Quantum computing before fault tolerance

Evidence for quantum advantage in computation

Quantum algorithms with speedups over classical

Shor’s algorithm

Simulation of Hamiltonian dynamics

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Evidence for quantum advantage in computation

Quantum algorithms with speedups over classical

Shor's algorithm

Simulation of Hamiltonian dynamics

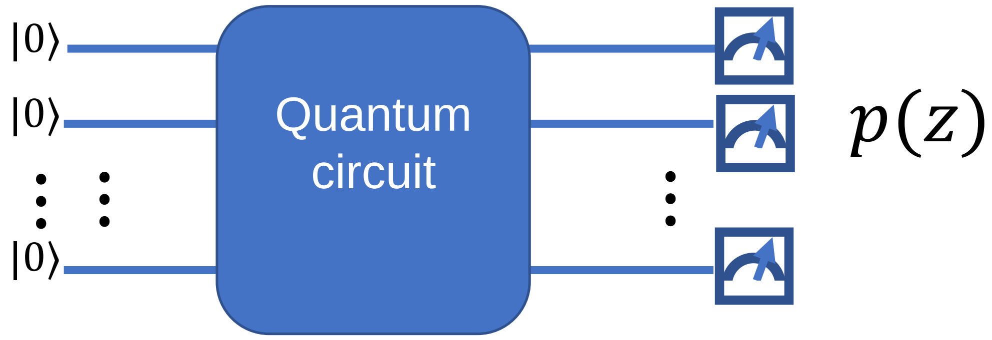
$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Sampling from classically hard distributions

Boson sampling

IQP circuits

Random quantum circuits



Evidence for quantum advantage in computation

Quantum algorithms with speedups over classical

Shor's algorithm

Simulation of Hamiltonian dynamics

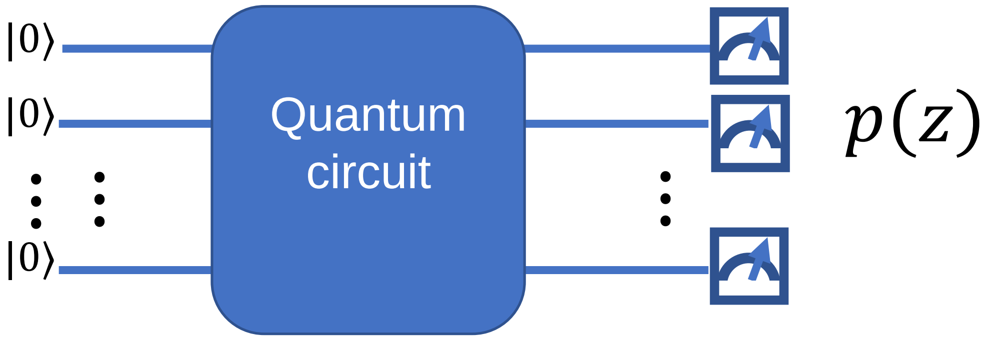
$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Sampling from classically hard distributions

Boson sampling

IQP circuits

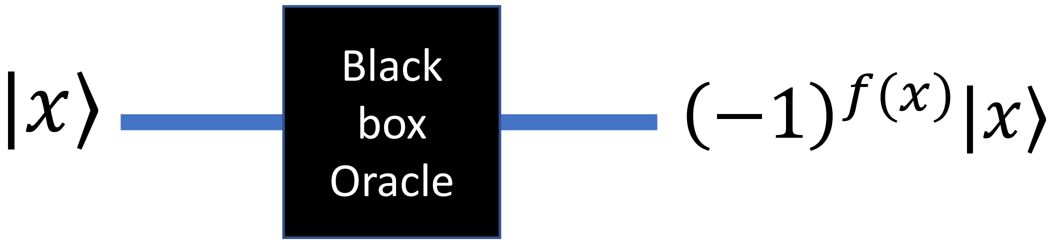
Random quantum circuits



Provable speedups relative to an oracle

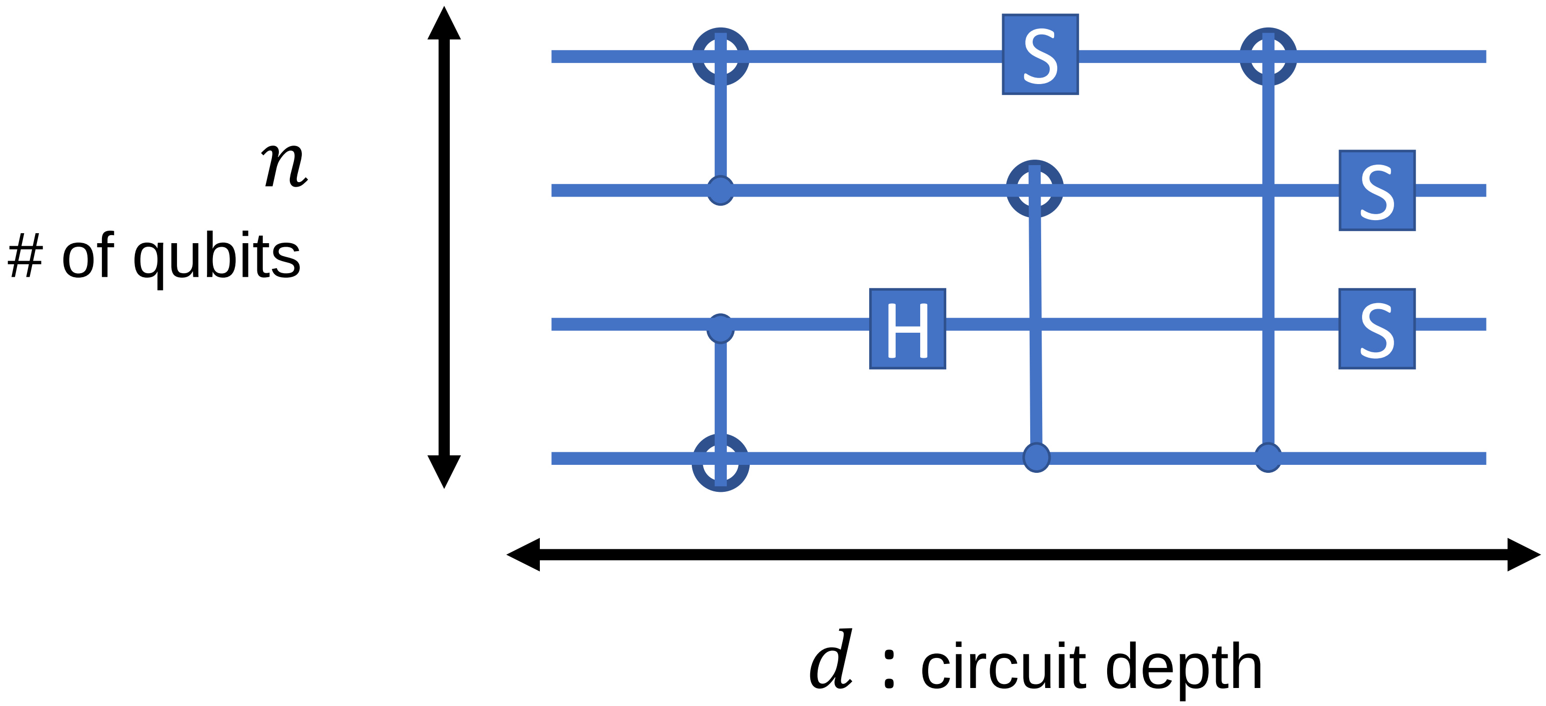
Bernstein-Vazirani

Simon's problem



A quantum computer is subject to noise

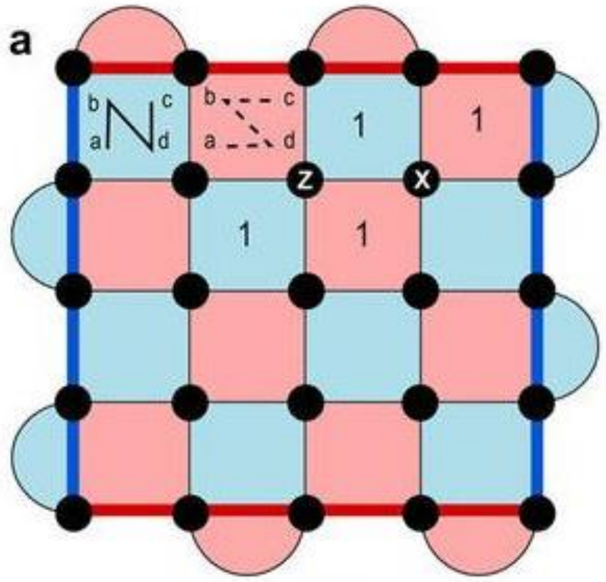
Toy model: errors occur randomly at all locations in a quantum circuit.



Naively seem to need **short depth** or **few qubits** to avoid errors.

Error correction and fault-tolerance

Quantum information can be protected using error correcting codes.

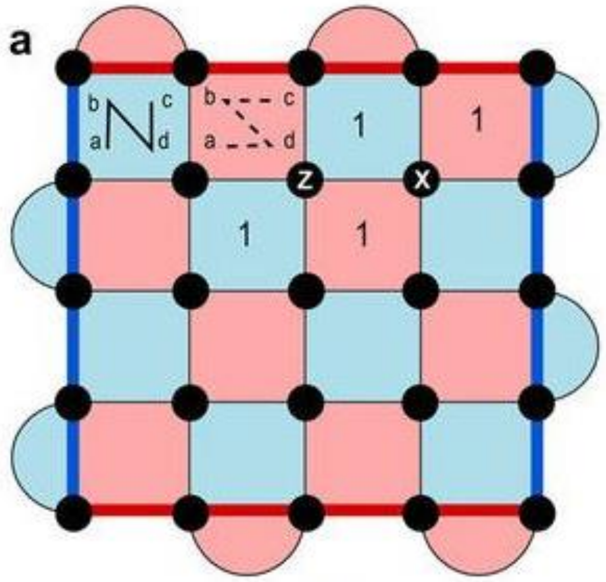


A logical qubit is composed of multiple physical qubits

Image source: [Gambetta, Chow, Steffen 2017]

Error correction and fault-tolerance

Quantum information can be protected using error correcting codes.



