Average-Case Quantum Advantage for Shallow Circuits

François Le Gall
Kyoto University

CCC'19
18 July 2019

Quantum Computational Complexity

Research on quantum algorithms (e.g., Shor's algorithm for integer factoring) gives strong evidence that quantum computation is more powerful than classical computation

Can we <u>prove</u> that quantum computation is more powerful than classical computation?

✓ Many proofs known for models like query complexity or communication complexity (lower bounds can be easily proven in these models)

✓ What about the "basic" models (Turing machines or, equivalently, circuits)?

BQP : class of Boolean functions that can be computed w.h.p. by (uniform) poly-size quantum circuits

➡ Relativized separations for complexity classes

[Bernstein and Vazirani 1993] $\exists$oracle O s.t. $\mathrm{BQP}^O \not\subseteq \mathrm{BPP}^O$

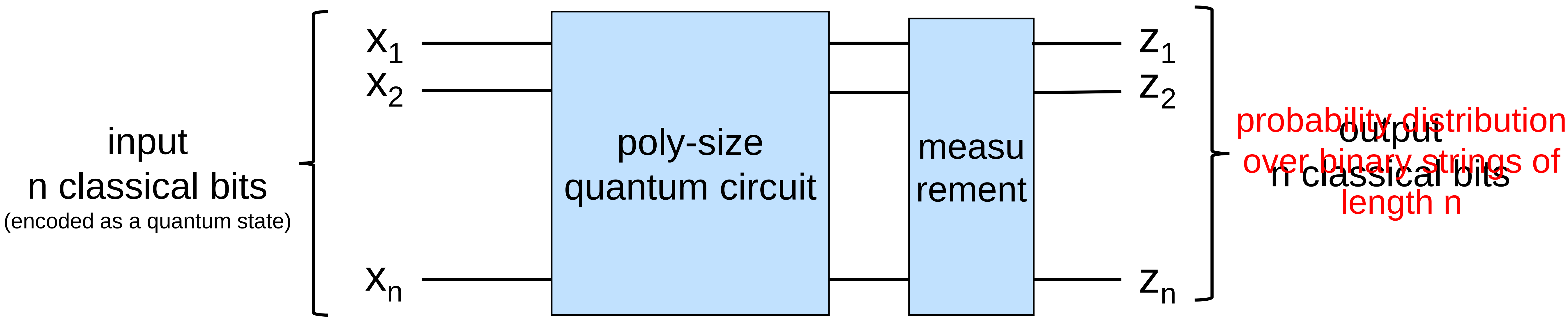
⋮

[Raz and Tal 2019] $\exists$oracle O s.t. $\mathrm{BQP}^O \not\subseteq \mathrm{PH}^O$

➡ Unrelativized separations for sampling problems

Separations for Sampling Problems

Consider families of quantum circuit with classical inputs and outputs



[Terhal and DiVincenzo 2002]

Quantum circuits can sample from probability distributions that cannot be efficiently sampled <u>exactly</u> by a classical computer, unless the polynomial hierarchy collapses

[Aaronson and Arkhipov 2011]

Assuming some conjectures on the hardness of the permanent, quantum circuits can sample from probability distributions that cannot be efficiently sampled by a classical computer, <u>even approximately (with additive precision)</u>, unless the polynomial hierarchy collapses

Separations for Sampling Problems

Many further investigations:

[Bremner et al. 2010,16,17] [Aaronson and Arkhipov 2014]
[Morimae et al. 2014] [Fahri and Harrow 2016]
[Fujii and Tamate 2016] [Aaronson and Chen 2017]
[Fujii et al. 2018] [Bouland et al. 2019]

- ✓ replace the conjectures by others (weaker) conjectures
- ✓ use weaker complexity-theoretical assumptions
- ✓ prove the superiority of quantum computation even for weaker models: random quantum circuits, constant-depth quantum circuits (instantaneous quantum polynomial-time computation), noisy quantum circuits

motivation: easy to implement in the near future

CONCLUSION

Under plausible conjectures and/or complexity-theoretical assumptions, even weak classes of quantum circuits (e.g., constant-depth circuits) can sample from probability distributions that cannot be efficiently sampled (even approximately) by a classical computer

unproven conjectures

standard complexity-theoretical assumption

Can similar results be proven without relying on any conjecture or assumption?

Assuming some conjectures on the hardness of the permanent, quantum circuits can sample from probability distributions that cannot be efficiently sampled by a classical computer, even approximately (with additive precision), unless the polynomial hierarchy collapses

Unconditional Separations

Theorem ([Bravyi, Gosset, König 17]) – informal version

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. <u>on all inputs</u> requires Ω(log n) depth.

worst-case classical hardness

- no conjecture or assumption
- separates only quantum constant depth and classical logarithmic depth

Remark 1: in this talk all the circuits have bounded fanin

Remark 2: the computational problem can be defined as a <u>sampling problem</u> or a relation

Our result – informal version

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. on a non-negligible fraction of inputs

Can similar results be proven without relying on any conjecture or assumption?

Remark 3: similar results have been obtained independently by several other researchers
[Bravyi, Gosset, König 18], [Bene Watts, Kothari, Schaeffer, Tal 19], [Coudron, Stark, Vidick 18]
(comparison given in later slides)

Graph States

Definition (Graph State)

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

The graph state corresponding to a graph G is the quantum state obtained by the following process:

1. Prepare one quantum bit in state $|+\rangle$ for each node of G
2. Apply a “controlled-Z operation” on the qubits corresponding to each edge of G

If the graph has constant degree then the corresponding graph state can be constructed by a constant-depth quantum circuit

We will see that such quantum states still exhibit some “global entanglement” that cannot be simulated in constant-depth by classical circuits

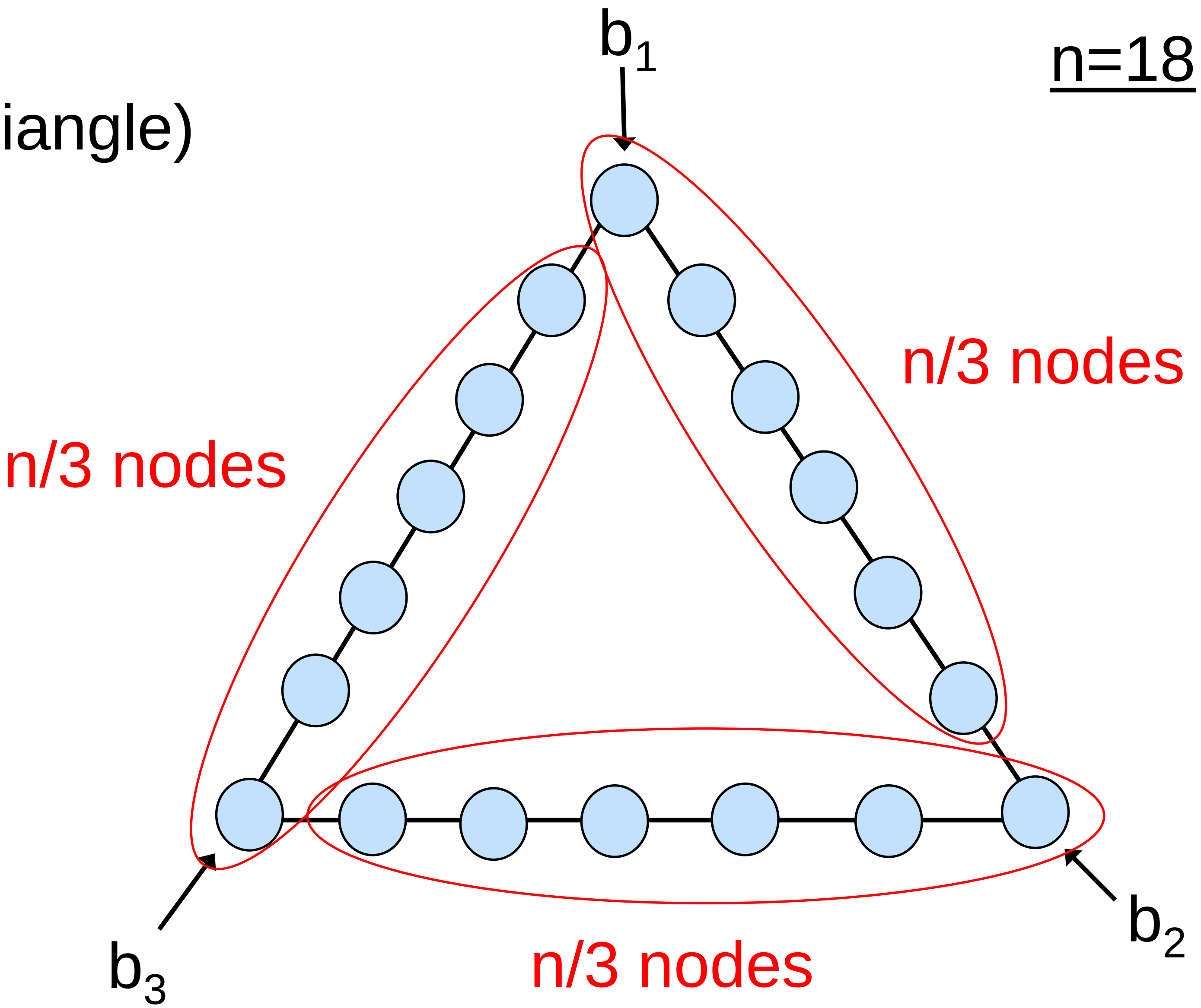
Key Prior Work on Nonlocality [Barrett et al. 07]

multiple of 3

Consider a ring of size n (seen as a triangle)

