Nonlocal games and low-depth circuits

NATHAN JU

Can we **unconditionally** show that quantum circuits are more powerful than classical circuits?

IS THERE A TASK SOLVABLE ONLY BY QUANTUM CIRCUITS?

Bravyi, Gosset, Konig [2017]: Yes! A low-depth classical circuit will fail on *at least one input*, and a low-depth

Le Gall [2019] ail on *almost all inputs*.

Proofs of hardness based on well-known nonlocal games.

Bravyi, Gosset, Konig, Tomamichel [2019]: Even a *noisy* quantum circuit will beat a *noiseless* classical circuit.

Watts, Kothari, Schaeffer, Tal [2019]: A *more powerful type of classical circuit* will fail on many inputs, while a quantum circuit always succeeds.

Grier, Schaeffer [2019]: An ***even more*** powerful type of classical circuit will fail on many inputs, while a quantum circuit always succeeds.

The general recipe: Bounds from algorithms

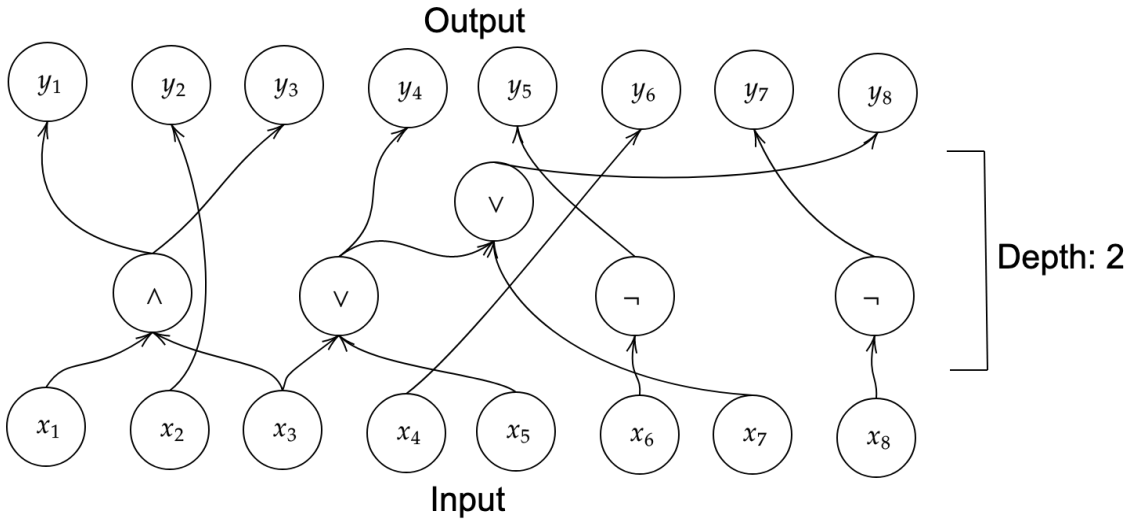
1. Suppose we could use a classical circuit to solve some task with probability p.

2. If p is too high, then we can create a classical algorithm/strategy for a nonlocal game that succeeds with impossibly high probability. (The "algorithm")

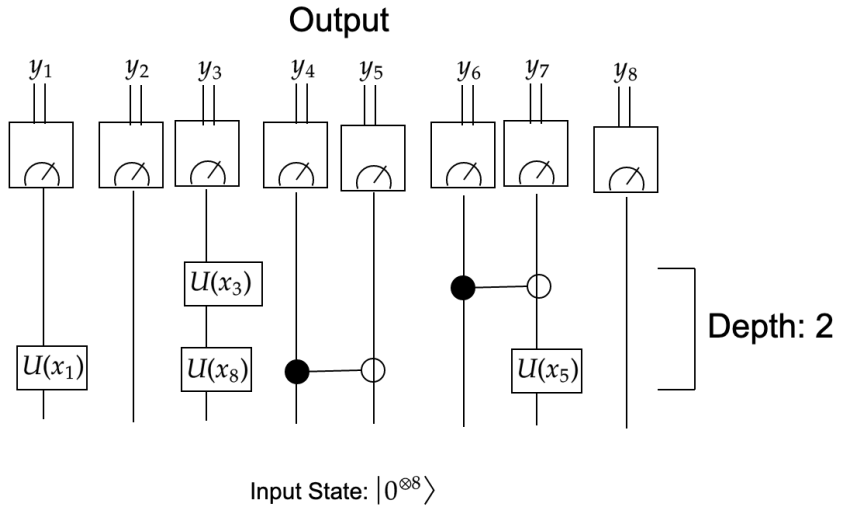
3. So p must be small. (The "bound")

What are low-depth circuits?