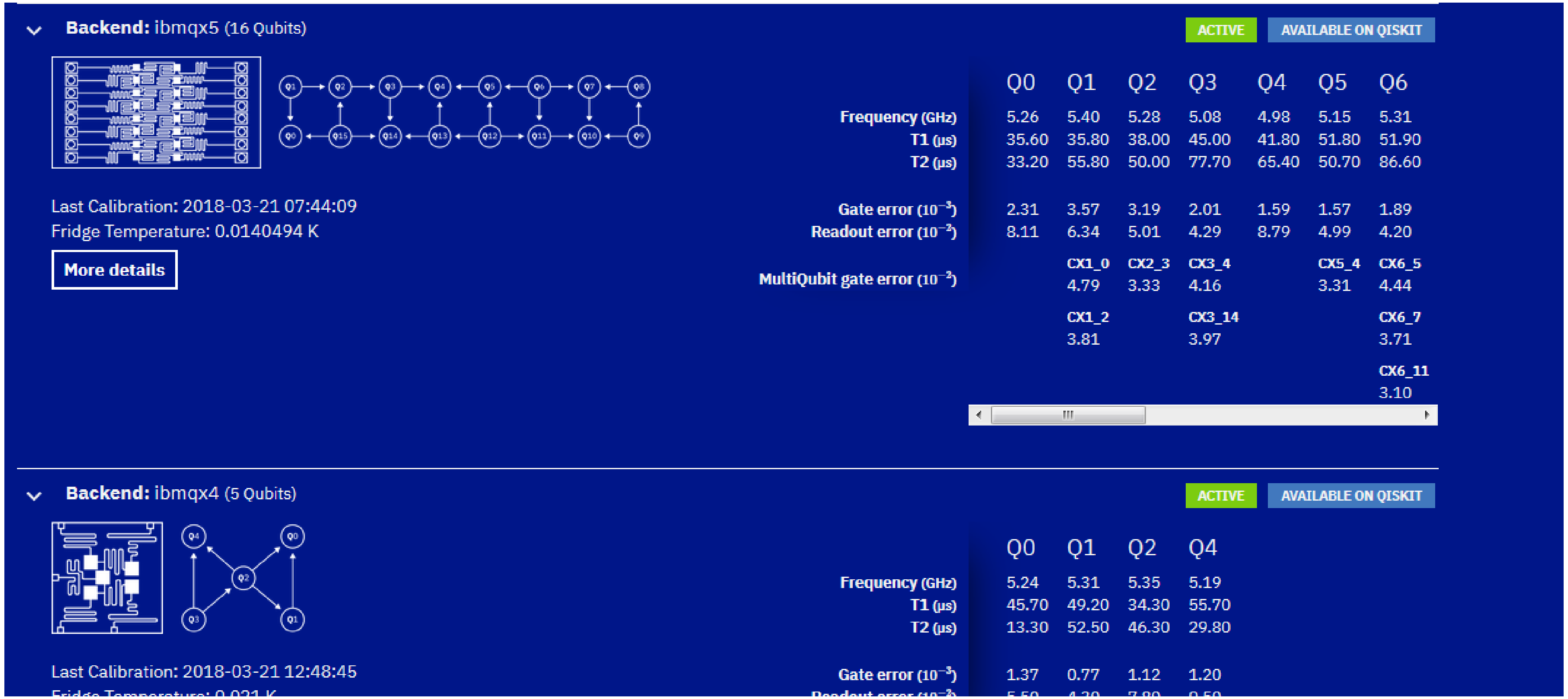
A logical qubit is composed of multiple physical qubits

Using quantum error correction it is possible to compute fault-tolerantly.
The overhead is impractical for now.

Image source: [Gambetta, Chow, Steffen 2017]

Machines now exist

IBM Q experience https://quantumexperience.ng.bluemix.net/qx/devices



Future quantum computers may be too big to simulate on a classical computer.
What does this mean?

Approximate Quantum Computing: From advantage to applications

December 6-8, 2017 @ Yorktown Heights, NY

Modest-sized quantum computers now exist in the real world and the next generation of these devices may be too big to simulate on a classical computer. A quantum computer which is too big to classically simulate has an inherent computational advantage of sorts. How can we harness this advantage, sufficiently protect it from noise, and use it to solve computational problems of interest? Can we achieve these goals without incurring large overheads such as those required for fault-tolerant quantum computation? These are the central questions in an emerging field of approximate quantum computing which touches upon areas including quantum advantage, quantum simulation, hardware-efficient algorithms, heuristic quantum algorithms, error mitigation, and more.

Quantum Computing in the NISQ era and beyond

John Preskill

(Submitted on 2 Jan 2018 (v1), last revised 27 Jan 2018 (this version, v2))

Noisy Intermediate-Scale Quantum (NISQ) technology will be available in the near future. Quantum computers with 50-100 qubits may be able to perform tasks which surpass the capabilities of today's classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably. NISQ devices will be useful tools for exploring many-body quantum physics, and may have other useful applications, but the 100-qubit quantum computer will not change the world right away --- we should regard it as a significant step toward the more powerful quantum technologies of the future. Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing.

Comments: 22 pages. Based on a Keynote Address at Quantum Computing for Business, 5 December 2017. (v2) Minor corrections
Subjects: **Quantum Physics (quant-ph)**; Strongly Correlated Electrons (cond-mat.str-el)
Cite as: **arXiv:1801.00862 [quant-ph]**
(or **arXiv:1801.00862v2 [quant-ph]** for this version)

Quantum computing before fault tolerance

What can we do with **limited or no error correction**, using **short depth circuits** over a **gate set determined by architecture?**

Quantum computing before fault tolerance

What can we do with **limited or no error correction**, using **short depth circuits** over a **gate set determined by architecture?**

Heuristic algorithms

QAOA [Farhi Goldstone Gutmann 2014]

Quantum variational eigensolver [Peruzzo et al. 2013]

(i.e., for quantum chemistry) [Kandala et al. 2017]

Quantum machine learning [Otterbach et al. 2017]

Quantum computing before fault tolerance

What can we do with **limited or no error correction**, using **short depth circuits** over a **gate set determined by architecture?**

Heuristic algorithms

QAOA [Farhi Goldstone Gutmann 2014]
Quantum variational eigensolver [Peruzzo et al. 2013]
(i.e., for quantum chemistry) [Kandala et al. 2017]
Quantum machine learning [Otterbach et al. 2017]

Classically hard sampling tasks

IQP [Bremner Josza Shepherd 2010]
Random quantum circuits [Boixo et al. 2016]

Quantum computing before fault tolerance

What can we do with **limited or no error correction**, using **short depth circuits** over a **gate set determined by architecture?**

Heuristic algorithms

QAOA [Farhi Goldstone Gutmann 2014]
Quantum variational eigensolver [Peruzzo et al. 2013]
(i.e., for quantum chemistry) [Kandala et al. 2017]
Quantum machine learning [Otterbach et al. 2017]

Classically hard sampling tasks

IQP [Bremner Josza Shepherd 2010]
Random quantum circuits [Boixo et al. 2016]

Validate and verify

Quantum computing before fault tolerance

What can we do with **limited or no error correction**, using **short depth circuits** over a **gate set determined by architecture?**

Heuristic algorithms

QAOA [Farhi Goldstone Gutmann 2014]
Quantum variational eigensolver [Peruzzo et al. 2013]
(i.e., for quantum chemistry) [Kandala et al. 2017]
Quantum machine learning [Otterbach et al. 2017]

Classically hard sampling tasks

IQP [Bremner Josza Shepherd 2010]
Random quantum circuits [Boixo et al. 2016]

Validate and verify

To make progress, address broader questions in algorithms and complexity…

Which restricted forms of quantum computation can be more powerful than classical computers?

Which are classically simulable?

Quantum advantage with shallow circuits

Sergey Bravyi, DG, Robert Koenig. arXiv:1704.00690

Evidence for quantum advantage in computation

Quantum algorithms with speedups over classical

Shor's algorithm

Simulation of Hamiltonian dynamics

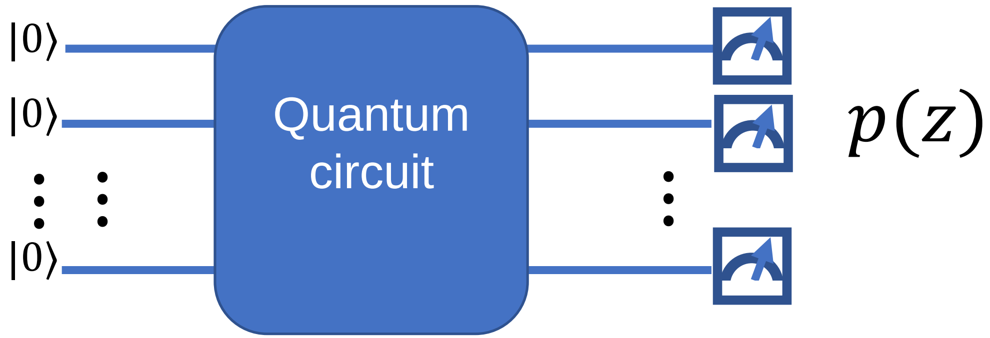
$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Sampling from classically hard distributions

Boson sampling

IQP circuits

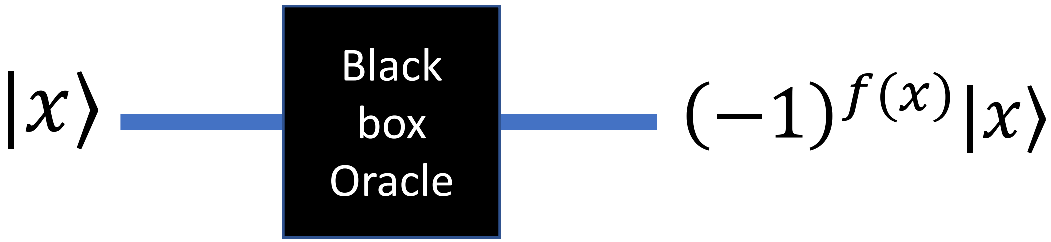
Random quantum circuits



Provable speedups relative to an oracle

Bernstein-Vazirani

Simon's problem



Evidence for quantum advantage in computation

Quantum algorithms with speedu

These speedups disappear if the classical algorithms can be improved

Shor's algorithm

Simulation of Hamiltonian dynam

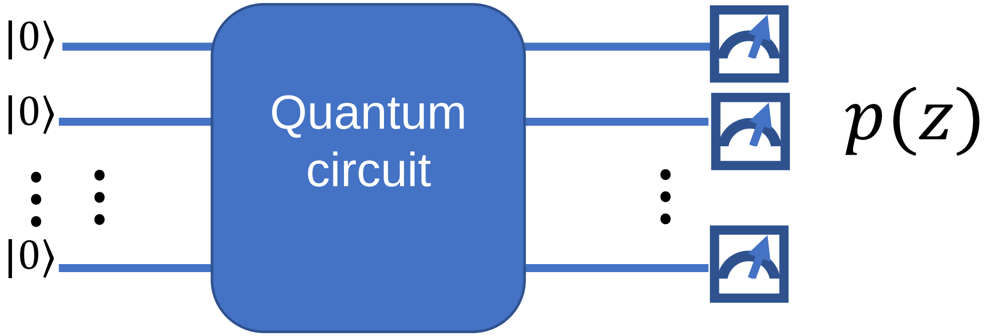
$H|\psi\rangle$

Sampling from classically hard distributions

Boson sampling

IQP circuits

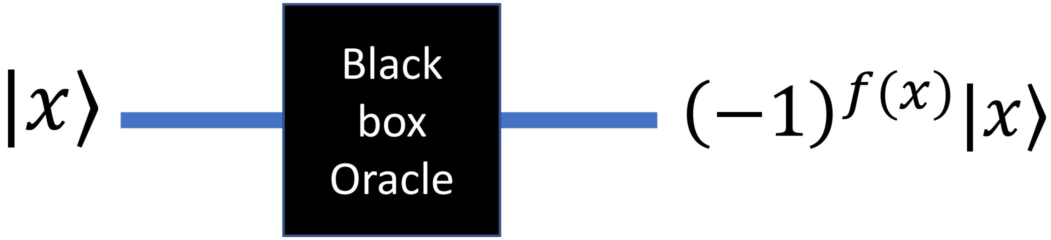
Random quantum circuits



Provable speedups relative to an oracle

Bernstein-Vazirani

Simon's problem



Evidence for quantum advantage in computation

Quantum algorithms with speedu

Shor's algorithm

Simulation of Hamiltonian dynam

These speedups disappear if the classical algorithms can be improved

$H|\psi\rangle$

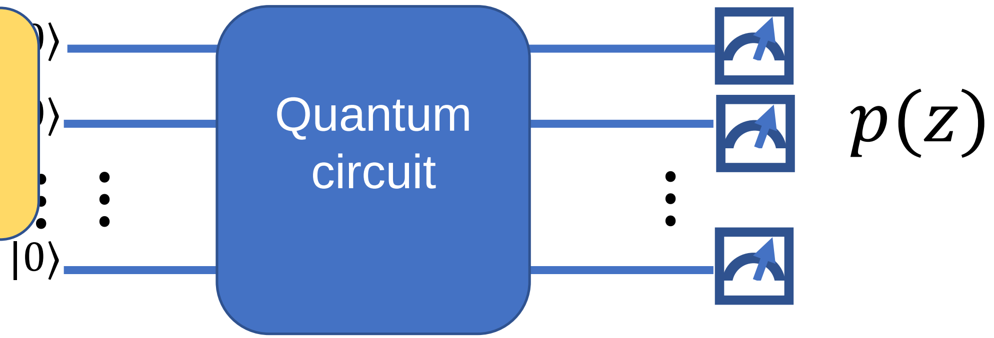
Sampling fro

Boson samp

IQP circuits

Random quantum circuits

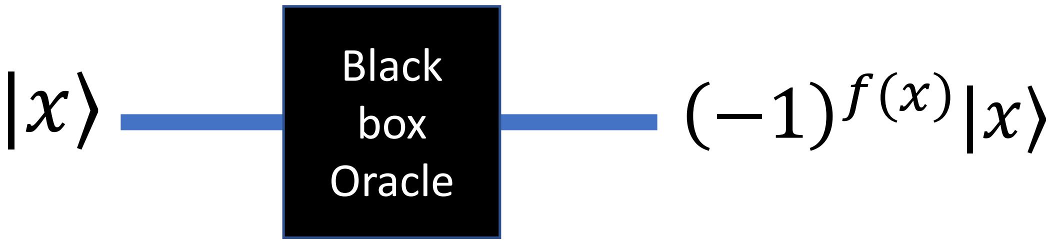
Assumes complexity-theoretic and other conjectures.



