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

- A million dollar question: Show an explicit function which requires superpolynomial size circuits!

- For functions in NP the best circuit lower bound we know is $5n - o(n)$ [LR01, IM02]

- The smallest complexity class we know to contain a function requiring superpolynomial size circuits is MAEXP! [BFT98]

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 is its number of leaves.

- PARITY has formula size $\theta(n^2)$ [Khr71].

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

- The best lower bound for a function in NP is $n^{3-o(1)}$ [Hås98].

An Aside: Lower Bound Philosophy

- Let's look at our job as computer scientists from the point of view of computer scientists.

- How difficult is the problem of proving lower bounds?

- We will consider a lower bound technique efficient if it can be computed in time polynomial in the size of the truth table of f.

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

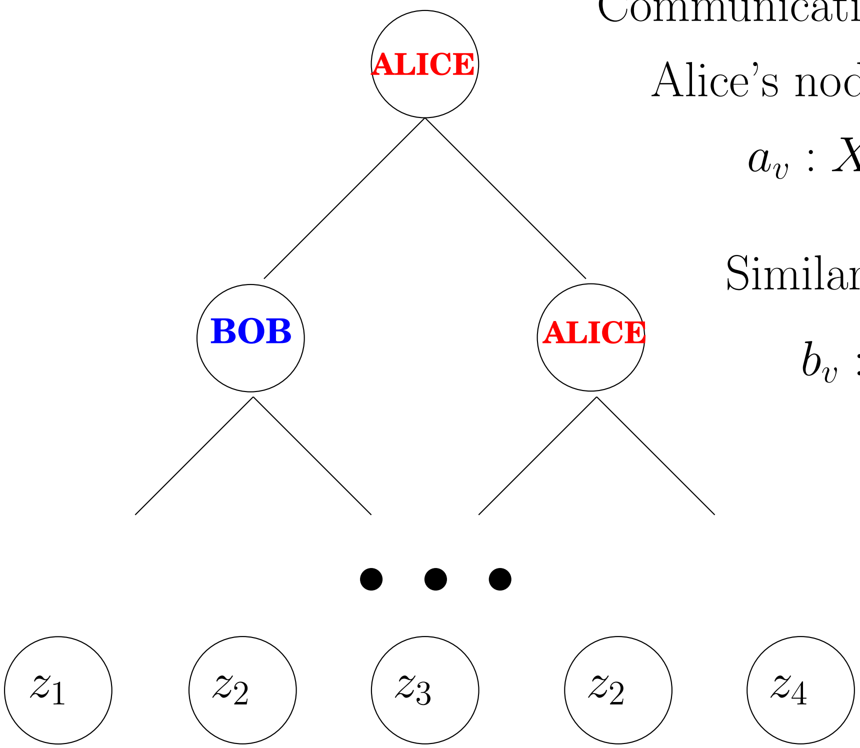
$$R_f = \{(x,y,i) : x \in X,\ y \in Y,\ x_i \neq y_i\}$$

- 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:

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

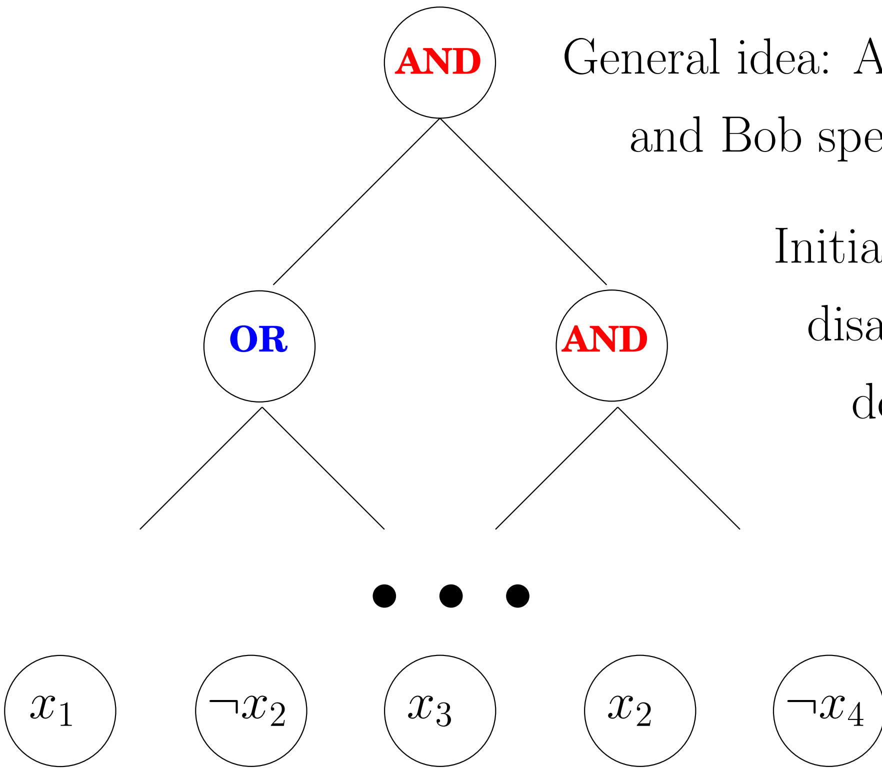
Similarly, Bob's nodes labelled

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

Leaves labelled by elements $z \in Z$.