Classical low-depth circuit
Input *x* manipulated by logical operations



Quantum low-depth circuit
Input *x* determines unitaries to perform



Depth: *O(1)*

Magic Square Game

x_{11}	x_{12}	x_{13}
x_{21}	x_{22}	x_{23}
x_{31}	x_{32}	x_{33}

$x_{11}x_{12}x_{13} = +1$

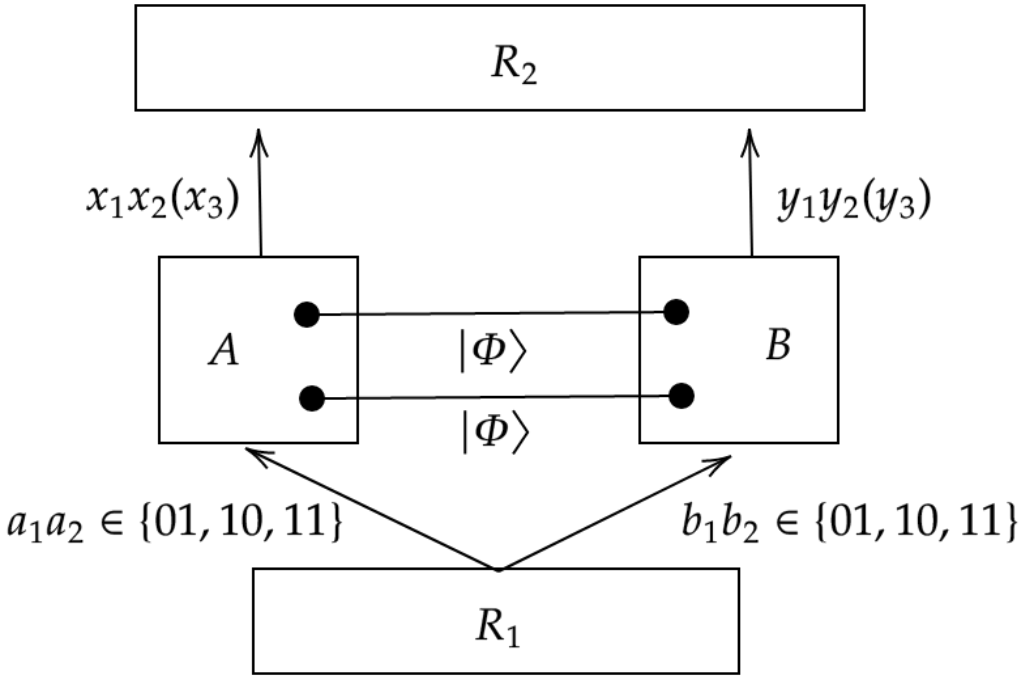
$x_{12}x_{22}x_{32} = -1$

No classical strategy can do better than 8/9 over uniform input.

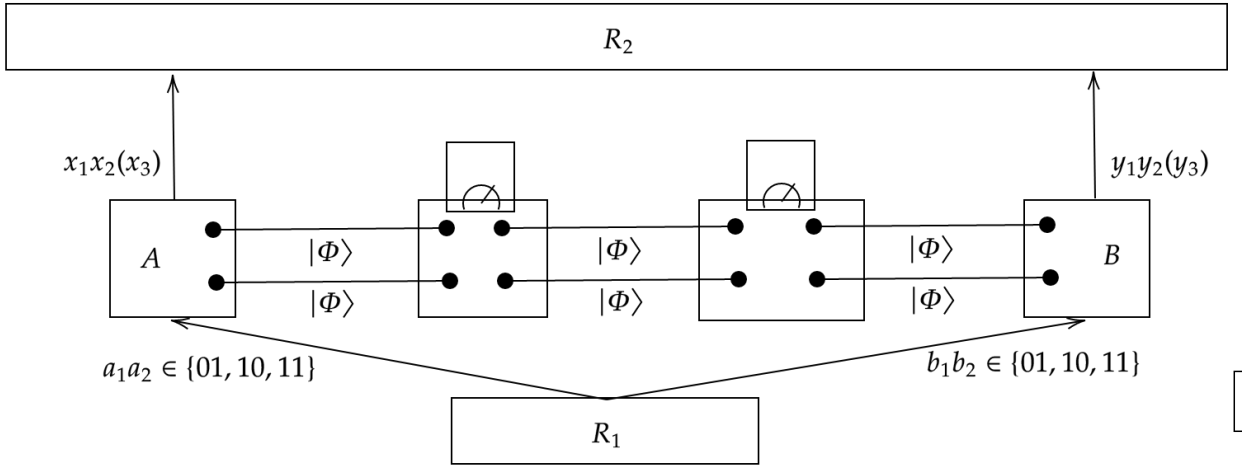
$X \otimes X$	$Y \otimes Z$	$Z \otimes Y$
$Y \otimes Y$	$Z \otimes X$	$X \otimes Z$
$Z \otimes Z$	$X \otimes Y$	$Y \otimes X$

This quantum strategy succeeds deterministically.

