On Quantum vs. Classical Communication Complexity

Dmitry Gavinsky

Institute of Mathematics, Praha
Czech Academy of Sciences
The setting of communication complexity is one of the strongest computational models, as of today, where people have tools to prove “hardness”.

This can be used to compare the computational power of two communication regimes via demonstrating a problem that has an efficient solution in one regime, but not in the other.

Many researchers have applied this methodology to argue qualitative advantage of quantum over classical communication models; this talk aims to survey some old and new results.
One-way communication

Alice receives $X$ and Bob receives $Y$. Alice sends a message to Bob. Bob outputs the answer to the input ($X$, $Y$).
One-way communication

- Alice receives $X$ and Bob receives $Y$.
- Alice sends a message to Bob.
- Bob outputs the answer to the input $(X, Y)$. 
Two-way communication

- Alice receives $X$ and Bob receives $Y$.
- They speak.
- Bob outputs the answer to the input $(X, Y)$. 

![Diagram showing two-way communication between Alice and Bob](image)
Simultaneous message passing (SMP)

- Alice receives $X$ and Bob receives $Y$.
- Alice and Bob send one message each to the referee.
- The referee outputs the answer to the input $(X, Y)$. 
Randomised and quantum communication complexity

Communication protocols that use randomness are *randomised*, and those that send qubits are *quantum*. 
Randomised and quantum communication complexity

- Communication protocols that use randomness are *randomised*, and those that send qubits are *quantum*.
- The cost of a communication protocol is the total number of bits/qubits that all its participants send.
Randomised and quantum communication complexity

- Communication protocols that use randomness are \textit{randomised}, and those that send qubits are \textit{quantum}.

- The cost of a communication protocol is the total number of bits/qubits that all its participants send.

- The complexity of a problem in a given communication model is the minimum cost of a protocol that produces a correct answer with high probability.
Randomised and quantum communication complexity

- Communication protocols that use randomness are *randomised*, and those that send qubits are *quantum*.
- The cost of a communication protocol is the total number of bits/qubits that all its participants send.
- The complexity of a problem in a given communication model is the minimum cost of a protocol that produces a correct answer with high probability.
- The communication complexity class corresponding to a communication model is the family of problems with at most poly-logarithmic complexity in that model.
Shared randomness and shared entanglement

- All communication models that we have seen can be “augmented” by allowing Alice and Bob (but *not the referee*) to use shared randomness, or even shared entanglement.
Shared randomness and shared entanglement

- All communication models that we have seen can be “augmented” by allowing Alice and Bob (but *not the referee*) to use shared randomness, or even shared entanglement.

- Shared randomness matters only in the SMP regime, as $O(\log n)$ shared random bits are always sufficient.
Shared randomness and shared entanglement

- All communication models that we have seen can be “augmented” by allowing Alice and Bob (but not the referee) to use shared randomness, or even shared entanglement.

- Shared randomness matters only in the SMP regime, as $O(\log n)$ shared random bits are always sufficient.

- We do not have, as of today, any meaningful upper bound on the amount of entanglement that can be required for an efficient communication protocol to exist. Accordingly, shared entanglement can, potentially, enrich any quantum model.
Shared randomness and shared entanglement

- All communication models that we have seen can be “augmented” by allowing Alice and Bob (but not the referee) to use shared randomness, or even shared entanglement.

- Shared randomness matters only in the SMP regime, as $O(\log n)$ shared random bits are always sufficient.

- We do not have, as of today, any meaningful upper bound on the amount of entanglement that can be required for an efficient communication protocol to exist. Accordingly, shared entanglement can, potentially, enrich any quantum model.

- One can consider classical communication models with shared entanglement, which can be interesting only in the case of SMP (as otherwise teleportation can “emulate” quantum communication). As well, one may consider the quantum SMP model with shared randomness.
Separating communication complexity classes via total functions, partial functions and relations

- Separating two classes via a problem that is a total function is the “strongest” evidence of their difference.
- Separating via a partial function is “less convincing”.
- Separating via a relation is the “weakest”.