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

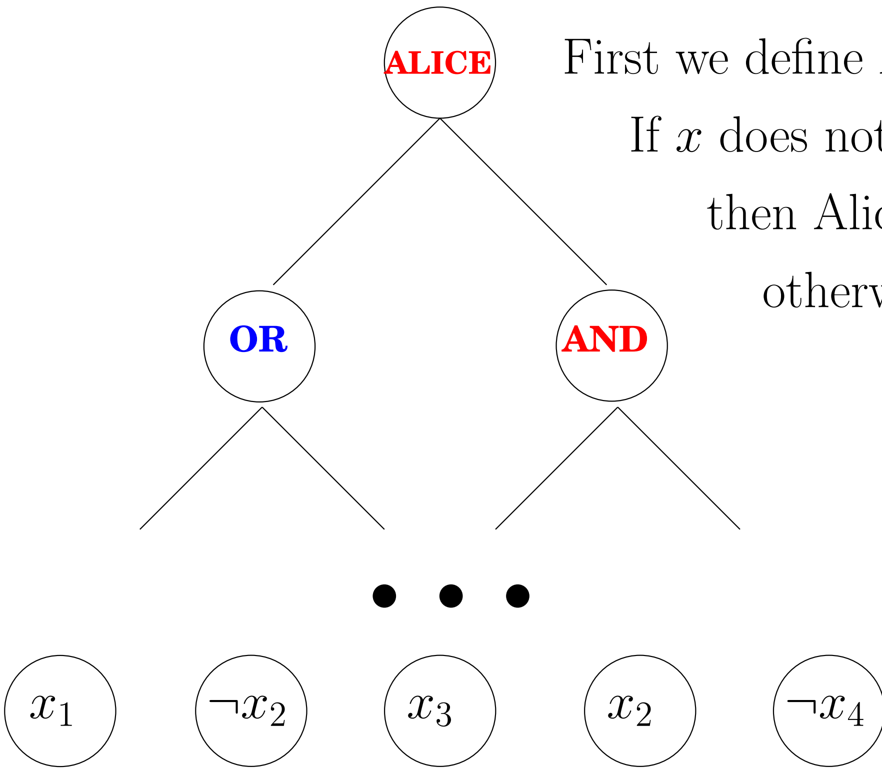
Proof by picture: $C^P(R_f) \leq \mathrm{L}(f)$.



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

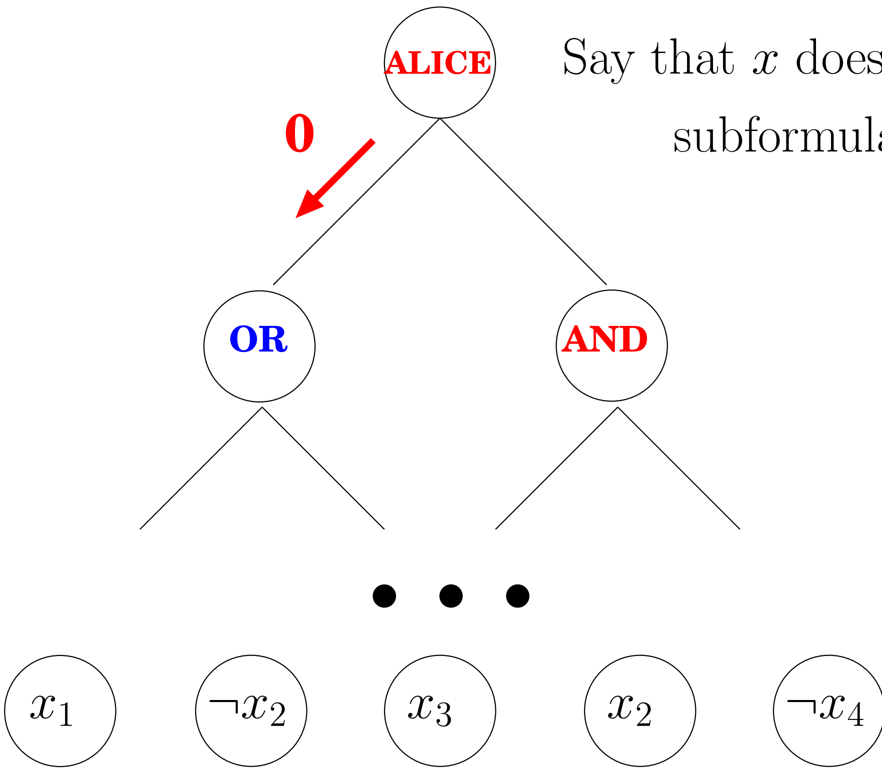
Initially, $f(x) \neq f(y)$ and we maintain this disagreement on subformulas as we move down the tree.