Each "corner" gets a bit as input

Each node will output one bit



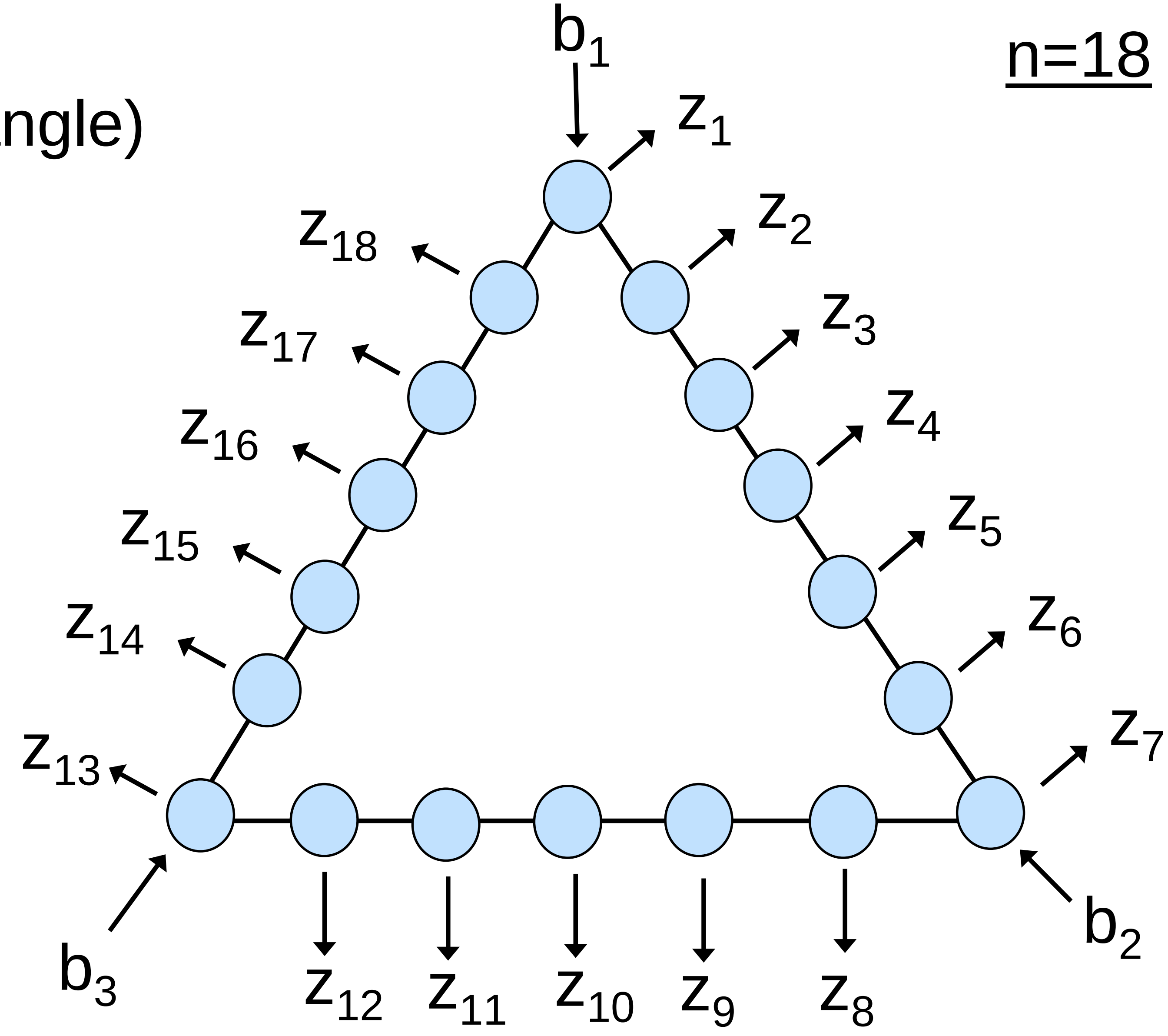
Key Prior Work on Nonlocality [Barrett et al. 07]

multiple of 3

Consider a ring of size n (seen as a triangle)

Each "corner" gets a bit as input

Each node will output one bit



Key Prior Work on Nonlocality [Barrett et al. 07]

multiple of 3

Consider a ring of size n (seen as a triangle)

Each “corner” gets a bit as input

Each node will output one bit

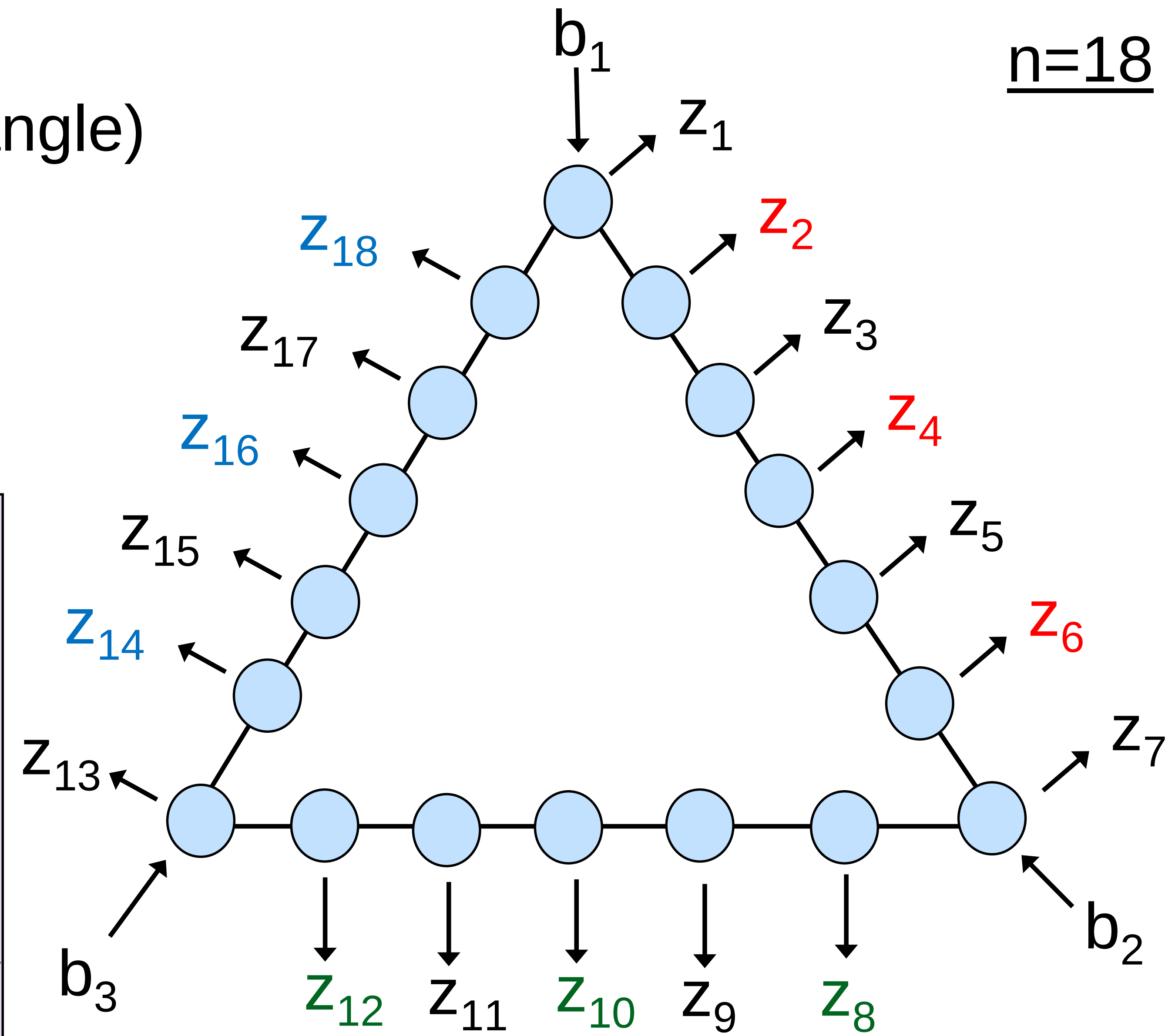
Define the following 4 bits:

$m_R = z_2 \oplus z_4 \oplus z_6$
(parity of the outputs of the nodes of even index on the right)

$m_B = z_8 \oplus z_{10} \oplus z_{12}$
(parity of the outputs of the nodes of even index on the bottom)

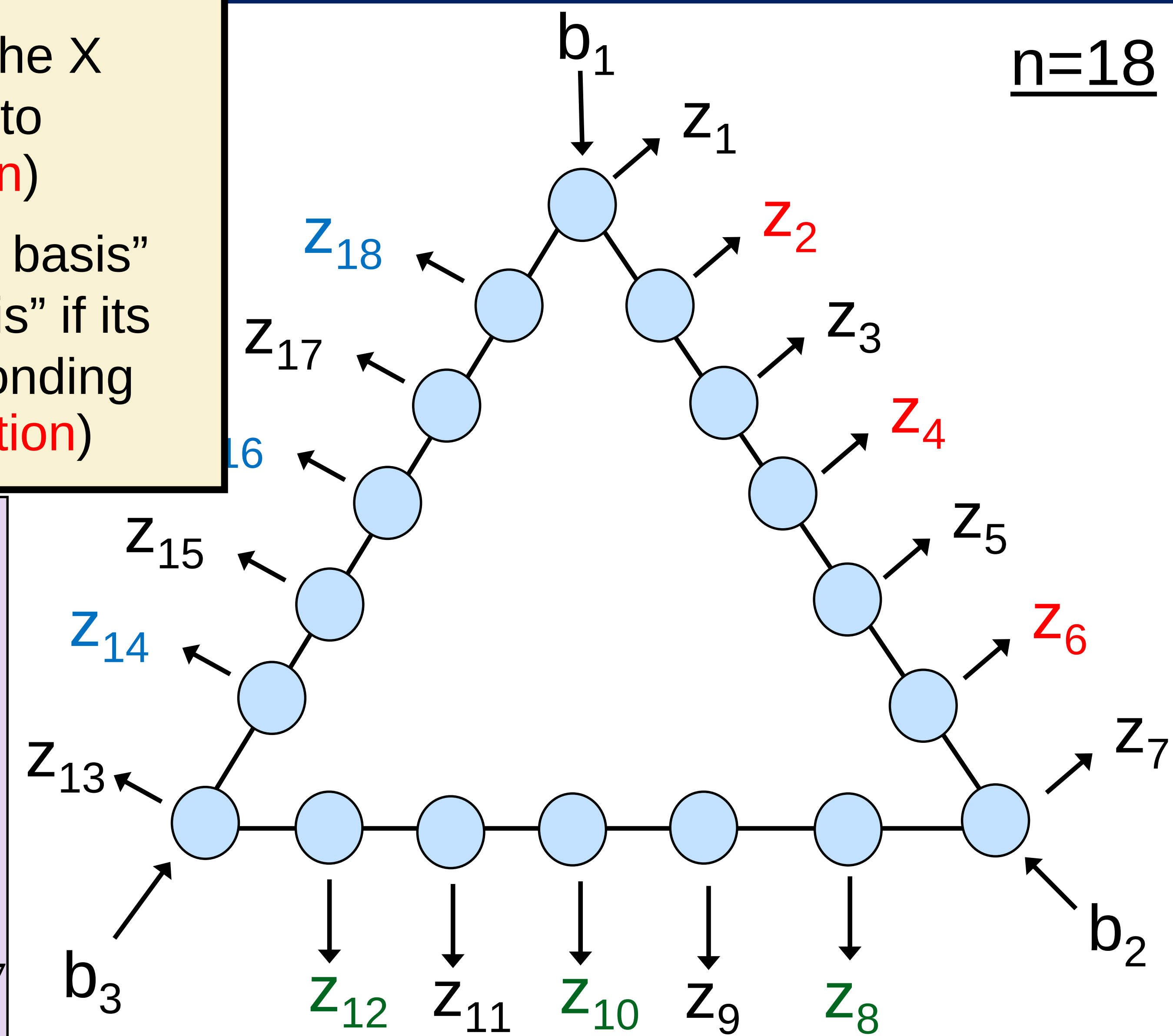
$m_L = z_{14} \oplus z_{16} \oplus z_{18}$
(parity of the outputs of the nodes of even index on the left)