There are known cases where a quantum communication complexity class can be separated from a classical one via a relation, while a functional separation is impossible. There are “conjectured cases” where a quantum class can be separated from a classical one via a partial function, but not via a total one.
Separating communication complexity classes via total functions, partial functions and relations

- Separating two classes via a problem that is a total functions is the “strongest” evidence of their difference. Separating via a partial function is “less convincing”. Separating via a relation is the “weakest”.
- There are known cases where a quantum communication complexity class can be separated from a classical one via a relation, while a functional separation is impossible.
Separating communication complexity classes via total functions, partial functions and relations

- Separating two classes via a problem that is a total functions is the “strongest” evidence of their difference. Separating via a partial function is “less convincing”. Separating via a relation is the “weakest”.

- There are known cases where a quantum communication complexity class can be separated from a classical one via a relation, while a functional separation is impossible.

- There are “conjectured cases” where a quantum class can be separated from a classical one via a partial function, but not via a total one.
Some known examples of quantum advantage

(please note the notation)
Some known examples of quantum advantage
(please note the notation)

- **Q vs. R**: In 1999 Raz demonstrated a *partial function* that had an efficient quantum two-way protocol, but no classical two-way protocol.
Some known examples of quantum advantage

(please note the notation)

- **Q vs. R**: In 1999 Raz demonstrated a *partial function* that had an efficient quantum two-way protocol, but no classical two-way protocol.

- **Q∥ vs. R∥**: In 2001 Buhrman, Cleve, Watrous and de Wolf showed that a *total function* had an efficient quantum SMP-protocol, but no classical SMP-protocol (without shared randomness).
Some known examples of quantum advantage

(please note the notation)

- $Q$ vs. $R$: In 1999 Raz demonstrated a partial function that had an efficient quantum two-way protocol, but no classical two-way protocol.
- $Q^\parallel$ vs. $R^\parallel$: In 2001 Buhrman, Cleve, Watrous and de Wolf showed that a total function had an efficient quantum SMP-protocol, but no classical SMP-protocol (without shared randomness).
- $Q^1$ vs. $R^1$: In 2004 Bar-Yossef, Jayram and Kerenidis demonstrated a relation that had an efficient quantum one-way communication protocol, but no classical one-way protocol.
Some known examples of quantum advantage

(please note the notation)

- **Q vs. R**: In 1999 Raz demonstrated a *partial function* that had an efficient quantum two-way protocol, but no classical two-way protocol.

- **Q\| vs. R\|**: In 2001 Buhrman, Cleve, Watrous and de Wolf showed that a *total function* had an efficient quantum SMP-protocol, but no classical SMP-protocol (without shared randomness).

- **Q\^[1] vs. R\^[1]**: In 2004 Bar-Yossef, Jayram and Kerenidis demonstrated a *relation* that had an efficient quantum one-way communication protocol, but no classical one-way protocol.

- **Q\^[1] vs. R\^[1]**: In 2008 in a joint work with Kempe, Kerenidis, Raz and de Wolf the same separation has been demonstrated via a *partial function*. 
Some known examples of quantum advantage
(please note the notation)

- **Q vs. R**: In 1999 Raz demonstrated a *partial function* that had an efficient quantum two-way protocol, but no classical two-way protocol.
- **Q∥ vs. R∥**: In 2001 Buhrman, Cleve, Watrous and de Wolf showed that a *total function* had an efficient quantum SMP-protocol, but no classical SMP-protocol (without shared randomness).
- **Q1 vs. R1**: In 2004 Bar-Yossef, Jayram and Kerenidis demonstrated a *relation* that had an efficient quantum one-way communication protocol, but no classical one-way protocol.
- **Q1 vs. R1**: In 2008 in a joint work with Kempe, Kerenidis, Raz and de Wolf the same separation has been demonstrated via a *partial function*.
- **Q1 vs. R**: In 2010 Klartag and Regev showed a *partial function* with an efficient quantum one-way protocol, but no classical two-way protocol.
Some known examples of quantum advantage
(please note the notation)