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



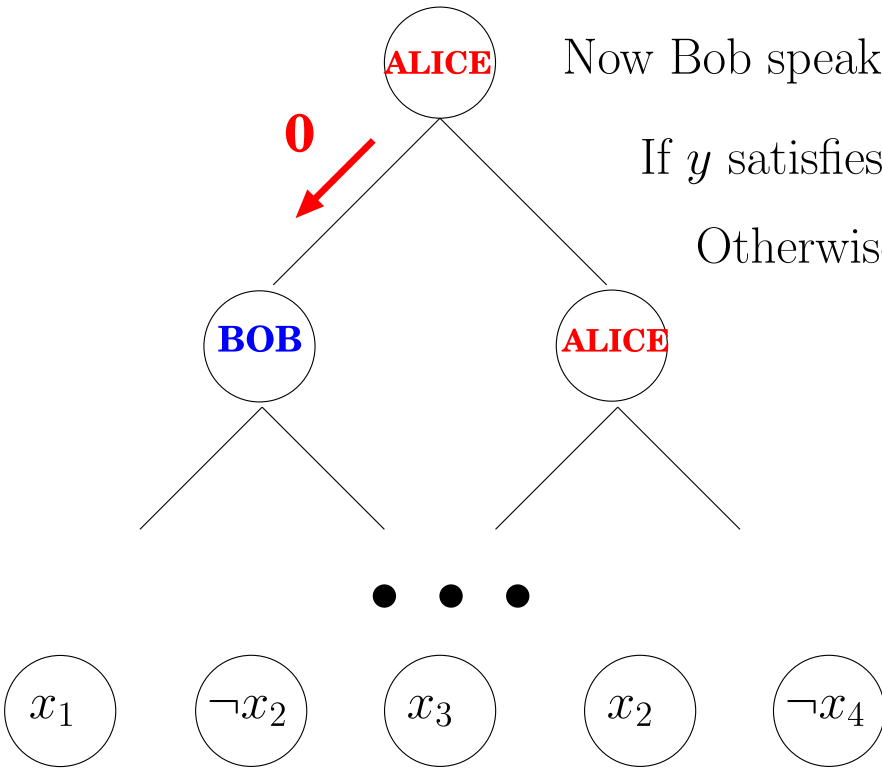
First we define Alice's action at the top node:
If x does not satisfy the left subformula,
then Alice sends the bit 0;
otherwise she sends the bit 1.

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



Say that x does not satisfy the left subformula.

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

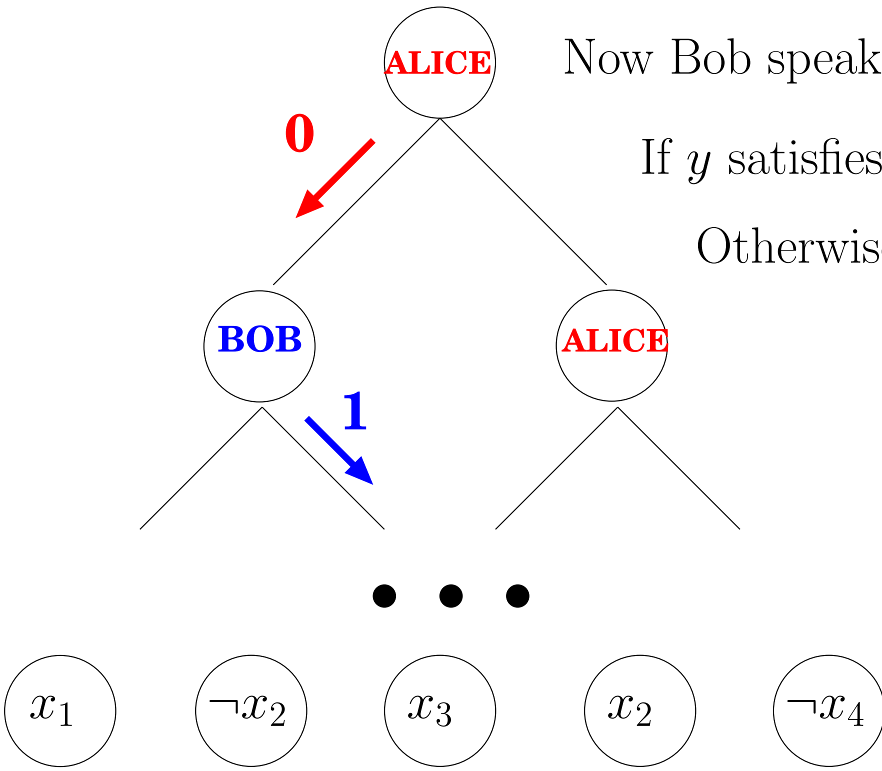


Now Bob speaks at the OR gate:

If y satisfies the left subformula, Bob says 0.

Otherwise, he says 1.

