The Power of Super-Log Number of Players

Arkadev Chattopadhyay

(TIFR, Mumbai)

Joint with:

Michael Saks (Rutgers)

A Conjecture

$f:\{0,1\}^n \to \{0,1\}$ $\quad$ $g:\{0,1\}^k \to \{0,1\}$.

$(f \circ g)(X_1, X_2, \cdots, X_k) =$ $\quad$ $f(g(C_1), g(C_2), \ldots, g(C_n))$

Question: Complexity of (MAJ ∘ MAJ)?

Observation:

$$\text{Let } D_k^{\text{sim}}(\text{MAJ} \circ \text{MAJ}) = (\log n)^{\omega(1)}$$

$\Rightarrow$ MAJ ∘ MAJ $\notin$ ACC^0

a la Beigel-Tarui'91

$\Rightarrow$ MAJ $\notin$ ACC^0

Proposed by Babai-Kimmel-Lokam'95

	0	1	0	1	1	0	0
X_1	0	1	1	1	1	1	1
X_2	1	1	0	1	1	0	1
X_3	0	1	1	1	1	0	0
	.	.	.	.	.	.	.
	.	.	.	.	.	.	.
X_k	1	1	1	1	1	1	0

n

Some Upper Bounds

	Popular Names	$k \geq 3$
		Deterministic
SYM ∘ AND	**{GIP, Disj,…}**	$O(n/2^k + k \cdot \log n)$.
		Grolmusz'91, Pudlak
		Almost- Simultaneous
SYM ∘ g	{GIP, MAJ ∘ MAJ, Disj…}	$O(k.(\log n)^2)$, $k \geq \log n + 2$.
g: compressible and symmetric		**Babai-Gal-Kimmel-Lokam'02**
		Simultaneous
SYM ∘ ANY		$O(k.(\log n)^2)$, $k \geq \log n + 4$.
		Ada-C-Fawzi-Nguyen'12
		Simultaneous

Block Composition

f:$\{0,1\}^n \to \{0,1\}$ g:$\{0,1\}^{k\times r} \to \{0,1\}$.

$(f_n \circ g_r)(X_1, X_2, \cdots, X_k) =$ $f(g(A_1), g(A_2), \ldots, g(A_n))$

Conjecture:

$$D_k^{\mathrm{sim}}\left(\mathrm{MAJ}_{\sqrt{n}} \circ \mathrm{MAJ}_{\sqrt{n}}\right) = (\log n)^{\omega(1)}.$$

Fact:

$\Rightarrow$ MAJ $\notin$ ACC^0

Babai-Gal-Kimmel-Lokam'02

$n = 2$
$r = 3$

	A_1			A_2		
X_1	0	1	1	1	1	1
X_2	1	1	0	1	1	1
X_3	0	1	1	1	1	0
	.	.	.	.	.	.
	.	.	.	.	.	.
X_k	1	1	1	1	1	0

Still Open!

Even for interactive protocols

Our Result

Theorem: $\mathrm{SYM}_n \circ \mathrm{ANY}_r$ has a 2-round k-party deterministic protocol of cost

$$\big(1 + 2^r \ln(2n)\big)\big(r + \log(2n)\big)$$

when,

$$k \geq \big(1 + 2^r \ln(2n)\big).$$

r = O(log log n)

$$\mathrm{Cost} = (\log n)^{O(1)}$$

Remark 1: First protocol for r > 1.

Remark 2: $f_n \circ \mathrm{MAJ}_s \in f_n \circ \mathrm{ANY}_{\log s}.$

Corollary: $\mathrm{MAJ} \circ \mathrm{MAJ}_r$ has efficient protocol when r is poly-log and k is a sufficiently large poly-log.