- **Q vs. R**: In 1999 Raz demonstrated a *partial function* that had an efficient quantum two-way protocol, but no classical two-way protocol.
- **Q∥ vs. R∥**: In 2001 Buhrman, Cleve, Watrous and de Wolf showed that a *total function* had an efficient quantum SMP-protocol, but no classical SMP-protocol (without shared randomness).
- **Q1 vs. R1**: In 2004 Bar-Yossef, Jayram and Kerenidis demonstrated a *relation* that had an efficient quantum one-way communication protocol, but no classical one-way protocol.
- **Q1 vs. R1**: In 2008 in a joint work with Kempe, Kerenidis, Raz and de Wolf the same separation has been demonstrated via a *partial function*.
- **Q1 vs. R**: In 2010 Klartag and Regev showed a *partial function* with an efficient quantum one-way protocol, but no classical two-way protocol.
- **Q∥,ent vs. R**: In 2016 a *partial function* has been demonstrated that had an efficient quantum SMP-protocol with entanglement, but no classical two-way protocol.
Barely-possible quantum protocols

To separate between $Q$ and $R$, a "complete" function for quantum 2-round protocols has been used. To demonstrate the advantage of $Q$ over $R$, a complete function for quantum 1-way protocols has been used. I.e., all functional separations "against $R$", except for the "$Q \parallel_{ent} vs. R" result, have been obtained via "barely-possible quantum protocols". It is not clear whether $Q \parallel_{ent}$ (or any of its "augmented" modifications) has a complete function.
Barely-possible quantum protocols

To separate between $Q$ and $R$, a “complete” function for quantum 2-round protocols has been used.
Barely-possible quantum protocols

- To separate between $Q$ and $R$, a “complete” function for quantum 2-round protocols has been used.
- To demonstrate the advantage of $Q^1$ over $R$, a complete function for quantum 1-way protocols has been used.
Barely-possible quantum protocols

- To separate between $Q$ and $R$, a “complete” function for quantum 2-round protocols has been used.
- To demonstrate the advantage of $Q^I$ over $R$, a complete function for quantum 1-way protocols has been used.
- I.e., all functional separations “against $R$”, except for the “$Q^\parallel,\text{ent}$ vs. $R$” result, have been obtained via “barely-possible quantum protocols”. It is not clear whether $Q^\parallel$ (or any of its “augmented” modifications) has a complete function.
### The separating objects

<table>
<thead>
<tr>
<th></th>
<th>Nearly-possible for classical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nearly-manageable by the classical model</td>
<td></td>
</tr>
</tbody>
</table>
Nearly-manageable by the classical model

- To separate between $Q^\parallel$ and $R^\parallel$, the equality function has been used.
Nearly-manageable by the classical model

- To separate between $Q \parallel$ and $\mathcal{R} \parallel$, the *equality function* has been used.
- In a recent joint work with Bavarian and Ito it has been shown that the equality function was the weakest communication problem that could be solved efficiently in $\mathcal{R} \parallel^{pub}$ but not in $\mathcal{R} \parallel$. 
Nearly-manageable by the classical model

- To separate between $Q\parallel$ and $R\parallel$, the equality function has been used.
- In a recent joint work with Bavarian and Ito it has been shown that the equality function was the weakest communication problem that could be solved efficiently in $R\parallel,\text{pub}$ but not in $R\parallel$.
- That is, the choice of the equality function for the above separation can be justified (retroactively) as taking one of the weakest problems that can be solved efficiently in $R\parallel,\text{pub}$ – a class that is “slightly above” $R\parallel$ – but not in $R\parallel$ itself.
The separating objects | “Parity-inspired” problems

Separations via “parity-inspired” problems
Separations via “parity-inspired” problems

* To separate between $Q^1$ and $R^1$, the hidden matching (HM) relation has been used:

HM Alice receives $X \in \{0, 1\}^n$; Bob receives one of $n/2$ “canonical” perfect matchings on $[n]$; a valid answer is $(t, X_i \oplus X_j)$, where $(i, j)$ is the $t$’th edge in Bob’s matching.