Provable speedups relative to an oracle

Bernstein-Vazirani

Simon's problem



Evidence for quantum advantage in computation

Quantum algorithms with speedu

Shor's algorithm

Simulation of Hamiltonian dynam

$H|\psi\rangle$

These speedups disappear if the classical algorithms can be improved

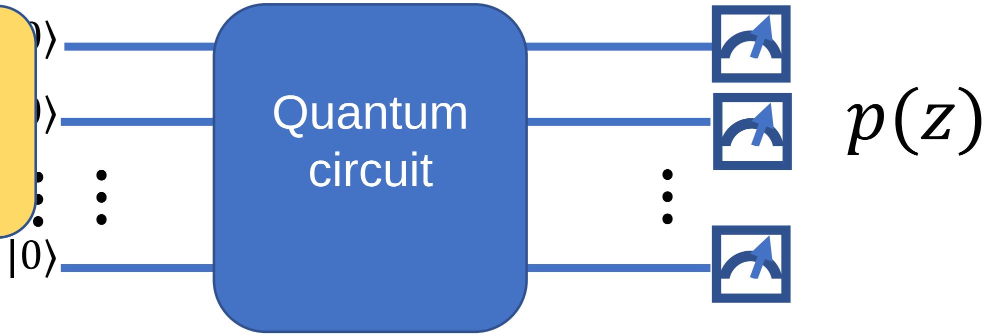
Sampling fro

Boson samp

IQP circuits

Random quantum circuits

Assumes complexity-theoretic and other conjectures.

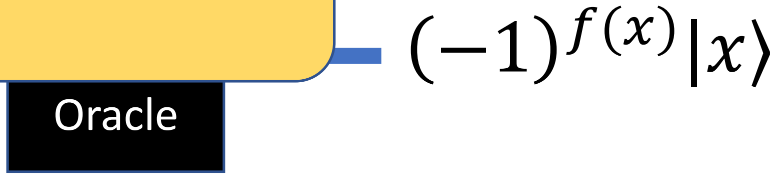


Provable speedups relati

Bernstein-Vazirani

Simon's problem

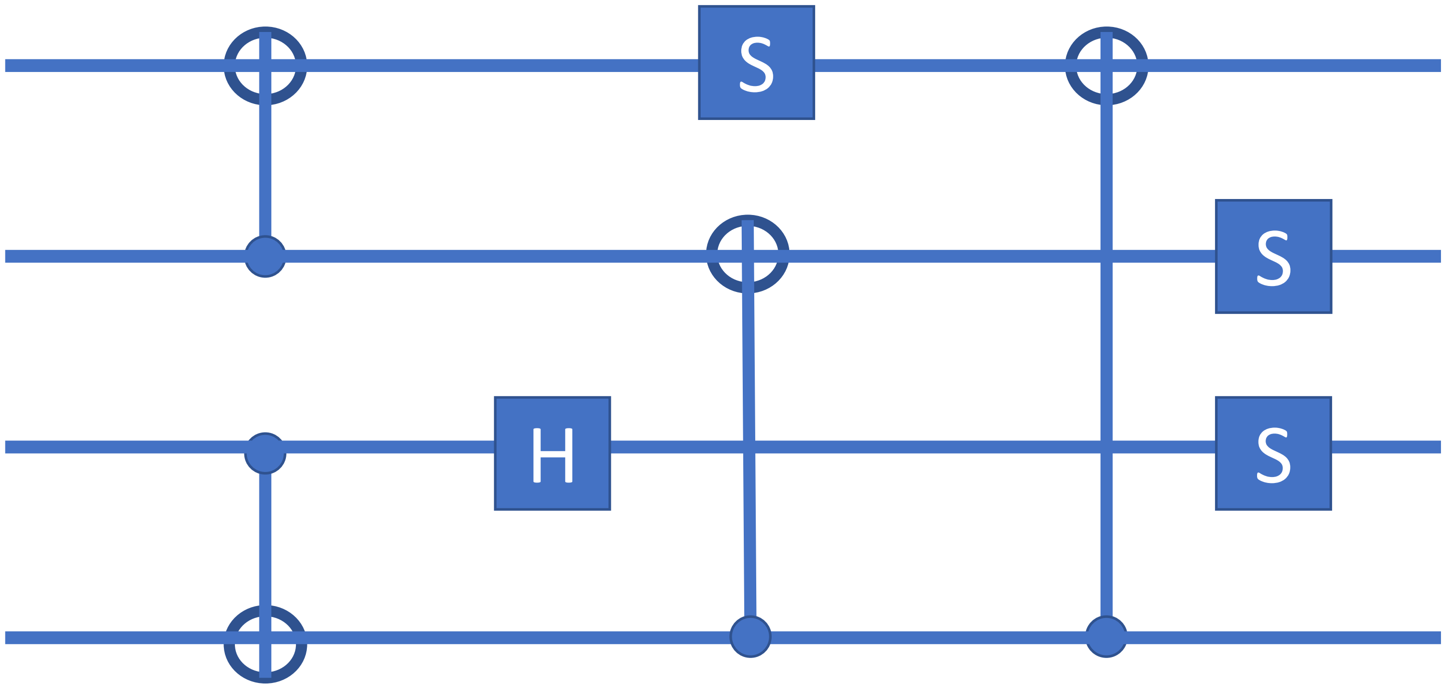
Oracles do not exist in the real world.



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

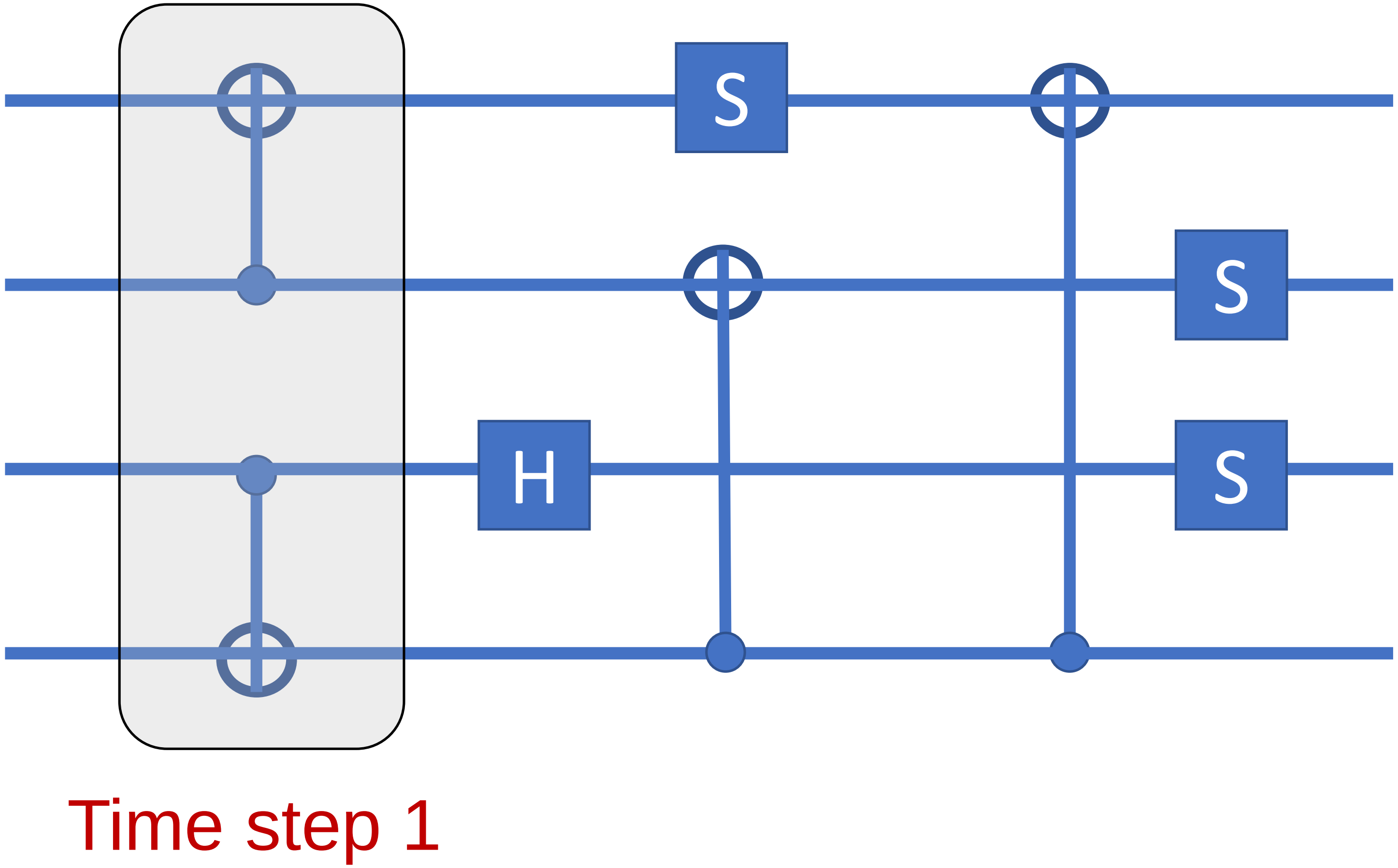
Circuit depth

Circuit depth is the number of time steps allowing for parallel gates.