$m_{odd} = z_1 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_9 \oplus z_{11} \oplus z_{13} \oplus z_{15} \oplus z_{17}$
(parity of the outputs of all the nodes of odd index)



PROTOCOL

1. The nodes prepare the graph state corresponding to the whole triangle (each node only needs to communicate with its two nearest neighbors)
2. Each non-corner node measures its qubit “in the X basis” and then outputs the bit corresponding to the measurement outcome (no communication)
3. Each corner node measures its qubit “in the X basis” if its input bit is 0, or measures it “in the Y basis” if its input bit is 1, and then outputs the bit corresponding to the measurement outcome (no communication)



$m_R = z_2 \oplus z_4 \oplus z_6$

(parity of the outputs of the nodes of even index on the right)

$m_B = z_8 \oplus z_{10} \oplus z_{12}$

(parity of the outputs of the nodes of even index on the bottom)

$m_L = z_{14} \oplus z_{16} \oplus z_{18}$

(parity of the outputs of the nodes of even index on the left)

$m_{odd} = z_1 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_9 \oplus z_{11} \oplus z_{13} \oplus z_{15} \oplus z_{17}$

(parity of the outputs of all the nodes of odd index)

Claim 1: This quantum protocol samples from the uniform distribution over all binary strings $(z_1, z_2, \dots, z_n) \in \{0,1\}^n$ satisfying the following condition:

$$\begin{cases} m_{odd} = 0 & \text{if } (b_1, b_2, b_3) = (0,0,0) \\ m_{odd} \oplus m_R = 1 & \text{if } (b_1, b_2, b_3) = (1,1,0) \\ m_{odd} \oplus m_B = 1 & \text{if } (b_1, b_2, b_3) = (0,1,1) \\ m_{odd} \oplus m_L = 1 & \text{if } (b_1, b_2, b_3) = (1,0,1) \end{cases}$$

Claim 2: Any classical protocol that samples (even approximately) from the same distribution requires communication between two nodes at distance Ω(n).

✓ Consider any classical protocol in which no communication occurs between two nodes located at distance ≥ n/6

m_R is an affine function of b_1 and b_2 because:

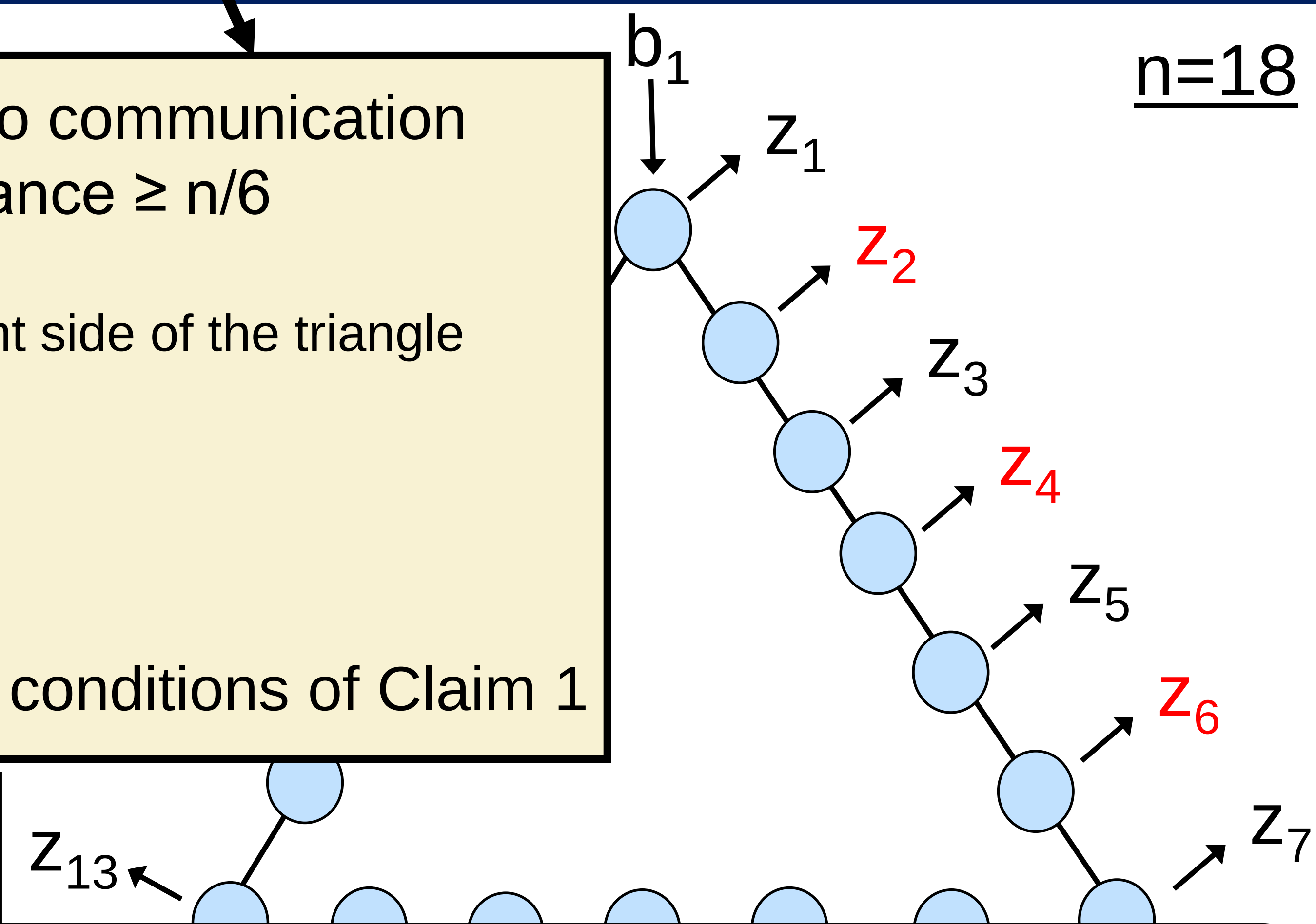
- b_3 is at distance n/3 of any node on the right side of the triangle
- b_1 and b_2 are at distance n/6

m_B is an affine function of b_2 and b_3

m_L is an affine function of b_1 and b_3

m_{odd} is an affine function of b_1, b_2 and b_3

✓ Such functions cannot satisfy all the linear conditions of Claim 1



$m_R = z_2 \oplus z_4 \oplus z_6$

(parity of the outputs of the nodes of even index on the right)

This computational problem can be solved with local communication in the quantum setting but requires long-distance communication in the classical setting

"quantum advantage for distributed computing over a ring"

Claim 1: This quantum protocol samples from the uniform distribution over all binary strings $(z_1, z_2, \dots, z_n) \in \{0,1\}^n$ satisfying the following condition:

$$\begin{cases} m_{odd} = 0 & \text{if } (b_1, b_2, b_3) = (0,0,0) \\ m_{odd} \oplus m_R = 1 & \text{if } (b_1, b_2, b_3) = (1,1,0) \\ m_{odd} \oplus m_B = 1 & \text{if } (b_1, b_2, b_3) = (0,1,1) \\ m_{odd} \oplus m_L = 1 & \text{if } (b_1, b_2, b_3) = (1,0,1) \end{cases}$$

Worst-Case Quantum Advantage for Circuits

Theorem ([Bravyi, Gosset, König 17])

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

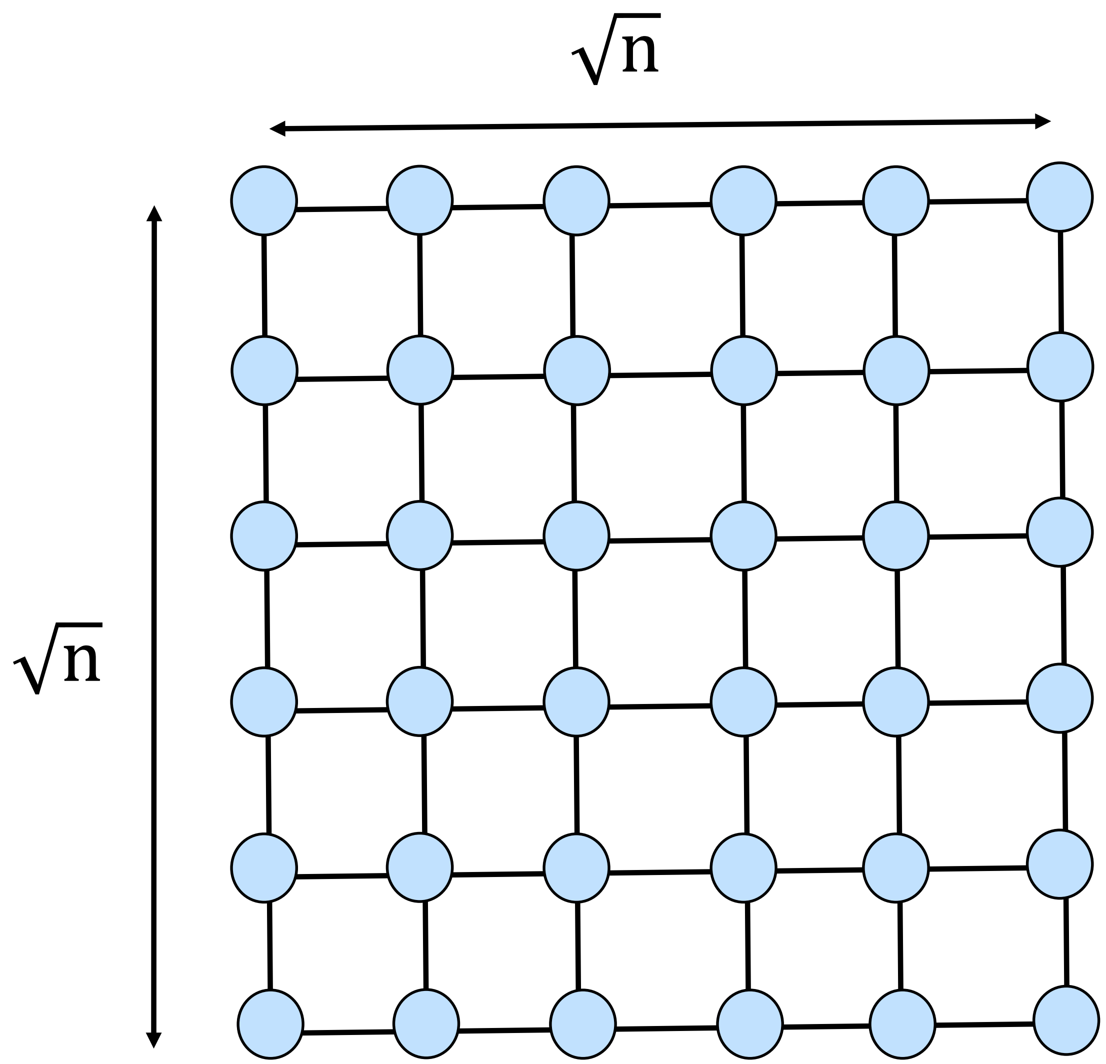
(ii) any classical circuit that solves it w.h.p. on all inputs requires $\Omega(\log n)$ depth.