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

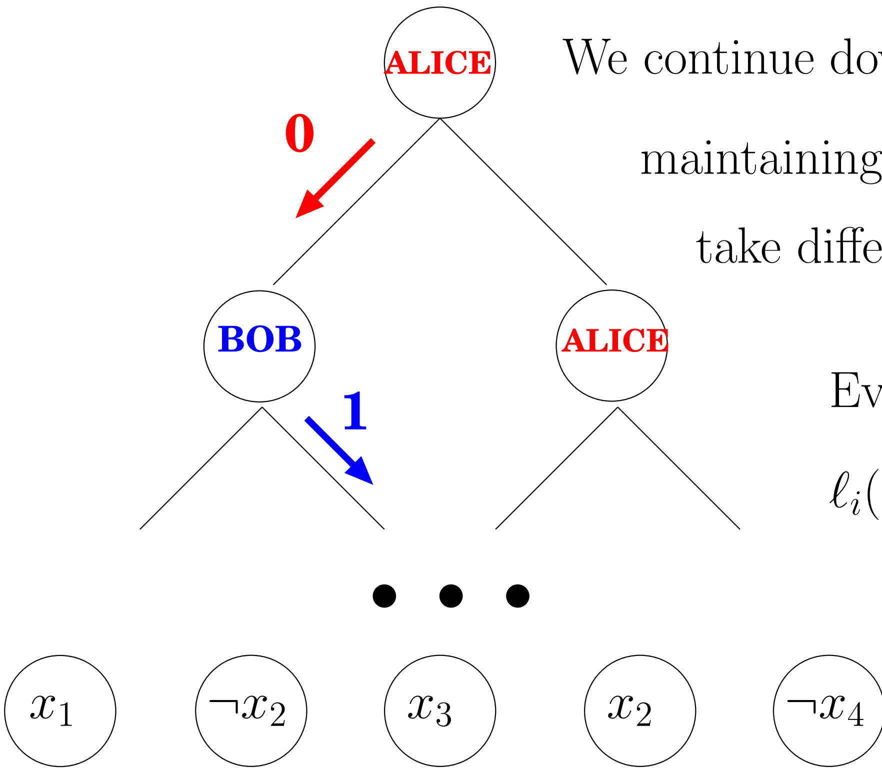


Now Bob speaks at the OR gate:

If y satisfies the left subformula, Bob says 0.

Otherwise, he says 1.

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

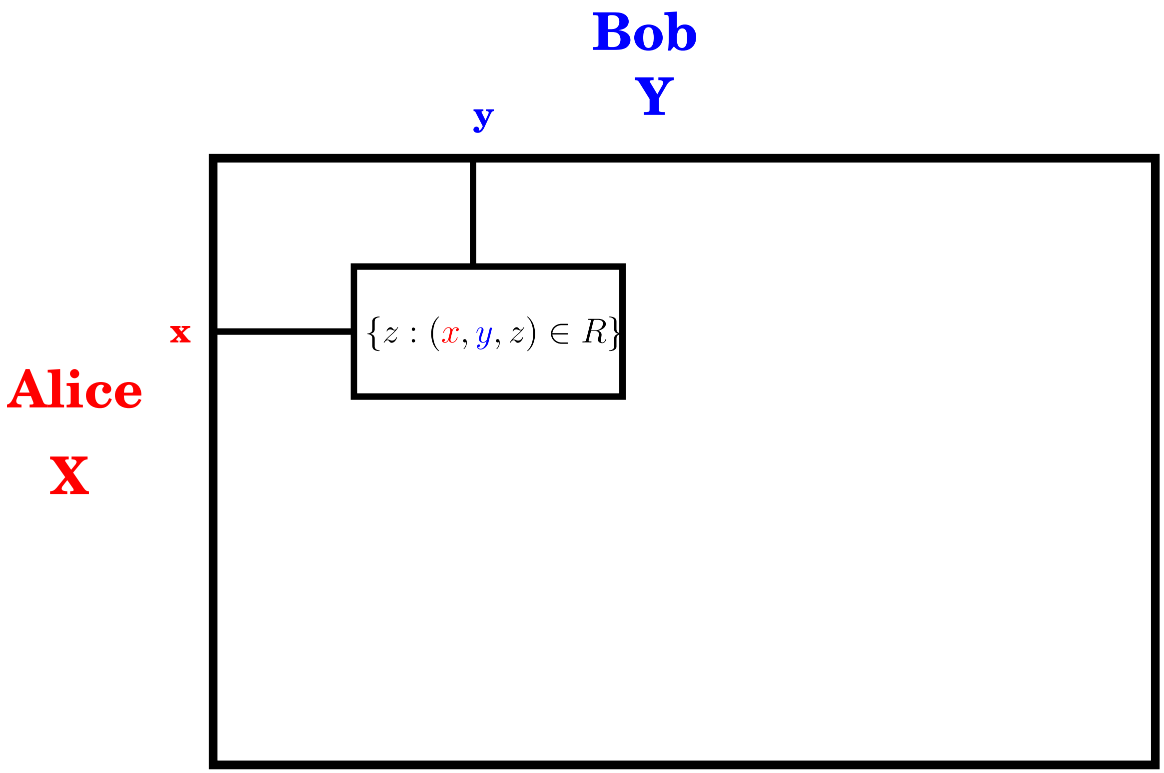


We continue down the tree in a similar fashion, maintaining the property that x and y take different values on subformulas.

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.

