Deterministic Lifting Theorems for One-Way Number-on-Forehead Communication

Guangxu Yang

Jiapeng Zhang

USC University of Southern California

One-Way Number-on-Forehead Communication

$F: [N]^3 \to \{0,1\}$

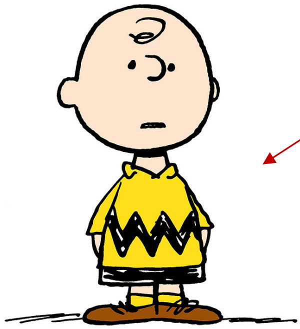
Alice
$y, z \in [N]\times[N]$

$\pi_A(y,z)$ → Bob

Bob
$x, z \in [N]\times[N]$

$\pi_A(y,z)$ → Charlie

$\pi_B(x,z)$ → Charlie



Charlie
$x, y \in [N]\times[N]$

$F(x,y,z)$

Applications:
Circuit complexity [HG90, PRS97, Cha07, VW07],
Cryptography [CKGS98, BDFP17],
Streaming algorithms [KMPV19, VW07].

One-Way Number-on-Forehead Communication

One-way Number-on-Forehead Communication Complexity

Alice holds $y, z \in [N]$, Bob holds $x, z \in [N]$, Charlie holds $x, y \in [N]$, they collaborate to compute a function $F: [N]^3 \to \{0,1\}$. A three-party protocol Π proceeds as follows:

- Alice sends message $\Pi_A(y, z)$ to Bob and Charlie.
- Bob sends messages $\Pi_B(x, z, \Pi_A(y, z))$ to Charlie.
- Charlie outputs $F(x, y, z)$ depends on $(\Pi_A(y, z), \Pi_B(x, z, \Pi_A(y, z)), x, y)$.

The deterministic one-way NOF communication complexity is the maximum total length $|\Pi_A| + |\Pi_B|$ over all inputs, denoted by $\mathrm{OCC}(F)$.

An important open problem [BDPW10] : Optimal explicit separation between the randomized and deterministic one-way NOF communication

$F: [N]^3 \to \{0,1\}$ The deterministic one-way NOF communication complexity of F is $\Omega(\log N)$, but the randomized one-way NOF communication complexity of F is $O(1)$.

Previous results: $\Omega(\log\log N)$ vs $O(1)$ [BGG06] and $\Omega(\log^{1/3} N)$ vs $O(1)$ [KLM24]

Deterministic Lifting Theorems for One-Way Number-on-Forehead Communication

Proving analogs of query to communication lifting theorems for even 3 parties in the number-on-forehead (NOF) communication model would be a huge breakthrough.

One-Way Communication

One-way Communication Complexity

Alice holds $z \in [N]$ and Bob holds $w \in [N]$. Alice sends a single message π(z) to Bob, and Bob outputs f (z, w) based on w and the received message.

The deterministic communication complexity is the maximum length of the message | π(z) | over all possible inputs, denoted by DCC(f).

Alice

$z \in [N]$

$\pi(z)$

$f(z, w)$

Bob

$w \in [N]$

One-Way Communication

Theorem 1

For any $z_0, z_1 \in Z$, There is a $v \in [N]$ such that $f(z_0, v) \neq f(z_1, v)$.

$M(f)$ is an matrix where each entry at position (z, w) is $f(z, w)$

For any $f: [N]\times[N] \to \{0,1\}$, we use $M(f)$ to denote the communication matrix corresponding to f and Z denote the set of distinct rows of $M(f)$.

The deterministic one-way communication complexity of f is $\log|Z|$.

The communication matrix of f

$[N]$

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

Π →

π_1

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

π_2

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

π_3

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

One-Way Communication

Theorem 1

For any $f: [N] \times [N] \to \{0,1\}$, we use $M(f)$ to denote the communication matrix corresponding to f and Z denote the set of distinct rows of $M(f)$.

The deterministic one-way communication complexity of f is $\log |Z|$.

The communication matrix of f

$[N]$

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

Π →

y

π_1

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

π_2

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

π_3

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

One-Way Communication

Theorem 2

The deterministic one-way communication complexity of Equality function (EQ) is $\log N$

$[N]$ (columns) × $[N]$ (rows):

