Quantum versus Classical Separation in Simultaneous Number-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 $O\ (\log n)$.

An important open problem [JJGL24] : Explicit separation between the randomized and quantum NOF communication

Main Theorem: The randomized simultaneous NOF communication complexity of F is $\Omega(n^{1/16})$, but the quantum simultaneous NOF communication complexity of F is $O\ (\log n)$.

Simultaneous Number-on-Forehead Communication

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

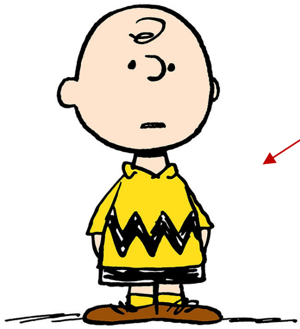
Alice
$y, z \in \{0,1\}^n$

Public Randomness $r \in \{0,1\}^*$

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

$\pi_A(y, z, r)$

$\pi_B(x, z, r)$



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

$F(x, y, z)$

Applications:
Circuit complexity [HG90, PRS97,Cha07,VW07]
Cryptography [CKGS98, BDFP17]

Simultaneous Number-on-Forehead Communication

Alice holds $y, z \in \{0,1\}^n$, Bob holds $x, z \in \{0,1\}^n$, Charlie holds $x, y \in \{0,1\}^n$, they collaborate to compute a search problem $S \subseteq X \times Y \times Z \times Q$ . .A three-party protocol Π proceeds as follows:

- Alice sends message $\Pi_A(y, z, r)$ to Charlie.
- Bob sends messages $\Pi_B(x, z, r)$ to Charlie.
- Charlie outputs a solution $q \in Q$ depends on $(\Pi_A(y, z, r), \Pi_B(x, z, r), x, y, r)$
- The protocol Π computes S with error ϵ if for any (x,y,z), $\Pr_r[(x, y, z, q) \in S] \geq 1 - \epsilon$.

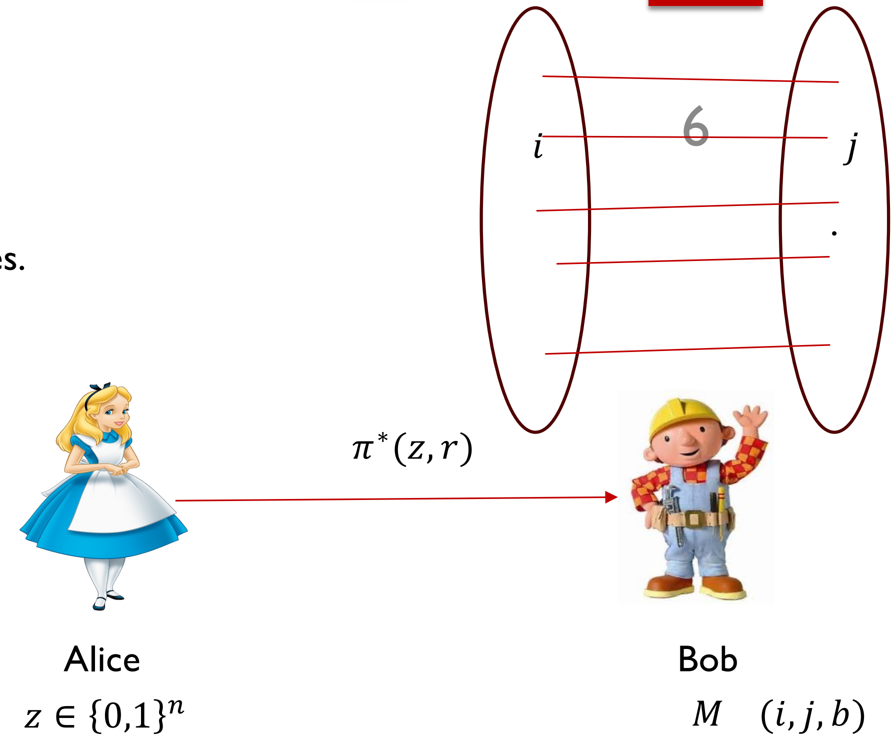
The randomized simultaneous NOF communication complexity is the maximum total length $|\Pi_A| + |\Pi_B|$ over all inputs, denoted by $\mathrm{SCC(F)}$.

Warmup:
Quantum versus Classical Separation in One-way Communication

Quantum versus Classical Separation in One-way Communication

$\mathcal{M}_n$ be the set of perfect matching in the bipartite graph over n nodes.

Hidden Matching Problem(HM)
Alice holds $z \in \{0,1\}^n$, Bob holds $\mathrm{M} \in \mathcal{M}_n$,Bob output a (i, j, b) such that (i, j) is an edge in M and $b = z_i \oplus z_j$.