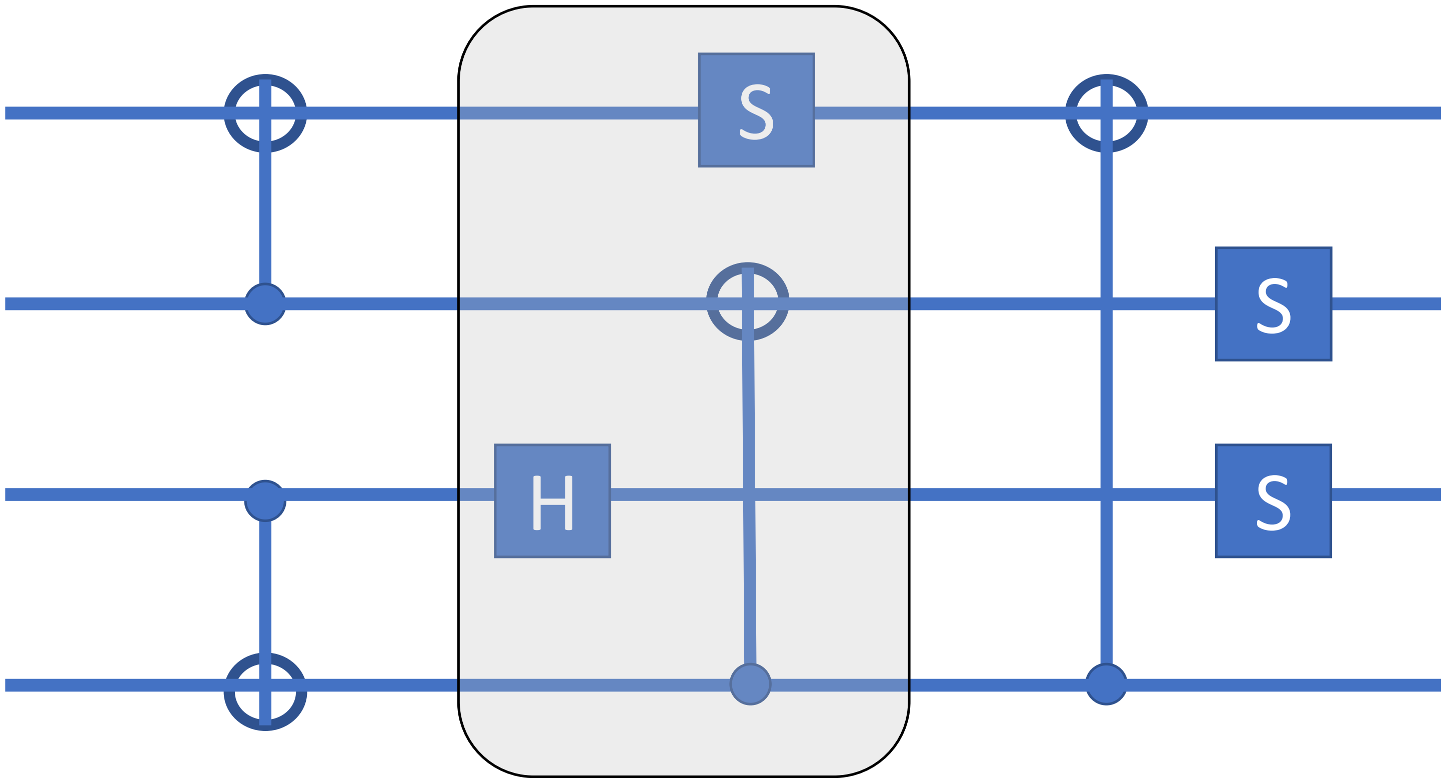
Circuit depth

Circuit depth is the number of time steps allowing for parallel gates.



Circuit depth

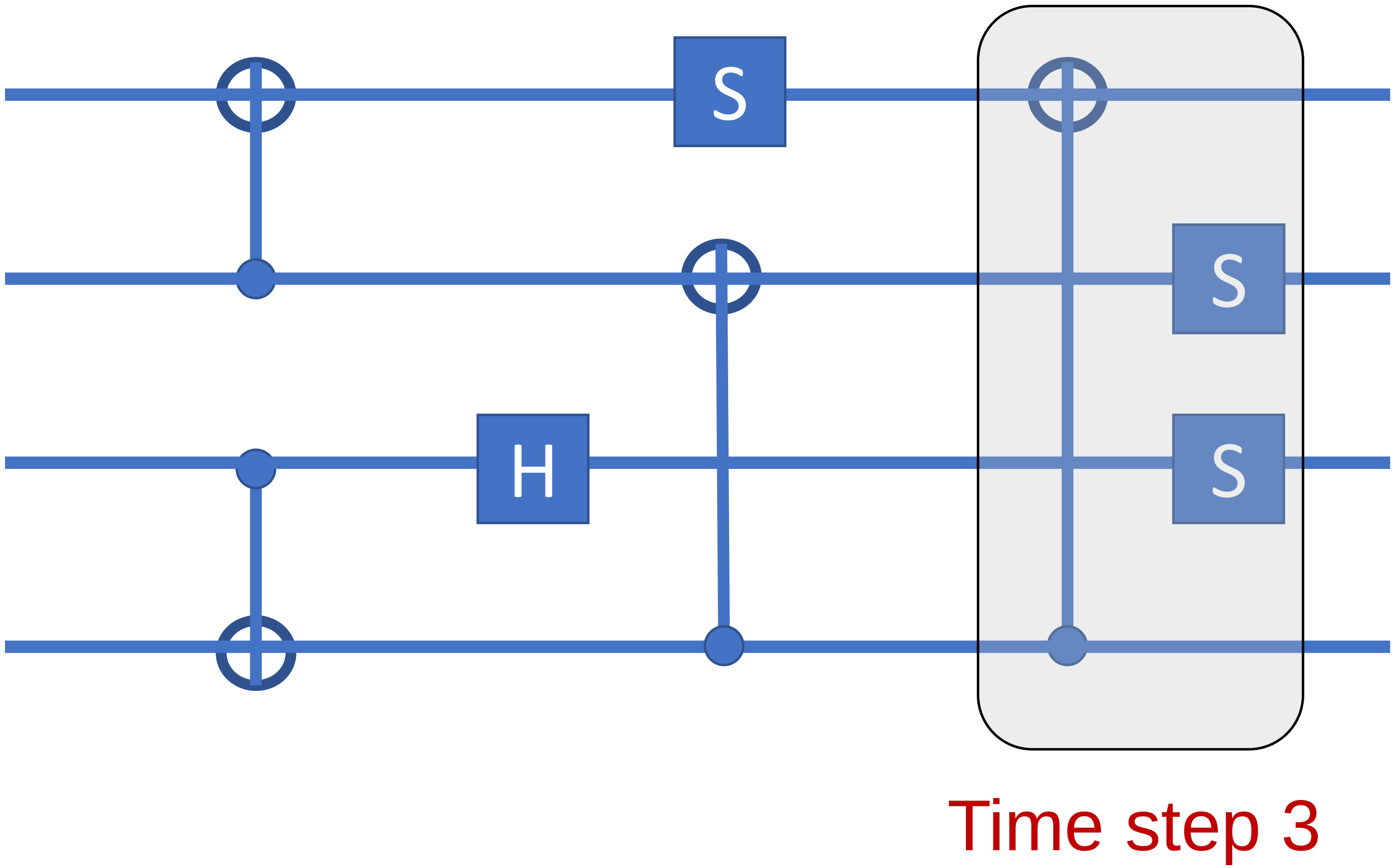
Circuit depth is the number of time steps allowing for parallel gates.



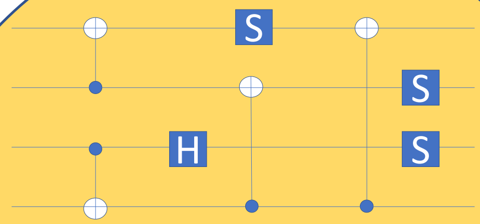
Time step 2

Circuit depth

Circuit depth is the number of time steps allowing for parallel gates.

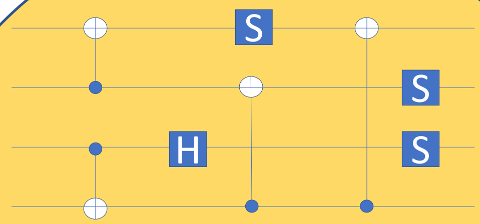


Constant-time parallel quantum computation



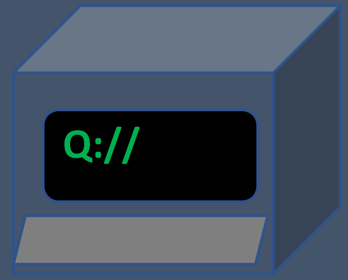
Constant-depth quantum circuits

Constant-time parallel quantum computation



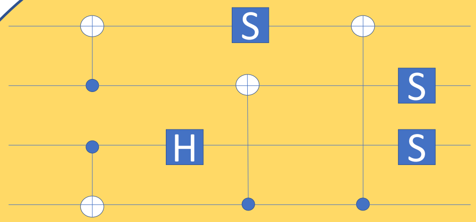
Constant-depth quantum circuits

Algorithms for small quantum computers



Constant-time parallel quantum computation

Algorithms for small quantum computers



Constant-depth quantum circuits

Structure/Simulation

Limits on state preparation.
[Eldar, Harrow 2015]

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

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

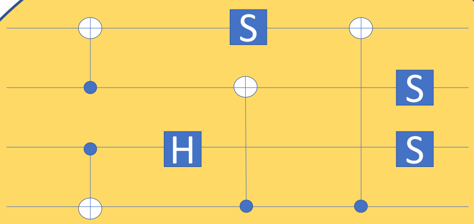
Constant-time parallel quantum computation

Structure/Simulation

Limits on state preparation. [Eldar, Harrow 2015]

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

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



Constant-depth quantum circuits

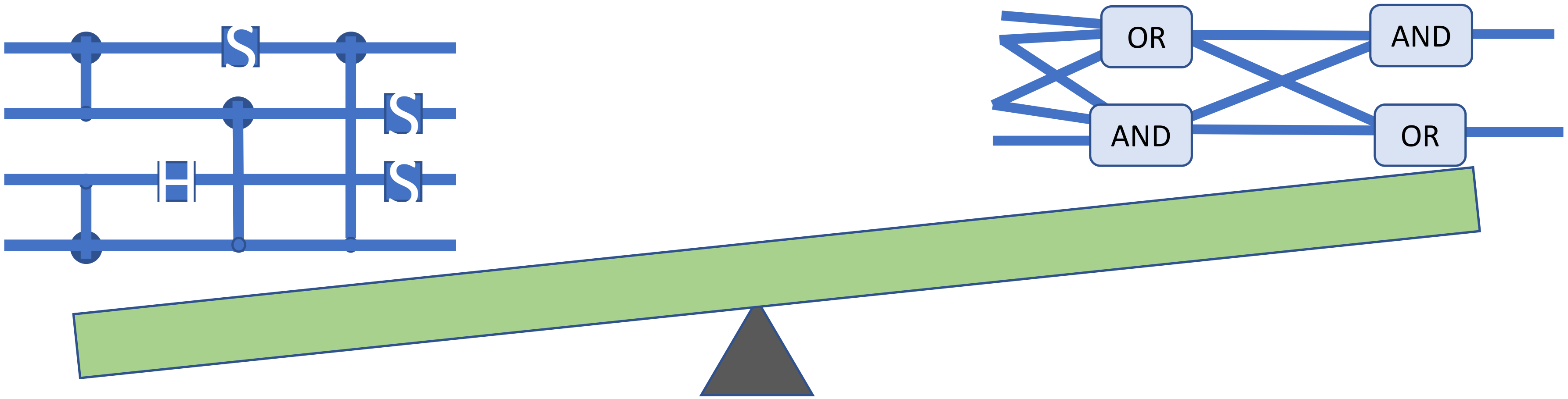
Algorithms for small quantum computers

Computational power

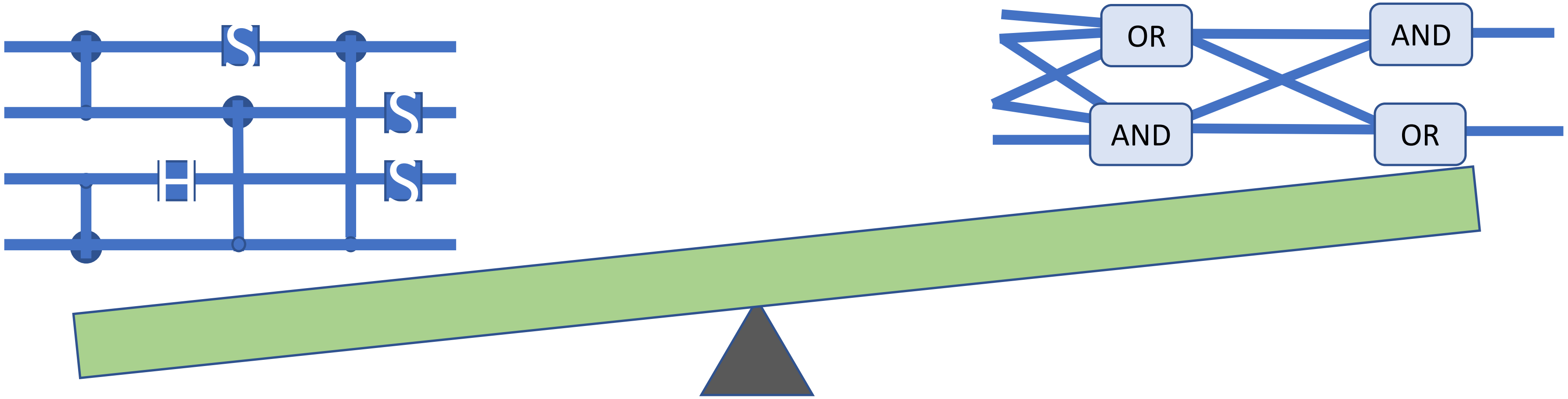
Hardness of exact simulation. [Terhal, Divincenzo 02]

Hardness for approximate simulation
[Gao et al. 17]
[Bermejo-Vega et al. 17]

Big question: Can constant-depth quantum circuits solve a problem that polynomial time classical computers can't?