1							
	1						
		1					
			1				
				1			
					1		
						1	
							1

$EQ(z, w) = 1$ if and only if $z = w$

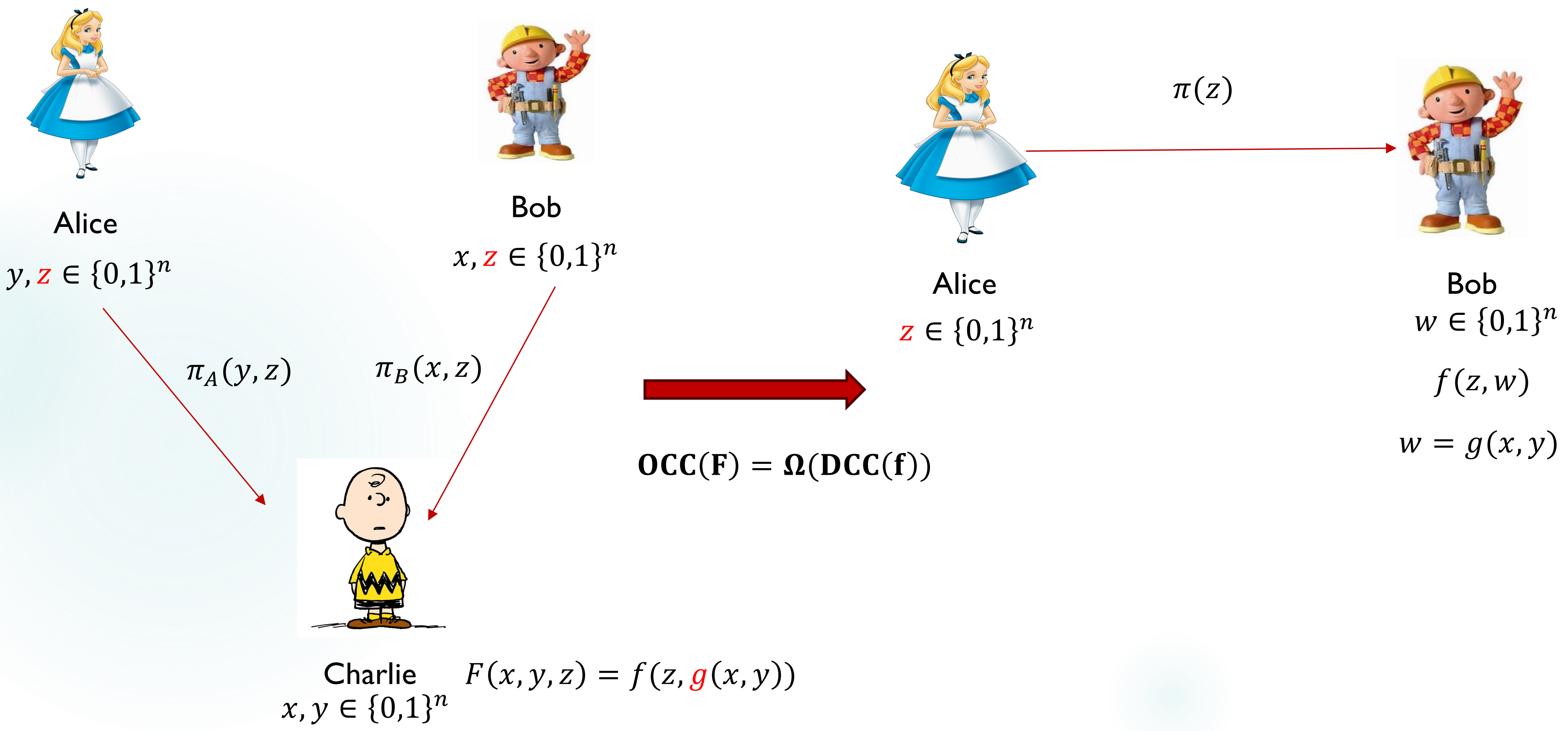
An optimal separation between the randomized and deterministic:

The deterministic one-way communication complexity of EQ is $\Omega(\log N)$, but the randomized one-way communication complexity of EQ is $O(1)$.

By hashing

Can we prove the optimal separation between the randomized and deterministic one-way NOF communication via EQ ?

