Randomized and Quantum Lifting for One-Way Conservative NOF Model

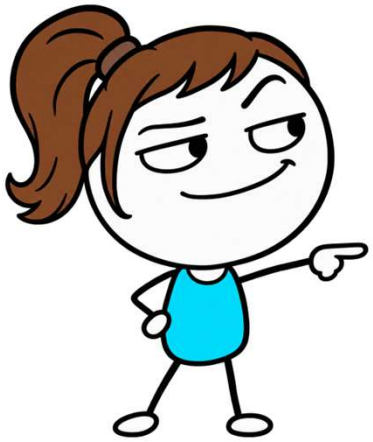
Haoyu Wang (The Pennsylvania State University)

Joint work with Pei Wu (The Pennsylvania State University)

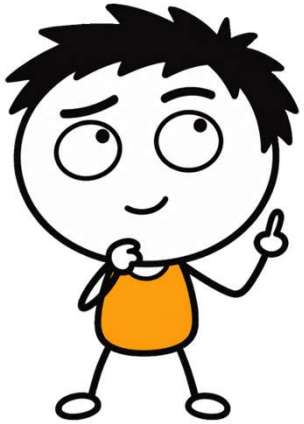
Part 1. Introduction

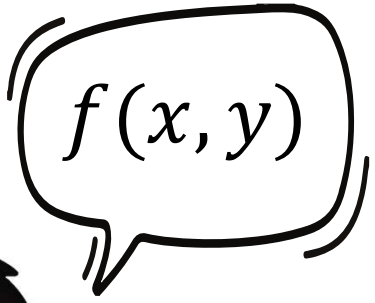
One-way 2-party model

r: public randomness



$\Pi(y, r)$: 1011011⋯





Alice: y

Bob: x

Communication complexity

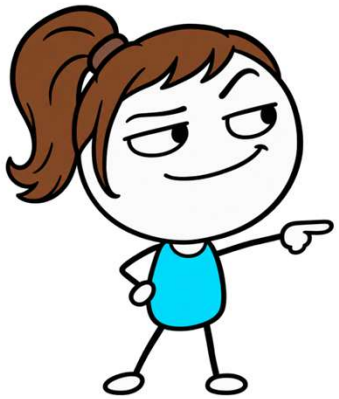
- **Cost**: the length of message $\left|\Pi(y,r)\right|$ **;**
- **Goal**: outputs $f(x,y)$ correctly with probability $\geq \frac{2}{3}$ **;**

How long must $\left|\Pi(y,r)\right|$ be?

Let $\mathrm{R}^{\rightarrow}_{2/3}(f) := \min_{\Pi} \max_{y,r} \left|\Pi(y,r)\right|$

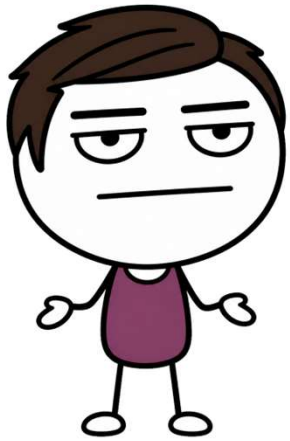
One-way NOF model

r: public randomness

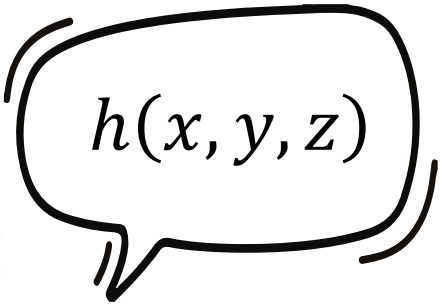


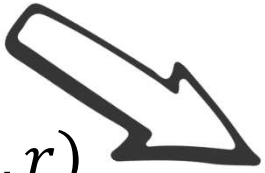
Lingling: y, z

$\Pi_{L,S}(y,z,r)$

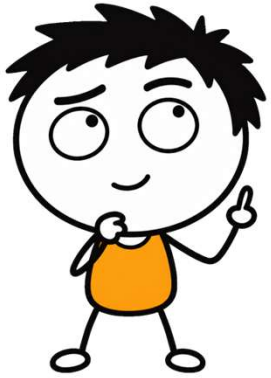


Sam: x, y

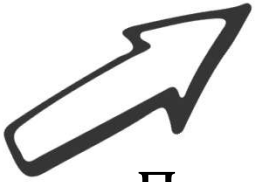




$\Pi_{L,D}(y,z,r)$



Daming: x, z



$\Pi_{D,S}(x,z,r)$

Why we study one-way NOF model?