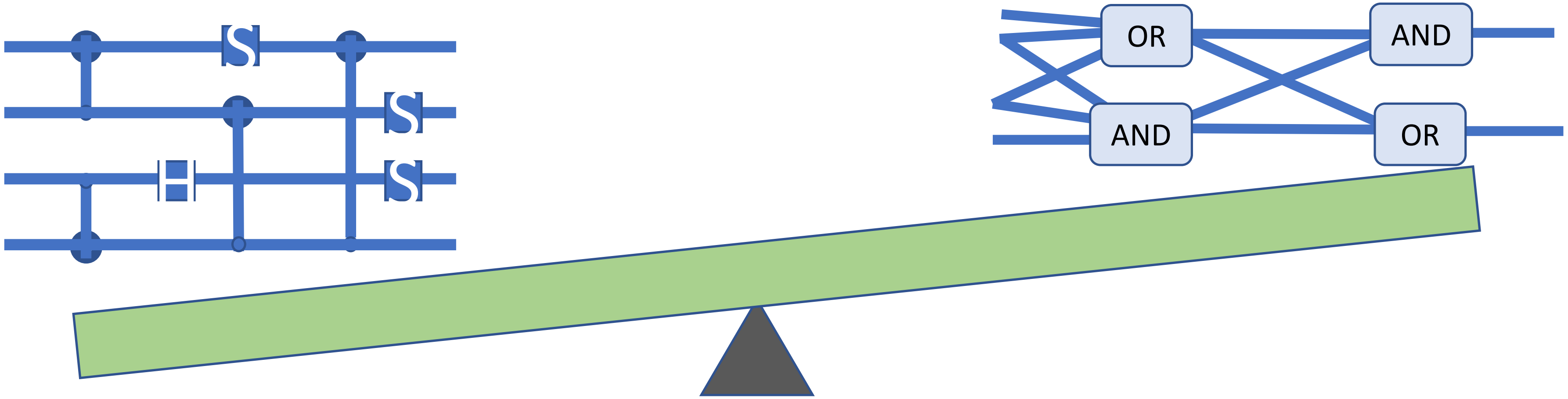


Big question: Can constant-depth quantum circuits solve a problem that polynomial time classical computers can't?



Smaller question: Can constant-depth quantum circuits solve a problem that constant-depth classical circuits can't?

Big question: Can constant-depth quantum circuits solve a problem that polynomial time classical computers can't?



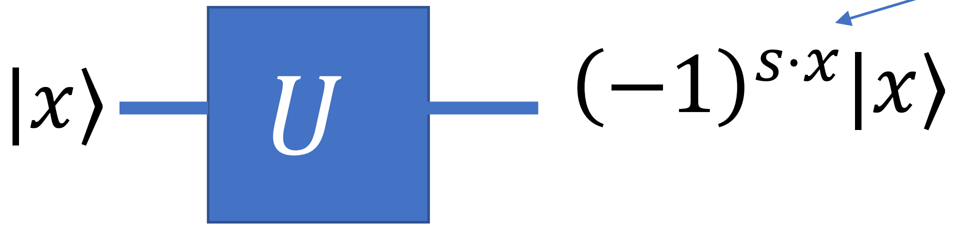
Smaller question: Can constant-depth quantum circuits solve a problem that constant-depth classical circuits can't? YES…

The computational problem we consider can be viewed as a non-oracular version of the Bernstein-Vazirani problem…

Review: hiding a linear function in an oracle

[Bernstein-Vazirani 1993]

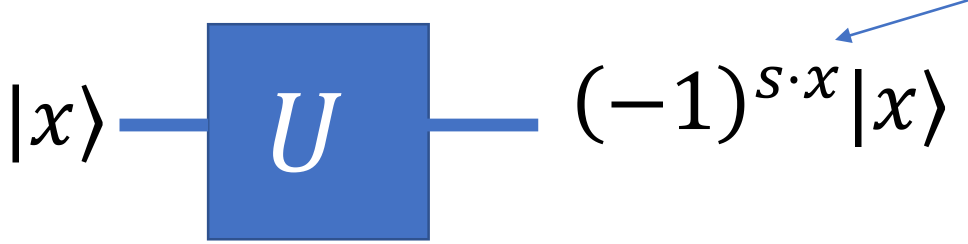
Goal: Find $z \in \{0,1\}^n$ using few queries to a quantum oracle:



Linear Boolean function parameterized by a "secret" bit string z

Review: hiding a linear function in an oracle
[Bernstein-Vazirani 1993]

Goal: Find $z \in \{0,1\}^n$ using few queries to a quantum oracle:



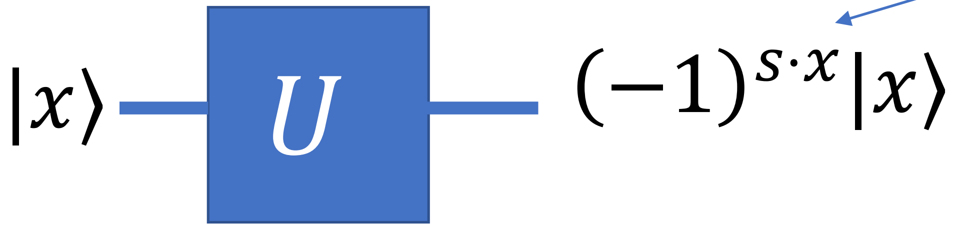
Linear Boolean function parameterized by a “secret” bit string z

We only need to use the quantum oracle once: $|s\rangle = H^{\otimes n} U H^{\otimes n} |0^n\rangle$.

In contrast, a classical algorithm needs n queries to a classical oracle computing $s \cdot x$.

Review: hiding a linear function in an oracle
[Bernstein-Vazirani 1993]

Goal: Find $z \in \{0,1\}^n$ using few queries to a quantum oracle:



Linear Boolean function parameterized by a "secret" bit string z

We only need to use the quantum oracle once: $|s\rangle = H^{\otimes n} U H^{\otimes n} |0^n\rangle$.

In contrast, a classical algorithm needs n queries to a classical oracle computing $s \cdot x$.

Where else can we hide a linear function?

Hiding a linear function in a quadratic form

A Symmetric $n \times n$ binary matrix

$$\ker(A) = \{x : Ax = 0 \bmod 2\}$$

$$q(x) = x^T A x \mod 4$$

Hiding a linear function in a quadratic form

A Symmetric $n \times n$ binary matrix

$$\ker(A) = \{x\colon Ax = 0 \bmod 2\}$$

$$q(x) = x^T A x \mod 4$$

Fact: There is a secret bit string z such that

$$q(x) = 2z^T x \qquad x \in \ker(\mathrm{A})$$

Hiding a linear function in a quadratic form

A Symmetric $n \times n$ binary matrix

$$\ker(A) = \{x : Ax = 0 \bmod 2\}$$

$$q(x) = x^T A x \mod 4$$

Hidden Linear Function problem: Given A, find a secret bit string z such that

$$q(x) = 2z^T x \qquad x \in \ker(\mathrm{A})$$

Hiding a linear function in a 2D quadratic form

A Symmetric $n \times n$ binary matrix

$$\ker(A) = \{x: Ax = 0 \bmod 2\}$$

$$q(x) = x^T A x \mod 4$$

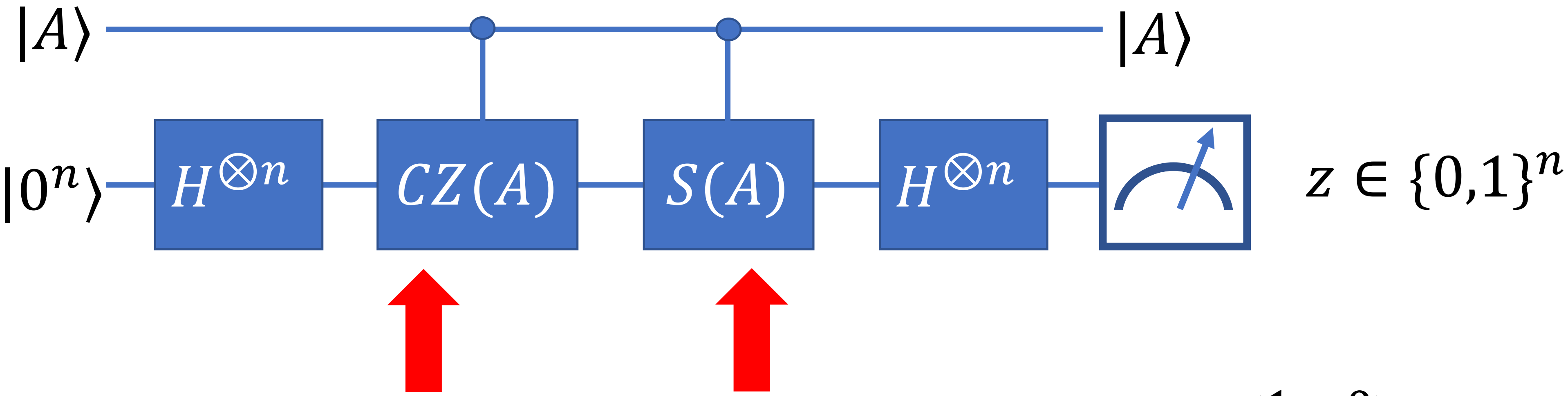
View A as adjacency matrix.