Deterministic Lifting Theorem



Two-source extractor

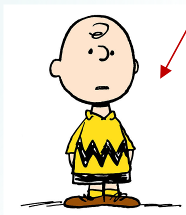
Alice

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

Bob

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

$\pi_A(y, z)$ $\pi_B(x, z)$



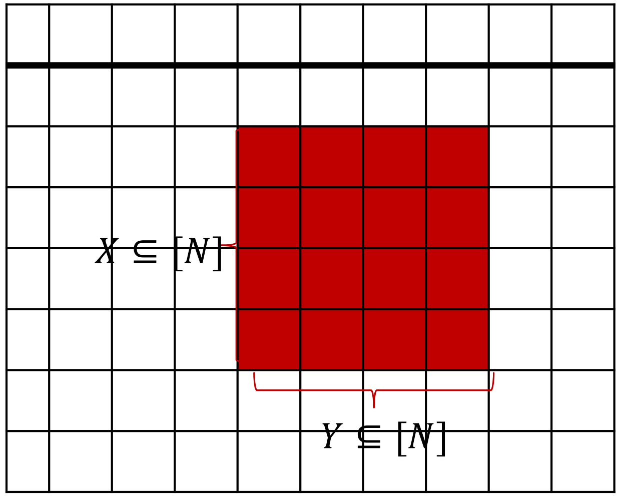
Charlie

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

$F(x, y, z) = f(z, g(x, y))$

$EQ(x, y, z) = 1$ if and only if $x = y = z$ ✗

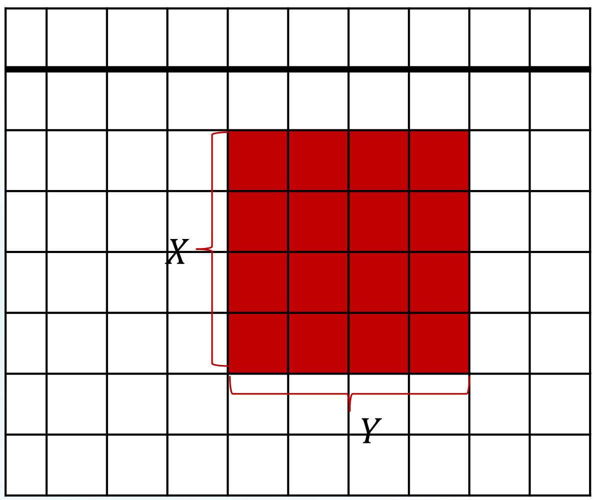
The communication matrix of $g: [N] \times [N] \rightarrow [q]$



$|X||Y| \geq \frac{N^2}{q}$ $\{g(x, y): x \in X, y \in Y\} = [q]$

Two-source extractor

The communication matrix of $\mathrm{IP}: [N]\times[N] \rightarrow [q]$



$\{\mathrm{IP}(x,y): x \in X, y \in Y\} = [q]$

Definition 3

Let q be a prime power and $k \geq 5$. we define the gadget function g is the inner-product function $\mathrm{IP}:\ F_q^k \times F_q^k \rightarrow F_q$ given by

$$\mathrm{IP} = \langle\ x, y\ \rangle\ = \sum_{i=1}^{k} x_i y_i\ mod\ \ q$$

By standard fourier analysis

Two Source Extractor Lemma

Set $N\ =\ q^k$ for some constant $k \geq\ 5$, then for any $X, Y \subset [N]$ with size $|X|\times |Y| \geq \frac{N^2}{q}$,

$$\{\mathrm{IP}(x,y): x \in X, y \in Y\} = [q]$$

Deterministic Lifting Theorem

Definition 4 [Lifted problem in NOF]

For any two-party function f: $[q]\times[q] \rightarrow \{0,1\}$ and a gadget function IP: $[N]\times[N] \rightarrow [q]$, the lifted problem, denoted by $f \circ \mathrm{IP}$: $[N]\times[N]\times[q] \rightarrow \{0,1\}$ is defined by,

$$f \circ \mathrm{IP}(x,y,z) = f(z, \mathrm{IP}(x,y))$$

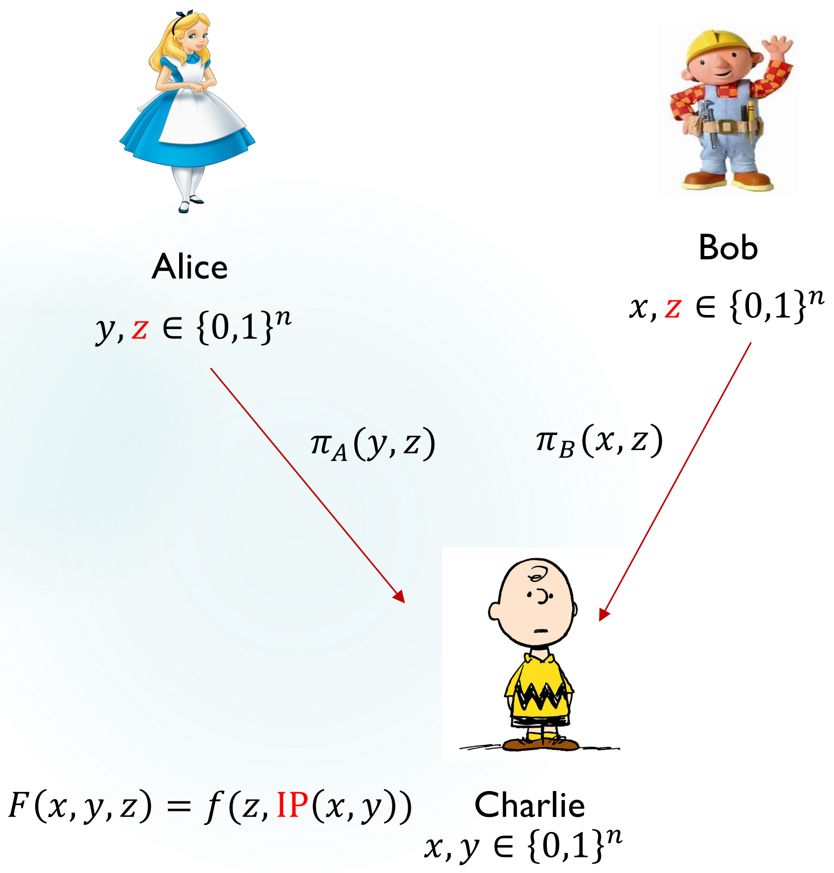
In the NOF setting, we assume that Alice has the input (y,z), Bob has the input (x,z), and Charlie has the input (x, y).

