Nondeterministic and Randomized Boolean Hierarchies in Communication Complexity

ICALP 2020

Toniann Pitassi · **Morgan Shirley** · Thomas Watson

1. Communication complexity

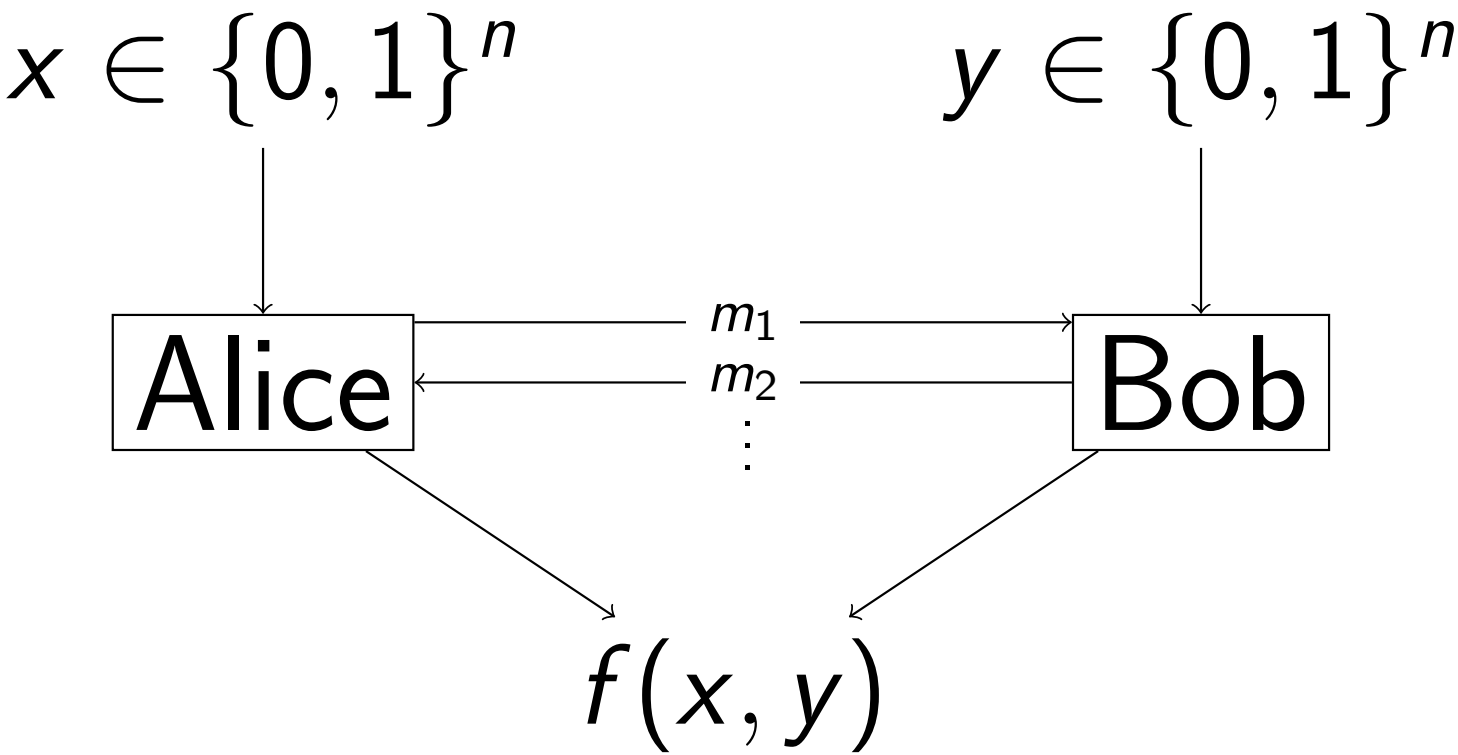
2. Motivations

3. Main results

   3.1 The Randomized Boolean Hierarchy in communication complexity does not collapse

   3.2 $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}}$ vs. $\mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$

