Quantum advantage with shallow circuits

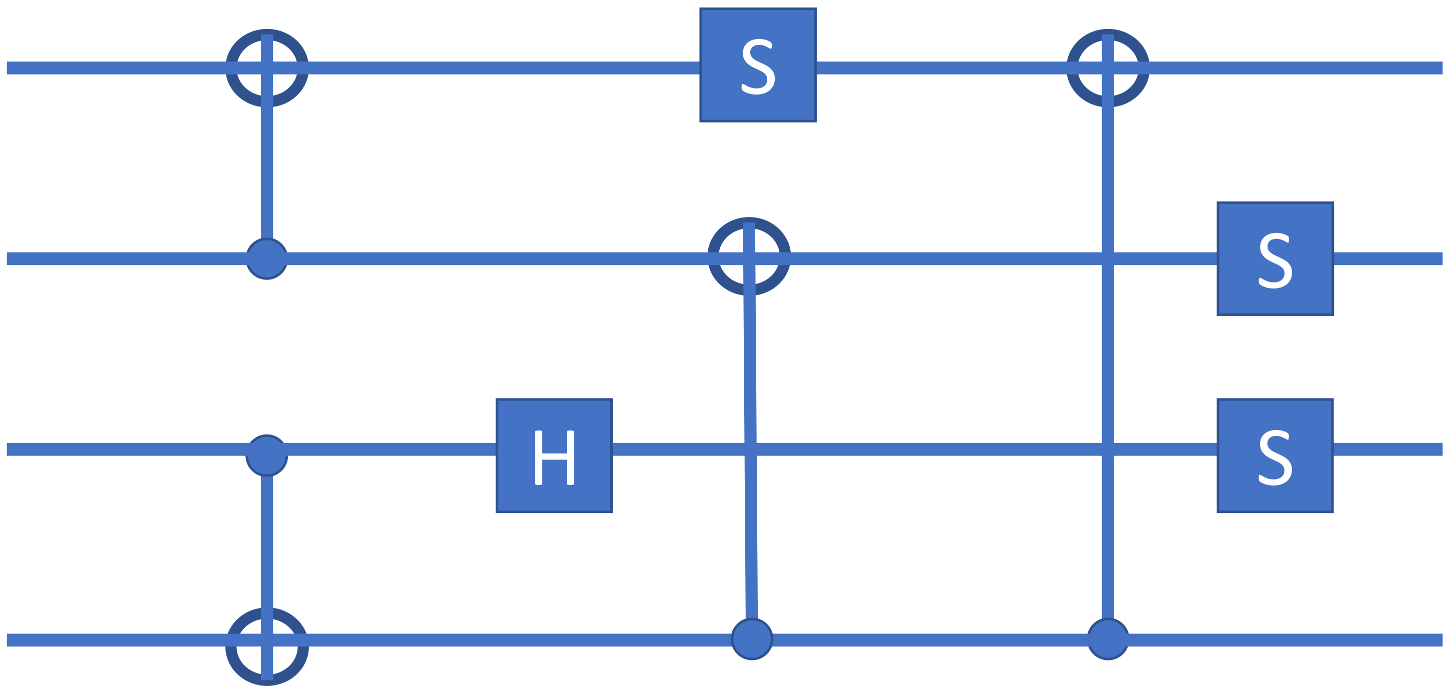
arXiv:1704.00690

Sergey Bravyi (IBM)
David Gosset (IBM)
Robert Koenig (Munich)

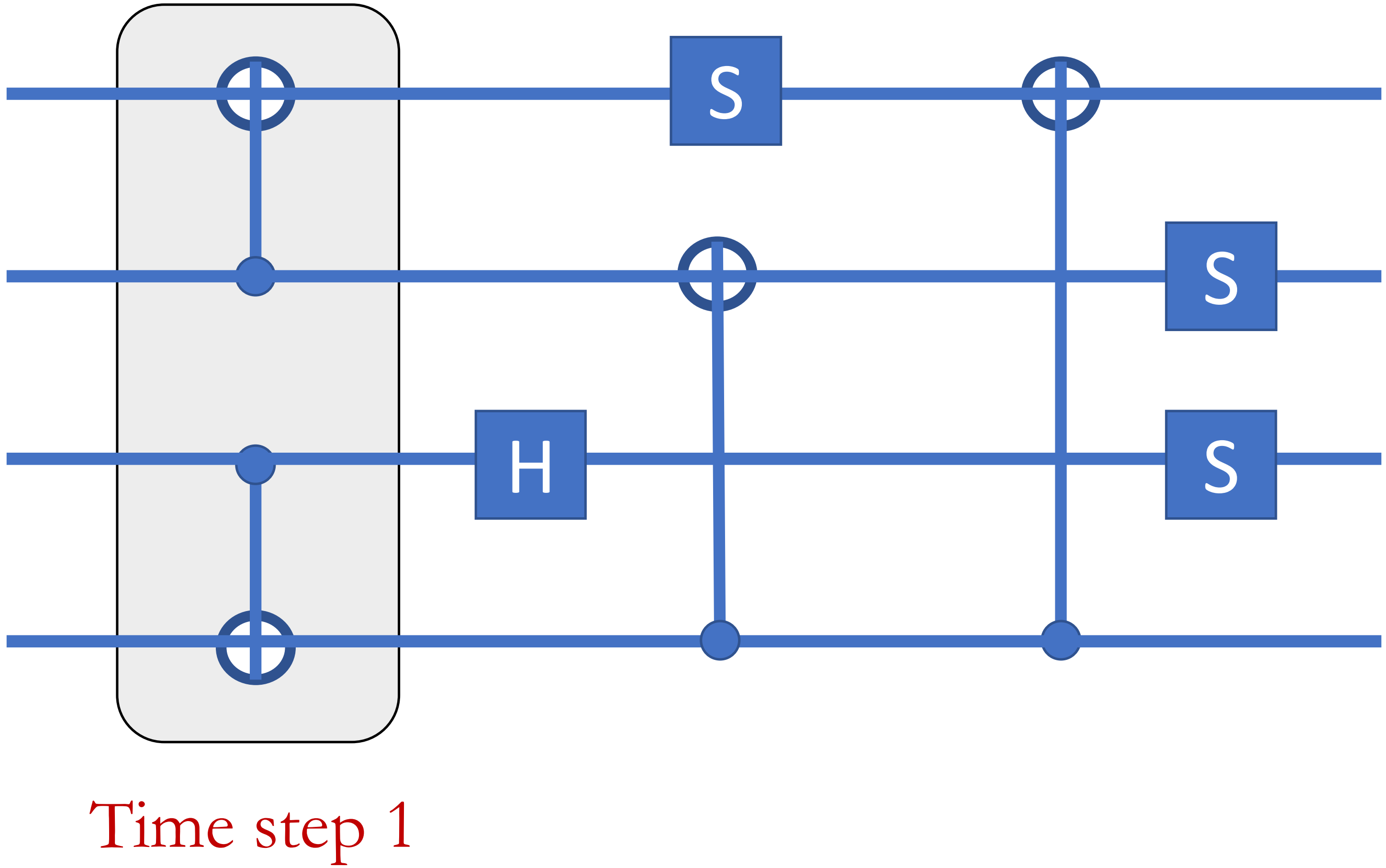
In this talk I will describe a **provable**, **non-oracular**, quantum speedup which is attained by constant-depth quantum circuits in a 2D architecture.

I. Overview

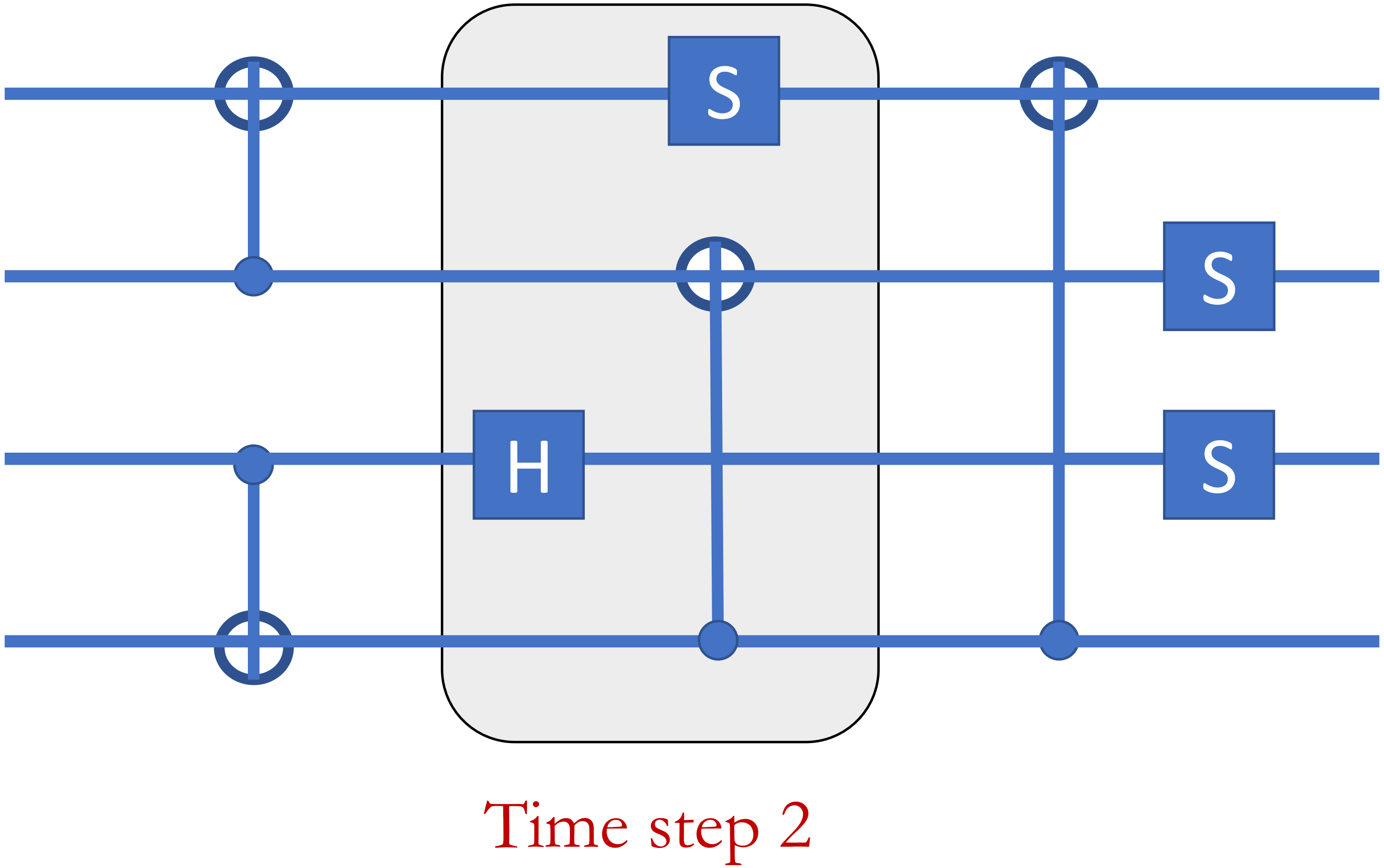
A **depth-d quantum circuit** consists of d time steps.
Each time step contains one- and two-qubit gates acting on disjoint qubits.



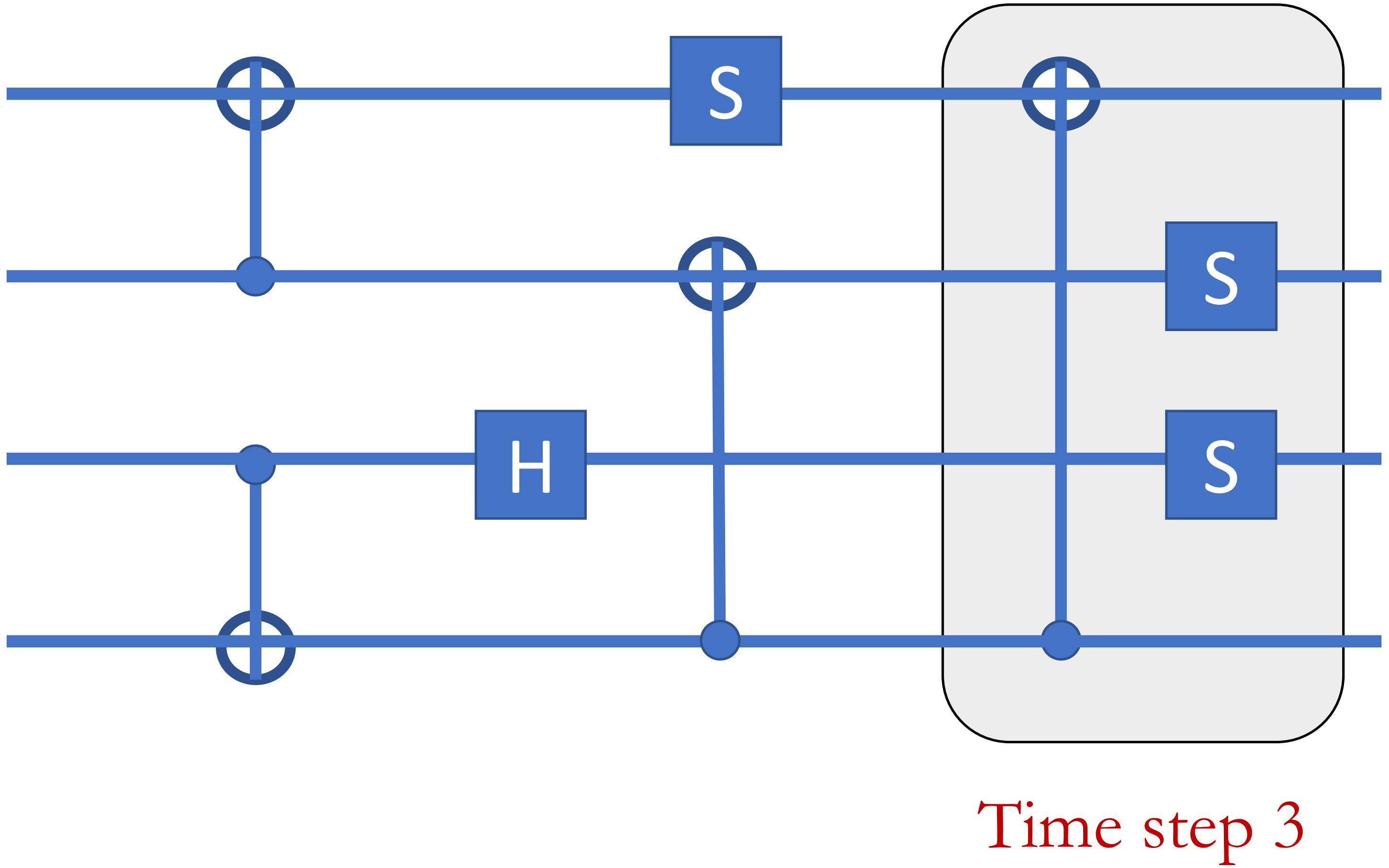
A **depth-d quantum circuit** consists of d time steps.
Each time step contains one- and two-qubit gates acting on disjoint qubits.



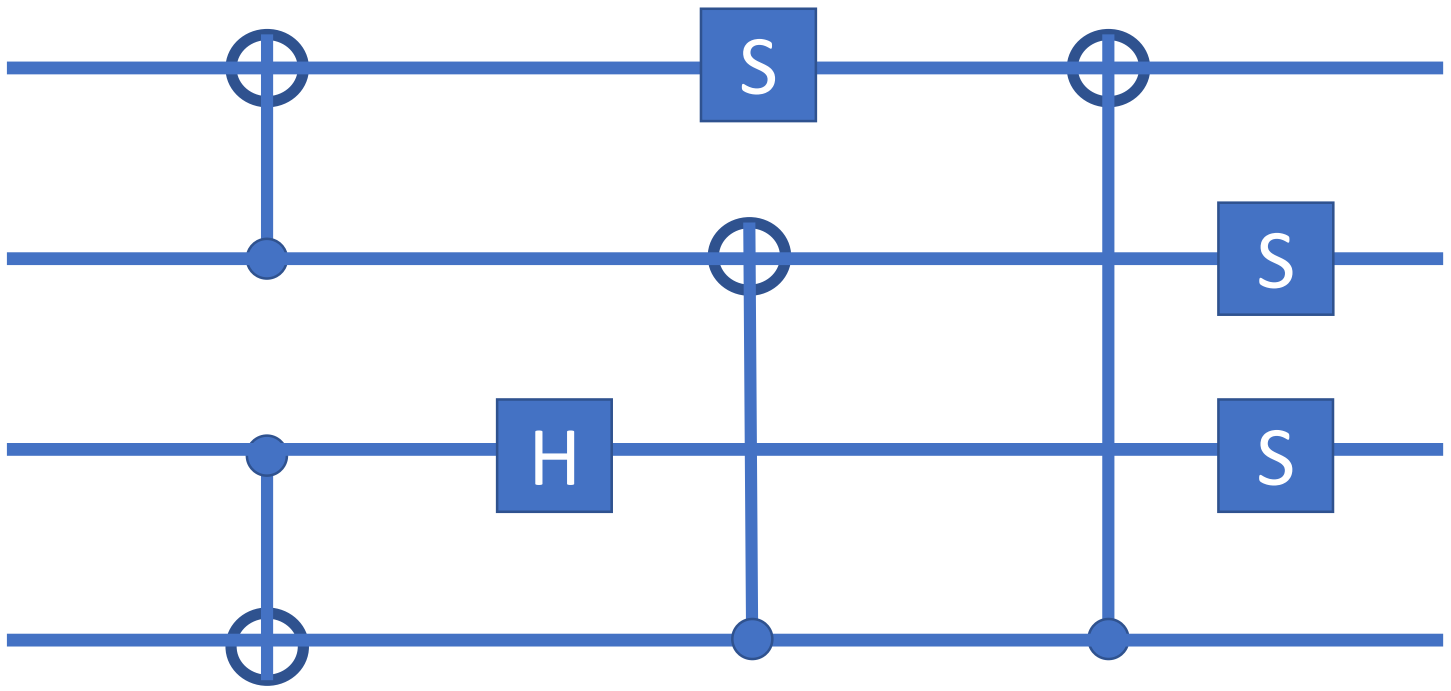
A **depth-*d* quantum circuit** consists of d time steps.
Each time step contains one- and two-qubit gates acting on disjoint qubits.



