_k$
- Player 2 checks $x_1 = x_3 = \cdots = x_k$

ACC^0 and Sym$^+$

Sym$^+(s, k)$ = depth-2 circuits whose top gate is a symmetric gate of fan-in s, and each bottom gate is an AND gate of fan-in k



- $\mathrm{ACC}^0 \subset \mathrm{SYM}^+(2^{\mathrm{polylog}\, n}, \mathrm{polylog}\, n)$ [Yao90, BT94]
- f is computed by a $\mathrm{SYM}^+(s, k-1)$ circuit $\Rightarrow$ for any partition of the input between k players, there is a protocol of cost $\mathcal{O}(k \log s)$ computing f

$F(x, y) = f(x \oplus y)$ is symmetric iff f is symmetric

Symmetric XOR and AND functions

$F(x, y) = f(x \oplus y)$ is symmetric iff f is symmetric

$\rightarrow f(x)$ depends only on $|x|$. Hence $f : \{0, \ldots, n\} \rightarrow \{0, 1\}$

Symmetric XOR and AND functions

$F(x, y) = f(x \oplus y)$ is symmetric iff f is symmetric

$\rightarrow f(x)$ depends only on $|x|$. Hence $f : \{0, \ldots, n\} \rightarrow \{0, 1\}$

- $t(f) = \min\{p : f(p-1) \neq f(p)\}$
- $\ell_0(f) = \min\{p \leq n/2 : f(i) = f(n/2) \text{ for } i \in [p, n/2]\}$
- $\ell_1(f) = \min\{p \leq n/2 : f(i) = f(n/2) \text{ for } i \in [n/2, n-p]\}$
- $\ell(f) = \min\{p : f(i) = f(i+1) \text{ for } i \in [p, n-p-1]\}$
- $r(f) = \min\{p : f(i) = f(i+2) \text{ for } i \in [p, n-p-2]\}$

Ramsey numbers and $\textsc{Eval}_G$

$\textsc{Eval}_G$

For any Abelian group G and $x_1, \ldots, x_k \in G$:

$$\textsc{Eval}_G(x_1, \ldots, x_k) = 1 \Leftrightarrow x_1 + \cdots + x_k = 0$$

For any Abelian group G and $x_1, \ldots, x_k \in G$:

$$\textsc{Eval}_G(x_1, \ldots, x_k) = 1 \Leftrightarrow x_1 + \cdots + x_k = 0$$

Communication complexity:

- $\mathrm{R}_k^{||}(\textsc{Eval}_G) = \mathcal{O}(1)$ since

$$x_1 + \cdots + x_k = 0 \Leftrightarrow x_1 = -(x_2 \cdots + x_k)$$

- $\mathrm{D}_k(\textsc{Eval}_G) \rightarrow$ connections to Ramsey theory

k-dimensional corner in G^k:

$$(x_1, x_2, \ldots, x_k), (x_1 + \lambda, x_2, \ldots, x_k), (x_1, x_2 + \lambda, \ldots, x_k), \ldots, (x_1, x_2, \ldots, x_k + \lambda)$$

k-dimensional corner in G^k:

$$(x_1, x_2, \ldots, x_k), (x_1 + \lambda, x_2, \ldots, x_k), (x_1, x_2 + \lambda, \ldots, x_k), \ldots, (x_1, x_2, \ldots, x_k + \lambda)$$

Ramsey numbers:

- $c_k^{\angle}(G)$ = min # of colors to avoid monochromatic k-dim corner in G^k
- $r_k^{\angle}(G)$ = size of largest subset of G^k without any k-dim corner

k-dimensional corner in G^k:

$$(x_1, x_2, \ldots, x_k), (x_1 + \lambda, x_2, \ldots, x_k), (x_1, x_2 + \lambda, \ldots, x_k), \ldots, (x_1, x_2, \ldots, x_k + \lambda)$$

Ramsey numbers:

- $c_k^{\angle}(G)$ = min # of colors to avoid monochromatic k-dim corner in G^k
- $r_k^{\angle}(G)$ = size of largest subset of G^k without any k-dim corner