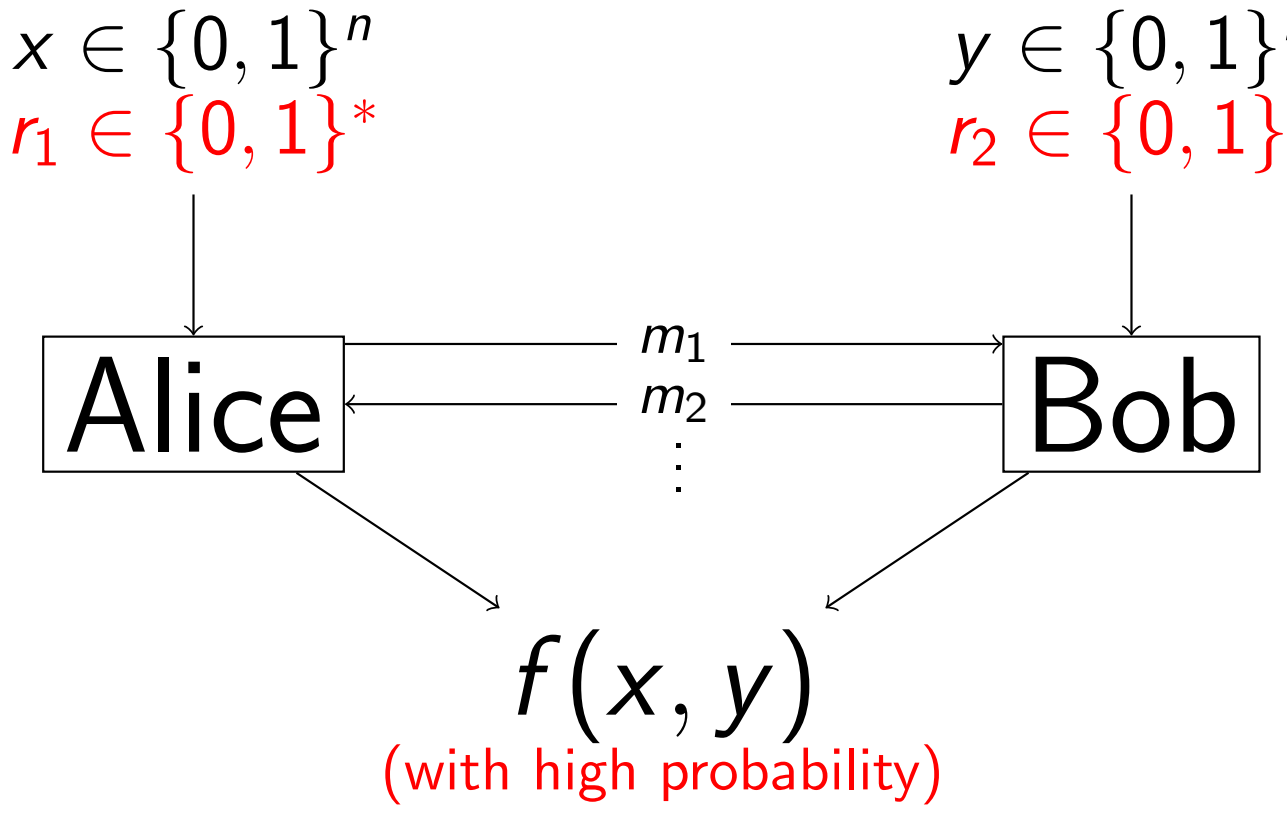
Communication Complexity[1]



The cost of the protocol is the *number of bits exchanged*.

[1] Yao, "Some Complexity Questions Related to Distributive Computing".