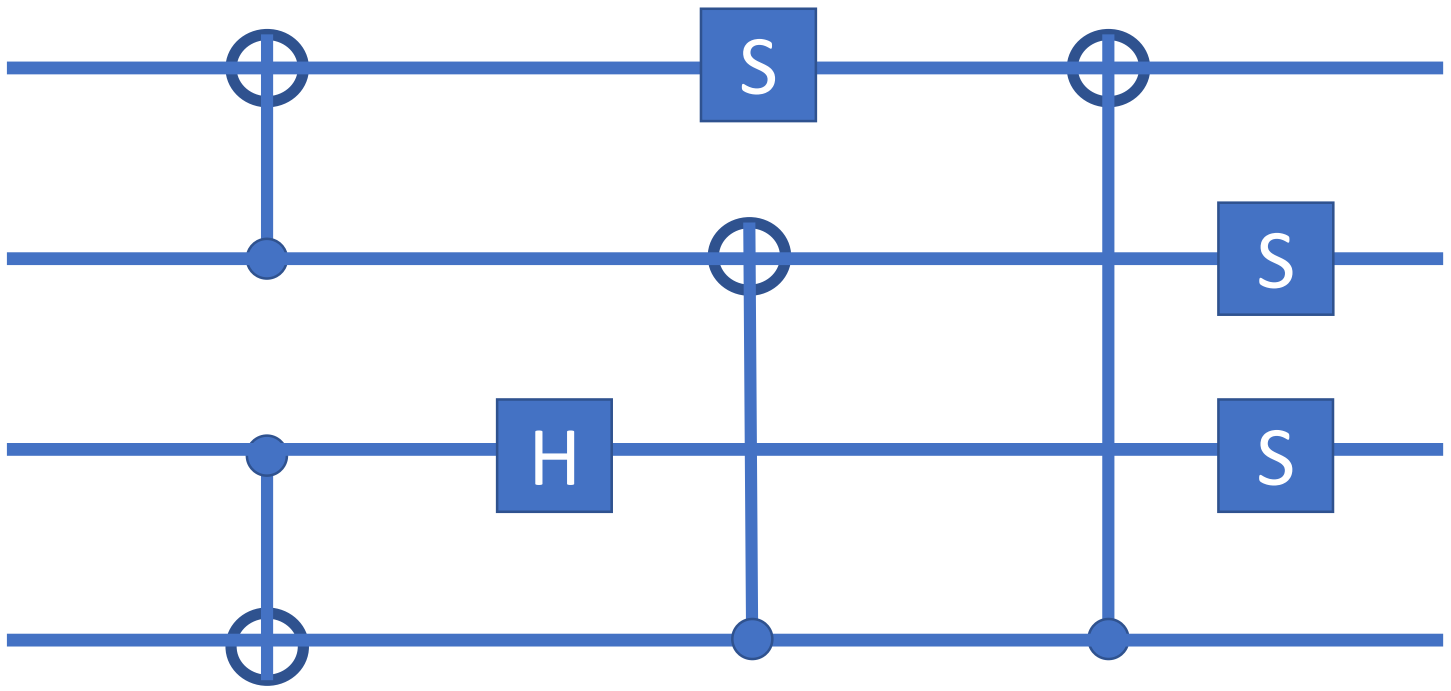
A **depth-*d* quantum circuit** consists of d time steps.
Each time step contains one- and two-qubit gates acting on disjoint qubits.



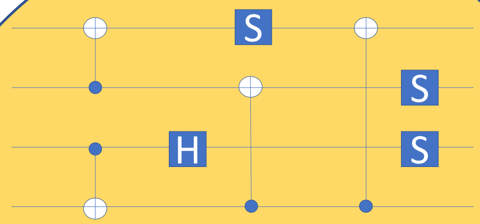
A **depth-d quantum circuit** consists of d time steps.
Each time step contains one- and two-qubit gates acting on disjoint qubits.



A **depth-d quantum circuit** consists of d time steps.
Each time step contains one- and two-qubit gates acting on disjoint qubits.



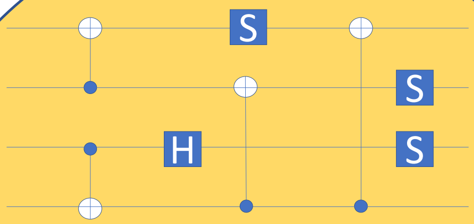
We are interested in **constant-depth quantum circuits**, for which $d = O(1)$.



Constant-depth quantum circuits

Constant-time quantum computation

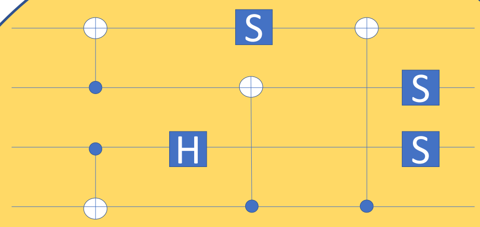
How much does parallelism buy us if we only have a fixed computation time?



Constant-depth quantum circuits

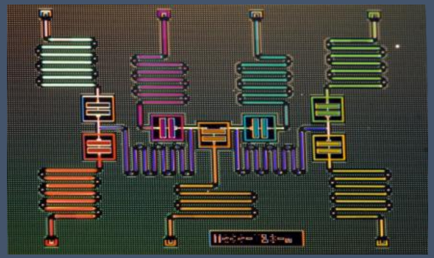
Constant-time quantum computation

How much does parallelism buy us if we only have a fixed computation time?



Constant-depth quantum circuits

Quantum algorithms for small quantum computers



Constant-time quantum computation

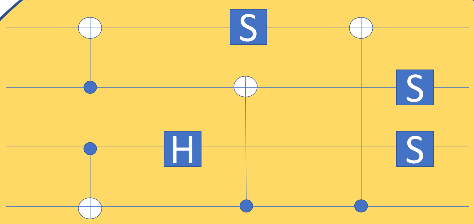
How much does parallelism buy us if we only have a fixed computation time?

Structure/Simulation

Cannot prepare codewords of good quantum codes [Eldar, Harrow 2015]

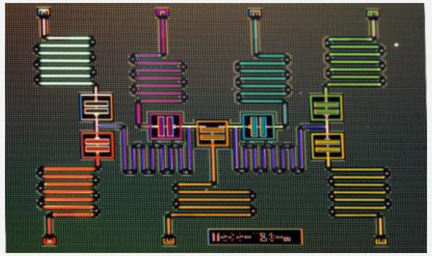
Efficient classical simulation of depth-2 circuits [Terhal, Divincenzo 2002]

General simulation algorithms (superpolynomial) [Aaronson, Chen 2016]



Constant-depth quantum circuits

Quantum algorithms for small quantum computers



Constant-time quantum computation

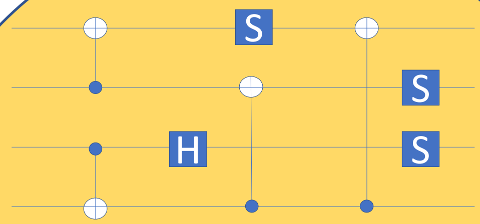
How much does parallelism buy us if we only have a fixed computation time?

Structure/Simulation

Cannot prepare codewords of good quantum codes
[Eldar, Harrow 2015]

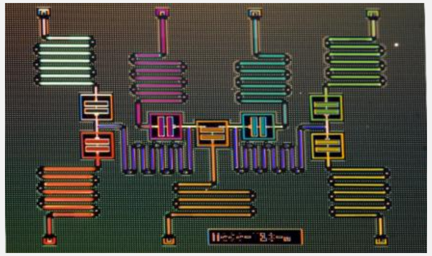
Efficient classical simulation of depth-2 circuits
[Terhal, Divincenzo 2002]

General simulation algorithms (superpolynomial)
[Aaronson, Chen 2016]



Constant-depth quantum circuits

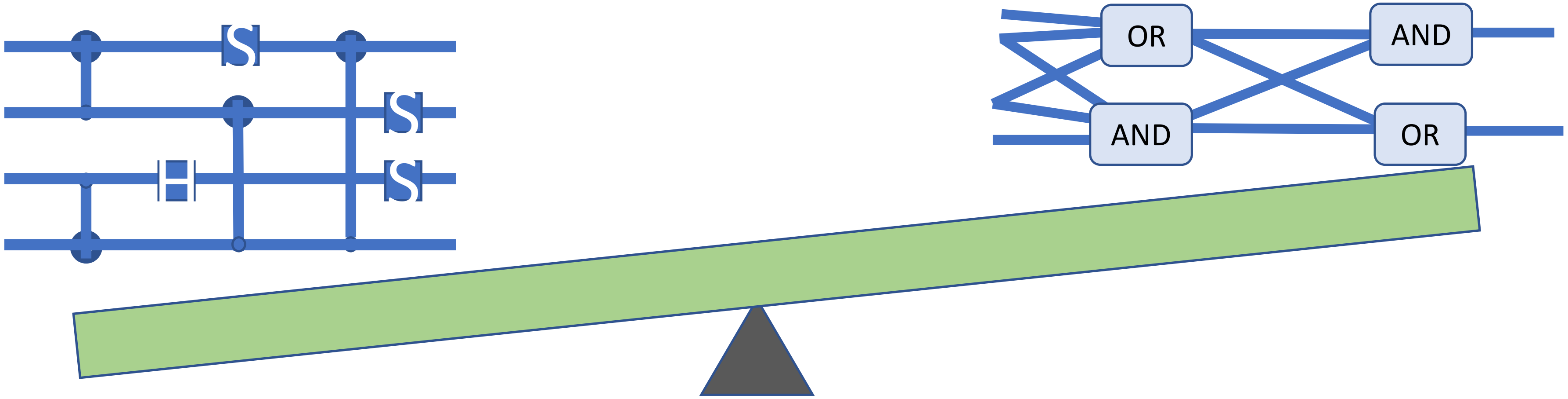
Quantum algorithms for small quantum computers



Beat poly-time classical computation?

Constant-depth unlikely to be classically simulable.
[Terhal, Divincenzo 02]

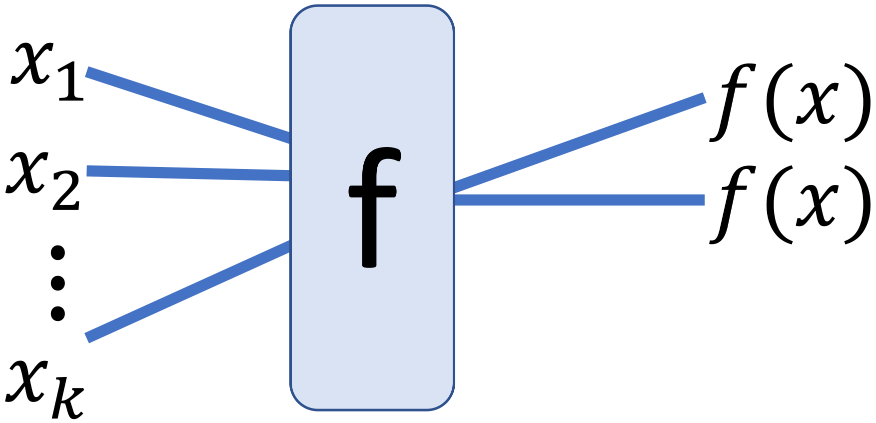
Beat the best classical computers for some task?
[Gao et al. 17]
[Bermejo-Vega et al. 17]
…uses IQP results…
[Bremner, Montanaro, Shepherd 16]



This talk: Are constant-depth quantum circuits more powerful than constant-depth classical circuits?

Classical circuits

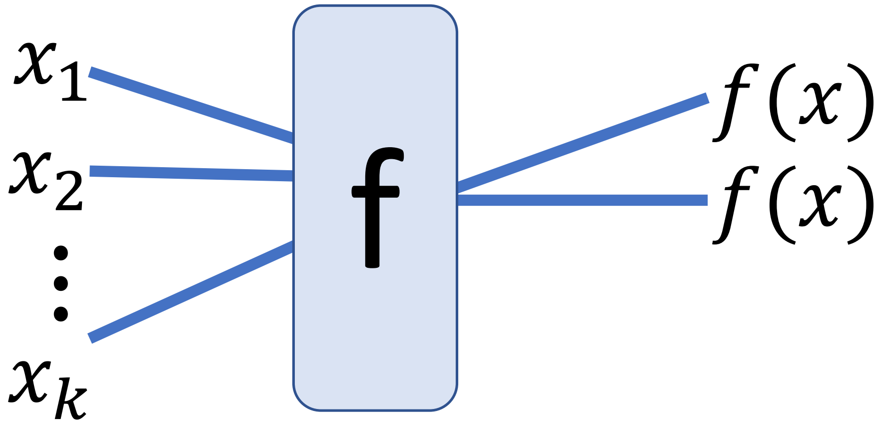
A classical gate computes a boolean function $f: \{0,1\}^k \rightarrow \{0,1\}$



Classical circuits

A classical gate computes a boolean function $f\colon \{0,1\}^k \to \{0,1\}$

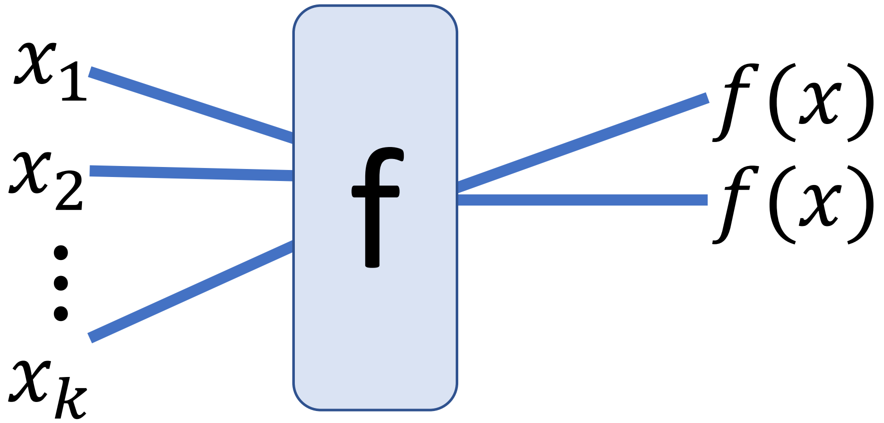
Number of input bits k is called the **fan-in**



Classical circuits

A classical gate computes a boolean function $f\colon\{0,1\}^k \to \{0,1\}$

Number of input bits k is called the **fan-in**

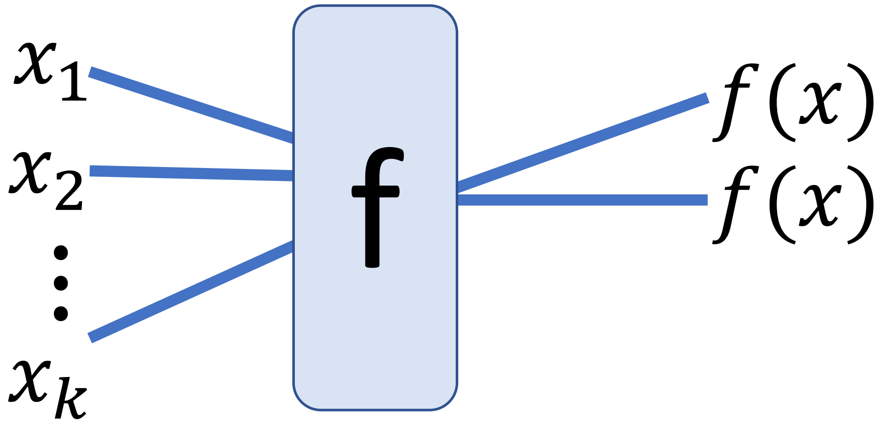


Number of times the output is used is called the **fan-out**

Classical circuits

A classical gate computes a boolean function $f: \{0,1\}^k \rightarrow \{0,1\}$

Number of input bits k is called the **fan-in**



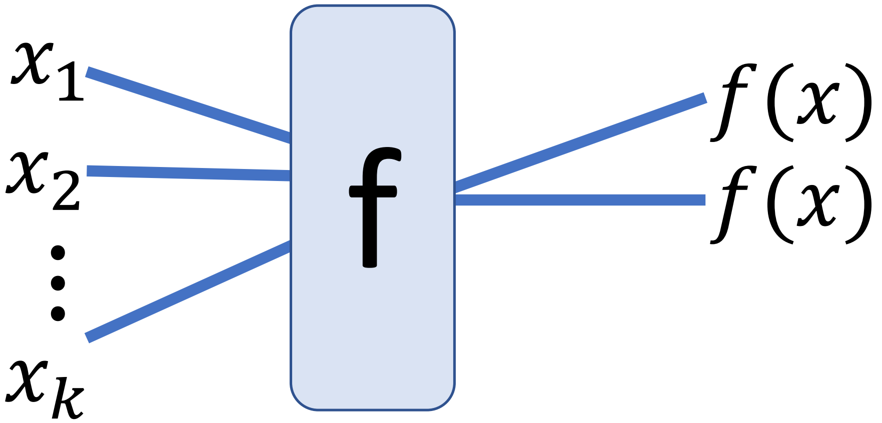
Number of times the output is used is called the **fan-out**

We consider circuits composed of **bounded fan-in gates**, i.e., $k = O(1)$.
We do not restrict the fan-out.

Classical circuits

A classical gate computes a boolean function $f: \{0,1\}^k \to \{0,1\}$

Number of input bits k is called the **fan-in**

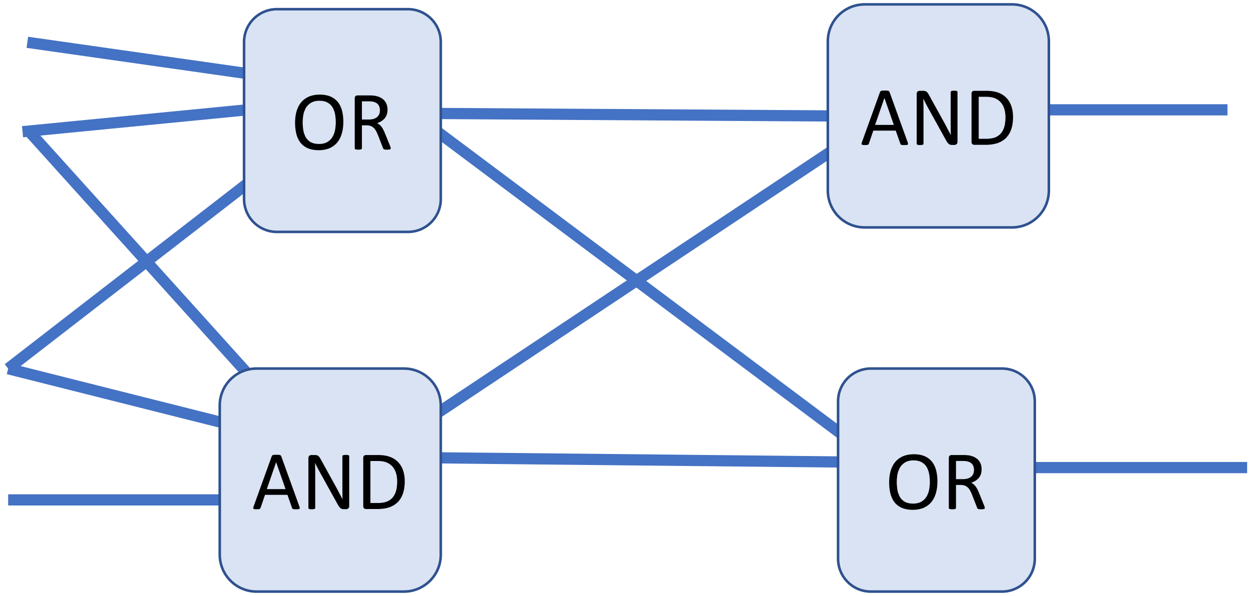


Number of times the output is used is called the **fan-out**

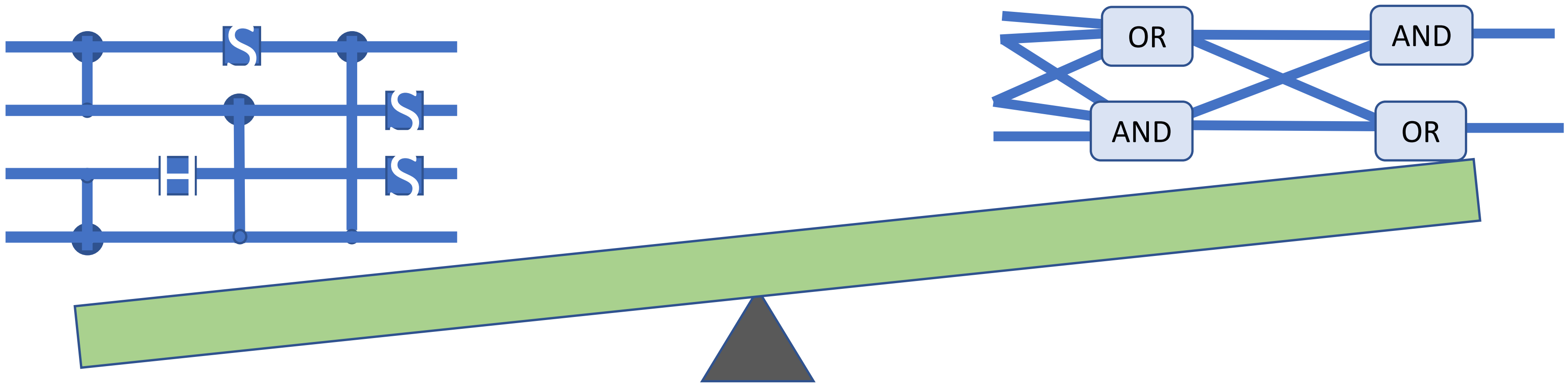
We consider circuits composed of **bounded fan-in gates**, i.e., $k = O(1)$.
We do not restrict the fan-out.