Deterministic Lifting Theorem

For any Boolean function $f: [q]\times[q] \rightarrow \{0,1\}$, we have

$$\mathrm{OCC}(f \circ \mathrm{IP}) = \Theta(\mathrm{DCC}(f))$$

The Proof of Deterministic Lifting Theorems



Our goal: $\mathrm{OCC}(f \circ \mathrm{IP}) = \Theta(\mathrm{DCC}(f))$

$$\mathrm{OCC}(f \circ \mathrm{IP}) = O(\mathrm{DCC}(f))$$

Theorem 1:

The deterministic one-way communication complexity of f is $\log |Z|$.

$$\mathrm{OCC}(f \circ \mathrm{IP}) = \Omega(\log |Z|)$$

Proof by contradiction:

Theorem 2

For any protocol Π with deterministic one-way NOF communication complexity at most $\frac{\log |Z|}{2}$, there exists (π_A^*, π_B^*) along with distinct elements $z_0, z_1 \in [Z]$ and a pair $(x, y) \in [N] \times [N]$, such that

$$\Pi_A^*(y, z_1) = \Pi_A^*(y, z_0) = \pi_A^* \ and \ \Pi_B^*(x, z_1) = \Pi_B^*(x, z_0) = \pi_B^*$$

But

$$f(z_0, \mathrm{IP}(x, y)) \neq f(z_1, \mathrm{IP}(x, y))$$

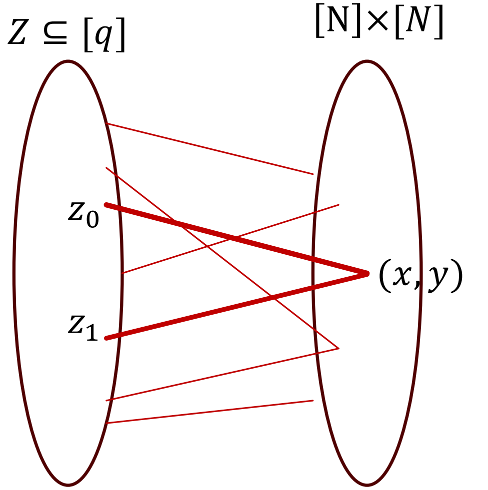
Proof

Theorem 2: For any protocol Π with deterministic one-way NOF communication complexity at most $\frac{\log|Z|}{2}$, there exists (π_A^*, π_B^*) along with distinct elements $z_0, z_1 \in [Z]$ and a pair $(x, y) \in [N] \times [N]$, such that

$$\Pi_A^*(y, z_1) = \Pi_A^*(y, z_0) = \pi_A^* \text{ and } \Pi_B^*(x, z_1) = \Pi_B^*(x, z_0) = \pi_B^*$$

But

$$f\big(z_0, \mathrm{IP}(x, y)\big) \neq f\big(z_1, \mathrm{IP}(x, y)\big)$$



$$f\big(z_0, \mathrm{IP}(x, y)\big) \neq f\big(z_1, \mathrm{IP}(x, y)\big)$$

Proof

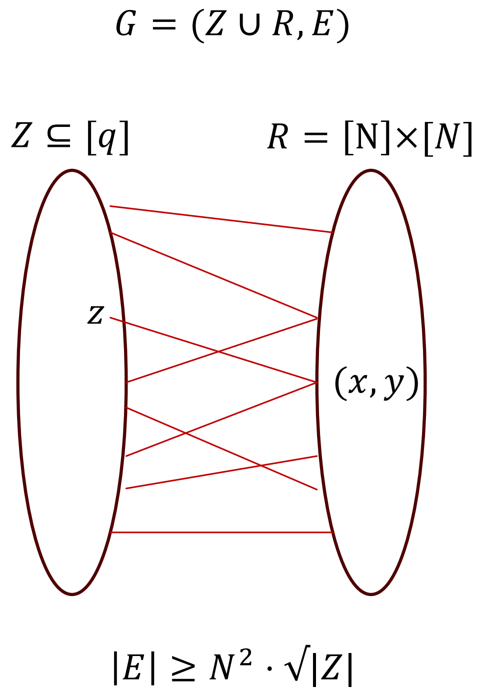
Lemma 1

For any protocol Π with deterministic one-way NOF communication complexity $\frac{\log|Z|}{2}$, there exists a messgae pair (π_A^*, π_B^*) such that the following set E has size at least

$$|E| \geq \frac{N^2 \cdot |Z|}{\sqrt{|Z|}} = N^2 \cdot \sqrt{|Z|}$$

Here, the set E is defined as:

$$E = \{(z, x, y) \in Z \times [N] \times [N]: \ \Pi_A^*(y, z) = \pi_A^* \ and \ \Pi_B^*(x, z) = \pi_B^* \}.$$



Proof: By the pigeonhole principle. The number of inputs is $N^2 \cdot |Z|$ and the number of messages is $2^{\log\frac{|Z|}{2}} = \sqrt{|Z|}$.