Consider a square grid of n nodes

Let m be the number of edges ($m = \Theta(n)$)

The input of the computational problem is a pair $(a,b) \in \{0,1\}^m \times \{0,1\}^n$

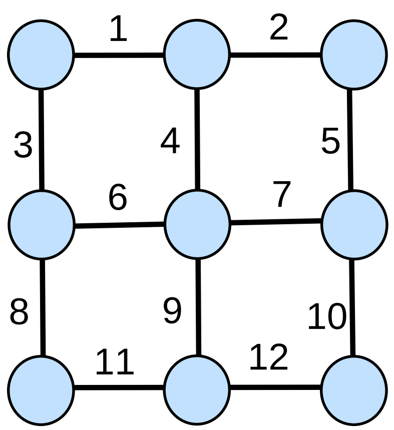
The computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding the graph specified by the string a



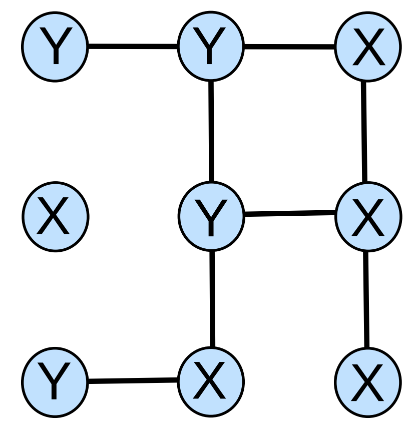
example: $n = 9$

$a = 110110101110 \longrightarrow$ keep only the edges number 1,2,4,5,7,9,10,11

$b = 110010100 \longrightarrow$ measure nodes 1,2,5,7 in the Y basis, and the others in the X basis



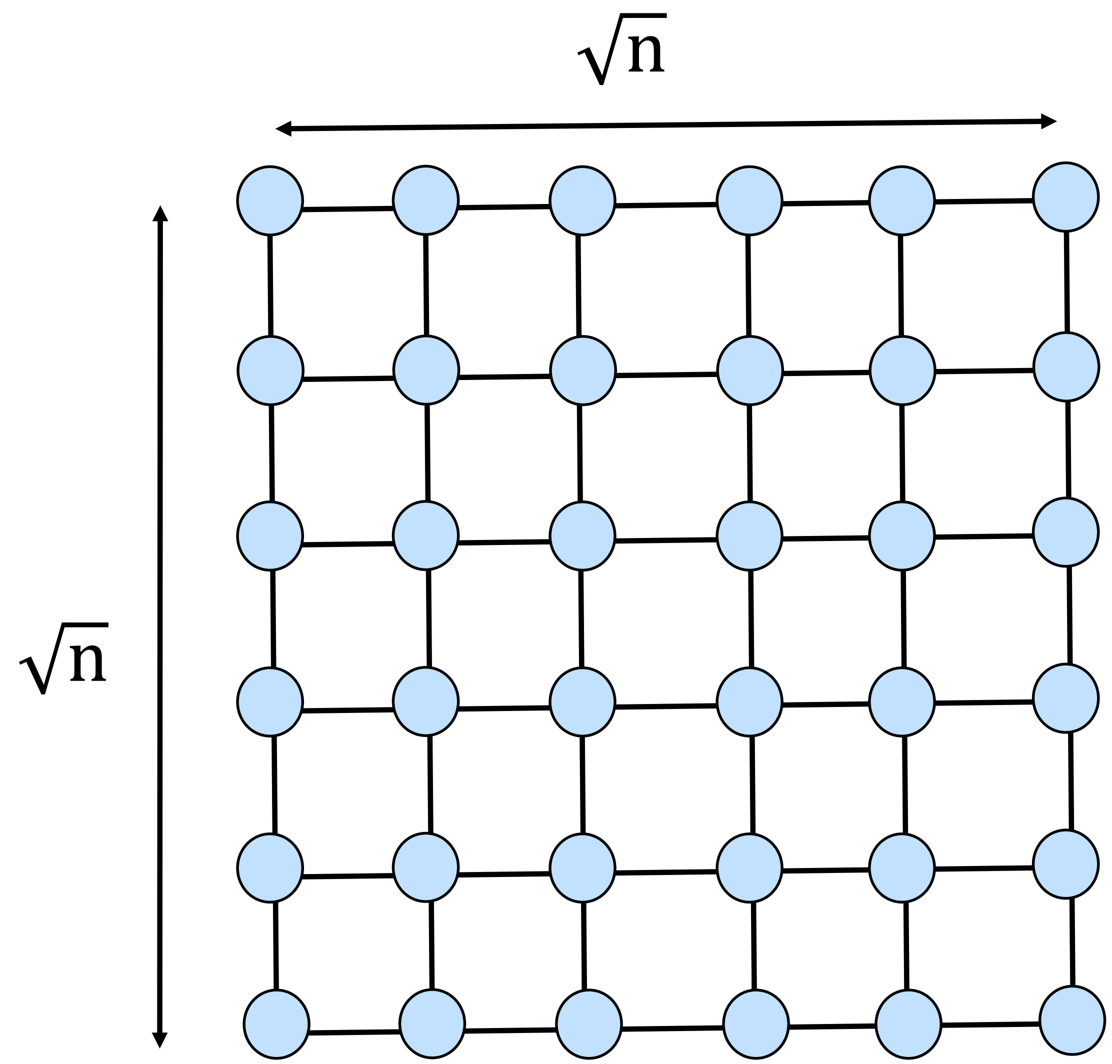
$m = 12$



Consider a square grid of n nodes

Let m be the number of edges ($m = \Theta(n)$)

The input of the computational problem is a pair $(a,b) \in \{0,1\}^m \times \{0,1\}^n$



The computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding the graph specified by the string a

Worst-Case Quantum Advantage for Circuits

straightforward: graph states on constant-degree graphs can be constructed by a constant-depth quantum circuit

Theorem ([Bravyi, Gosset, König 17])

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

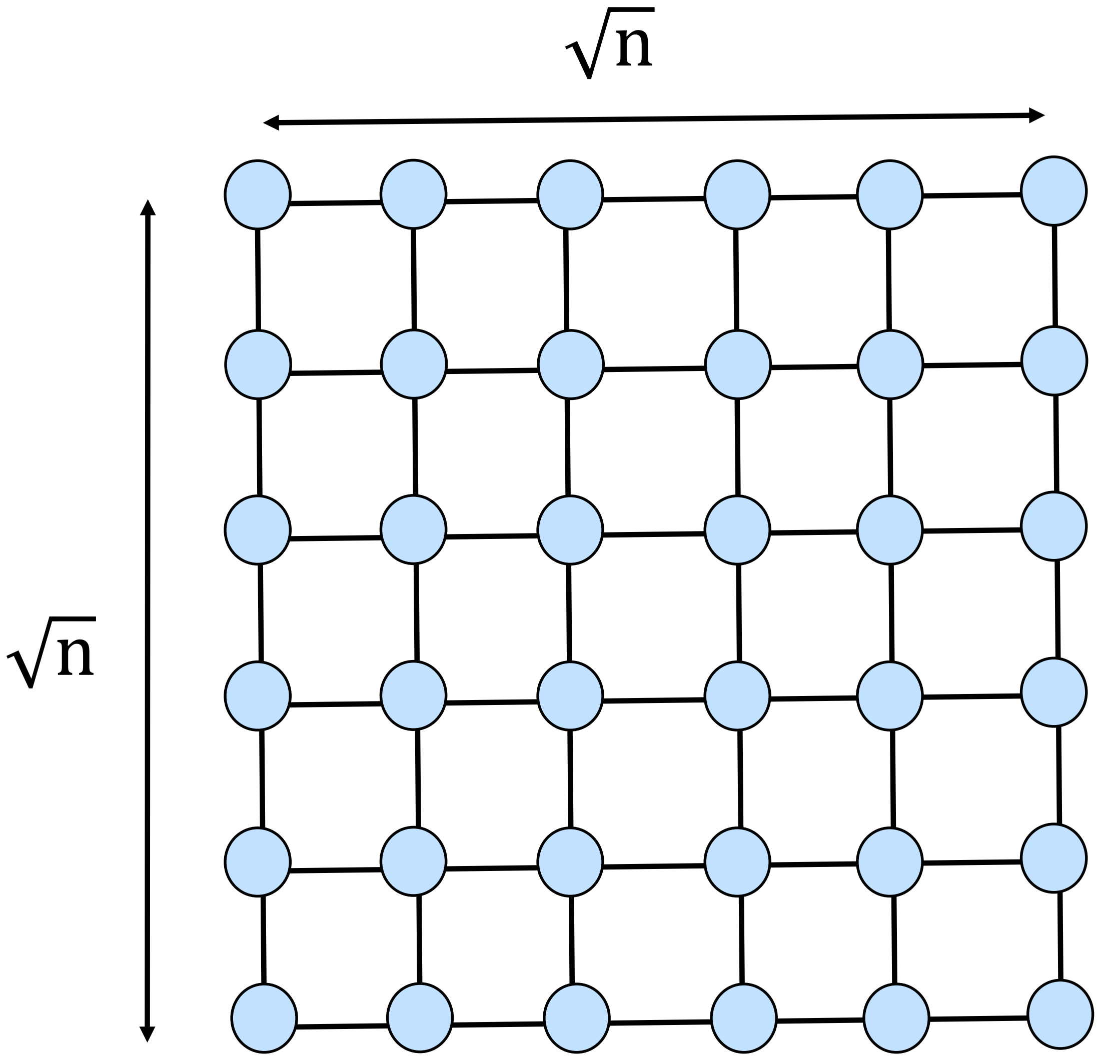
(ii) any classical circuit that solves it w.h.p. on all inputs requires $\Omega(\log n)$ depth.