Constant-depth classical circuits

A depth-d classical circuit consists of d layers (time steps) of gates.



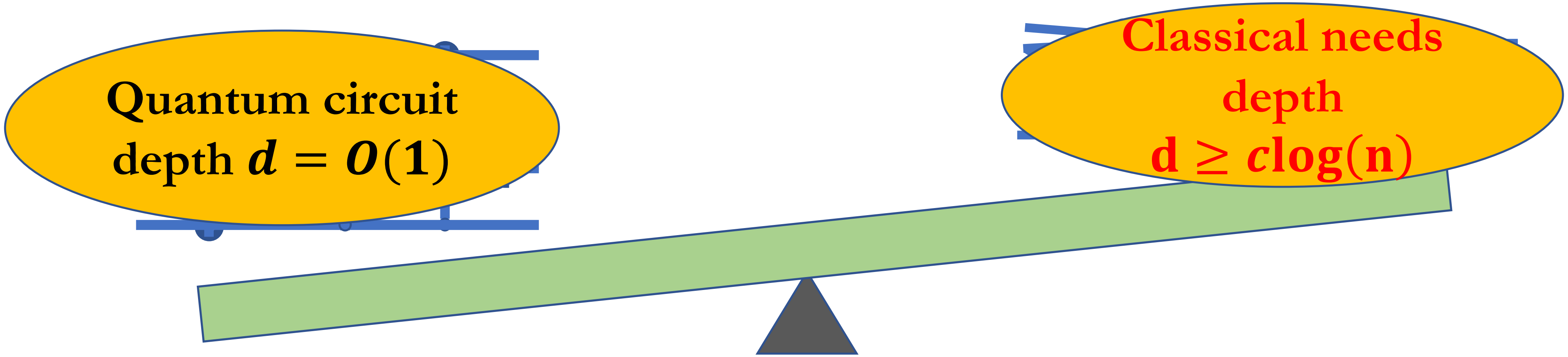
We consider constant-depth circuits composed of bounded fan-in gates.
This class of circuits is known as NC^0.
We also allow the circuit to be probabilistic (random input bits are provided).



Our result:

We describe a computational problem that is solved with certainty by a constant-depth quantum circuit.

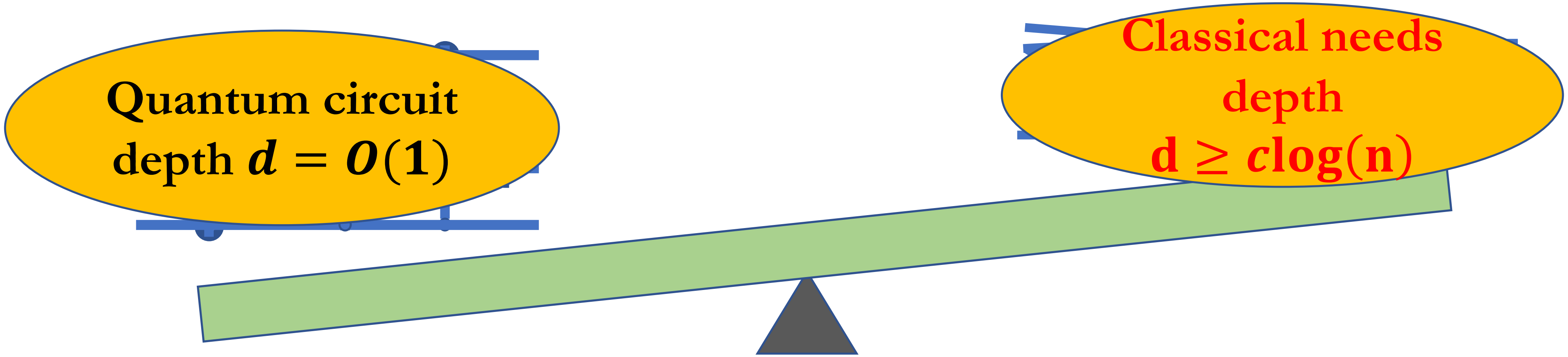
We prove that any classical circuit which solves the problem with high probability must have depth increasing logarithmically with input size.



Our result:

We describe a computational problem that is solved with certainty by a constant-depth quantum circuit.

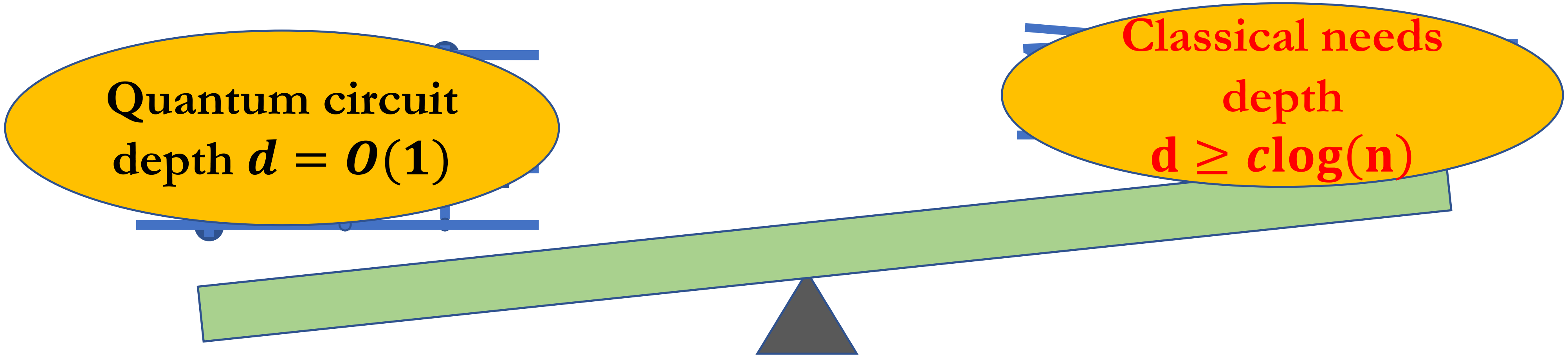
We prove that any classical circuit which solves the problem with high probability must have depth increasing logarithmically with input size.



Our result:

We describe a computational problem that is solved with certainty by a constant-depth quantum circuit **(also: all gates act locally on a 2D grid).**

We prove that any classical circuit which solves the problem with high probability must have depth increasing logarithmically with input size.



Our result:

We describe a computational problem that is solved with certainty by a constant-depth quantum circuit **(also: all gates act locally on a 2D grid).**

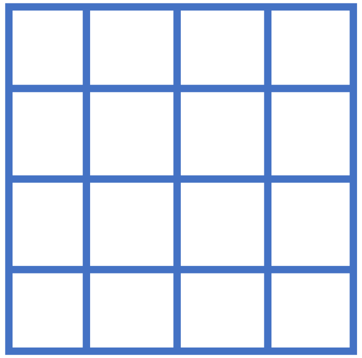
We prove that any classical circuit which solves the problem with high probability must have depth increasing logarithmically with input size.

The quantum speedup is unconditional
(does not rely on complexity-theoretic conjectures and is non-oracular)

II. The 2D Hidden Linear Function Problem

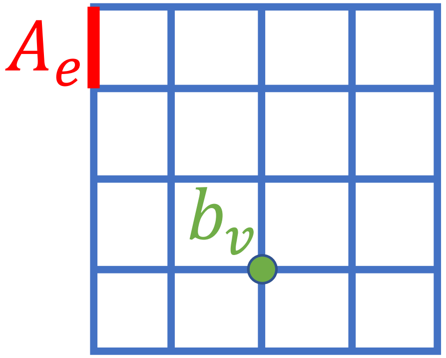
Quadratic form on a grid

Let $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ be an $\mathrm{N} \times \mathrm{N}$ grid graph. Write $n = N^2 = |V|$



Quadratic form on a grid

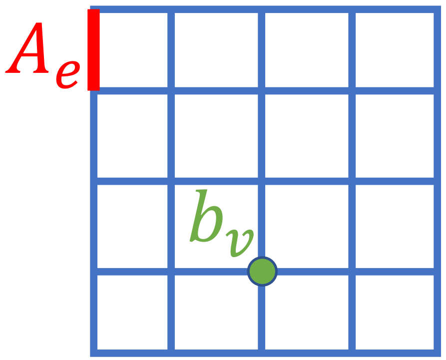
Let $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ be an $\mathrm{N} \times \mathrm{N}$ grid graph.   Write $n = N^2 = |V|$



Choose coefficients $A_e \in \{0,1\}$ for each edge and $b_v \in \{0,1\}$ for each vertex.

Quadratic form on a grid

Let $G = (V, E)$ be an $N \times N$ grid graph. Write $n = N^2 = |V|$



Choose coefficients $A_e \in \{0,1\}$ for each edge and $b_v \in \{0,1\}$ for each vertex.

Any choice of coefficients defines a quadratic form $q\colon \{0,1\}^n \to \mathbb{Z}_4$

$$q(x) = \sum_{e=(v,w)\in E} 2A_e x_v x_w - \sum_{v\in V} b_v x_v$$

The quadratic form hides a linear function

Define a set

$$\mathcal{L}_q = \{x \in \mathbb{F}_2^n\colon\ q(x \oplus y) = q(x) + q(y)\ \text{ for all } y \in \mathbb{F}_2^n\}$$

The quadratic form hides a linear function

Define a set

$$\mathcal{L}_q = \{x \in \mathbb{F}_2^n\colon\; q(x \oplus y) = q(x) + q(y) \;\text{ for all } y \in \mathbb{F}_2^n\}$$

Lemma
The set $\mathcal{L}_q$ is a linear subspace of $\mathbb{F}_2^n$. Furthermore, there is a "secret" bit string $z \in \{0,1\}^n$ such that

$$q(x) = 2z^T x \qquad \forall x \in \mathcal{L}_q$$

The quadratic form hides a linear function

Define a set

$$\mathcal{L}_q = \{x \in \mathbb{F}_2^n : \; q(x \oplus y) = q(x) + q(y) \; \text{ for all } y \in \mathbb{F}_2^n\}$$

Lemma
The set $\mathcal{L}_q$ is a linear subspace of $\mathbb{F}_2^n$. Furthermore, there is a "secret" bit string $z \in \{0,1\}^n$ such that

$$q(x) = 2z^T x \qquad \forall x \in \mathcal{L}_q$$

Define a computational problem where the goal is to find a secret bit string…

The 2D Hidden Linear Function Problem

Input: Coefficients $A \in \{0,1\}^{|E|}$ and $b \in \{0,1\}^{|V|}$.

Specifies a quadratic form $\boldsymbol{q(x)}$ and a subspace $\boldsymbol{\mathcal{L}_q \subseteq \mathbb{F}_2^n}$

The 2D Hidden Linear Function Problem

Input: Coefficients $A \in \{0,1\}^{|E|}$ and $b \in \{0,1\}^{|V|}$.

Specifies a quadratic form $\boldsymbol{q(x)}$ and a subspace $\boldsymbol{\mathcal{L}_q \subseteq \mathbb{F}_2^n}$

Output: A "secret" bit string $z \in \{0,1\}^n$ such that

$$q(x) = 2z^T x \quad \forall x \in \mathcal{L}_q$$

The 2D Hidden Linear Function Problem

Input: Coefficients $A \in \{0,1\}^{|E|}$ and $b \in \{0,1\}^{|V|}$.

Specifies a quadratic form $q(x)$ and a subspace $\mathcal{L}_q \subseteq \mathbb{F}_2^n$

Output: A "secret" bit string $z \in \{0,1\}^n$ such that

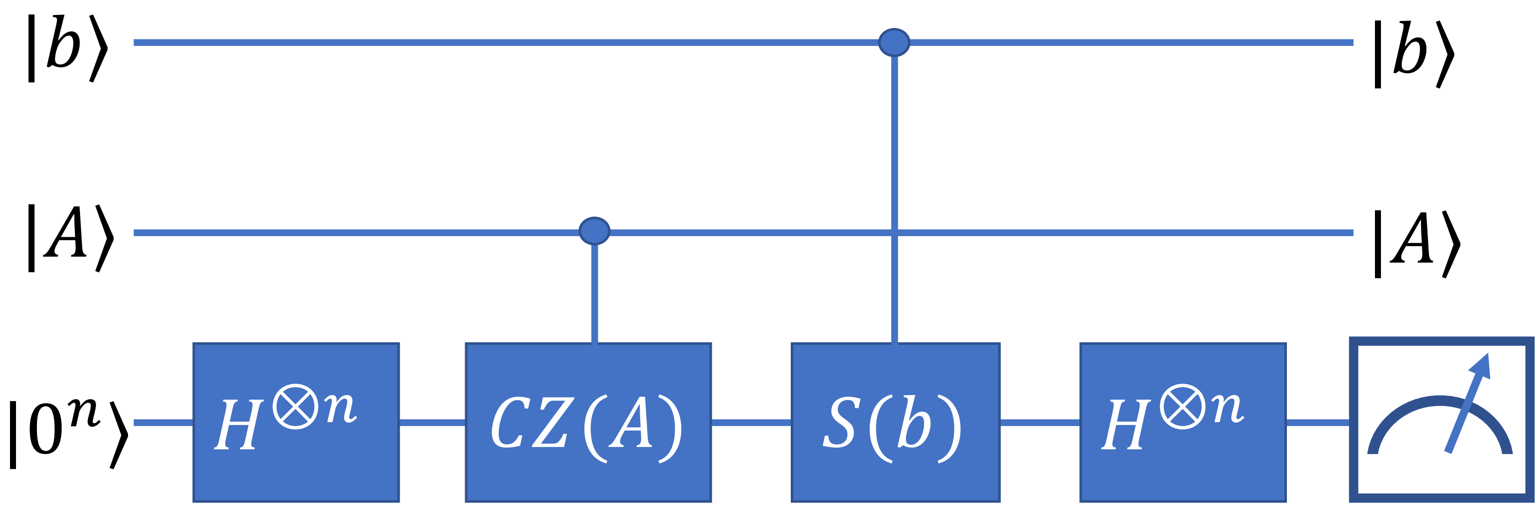
$$q(x) = 2z^T x \quad \forall x \in \mathcal{L}_q$$

Can be viewed as a non-oracular version of the Bernstein-Vazirani problem.
[Bernstein Vazirani 1993]

In general each instance of the 2D HLF has many valid solutions z .

Quantum algorithm

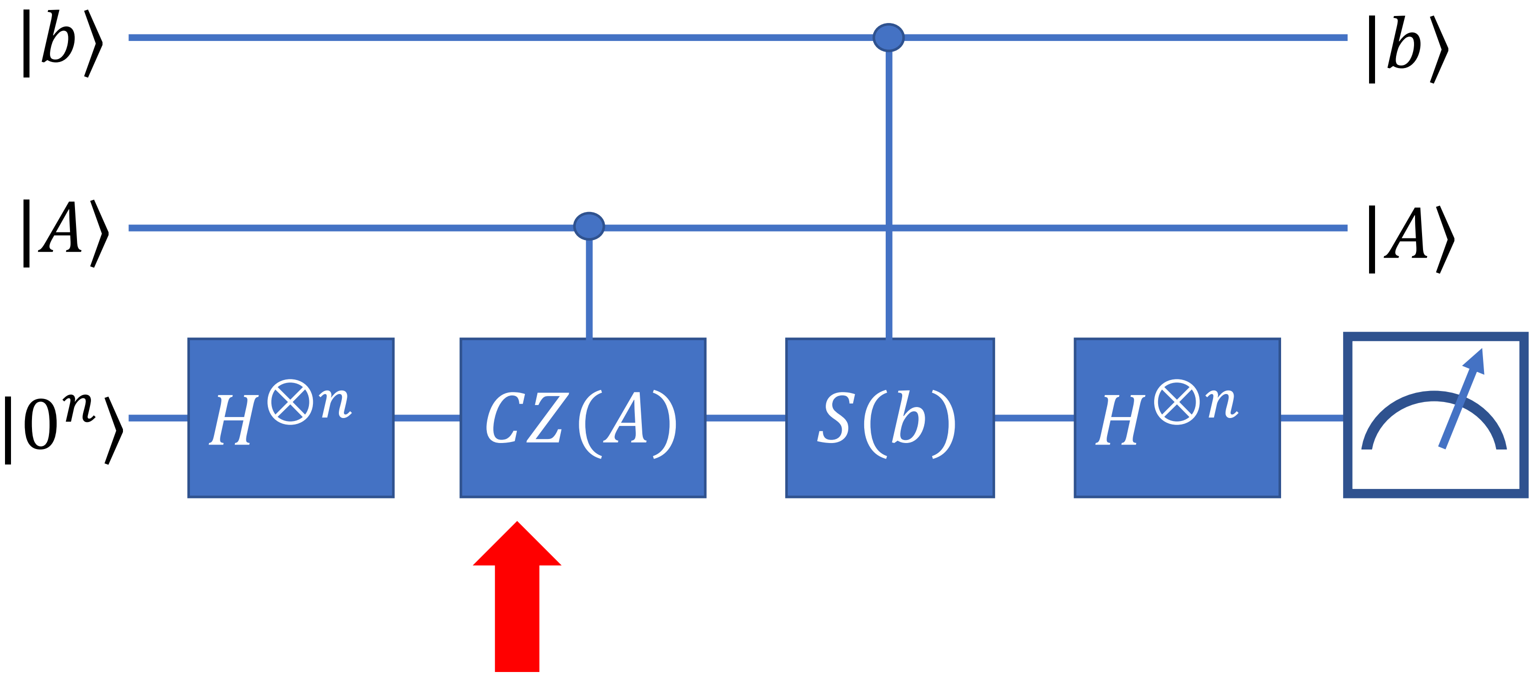
A qubit for each vertex of the $N \times N$ grid