Randomized Communication Complexity

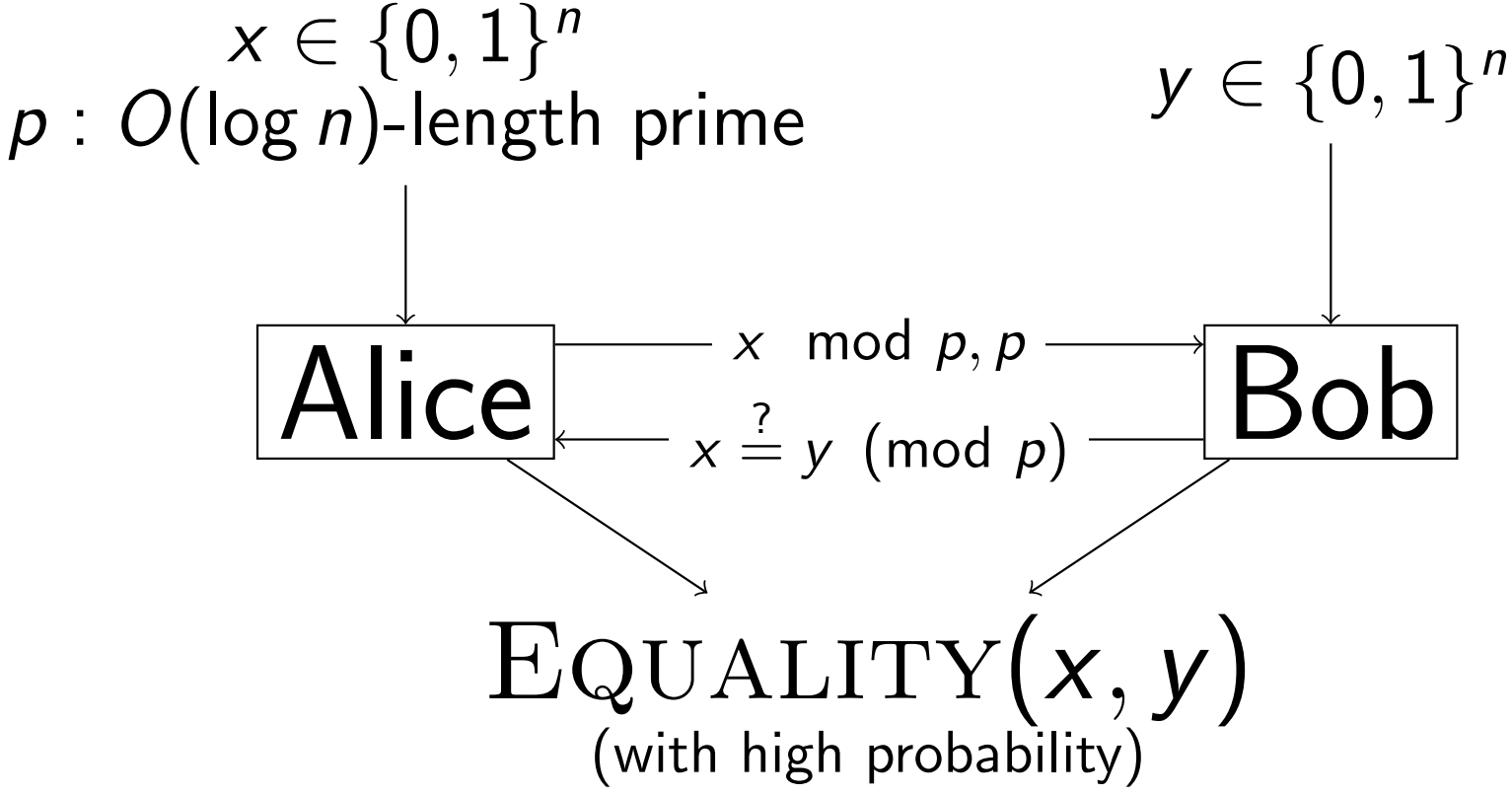


Classical Complexity:
P vs BPP still open

Communication Complexity:
Randomness helps!

Randomized Communication Complexity

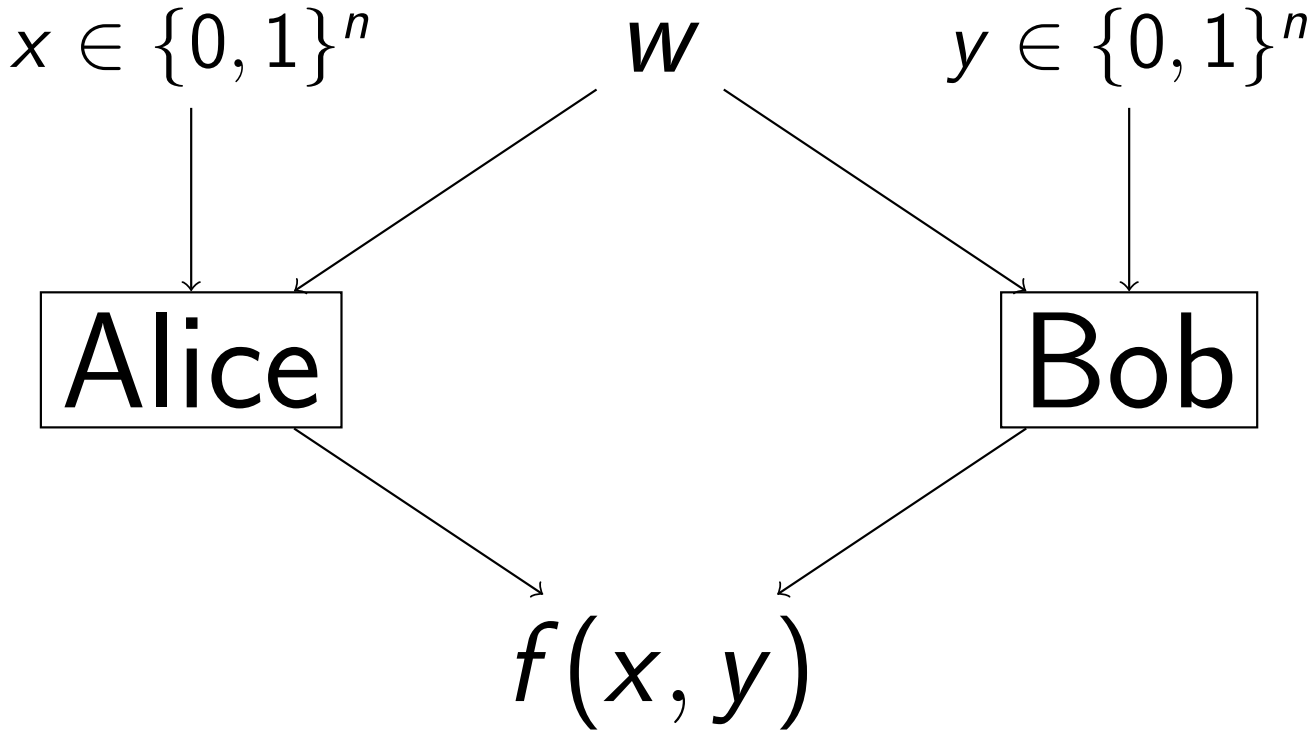
$\textsc{Equality}(x, y) = 1 \Leftrightarrow x = y$