Chandra, Furst and Lipton [CFL83]:

$$\log(c_k^{\angle}(G)) \leq \mathrm{D}_{k+1}(\textsc{Eval}_G) \leq k + \log(c_k^{\angle}(G))$$

Chandra, Furst and Lipton [CFL83]:

$$\log(c_k^{\angle}(G)) \leq \mathrm{D}_{k+1}(\textsc{Eval}_G) \leq k + \log(c_k^{\angle}(G))$$

Ramsey numbers and $\textsc{Eval}_{\mathbb{F}_p^n}$

Motivations for $G = \mathbb{F}_p^n$:

- the proofs are easier and cleaner
- they can be adapted to any other group [Gre05]
- $\textsc{Eval}_{\mathbb{F}_p^n} \in \textsc{Sym} \circ \textsc{Sym}_p$

Motivations for $G = \mathbb{F}_p^n$:

- the proofs are easier and cleaner
- they can be adapted to any other group [Gre05]
- $\textsc{Eval}_{\mathbb{F}_p^n} \in \textsc{Sym} \circ \textsc{Sym}_p$

Prior work:

- $\mathrm{D}_3(\textsc{Eval}_{\mathbb{F}_p^n}) = \omega(1)$ [LM07]
- $c_k^{\angle}(\mathbb{F}_2^n) \leq \mathcal{O}\left(2^{n/2^{k-2}} n^{k+1}\right)$ [ACFN15]
- an explicit large corner free set over $\mathbb{F}_2^n$ [ACFN15]
- $c_k^{\angle}(\mathbb{F}_p^n) \leq 2^{\mathcal{O}\left(p \log^2 n\right)} p^{\mathcal{O}(p \log n)}$ when $k > 1 + p \log(3n)$ [CS14]

Ramsey numbers and $\text{EVAL}_{\mathbb{F}_p^n}$

Motivations for $G = \mathbb{F}_p^n$:

- the proofs are easier and cleaner
- they can be adapted to any other group [Gre05]
- $\text{EVAL}_{\mathbb{F}_p^n} \in \text{SYM} \circ \text{SYM}_p$

Prior work:

- $D_3(\text{EVAL}_{\mathbb{F}_p^n}) = \omega(1)$ [LM07]
- $c_k^{\angle}(\mathbb{F}_2^n) \leq \mathcal{O}\left(2^{n/2^{k-2}} n^{k+1}\right)$ [ACFN15]
- an explicit large corner free set over $\mathbb{F}_2^n$ [ACFN15]
- $c_k^{\angle}(\mathbb{F}_p^n) \leq 2^{\mathcal{O}\left(p \log^2 n\right)} p^{\mathcal{O}(p \log n)}$ when $k > 1 + p \log(3n)$ [CS14]

Our result:

- the first explicit large corner-free set over $\mathbb{F}_p^n$, of size $\frac{p^{nk}}{C^{k^2} p^{k+k^2}}$

Our contribution: the first explicit large corner-free set in $\mathbb{F}_p^n$

Results

Our contribution: the first explicit large corner-free set in $\mathbb{F}_p^n$

Definitions:

- $M \in (\mathbb{F}_p^n)^k$ is seen as a $k \times n$ matrix over $\mathbb{F}_p$
- $d(c, c_j) =$ Hamming distance between columns c and c_j
- $n_{i,c}(M) =$ number of columns at distance i to c in M

Results

Our contribution: the first explicit large corner-free set in $\mathbb{F}_p^n$

Definitions:

- $M \in (\mathbb{F}_p^n)^k$ is seen as a $k \times n$ matrix over $\mathbb{F}_p$
- $d(c, c_j) =$ Hamming distance between columns c and c_j
- $n_{i,c}(M) =$ number of columns at distance i to c in M

For any $c \in \mathbb{F}_p^k$, $N_k = 0$ and $N_0, \ldots, N_{k-1} \geq 0$ such that $\sum_{i=0}^{k} N_i = n$:

$$S_c^k = \{M \in (\mathbb{F}_p^n)^k : \forall i \in \{0, \ldots, k\}, n_{i,c}(M) = N_i\}$$

is a corner-free set.

