The Quantum Adversary Method and Classical Formula Size Lower Bounds

Troy Lee
CWI, University of Amsterdam

Joint work with: Sophie Laplante and Mario Szegedy

Circuit Complexity

- Million dollar question: Show an explicit function which requires superpolynomial size circuits
- For functions in NP the best circuit lower bound we know is $5n - o(n)$ [Lachish and Raz 01, Iwama and Morizumi 02]
- The smallest complexity class we know to contain a function requiring superpolynomial size circuits is MAEXP [Buhrman, Fortnow, and Thierauf 98]

Formula Size

- Weakening of the circuit model—a formula is a binary tree with internal nodes labelled by AND, OR and leaves labelled by literals. The size of a formula, denoted $\mathsf{L}(f)$, is its number of leaves.

- PARITY has formula size $\theta(n^2)$ [Khrapchenko 71].

- The best lower bound for a function in NP is $n^{3-o(1)}$ [Håstad 98].

- Showing superpolynomial formula size lower bounds for a function in NP would imply NP $\neq$ NC^1.

Two Step Transformation

- We transform the problem of proving lower bounds on formula size in two steps:
  - First, we use the exact characterization of formula size in terms of a communication game [Karchmer and Wigderson 88]
  - We then lower bound the well known "rectangle bound" from communication complexity

Karchmer–Wigderson Game [KW88]

- Elegant characterization of formula size in terms of a communication game.

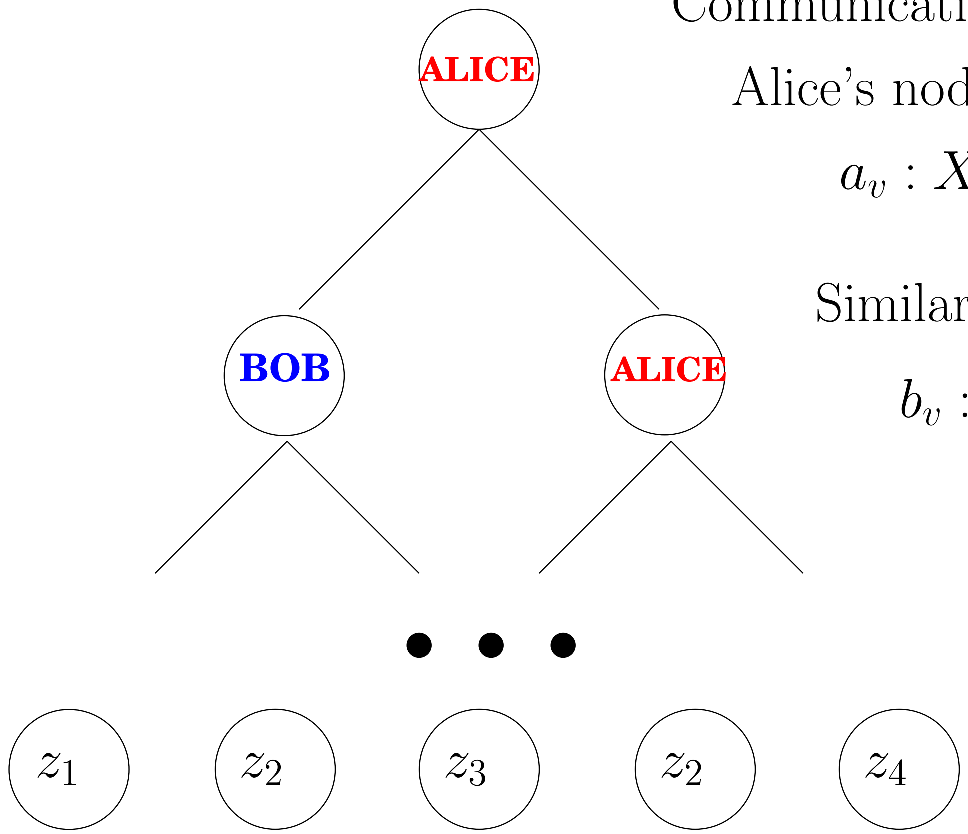
- For a Boolean function f, let $X = f^{-1}(0)$ and $Y = f^{-1}(1)$. Consider $R_f = \{(x, y, i) : x \in X,\ y \in Y,\ x_i \neq y_i\}$

- The game is then the following: Alice is given $x \in X$, Bob is given $y \in Y$ and they wish to find i such that $(x, y, i) \in R_f$.

- Karchmer–Wigderson Thm: The number of leaves in a best communication protocol for R_f equals the formula size of f.

Communication complexity of relations

$R \subseteq X \times Y \times Z$



Communication protocol is a binary tree:

Alice's nodes labelled by a function:

$$a_v : X \longrightarrow \{0, 1\}$$

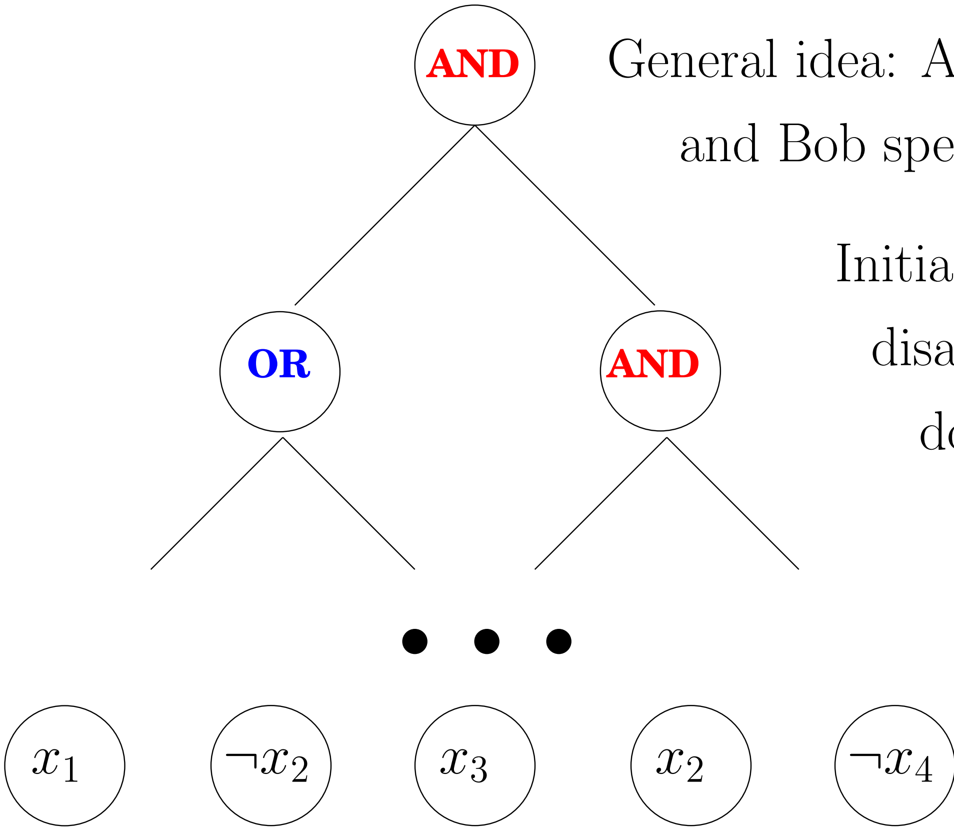
Similarly, Bob's nodes labelled

$$b_v : Y \longrightarrow \{0, 1\}$$

Leaves labelled by elements $z \in Z$.

Denote by $C^P(R)$ the number of leaves in a best protocol for R.

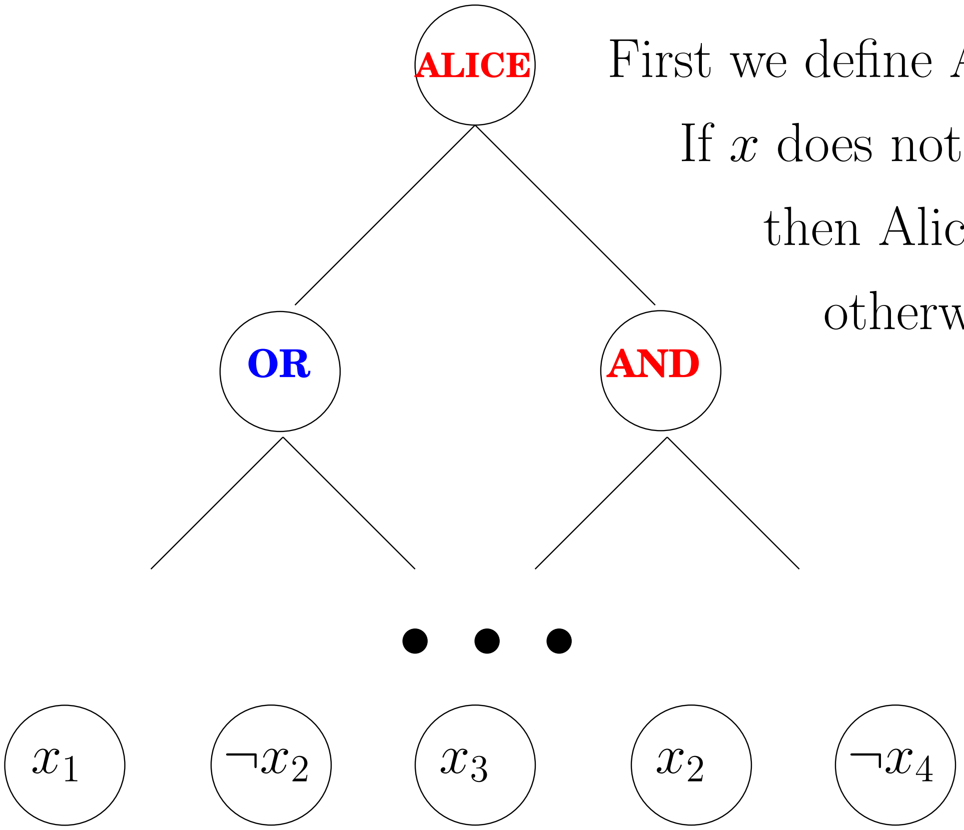
Proof by picture: $C^P(R_f) \leq \mathsf{L}(f)$.



General idea: Alice speaks at AND nodes and Bob speaks at OR nodes.

Initially, $f(x) \neq f(y)$ and we maintain this disagreement on subformulas as we move down the tree.

Proof by picture: $C^P(R_f) \leq \mathsf{L}(f)$.



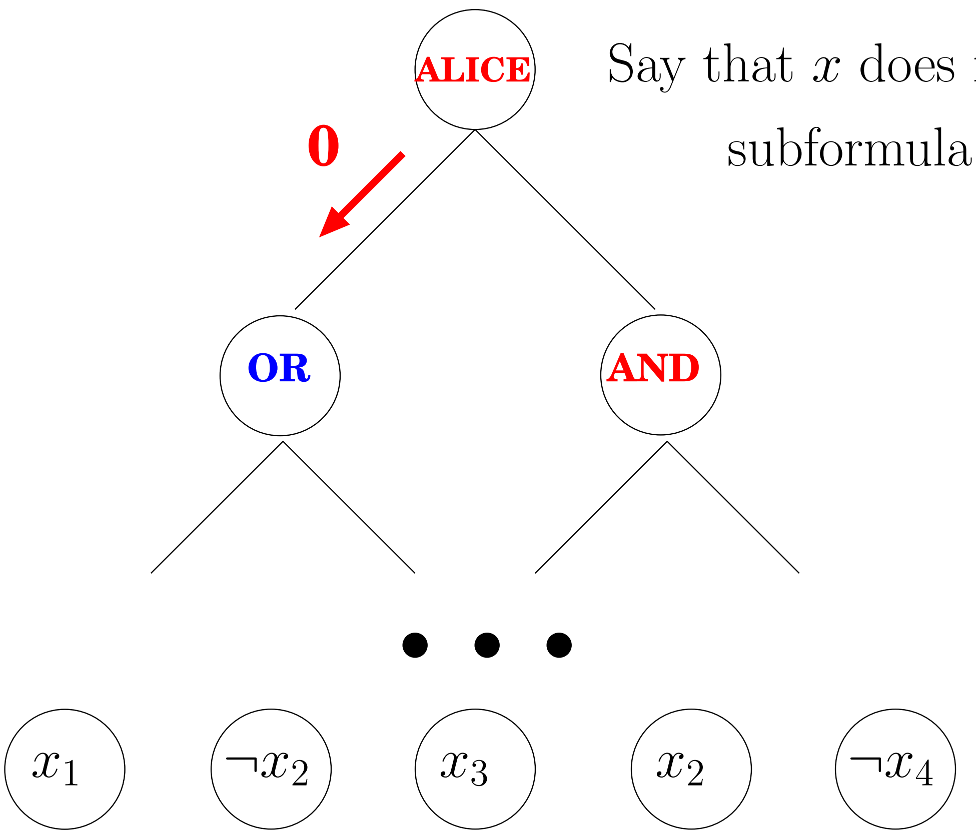
First we define Alice's action at the top node:

If x does not satisfy the left subformula,

then Alice sends the bit 0;

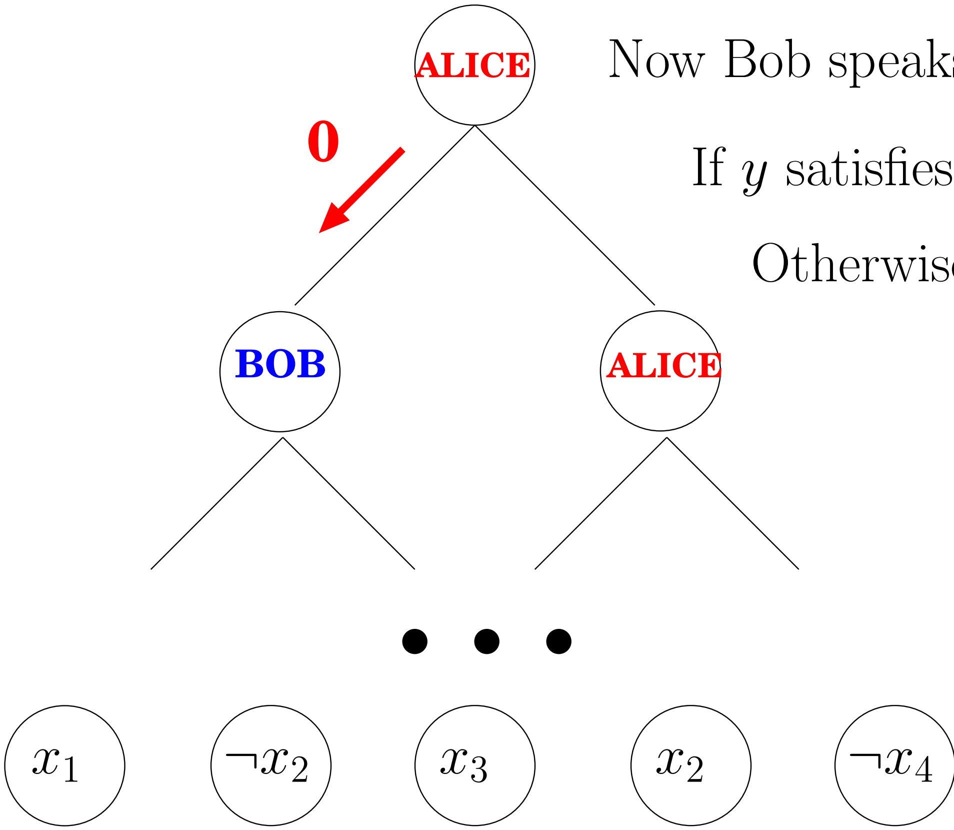
otherwise she sends the bit 1.

Proof by picture: $C^P(R_f) \leq \mathsf{L}(f)$.



Say that x does not satisfy the left subformula.

Proof by picture: $C^P(R_f) \leq \mathsf{L}(f)$.

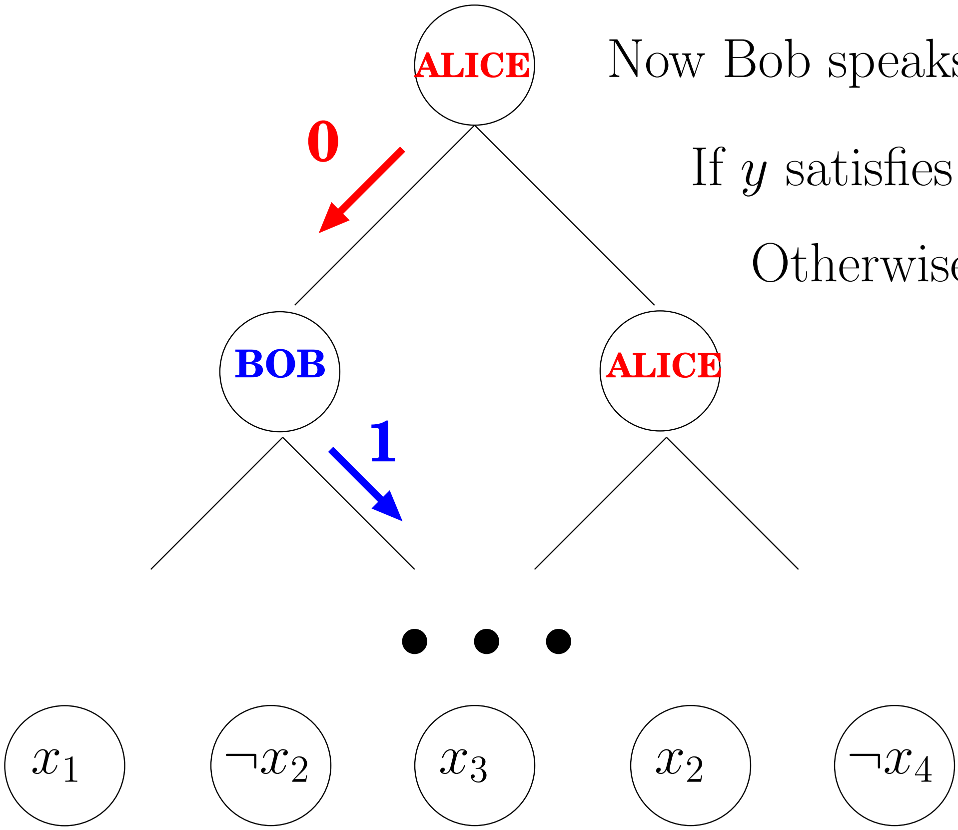


Now Bob speaks at the OR gate:

If y satisfies the left subformula, Bob says 0.

Otherwise, he says 1.

Proof by picture: $C^P(R_f) \leq \mathsf{L}(f)$.

