Small Error Versus Unbounded Error Protocols in the NOF Model

Nikhil S.Mande

Tata Institute of Fundamental Research, Mumbai, India

May 24, 2016

Joint work with Arkadev Chattopadhyay

Low-Depth Complexity Workshop, St. Petersburg

NOF Model

NOF Model

- k players $P_1, \ldots, P_k$ each with an input $x_i \in \{-1, 1\}^{N_i}$.

NOF Model

- k players $P_1, \ldots, P_k$ each with an input $x_i \in \{-1, 1\}^{N_i}$.
- Target function $f : \{-1, 1\}^{N_1 + \cdots + N_k} \to \{-1, 1\}$.

NOF Model

- k players $P_1, \ldots, P_k$ each with an input $x_i \in \{-1, 1\}^{N_i}$.
- Target function $f : \{-1, 1\}^{N_1 + \cdots + N_k} \rightarrow \{-1, 1\}$.
- Player P_i sees all inputs except x_i.

NOF Model

- k players $P_1, \ldots, P_k$ each with an input $x_i \in \{-1, 1\}^{N_i}$.
- Target function $f : \{-1, 1\}^{N_1 + \cdots + N_k} \to \{-1, 1\}$.
- Player P_i sees all inputs except x_i.
- Each player has unbounded computational power.

NOF Model

- k players $P_1, \ldots, P_k$ each with an input $x_i \in \{-1, 1\}^{N_i}$.
- Target function $f : \{-1, 1\}^{N_1 + \cdots + N_k} \to \{-1, 1\}$.
- Player P_i sees all inputs except x_i.
- Each player has unbounded computational power.
- Communication by writing on blackboard (broadcast).

NOF complexity classes

NOF complexity classes

Definition ($\mathrm{PP}_k^{cc}, \mathrm{UPP}_k^{cc}$)

$$\mathrm{PP}_k(f) \equiv \min_{\epsilon}\left[R_{\epsilon}^{pub}(f) + \log\left(\frac{1}{\epsilon}\right)\right], \quad \mathrm{UPP}_k(f) \equiv \min_{\epsilon}\left[R_{\epsilon}^{priv}(f)\right]$$

NOF complexity classes

Definition ($\mathrm{PP}_k^{cc}, \mathrm{UPP}_k^{cc}$)

$$\mathrm{PP}_k(f) \equiv \min_{\epsilon}\left[R_{\epsilon}^{pub}(f) + \log\left(\frac{1}{\epsilon}\right)\right], \quad \mathrm{UPP}_k(f) \equiv \min_{\epsilon}\left[R_{\epsilon}^{priv}(f)\right]$$

Define $(\mathrm{U})\mathrm{PP}_k^{cc} = \{f : (\mathrm{U})\mathrm{PP}_k(f) = polylog(n)\}$

NOF complexity classes

Definition ($\mathrm{PP}_k^{cc}, \mathrm{UPP}_k^{cc}$)

$$\mathrm{PP}_k(f) \equiv \min_{\epsilon} \left[R_{\epsilon}^{pub}(f) + \log\left(\frac{1}{\epsilon}\right)\right], \quad \mathrm{UPP}_k(f) \equiv \min_{\epsilon} \left[R_{\epsilon}^{priv}(f)\right]$$

Define $(\mathrm{U})\mathrm{PP}_k^{cc} = \{f : (\mathrm{U})\mathrm{PP}_k(f) = \mathit{polylog}(n)\}$

- Not hard: $\mathrm{PP}_k^{cc} \subseteq \mathrm{UPP}_k^{cc}$. (Follows from Newman's Theorem).

Prior work

Prior work

- $\mathrm{PP}_2^{cc} \subsetneq \mathrm{UPP}_2^{cc}$ (Buhrman et al.['07], Sherstov['08]).

Prior work

- $PP_2^{cc} \subsetneq UPP_2^{cc}$ (Buhrman et al.['07], Sherstov['08]).
- Buhrman et al. show an $\Omega(n^{1/3})$ PP_k lower bound for functions in UPP_k^{cc} for $k = 2$, Sherstov shows $\Omega(n^{1/2})$.

Prior work

- $\mathrm{PP}_2^{cc} \subsetneq \mathrm{UPP}_2^{cc}$ (Buhrman et al.['07], Sherstov['08]).
- Buhrman et al. show an $\Omega(n^{1/3})$ PP_k lower bound for functions in UPP_k^{cc} for $k = 2$, Sherstov shows $\Omega(n^{1/2})$.
- $\mathrm{PP}_k^{cc} \subsetneq \mathrm{UPP}_k^{cc}$, $k \leq O(\log\log(n))$ (follows from Beigel ['94] + Sherstov['14]). Shows an $\Omega(n^{1/3})$ lower bound.