Consider a square grid of n nodes

Let m be the number of edges ($m = \Theta(n)$)

The input of the computational problem is a pair $(a,b) \in \{0,1\}^m \times \{0,1\}^n$

The computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding the graph specified by the string a



Proof of the Classical Lower Bound [Bravyi, Gosset, König 17]

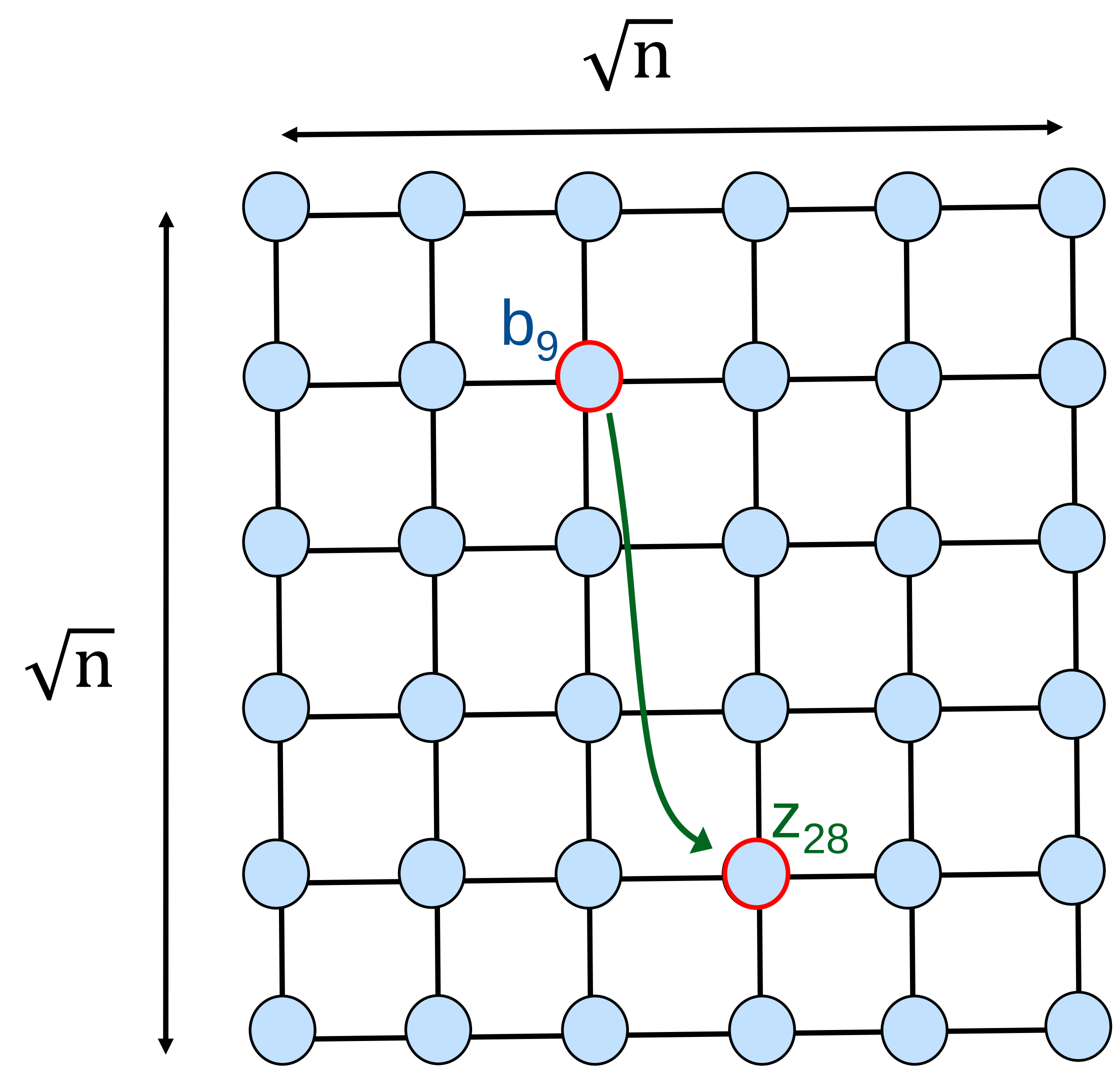
- ✓ Consider any classical circuit of depth $\leq \frac{1}{100} \log n$ that solves our problem
- ✓ The circuit has m + n input wires and n output wires
- ✓ Each of the n input wires that represent $b \in \{0,1\}^n$ corresponds to one node of the grid
  Each of the n output wires (which represent $z \in \{0,1\}^n$) corresponds to one node of the grid
- ✓ We will write the input-output dependences of the circuit by arrows on the grid

Consider a square grid of n nodes

Let m be the number of edges (m = Θ(n))

The input of the computational problem is a pair $(a,b) \in \{0,1\}^m \times \{0,1\}^n$

The computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding the graph specified by the string a



Proof of the C

Claim (trivial): In a classical circuit of small depth and bounded fanin, any output bit can depend only on a small amount of input bits

✓ Consider any classical circuit of depth $\leq \frac{1}{100}\log n$ that solves our problem

✓ The circuit has m + n input wires and n output wires

✓ Each of the n input wires that represent $b \in \{0,1\}^n$ corresponds to one node of the grid
Each of the n output wires (which represent $z \in \{0,1\}^n$) corresponds to one node of the grid

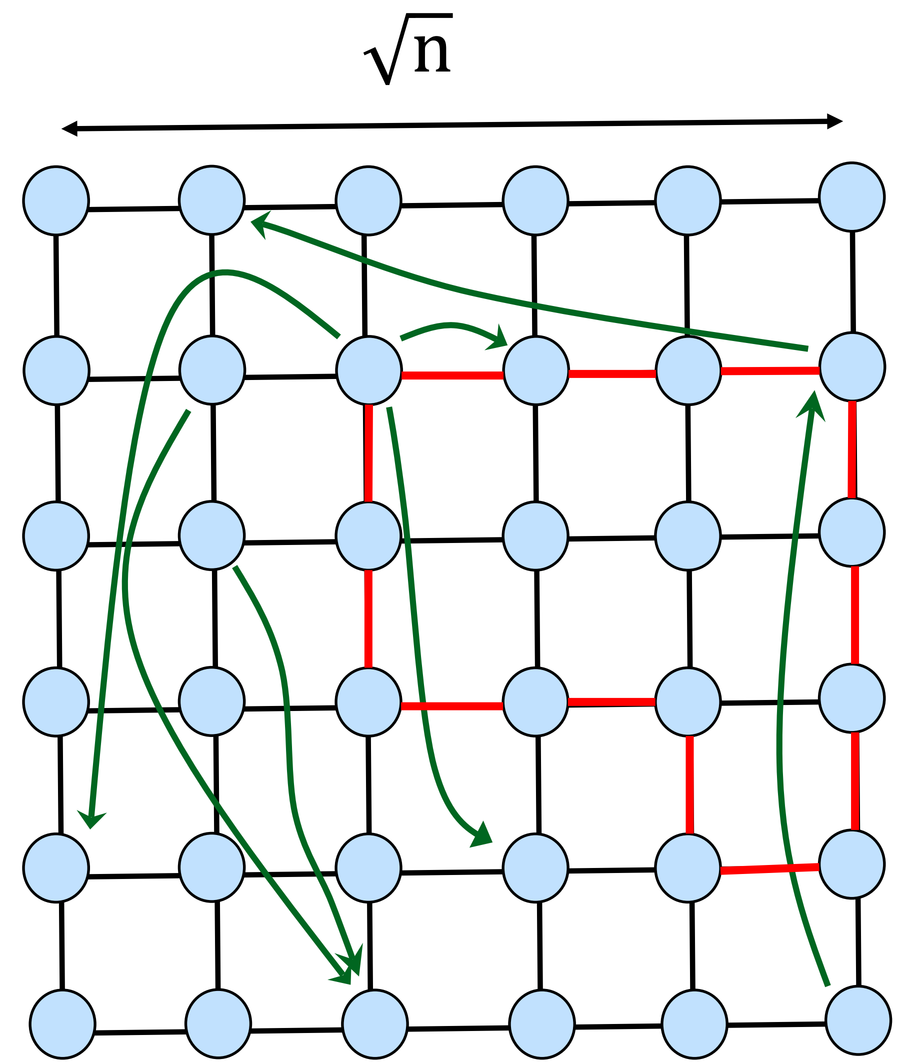
✓ We will write the input-output dependences of the circuit by arrows on the grid

⇨ Each node cannot be the endpoint of too many arrows

⇨ There exists a long cycle that avoids all long arrows (i.e., does not contain both extremities of any long arrow)

✓ Consider the string a that specifies this long cycle

✓ The circuit cannot work for all strings b, from the argument from the first part of the talk



The computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding the graph specified by the string a

Worst-Case Quantum Advantage for Circuits

straightforward: graph states on constant-degree graphs can be constructed by a constant-depth quantum circuit

Theorem ([Bravyi, Gosset, König 17])

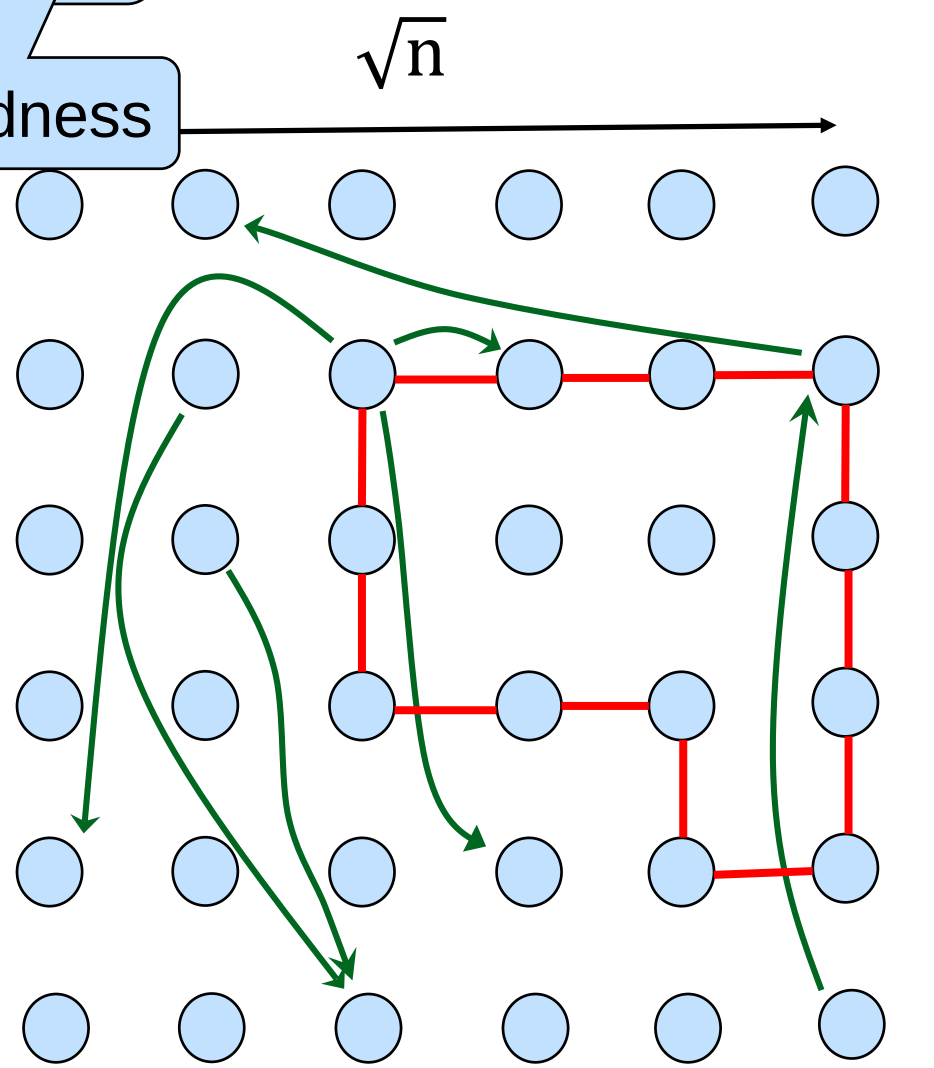
There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. on all inputs requires Ω(log n) depth.