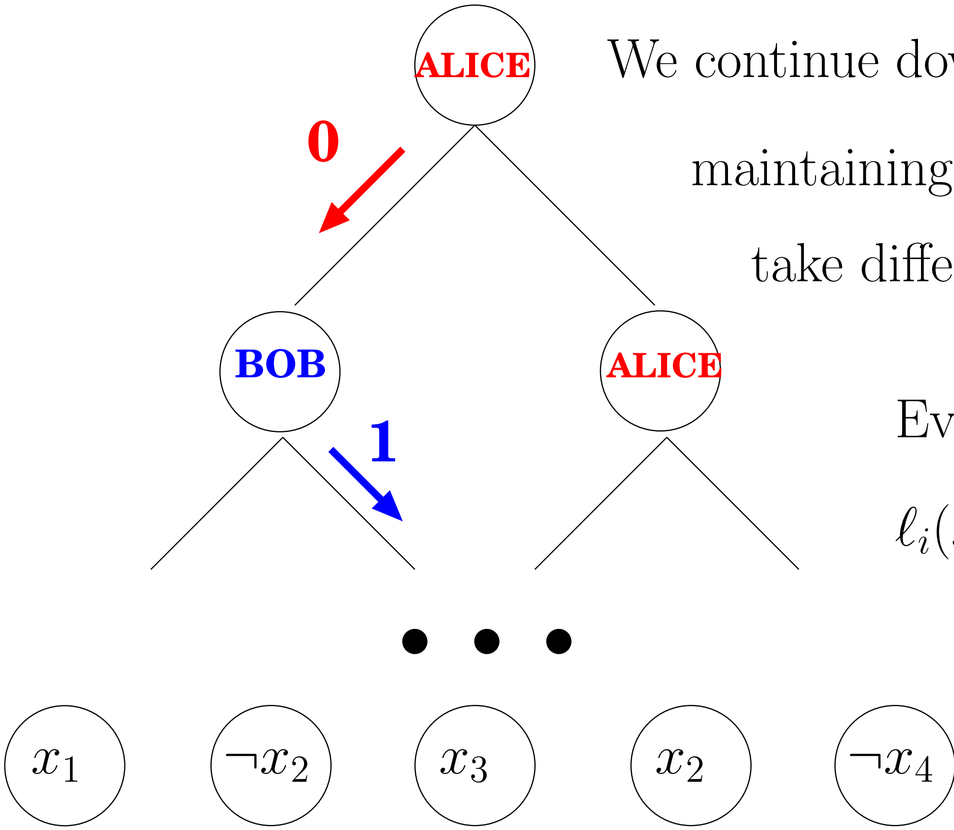


Now Bob speaks at the OR gate:

If y satisfies the left subformula, Bob says 0.

Otherwise, he says 1.

Proof by picture: $C^P(R_f) \leq \mathsf{L}(f)$.

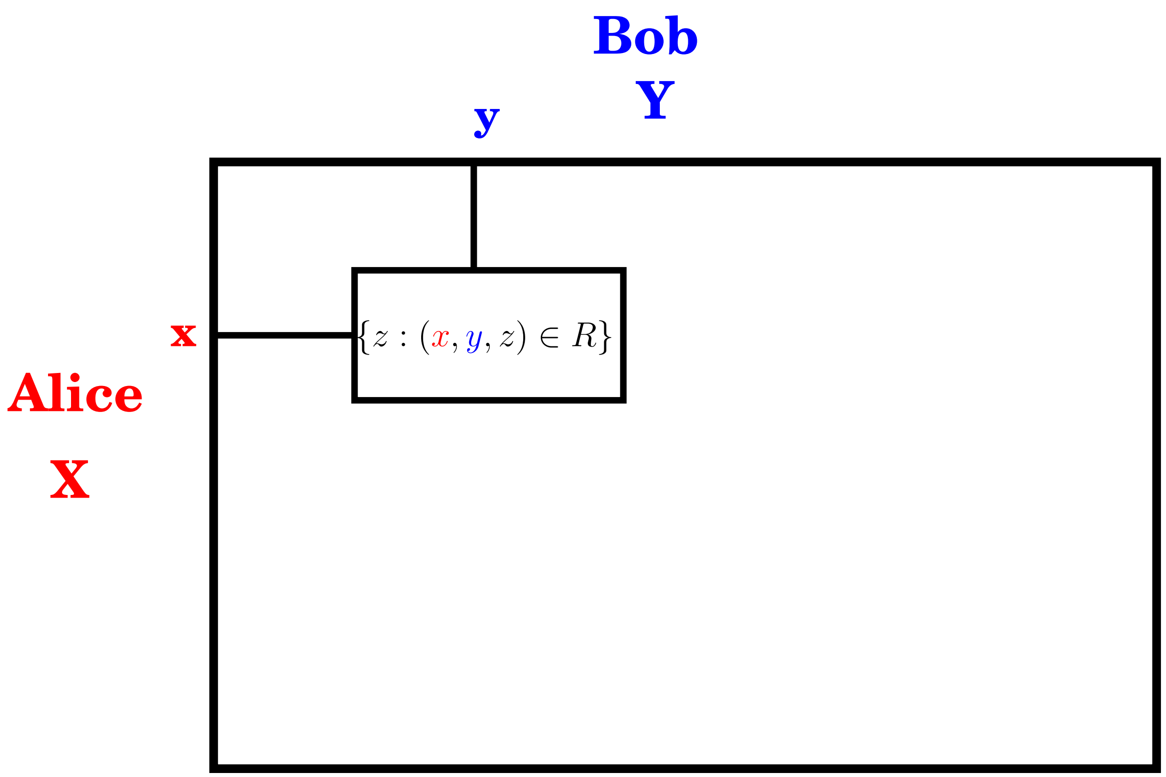


We continue down the tree in a similar fashion, maintaining the property that x and y take different values on subformulas.

Eventually, we reach a literal ℓ_i such that $\ell_i(x) \neq \ell_i(y)$ and so x and y differ on bit i.

