Exponential Separation of Quantum and Classical One-Way Numbers-on-Forehead Communication

Guangxu Yang **Jiapeng Zhang**

USC University of Southern California

Quantum versus Classical Separation

- Quantum versus classical separation is a central goal in understanding the potential advantages of quantum computation.

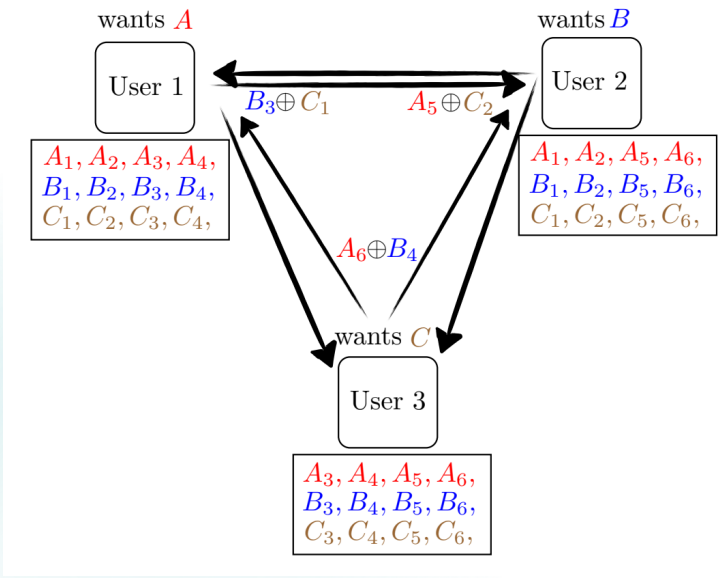
- Previous works only for two party communication complexity [BCW98, Raz99, BYJK04, GKK+07, RK11, Gav16, GRT22, Gav19, Gav20, GGJL24]

  The randomized communication complexity of F is $\Omega(poly(n))$, but the quantum communication complexity of F is $O(\log n)$.

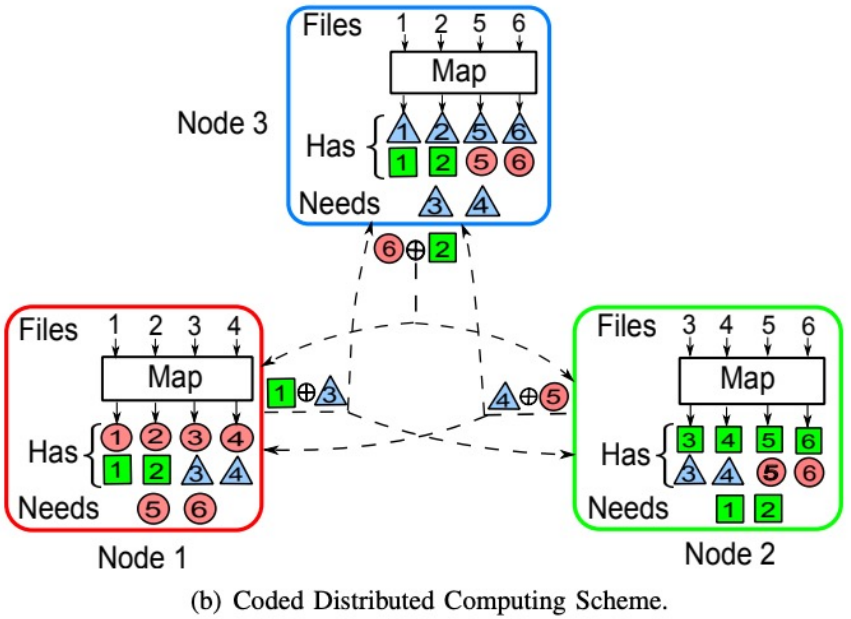
- Communication separations have also motivated experimental demonstrations of quantum advantage [TSB+05, XAW+15, GXY+16, KKD19, SLW+25, ABK24,KDG+25].

Communication with overleap inputs

- Data redundancy typically helps reduce communication costs.



D2D caching: TIT 2015



(b) Coded Distributed Computing Scheme.

Coded Distributed Computing: TIT 2017

Can quantum communication still offer an exponential advantage even in the presence of substantial redundancy?