Theorem 1 [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 $(\log n)$.

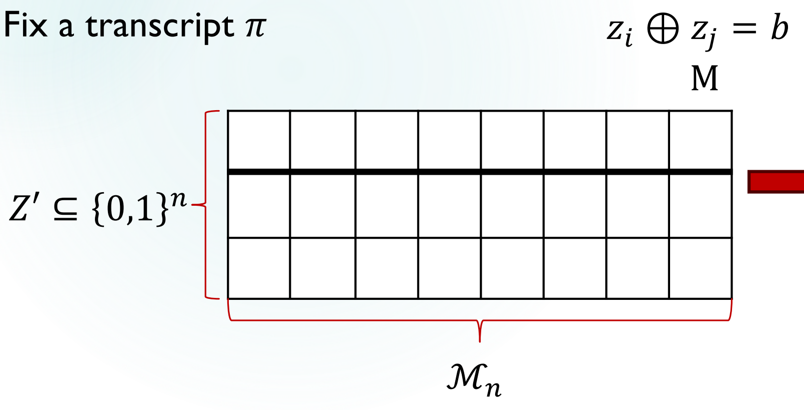
Lower bound via encoding arguments

[BYJK04]: The randomized one-way communication complexity of HM is $\Omega(n^{1/2})$.

Hidden Matching Problem(HM)

Alice holds $z \in \{0,1\}^n$, Bob holds $\mathrm{M} \in \mathcal{M}_n$. Bob output a (i, j, b) such that (i, j) is an edge in M and $b = z_i \oplus z_j$.

Fix a transcript π



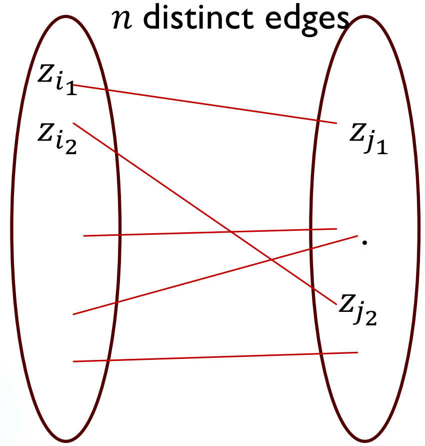
$z_{i_1} \oplus z_{j_1} = b_1$

$z_{i_2} \oplus z_{j_2} = b_2$

……..

$z_{i_n} \oplus z_{j_n} = b_n$

$m = n/2$

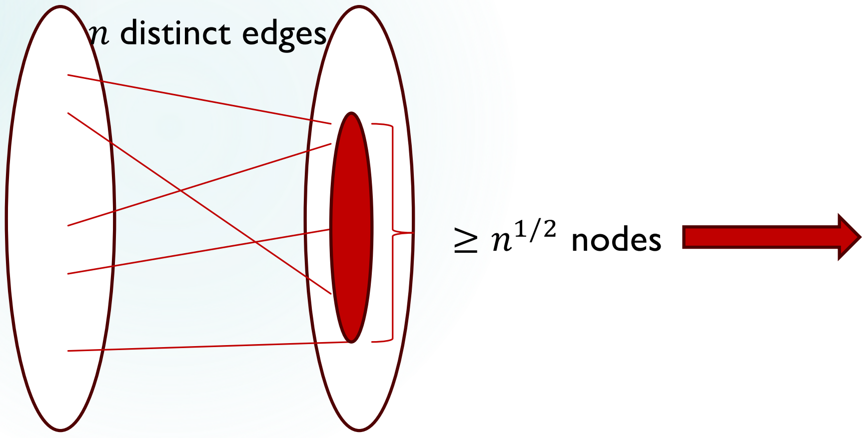


Lower bound via encoding arguments

[BYJK04]: The randomized one-way communication complexity of HM is $\Omega(n^{1/2})$.

Hidden Matching Problem(HM)

Alice holds $z \in \{0,1\}^n$, Bob holds $\mathrm{M} \in \mathcal{M}_n$. Bob output a (i, j, b) such that (i, j) is an edge in M and $b = z_i \oplus z_j$.



$H(Z) - H(Z|\pi) = \Omega(n^{1/2})$

Upper bound

[BYJK04]: The quantum one-way communication complexity of HM is $\mathrm{O}(\log n)$.