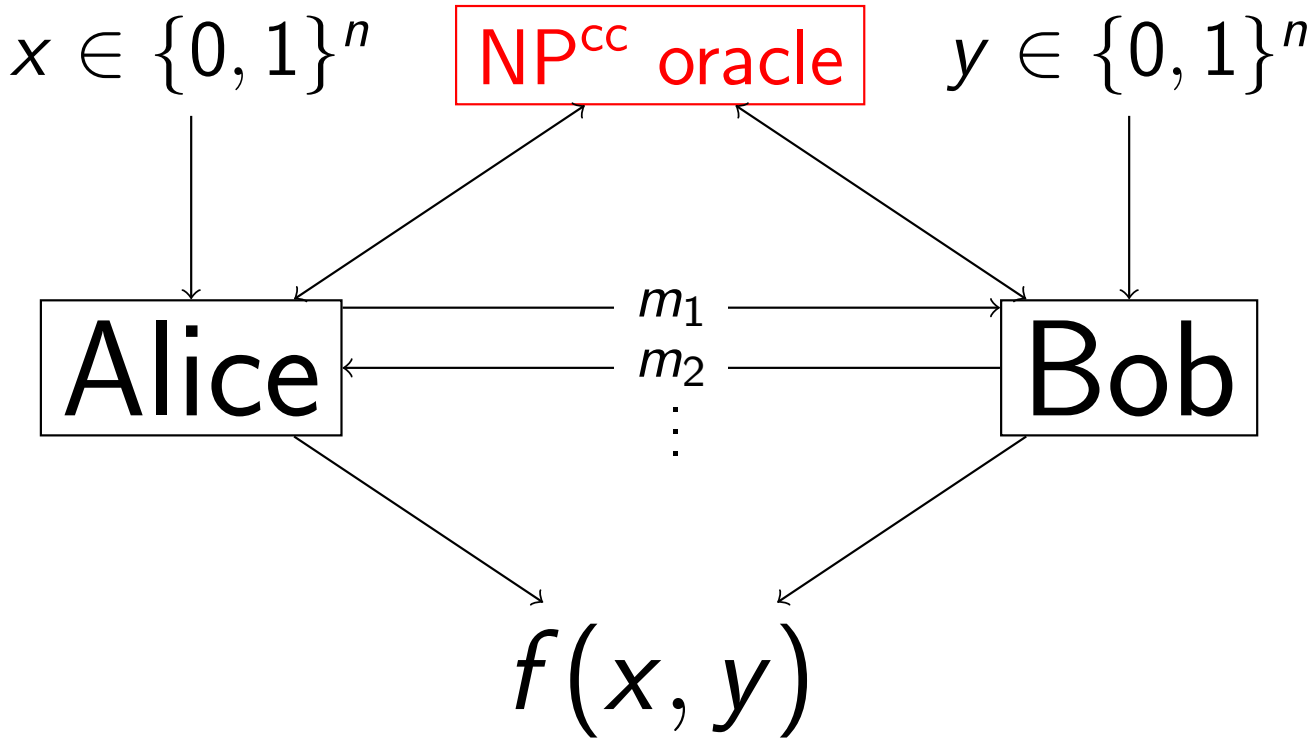
Communication Complexity Classes

- Deterministic: P^{cc}
- Randomized (Bounded-error): $\mathrm{BPP}^{\mathrm{cc}}$
- Randomized (No false negatives): $\mathrm{coRP}^{\mathrm{cc}}$
- Nondeterministic: $\mathrm{NP}^{\mathrm{cc}}$
- Deterministic with nondeterministic oracle: $\mathrm{P}^{\mathrm{NPcc}}$

$\mathsf{NP}^{\mathsf{cc}}$



$\mathrm{P}^{\mathrm{NP^{cc}}}$



Oracles in Communication Complexity

Alice and Bob want to compute function f.

They are allowed to make an **oracle call** to a function g.

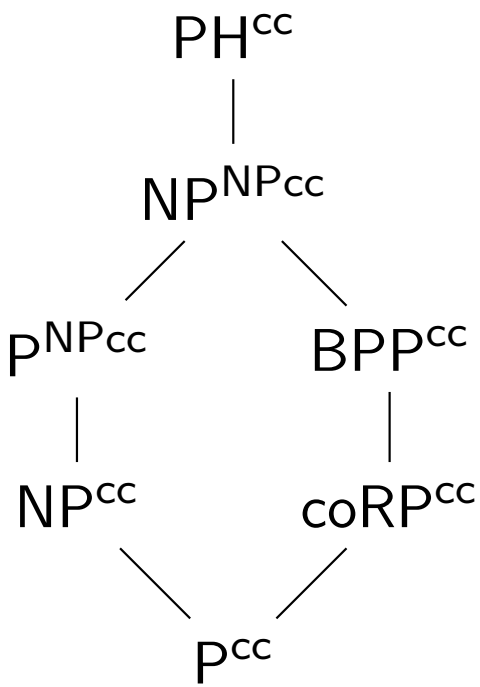
To do this, they each *privately* write down inputs x', y' to g.

The cost of the oracle call is based on the model. For example, if the model is $\mathrm{P}^{\mathrm{NP^{cc}}}$, they are charged the $\mathrm{NP}^{\mathrm{cc}}$ cost of g.