One-Way Number-on-Forehead Communication

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

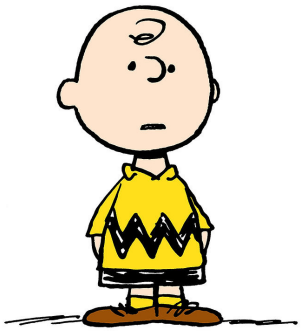
$\pi_A(y,z)$



$\pi_A(y,z)$



$\pi_B(x,z)$



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

Alice

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

Bob

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

Charlie

$F(x,y,z)$

$$\mathrm{OCC}^{\mathrm{NOF}}(\mathrm{F}) = \min_{\Pi}\{\,|\Pi|:\ \Pi(x,y,z) = F(x,y,z)\ \ \forall\, x,y,z\}$$

Why we study one-way NOF

Circuit Lower Bounds:

- Proving ω (log n) lower bounds for any function f in k-party deterministic one-way NOF communication when k = log n will imply $f \notin ACC^0$ circuits [BT94,HG91]
- Proving strong **three**-party deterministic one-way NOF communication lower bounds for some problems will imply the size-depth trade-off of Boolean circuits [Val77,PRS97]

Applications:

- Additive combinatorics [LPS17], Cryptography [CKGS98, BDFP17], Streaming algorithms [KMPV19,VW07], Distributed computing [DKO14], Space-bounded pseudorandom generators [BNS92, GR14], Oblivious branching program lower bounds [VW07].

Quantum versus Classical Separation

- Previous works only for two party communication complexity [BCW98, Raz99, BYJK04, GKK+07, RK11, Gav16, GRT22, Gav19, Gav20, GGJL24]

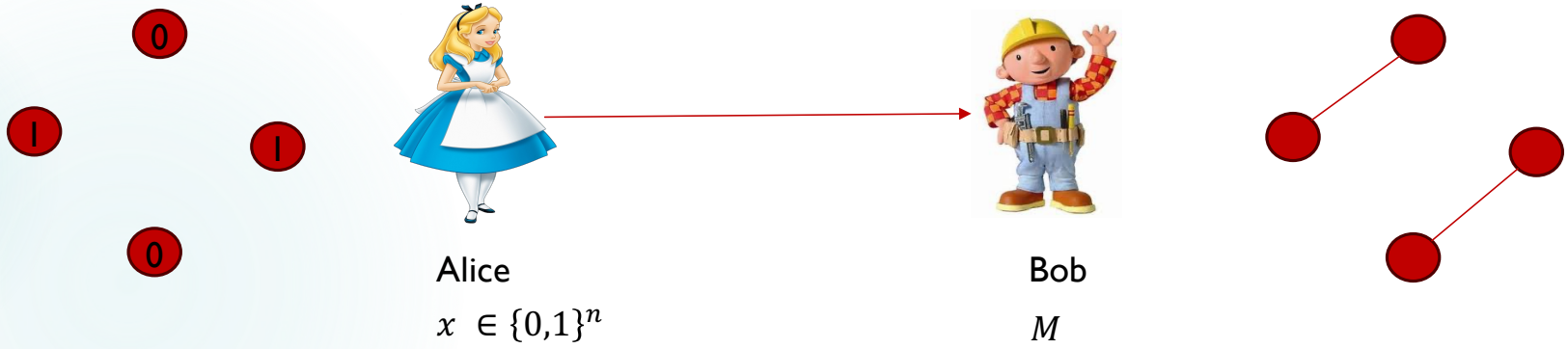
- An important open problem [GP08] : Explicit separation between the randomized and quantum one-way NOF communication.

Main Theorem of This Paper: For a search problem F :

The randomized one-way k-party NOF communication complexity of F is $\Omega(n^{\frac{1}{3}}/2^{k/3})$, but the quantum one-way NOF communication complexity of F is $O(\log n)$.

One Way Communication Complexity

Hidden Matching Problem (HM): Alice holds x ∈ $\{0,1\}^n$, Bob holds a perfect matching M on n nodes, Bob output a (i, j, b) such that (i, j) is an edge in M and $b = x_i \oplus x_j$.



Theorem I [BYJK04] :
The randomized one-way communication complexity of HM is $\Omega(n^{1/2})$, but the quantum one-way communication complexity of HM is $O(\log n)$.