Output
$z \in \{0,1\}^n$

Quantum algorithm

A qubit for each vertex of the $N \times N$ grid

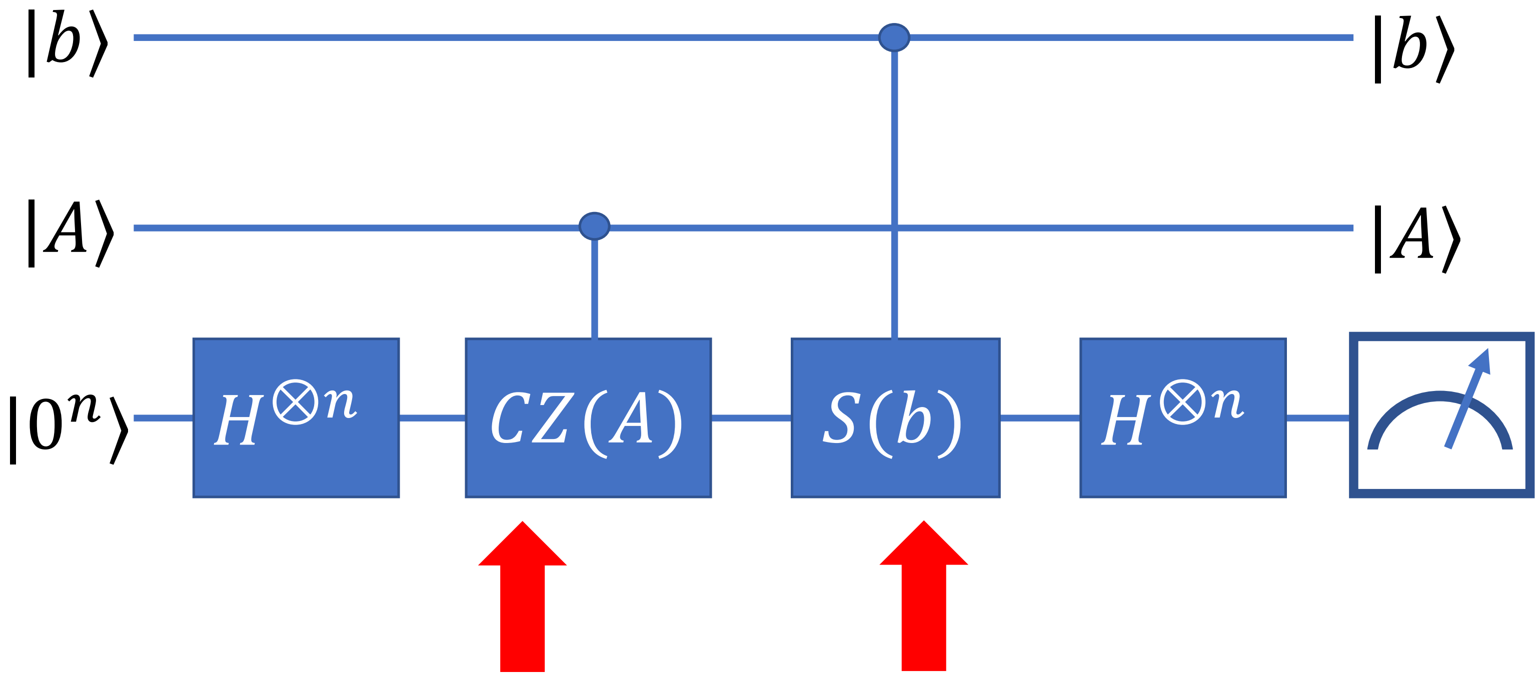


Output
$z \in \{0,1\}^n$

Apply $\mathrm{CZ}_{\mathrm{v,w}}$ for edges $e = \{v, w\}$ with $\mathrm{A_e} = 1$

Quantum algorithm

A qubit for each vertex of the $N \times N$ grid



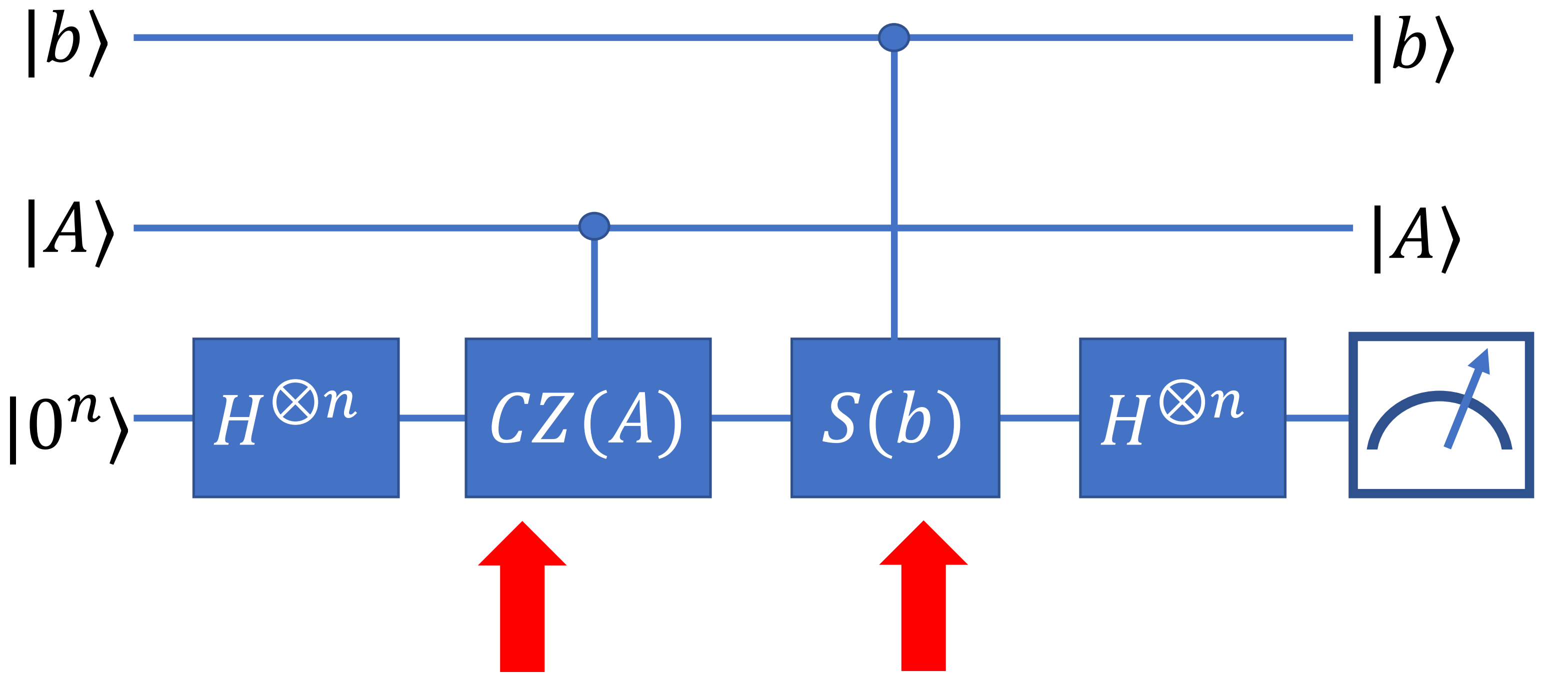
Output
$z \in \{0,1\}^n$

Apply $\mathrm{CZ}_{\mathrm{v,w}}$ for edges $e = \{v, w\}$ with $\mathrm{A_e} = 1$

Apply phase gate S_v to qubits with $b_v = 1$

Quantum algorithm

A qubit for each vertex of the $N \times N$ grid



Output
$z \in \{0,1\}^n$

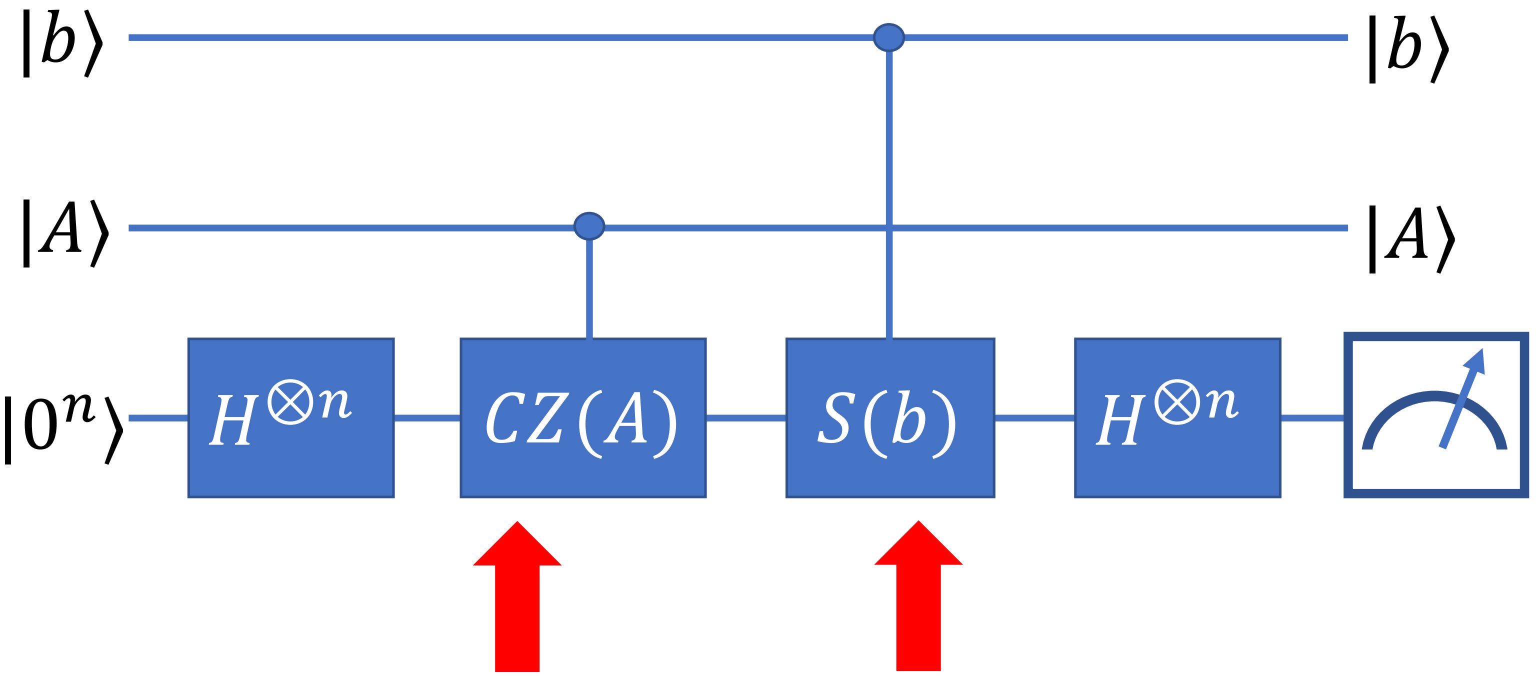
Apply $\mathrm{CZ}_{\mathrm{v,w}}$ for edges $e = \{v, w\}$ with $\mathrm{A_e} = 1$

Apply phase gate S_v to qubits with $b_v = 1$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

Quantum algorithm

A qubit for each vertex of the $N \times N$ grid



Output $z \in \{0,1\}^n$

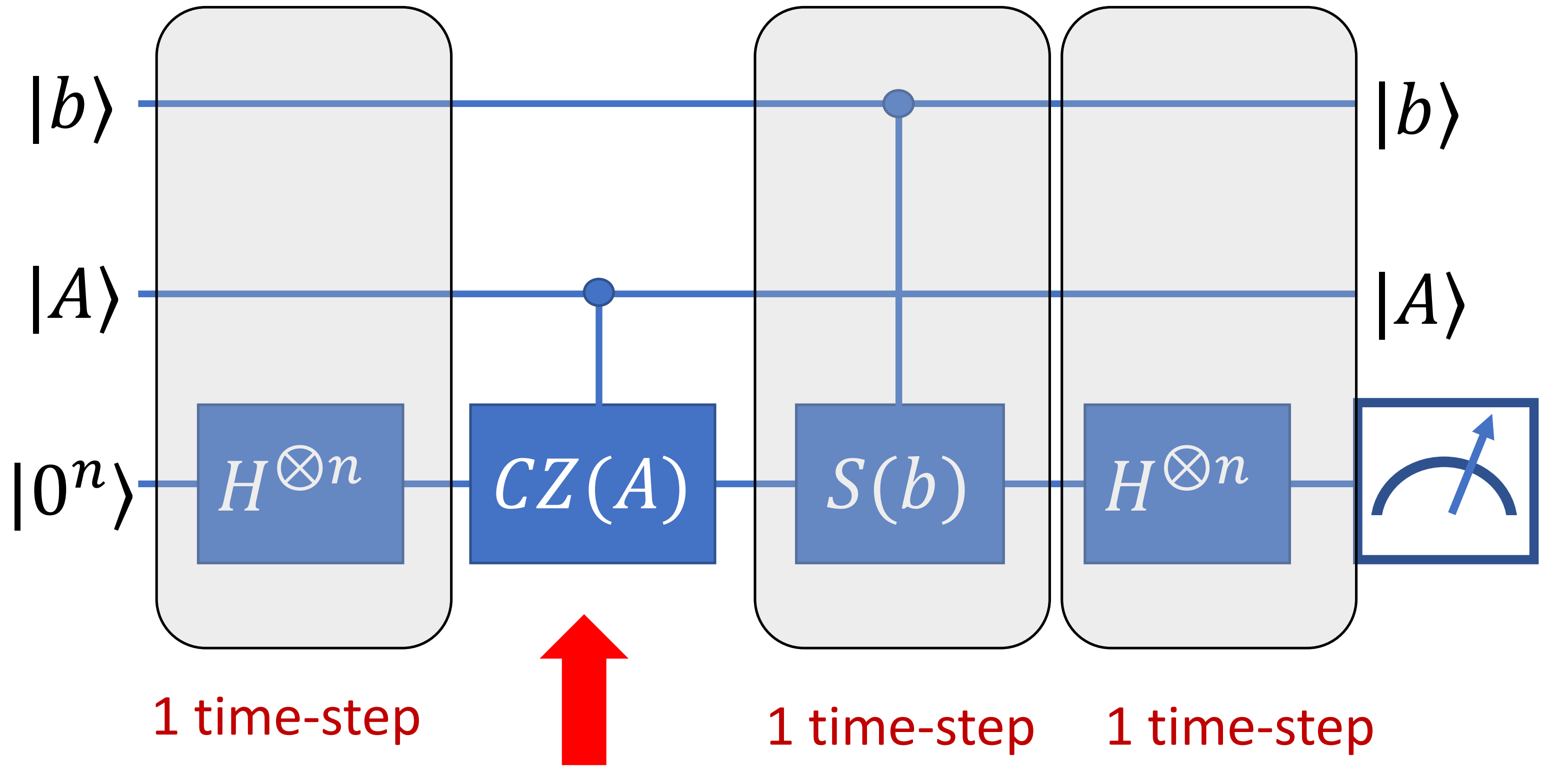
Apply $\mathrm{CZ}_{v,w}$ for edges $e = \{v, w\}$ with $\mathrm{A_e} = 1$

Apply phase gate S_v to qubits with $b_v = 1$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

Fact: The output z is a uniformly random solution to the 2D HLF Problem.

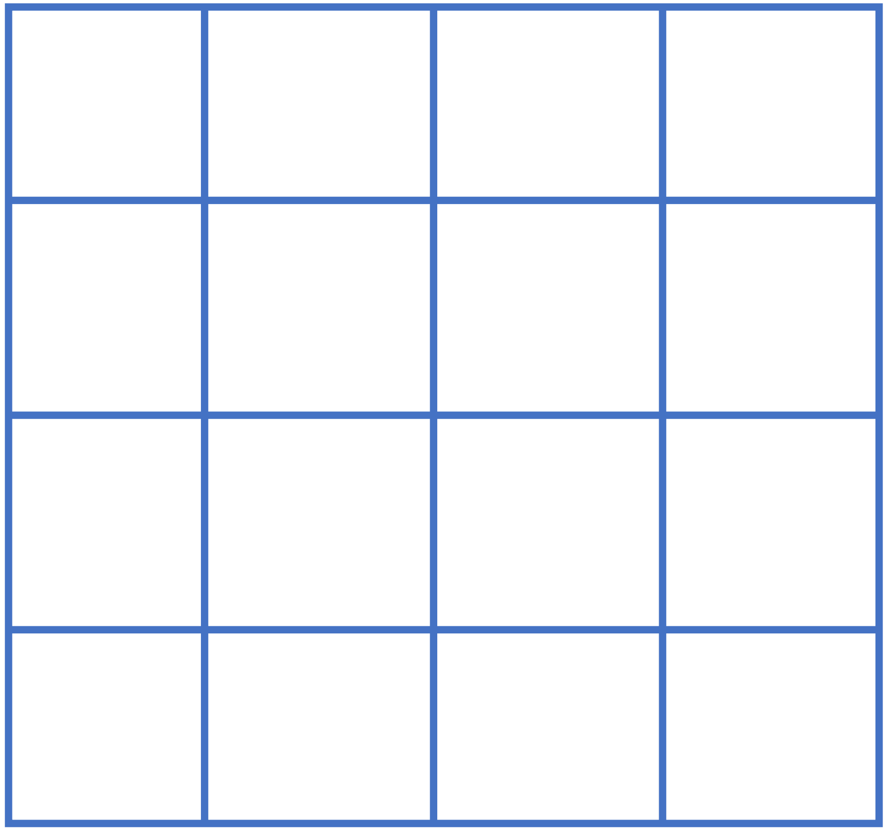
The algorithm can be implemented in constant-depth



Four layers of **CCZ** gates.
(even/odd vertical/horizontal edges)
Decompose **CCZ** gates into 1- and 2-qubit gates.