Communication Complexity Classes

- Deterministic: P^{cc}
- Randomized (Bounded-error): $\mathrm{BPP}^{\mathrm{cc}}$
- Randomized (No false negatives): $\mathrm{coRP}^{\mathrm{cc}}$
- Nondeterministic: $\mathrm{NP}^{\mathrm{cc}}$
- Deterministic with nondeterministic oracle: $\mathrm{P}^{\mathrm{NPcc}}$
- Polynomial hierarchy: $\mathrm{PH}^{\mathrm{cc}} = \mathrm{NP}^{\mathrm{NPcc}} \cup \mathrm{NP}^{\mathrm{NP}^{\mathrm{NP}}\mathrm{cc}} \cup \ldots$

Relationships Between Classes



PH^{cc} has deep connections to questions about matrix rigidity.[2]

Unfortunately, we don't even understand the *second level* of the Polynomial Hierarchy!

[2] Razborov, *On Rigid Matrices*; Alman and Williams, "Probabilistic Rank and Matrix Rigidity".

$\mathrm{BPP}^{\mathrm{cc}}$ vs $\mathrm{P}^{\mathrm{NPcc}}$

What is the relationship between $\mathrm{BPP}^{\mathrm{cc}}$ and $\mathrm{P}^{\mathrm{NPcc}}$?

- $\mathrm{P}^{\mathrm{NPcc}} \not\subset \mathrm{BPP}^{\mathrm{cc}}$ (example: Set Disjointness)
- If partial functions are allowed: $\mathrm{BPP}^{\mathrm{cc}} \not\subset \mathrm{P}^{\mathrm{NPcc}}$
- Only total functions: still open!

Total Functions vs Partial Functions

When partial functions are allowed, protocols can
break the rules of the model on inputs not in the support!

$\mathbf{P^{cc}}$ vs $\mathbf{NP^{cc} \cap coNP^{cc}}$:

- Total functions only[3]: $P^{cc} = NP^{cc} \cap coNP^{cc}$
- Partial functions allowed: $P^{cc} \subsetneq NP^{cc} \cap coNP^{cc}$

[3] Aho, Ullman, and Yannakakis, "On notions of information transfer in VLSI circuits".

First step towards solving $\mathbf{BPP^{cc}}$ vs $\mathbf{P^{NPcc}}$:

Does $\mathrm{BPP}^{\mathrm{cc}} = \mathrm{P}^{\mathrm{RPcc}}$?

$\mathrm{BPP}^{\mathrm{cc}}$ vs $\mathrm{P}^{\mathrm{RPcc}}$

Conjecture (disproven): For total functions, $\mathrm{BPP}^{\mathrm{cc}} = \mathrm{P}^{\mathrm{EQcc}}$ (oracle calls must be to the $\textsc{Equality}$ function)

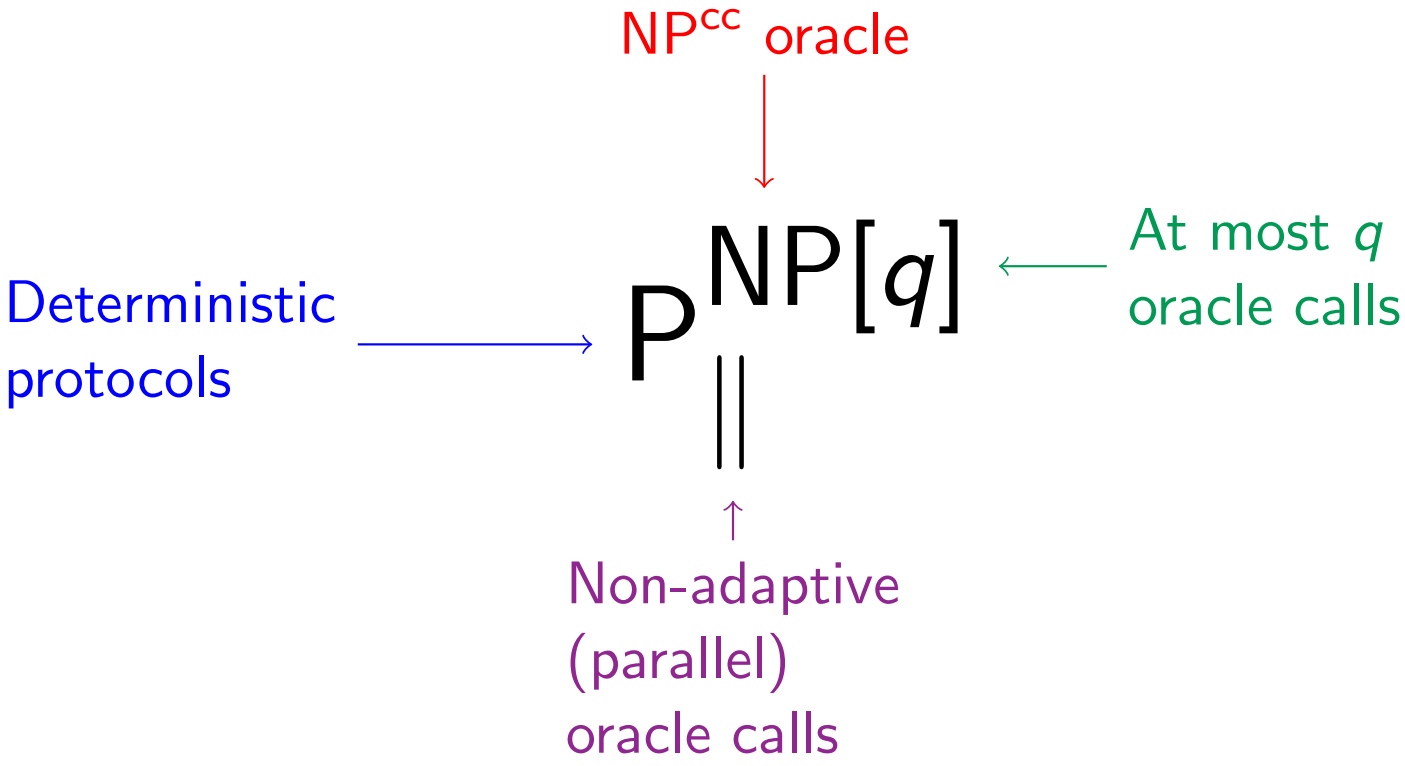
Theorem (CLV19)[4]: There is an infinite sequence of functions $f_1, f_2, \cdots \in \mathrm{coRP}^{\mathrm{cc}}$ such that