Hidden Matching Problem

Simplified Hidden Matching Problem: Alice holds $x \in \{0,1\}^n$, Bob holds $k \in [n]$, Bob output a (i, j, b) such that (i, j) is an edge in M_k and $b = x_i \oplus x_j$.

where M_k is a perfect matching obtained by cyclically shifting the indices of the second partition by k. Let $m = n/2$

$$M_k := \left\{\left(\ell, m + \left((k + \ell) \bmod m\right)\right) : \ell \in [m]\right\}.$$

Theorem I [BYJK04] :

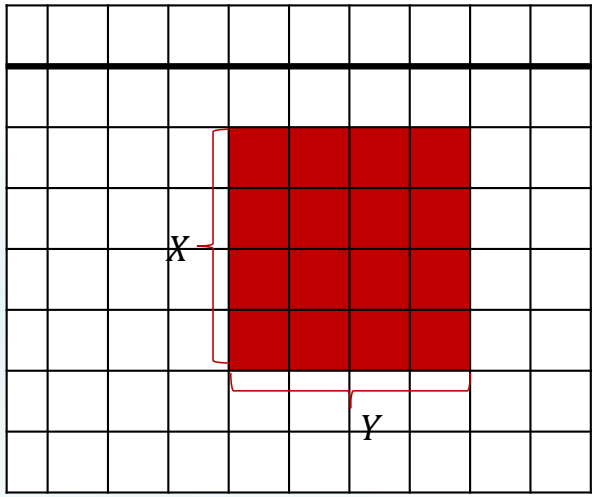
The randomized one-way communication complexity of HM is $\Omega(n^{1/2})$, but the quantum one-way communication complexity of HM is $O(\log n)$.

Quantum versus Classical Separation

Could we lift the quantum advantage in one-way communication to one-way NOF communication ?

IP is a two-source extractor

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



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

Definition 2

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

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

By standard fourier analysis

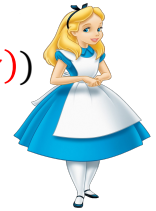
Two Source Extractor Lemma

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

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

Lifted Hidden Matching in One-Way NOF

$F(k, y, z) = HM(k, \mathrm{IP}(y, z))$



Alice

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

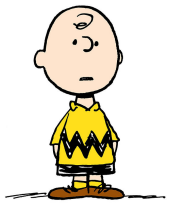
$\Pi_A(y, z, r)$



Bob

M_k, z

$\Pi_B(k, z, r)$



Charlie

M_k, y

Lifted Hidden Matching Problem (LHM)

Let $n_0 = n^{2/3}$, $\mathrm{IP}: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{n_0}$, $k \in [n_0]$.

Alice holds $y, z \in \{0,1\}^n$, Bob holds $k \in [n_0], z \in \{0,1\}^n$, Charlie holds $k \in [n_0], y \in \{0,1\}^n$.

Charlie outputs (i, j, b) such that (i, j) is an edge in M_k and $b = \mathrm{IP}(y, z)_i \oplus \mathrm{IP}(y, z)_j$

The quantum one-way NOF communication complexity of LHM is $O(\log n)$.

The randomized one-way NOF communication complexity of LHM is $\Omega(n^{1/3})$.

Step 1: Simplifying the protocols

$\mathsf{F}(k, y, z) = HM(\mathrm{IP}(y, z), k)$



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

Alice

$\Pi = (\Pi_A, \Pi_B)$

$\Pi_A(y, z, r)$



Bob

M_k, z

$\Pi_B(M_k, z, r)$

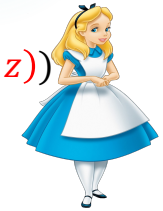


Charlie

M_k, y

$|\Pi_A^*| = |\Pi_A|$ and $|\Pi_B^*| = n_0 \cdot |\Pi_B|$

$\mathsf{F}(M, y, z) = HM(k, \mathrm{IP}(y, z))$



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

Alice

$\Pi^* = (\Pi_A^*, \Pi_B^*)$

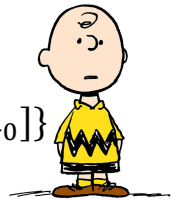
$\Pi_A^*(y, z, r)$



Bob

z

$\Pi_B^*(z, r) = \{\Pi_B(M_k, z, r) : k \in [n_0]\}$



Charlie

M_k, y

Step 2: Information from Alice



Alice

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

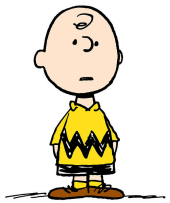
$\Pi_A^*(y,z,r)$



Bob

z

$\Pi_B^*(z,r)$



Charlie

M_k, y

Case 1:

Alice's message contains sufficient information about $\mathrm{IP}(y,z)$ such that Charlie can solve $\mathrm{HM}(\mathrm{k}, \mathrm{IP}(\mathrm{y},\mathrm{z}))$.