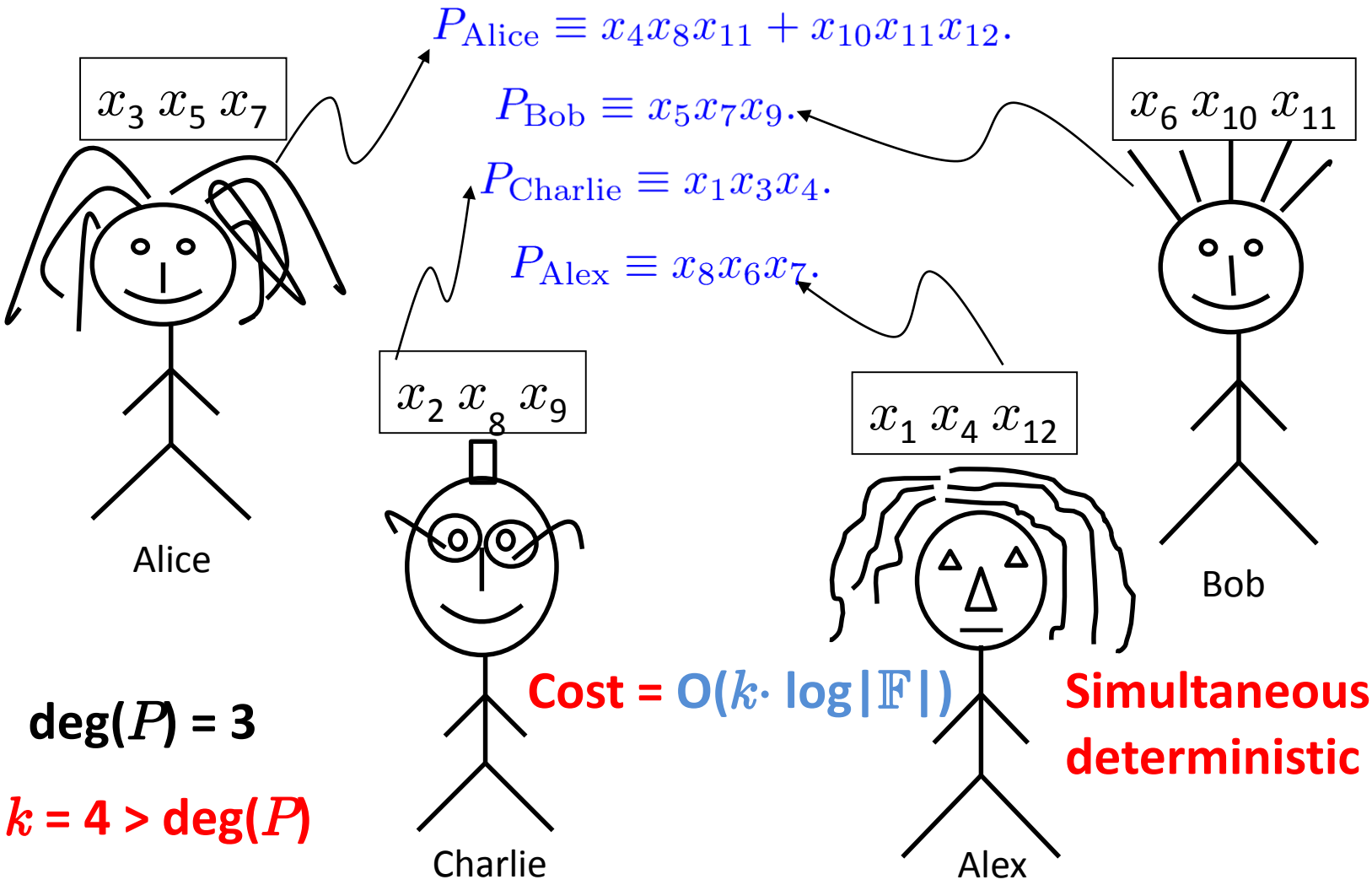
Main Ingredients

- Computing k-1 degree polynomials is easy for k-players. (Goldman-Hastad'90's)

- **Degree reduction by basis change. (New Idea)**

Low degree Polynomials

$$P \equiv \underbrace{x_1x_3x_4}_{\text{Bob, Charlie}} + \underbrace{x_5x_7x_9}_{\text{Bob, Alex}} + \underbrace{x_4x_8x_{11}}_{\text{Alice}} + \underbrace{x_8x_6x_7}_{\text{Alex}} + \underbrace{x_{10}x_{11}x_{12}}_{\text{Alice, Charlie}}.$$



deg(P) = 3

k = 4 > deg(P)