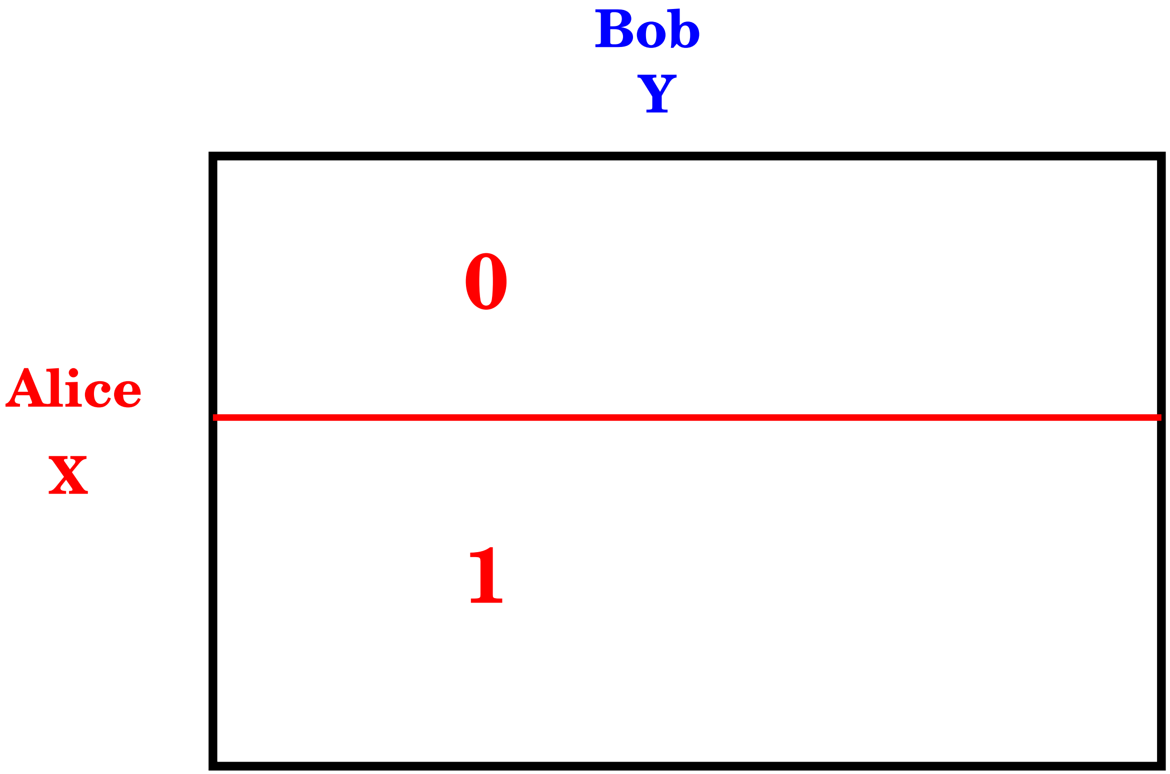
Communication Complexity and the Rectangle Bound

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



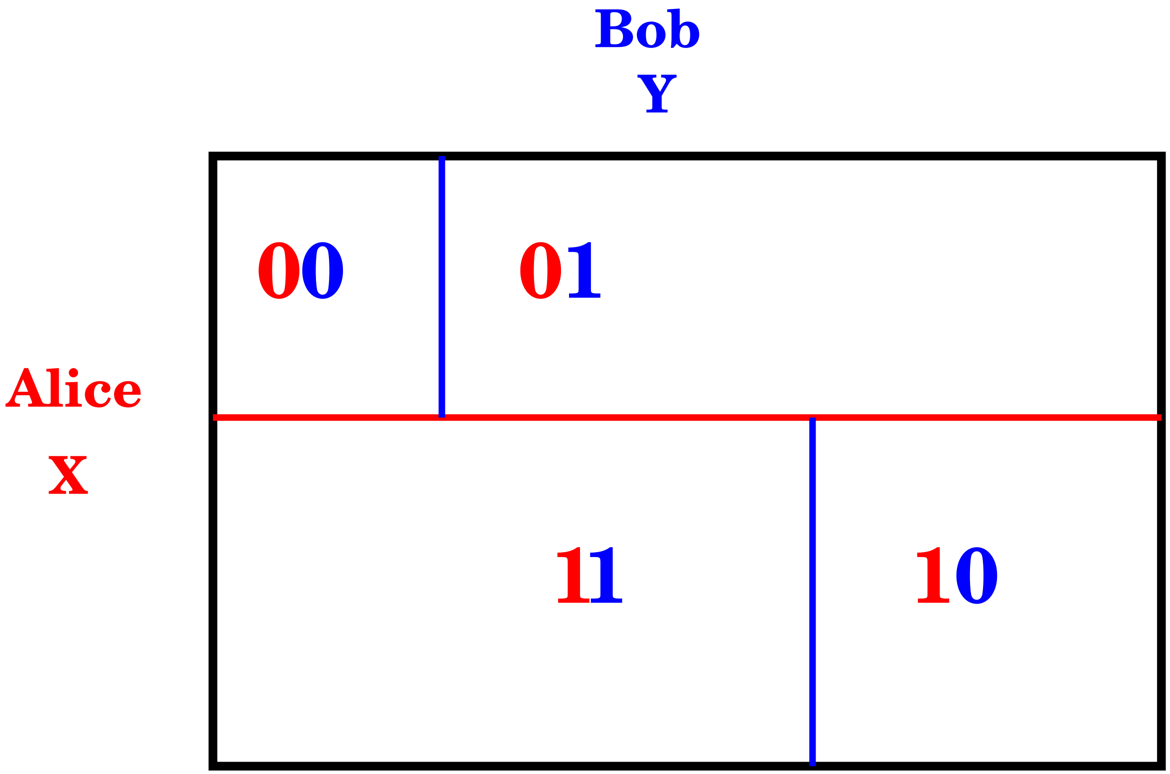
Communication Complexity and the Rectangle Bound