The Quantum Strategy

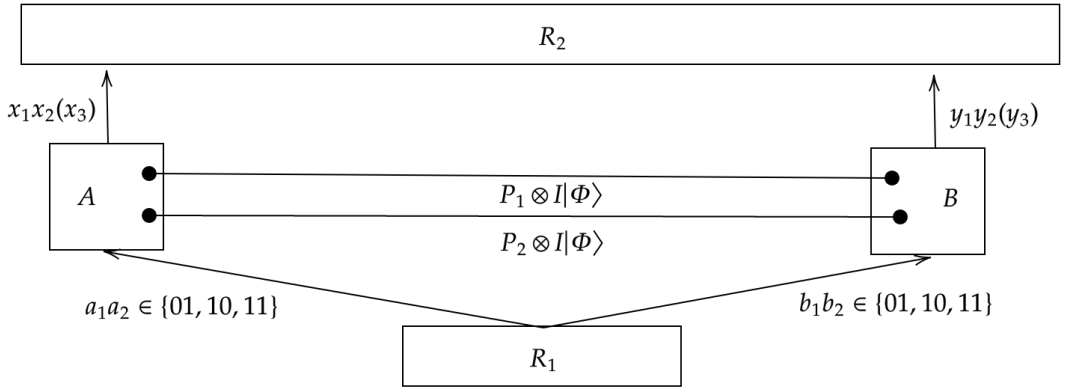


Quantum Strategy via Entanglement Swapping

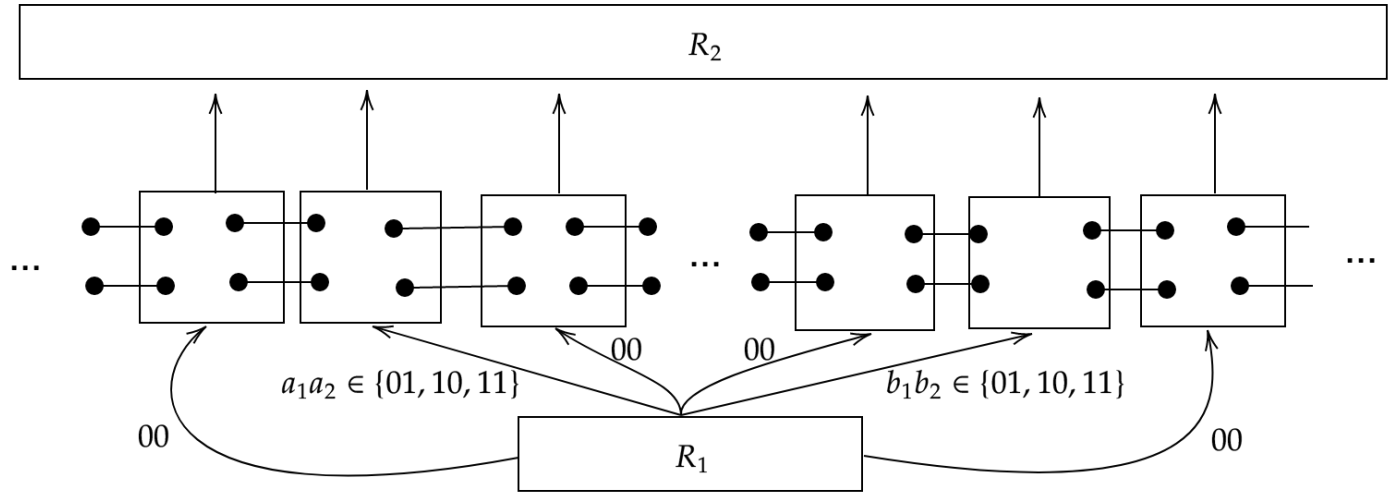


Alice and Bob can win the Magic Square Game if they know the measurement outcomes in the middle

This is equivalent to:



The task solved by low-depth quantum circuit



Referee randomly choses sites *i* and *j* and sends Magic Square input

Referee sends every other site *00* to indicate entanglement swap

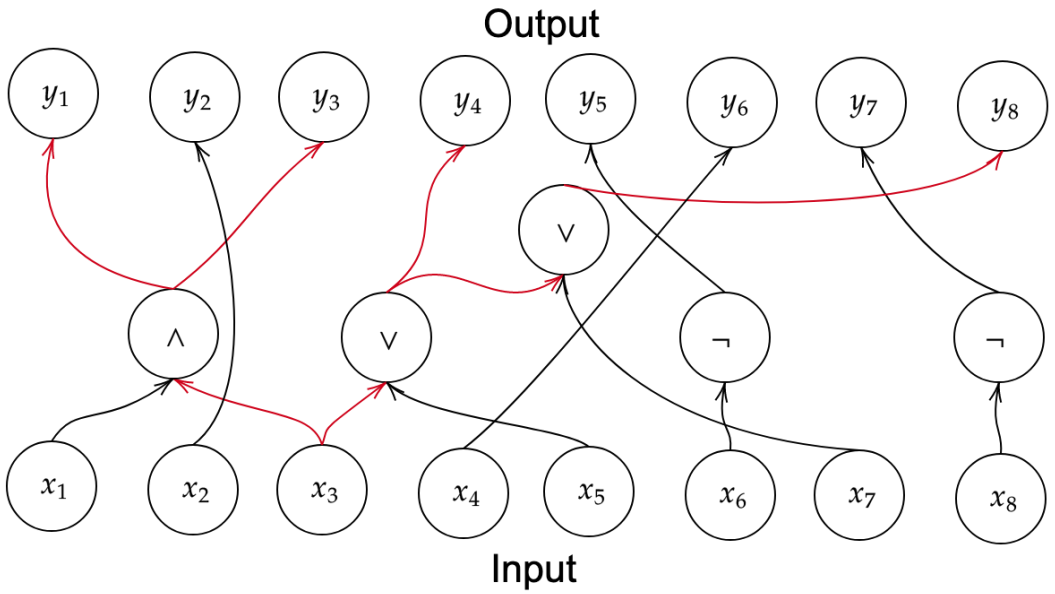
Sites follow corresponding protocol and output measurements