Results

Our contribution: the first explicit large corner-free set in $\mathbb{F}_p^n$

Definitions:

- $M \in (\mathbb{F}_p^n)^k$ is seen as a $k \times n$ matrix over $\mathbb{F}_p$
- $d(c, c_j) =$ Hamming distance between columns c and c_j
- $n_{i,c}(M) =$ number of columns at distance i to c in M

For any $c \in \mathbb{F}_p^k$, $N_k = 0$ and $N_0, \dots, N_{k-1} \geq 0$ such that $\sum_{i=0}^k N_i = n$:

$$S_c^k = \{M \in (\mathbb{F}_p^n)^k : \forall i \in \{0, \dots, k\}, n_{i,c}(M) = N_i\}$$

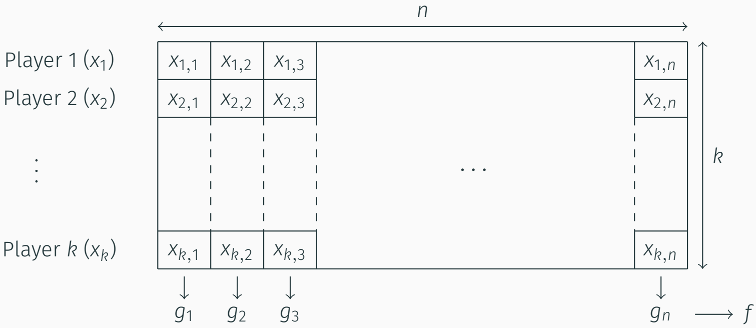
is a corner-free set.

If $k \geq \left\lceil \frac{\log n}{\log\left(1+\frac{1}{p-1}\right)} \right\rceil$ and $N_i = \left\lfloor \binom{k}{i} \frac{(p-1)^i}{p^k} n \right\rfloor$ then $|S_c^k| \geq \frac{p^{nk}}{C^{k^2} p^{k+k^2}}$

The $\log n$ barrier and composed functions

Given $f : \{0,1\}^n \to \{0,1\}$ and $\overrightarrow{g} = (g_1, \ldots, g_n)$ where $g_i : \{0,1\}^k \to \{0,1\}$:

$$f \circ \overrightarrow{g}(x_1, \ldots, x_k) = f(\ldots, g_i(x_{1,i}, \ldots, x_{k,i}), \ldots)$$



Composed functions

Definitions:

- $f \circ g$ if $g_1 = \cdots = g_n$
- Symmetric = invariant under any permutation of the input
- $\textsc{Any} \circ \overrightarrow{\textsc{Any}}$, $\textsc{Any} \circ \textsc{Any}$, $\textsc{Sym} \circ \overrightarrow{\textsc{Any}}$, $\textsc{Sym} \circ \textsc{Sym}$...

Composed functions

Definitions:

- $f \circ g$ if $g_1 = \cdots = g_n$
- Symmetric = invariant under any permutation of the input
- $\textsc{Any} \circ \overrightarrow{\textsc{Any}}$, $\textsc{Any} \circ \textsc{Any}$, $\textsc{Sym} \circ \overrightarrow{\textsc{Any}}$, $\textsc{Sym} \circ \textsc{Sym}$...

Motivations:

- very simple structure
- most of the important functions: $\mathrm{GIP} = \mathrm{MOD}_2 \circ \mathrm{AND} \in \textsc{Sym} \circ \textsc{Sym}$, $\mathrm{MAJ} \circ \mathrm{MAJ} \in \textsc{Sym} \circ \textsc{Sym}$, $\mathrm{DISJ} = \mathrm{NOR} \circ \mathrm{AND} \in \textsc{Sym} \circ \textsc{Sym}$
- major open problems still unknown for composed functions

Prior work

Conjecture ([BKL95]): $\mathrm{MAJ} \circ \mathrm{MAJ}$ breaks the $\log n$ barrier

Prior work

Conjecture ([BKL95]): $\mathrm{MAJ} \circ \mathrm{MAJ}$ breaks the $\log n$ barrier

When $k = \Omega(\log n)$:

- $\mathrm{D}_k(f \circ g) = \mathcal{O}\left(\log^2 n\right)$ for $f \circ g \in \textsc{Sym} \circ \mathrm{AND}$ [Gro94]
- $\mathrm{D}_k^{||}(f \circ g) = \mathcal{O}\left(\log^3 n\right)$ for $f \circ g \in \textsc{Sym} \circ \textsc{Comp}$ [BGKL04]
- $\mathrm{D}_k^{||}(f \circ \overrightarrow{g}) = \mathcal{O}\left(\log^3 n\right)$ for $f \circ \overrightarrow{g} \in \textsc{Sym} \circ \overrightarrow{\textsc{Any}}$ [ACFN15]

Prior work

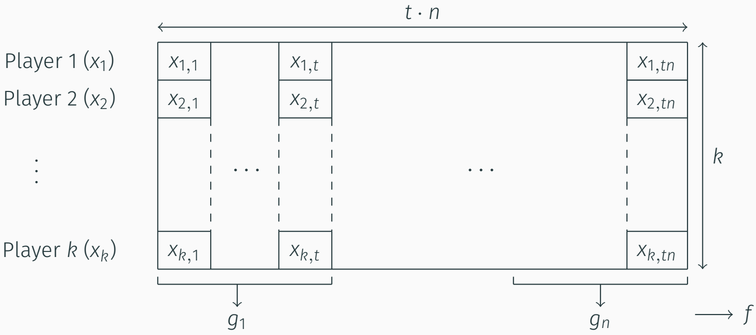
Conjecture ([BKL95]): $\mathrm{MAJ} \circ \mathrm{MAJ}$ breaks the $\log n$ barrier

When $k = \Omega(\log n)$:

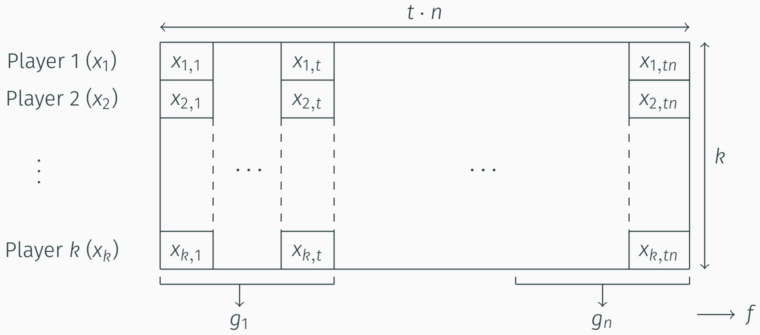
- $\mathsf{D}_k(f \circ g) = \mathcal{O}\left(\log^2 n\right)$ for $f \circ g \in \textsc{Sym} \circ \mathrm{AND}$ [Gro94]
- $\mathsf{D}_k^{||}(f \circ g) = \mathcal{O}\left(\log^3 n\right)$ for $f \circ g \in \textsc{Sym} \circ \textsc{Comp}$ [BGKL04]
- $\mathsf{D}_k^{||}(f \circ \vec{g}) = \mathcal{O}\left(\log^3 n\right)$ for $f \circ \vec{g} \in \textsc{Sym} \circ \overrightarrow{\textsc{Any}}$ [ACFN15]

$\rightarrow$ none of the functions in $\textsc{Sym} \circ \overrightarrow{\textsc{Any}}$ can break the $\log n$ barrier