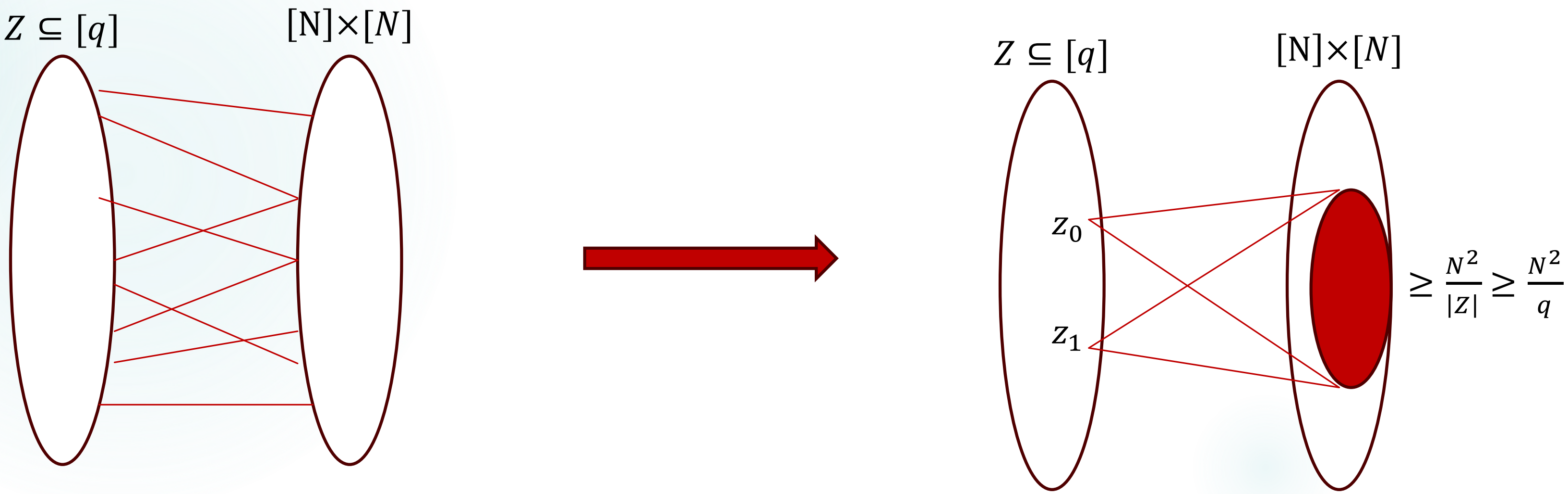
Proof

Graph Lemma

Let $G = (Z \cup R, E)$ be a bipartite graph with $R = [N]\times[N]$ and $|E| \geq N^2 \cdot \sqrt{|Z|}$. Then there exists distinct $z_0, z_1 \in Z$ such that

$$|N(z_0) \cap N(z_1)| \geq \frac{N^2}{|Z|}$$

where $N(z) \subseteq R$ denote the neighborhoods of z in R.



Proof of the graph lemma

Proof of the Graph Lemma:

We prove it by a probabilistic argument. We random sample z_0, z_1 uniformly,

$$E[|N(z_0) \cap N(z_1)|] \geq \frac{N^2}{|Z|}$$

Let $\mathbb{I}(z,r) := \mathbb{I}\{(z,r) \in E\}$ denote the indicator function for whether the edge (z,r) exists in E
Then we have

$$\mathrm{E}[\mathrm{N}(\mathrm{z}_0) \cap N(\mathrm{z}_1)] = \sum_{r \in R} \mathrm{E}[\mathbb{I}(z_0, r) \cdot \mathbb{I}(z_1, r)] = \sum_{r \in R} (E[\mathbb{I}(z,r)])^2 \geq \frac{1}{N^2} \cdot \left(\sum_{r \in R} E[\mathbb{I}(z,r)]\right)^2 = \frac{1}{N^2} \cdot \left(\sum_{r \in R} \frac{\deg(r)}{|Z|}\right)^2 = \frac{1}{N^2} \cdot \frac{|E|^2}{|Z|^2} \geq \frac{N^2}{|Z|}$$