Main results

Main results

- $\mathrm{PP}_k^{cc} \subsetneq \mathrm{UPP}_k^{cc}, k \leq \Theta(\log(n))$.

Main results

- $\mathrm{PP}_k^{cc} \subsetneq \mathrm{UPP}_k^{cc}, k \leq \Theta(\log(n))$.
- $\Omega\left(\frac{\sqrt{n}}{4^k}\right)$ PP_k lower bound for functions in UPP_k^{cc}.

Main results

- $\mathrm{PP}_k^{cc} \subsetneq \mathrm{UPP}_k^{cc}, k \leq \Theta(\log(n))$.
- $\Omega\left(\frac{\sqrt{n}}{4^k}\right)$ PP_k lower bound for functions in UPP_k^{cc}.
- There exists a function that is computed very efficiently by $\mathrm{THR} \circ \mathrm{PAR}_{k+1}$ circuits but requires $2^{\Omega\left(\frac{\sqrt{n}}{4^k}\right)}$ size to be computed by depth-three circuits of the form $\mathrm{MAJ} \circ \mathrm{THR} \circ \mathrm{ANY}_k$.

Target function

Target function

Definition (Goldmann, Håstad, Razborov ['92])

Let

$$P(x, y_1, \ldots, y_k) \equiv \sum_{i=0}^{n-1} \sum_{j=0}^{n4^k-1} 2^i {y_1}_j \ldots {y_k}_j (x_{i,2j} + x_{i,2j+1})$$

where $x \in \{\pm 1\}^{2n^2 4^k}$, $y_i \in \{\pm 1\}^{n4^k}$ for each i.
Then, $\mathrm{GHR}_k^N(x, y_1, \ldots, y_k) \equiv sgn(2P(x, y_1, \ldots, y_k) + 1)$, where $N = 2n^2 4^k$.

Discrepancy and Cylinder Intersections

Discrepancy and Cylinder Intersections

- A subset $S_i \subseteq X_1 \times \cdots \times X_k$ is a cylinder in the ith direction if membership in S_i doesn't depend on the ith coordinate.

Discrepancy and Cylinder Intersections

- A subset $S_i \subseteq X_1 \times \cdots \times X_k$ is a cylinder in the ith direction if membership in S_i doesn't depend on the ith coordinate.
- S is a cylinder intersection if it can be written as $S = \cap_{i=1}^{k} S_i$.

Discrepancy and Cylinder Intersections

- A subset $S_i \subseteq X_1 \times \cdots \times X_k$ is a cylinder in the ith direction if membership in S_i doesn't depend on the ith coordinate.
- S is a cylinder intersection if it can be written as $S = \cap_{i=1}^{k} S_i$.

Lemma (Folklore)

$R_\epsilon^{pub}(f) \geq \log(2\epsilon / \min_\mu Disc_\mu^k(f))$.

Discrepancy and Cylinder Intersections

- A subset $S_i \subseteq X_1 \times \cdots \times X_k$ is a cylinder in the ith direction if membership in S_i doesn't depend on the ith coordinate.
- S is a cylinder intersection if it can be written as $S = \cap_{i=1}^{k} S_i$.

Lemma (Folklore)

$R_{\epsilon}^{pub}(f) \geq \log(2\epsilon / \min_{\mu} Disc_{\mu}^{k}(f))$.

Thus, PP_k lower bounds exactly correspond to discrepancy upper bounds.

Discrepancy

Discrepancy

Let $f : X_1 \times \cdots \times X_k \to \{-1, 1\}$.

Definition

Let μ be a distribution on $X_1 \times \cdots \times X_k$. The discrepancy of f according to μ, $Disc_\mu^k(f)$ is

$$\max_S \left| \mu(f^{-1}(1) \cap S) - \mu(f^{-1}(-1) \cap S) \right|$$

where the maximum is taken over all cylinder intersections S.

Discrepancy under product distributions

Discrepancy under product distributions

Lemma (Folklore)

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, *and* μ *any product distribution. Then,*

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

Proof Outline - 1

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, and μ any product distribution. Then,

$$(Disc_\mu^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1}\left[\left|\mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k})\right|\right]$$

Proof Outline - 1

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, *and* μ *any product distribution. Then,*

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

- We construct a distribution μ that makes all $y_i's$ uniform and independent of each other.