…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

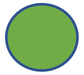
Example:



Place a qubit at each vertex

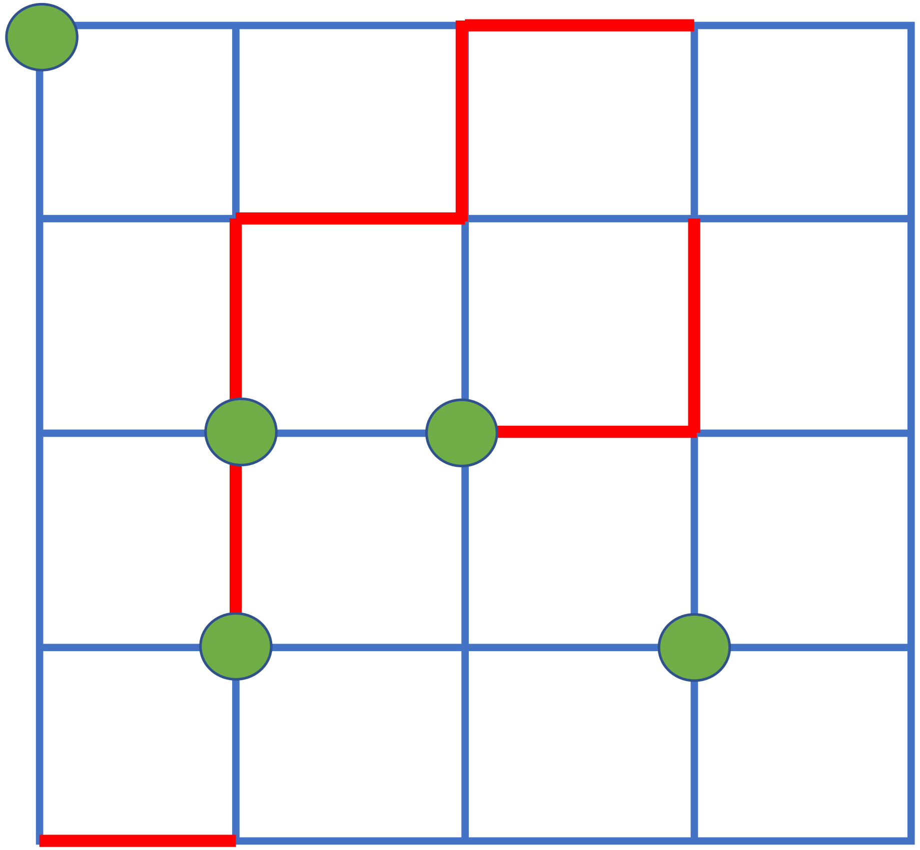
Place input bits on vertices and edges:

 : Edge with $A_e = 1$

 : Vertex with $b_v = 1$

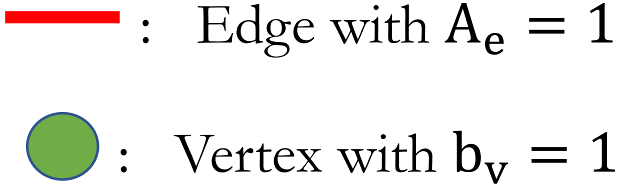
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



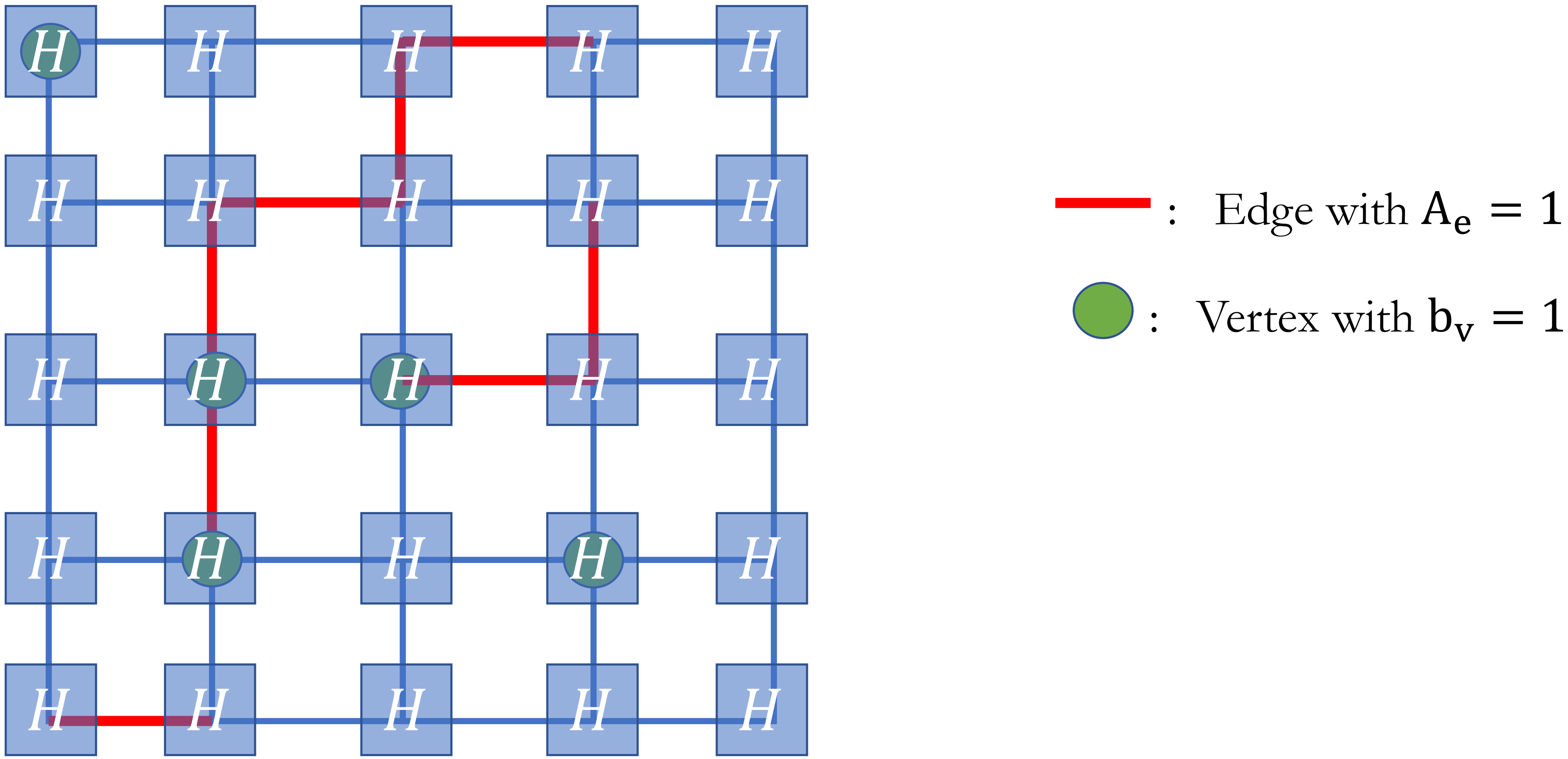
Place a qubit at each vertex

Place input bits on vertices and edges:



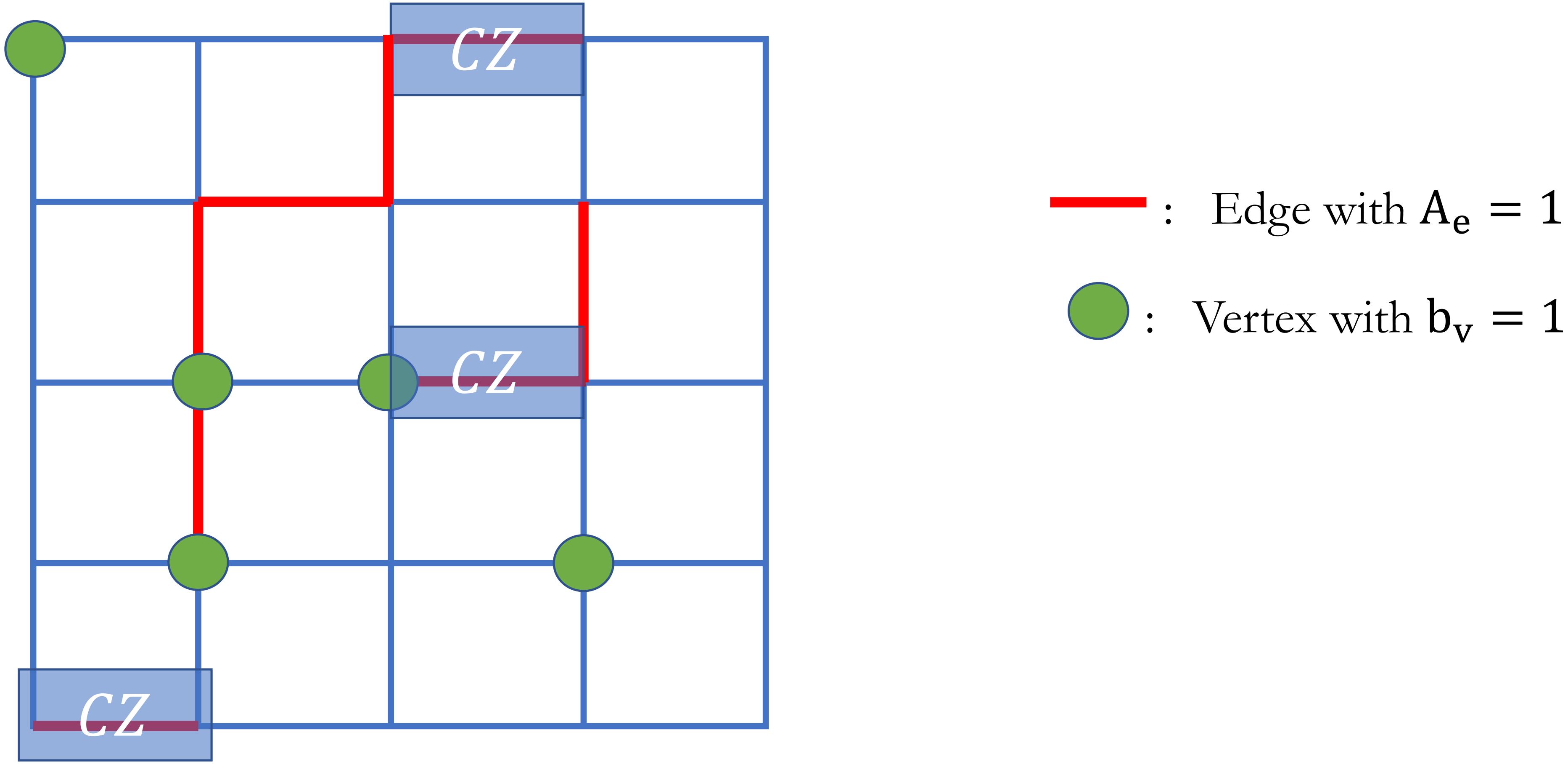
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



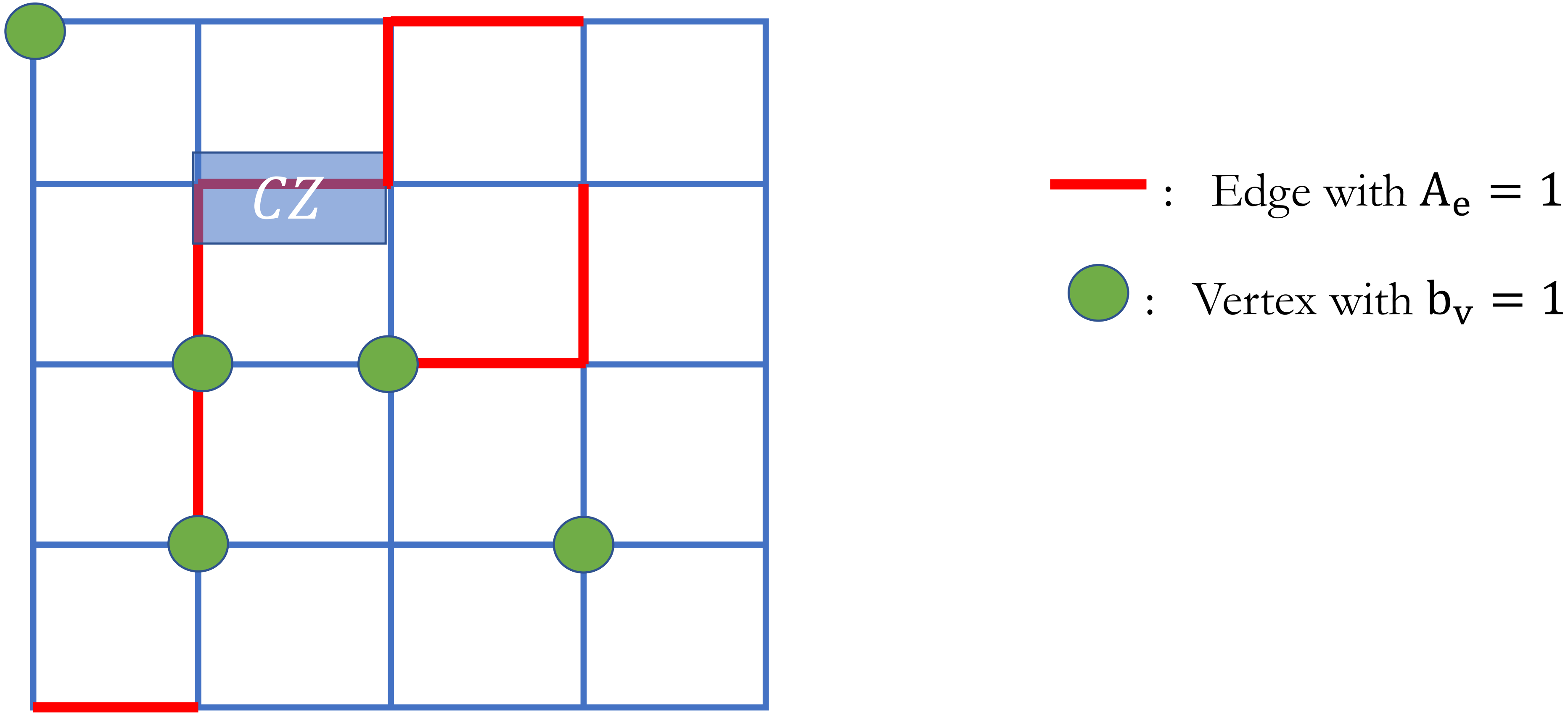
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



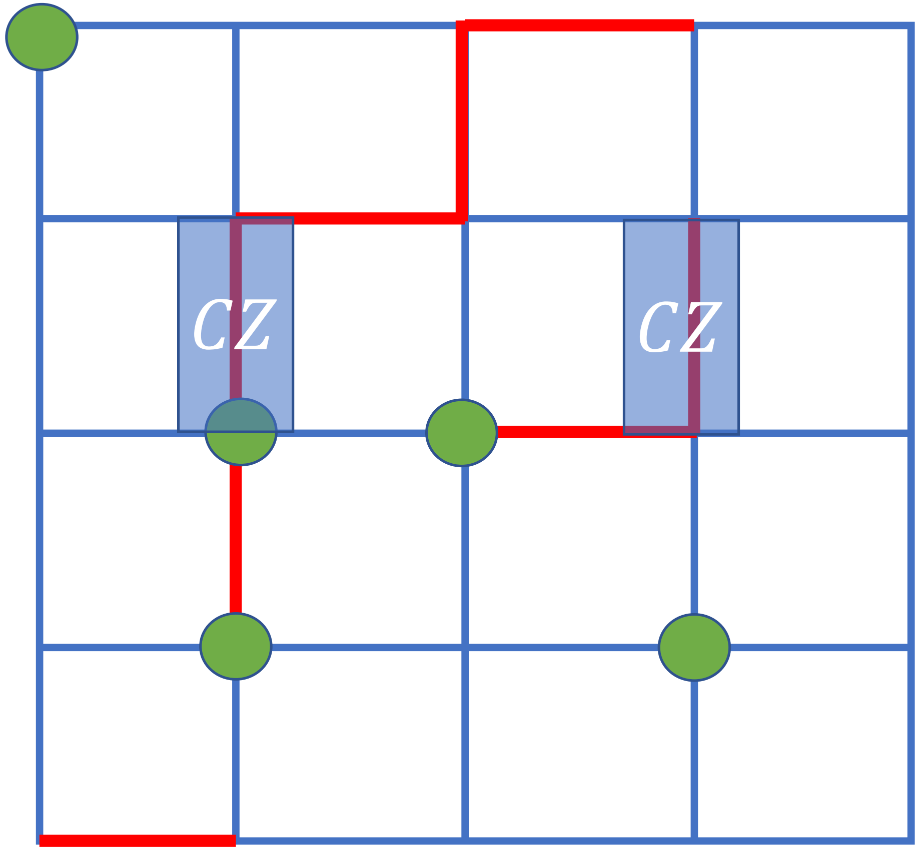
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:

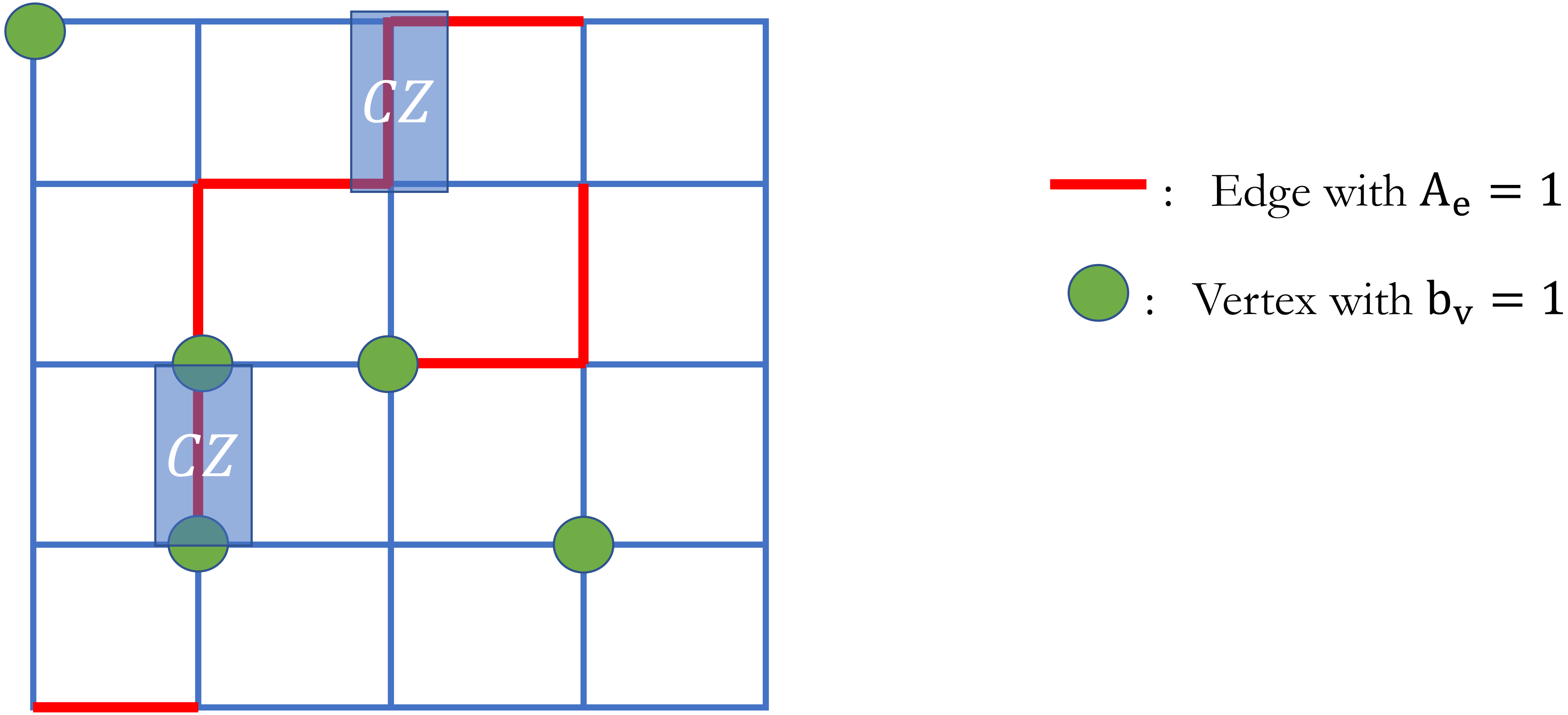


: Edge with $A_e = 1$

: Vertex with $b_v = 1$

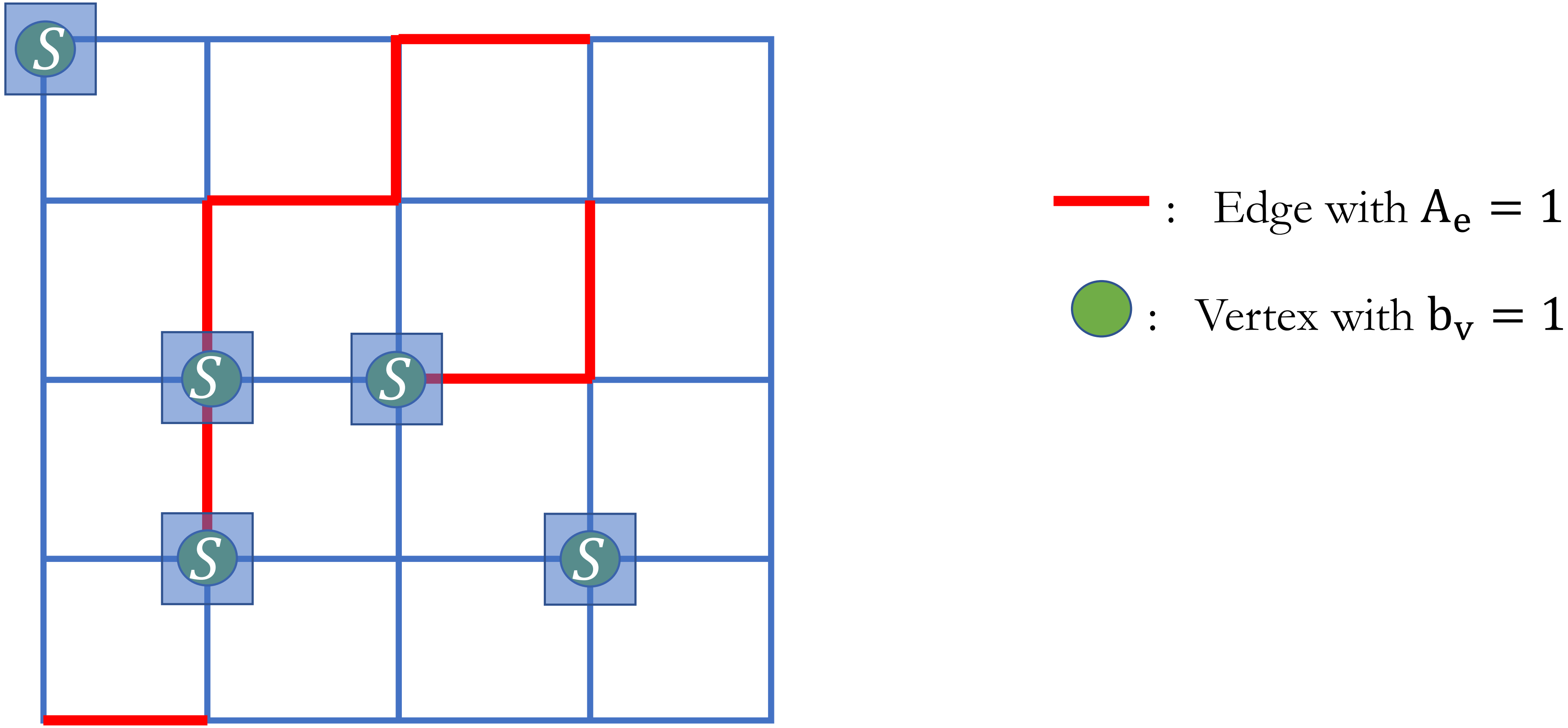
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



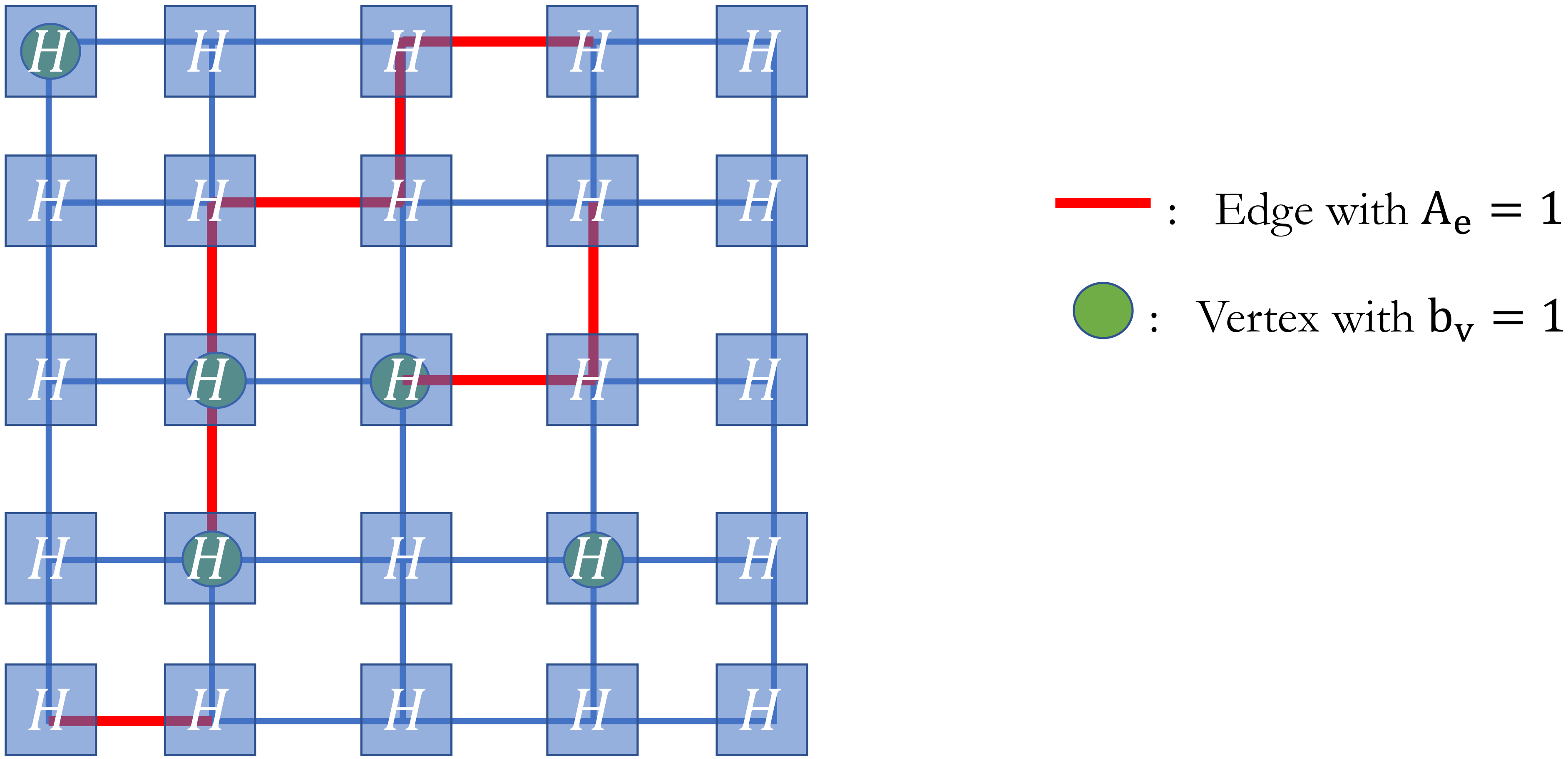
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



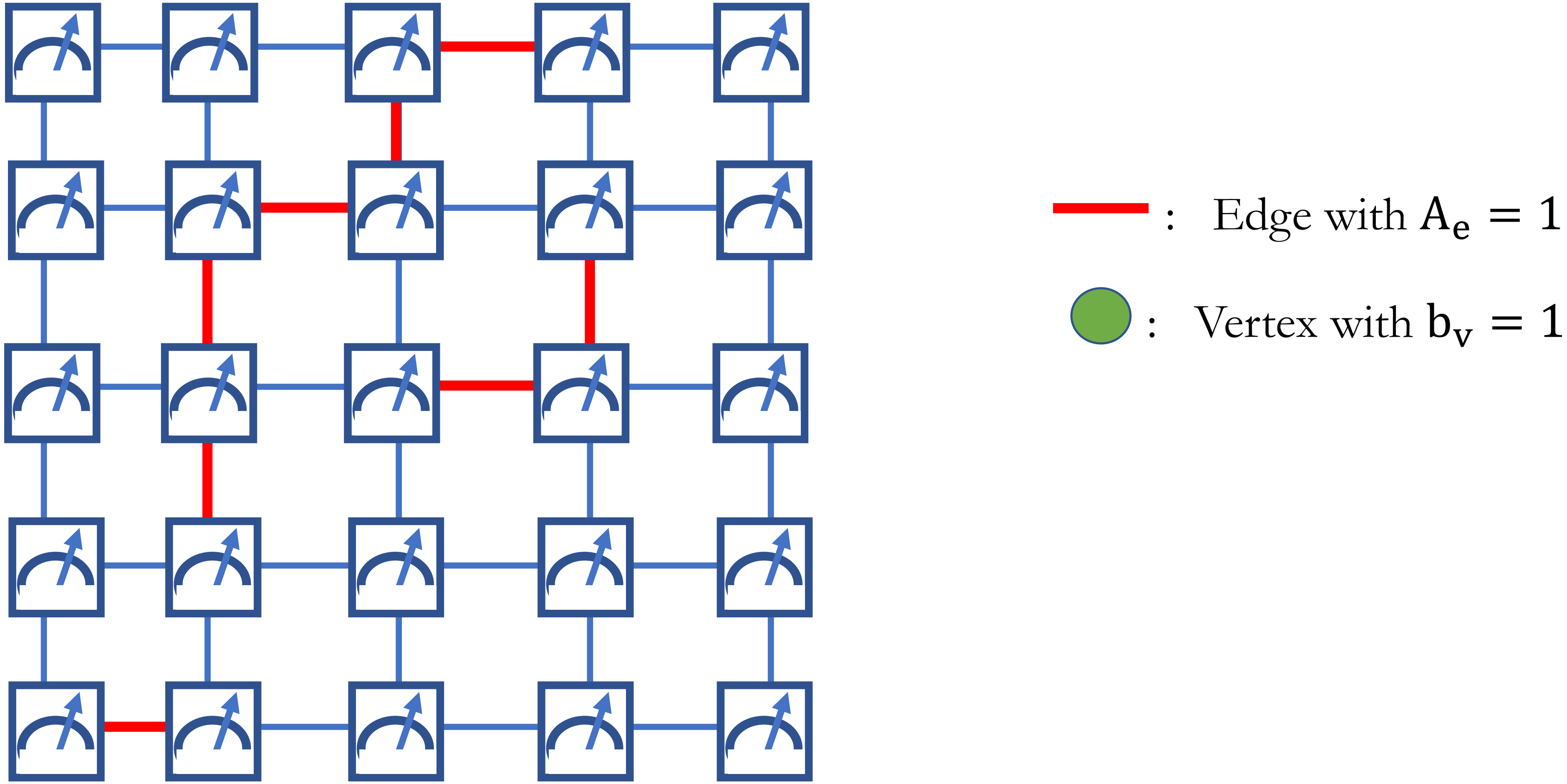
…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



…it only requires classically controlled Clifford gates between nearest neighbor qubits on a 2D grid.

Example:



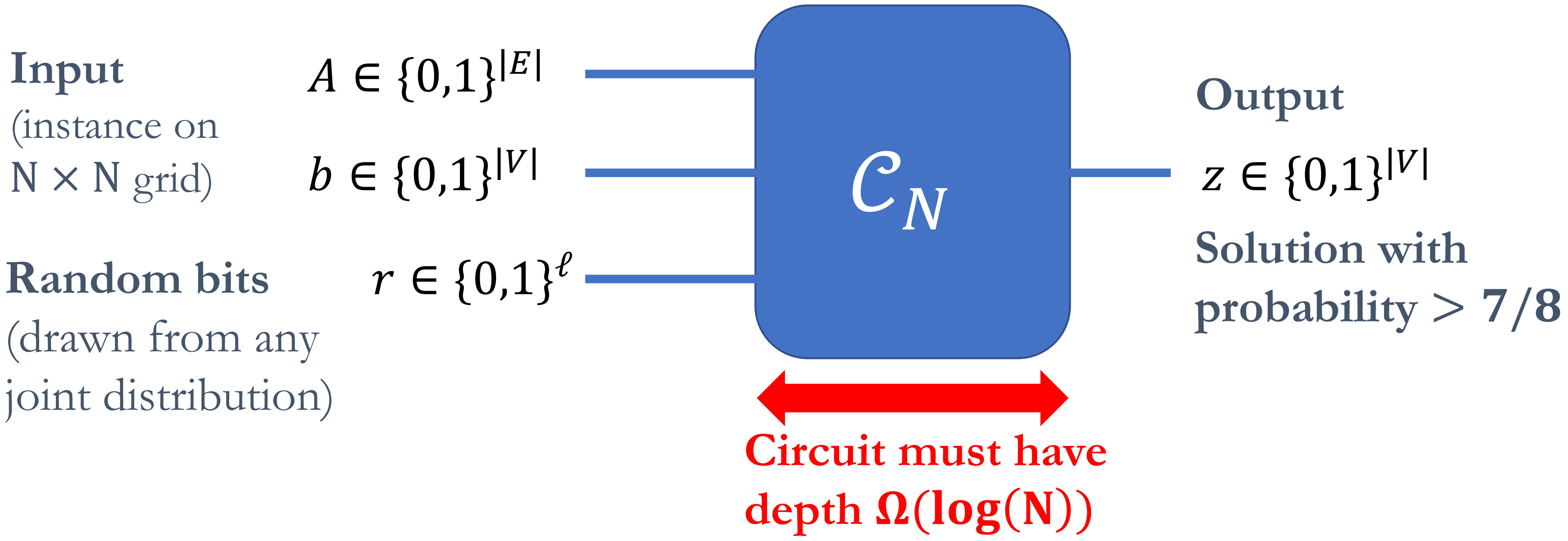
The 2D HLF problem is solved by a constant-depth quantum circuit with gates acting locally in 2D.

Next we show that it cannot be solved by a constant-depth classical circuit…

III. Classical lower bound

Theorem: The following holds for all sufficiently large N. Let $\mathcal{C}_N$ be a classical probabilistic circuit composed of gates of fan-in $\leq K$ which solves size-N instances of the 2D HLF Problem with probability greater than $7/8$. Then

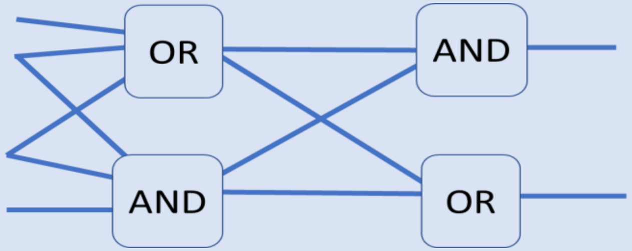
$$\mathrm{depth}(\mathcal{C}_N) \geq \frac{\log(N)}{8\log(K)}$$


Input
(instance on
N × N grid)
$A \in \{0,1\}^{|E|}$
$b \in \{0,1\}^{|V|}$
Random bits
(drawn from any
joint distribution)
$r \in \{0,1\}^{\ell}$
$\mathcal{C}_N$
Output
$z \in \{0,1\}^{|V|}$
Solution with
probability > 7/8
Circuit must have
depth $\Omega(\log(N))$

Proof Ideas

Locality in shallow classical circuits

Each output bit can only depend on $O(1)$ input bits.

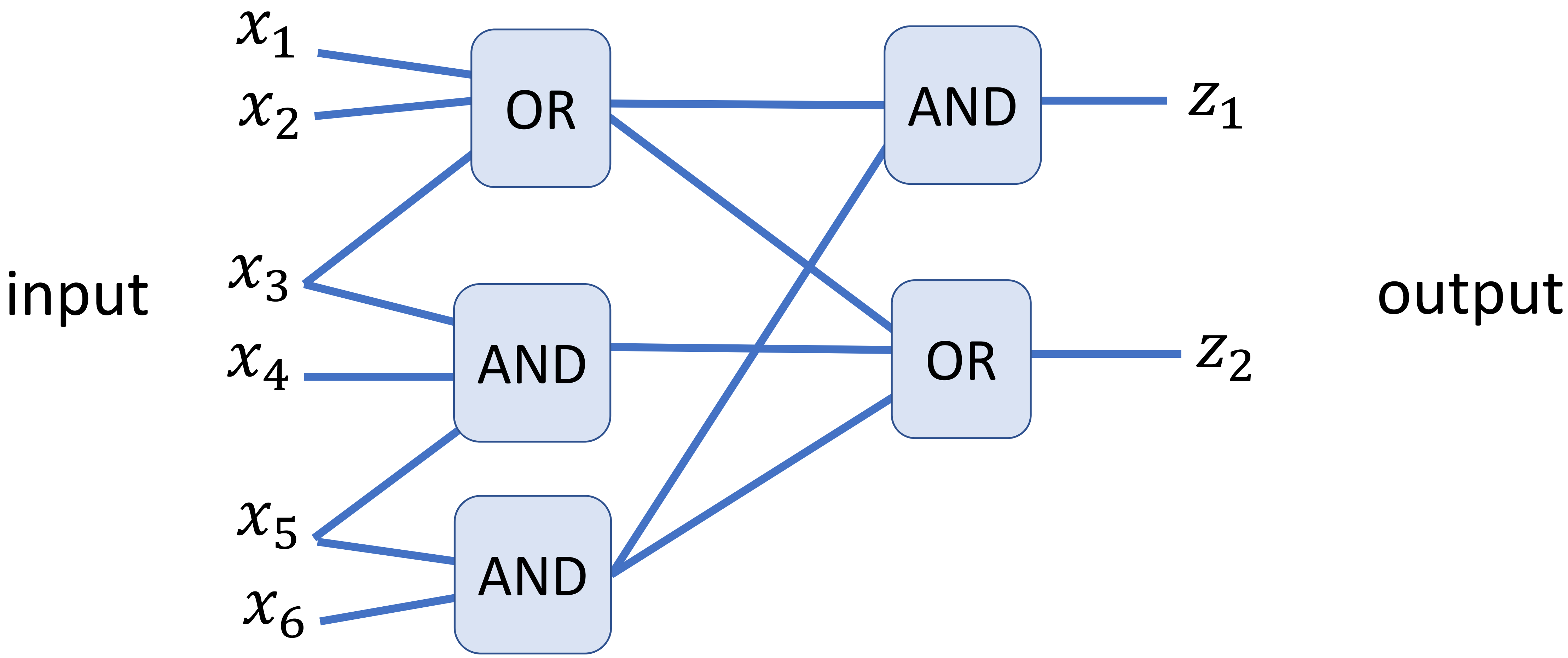


Vs.