- $f_1 \notin \mathrm{P}^{\mathrm{EQcc}}$
- $\forall i, f_i \notin \mathrm{P}^{f_{i-1}\mathrm{cc}}$

[4] Chattopadhyay, Lovett, and Vinyals, "Equality Alone Does Not Simulate Randomness".

Main idea: How does the strength of $\mathrm{P}^{\mathrm{RPcc}}$ change when we **limit the number of oracle calls**?

This concept is captured by the **Randomized Boolean Hierarchy.**


NP^cc oracle
Deterministic protocols
P^NP[q]
At most q oracle calls
Non-adaptive (parallel) oracle calls

Nondeterministic Boolean Hierarchy

$\mathrm{NP}^{\mathrm{cc}} = \mathrm{NP}(1)^{\mathrm{cc}}$ $\quad \mathrm{NP}(2)^{\mathrm{cc}}$ $\quad \mathrm{NP}(3)^{\mathrm{cc}}$ $\quad \ldots$

$\mathrm{coNP}(1)^{\mathrm{cc}} = \mathrm{coNP}^{\mathrm{cc}}$ $\quad \mathrm{coNP}(2)^{\mathrm{cc}}$ $\quad \mathrm{coNP}(3)^{\mathrm{cc}}$

- Protocol specifies functions $g_1, g_2, \ldots g_q \in \mathrm{NP}^{\mathrm{cc}}$
- $\mathrm{NP}(q)^{\mathrm{cc}}$: Are there an **odd** number of i such that $g_i(x, y) = 1$?
- $\mathrm{coNP}(q)^{\mathrm{cc}}$: Are there an **even** number of i such that $g_i(x, y) = 1$?

Nondeterministic Boolean Hierarchy

Previously studied in both classical complexity[5] and communication complexity[6].

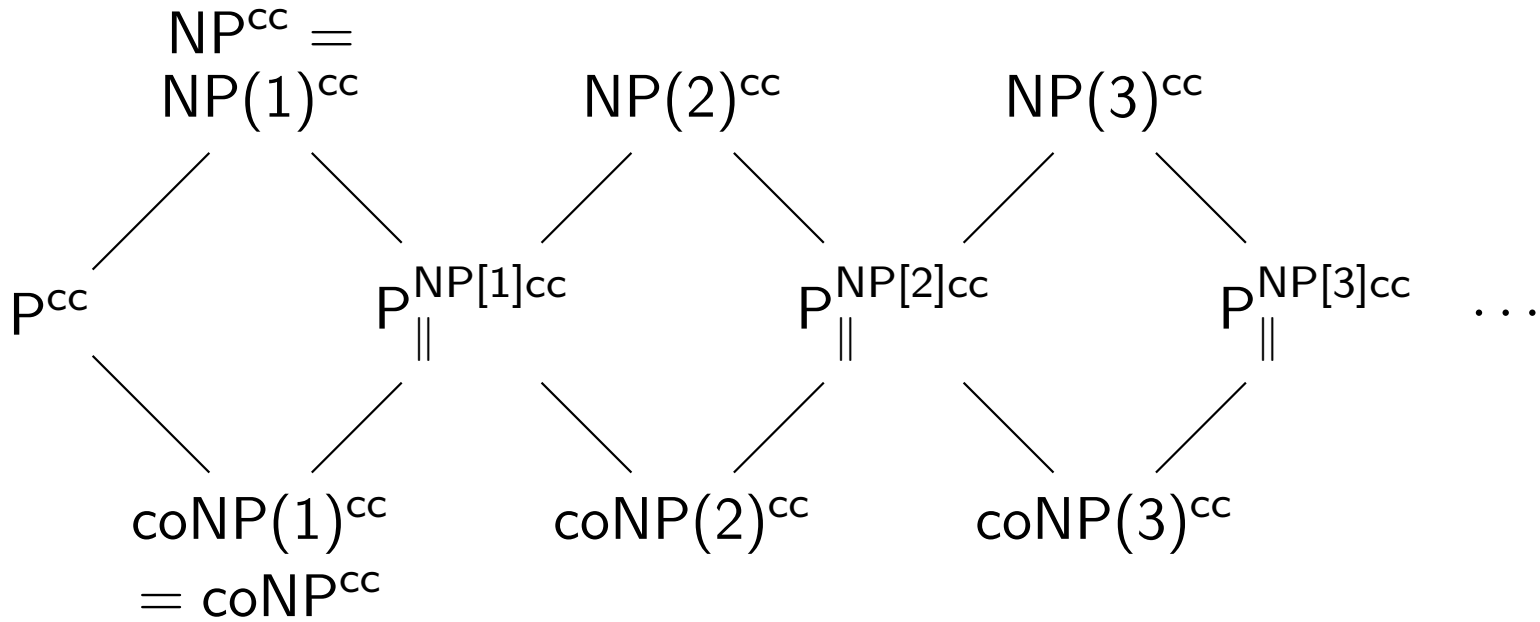
There are multiple definitions. We use this "parity" definition because it gives simpler proofs!