Cauchy–Schwarz inequality
and $R = N^2$

$$|E| = \sum_{r \in R} \deg(r) \quad |E| \geq N^2 \cdot \sqrt{|Z|}$$

Proof

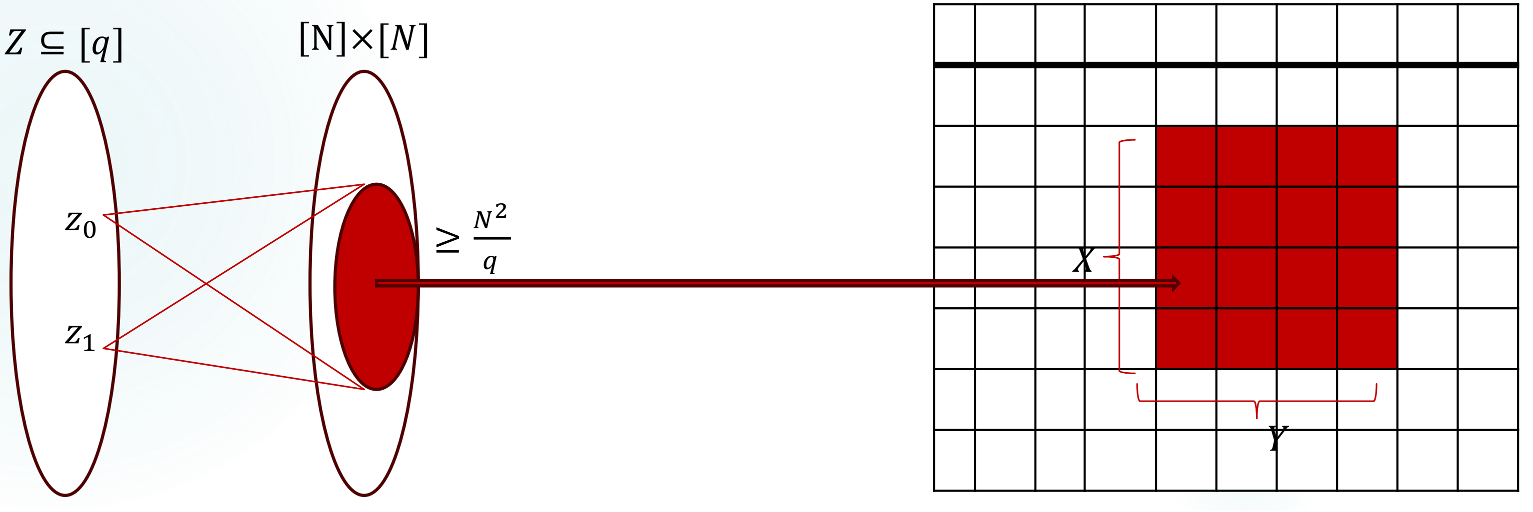
Rectangle Lemma

Let $R = \{(x, y)\colon (x, y, z_0) \in E\} \cap \{(x, y)\colon (x, y, z_1) \in E\}$. Then

R is a rectangle,, i.e., $R = X \times Y$ for some $X, Y \subseteq \{0,1\}^n$.

where $E = \{(z, x, y) \in Z \times [N] \times [N]\colon \Pi_A^*(y, z) = \pi_A^* \ and\ \Pi_B^*(x, z) = \pi_B^*\}$.

The communication matrix of $\mathrm{IP}\colon [N] \times [N] \to [q]$



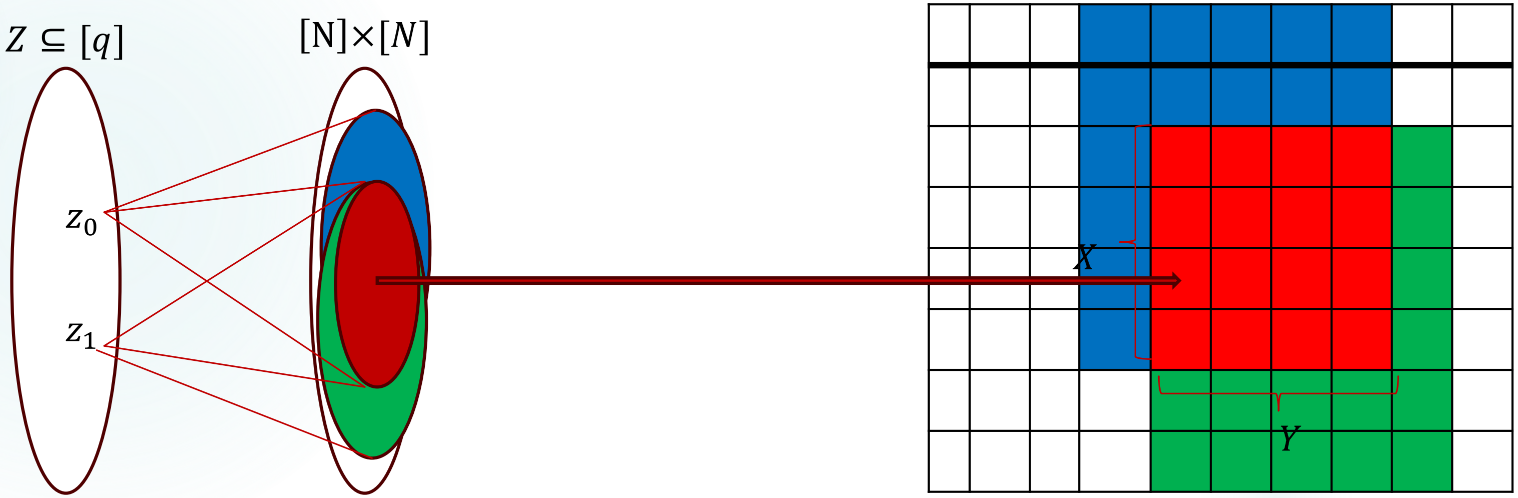
Proof of Rectangle Lemma

Let $R = \underbrace{\{(x,y) : (x,y,z_0) \in E\}}_{R_0} \cap \underbrace{\{(x,y) : (x,y,z_1) \in E\}}_{R_1}$.