Quantum nonlocality

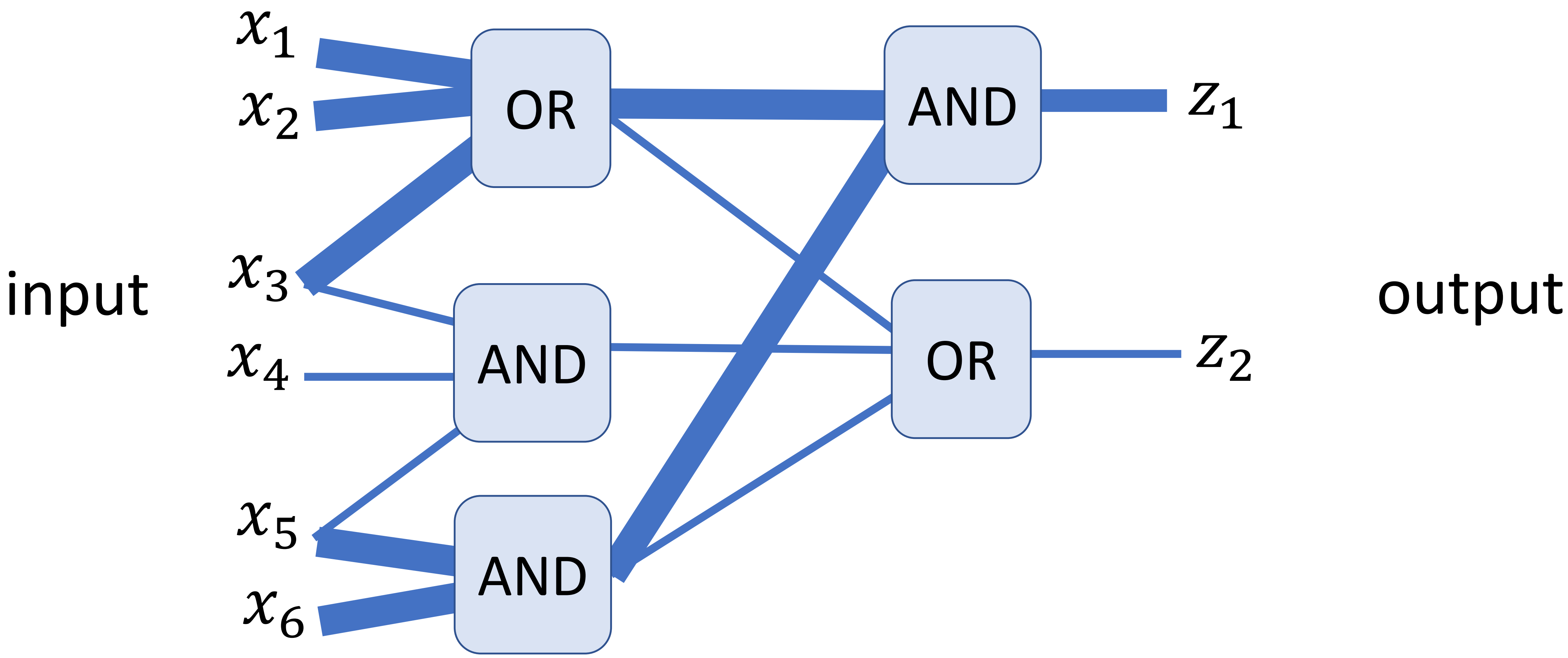
Measurement statistics of entangled quantum states cannot be reproduced by local hidden variable models

Locality in classical circuits



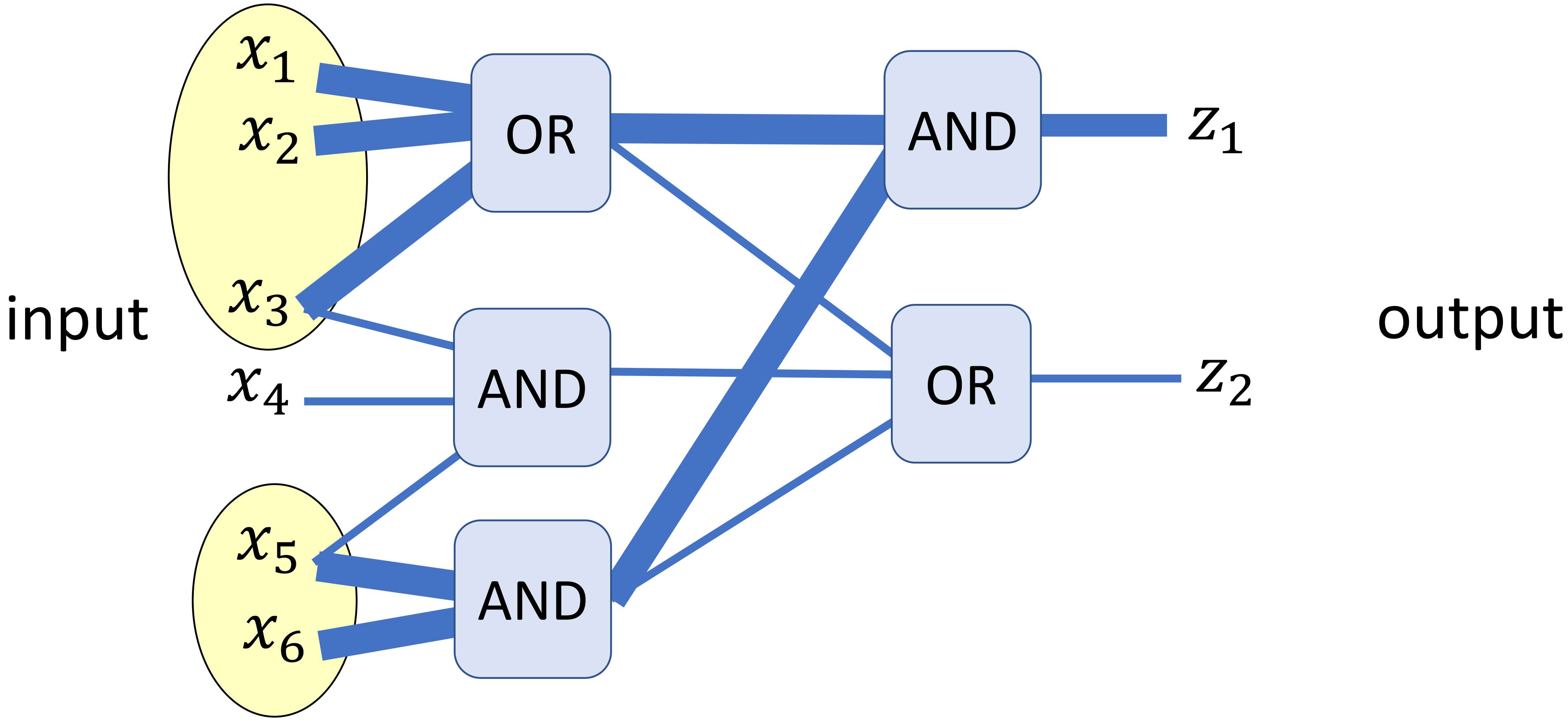
The **lightcone** $L(z_k)$ of an output bit z_k is the set of input bits x_i that are causally connected to z_k.

Locality in classical circuits



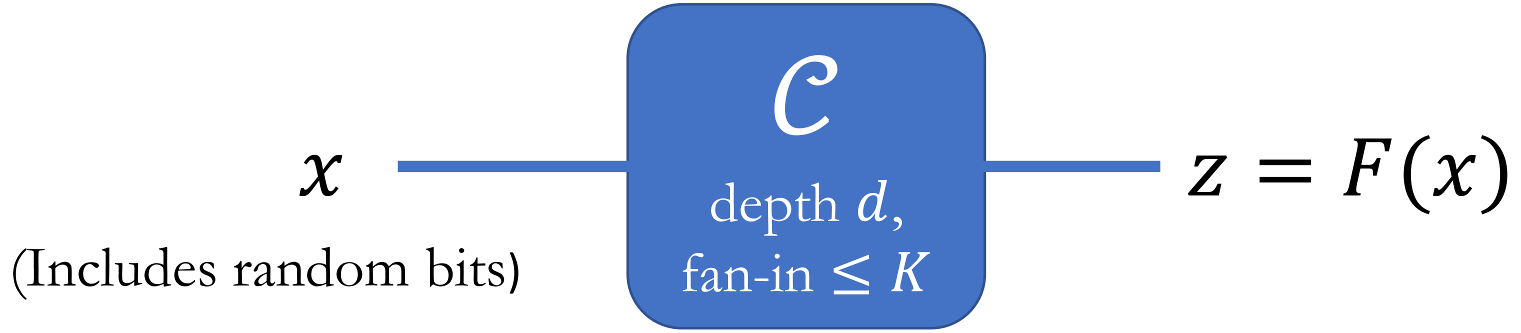
The **lightcone** $L(z_k)$ of an output bit z_k is the set of input bits x_i that are causally connected to z_k.

Locality in classical circuits



The **lightcone** $L(z_k)$ of an output bit z_k is the set of input bits x_i that are causally connected to z_k.

Locality in classical circuits



"Constant-depth locality": Lightcones of output bits have constant size

$$|L(z_k)| \leq K^d$$

We'll see that the 2D Hidden Linear Function problem cannot be solved by "constant-depth local" circuits. First consider simpler forms of locality…

Quantum nonlocality beats completely local circuits

[Greenburger et al. 1990][Mermin 1990]

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

satisfies:

$$\begin{cases} P|GHZ\rangle = |GHZ\rangle \\ P \in \{XXX, -XYY, -YXY, -YYX\} \end{cases}$$

Quantum nonlocality beats completely local circuits

[Greenburger et al. 1990][Mermin 1990]

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

satisfies:

$$P|GHZ\rangle = |GHZ\rangle$$

$$P \in \{XXX, -XYY, -YXY, -YYX\}$$

Choose bits b_1, b_2, b_3 and then measure each qubit of $|\mathrm{GHZ}\rangle$ in either the X basis (if $b_j = 0$) or the Y basis (if $b_j = 1$). Outcomes $z_j \in \{-1, +1\}$ satisfy:

$$i^{b_1+b_2+b_3} z_1 z_2 z_3 = 1 \quad \textbf{whenever} \quad b_1 \oplus b_2 \oplus b_3 = 0$$

"GHZ relation"

Quantum nonlocality beats completely local circuits

[Greenburger et al. 1990][Mermin 1990]

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$ satisfies:

$$P|GHZ\rangle = |GHZ\rangle$$

$$P \in \{XXX, -XYY, -YXY, -YYX\}$$

Choose bits b_1, b_2, b_3 and then measure each qubit of $|\mathrm{GHZ}\rangle$ in either the X basis (if $b_j = 0$) or the Y basis (if $b_j = 1$). Outcomes $z_j \in \{-1, +1\}$ satisfy:

$$i^{b_1+b_2+b_3} z_1 z_2 z_3 = 1 \quad \text{whenever} \quad b_1 \oplus b_2 \oplus b_3 = 0$$

"GHZ relation"

The GHZ relation cannot be satisfied by a completely local classical probabilistic circuit where each output bit z_j is correlated with at most one of the input bits b_k.

Quantum nonlocality beats geometrically local circuits

[Barrett et al. 2007]

Graph state on an M-cycle (M even): $|\Phi_M\rangle = \left(\prod_{j=1}^{M} CZ_{j,j+1}\right) H^{\otimes M} |0^M\rangle$

Quantum nonlocality beats geometrically local circuits

[Barrett et al. 2007]

Graph state on an M-cycle (M even): $|\Phi_M\rangle = \left(\prod_{j=1}^{M} CZ_{j,j+1}\right) H^{\otimes M}|0^M\rangle$

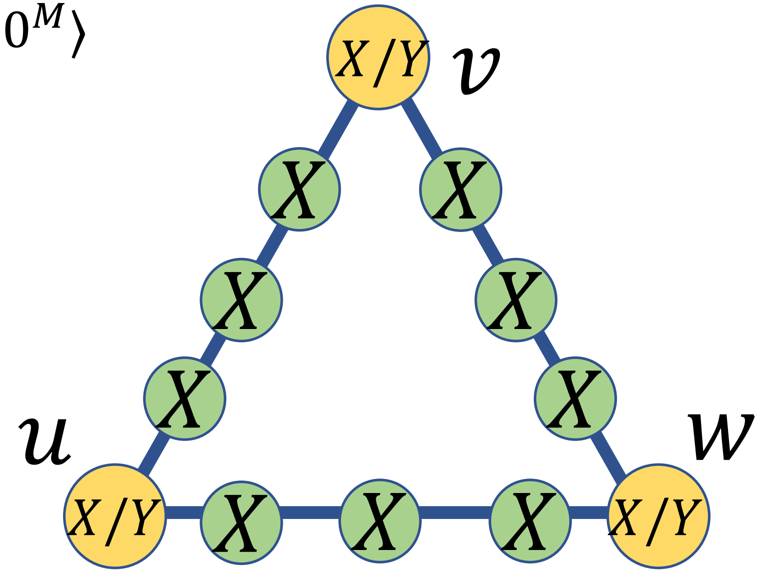
Choose 3 qubits u, v, w on the even sublattice. Measure u, v, w in X or Y basis and all other qubits in X basis.

Quantum nonlocality beats geometrically local circuits

[Barrett et al. 2007]

Graph state on an M-cycle (M even): $|\Phi_M\rangle = \left(\prod_{j=1}^{M} CZ_{j,j+1}\right) H^{\otimes M}|0^M\rangle$

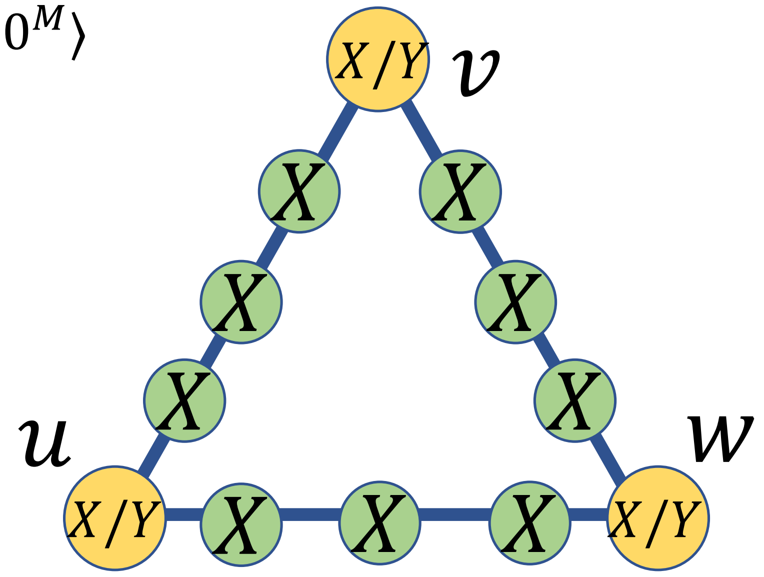
Choose 3 qubits u, v, w on the even sublattice. Measure u, v, w in X or Y basis and all other qubits in X basis.



Quantum nonlocality beats geometrically local circuits

[Barrett et al. 2007]

Graph state on an M-cycle (M even): $|\Phi_M\rangle = \left(\prod_{j=1}^{M} CZ_{j,j+1}\right) H^{\otimes M}|0^M\rangle$



Choose 3 qubits u, v, w on the even sublattice. Measure u, v, w in X or Y basis and all other qubits in X basis.

Input

$b_u, b_v, b_w \in \{0,1\}$

Measurement bases

Output

$z \in \{0,1\}^M$

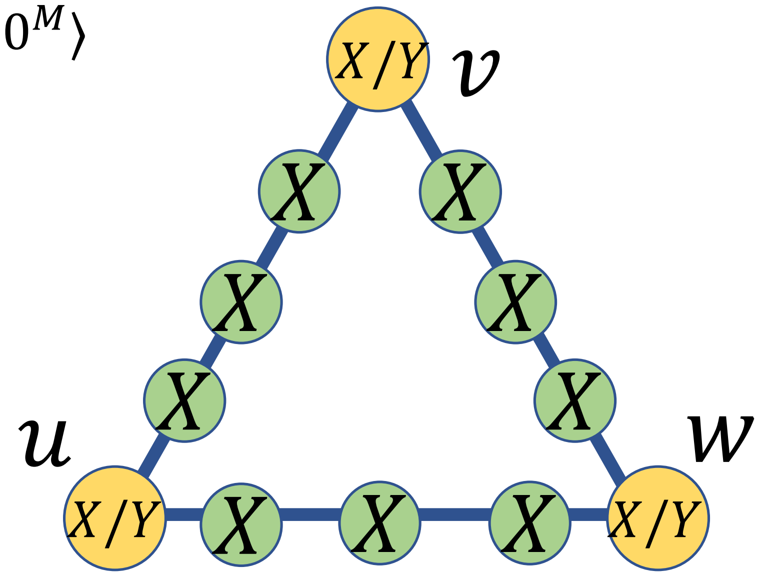
Measurement outcomes

Quantum nonlocality beats geometrically local circuits

[Barrett et al. 2007]

Graph state on an M-cycle (M even): $|\Phi_M\rangle = \left(\prod_{j=1}^{M} CZ_{j,j+1}\right) H^{\otimes M}|0^M\rangle$

Choose 3 qubits u, v, w on the even sublattice. Measure u, v, w in X or Y basis and all other qubits in X basis.



Input

$b_u, b_v, b_w \in \{0,1\}$

Measurement bases

Output

$z \in \{0,1\}^M$

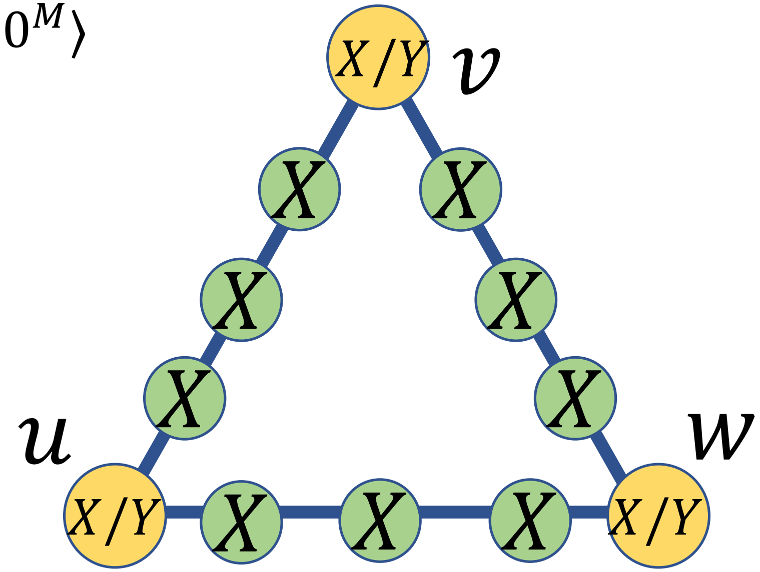
Measurement outcomes

Fact: Input/output satisfy a **"cycle relation"** $R(b_u, b_v, b_w, z) = 1$ similar to the GHZ relation.