---

[5] Wechsung, "On the Boolean Closure of NP"; Cai and Hemachandra, "The Boolean Hierarchy: Hardware over NP"; Köbler, Schöning, and Wagner, "The Difference and Truth-Table Hierarchies for NP"; Wagner, "Bounded Query Computations"; Beigel, "Bounded Queries to SAT and the Boolean Hierarchy".

[6] Halstenberg and Reischuk, "Relations Between Communication Complexity Classes".

Nondeterministic Boolean Hierarchy



For all constant q, $\mathrm{NP}(q)^{\mathrm{cc}} \subsetneq \mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}} \subsetneq \mathrm{NP}(q+1)^{\mathrm{cc}}$.[7]

[7] Halstenberg and Reischuk, "Relations Between Communication Complexity Classes".

Question: What is the relationship between $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}}$ and $\mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$?

P^{cc} vs $\mathrm{NP}^{\mathrm{cc}} \cap \mathrm{coNP}^{\mathrm{cc}}$:

- Total functions only: $\mathrm{P}^{\mathrm{cc}} = \mathrm{NP}^{\mathrm{cc}} \cap \mathrm{coNP}^{\mathrm{cc}}$
- Partial functions allowed: $\mathrm{P}^{\mathrm{cc}} \subsetneq \mathrm{NP}^{\mathrm{cc}} \cap \mathrm{coNP}^{\mathrm{cc}}$

$\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}}$ vs $\mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$ (Our result):

- Total functions only: $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}} = \mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$
- Partial functions allowed: $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}} \subsetneq \mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$

Randomized Boolean Hierarchy

Replace $\mathrm{NP}^{\mathrm{cc}}$ oracles with $\mathrm{RP}^{\mathrm{cc}}$ oracles to get the Randomized Boolean Hierarchy!

This was studied previously in classical complexity[8] but not yet in communication complexity.

[8] Bertoni et al., "Generalized Boolean Hierarchies and Boolean Hierarchies over RP".

Randomized Boolean Hierarchy: Example

$\textsc{Equality} \in \mathsf{coRP}^{\mathsf{cc}} = \mathsf{coRP}(1)^{\mathsf{cc}}$

$\textsc{NonEq} \in \mathsf{RP}^{\mathsf{cc}} = \mathsf{RP}(1)^{\mathsf{cc}}$

$\oplus_q \textsc{NonEq} \in \mathsf{RP}(q)^{\mathsf{cc}}$:

- $x = (x_1, x_2, \ldots x_q)$, $y = (y_1, y_2, \ldots y_q)$
- Are there an odd number of i such that $x_i \neq y_i$?

$\overline{\oplus_q \textsc{NonEq}} \in \mathsf{coRP}(q)^{\mathsf{cc}}$

- $x = (x_1, x_2, \ldots x_q)$, $y = (y_1, y_2, \ldots y_q)$
- Are there an <u>even</u> number of i such that $x_i \neq y_i$?

Theorem: The Randomized Boolean Hierarchy in communication complexity is **infinite**

$$(\mathrm{RP}(q)^{\mathrm{cc}} \subsetneq \mathrm{P}_{\|}^{\mathrm{RP}[q]} \subsetneq \mathrm{RP}(q+1)^{\mathrm{cc}})$$

Theorem: $\mathrm{P}_{\parallel}^{\mathrm{NP}[q]\mathrm{cc}} = \mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$ for <u>total functions</u>

$\mathrm{P}_{\parallel}^{\mathrm{NP}[q]\mathrm{cc}} \subsetneq \mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$ for <u>partial functions</u>

Theorem: $\mathsf{P}_{\|}^{\mathsf{RP}[q]\mathsf{cc}} = \mathsf{RP}(q+1)^{\mathsf{cc}} \cap \mathsf{coRP}(q+1)^{\mathsf{cc}}$ for <u>total functions</u>

$\mathsf{P}_{\|}^{\mathsf{RP}[q]\mathsf{cc}} \subsetneq \mathsf{RP}(q+1)^{\mathsf{cc}} \cap \mathsf{coRP}(q+1)^{\mathsf{cc}}$ for <u>partial functions</u>

1. Communication complexity

2. Motivations

3. Main results

   3.1 The Randomized Boolean Hierarchy in communication complexity does not collapse

   3.2 $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}}$ vs. $\mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$