Possible answer: $(n/2-1, 1)$
Separations via “parity-inspired” problems

- To separate between $Q^1$ and $R^1$, the hidden matching (HM) relation has been used:

  **HM** Alice receives $X \in \{0, 1\}^n$; Bob receives one of $n/2$ “canonical” perfect matchings on $[n]$; a valid answer is $(t, X_i \oplus X_j)$, where $(i, j)$ is the $t$’th edge in Bob’s matching.

- To do the same via a (partial) function, several natural “functional versions” of HM can be used, e.g., this one:
  
  Alice receives $X \in \{0, 1\}^n$, Bob receives a matching and $Z \in \{0, 1\}^\lfloor n/2 \rfloor$. Is “$(t, Z_t)$” for $t \Subset \lceil n/2 \rceil$ likely to be a valid answer to HM?
Separations via “parity-inspired” problems

- To separate between $Q^1$ and $R^1$, the hidden matching (HM) relation has been used:

  **HM** Alice receives $X \in \{0, 1\}^n$; Bob receives one of $n/2$ “canonical” perfect matchings on $[n]$; a valid answer is $(t, X_i \oplus X_j)$, where $(i, j)$ is the $t$’th edge in Bob’s matching.

- To do the same via a (partial) function, several natural “functional versions” of HM can be used, e.g., this one:

  Alice receives $X \in \{0, 1\}^n$, Bob receives a matching and $Z \in \{0, 1\}^{n/2}$. Is “$(t, Z_t)$” for $t \in [n/2]$ likely to be a valid answer to HM?

- The gapped folded Hamming distance (GFHD) function, that has been used to demonstrate the advantage of $Q^\parallel, \text{ent}$ over $R$ can be viewed as “gluing together” two (functional) instances of HM:
To separate between $Q^1$ and $R^1$, the hidden matching (HM) relation has been used:

**HM** Alice receives $X \in \{0, 1\}^n$; Bob receives one of $n/2$ “canonical” perfect matchings on $[n]$; a valid answer is $(t, X_i \oplus X_j)$, where $(i, j)$ is the $t$’th edge in Bob’s matching.

To do the same via a (partial) function, several natural “functional versions” of HM can be used, e.g., this one:

Alice receives $X \in \{0, 1\}^n$, Bob receives a matching and $Z \in \{0, 1\}^{n/2}$. Is “$(t, Z_t)$” for $t \in \lceil n/2 \rceil$ likely to be a valid answer to HM?

The gapped folded Hamming distance (GFHD) function, that has been used to demonstrate the advantage of $Q||^{ent}$ over $R$ can be viewed as “gluing together” two (functional) instances of HM:

**GFHD** Alice receives $X \in \{0, 1\}^n$; Bob receives $Y \in \{0, 1\}^n$. Is there a canonical matching, with respect to which and $t \in \lceil n/2 \rceil$ the $t$’th valid answer to the instance of HM given by $X$ is likely to be also a valid answer to the instance of HM given by $Y$?
**GFHD** – a partial function easy for $Q\parallel,^{\text{ent}}$ and hard for $R$

- Recall the previous definition of GFHD:

  Alice receives $X \in \{0, 1\}^n$; Bob receives $Y \in \{0, 1\}^n$. Is there a canonical matching, with respect to which and $t \in [n/2]$ the $t'$th valid answer to the instance of $HM$ given by $X$ is likely to be also a valid answer to the instance of $HM$ given by $Y$?
**GFHD** – a partial function easy for \( Q^{\|,\text{ent}} \) and hard for \( R \)

- Recall the previous definition of **GFHD**:
  - Alice receives \( X \in \{0, 1\}^n \); Bob receives \( Y \in \{0, 1\}^n \). Is there a canonical matching, with respect to which and \( t \in [n/2] \) the \( t \)’th valid answer to the instance of **HM** given by \( X \) is likely to be also a valid answer to the instance of **HM** given by \( Y \)?
  - The \( n/2 \) canonical matchings are
    
    \[(1, n/2 + 1 + \ell), \ldots, (n/2, n/2 + \ell)\]

    for \( 0 \leq \ell < n/2 \).
**GFHD** – a partial function easy for $Q_{\parallel,\text{ent}}$ and hard for $R$

- Recall the previous definition of GFHD:

  Alice receives $X \in \{0,1\}^n$; Bob receives $Y \in \{0,1\}^n$. Is there a canonical matching, with respect to which and $t \in [n/2]$ the $t$'th valid answer to the instance of $HM$ given by $X$ is likely to be also a valid answer to the instance of $HM$ given by $Y$?