By the randomized one-way communication complexity of HM ,

$$|\Pi_A| = |\Pi_A^*| = \Omega(\sqrt{n_0}) = \Omega(n^{1/3})$$

$\mathrm{LHM}(\mathrm{k},\mathrm{y},\mathrm{z}) = \mathrm{HM}(\mathrm{k}, \mathrm{IP}(\mathrm{y},\mathrm{z}))$ $\quad \mathrm{IP}: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{n_0}$

Step 3: Information form Bob



Alice

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

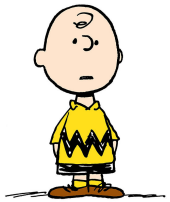
$\Pi_A^*(y, z, r)$



Bob

z

$\Pi_B^*(z, r)$

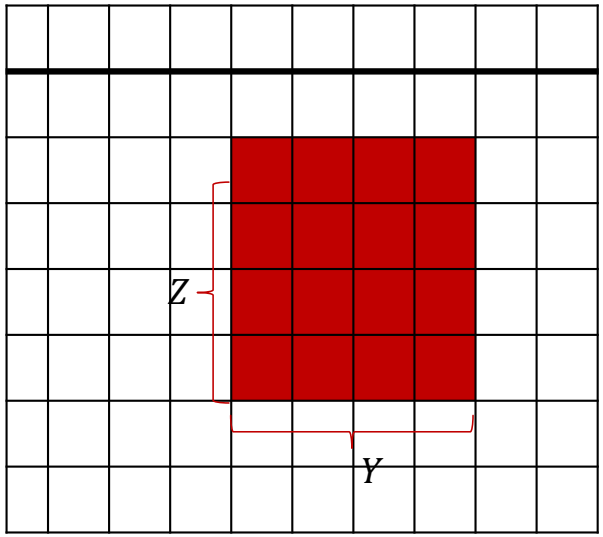


Charlie

M, y

$\mathrm{LHM}(\mathrm{k}, \mathrm{y}, \mathrm{z}) = \mathrm{HM}(\mathrm{k}, \mathrm{IP}(\mathrm{y}, \mathrm{z}))$

Case 2:
Bob sends sufficient information about z through one-way communication such that Charlie can solve $\mathrm{HM}(\mathrm{k}, \mathrm{IP}(\mathrm{y}, \mathrm{z}))$.



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

Step 3: Information form Bob



Alice

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

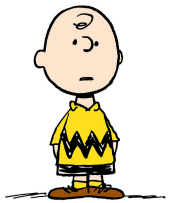
$\Pi_A^*(y, z, r)$



Bob

z

$\Pi_B^*(z, r)$



Charlie

M_k, y

$\mathrm{LHM}(\mathrm{k}, \mathrm{y}, \mathrm{z}) = \mathrm{HM}(\mathrm{k}, \mathrm{IP}(\mathrm{y}, \mathrm{z}))$

Case 2:

Bob sends sufficient information about z through one-way communication such that Charlie can solve $\mathrm{HM}(\mathrm{k}, \mathrm{IP}(\mathrm{y}, \mathrm{z}))$.

By the two-source extractor properties of IP,

$$|\Pi_B^*| = \Omega(n)$$

By the properties of Π_B^* ,

$$|\Pi_B| = \Omega\left(\frac{\Pi_B^*}{n_0}\right) = \Omega(n^{1/3})$$

Finishing the proof



Alice

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

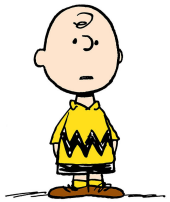
$\Pi_A^*(y, z, r)$



Bob

z

$\Pi_B^*(z, r)$



Charlie

M_k, y

$\mathrm{LHM}(k, y, z) = \mathrm{HM}(k, \mathrm{IP}(y, z))$

One of Case 1 and Case 2 must be true:

$\mathrm{ORCC}^{\mathrm{NOF}}(\mathrm{LHM}) = |\Pi_A| + |\Pi_B| = \Omega(n^{1/3})$

Open Problem

- Recently, in the joint work with Haoyu Wang and Pei Wu, we prove the first exponential quantum Advantage three-party NOF communication.

Could we prove exponential quantum advantage in k-party NOF communication ?