- **Circuit lower bounds**: Small shallow circuits induce low-cost one-way NOF protocols. ----[Håstad–Goldmann, FOCS1990]; [Beigel–Tarui, Comput. Complex.1994];

- **Additive combinatorics**: NOF lower bounds are directly tied to progression-free sets, corners, and Ruzsa–Szemerédi graphs. Progress flows both ways. ----[Linial–Pitassi–Shraibman, ITCS2019]; [Linial–Shraibman, CCC2021]; [Jaber et al., FOCS2025];

Why we study one-way NOF model?

- **Pseudorandomness**: Small-space distinguishers induce low-cost NOF protocols. ----[Babai–Nisan–Szegedy, STOC1989]; [Ganor–Raz, RANDOM2014];

- **Cryptography**: indistinguishability in NOF model powers leakage-resilient cryptography. ----[Kumar–Meka–Sahai, FOCS2019]; [Li–Ma–Quach–Wichs, CRYPTO2020]

- **Applications**: Streaming algorithms; Distributed computing; [Kallaugher et al., PODS2019]; [Drucker–Kuhn–Oshman, PODC2014]

Why we study one-way NOF model?

- **Quantum advantage**: randomized one-way NOF lower bounds on certain quantum-friendly function can show quantum advantage;

Open problem: prove strong lower bounds of one-way NOF model.

Research History (one-way NOF, to name a few)

- [Viola–Wigderson, FOCS 2007]: $\mathrm{Poly}(n)$ randomized lower bounds for one-way pointer jumping and DISJ.
- [Jain–Klauck–Nayak, STOC 2008]: $\Omega\left(\sqrt{n}\right)$ for randomized 3-party one-way DISJ.
- [Gavinsky–Pudlák, CCC 2008]: $n^{\Omega\left(1/k^2\right)}$ randomized lower bound for an one-way NOF search problem; exponential quantum advantage.
- **[Yang–Zhang, preprint 2025]**: A generic **deterministic lifting** theorem.
- **[Yang–Zhang, FOCS 2026]**: A **lifted** search problem requires $\Omega\left(n^{1/3}/2^k\right)$ randomized lower bound; exponential quantum advantage.