Alice sends the state

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{z_i} |i\rangle$$

Bob performs a measurement on the state $|\psi\rangle$ in the orthonormal basis

$$B = \{\frac{1}{\sqrt{2}}(|k\rangle \pm |l\rangle) | (k, l) \in M\}.$$

The probability that the outcome of the measurement is a basis state $\frac{1}{\sqrt{2}}(|k\rangle \pm |l\rangle$ is

$$\frac{1}{\sqrt{2}}(|k\rangle + |l\rangle: \quad \left|\left\langle\psi\right|\frac{1}{\sqrt{2}}(|k\rangle + |l\rangle)\right|^2 = \frac{1}{2n}\left((-1)^{x_k} + (-1)^{x_\ell}\right)^2 \qquad \frac{2}{n} \ \ if\ x_k \oplus x_\ell = 0\ and\ 0\ otherwise$$

$$\frac{1}{\sqrt{2}}(|k\rangle - |l\rangle): \quad \left|\left\langle\psi\right|\frac{1}{\sqrt{2}}(|k\rangle - |l\rangle)\right|^2 = \frac{1}{2n}\left((-1)^{x_k} - (-1)^{x_\ell}\right)^2 \qquad \frac{2}{n} \ \ if\ x_k \oplus x_\ell = 1\ and\ 0\ otherwise$$

Quantum versus Classical Separation in Simultaneous NOF Communication via lifting

Quantum versus Classical Separation

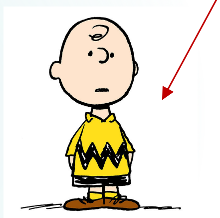
Alice

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

Bob

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

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



Charlie

$y \in T, x \in S$ $\quad$ $F(z, g(x,y))$

Let $g: T \times S \to [m]$ be a gadget function

Gadgeted Hidden Matching Problem (GHM)

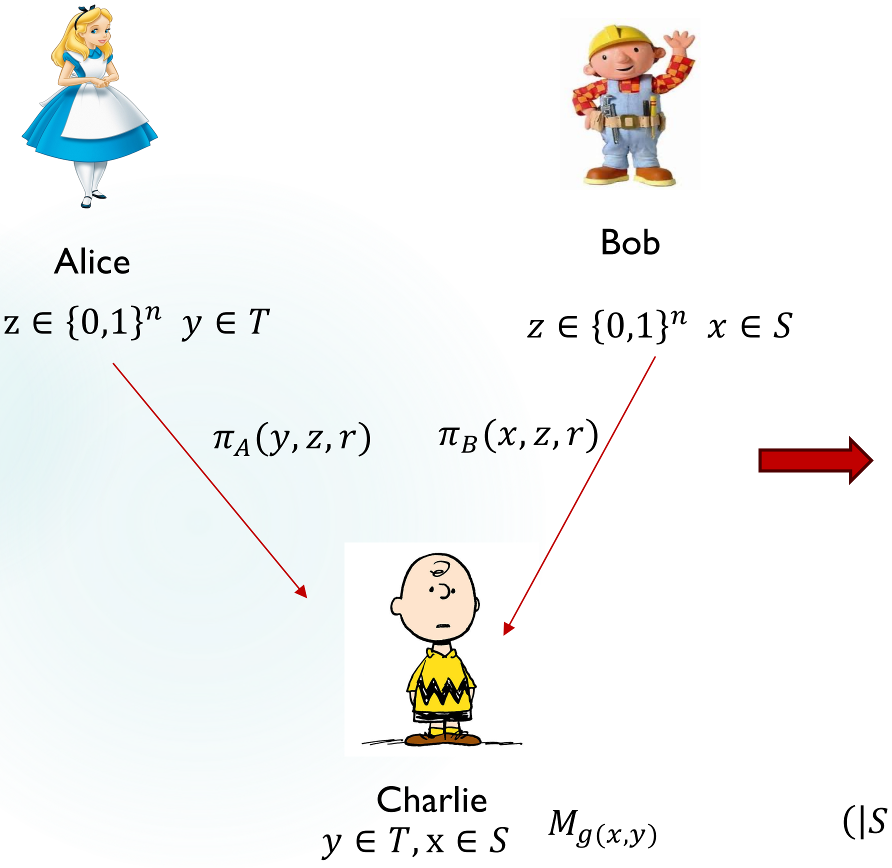
Alice holds $z \in \{0,1\}^n, y \in T$, Bob holds $z \in \{0,1\}^n, x \in S$, Charlie holds $y \in T, x \in S$. Charlie output a (i,j,b) such that (i,j) is an edge in $M_{g(x,y)}$ and $b = z_i \oplus z_j$.

Main Theorem:

The randomized simultaneous NOF communication complexity communication complexity of GHM is $\Omega(n^{1/16})$, but the quantum simultaneous NOF communication complexity communication complexity of GHM is $O(\log n)$.