Task to solve: Given *{0,1}*-string of the form above, output any outcome that occurs with non-zero probability

How well can a low-depth classical circuit solve this problem?

(BOUNDED FAN-IN CIRCUIT)

Inputs have small "influence"



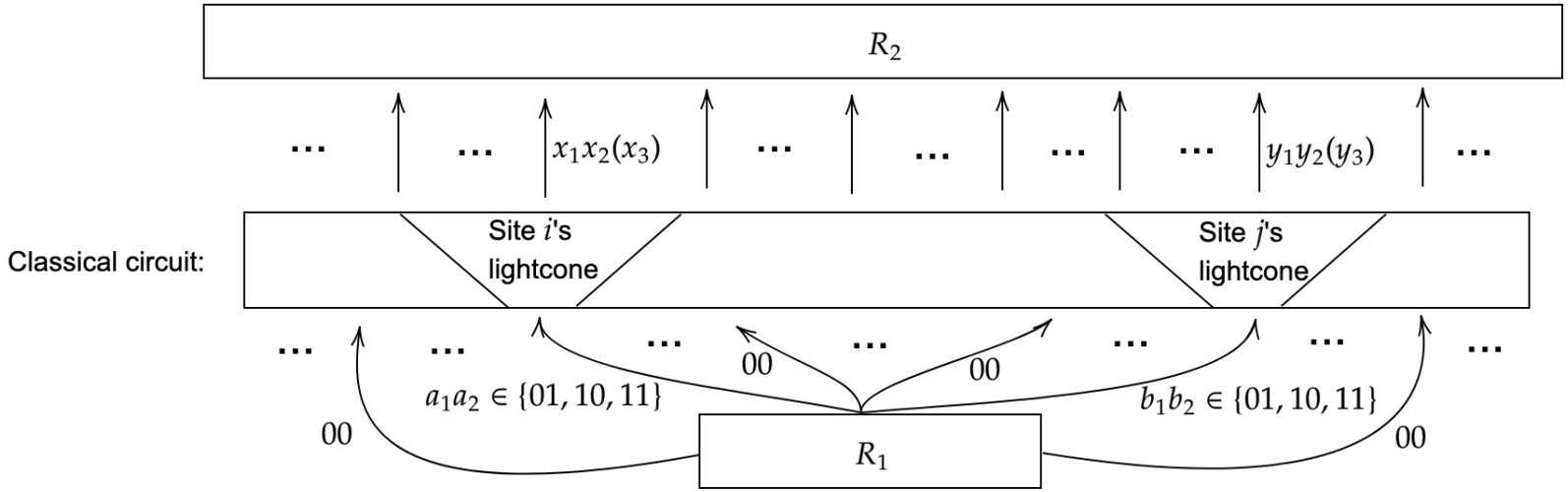
Lightcone *(L)* of an input bit is the set of output bits that it influences