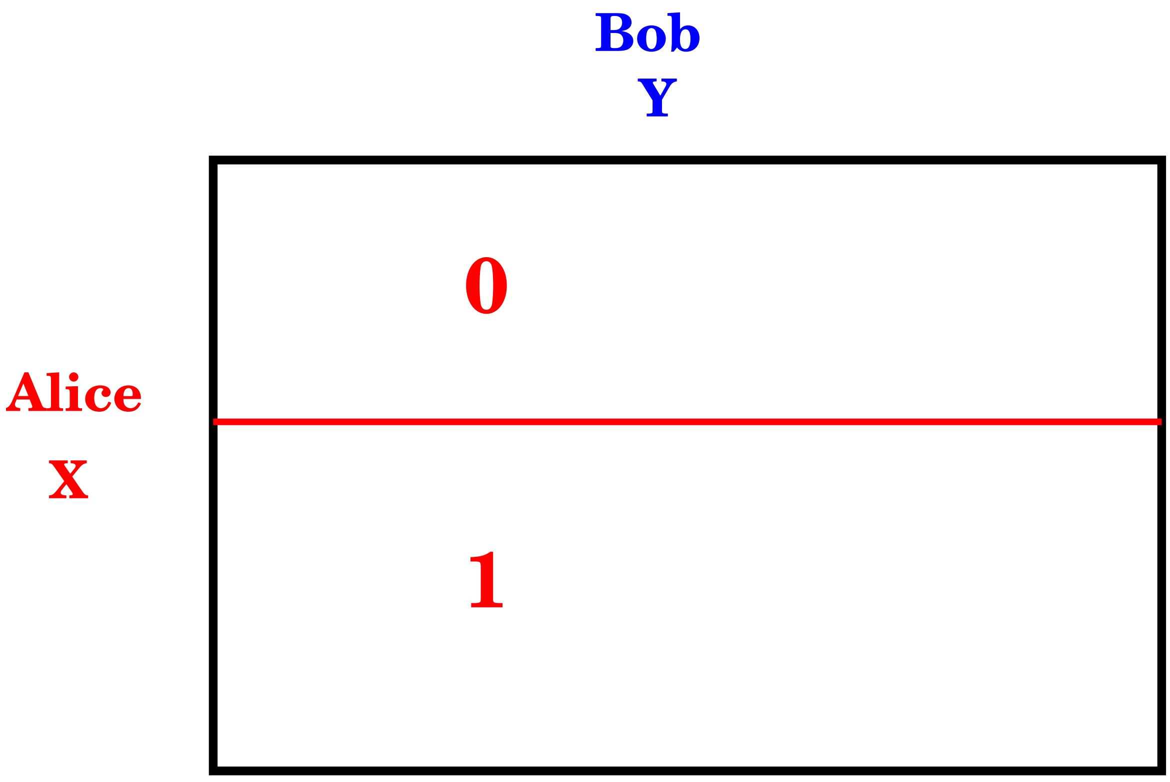
Communication Complexity and the Rectangle Bound

$$R \subseteq X \times Y \times Z$$



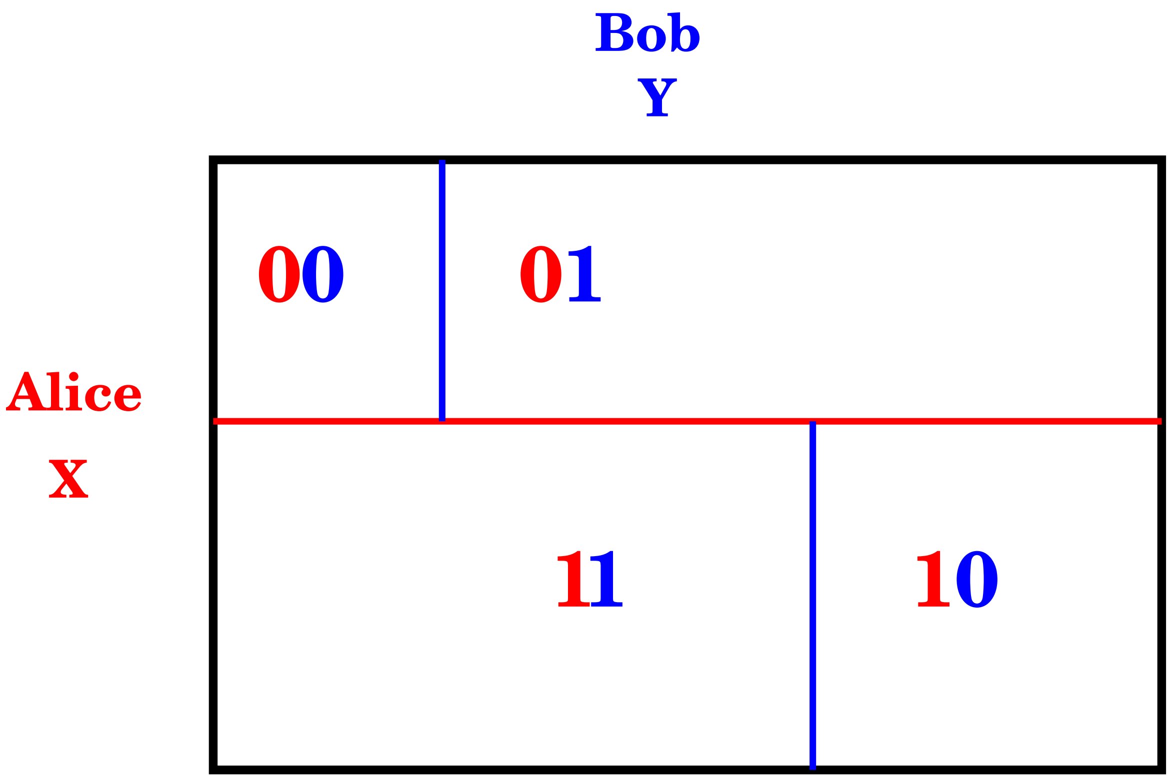
Communication Complexity and the Rectangle Bound