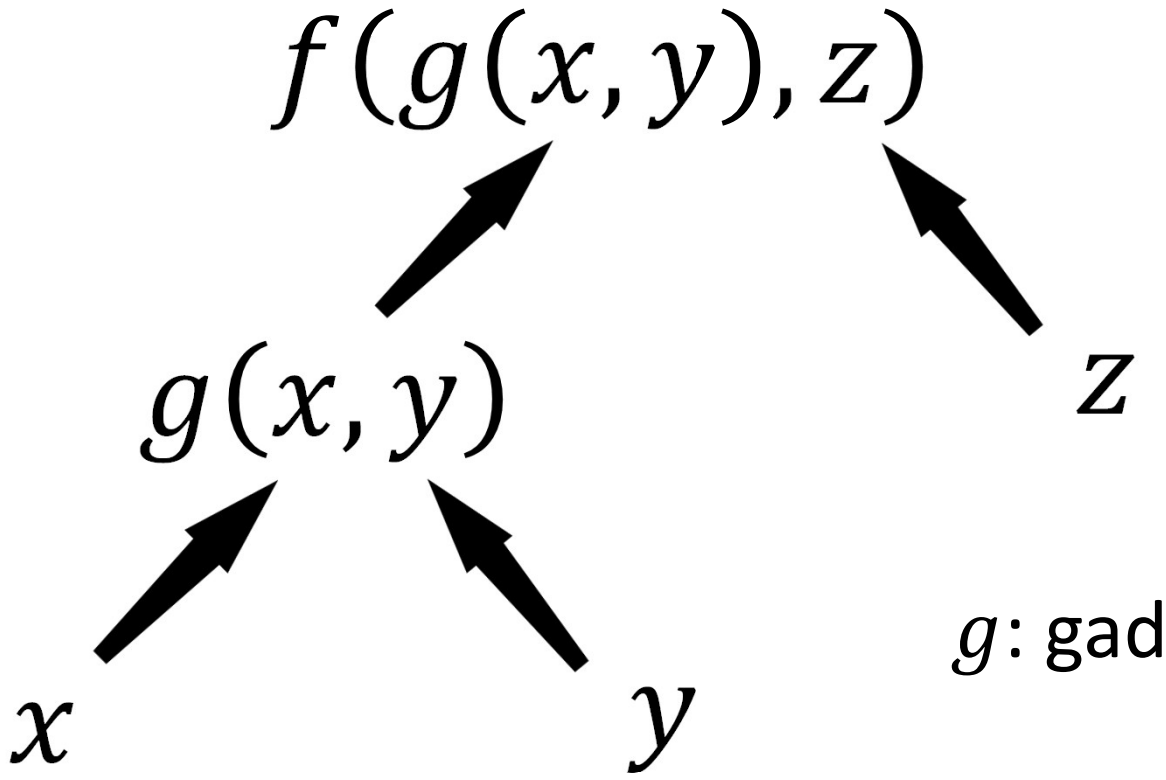
Part 2. Randomized lifting theorem

Why randomized NOF lower bound is hard?

- Players' views are highly correlated.
- Hitting (deterministic) vs. Mixing (randomized).
- Generic discrepancy/norm methods lower bound **quantum** and **randomized** models **simultaneously**. ----[Lee–Schechtman–Shraibman, CCC 2009]; [Sherstov, STOC 2013];

Lifting: transfer lower bounds from a simpler model to a richer one.

Lifted function: from 2-party f to 3-party $f \circ g$



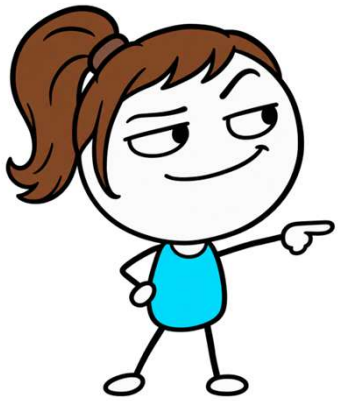
g: gadget function

A moderate restriction: **terminal-conservative**

The final player′s view:

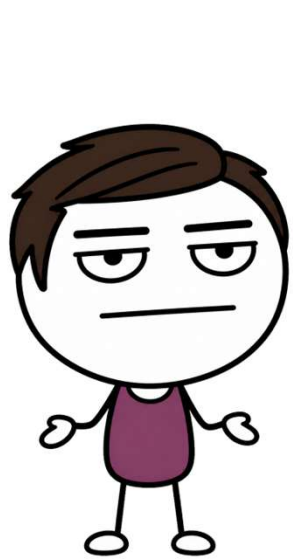
$g(x, y)$ vs. x, y

One-way conservative NOF model



Lingling: y, z

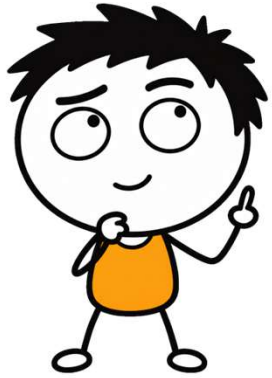
$\Pi_{L,S}(y, z, r)$



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

Sam: $g(x, y)$

$\Pi_{L,D}(y, z, r)$



Daming: x, z

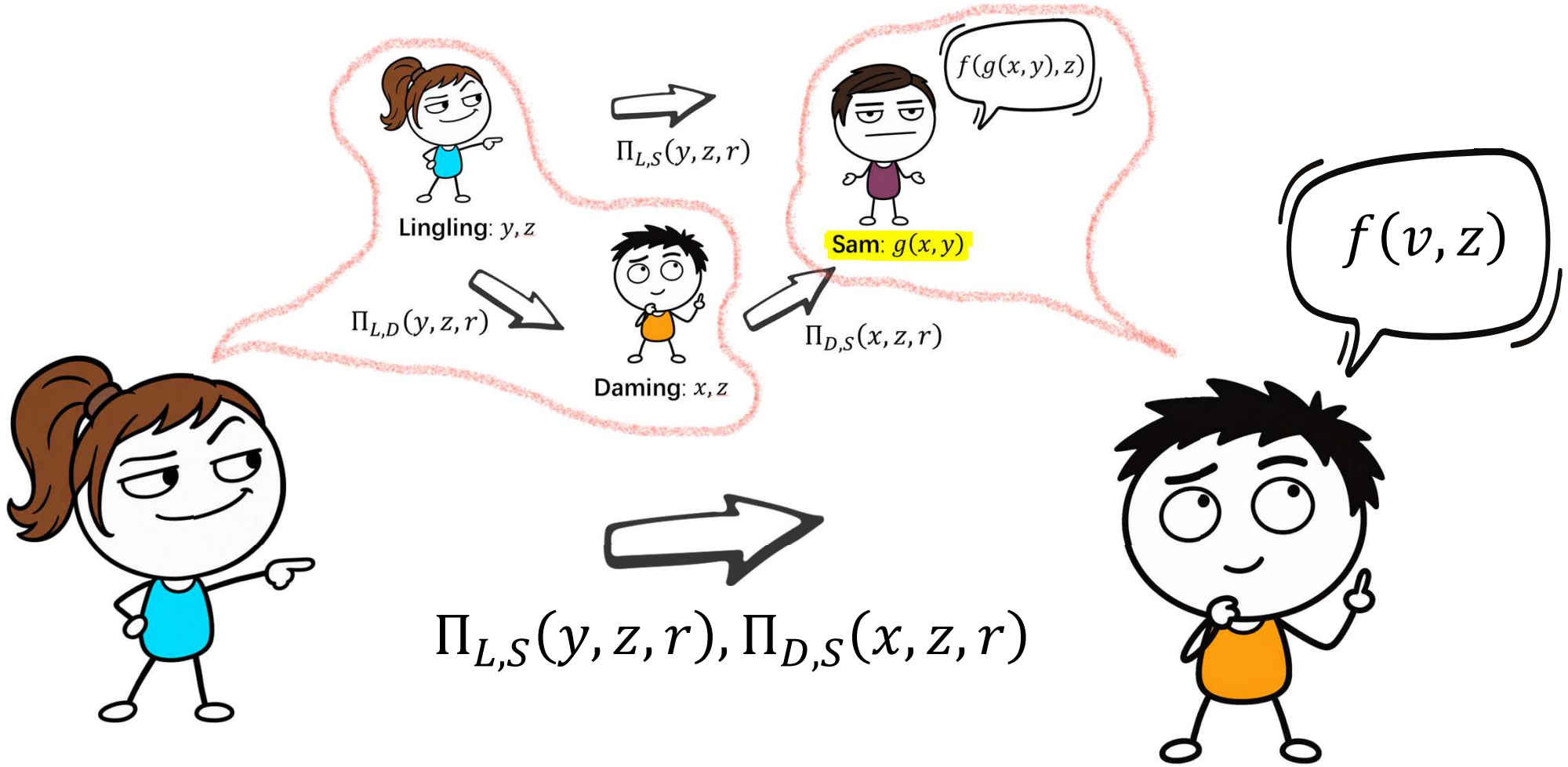
$\Pi_{D,S}(x, z, r)$

Inner Product: $\mathrm{IP}_{q,r}(x,y) = \sum_{i=1}^{r} x_i\, y_i \mod q$

Let $f \circ \mathrm{IP}_{q,r}(x,y,z) := f\left(\mathrm{IP}_{q,r}(x,y), z\right)$

Our result: $\forall f,\ \mathrm{R}_{2/3}^{\mathrm{cons},\rightarrow}\left(f \circ \mathrm{IP}_{q,r}\right) \geq\ \Omega\left(\mathrm{R}_{2/3}^{\rightarrow}(f)\right)$

Idea: each one-way conservative NOF protocol induces a one-way 2-party protocol;



Alice: z;
sample x, y uniformly;

Bob: v; takes $g(x,y)$ as v , and outputs the same answer as **Sam**;

Proof Sketch:

- True transcript $\Pi_{z,r}^{true}(x,y)$: (x,y) is uniform random with $g(x,y)=v$;
- Alice's simulation $\Pi_{z,r}^{sim}(x,y)$: (x,y) is uniform random in the whole universe;
- The pseudo-randomness of $g:=\mathrm{IP}_{q,r}$ guarantees $\Pi_{z,r}^{true}(x,y)\approx\Pi_{z,r}^{sim}(x,y)$;
- By the similar transcript and the same decoder, Bob only suffers a small loss on successful probability.

Corollary (exponential quantum advantage):
There exists a **Boolean function** F such that

$$\mathrm{R}_{2/3}^{\mathrm{cons},\rightarrow}(F) = \Omega\left(\sqrt{n}\right)$$

vs.