$$L(x_3) = \{y_1, y_3, y_4, y_8\}$$

Most input bits have small lightcones

$$|L(x_2)| = |L(x_4)| = |L(x_6)| = |L(x_7)| = |L(x_8)| = 1$$

Small lightcones in the generalized Magic Square Game

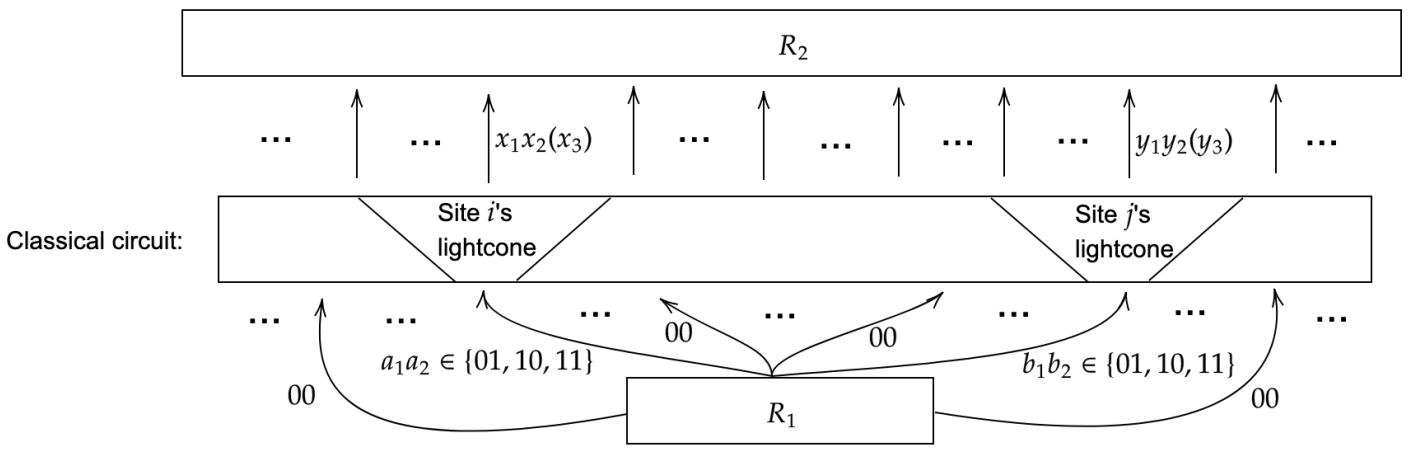


1. Suppose the output of this classical circuit matches the quantum circuit "with probability p"

2. Then the output has Alice and Bob's outcomes, along with the entanglement swap outcomes between them. Recall A/B can win Magic Square game if they know these swap outcomes.

3. Given site i's input, one can calculate every output except for site j's lightcone (vice versa)

The "algorithm" (classical strategy) for Magic Square game



1. Alice and Bob each take a copy of the circuit
2. Alice (Bob) receives inputs a_1a_2 (b_1b_2)
3. Alice (Bob) inserts inputs to site *i (j)* and *00* elsewhere except site *j (i)*
4. Alice (Bob) extracts entanglement swap outputs and $x_1x_2(x_3)$ $(y_1y_2(y_3))$
5. Alice and Bob correct outputs using swap outcomes outside of each other's lightcones

The "bound"

So the probability of the classical circuit's success, *p,* can't be too large. Otherwise, Alice and Bob can win the Magic Square game with impossibly high probability.

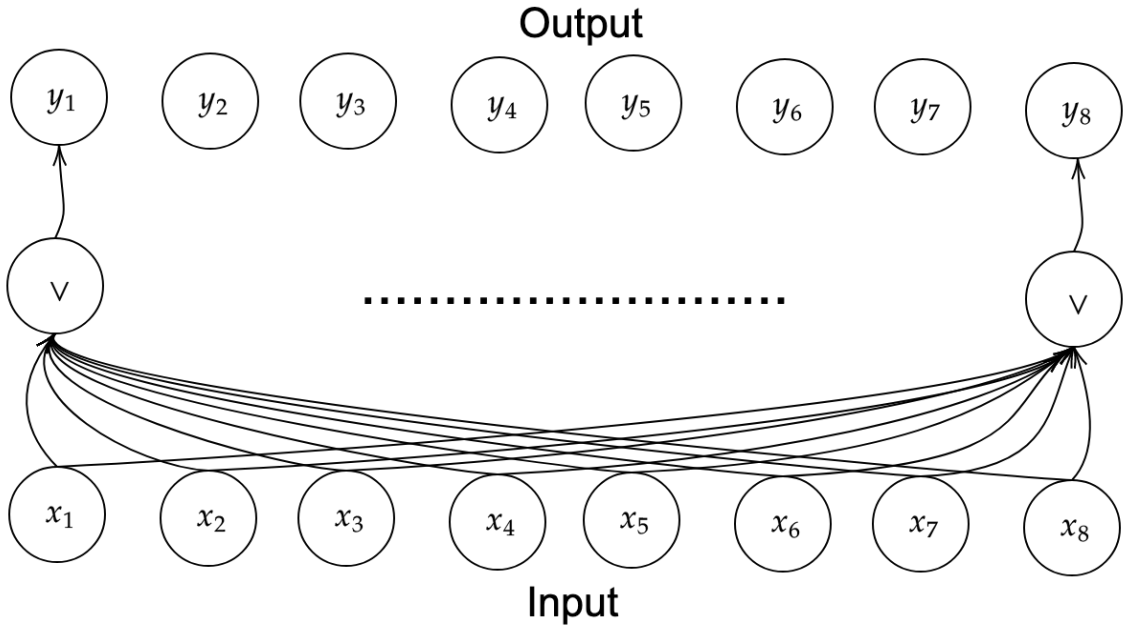
Punchline: A classical circuit of *low-depth* and *bounded fan-in* has low locality (output bits are dependent on very few inputs).

Low locality circuits have independent lightcones.

Independent lightcones give independent strategies for nonlocal games.

How well can classical **unbounded fan-in** do on nonlocal tasks?