Quantum nonlocality beats geometrically local circuits

[Barrett et al. 2007]

Graph state on an M-cycle (M even): $|\Phi_M\rangle = \left(\prod_{j=1}^{M} CZ_{j,j+1}\right) H^{\otimes M}|0^M\rangle$



Choose 3 qubits u, v, w on the even sublattice. Measure u, v, w in X or Y basis and all other qubits in X basis.

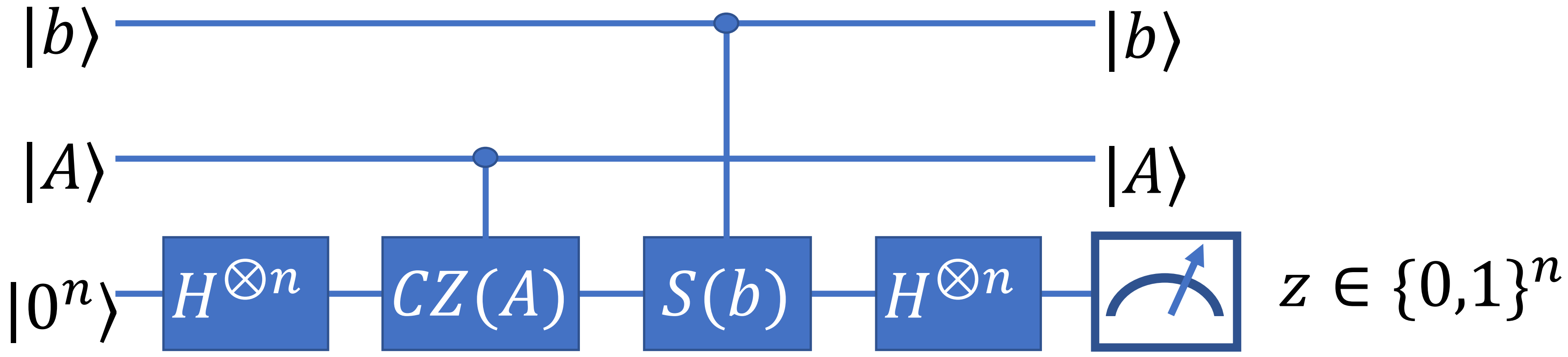
Input		Output
$b_u, b_v, b_w \in \{0,1\}$	→	$z \in \{0,1\}^M$
Measurement bases		Measurement outcomes

Fact: Input/output satisfy a **"cycle relation"** $R(b_u, b_v, b_w, z) = 1$ similar to the GHZ relation.

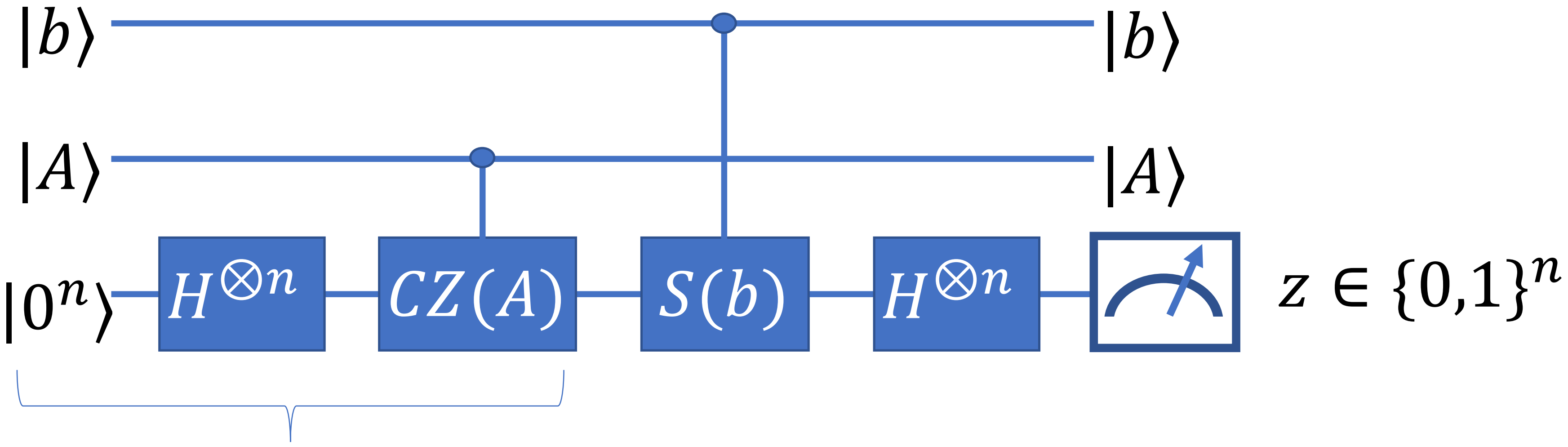
Lemma: Suppose a classical circuit satisfies the cycle relation with probability $> 7/8$. Then some output bit z_k is correlated with a **distant** input bit b_u, b_v or b_w.
(this means it is not the nearest vertex of the triangle)

…How is this related to the 2D Hidden Linear Function Problem?

…How is this related to the 2D Hidden Linear Function Problem?

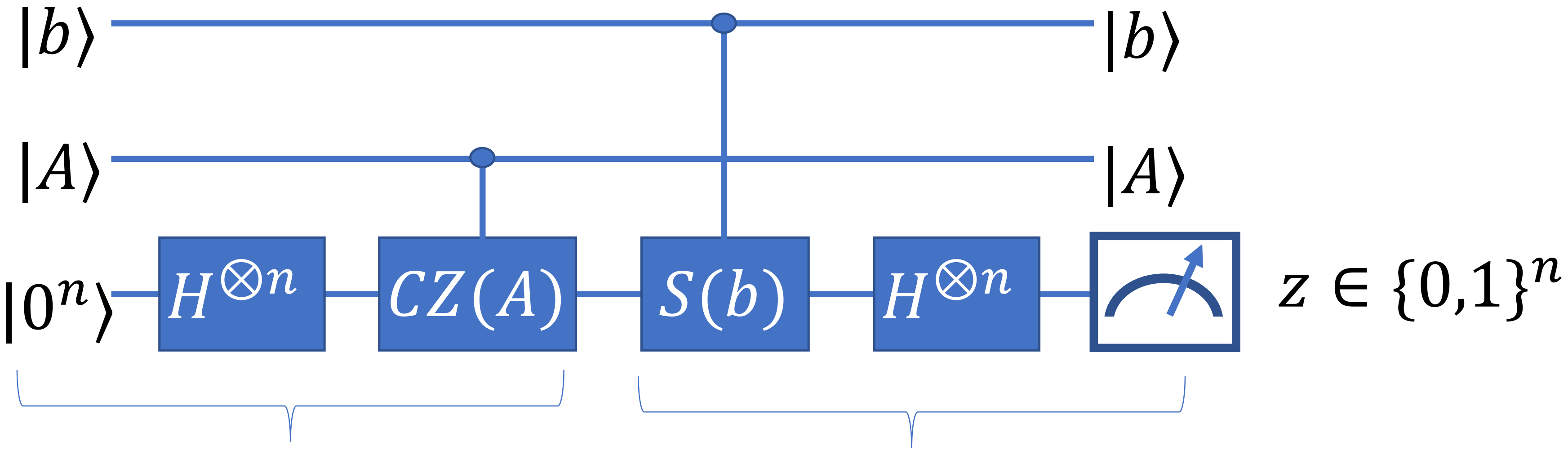


…How is this related to the 2D Hidden Linear Function Problem?



Prepare graph state for graph with adjacency matrix A

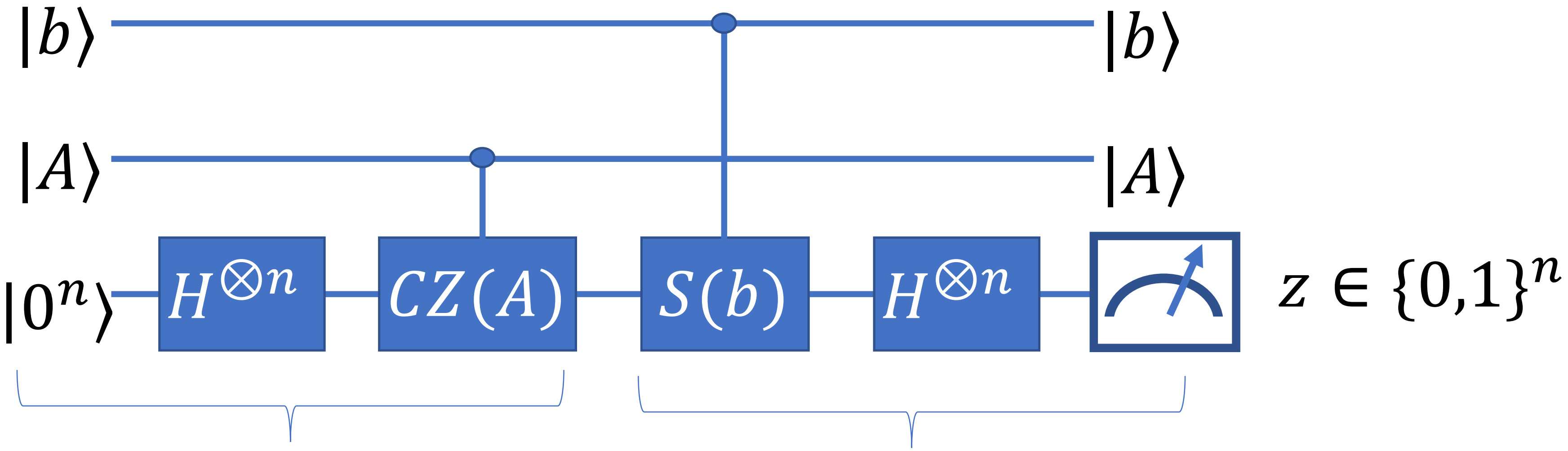
…How is this related to the 2D Hidden Linear Function Problem?



Prepare graph state for graph with adjacency matrix A

Measure jth qubit in X or Y basis depending on b_j

…How is this related to the 2D Hidden Linear Function Problem?

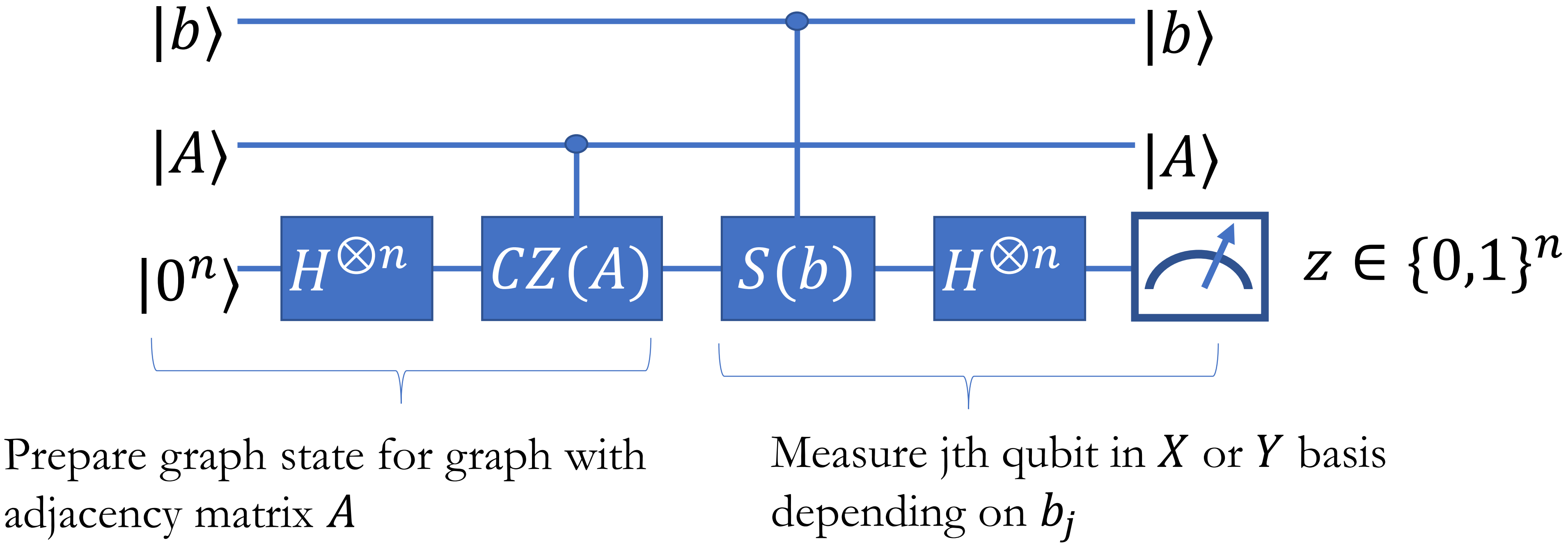


Prepare graph state for graph with adjacency matrix A

Measure jth qubit in X or Y basis depending on b_j

Choosing A to describe the adjacency matrix of a cycle and choosing b appropriately we infer (from Barrett et al.) a cycle relation satisfied by input/output.

…How is this related to the 2D Hidden Linear Function Problem?



Choosing *A* to describe the adjacency matrix of a cycle and choosing *b* appropriately we infer (from Barrett et al.) a cycle relation satisfied by input/output.

A classical circuit which solves the 2D HLF problem must also satisfy all such cycle relations….

Quantum nonlocality beats “constant-depth local” circuits

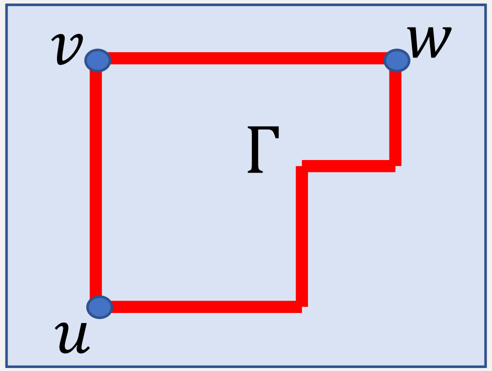
We use constant-depth locality (every output bit has constant-sized lightcone) and a probabilistic argument to prove the following:

Quantum nonlocality beats "constant-depth local" circuits

We use constant-depth locality (every output bit has constant-sized lightcone) and a probabilistic argument to prove the following:

Lemma: Suppose a classical circuit has depth less than $\frac{\log(N)}{8\log(K)}$.

Then we can find 3 vertices u, v, w on the even sublattice of the $N \times N$ grid and a cycle Γ which passes through them, such that **input bits $\boldsymbol{b_u}, \boldsymbol{b_v}, \boldsymbol{b_w}$ are not correlated with any distant output bits on $\boldsymbol{\Gamma}$.**

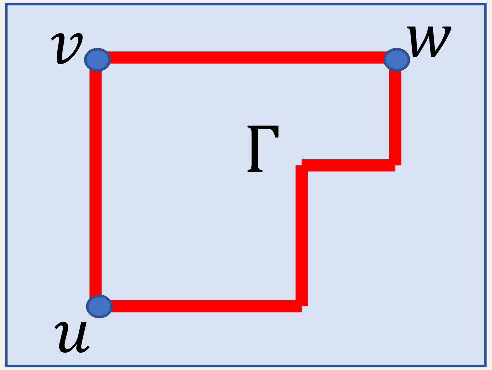


Quantum nonlocality beats "constant-depth local" circuits

We use constant-depth locality (every output bit has constant-sized lightcone) and a probabilistic argument to prove the following:

Lemma: Suppose a classical circuit has depth less than $\frac{\log(N)}{8\log(K)}$.

Then we can find 3 vertices u, v, w on the even sublattice of the $N \times N$ grid and a cycle Γ which passes through them, such that **input bits $\boldsymbol{b_u, b_v, b_w}$ are not correlated with any distant output bits on $\boldsymbol{\Gamma}$.**



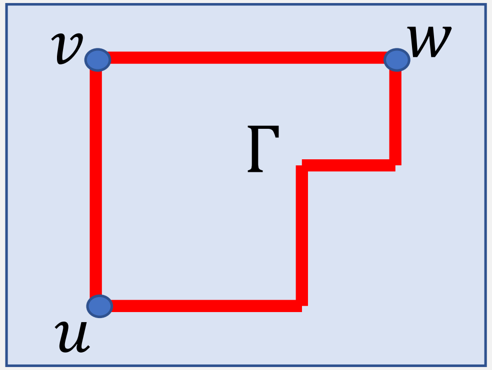
The circuit does not w.h.p satisfy the cycle relation for Γ

Quantum nonlocality beats "constant-depth local" circuits

We use constant-depth locality (every output bit has constant-sized lightcone) and a probabilistic argument to prove the following:

Lemma: Suppose a classical circuit has depth less than $\frac{\log(N)}{8\log(K)}$.

Then we can find 3 vertices u, v, w on the even sublattice of the $N \times N$ grid and a cycle Γ which passes through them, such that **input bits $\boldsymbol{b_u, b_v, b_w}$ are not correlated with any distant output bits on $\boldsymbol{\Gamma}$.**



→ The circuit does not w.h.p satisfy the cycle relation for Γ

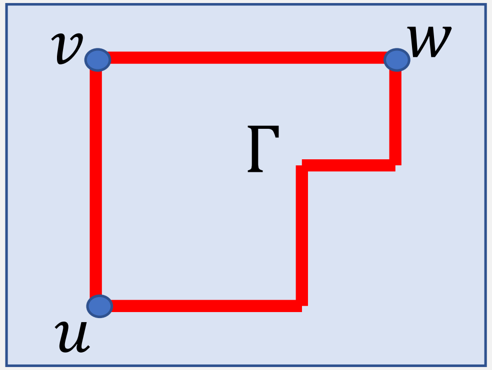
→ It does not w.h.p solve instances of 2D HLF problem where A is the adjacency matrix of Γ.

Quantum nonlocality beats “constant-depth local” circuits

We use constant-depth locality (every output bit has constant-sized lightcone) and a probabilistic argument to prove the following:

Lemma: Suppose a classical circuit has depth less than $\frac{\log(N)}{8\log(K)}$.

Then we can find 3 vertices u, v, w on the even sublattice of the $N \times N$ grid and a cycle Γ which passes through them, such that **input bits $\boldsymbol{b_u, b_v, b_w}$ are not correlated with any distant output bits on $\boldsymbol{\Gamma}$.**



⇒ The circuit does not w.h.p satisfy the cycle relation for Γ ⇒ It does not w.h.p solve instances of 2D HLF problem where A is the adjacency matrix of Γ.

This provides our lower bound on the depth of any classical circuit which solves the 2D HLF problem with probability greater than 7/8.

Open problems

Recursive HLF problems? The recursive version of Bernstein-Vazirani gives a superpolynomial speedup in query complexity.

Noisy constant-depth quantum circuits vs noiseless constant-depth classical circuits ?

Sampling problems? Can constant-depth quantum circuits sample from a distribution that can't be sampled by classical constant depth circuits? A recent characterization of distributions sampled by NC^0 circuits might be useful [Viola 2014].

Polynomial speed-up ? Constant-depth quantum algorithm solves the 2D HLF Problem in linear time. Best known classical algorithm takes time $O(n^2)$.