for any small-depth classical circuit there exists an input (a,b) such that the circuit does not work

worst-case classical hardness



- ✓ Consider the string a that specifies this long cycle
- ✓ The circuit cannot work for all strings b, from the argument from the first part of the talk

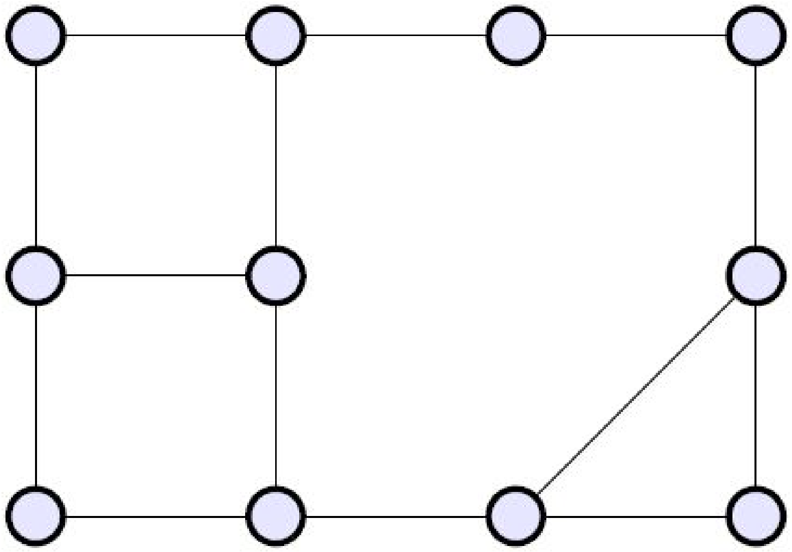
The computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding the graph specified by the string a

Getting Average-Case Hardness: Our Key Construction

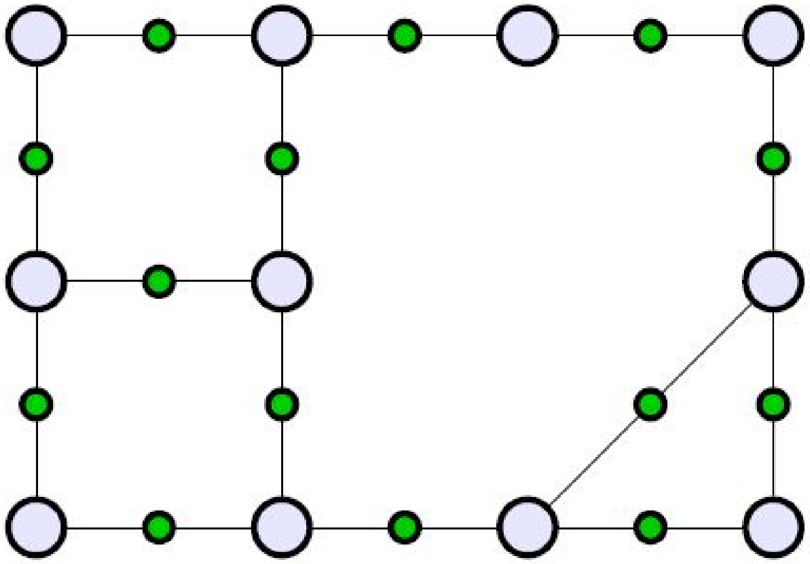
We generalize the nonlocality result described the first part of the talk to other kinds of graphs

Getting Average-Case Hardness: Our Key Construction

Given any graph

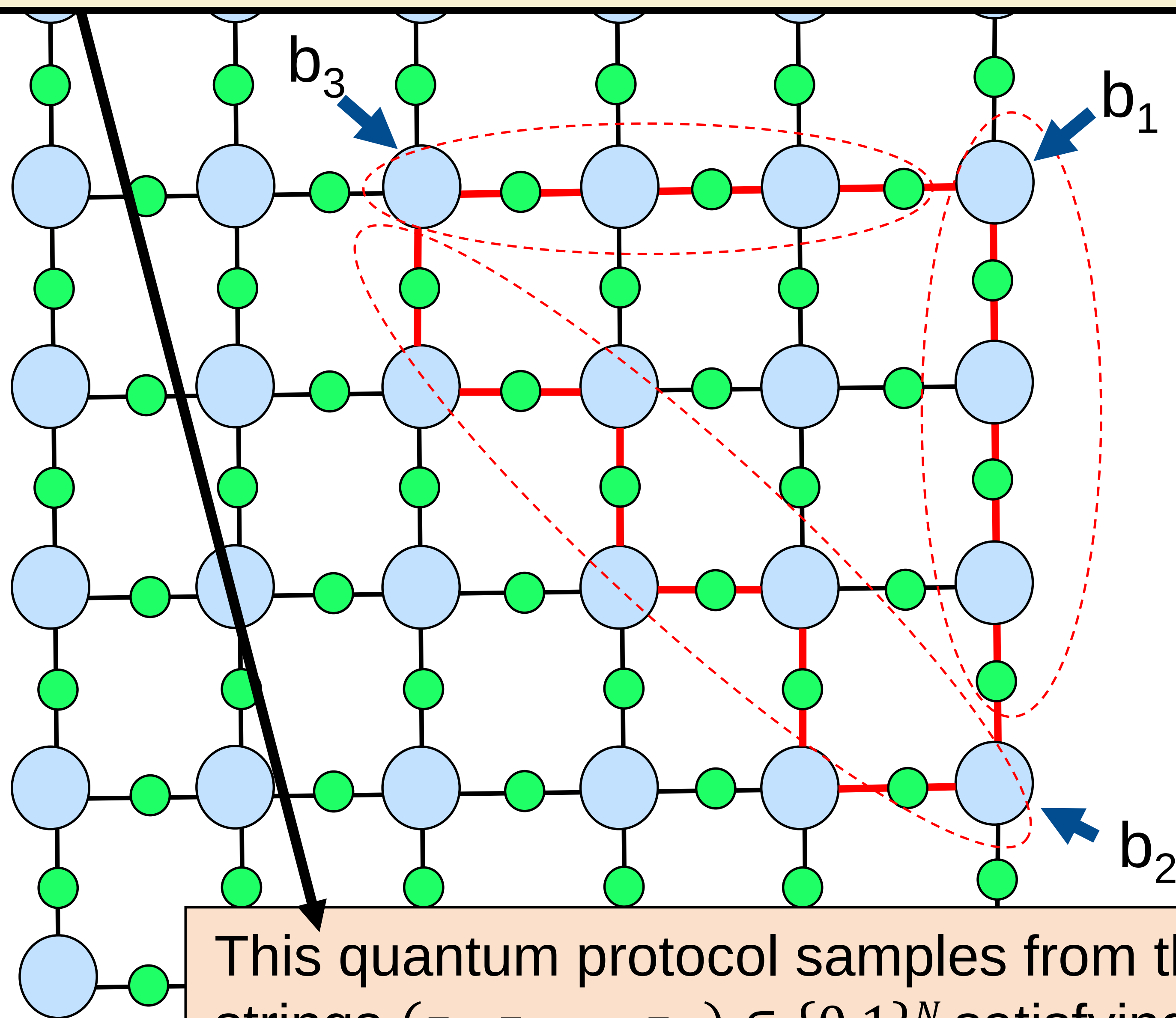


we define its “extended graph” as



Similar construction used in, e.g., [Fujii and Morimae 2017]

1. The nodes prepare the graph state corresponding to the whole graph (which has constant degree)
2. Each non-corner node (this includes the nodes outside the cycle) measures its qubit “in the X basis” and then outputs the bit corresponding to the measurement outcome
3. Each corner node measures its qubit “in the X basis” if its input bit is 0, or measures it “in the Y basis” if its input bit is 1, and then outputs the bit corresponding to the measurement outcome



- ✓ Consider any cycle and see it as a triangle by dividing it into three parts (of roughly the same size)
- ✓ Each corner gets a bit as input
- ✓ Each node of the graph will output a bit

N: total number of vertices of the whole graph

m_{all}: parity of the outputs of all blue nodes

m_R: parity of the outputs of all green nodes in the right side of the triangle

m_T: parity of the outputs of all green nodes in the top side of the triangle

m_L: parity of the outputs of all green nodes in the left side of the triangle

Claim: This quantum protocol samples from the uniform distribution over all binary strings $(z_1, z_2, \dots, z_N) \in \{0,1\}^N$ satisfying the following condition:

$$\begin{cases} m_{all} = 0 & \text{if } (b_1, b_2, b_3) = (0,0,0) \\ m_{all} \oplus m_R = 1 & \text{if } (b_1, b_2, b_3) = (1,1,0) \\ m_{all} \oplus m_L = 1 & \text{if } (b_1, b_2, b_3) = (0,1,1) \\ m_{all} \oplus m_T = 1 & \text{if } (b_1, b_2, b_3) = (1,0,1) \end{cases}$$

Claim: Any classical protocol that samples (even approximately) from the same distribution requires communication between two nodes on the cycle at distance Ω(N).