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



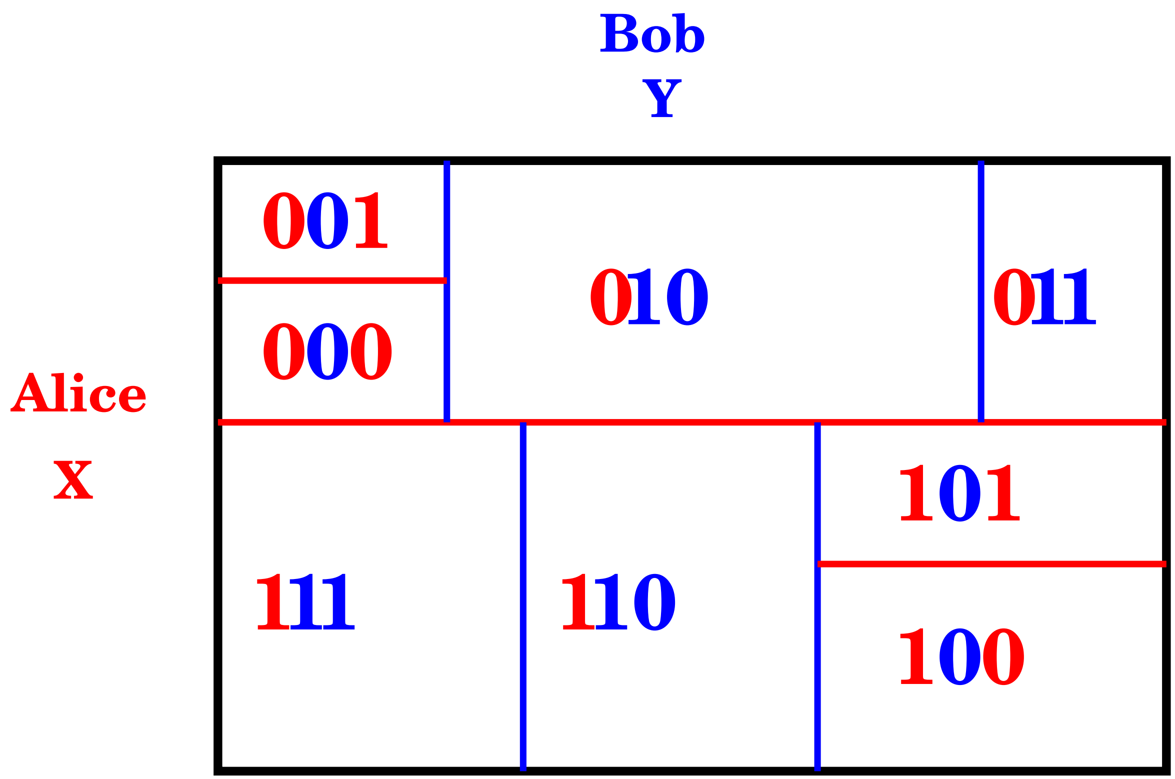
Communication Complexity and the Rectangle Bound

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



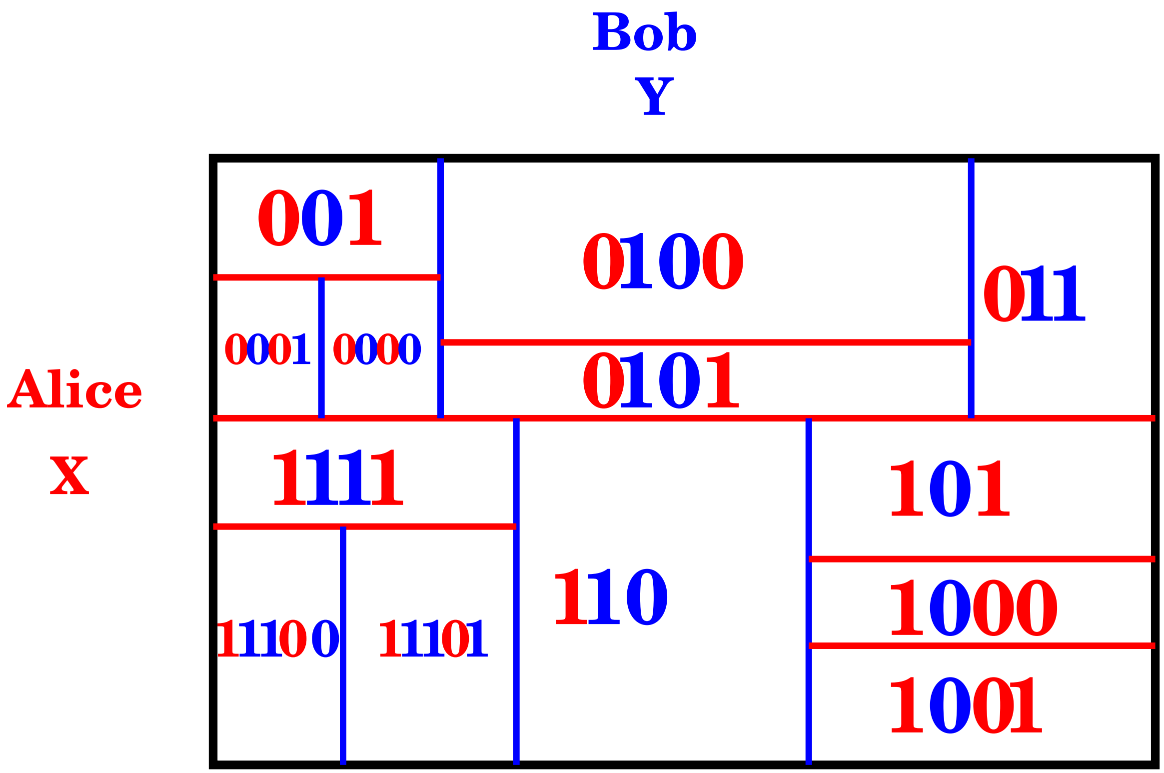
Communication Complexity and the Rectangle Bound