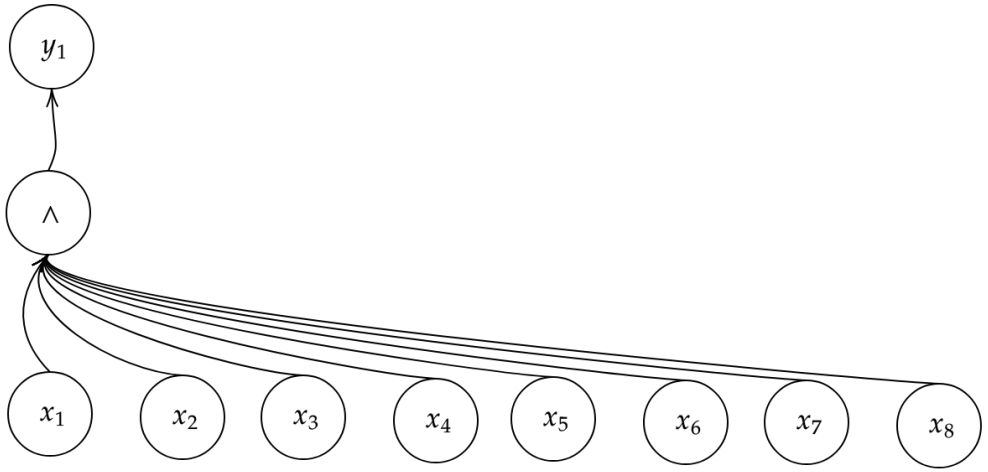
The "more powerful" classical circuit: unbounded fan-in



At a first approximation, it seems that unbounded fan-in circuits have high locality.

Low locality hidden in unbounded fan-in circuits

But there is something peculiar about locality with logical AND and logical OR



Conditioned on one input bit being 0, the output no longer depends on other inputs

Hastad's Switching Lemma

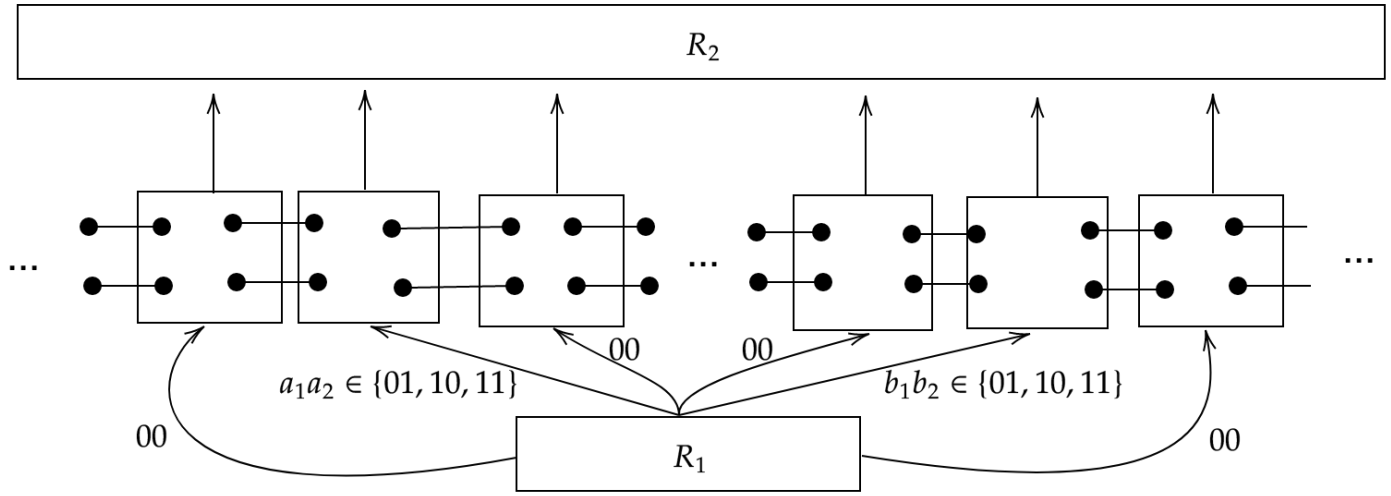
Hastad formalized this idea in 1987 with his celebrated "switching lemma"

Basically, by fixing some inputs to a *0* or *1* in a "random restriction", the unbounded fan-in circuit has low locality (outputs depend on few inputs)

Recent generalizations of the switching lemma to **multi-output** functions, the setting of non-local games

Generalized Magic Square game does not work for random restrictions

At a first glance, the previous nonlocal game, generalized Magic Square, is not adaptable to a random restriction



Most sites need to be all *00*

A nonlocal game more friendly to random restrictions: PHP

n-player Parity Halving Problem:

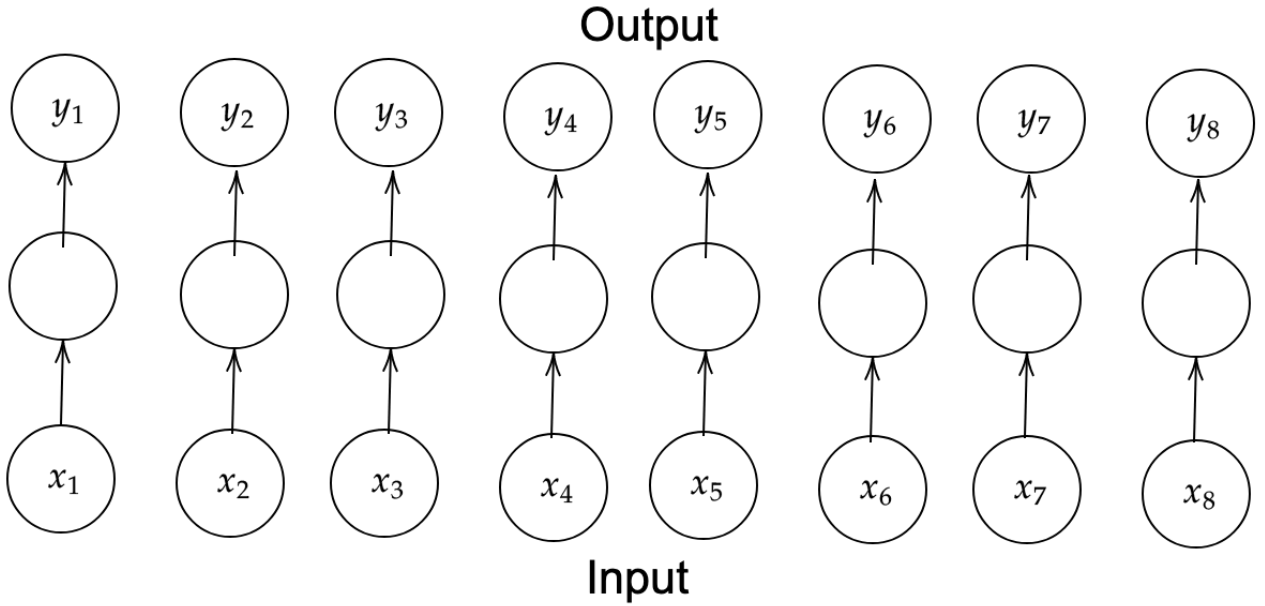
1. Each of *n* players receives a bit from even weight $x = x_1 x_2 \ldots x_n$
2. Each player outputs a bit of $y = y_1 y_2 \ldots y_n$
3. Players win if and only if $|y| \equiv |x|/2 \mod 2$

$$\frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$$

Deterministic quantum strategy: *n* players share a GHZ state. Measure in the Y-basis if receiving a 1. Otherwise, measure in the X-basis.

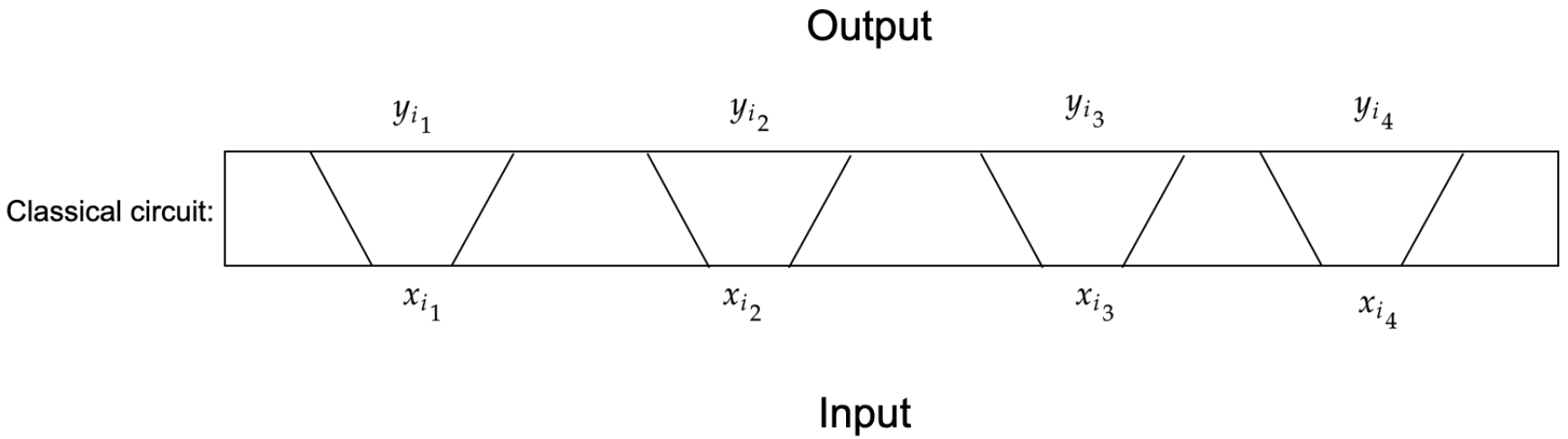
Classical strategy upper bound

No classical strategy can win with probability exceeding $\frac{1}{2} + 2^{-n/2}$ over uniformly random input



Bounded fan-in lightcone relations

First, consider how well a **bounded fan-in** circuit does on the task.