- ✓ In any classical protocol in which no long-distance communication occurs between nodes on the three sides:

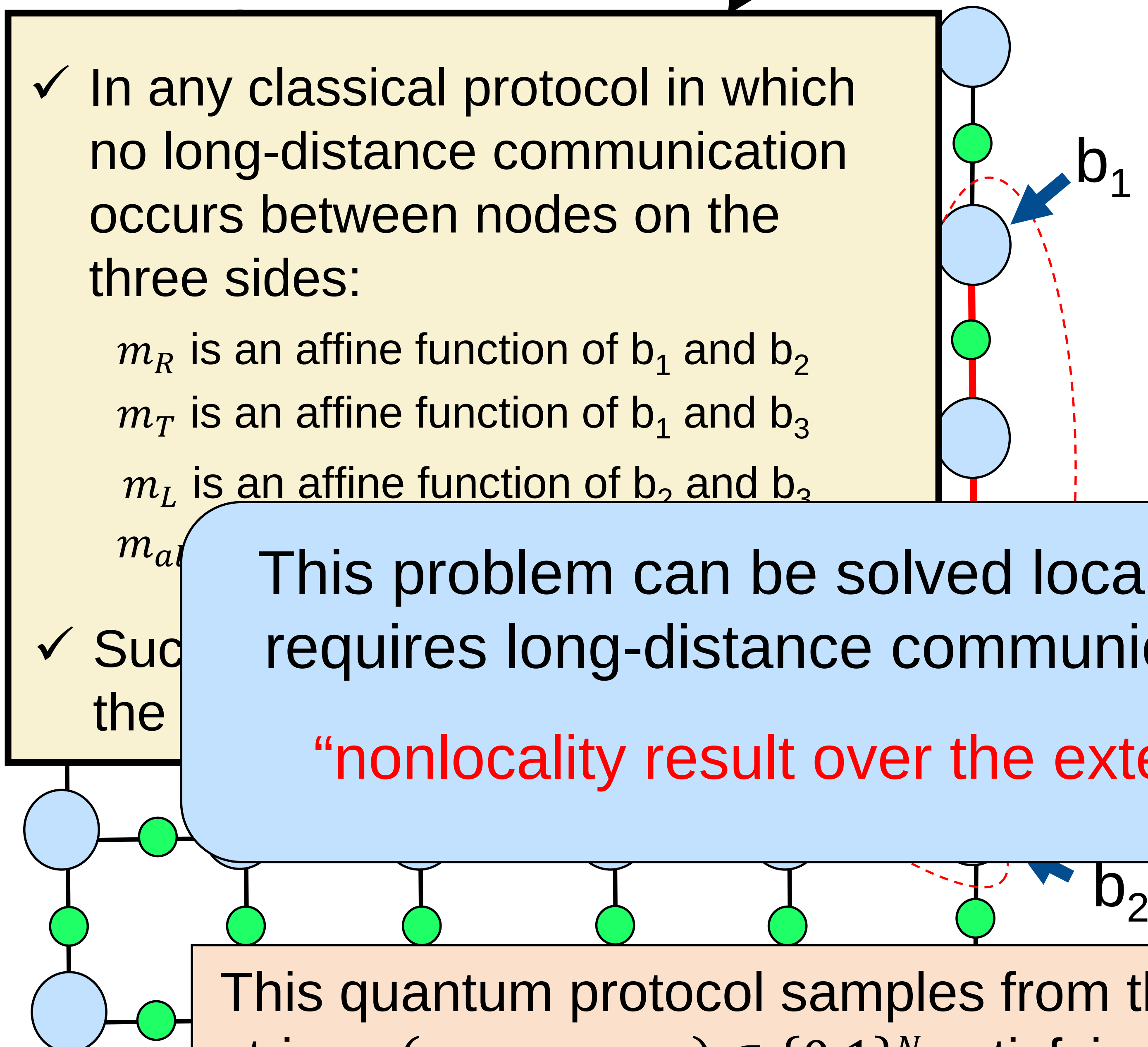
  m_R is an affine function of b_1 and b_2

  m_T is an affine function of b_1 and b_3

  m_L is an affine function of b_2 and b_3

  m_{al}

- ✓ Suc
  the



- ✓ Consider any cycle and see it as a triangle by dividing it into three parts (of roughly the same size)
- ✓ Each corner gets a bit as input
- ✓ Each node of the graph will output a bit

N: total number of vertices of the whole graph

s

es in the
triangle
es in the
triangle
m_L: parity of the outputs of all green nodes in the left side of the triangle

This problem can be solved locally in the quantum setting but requires long-distance communication in the classical setting

"nonlocality result over the extended graph of a 2D grid"

Claim: This quantum protocol samples from the uniform distribution over all binary strings $(z_1, z_2, \dots, z_N) \in \{0,1\}^N$ satisfying the following condition:

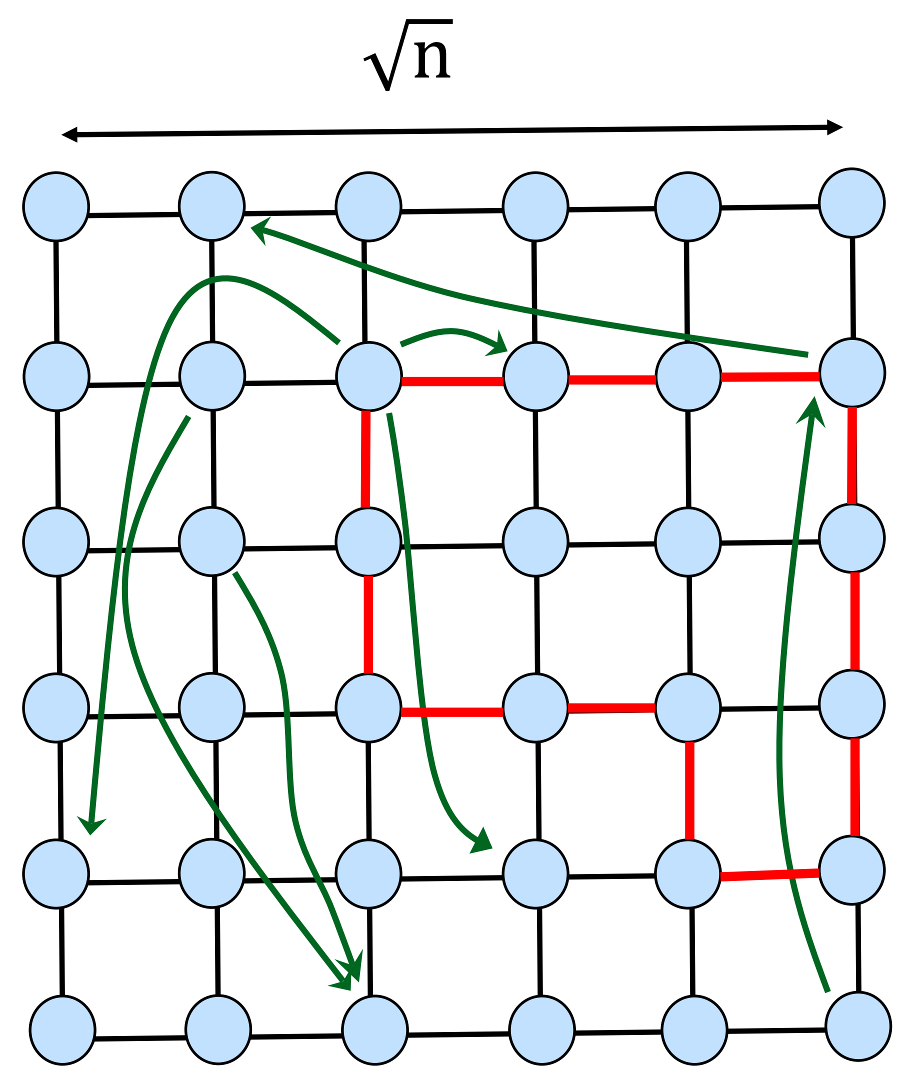
$$\begin{cases} m_{all} = 0 & \text{if } (b_1, b_2, b_3) = (0,0,0) \\ m_{all} \oplus m_R = 1 & \text{if } (b_1, b_2, b_3) = (1,1,0) \\ m_{all} \oplus m_L = 1 & \text{if } (b_1, b_2, b_3) = (0,1,1) \\ m_{all} \oplus m_T = 1 & \text{if } (b_1, b_2, b_3) = (1,0,1) \end{cases}$$

Proof of the Classical Lower Bound [Bravyi, Gosset, König 17]

- ✓ Consider any classical circuit of depth $\leq \frac{1}{100} \log n$ that solves our problem
- ✓ The circuit has m + n input wires and n output wires
- ✓ Each of the n input wires that represent $b \in \{0,1\}^n$ corresponds to one node of the grid
  Each of the n output wires (which represent $z \in \{0,1\}^n$) corresponds to one node of the grid

⇨ There exists a long cycle that avoids all long arrows (i.e., does not contain both extremities of any long arrow)

Needed to remove everything except this red cycle

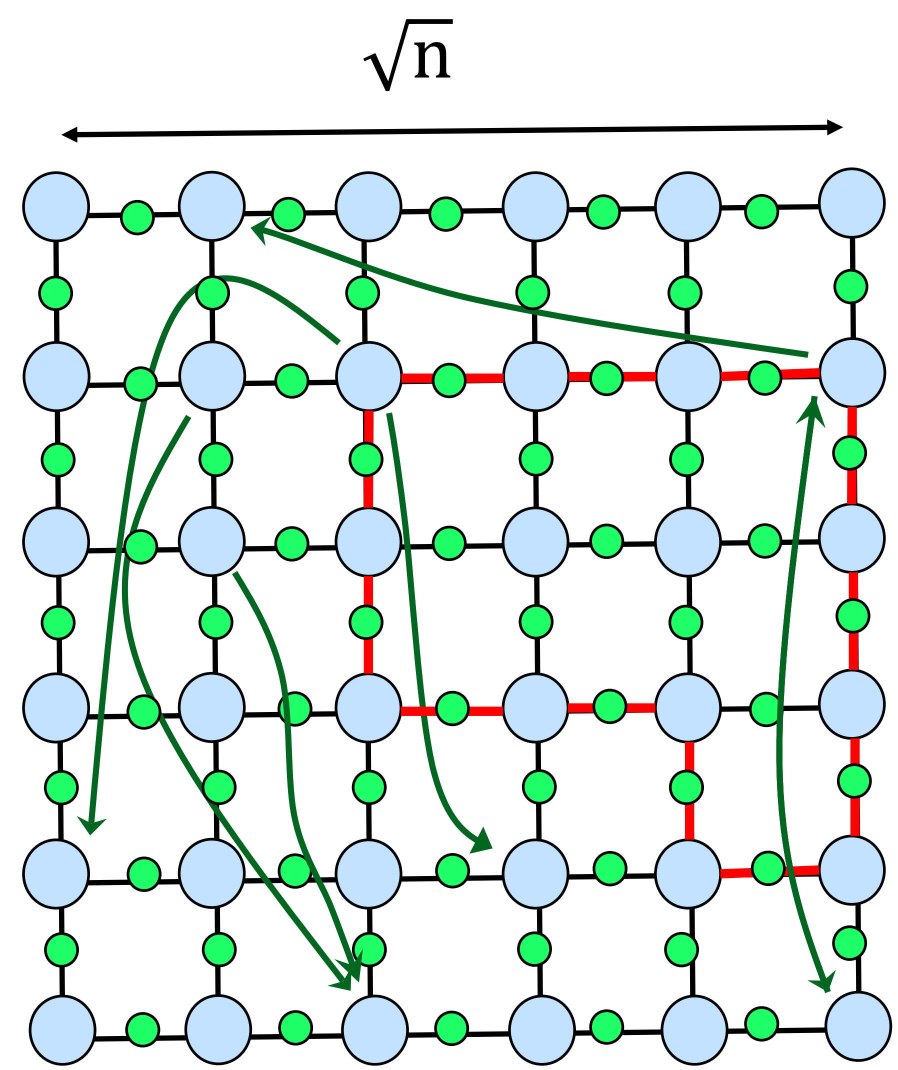


Proof of the Classical Lower Bound with our technique

- ✓ Consider any classical circuit of depth $\leq \frac{1}{100} \log n$ that solves our problem
- ✓ The circuit has m + n input wires and n output wires
- ✓ Each of the n input wires that represent $b \in \{0,1\}^n$ corresponds to one node of the grid
  Each of the n output wires (which represent $z \in \{0,1\}^n$) corresponds to one node of the grid