Local-independence protocols

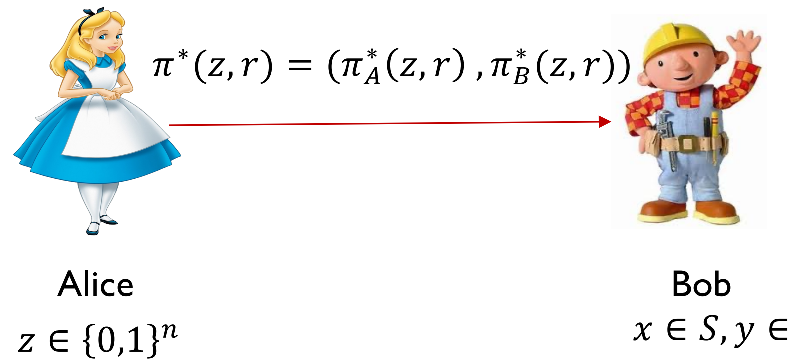
Gadgeted Hidden Matching Problem (GHM)



$$\pi_A^*(z,r) = (\pi_A(y,z,r))_{y \in T}$$

$$\pi_B^*(z,r) = (\pi_B(x,z,r))_{x \in S}$$

Lifted Hidden Matching Problem



$$M \in \mathcal{M}(S,T) = \{M_{g(x,y)} : x \in S, y \in T\}$$

$$(|S| + |T|) \cdot RCC^{NOF}(GHM) = RCC(LHM)$$

Proof via encoding arguments

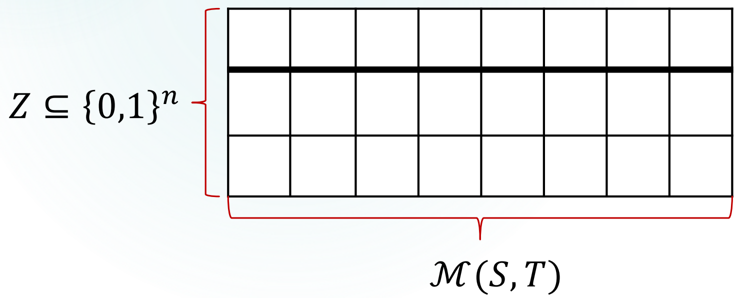
The randomized one-way communication complexity of LHM is $\Omega(n^{5/16})$.

Lifted Hidden Matching Problem (LHM)

Alice holds $z \in \{0,1\}^n$, Bob holds $\mathrm{M} \in \mathcal{M}(S,T) \subseteq \mathcal{M}_\mathrm{n}$

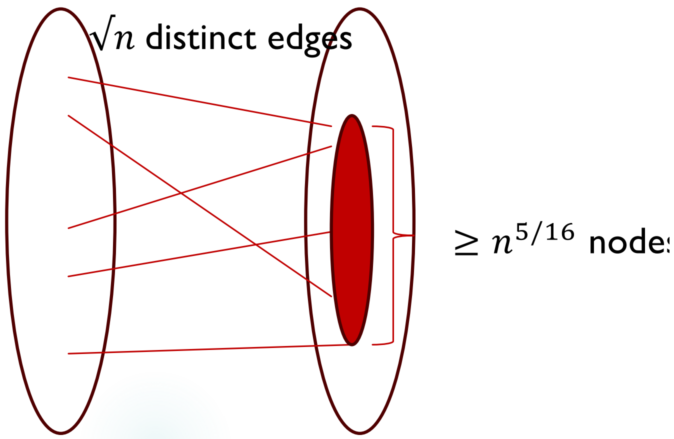
Bob output a (i,j,b) such that (i,j) is an edge in M and $b = z_i \oplus z_j$.

Fix a transcript π



Graph lemma

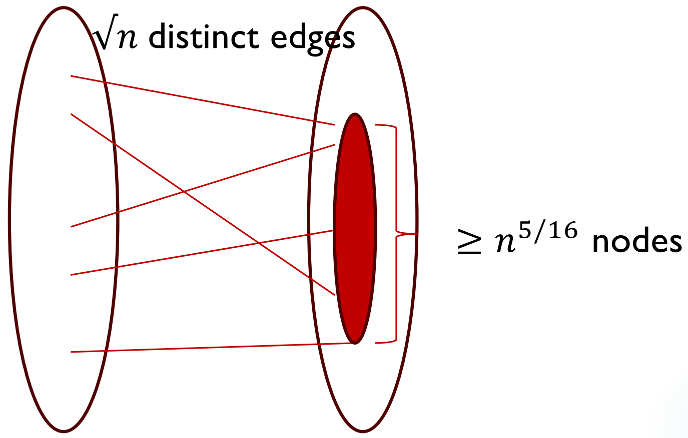
There exist S,T with $|S| = |T| = n^{1/4}$ such that



Proof of the graph lemma

By the probabilistic method

There exist S, T with $|S| = |T| = n^{1/4}$ such that



Open Problems

- An $\Omega(n^{1/2})$ vs $O(\log n)$ separation between the randomized and quantum simultaneous NOF communication

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