$E = \{(z,x,y) \in Z \times [N] \times [N] : \Pi_A^*(y,z) = \pi_A^* \text{ and } \Pi_B^*(x,z) = \pi_B^*\}$.

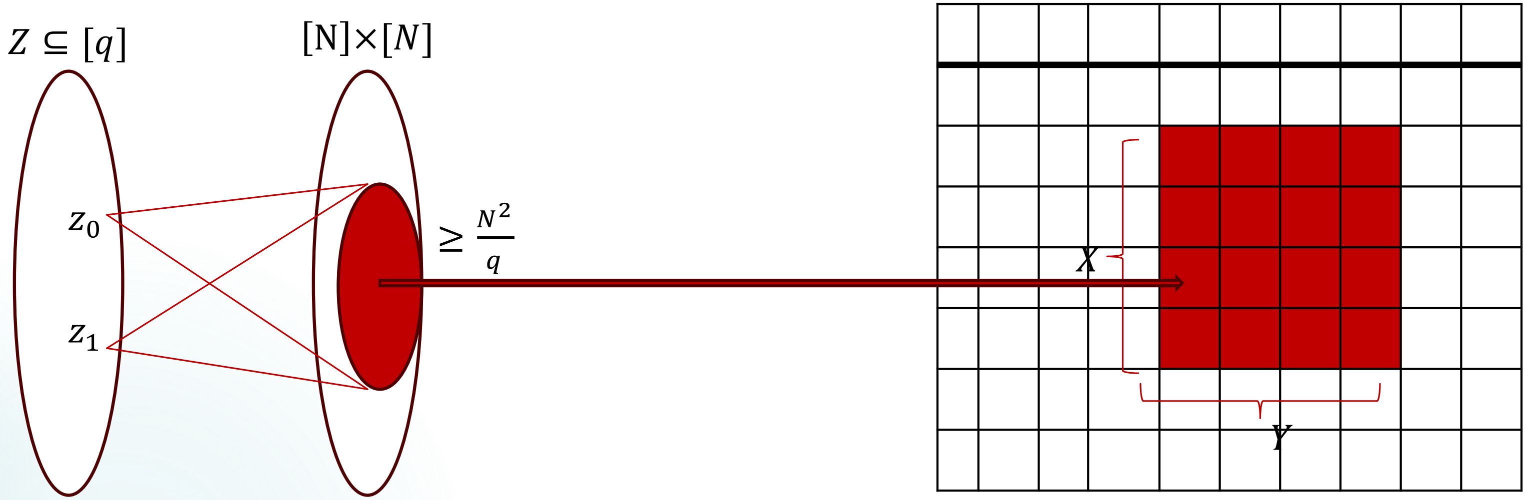
$R_0 = X_0 \times Y_0$ is a rectangle and $R_1 = X_1 \times Y_1$ is a rectangle $\Longrightarrow$ $R = (X_0 \cap X_1) \times (Y_0 \cap Y_1)$