Proof Outline - 1

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, *and* μ *any product distribution. Then,*

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1}\left[\left|\mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k})\right|\right]$$

- We construct a distribution μ that makes all $y_i's$ uniform and independent of each other.
- $x's$ are distributed such that $A_j = \frac{1}{2}\sum_{i=0}^{n-1} 2^i(x_{i,2j} + x_{i,2j+1})$ is binomially distributed for each $0 \leq j \leq n4^k - 1$.

Proof Outline - 1

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, and μ any product distribution. Then,

$$(Disc_\mu^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

- We construct a distribution μ that makes all $y_i's$ uniform and independent of each other.
- $x's$ are distributed such that $A_j = \frac{1}{2} \sum_{i=0}^{n-1} 2^i (x_{i,2j} + x_{i,2j+1})$ is binomially distributed for each $0 \leq j \leq n4^k - 1$.
- Note $\mathrm{GHR}_k^N(x, y_1, \ldots, y_k) = sgn(\sum_{j=0}^{n4^k} A_j {y_1}_j \cdots {y_k}_j)$.

Proof Outline - 2

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, *and* μ *any product distribution. Then,*

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

Proof Outline - 2

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1,1\}$, and μ any product distribution. Then,

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

- Will show that for many fixings of the $y_i's$, the inner expectation is small.

Proof Outline - 2

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, *and* μ *any product distribution. Then,*

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

- Will show that for many fixings of the $y_i's$, the inner expectation is small.
- Analyze the number and size of integral solutions to Hadamard constraints.

Proof Outline - 2

Lemma

Let $f : X \times Y_1 \times \cdots \times Y_k \to \{-1, 1\}$, *and* μ *any product distribution. Then,*

$$(Disc_{\mu}^{k+1}(f))^{2^k} \leq \mathbb{E}_{y_1^0, y_1^1, \ldots, y_k^0, y_k^1} \left[\left| \mathbb{E}_x \prod_{a \in \{0,1\}^k} f(x, y_1^{a_1}, \ldots, y_k^{a_k}) \right| \right]$$

- Will show that for many fixings of the $y_i's$, the inner expectation is small.
- Analyze the number and size of integral solutions to Hadamard constraints.
- Use anticoncentration properties of binomial distribution.

Circuit Lower Bounds

Circuit Lower Bounds

- Clearly, GHR_k can be computed by polynomial sized $\mathrm{THR} \circ \mathrm{PAR}_{k+1}$ circuits.

Circuit Lower Bounds

- Clearly, GHR_k can be computed by polynomial sized $\mathrm{THR} \circ \mathrm{PAR}_{k+1}$ circuits.

Lemma (Folklore)

For $f \in \mathrm{MAJ} \circ \mathrm{SYM} \circ \mathrm{ANY}_k$ of size s, and any partition of the input bits amongst $k+1$ players, there exists a randomized protocol computing f with advantage $\Omega(1/s)$ and cost $O(k \log(s))$.

Circuit Lower Bounds

- Clearly, GHR_k can be computed by polynomial sized $\mathsf{THR} \circ \mathsf{PAR}_{k+1}$ circuits.

Lemma (Folklore)

For $f \in \mathsf{MAJ} \circ \mathsf{SYM} \circ \mathsf{ANY}_k$ of size s, and any partition of the input bits amongst $k+1$ players, there exists a randomized protocol computing f with advantage $\Omega(1/s)$ and cost $O(k \log(s))$.

Lemma (GHR['92])

$$\mathsf{MAJ} \circ \mathsf{THR} \subseteq \mathsf{MAJ} \circ \mathsf{MAJ}$$

- GHR_k requires $2^{\Omega\left(\frac{\sqrt{n}}{4^k}\right)}$ size to be computed by $\mathsf{MAJ} \circ \mathsf{THR} \circ \mathsf{ANY}_k$ circuits.

Open questions

Open questions

- $\Omega(n)$ PP_k lower bound for an explicit function in UPP_k (open for 2 player case too)?

Open questions

- $\Omega(n)$ PP_k lower bound for an explicit function in UPP_k (open for 2 player case too)?
- Is GHR_k hard for $k > \log(n)$ players?

Open questions

- $\Omega(n)$ PP_k lower bound for an explicit function in UPP_k (open for 2 player case too)?
- Is GHR_k hard for $k > \log(n)$ players?
- Can we find an explicit f not in UPP_3^{cc}? This will show that f is not in polynomial size $\mathrm{THR} \circ \mathrm{THR}$ (Hansen, Podolskii ['15]).

Thank You!