Composed functions of block-width t

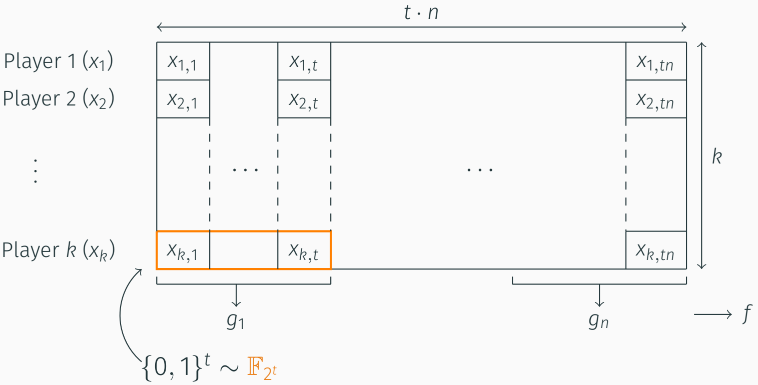


Composed functions of block-width t

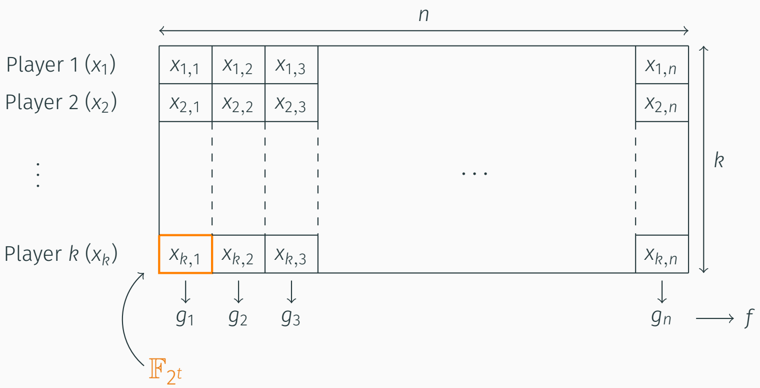


- $\mathrm{MAJ}_t : \{0,1\}^{k \cdot t} \to \{0,1\}$
- Conjecture : $\mathrm{MAJ} \circ \mathrm{MAJ}_{\sqrt{n}}$ breaks the barrier

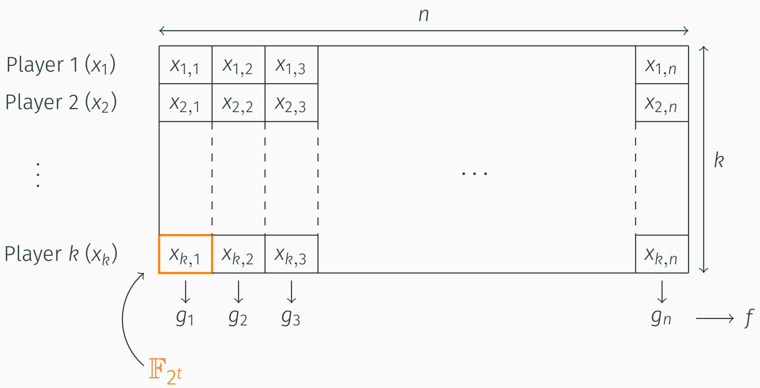
Composed functions of block-width t



Composed functions of block-width t



Composed functions of block-width t



Given $f : \{0,1\}^n \to \{0,1\}$ and $\overrightarrow{g} = (g_1, \ldots, g_n)$ where $g_i : \mathbb{F}_p^k \to \{0,1\}$:

$$f \circ \overrightarrow{g}(x_1, \ldots, x_k) = f(\ldots, g_i(x_{1,i}, \ldots, x_{k,i}), \ldots)$$

$\rightarrow$ $\textsc{Any} \circ \overrightarrow{\textsc{Any}_p}, \textsc{Any} \circ \textsc{Any}_p, \textsc{Sym} \circ \textsc{Any}_p, \ldots$

Prior work

Conjecture: $\mathrm{MAJ} \circ \mathrm{MAJ}_{\sqrt{\log n}}$ breaks the $\log n$ barrier

Prior work

Conjecture: $\mathrm{MAJ} \circ \mathrm{MAJ}_{\sqrt{\log n}}$ breaks the $\log n$ barrier

When $k = \Omega(\operatorname{polylog} n)$:

- $\mathrm{D}_k^{||}(f \circ \vec{g}) = \mathcal{O}\left(\log^3 n\right)$ for $f \circ \vec{g} \in \textsc{Sym} \circ \overrightarrow{\textsc{Any}_2}$ [ACFN15]
- $\mathrm{D}_k(f \circ g) = \mathcal{O}\left(polylogn\right)$ for $f \circ g \in \textsc{Sym} \circ \overrightarrow{\textsc{Any}_p}$ and $p \leq \operatorname{polylog} n$ [CS14]

Prior work

Conjecture: $\mathrm{MAJ} \circ \mathrm{MAJ}_{\sqrt{\log n}}$ breaks the $\log n$ barrier

When $k = \Omega(\operatorname{polylog} n)$:

- $D_k^{||}(f \circ \vec{g}) = \mathcal{O}\left(\log^3 n\right)$ for $f \circ \vec{g} \in \textsc{Sym} \circ \overrightarrow{\textsc{Any}_2}$ [ACFN15]
- $D_k(f \circ g) = \mathcal{O}\,(polylogn)$ for $f \circ g \in \textsc{Sym} \circ \overrightarrow{\textsc{Any}_p}$ and $p \leq \operatorname{polylog} n$ [CS14]

New results for constant p:

- $D_k^{||}(f \circ g) = \mathcal{O}\,(polylogn)$ for $f \circ g \in \textsc{Sym} \circ \textsc{Sym}_p$ $(k = \operatorname{polylog} n)$
- $D_k^{||}(f \circ g) = \mathcal{O}\,(polylogn)$ for $f \circ g \in \textsc{Sym} \circ \textsc{Comp}_p$ $(k \geq \operatorname{polylog} n)$
- $\mathrm{MAJ} \circ \mathrm{MAJ}_t$ cannot break the barrier for constant t

Proof sketch

Symmetric f and g over $\mathbb{F}_3$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

$y_{i,j}$ = # columns with i one's and j two's

Proof sketch

Symmetric f and g over $\mathbb{F}_3$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

$y_{i,j}$ = # columns with i one's and j two's

$\rightarrow y_{0,0} = 1$

Proof sketch

Symmetric f and g over $\mathbb{F}_3$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

$y_{i,j} =$ # columns with i one's and j two's

$\rightarrow y_{0,0} = 1, y_{1,0} = 2$

Proof sketch

Symmetric f and g over $\mathbb{F}_3$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$\downarrow$ $\downarrow$ $\ldots$ $\downarrow$

g g $g \longrightarrow f$

$y_{i,j}$ = # columns with i one's and j two's

$\to y_{0,0} = 1, y_{1,0} = 2, y_{1,1} = 1$

Proof sketch

Symmetric f and g over $\mathbb{F}_3$:

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

$g \quad g \quad \cdots \quad g \longrightarrow f$

$y_{i,j}$ = # columns with i one's and j two's
$\rightarrow y_{0,0} = 1, y_{1,0} = 2, y_{1,1} = 1, \ldots$

$\boxed{\text{Recovering the } y_{i,j}\text{'s is enough since } f \text{ and } g \text{ are symmetric}}$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

- Player 1 sends to the referee:

$$a^1_{i,j} = \#\text{ columns she sees with } i \text{ one's and } j \text{ two's}$$

$\rightarrow a^1_{0,0} = 2, a^1_{1,0} = 1, a^1_{1,1} = 3, \ldots$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

- Player 1 sends to the referee:

$$a^1_{i,j} = \#\text{ columns she sees with } i \text{ one's and } j \text{ two's}$$

  $\rightarrow a^1_{0,0} = 2, a^1_{1,0} = 1, a^1_{1,1} = 3, \ldots$
- Players 2 to 5 do the same

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a_{i,j}^1 + \cdots + a_{i,j}^5$$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} =$

Proof sketch

0	0	1	2	0	2	2	2	1	1
1	0	0	1	0	1	1	0	2	0
0	0	1	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
2	0	0	1	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0}$

Proof sketch

0	0	1	2	0	2	2	2	1	1
1	0	0	1	0	1	1	0	2	0
0	0	1	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
2	0	0	1	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0} + y_{1,0}$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0} + y_{1,0} + y_{0,1}$

Proof sketch

0	0	1	2	0	2	2	2	1	1
1	0	0	1	0	1	1	0	2	0
0	0	1	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
2	0	0	1	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0} + y_{1,0} + y_{0,1}$
- $b_{1,0} = 4y_{1,0}$

Proof sketch

0	0	1	2	0	2	2	2	1	1
1	0	0	1	0	1	1	0	2	0
0	0	1	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
2	0	0	1	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0} + y_{1,0} + y_{0,1}$
- $b_{1,0} = 4y_{1,0} + y_{1,1}$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0} + y_{1,0} + y_{0,1}$
- $b_{1,0} = 4y_{1,0} + y_{1,1} + 2y_{2,0}$