$$R \subseteq X \times Y \times Z$$



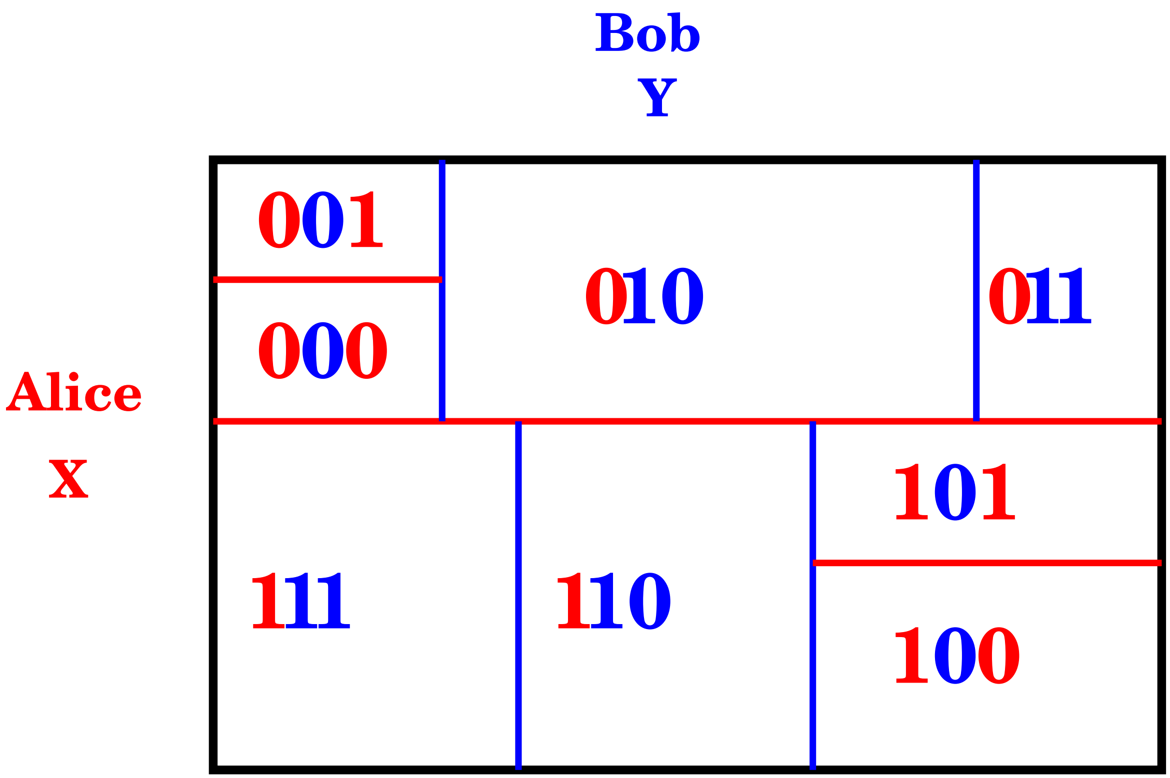
Communication Complexity and the Rectangle Bound

$$R \subseteq X \times Y \times Z$$



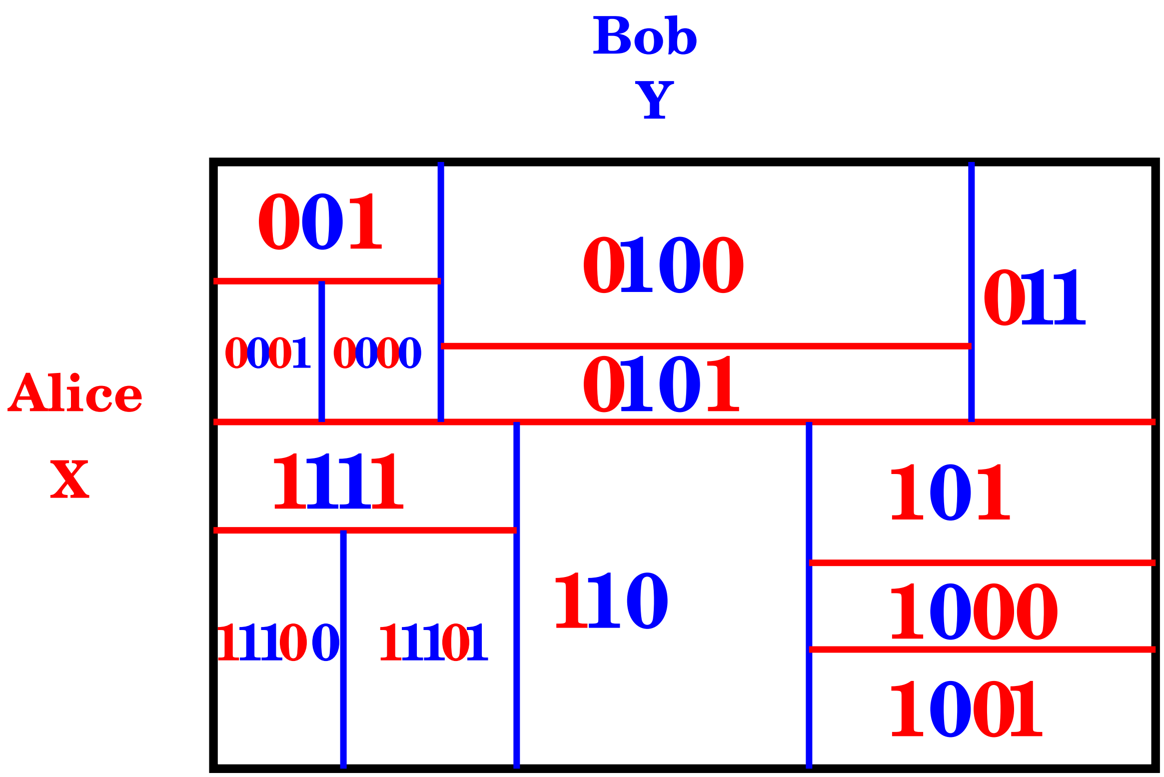
Communication Complexity and the Rectangle Bound

$R \subseteq X \times Y \times Z$



Communication Complexity and the Rectangle Bound

$$R \subseteq X \times Y \times Z$$



A rectangle S is monochromatic if there exists z such that $(x, y, z) \in S$ for all $(x, y) \in S$.

A successful protocol partitions $X \times Y$ into monochromatic rectangles.