⇨ There exists a long cycle that avoids all long arrows (i.e., does not contain both extremities of any long arrow)

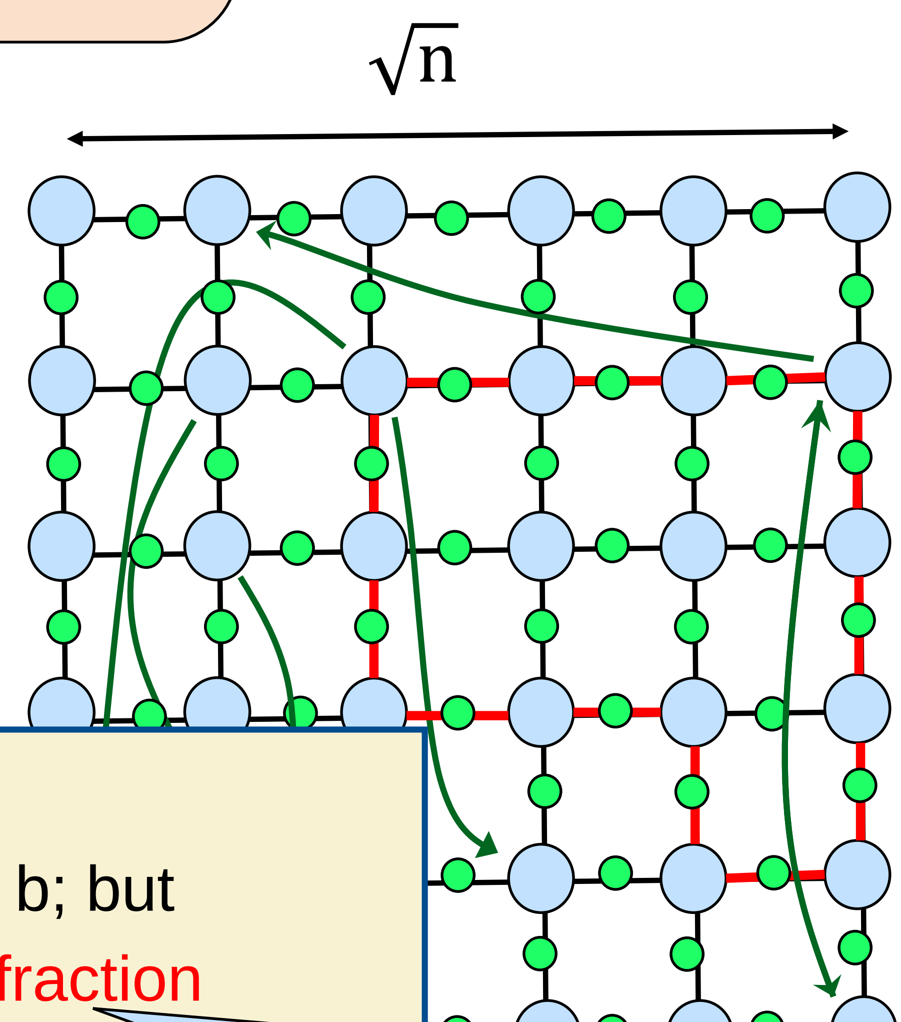
If we work with the extended graph of the grid, then no need to remove anything, since our new non-locality argument works on the whole graph (i.e., even when keeping the nodes outside the cycle)



New Computational Problem

We can define a new computational problem where the input is only the string b ∈ $\{0,1\}^n$

The new computational problem asks to sample from the distribution obtained when measuring, in the basis specified by the string b, the graph state corresponding to the extended graph of the square grid



If we work with the extended graph of the grid, then no need to remove anything, since our new non-locality argument works on the whole graph (i.e., even when keeping the nodes outside the cycle)

Our result

For this computational problem:

(i) a constant-depth quantum circuit solves it on all inputs b; but

(ii) any classical circuit that solves it w.h.p. on a constant fraction of the inputs b requires Ω(log n) depth.

average-case classical hardness

Final Remarks

✓ To obtain the final version of our average-case hardness result we use amplification (we require to solve in parallel multiple instances of the problem)

Our result (final version)

For this computational problem:

(i) a constant-depth quantum circuit solves it on all inputs b; but

(ii) any classical circuit that solves it w.h.p. on a non-negligible fraction of the inputs b requires Ω(log n) depth.

For this computational problem:

(i) a constant-depth quantum circuit solves it on all inputs b; but

(ii) any classical circuit that solves it w.h.p. on a constant fraction of the inputs b requires Ω(log n) depth.

average-case classical hardness

Final Remarks

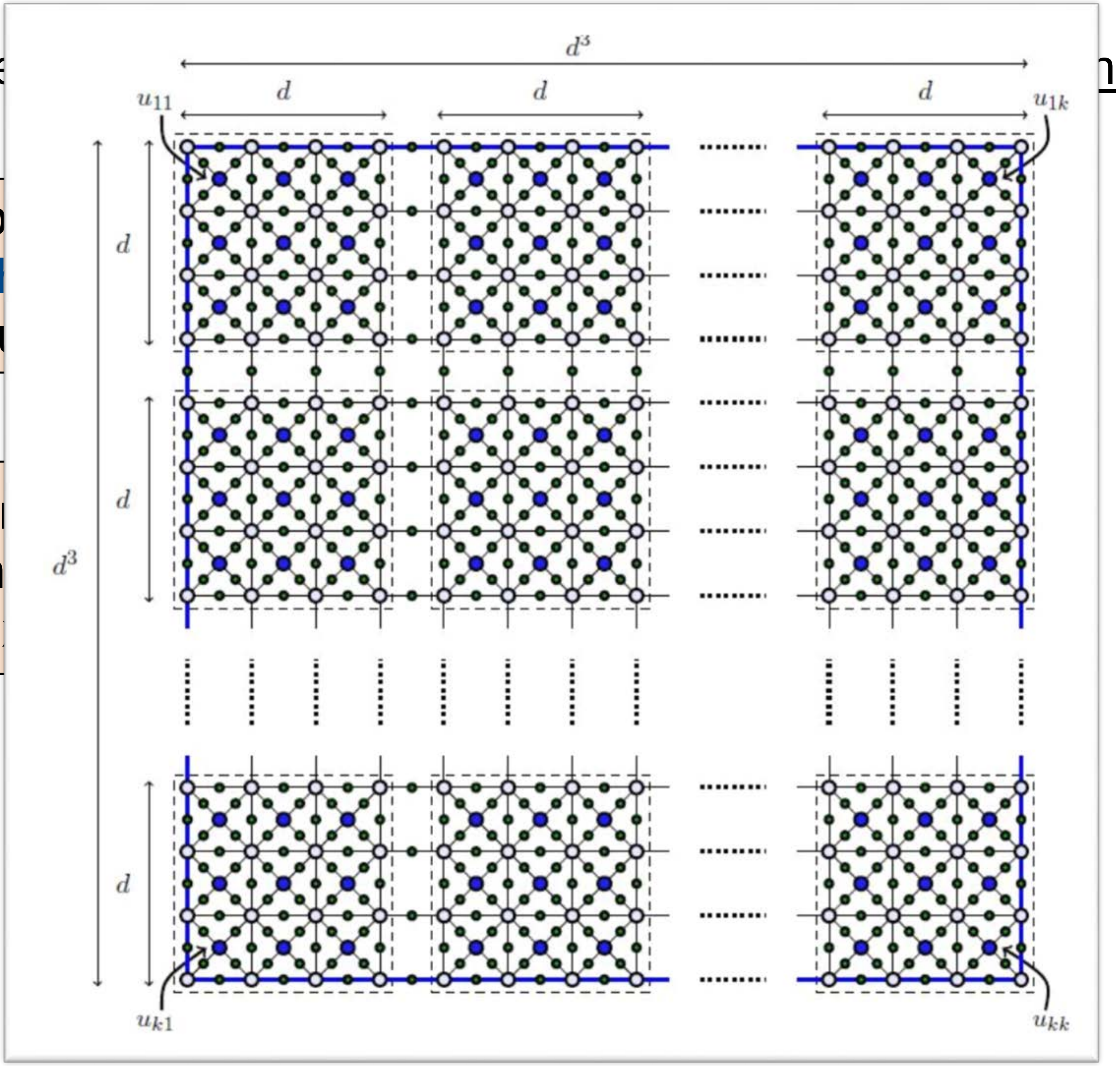
- ✓ To obtain the final version of our average-case hardness result we use amplification (we require to solve in parallel multiple instances of the problem)

- ✓ For technical reasons we work on a graph slightly more complicated

- ✓ While we considered a sampling proble

Sample from the distribution corresp
measuring, in the basis specified by t
the extended graph state of the sq

Output any outco
measurin
of the e



Relation with Concurrent Works

Theorem ([Bravyi, Gosset, König 17])

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. on all inputs requires $\Omega(\log n)$ depth.

Our result

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. on a non-negligible fraction of inputs requires $\Omega(\log n)$ depth.

Theorem ([Bravyi, Gosset, König 18] ← journal version)

finer analysis of the original construction

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. on all a constant fraction of inputs requires $\Omega(\log n)$ depth.

different construction

[Coudron, Stark, Vidick 18]: statement similar to ours, application to randomness expansion

new problem + techniques from classical circuit complexity

[Bene Watts, Kothari, Schaeffer, Tal 19]:
classical average-case hardness holds even for classical circuits with unbounded fanin

Conclusion and Open Problems

Our result: average-case quantum advantage for low-depth circuits

There exists a computational problem such that:

(i) a constant-depth quantum circuit solves it on all inputs; but

(ii) any classical circuit that solves it w.h.p. on a non-negligible fraction of inputs requires $\Omega(\log n)$ depth.

- no conjecture or assumption
- separates only quantum constant depth and classical logarithmic depth

Research direction #1: show advantage even for noisy quantum computation

[Bravyi, Gosset, König, Tomamichel 19] showed a noisy version of this theorem using error-correction techniques (for local noise)

Research direction #2: show advantage against stronger classes of classical circuits

Can this approach be generalized to show the advantage of low-depth quantum circuits over, say, classical circuits of depth $\Omega((\log n)^{1+\varepsilon})$?