Restrict to case where A describes a subgraph of $\sqrt{n} \times \sqrt{n}$ grid

2D Hidden Linear Function problem: Given A, find a secret bit string z such that

$$q(x) = 2z^T x \qquad x \in \ker(\mathrm{A})$$

Quantum algorithm for HLF problem



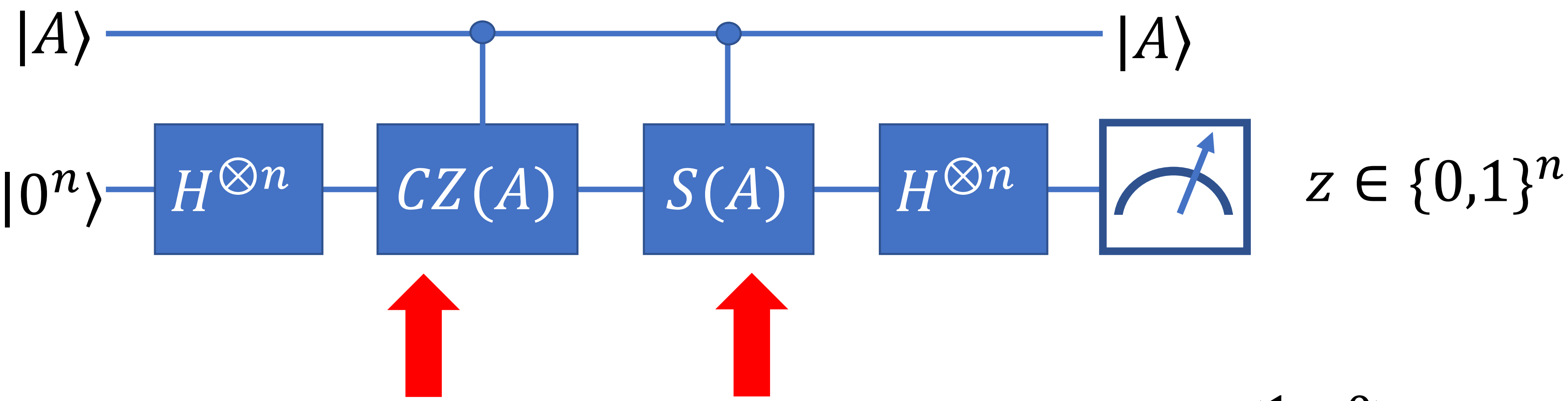
Apply $CZ_{v,w}$ if $A_{v,w} = 1$

Apply S_v if $A_{vv} = 1$

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

$$CZ = \mathrm{diag}(1,1,1,-1)$$

Quantum algorithm for HLF problem



Apply $CZ_{v,w}$ if $A_{v,w} = 1$

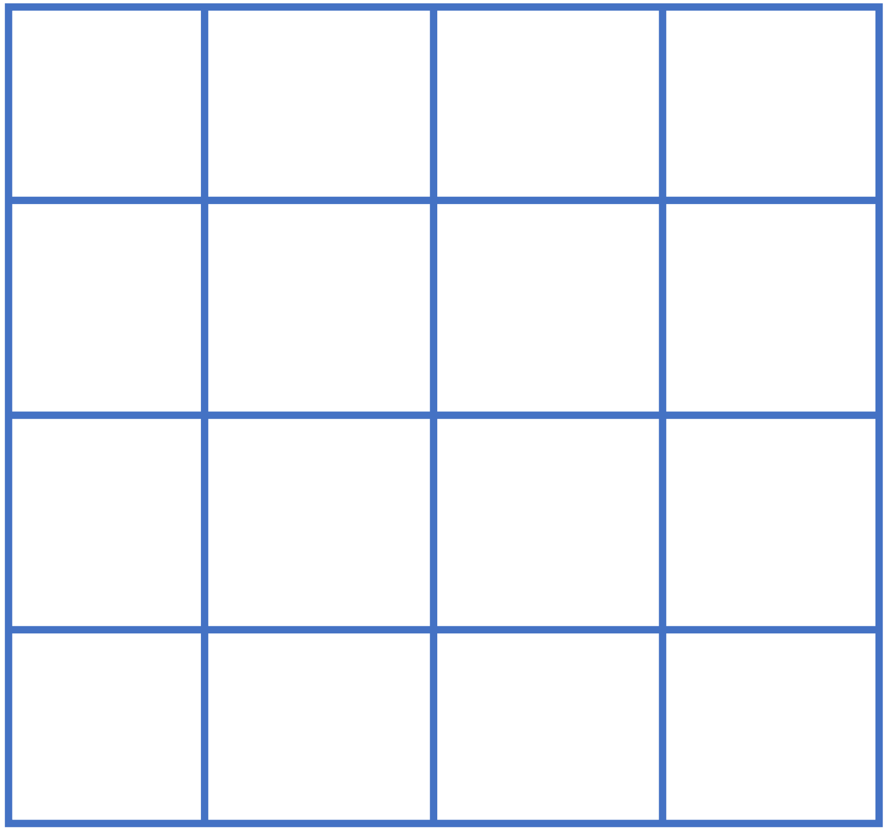
Apply S_v if $A_{vv} = 1$

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

$CZ = \text{diag}(1,1,1,-1)$

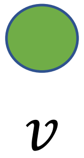
Fact: The output z is a uniformly random solution to the HLF problem

For the 2D HLF the algorithm has constant depth



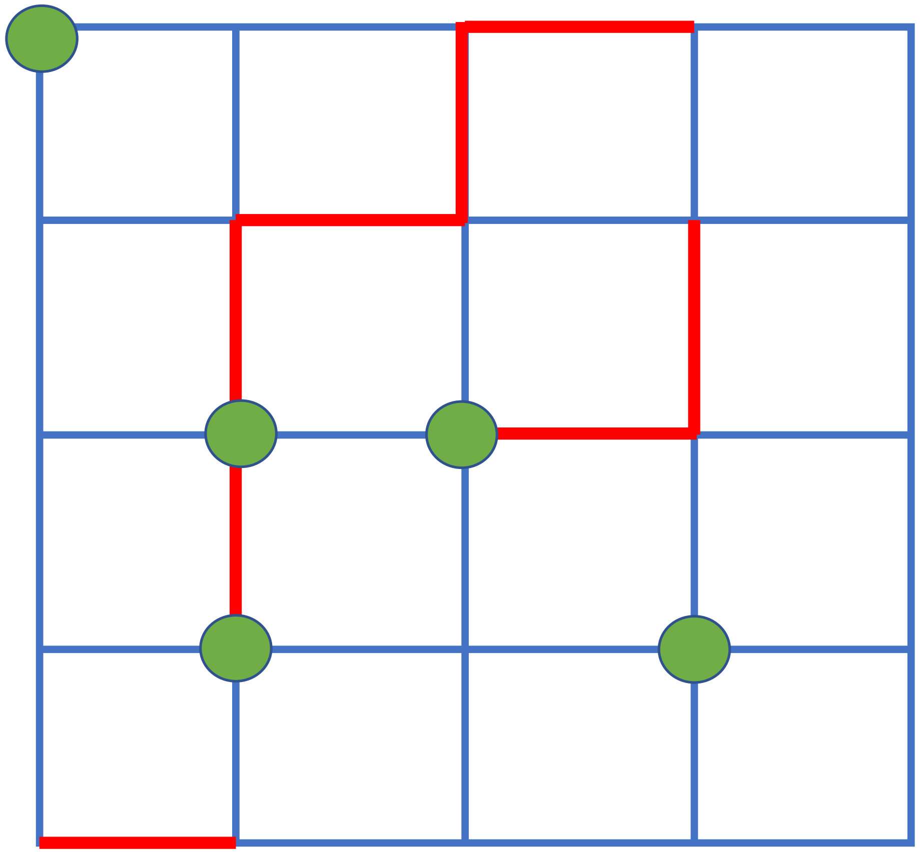
Place a qubit at each vertex
Place input bits on vertices and edges:

: Edge with $A_{vw} = 1$



: Vertex with $A_{vv} = 1$

Constant depth quantum algorithm

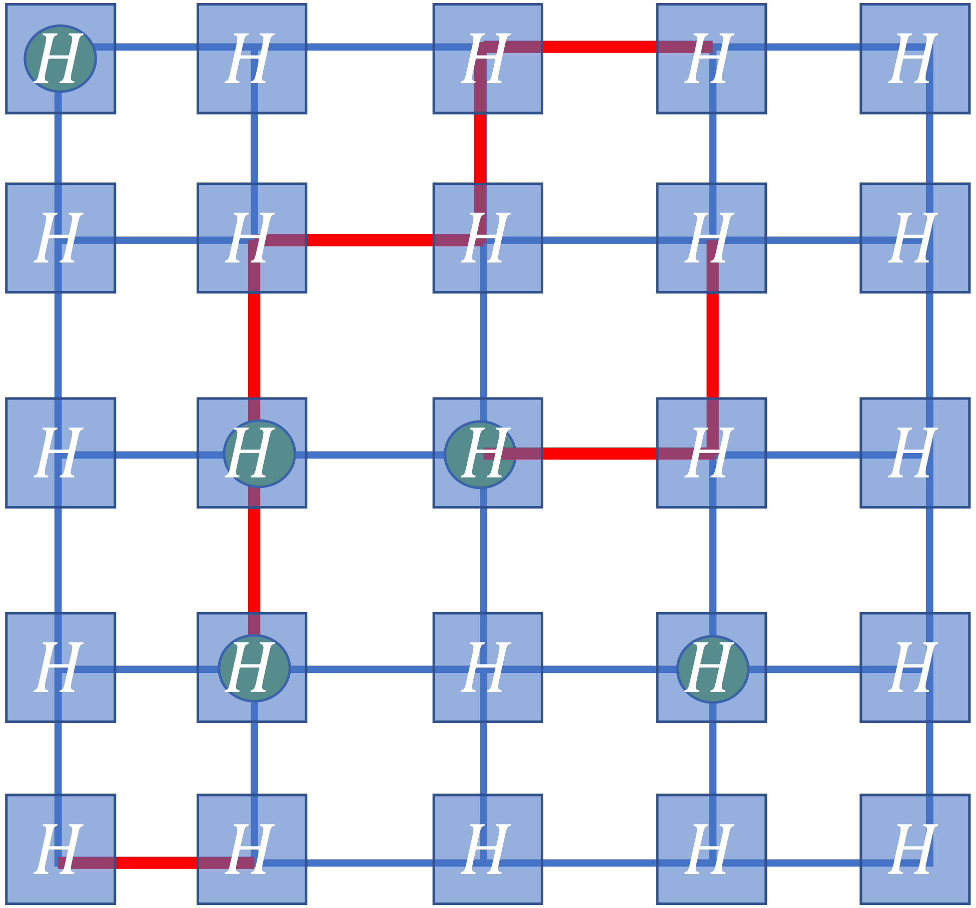


Place a qubit at each vertex
Place input bits on vertices and edges:

v —— w : Edge with $A_{vw} = 1$

● : Vertex with $A_{vv} = 1$
v

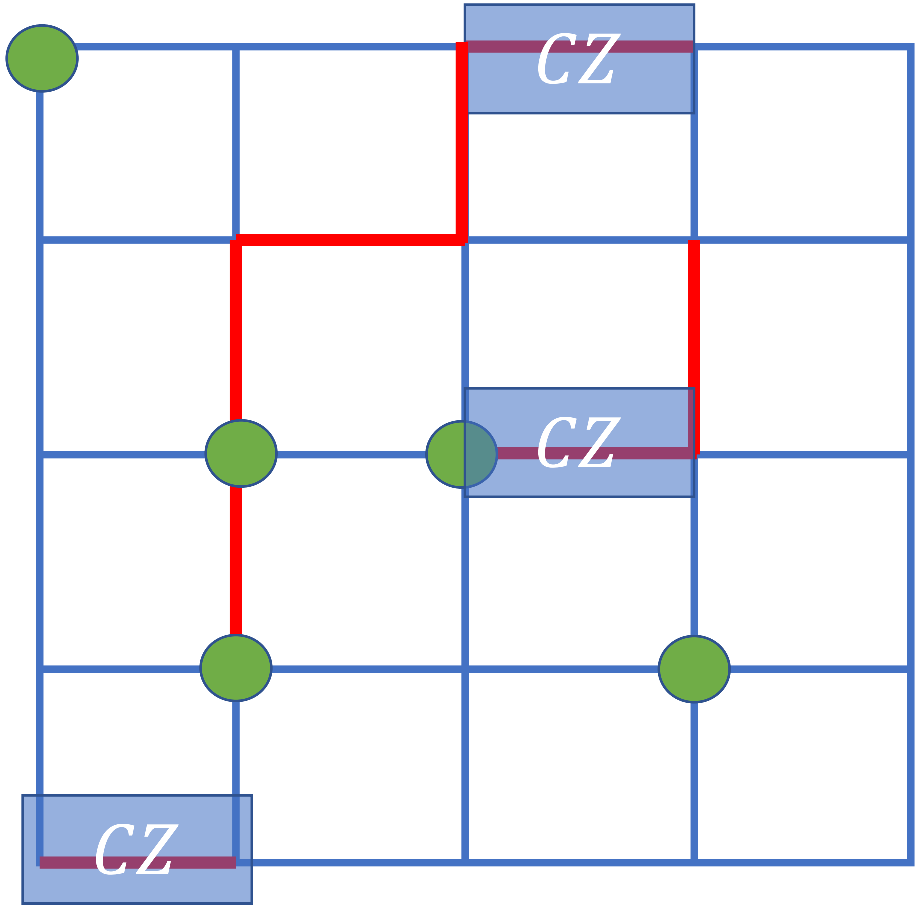
Constant depth quantum algorithm



v —— w : Edge with $A_{vw} = 1$

v : Vertex with $A_{vv} = 1$

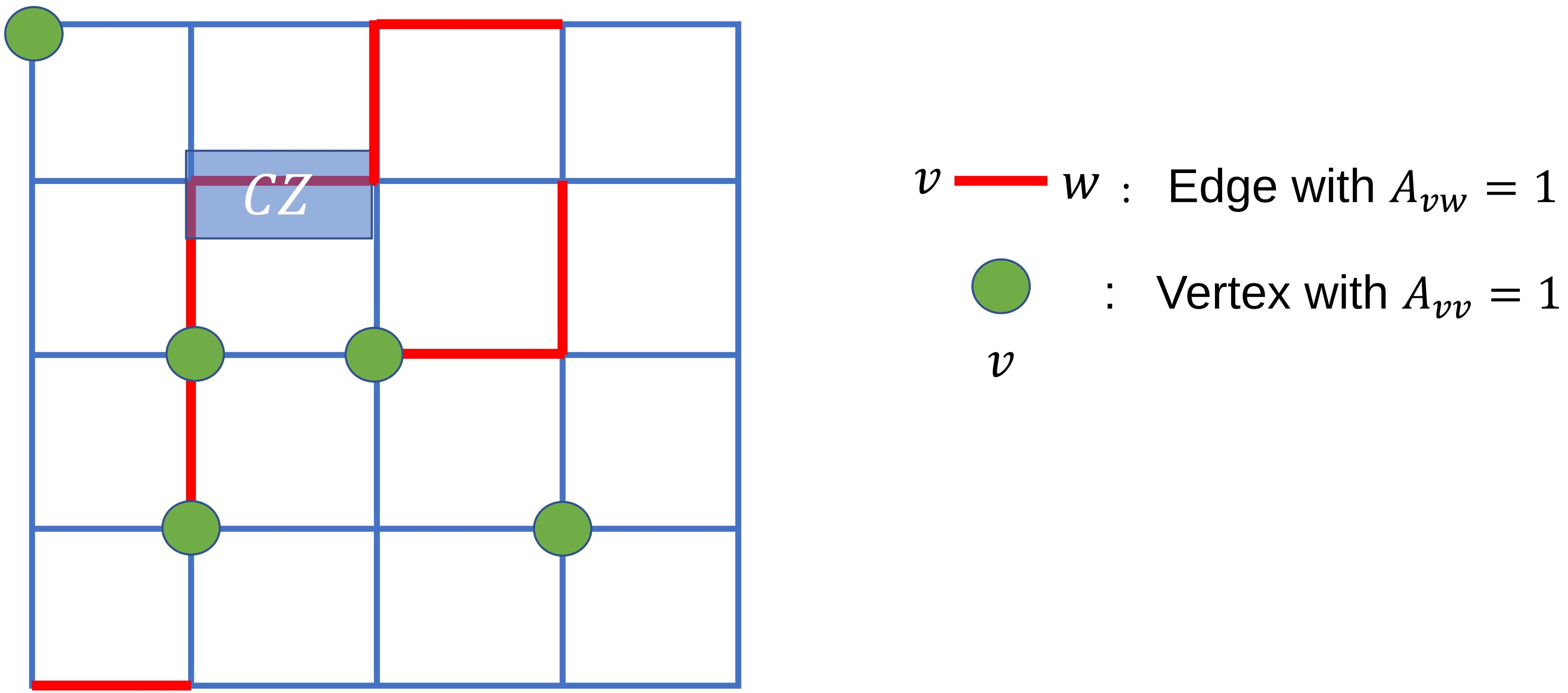
Constant depth quantum algorithm



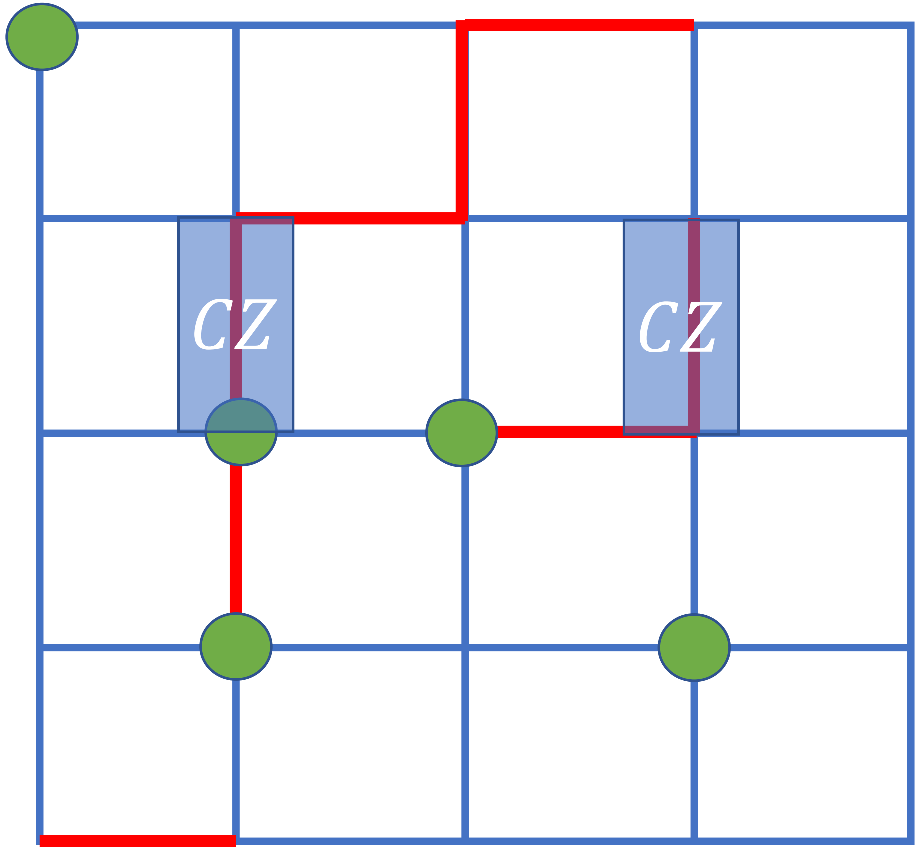
v —— w : Edge with $A_{vw} = 1$

v : Vertex with $A_{vv} = 1$

Constant depth quantum algorithm



Constant depth quantum algorithm

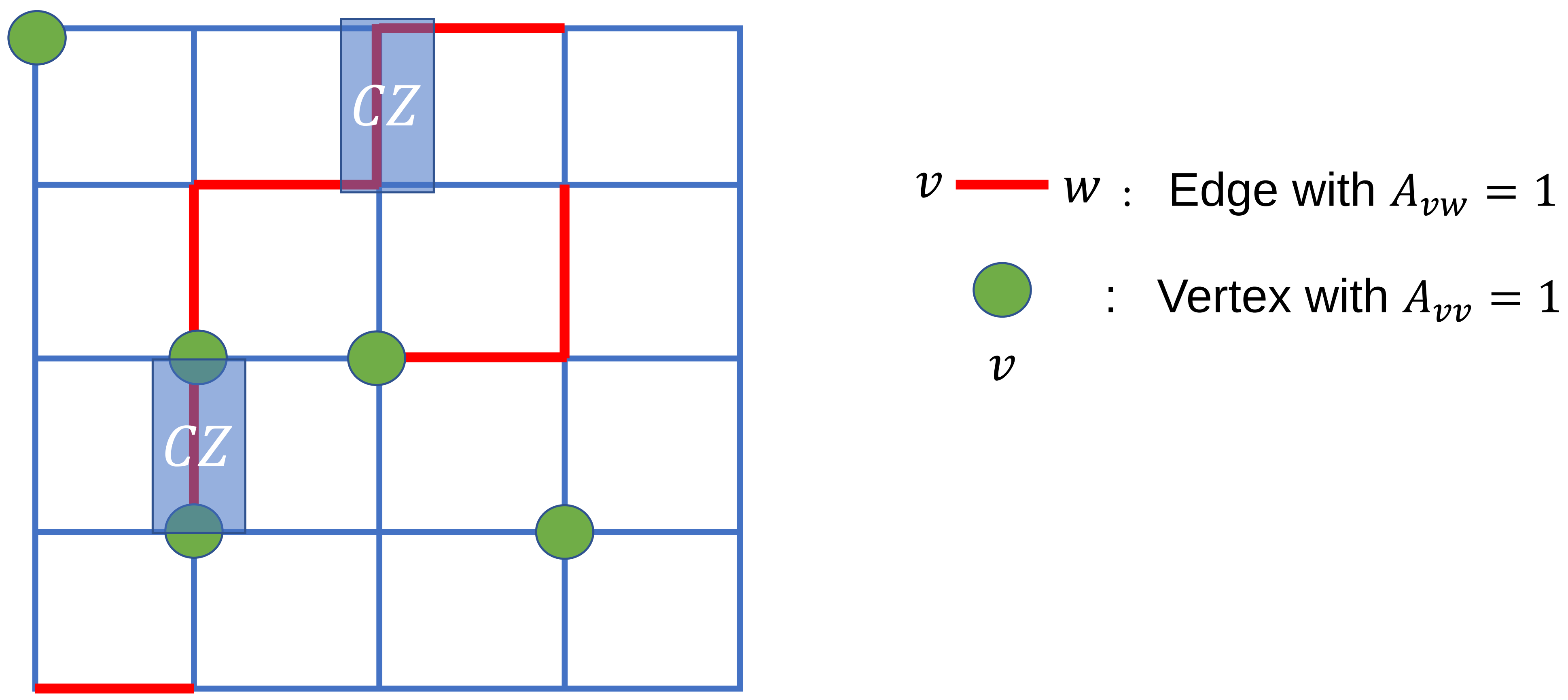


v —— w : Edge with $A_{vw} = 1$

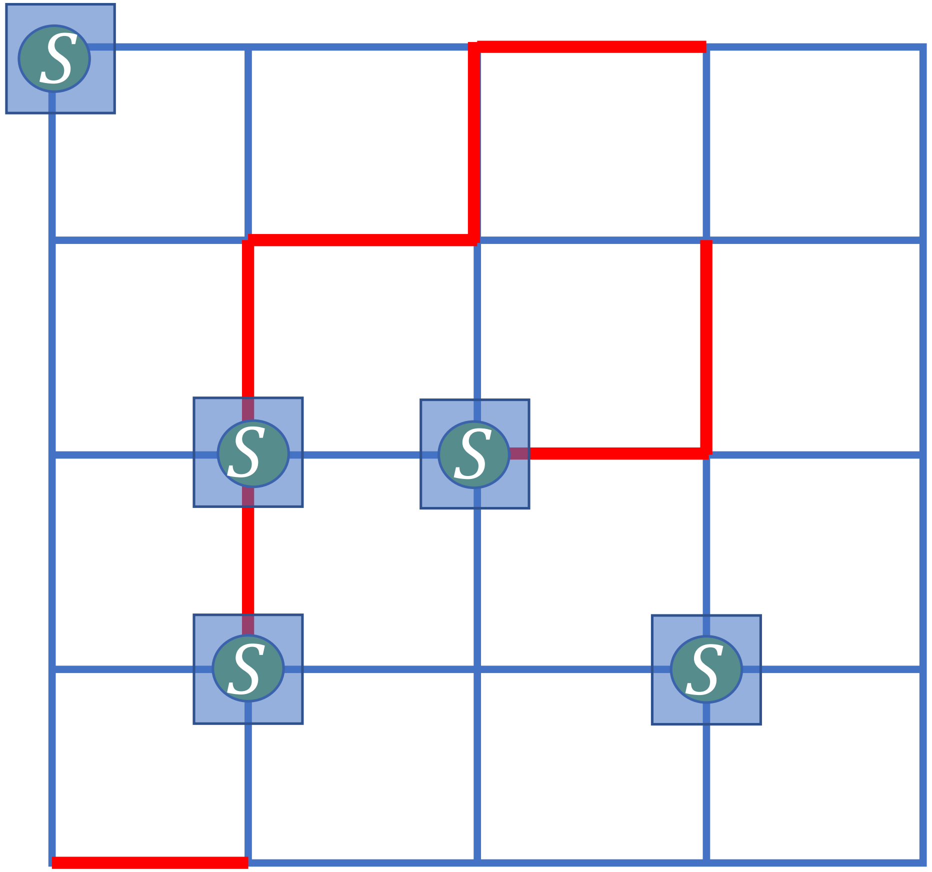
● : Vertex with $A_{vv} = 1$

v

Constant depth quantum algorithm



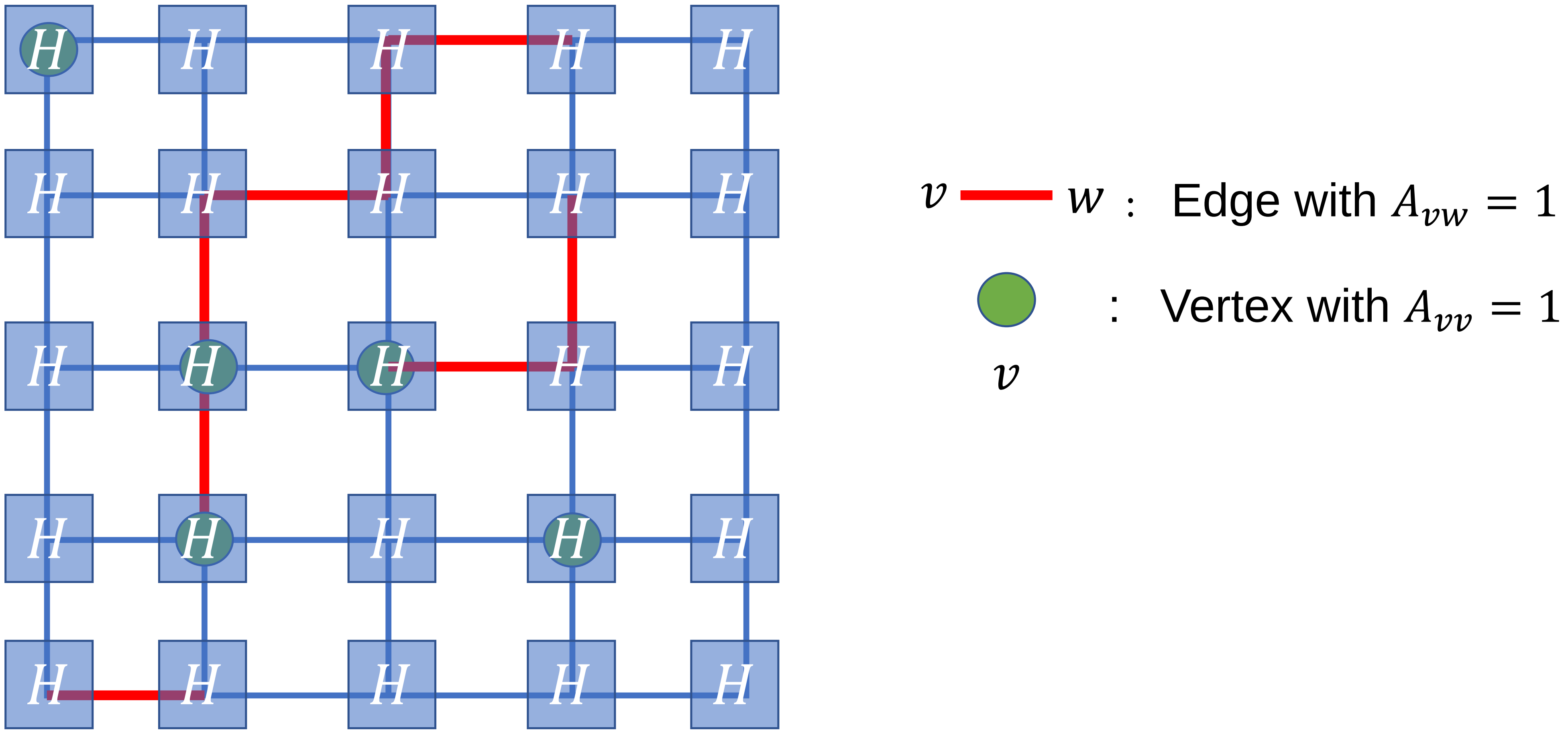
Constant depth quantum algorithm



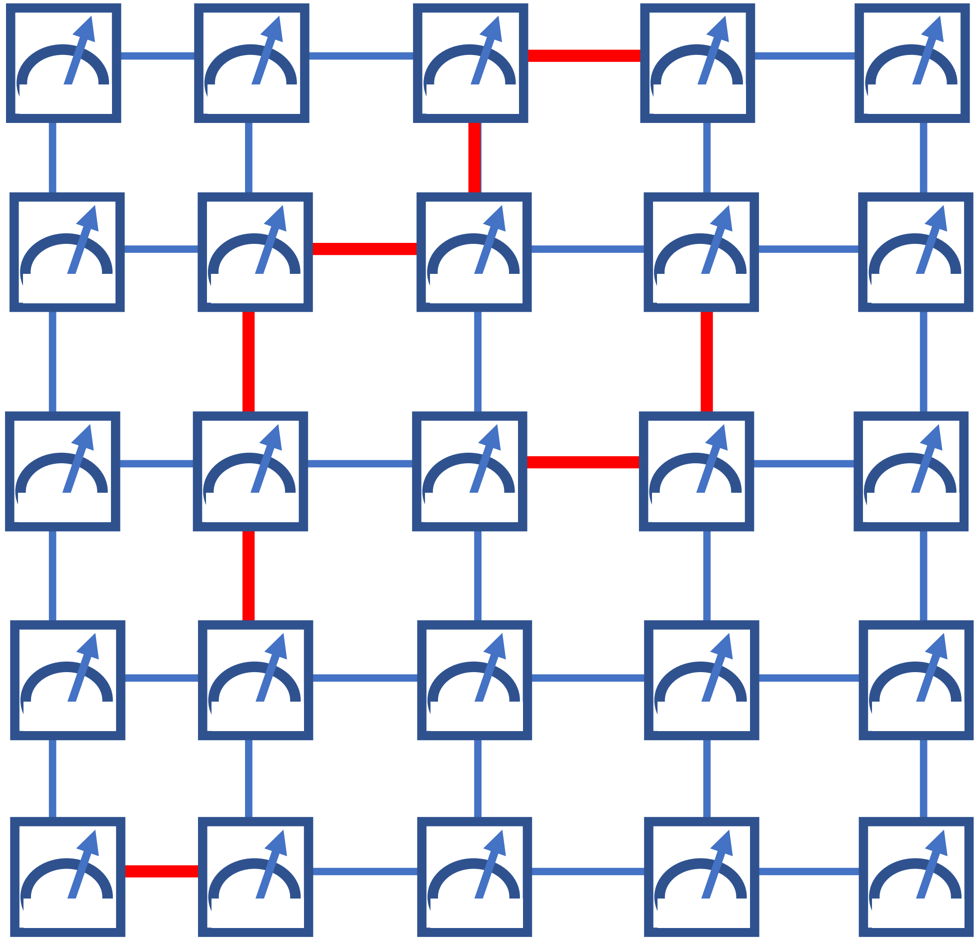
v —— w : Edge with $A_{vw} = 1$