Communication Complexity and the Rectangle Bound

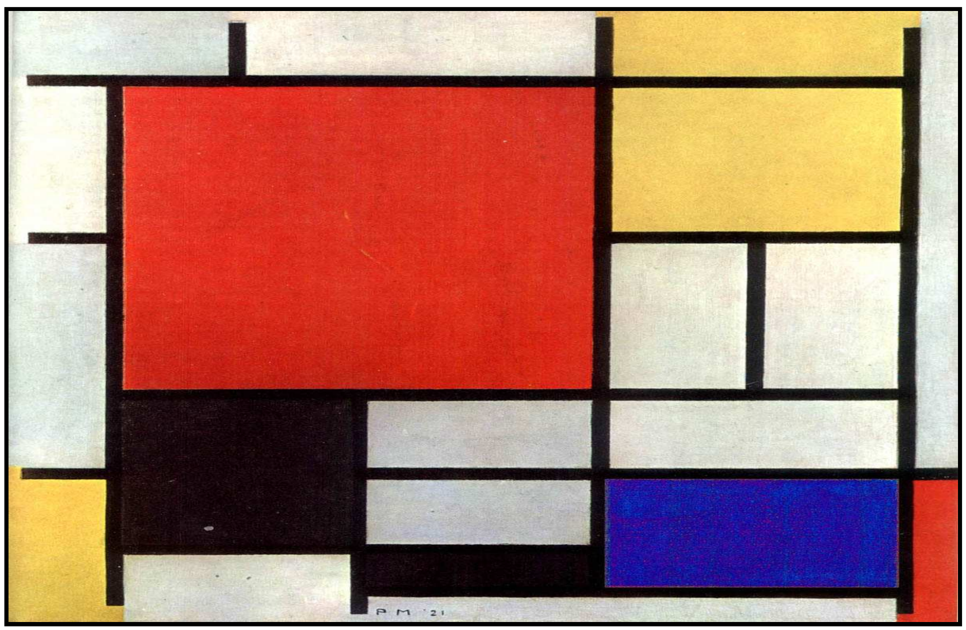
$$R \subseteq X \times Y \times Z$$

Bob

Y

Alice

X



Rectangle Bound

- We denote by $C^D(R)$ the size of a smallest partition of $X \times Y$ into monochromatic (with respect to R) rectangles. By the argument above, $C^D(R) \leq C^P(R)$.

- We can still hope to prove large lower bounds by focusing on the rectangle bound:

$$C^D(R) \leq C^P(R) \leq 2^{(\log C^D(R))^2}$$

- Being a purely combinatorial quantity, the rectangle bound is often easier to think about. On the other hand, it is in general NP hard to compute.

Approximating the rectangle bound

- If a size measure (of matrices) is subadditive on rectangles, then we can get a bound of the form:

$$\text{number of rectangles} \geq \frac{\text{size(everything)}}{\text{size(largest rectangle)}}.$$

- Many communication complexity bounds fit within this schema including rectangle area, or more generally probability mass, and matrix rank method of Razborov [Raz90].

- We add a new method within this framework based on the spectral norm.

Our main lemma: spectral norm squared is subadditive

- Spectral norm has several equivalent formulations. We use:

$$\|A\| = \max_{u,v\,:\|u\|=\|v\|=1} |u^T A v|$$

- Main Lemma: Let A be a matrix over $X \times Y$ and $\mathcal{R}$ be a partition of $X \times Y$ into rectangles. Then

$$\|A\|^2 \leq \sum_{R \in \mathcal{R}} \|A_R\|^2.$$

- Note that while $\|A + B\| \leq \|A\| + \|B\|$, for any A, B it is not true in general that $\|A + B\|^2 \leq \|A\|^2 + \|B\|^2$.

Proof of main lemma

Fix unit vectors u, v which maximize $|u^T A v|$. By definition,

$$\|A\| \;=\; |u^T A v| = |u^T (\sum_{R \in \mathcal{R}} A_R) v|$$

Proof of main lemma

Fix unit vectors u, v which maximize $|u^T A v|$. By definition,

$$\begin{aligned} \|A\| &= |u^T A v| = |u^T (\sum_{R \in \mathcal{R}} A_R) v| \\ &\le \sum_{R \in \mathcal{R}} |u^T A_R v| \end{aligned}$$

Proof of main lemma

Fix unit vectors u, v which maximize $|u^T Av|$. By definition,

$$\begin{aligned} \|A\| &= |u^T Av| = |u^T(\sum_{R\in\mathcal{R}} A_R)v| \\ &\leq \sum_{R\in\mathcal{R}} |u^T A_R v| \\ &\leq \sum_{R\in\mathcal{R}} \|A_R\| \ \|u_R\| \ \|v_R\| \end{aligned}$$

Proof of main lemma

Fix unit vectors u, v which maximize $|u^T A v|$. By definition,

$$
\begin{aligned}
\|A\| &= |u^T A v| = |u^T (\sum_{R \in \mathcal{R}} A_R) v| \\
&\leq \sum_{R \in \mathcal{R}} |u^T A_R v| \\
&\leq \sum_{R \in \mathcal{R}} \|A_R\| \; \|u_R\| \; \|v_R\| \\
&\leq \sqrt{\sum_{R \in \mathcal{R}} \|A_R\|^2} \sqrt{\sum_{R \in \mathcal{R}} \|u_R\|^2 \|v_R\|^2}
\end{aligned}
$$

Proof of main lemma

Fix unit vectors u, v which maximize $|u^T A v|$. By definition,

$$\begin{aligned}
\|A\| &= |u^T A v| = |u^T(\sum_{R\in\mathcal{R}} A_R)v| \\
&\leq \sum_{R\in\mathcal{R}} |u^T A_R v| \\
&\leq \sum_{R\in\mathcal{R}} \|A_R\| \; \|u_R\| \; \|v_R\| \\
&\leq \sqrt{\sum_{R\in\mathcal{R}} \|A_R\|^2} \sqrt{\sum_{R\in\mathcal{R}} \|u_R\|^2 \|v_R\|^2} \\
&= \sqrt{\sum_{R\in\mathcal{R}} \|A_R\|^2}.
\end{aligned}$$

Applying the lemma

From the lemma it follows that if $\mathcal{R}$ is an optimal rectangle partition of R_f, then

$$\max_{A \neq 0} \frac{\|A\|^2}{\max_{R \in \mathcal{R}} \|A_R\|^2} \leq C^D(R_f).$$

We want a method, however, that doesn't depend on knowing the optimal partition.

Monotonicity

- the rectangles in $\mathcal{R}$ are monochromatic, thus each rectangle is a subset of $D_i = \{(x, y) : x \in X, y \in Y, x_i \neq y_i\}$, for some $i \in [n]$.