- The $n/2$ canonical matchings are

  $$(1, n/2 + 1 + \ell), \ldots, (n/2, n/2 + \ell)$$

  for $0 \leq \ell < n/2$.

- The definition of GFHD can be reformulated (up to $n \leftrightarrow 2n$) as

  Alice receives $X_1, X_2 \in \{0,1\}^n$; Bob receives $Y_1, Y_2 \in \{0,1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \mathbf{0}$?

  Here $\sigma_\ell(w)$ is the $\ell$'th rotation of $w$ (also known as $\ell$-bit cyclic shift), which is the bit-string $w_{1-\ell} w_{2-\ell} \ldots$ (the indices are modulo $m$).
**GFHD** is *easy for* $Q^\parallel,_{\text{ent}}$

**GFHD** Alice receives $X_1, X_2 \in \{0, 1\}^n$; Bob receives $Y_1, Y_2 \in \{0, 1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \bar{0}$?
**GFHD is easy for $Q\parallel,\text{ent}$**

**GFHD** Alice receives $X_1, X_2 \in \{0, 1\}^n$; Bob receives $Y_1, Y_2 \in \{0, 1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \vec{0}$?

- If we fix $\ell_0 \in [n]$, a simple protocol can check whether $X_1 \oplus \sigma_{\ell_0}(X_2) \oplus Y_1 \oplus \sigma_{\ell_0}(Y_2) \approx \vec{0}$:

  $$\sum_{j=1}^n |j\rangle\langle j| \text{ players} \quad \Rightarrow \quad \sum_{j=1}^n (-1)^{X_1(j) + Y_1(j)} |j\rangle\langle j| \text{ referee} \quad \Rightarrow \quad \sum_{j=1}^n (-1)^{X_1(j) + Y_1(j)} |j\rangle\langle j|$$

  $$\sum_{k=1}^n |k\rangle\langle k| \quad \Rightarrow \quad \sum_{k=1}^n (-1)^{X_2(k) + Y_2(k)} |k\rangle\langle k| \quad \Rightarrow \quad \sum_{k=1}^n (-1)^{X_2(\sigma_{\ell_0}(k)) + Y_2(\sigma_{\ell_0}(k))} |k\rangle\langle k|$$

  and the inner product between the two registers held by the referee is

  $$1 - \frac{2}{n} \cdot |X_1 \oplus \sigma_{\ell_0}(X_2) \oplus Y_1 \oplus \sigma_{\ell_0}(Y_2)|_H.$$
**GFHD is easy for $Q^\parallel,\text{ent}$**

**GFHD** Alice receives $X_1, X_2 \in \{0, 1\}^n$; Bob receives $Y_1, Y_2 \in \{0, 1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \vec{0}$?

- If we fix $\ell_0 \in [n]$, a simple protocol can check whether $X_1 \oplus \sigma_{\ell_0}(X_2) \oplus Y_1 \oplus \sigma_{\ell_0}(Y_2) \approx \vec{0}$:

\[
\sum_{j=1}^{n} |j\rangle|j\rangle \quad \text{players} \quad \sum_{j=1}^{n} (-1)^{X_1(j)+Y_1(j)} |j\rangle|j\rangle \quad \text{referee} \quad \sum_{j=1}^{n} (-1)^{X_1(j)+Y_1(j)} |j\rangle|j\rangle \quad \sum_{k=1}^{n} (-1)^{X_2(\sigma_{\ell_0}(k)) + Y_2(\sigma_{\ell_0}(k))} |k\rangle|k\rangle,
\]

and the inner product between the two registers held by the referee is

\[
1 - \frac{2}{n} \cdot |X_1 \oplus \sigma_{\ell_0}(X_2) \oplus Y_1 \oplus \sigma_{\ell_0}(Y_2)|_H.
\]