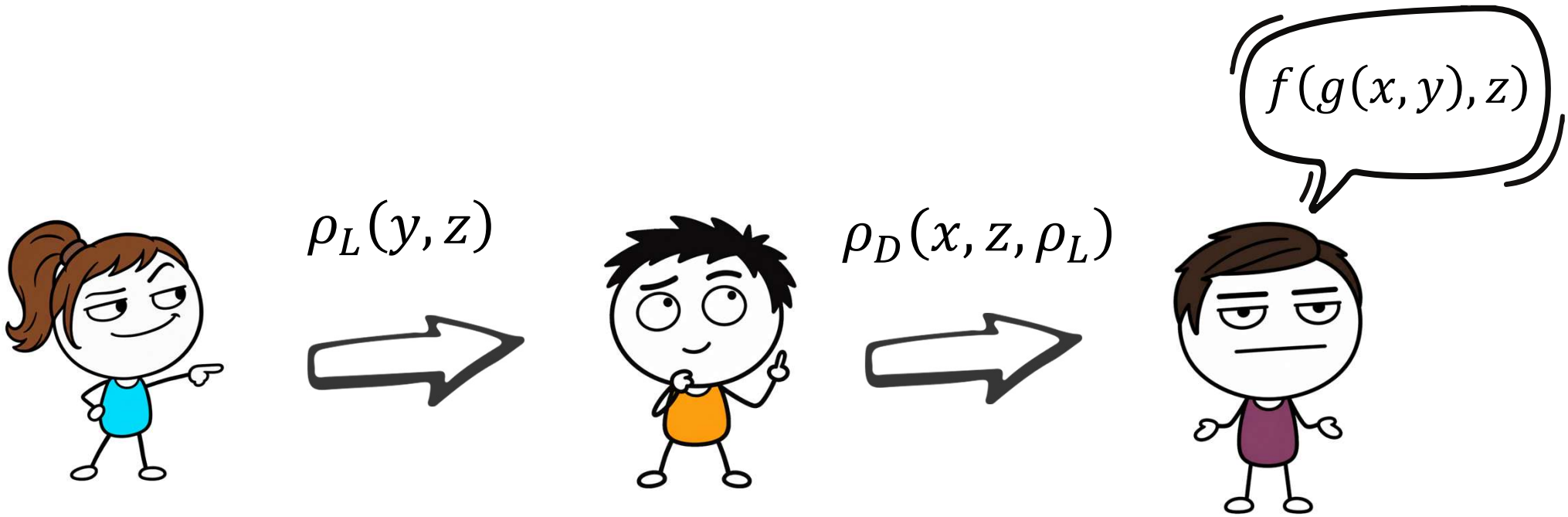
$$\mathrm{Q}_{2/3}^{\mathrm{cons},\rightarrow}(F) = \mathrm{O}(\log n)$$

Quantum advantage (to name a few)

Reference	Model	Problem type
[Bar-Yossef–Jayram–Kerenidis, STOC 2004]	One-way 2-party	Search problem
[Gavinsky et al., STOC 2007]	One-way 2-party	Boolean function
[Gavinsky–Pudlák, CCC 2008]	One-way non-interactive NOF	Search problem
[Yang–Zhang, FOCS 2026]	One-way NOF	Search problem
Ours	One-way conservative NOF	Boolean function

Part 3. Quantum lifting theorem.

Quantum one-way conservative NOF model



Linling: y, z **Daming**: x, z **Sam**: $g(x, y)$

Sam measures the state $\rho_D(x, z, \rho_L)$ and outputs the answer.

Our result: $\forall f,\ \mathrm{Q}_{2/3}^{\mathrm{cons},\rightarrow}\left(f \circ \mathrm{IP}_{q,r}\right) \geq\ \Omega\left(\mathrm{Q}_{2/3}^{\rightarrow}(f)\right)$

- Follows by the same protocol simulation idea;
- **Quantum upgrade**: the gadget $\mathrm{IP}_{q,r}$ fools the entire final quantum state—not just a classical transcript—so conditioning on $g(x, y) = v$ barely changes Sam's measurement.
- New toolkit for quantum communication complexity;

Open questions

- Build randomized lifting for the **one-way NOF model**. (originally raised by [Yang–Zhang, preprint 2025])

- **Better explicit gadgets**: improve the dependency on k (number of parties) from $1/2^k$ (Inner product, ours) to $1/\mathrm{poly}(k)$ (random gadgets).

- **Entanglement-assisted model**: can we build analogous quantum lifting theorem when players share entanglement.

- **Interactive/multi-pass** lifting theorems for more general NOF model.

Merci de votre attention !