- If A is nonnegative, then $\|A_R\| \leq \|A \circ D_i\|$

- Thus we obtain

$$\max_{A \geq 0} \frac{\|A\|^2}{\max_i \|A_i \circ D_i\|^2} \leq C^D(R_f) \leq \mathsf{L}(f).$$

An example: PARITY

- Consider a $2^{n-1} \times 2^{n-1}$ matrix A with rows indexed by strings of even parity, columns with strings of odd parity.

- Let $A[x, y] = 1$ if (x, y) have Hamming distance 1, and 0 otherwise.

- For the all 1 vector u we have $u^T A u = n2^{n-1}$, thus $\|A\| \geq n$.

- Each submatrix $A \circ D_i$ is identity matrix, thus $\|A \circ D_i\| = 1$.

The quantum adversary method emerges

Define

$$\mathsf{adv}(f) = \max_{A \geq 0} \frac{\|A\|}{\max_i \|A_i \circ D_i\|}$$

- We have shown that $\mathsf{adv}^2(f) \leq C^D(R_f) \leq \mathsf{L}(f)$

The quantum adversary method emerges

Define

$$\mathrm{adv}(f) = \max_{A \geq 0} \frac{\|A\|}{\max_i \|A_i \circ D_i\|}$$

- We have shown that $\mathrm{adv}^2(f) \leq C^D(R_f) \leq \mathrm{L}(f)$

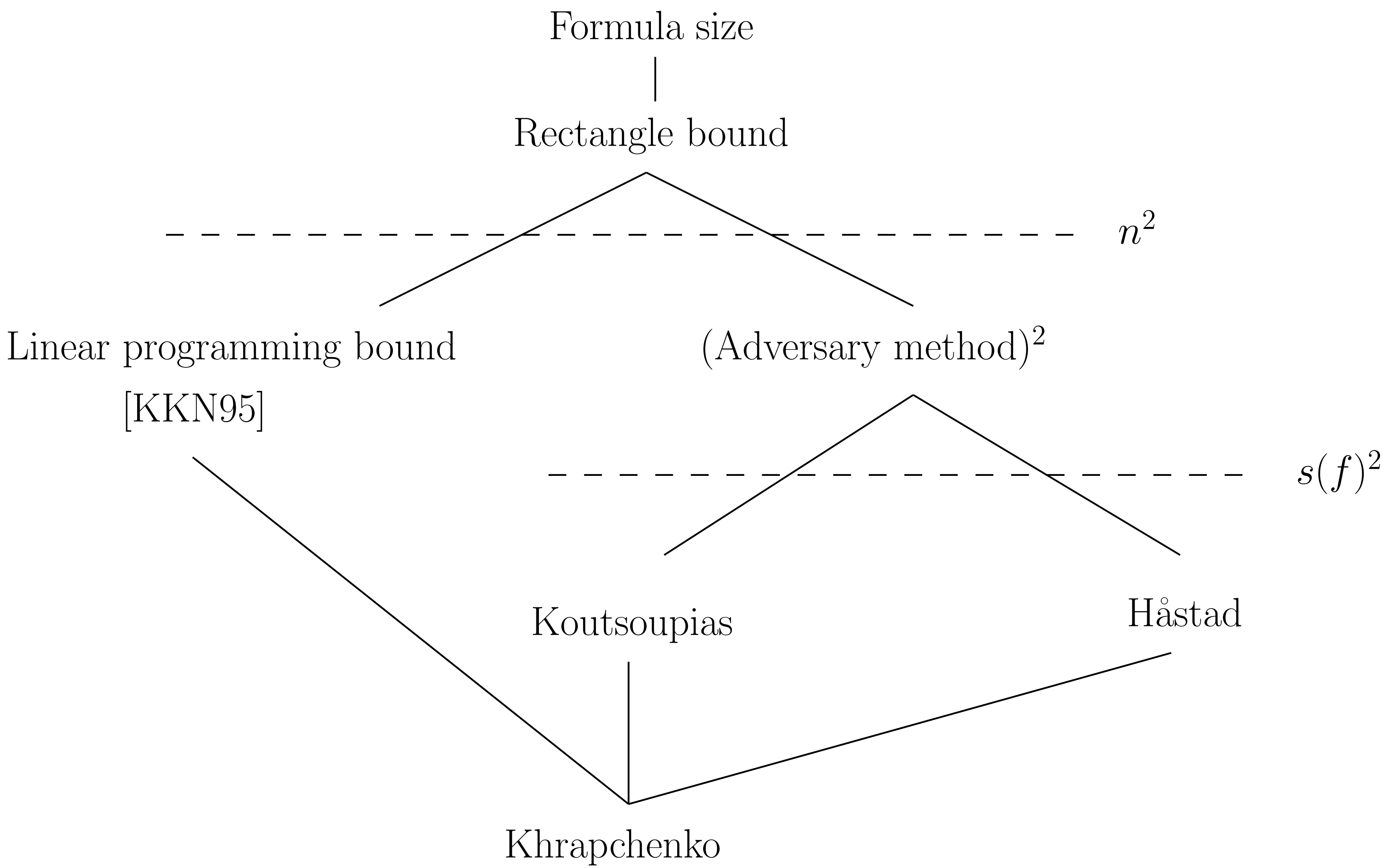
- It turns out that $\mathrm{adv}(f)$ is a lower bound on the quantum query complexity of f [Barnum, Saks, and Szegedy, 03]

More on the quantum adversary method

- The quantity adv(f) emerged over several years [Ambainis 02, Amb03, BSS03, Laplante and Magniez 04] in the context of quantum query complexity. Its many formulations were shown equivalent by [Špalek and Szegedy 05].

- It further follows from [ŠS05] that adv(f) can be computed in time polynomial in the size of the truth table of f, by reduction to semidefinite programming.

- Like some other bounds arising from semidefinite programming, the adversary method behaves very nicely under composition: in fact, adv(f^k) $=$ (adv(f))^k for any Boolean function f [Amb03, LLS05].


Formula size
Rectangle bound
n^2
Linear programming bound
[KKN95]
(Adversary method)^2
$s(f)^2$
Koutsoupias
Håstad
Khrapchenko

Open problems

- Is quantum query complexity squared a lower bound on formula size?

- Is approximate polynomial degree squared a lower bound on formula size?

- How does the linear programming bound of [Karchmer, Kushilevitz, and Nisan 95] relate to the adversary method?

- Are the rectangle bound and formula size polynomially related?