- Bringing the error of the above procedure down to $\varepsilon/n$ and repeating it (via quantum “un-computing”) for all $\ell_0 \in [n]$ gives a $Q^\parallel,\text{ent}$-protocol of cost $O(\log^2 n)$ that solves $GFHD$ with error probability less than $\varepsilon$.  

---
**GFHD is hard for \( R \)**

**GFHD** Alice receives \( X_1, X_2 \in \{0, 1\}^n \); Bob receives \( Y_1, Y_2 \in \{0, 1\}^n \). Is there \( \ell \in [n] \), such that \( X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \vec{0} \)?
**GFHD is hard for \( R \)**

GFHD Alice receives \( X_1, X_2 \in \{0, 1\}^n \); Bob receives \( Y_1, Y_2 \in \{0, 1\}^n \). Is there \( \ell \in [n] \), such that \( X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \bar{0} \)?

- \( R \) is about rectangles!
  
  First think about the equality function. If \( (X, Y) \subseteq A \times B \) is strongly “biased” towards \( X \neq Y \), then either \( A \) reveals \( \Omega(1) \) bits about \( X \subseteq A \) or \( B \) reveals \( \Omega(1) \) bits about \( Y \subseteq B \).
**GFHD is hard for \( R \)**

Alice receives \( X_1, X_2 \in \{0, 1\}^n \); Bob receives \( Y_1, Y_2 \in \{0, 1\}^n \). Is there \( \ell \in [n] \), such that \( X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \bar{0} \)?

- \( R \) is about rectangles!
  First think about the equality function. If \((X, Y) \subseteq A \times B\) is strongly “biased” towards \( X \neq Y \), then either \( A \) reveals \( \Omega(1) \) bits about \( X \subseteq A \) or \( B \) reveals \( \Omega(1) \) bits about \( Y \subseteq B \).

- Similarly, \( A \times B \) that witnesses negative answer to \( GFHD \) should contain \( \Omega(1) \) bits either about \( X_1 \oplus \sigma_\ell(X_2) \) for \((X_1, X_2) \subseteq A\), or about \( Y_1 \oplus \sigma_\ell(Y_2) \) for \((Y_1, Y_2) \subseteq B\) – for at least \( n/2 \) different values of \( \ell \).
Advantage of $Q^\parallel,\text{ent}$ over $R$ for a function $GFHD$

**GFHD is hard for $R$**

Alice receives $X_1, X_2 \in \{0, 1\}^n$; Bob receives $Y_1, Y_2 \in \{0, 1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \vec{0}$?

- $R$ is about rectangles!
  First think about the equality function. If $(X, Y) \subseteq A \times B$ is strongly “biased” towards $X \neq Y$, then either $A$ reveals $\Omega(1)$ bits about $X \subset A$ or $B$ reveals $\Omega(1)$ bits about $Y \subset B$.

- Similarly, $A \times B$ that witnesses negative answer to $GFHD$ should contain $\Omega(1)$ bits either about $X_1 \oplus \sigma_\ell(X_2)$ for $(X_1, X_2) \subseteq A$, or about $Y_1 \oplus \sigma_\ell(Y_2)$ for $(Y_1, Y_2) \subseteq B$ – for at least $n/2$ different values of $\ell$.

- One way to construct $A \subseteq \{0, 1\}^{n+n}$ that reveals “something” about $X_1 \oplus \sigma_\ell(X_2)$ for $(X_1, X_2) \in A$ and all $\ell \in [n]$ is to fix $\Omega(\sqrt{n})$ bits in $X_1$ and in $X_2$ – this would “cost” $\Omega(\sqrt{n})$ bits of entropy for $A$. If this were the only possible construction, that would give a strong lower bound.
**GFHD is hard for $\mathcal{R}$ – continued**

**GFHD** Alice receives $X_1, X_2 \in \{0, 1\}^n$; Bob receives $Y_1, Y_2 \in \{0, 1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \overline{0}$?