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



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

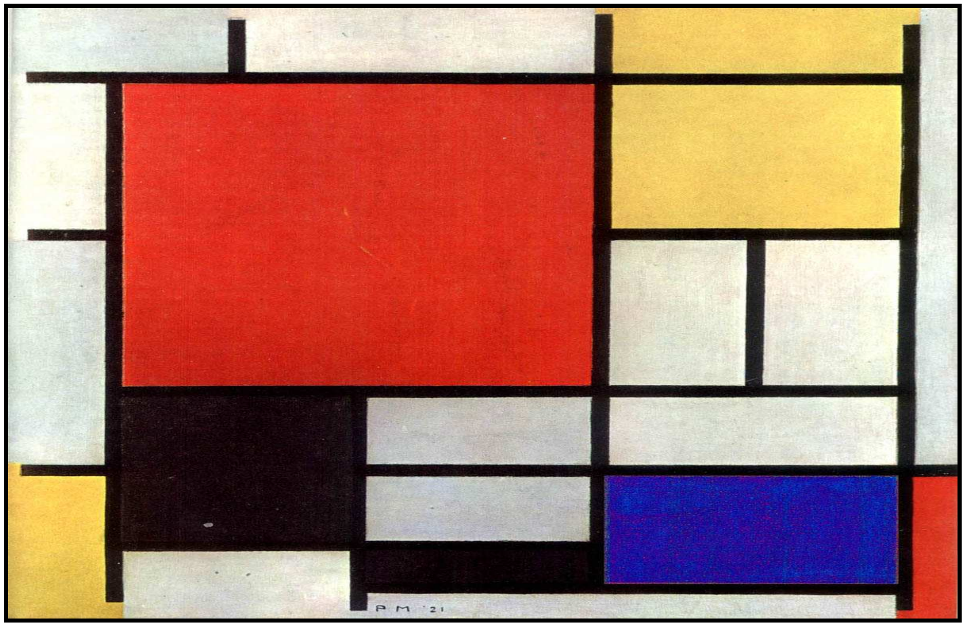
$$R \subseteq X \times Y \times Z$$

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, $C^D(R) \leq C^P(R)$.

- The rectangle bound is a purely combinatorial quantity.

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

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

- Major drawback—it is NP hard to compute.

Approximating the rectangle bound

- We will see that a measure on rectangles satisfying two properties, subadditivity and monotonicity, can be used to lower bound the rectangle bound.

- Several previous methods fit into this framework, including the rank method of Razborov [Raz90], and a probability on rectangles method (called B_* in Kushilevitz and Nisan).

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

An example: the rank method of Razborov

We know that $\mathrm{rk}(A+B) \leq \mathrm{rk}(A) + \mathrm{rk}(B)$ for any two matrices A, B. Thus if $\mathcal{R}$ is an optimal monochromatic rectangle partition of R_f, then

$$\max_A \frac{\mathrm{rk}(A)}{\max_{R \in \mathcal{R}} \mathrm{rk}(A_R)} \leq C^D(R_f) \leq \mathrm{L}(f).$$

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

An example: the rank method of Razborov

We now use the monotonicity property. As the rectangles are monochromatic, each rectangle R is a subset of $D_i = \{(x,y) : x \in X, y \in Y, x_i \neq y_i\}$, for some $i \in [n]$. For this i we have $\mathrm{rk}(A_R) \leq \mathrm{rk}(A \circ D_i)$. Thus

$$\max_A \frac{\mathrm{rk}(A)}{\max_i \mathrm{rk}(A \circ D_i)} \leq C^D(R_f) \leq \mathrm{L}(f).$$

Razborov uses this method to show superpolynomial *monotone* formula size lower bounds. He also shows, however, it is trivial for regular formula size [Raz92].

Our main lemma: spectral norm squared is subadditive

- Spectral norm has several equivalent formulations. We will use:

$$\|A\|_2 = \max_{u,v\,:|u|_2=|v|_2=1} |u^T A v|$$

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

$$\|A\|_2^2 \leq \sum_{R \in \mathcal{R}} \|A_R\|_2^2.$$

- Note that it is not true in general that $\|A+B\|_2^2 \leq \|A\|_2^2 + \|B\|_2^2$.