Theorem: For all q, $\mathsf{coRP}(q)^{\mathsf{cc}} \not\subset \mathsf{NP}(q)^{\mathsf{cc}}$

- $\overline{\oplus_q \textsc{NonEq}} \in \mathsf{coRP}(q)^{\mathsf{cc}}$
- $\overline{\oplus_q \textsc{NonEq}} \notin \mathsf{NP}(q)^{\mathsf{cc}}$

Intuition: $\textsc{Equality} \notin \mathsf{NP}^{\mathsf{cc}}$

Corollary: For all q, $\mathsf{coRP}(q)^{\mathsf{cc}} \neq \mathsf{RP}(q)^{\mathsf{cc}}$

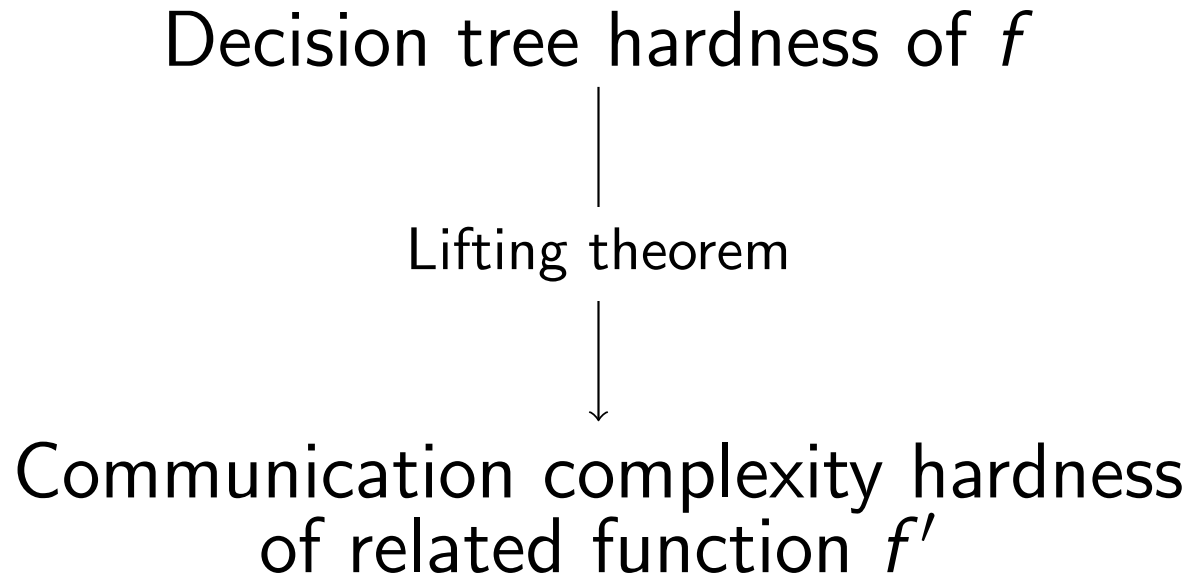
$\mathbf{P}_{\|}^{\mathbf{NP}[q]\mathbf{cc}}$ vs $\mathbf{NP}(q+1)^{\mathbf{cc}} \cap \mathbf{coNP}(q+1)^{\mathbf{cc}}$ (Our result):

- Total functions only: $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}} = \mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$
- Partial functions allowed: $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}} \subsetneq \mathrm{NP}(q+1)^{\mathrm{cc}} \cap \mathrm{coNP}(q+1)^{\mathrm{cc}}$

Total functions: constructive argument

Partial functions: **query-to-communication lifting**

Query-to-communication lifting



Query-to-communication lifting: details

- Hard function f for decision-tree model that represents $\mathrm{P}_{\|}^{\mathrm{NP}[q]}$
- Lifting shows that related function f' is hard for $\mathrm{P}_{\|}^{\mathrm{NP}[q]\mathrm{cc}}$
- f' is easy for $\mathrm{RP}(q+1)^{\mathrm{cc}} \cap \mathrm{coRP}(q+1)^{\mathrm{cc}}$

Additional details:

- Index gadget with size n^{20}
- $\mathrm{NP}(q)$ lifting theorem similar to P^{NP} lifting[9]
- $\mathrm{P}_{\|}^{\mathrm{NP}[q]}$ lifting theorem combination of $\mathrm{NP}(q)$ lifting and deterministic lifting[10]

[9] Göös et al., "Query-to-Communication Lifting for P^{NP}".

[10] Raz and McKenzie, "Separation of the Monotone NC Hierarchy"; Göös, Pitassi, and Watson, "Deterministic Communication vs. Partition Number".

Open problems

- What are the relationships between the Boolean Hierarchies and other natural complexity classes?
- Give a lifting theorem for the Randomized Boolean Hierarchy.
- What happens when we have a super-constant bound on the number of oracle calls?
- For total functions, is $\mathrm{BPP}^{\mathrm{cc}} = \mathrm{P}^{\mathrm{RPcc}}$?
- For total functions, is $\mathrm{BPP}^{\mathrm{cc}} \subset \mathrm{P}^{\mathrm{NPcc}}$?