Cost = O($k\cdot$ log$|\mathbb{F}|$)

Simultaneous k-party deterministic protocol

A Polynomial Fantasy

f:$\{0,1\}^n \to \{0,1\}$ g:$\{0,1\}^k \to \{0,1\} \subseteq \mathbb{F}_p$. Prime p > n

$g(X) \equiv P(X_1,\cdots,X_k)$ deg(P) $\leq k$

$P \equiv P_{high}(X) + P_{low}(X)$

deg = k deg < k

(SYM ∘ g) $(C_1,C_2,\cdots,C_n) = \sum_{i=1}^{n} P_{high}(C_i) + \sum_{i=1}^{n} P_{low}(C_i)$

Bad

easy k-player protocol of cost = k.log(p)

Fantasy: $P_{high}(Ci) = 0$ for all i **!!**

Shifted Basis

u-shifted

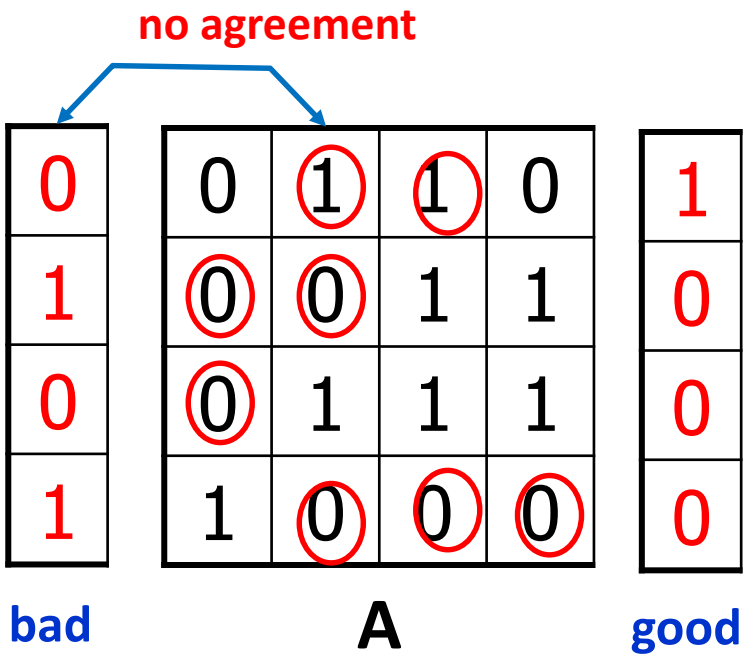
$$B^u \equiv \left\{ \prod_{i \in S} (x_i - u_i) \;\middle|\; S \subseteq [k] \right\}$$

$u = 0^k$ **gives standard basis**

Fact: B^u is a basis for every $u \in \{0,1\}^k$

Def: u is good for A if for all column C of A, u and C agree on some co-ordinate.

Example:



Good is Really Good

(SYM ∘ g) $(C_1, C_2, \cdots, C_n)$ = $\sum_{i=1}^{n} \mathrm{P}_{\mathrm{high}}^{u}(C_i) + \sum_{i=1}^{n} \mathrm{P}_{\mathrm{low}}^{u}(C_i)$

Apply u -shift

Bad
Zeroed out!

easy k-player protocol
of cost log(p)

Fact: $\mathrm{P}_{\mathrm{high}}^{u}(C) = 0$ for all C if u is good for A.

Good Shifts Are Aplenty

Observation: If $k \gg \log n + 1$, Player k spots many good shifts.

$$\Pr_u \left[u \text{ is bad} \right] \leq \frac{1}{2^{k-1}} \times n \ll 1$$

Protocol:

- Player k announces a good shift u.
- All players compute their portions using u.

Cost = k - 1

Simultaneous!

Cost = $k \cdot \log(p)$

= $O(k \cdot \log n)$

Extends to r = O(log log n).

Future Direction

- Can we go to r = O(log n)?
- Is $D_k^{\mathrm{sim}}\left(\mathrm{MAJ}_{\sqrt{n}} \circ \mathrm{MAJ}_{\sqrt{n}}\right) = \left(\log n\right)^{O(1)}$?

Thank You!