Proof of main lemma

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

$$\|A\|_2 \;=\; |u^T A v| = |u^T (\sum_{R \in \mathcal{R}} A_R) v|$$

Proof of main lemma

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

$$\begin{aligned} \|A\|_2 &= |u^T Av| = |u^T (\sum_{R \in \mathcal{R}} A_R) v| \\ &\leq \sum_{R \in \mathcal{R}} |u^T A_R v| \end{aligned}$$

Proof of main lemma

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

$$\begin{aligned} \|A\|_2 &= |u^T A v| = |u^T (\sum_{R \in \mathcal{R}} A_R) v| \\ &\leq \sum_{R \in \mathcal{R}} |u^T A_R v| \\ &\leq \sum_{R \in \mathcal{R}} \|A_R\|_2 \, |u_R|_2 \, |v_R|_2 \end{aligned}$$

Proof of main lemma

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

$$\begin{aligned}
\|A\|_2 &= |u^T Av| = |u^T(\sum_{R\in\mathcal{R}} A_R)v| \\
&\leq \sum_{R\in\mathcal{R}} |u^T A_R v| \\
&\leq \sum_{R\in\mathcal{R}} \|A_R\|_2 \ |u_R|_2 \ |v_R|_2 \\
&\leq \sqrt{\sum_{R\in\mathcal{R}} \|A_R\|_2^2}\sqrt{\sum_{R\in\mathcal{R}} |u_R|_2^2|v_r|_2^2}
\end{aligned}$$

Proof of main lemma

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

$$
\begin{aligned}
\|A\|_2 &= |u^T Av| = |u^T(\sum_{R\in\mathcal{R}} A_R)v| \\
&\leq \sum_{R\in\mathcal{R}} |u^T A_R v| \\
&\leq \sum_{R\in\mathcal{R}} \|A_R\|_2 \; |u_R|_2 \; |v_R|_2 \\
&\leq \sqrt{\sum_{R\in\mathcal{R}} \|A_R\|_2^2}\sqrt{\sum_{R\in\mathcal{R}} |u_R|_2^2 |v_R|_2^2} \\
&= \sqrt{\sum_{R\in\mathcal{R}} \|A_R\|_2^2}.
\end{aligned}
$$

Applying the lemma

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

$$\max_A \frac{\|A\|_2^2}{\max_{R \in \mathcal{R}} \|A_R\|_2^2} \leq C^D(R_f).$$

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 $\|A_R\|_2 \leq \|A \circ D_i\|_2$

- Thus we obtain

$$\max_A \frac{\|A\|_2^2}{\max_i \|A_i \circ D_i\|_2^2} \leq C^D(R_f) \leq \mathrm{L}(f).$$

- We now have a bound which can be computed in time polynomial in the truth table of f

The quantum adversary method emerges

Define

$$\mathrm{sumPI}(f) = \max_A \frac{\|A\|_2}{\max_i \|A_i \circ D_i\|_2}$$

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

- It turns out that $\mathrm{sumPI}(f)$ is a lower bound on the quantum query complexity of f! [BSS03]

- The quantity $\mathrm{sumPI}(f)$ has emerged over several years [Amb02, Amb03, BSS03, LM04] in the context of quantum query complexity, and has many nice properties and equivalent formulations [ŠS05].

More on the quantum adversary method

- The name sumPI comes from the following equivalent min max formulation

$$\mathrm{sumPI}(f) = \min_p \max_{x \in X, y \in Y} \frac{1}{\sum_{i: x_i \neq y_i} \sqrt{p_x(i) p_y(i)}}$$

- Using both the max min and min max formulations appropriately makes it easy to give exact characterizations of $\mathrm{sumPI}(f)$.

- For example, one can show $\mathrm{sumPI}(f)$ behaves very well under composition: $\mathrm{sumPI}(f^k) = (\mathrm{sumPI}(f))^k$ for any Boolean function f [Amb03, LLS05].

Khrapchenko's Method

- Define a bipartite graph, with left hand side a subset of $f^{-1}(0)$ and right hand side $f^{-1}(1)$.

- Connect x, y with an edge if they have Hamming distance 1

- Khrapchenko's bound is the product of the average degree of the left hand side with the average degree on the right hand side.

Generalizing Khrapchenko's Method

$$\max_{p_0, p_1, q} \min_{x,y} \frac{p_0(x) p_1(y)}{q^2(x,y)} \leq C^D(R_f) \leq \mathrm{L}(f)$$

- Define the matrix $A[x,y] = q(x,y)/\sqrt{p_0(x)p_1(y)}$.

- Then $\|A\|_2 \geq 1$.

- Each matrix $A \circ D_i$ has at most one entry in each row and column.

- Thus $\|A \circ D_i\|_2 \leq \max_{x,y} q(x,y)/\sqrt{p_0(x)p_1(y)}$.

Open problems

- Is quantum query complexity squared a lower bound on formula size?
- How about approximate polynomial degree?
- Are the rectangle bound and formula size polynomially related?
- How large is the rectangle bound for a random function?