- One way to construct $A \subseteq \{0, 1\}^{n+n}$ that reveals “something” about $X_1 \oplus \sigma_\ell(X_2)$ for $(X_1, X_2) \in A$ and all $\ell \in [n]$ is to fix $\Omega(\sqrt{n})$ bits in $X_1$ and in $X_2$ – this would “cost” $\Omega(\sqrt{n})$ bits of entropy for $A$. If this were the only possible construction, that would give a strong lower bound.

- There exists a “less wasteful” way to achieve the same: by fixing the parity of $X_1 \oplus X_2$ – this “costs” $A$ only 1 bit of entropy. 
  I.e., there exists a very large set that has the property, which we initially wanted to use in order to force the set to be small.
**GFHD is hard for \( R \) – continued**

Alice receives \( X_1, X_2 \in \{0,1\}^n \); Bob receives \( Y_1, Y_2 \in \{0,1\}^n \). Is there \( \ell \in [n] \), such that \( X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \bar{0} \)?

- One way to construct \( A \subseteq \{0,1\}^{n+n} \) that reveals “something” about \( X_1 \oplus \sigma_\ell(X_2) \) for \( (X_1, X_2) \in A \) and all \( \ell \in [n] \) is to fix \( \Omega(\sqrt{n}) \) bits in \( X_1 \) and in \( X_2 \) – this would “cost” \( \Omega(\sqrt{n}) \) bits of entropy for \( A \). If this were the only possible construction, that would give a strong lower bound.

- There exists a “less wasteful” way to achieve the same: by fixing the parity of \( X_1 \oplus X_2 \) – this “costs” \( A \) only 1 bit of entropy. I.e., there exists a very large set that has the property, which we initially wanted to use in order to force the set to be small.

- Note the “\( \approx \)” in the definition of GFHD!
GFHD is hard for $\mathcal{R}$ — continued

Alice receives $X_1, X_2 \in \{0,1\}^n$; Bob receives $Y_1, Y_2 \in \{0,1\}^n$. Is there $\ell \in [n]$, such that $X_1 \oplus \sigma_\ell(X_2) \oplus Y_1 \oplus \sigma_\ell(Y_2) \approx \bar{0}$?

- One way to construct $A \subseteq \{0,1\}^{n+n}$ that reveals “something” about $X_1 \oplus \sigma_\ell(X_2)$ for $(X_1, X_2) \in A$ and all $\ell \in [n]$ is to fix $\Omega\left(\sqrt{n}\right)$ bits in $X_1$ and in $X_2$ — this would “cost” $\Omega\left(\sqrt{n}\right)$ bits of entropy for $A$. If this were the only possible construction, that would give a strong lower bound.

- There exists a “less wasteful” way to achieve the same: by fixing the parity of $X_1 \oplus X_2$ — this “costs” $A$ only 1 bit of entropy.
  I.e., there exists a very large set that has the property, which we initially wanted to use in order to force the set to be small.

- Note the “$\approx$” in the definition of $GFHD$!
  It makes the second construction (and any other one, based on “long parities”) inappropriate: “$\approx$” requires noise-stability of any protocol for $GFHD$, while noise “erases long parities”. This leads to

$$\mathcal{R}(GFHD) \in \Omega\left(\sqrt{n}\right).$$
Open questions

Allowing quantum operations in the setting of communication complexity leads to a number of natural questions that are still open:
Allowing quantum operations in the setting of communication complexity leads to a number of natural questions that are still open:

- For total functions, can quantum models have any (super-polynomial) advantage over the corresponding classical models, stronger than $R^\parallel$?
Allowing quantum operations in the setting of communication complexity leads to a number of natural questions that are still open:

- For total functions, can quantum models have any (super-polynomial) advantage over the corresponding classical models, stronger than $R^\parallel$?

- More generally, when does quantum communication offer any (super-polynomial) advantage?