Due to low locality, there is some set S of input bits with independent lightcones

Classical strategy for |S|-player PHP

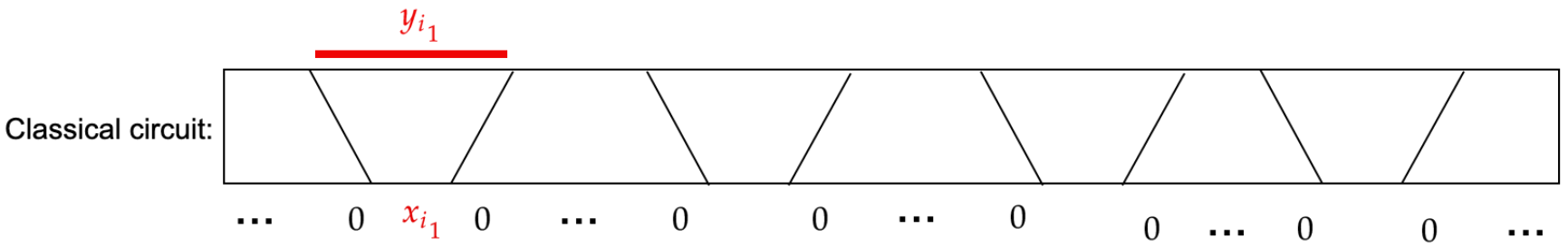
Suppose a classical circuit of **bounded fan-in** solves the *n*-player PHP w/p *p*

Strategy for |*S*|-player PHP:

1. Each of |*S*| players takes a copy of the circuit and is assigned an input variable in *S*
2. On input in *{0,1}* each player passes the input into their variable of the circuit and *0* for inputs outside of S
3. Each player evaluates the circuit and outputs the parity of the outputs in their lightcone

The "algorithm"

The classical strategy solves $|S|$-player PHP



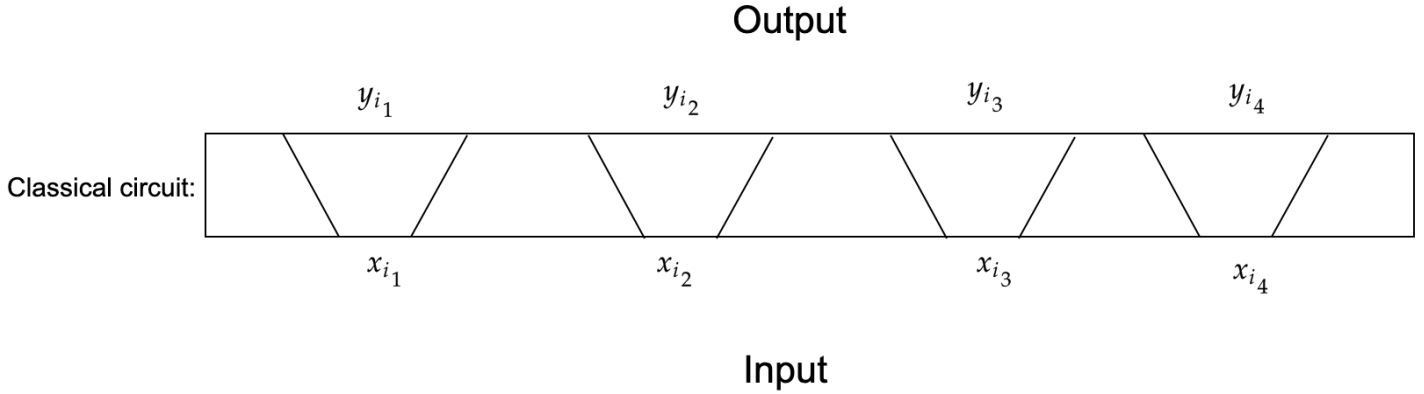
$$|y| \equiv |x|/2 \mod 2$$

So the probability p of success for a **bounded fan-in** circuit on the n-player PHP cannot be too high. (The "bound")

Unbounded fan-in circuits have low locality under random restriction

Recall the **switching lemma**: If we randomly restrict some input bits to values in *{0,1}*, then an **unbounded fan-in** circuit has low locality.

Low locality implies independent lightcones.



This is true *only* when input to circuit is consistent with random restriction

Classical strategy for unbounded fan-in circuit

Do the same thing as bounded fan-in, except each player also follows the random restriction wher

Classical ci

The punchline: Under a random restriction, an unbounded fan-in circuit has low locality.

A low locality circuit has independent lightcones.

Independent lightcones give classical strategies for nonlocal games.

So we can conclude that the classical **unbounded fan-in** circuit cannot do too well at this task.

The general theme (again): "Bounds from algorithms"

1. Suppose we could use a classical circuit to solve some task with probability p.

2. If p is too high, then we can create a classical algorithm/strategy for a nonlocal game that succeeds with impossibly high probability. (The "algorithm")

3. So p must be small. (The "bound")