Proof sketch

0	0	1	2	0	2	3	2	1	1
1	0	3	1	0	1	1	0	2	0
0	0	3	2	0	0	1	2	1	0
0	0	2	1	0	1	2	1	2	0
3	0	0	3	1	0	1	0	2	0

The referee computes:

$$b_{i,j} = a^1_{i,j} + \cdots + a^5_{i,j}$$

Note that:

- $b_{0,0} = 5y_{0,0} + y_{1,0} + y_{0,1}$
- $b_{1,0} = 4y_{1,0} + y_{1,1} + 2y_{2,0}$
- $\ldots$

$$b_{i,j} = (k - (i + j))y_{i,j} + (i + 1)y_{i+1,j} + (j + 1)y_{i,j+1}$$

Proof sketch

Let $(b_{i_1,\ldots,i_p})_{0\leq i_1+\cdots+i_p\leq k-1}$ be integers. Consider the system of equations:

$$\begin{cases} (k-(i_1+\cdots+i_p))y_{i_1,\ldots,i_p} + \sum_{j=1}^{p}(i_j+1)y_{i_1,\ldots,i_{j-1},i_j+1,i_{j+1},\ldots,i_p} = b_{i_1,\ldots,i_p} \\ 0 \leq i_1+\cdots+i_p \leq k-1 \end{cases}$$

Assume further that

$$y_{i_1,\ldots,i_p} \geq 0,\ 0 \leq i_1+\cdots+i_p \leq k \quad \text{and} \quad \sum_{i_1+\cdots+i_p\leq k} y_{i_1,\ldots,i_p} \leq n$$

Proof sketch

Let $(b_{i_1,\dots,i_p})_{0\leq i_1+\dots+i_p\leq k-1}$ be integers. Consider the system of equations:

$$\begin{cases} (k-(i_1+\cdots+i_p))y_{i_1,\dots,i_p} + \sum_{j=1}^{p}(i_j+1)y_{i_1,\dots,i_{j-1},i_j+1,i_{j+1},\dots,i_p} = b_{i_1,\dots,i_p} \\ 0 \leq i_1+\cdots+i_p \leq k-1 \end{cases}$$

Assume further that

$$y_{i_1,\dots,i_p} \geq 0,\ 0 \leq i_1+\cdots+i_p \leq k \quad and \quad \sum_{i_1+\cdots+i_p\leq k} y_{i_1,\dots,i_p} \leq n$$

Theorem

If $k > 1+5^p \log n$ then it admits at most one integral solution.

Proof sketch

Let $(b_{i_1,\ldots,i_p})_{0\le i_1+\cdots+i_p\le k-1}$ be integers. Consider the system of equations:

$$\begin{cases} (k-(i_1+\cdots+i_p))y_{i_1,\ldots,i_p} + \sum_{j=1}^{p}(i_j+1)y_{i_1,\ldots,i_{j-1},i_j+1,i_{j+1},\ldots,i_p} = b_{i_1,\ldots,i_p} \\ 0 \le i_1+\cdots+i_p \le k-1 \end{cases}$$

Assume further that

$$y_{i_1,\ldots,i_p} \ge 0,\ 0 \le i_1+\cdots+i_p \le k \quad \textit{and} \quad \sum_{i_1+\cdots+i_p\le k} y_{i_1,\ldots,i_p} \le n$$

Theorem

If $k > 1 + 5^p \log n$ then it admits at most one integral solution.

$\rightarrow$ the referee recovers the $y_{i,j}$'s and computes the output

Proof sketch

Conclusion:

- [BGKL04] proved the uniqueness for $p = 2$
- we generalized to any p
- sending all the $a_{i,j}^{\ell}$ has cost $\mathcal{O}\left(k(k+p)\log n\right) \to$ not efficient is $k = \omega(\operatorname{polylog} n)$ (compressibility)

Proof sketch

Conclusion:

- [BGKL04] proved the uniqueness for $p = 2$
- we generalized to any p
- sending all the $a_{i,j}^{\ell}$ has cost $\mathcal{O}\left(k(k+p)\log n\right) \rightarrow$ not efficient is $k = \omega(\operatorname{polylog} n)$ (compressibility)

Future work:

- remove the compressibility condition
- handle larger p