The communication matrix of IP: $[N] \times [N] \rightarrow [q]$



Proof

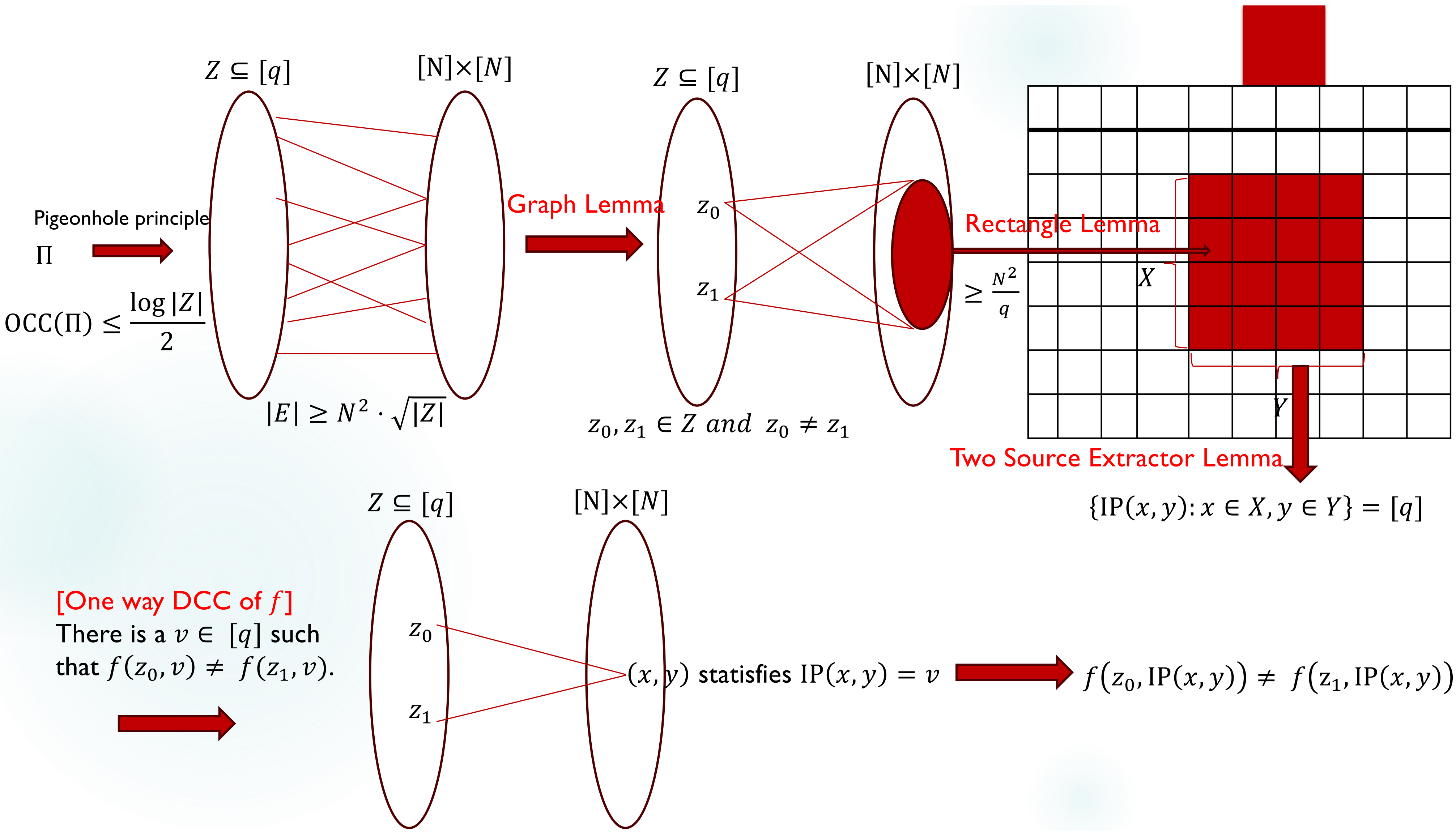
The communication matrix of $\mathrm{IP}: [N]\times[N] \to [q]$



$z_0, z_1 \in Z \; and \; z_0 \neq z_1$

Two Source Extractor Lemma $\{\mathrm{IP}(x,y): x \in X, y \in Y\} = [q]$

- Recall that $z_0, z_1 \in Z \; and \; z_0 \neq z_1$, there is a $v \in [q]$ such that $f(z,v) \neq f(z',v)$. [One way DCC of f]
- Since $\{\mathrm{IP}(x,y): x \in X, y \in Y\} = [q]$, there is a pair $(x,y) \in X\times Y$ such that $\mathrm{IP}(x,y) = v$. [Two Source Extractor
- We have $f\big(z_0, \mathrm{IP}(x,y)\big) \neq f\big(z_1, \mathrm{IP}(x,y)\big)$. [One way NOF DCC of $f \circ \mathrm{IP}$]


Pigeonhole principle
Π
OCC(Π) ≤ log |Z| / 2
Z ⊆ [q]
[N]×[N]
|E| ≥ N² · √|Z|
Graph Lemma
Z ⊆ [q]
[N]×[N]
z₀
z₁
z₀, z₁ ∈ Z and z₀ ≠ z₁
Rectangle Lemma
≥ N²/q
X
Y
Two Source Extractor Lemma
{IP(x, y): x ∈ X, y ∈ Y} = [q]
[One way DCC of f]
There is a v ∈ [q] such
that f(z₀, v) ≠ f(z₁, v).
Z ⊆ [q]
[N]×[N]
z₀
z₁
(x, y) statisfies IP(x, y) = v
f(z₀, IP(x, y)) ≠ f(z₁, IP(x, y))

Our contribution

- One way NOF deterministic lifting theorem

For any Boolean function $f : [N] \times [N] \to \{0,1\}$, we have

$$\mathrm{OCC}(f \circ \mathrm{IP}) = \Theta(\mathrm{DCC}(f))$$

- An optimal explicit separation between the randomized and deterministic one-way NOF communication

The deterministic one-way NOF communication complexity of $\mathrm{EQ} \circ \mathrm{IP}$ is $\Omega(\log N)$,
but the randomized one-way NOF communication complexity of $\mathrm{EQ} \circ \mathrm{IP}$ is $O(1)$.

- A new proof of the $\Omega(n)$ deterministic one-way three-party NOF communication complexity of set disjointness

Open Problems

- One way NOF randomized lifting theorem

For any Boolean function $f : [N] \times [N] \rightarrow \{0,1\}$, we have

$$\mathrm{ORCC}(f \circ \mathrm{IP}) = \Theta(\mathrm{RCC}(f))$$

- An optimal explicit separation between the randomized and quantum one-way NOF communication

- A proof of the $\Omega(n)$ randomized one-way three-party NOF communication complexity of set disjointness (Best known bound is $\Omega(\sqrt{n})$)