● v : Vertex with $A_{vv} = 1$

Constant depth quantum algorithm



Constant depth quantum algorithm



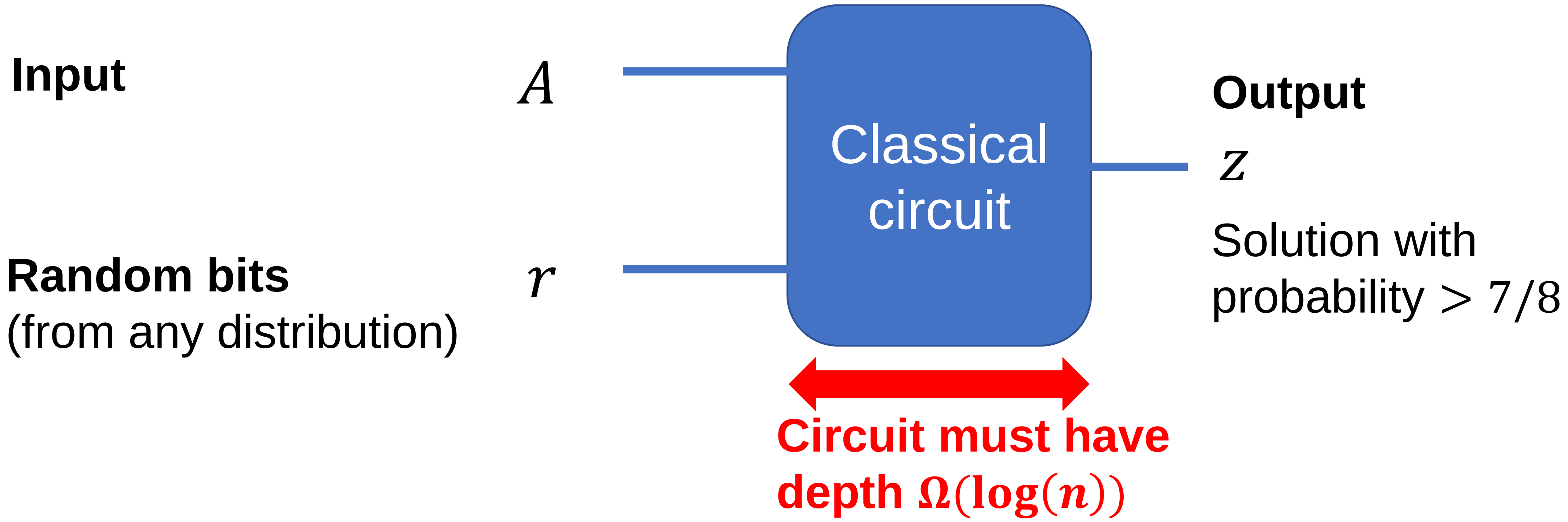
v —— w : Edge with $A_{vw} = 1$

● v : Vertex with $A_{vv} = 1$

Classical circuits require log depth

Theorem [Bravyi DG Koenig 2017]
Any classical probabilistic circuit composed of gates of fan-in $\leq K$ which solves the 2D HLF Problem with probability greater than $7/8$ has

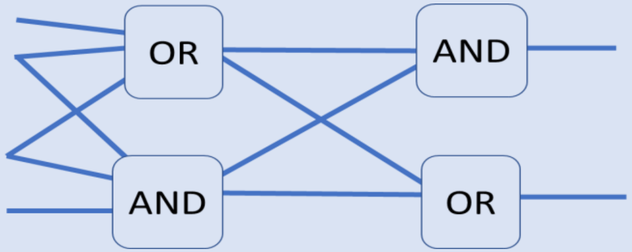
$$\text{depth} \geq \frac{\log(n)}{8\log(K)}$$


Input
A
Random bits
(from any distribution)
r
Classical circuit
Output
z
Solution with probability > 7/8
Circuit must have depth Ω(log(n))

Proof ideas

Locality in shallow classical circuits

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



Vs.

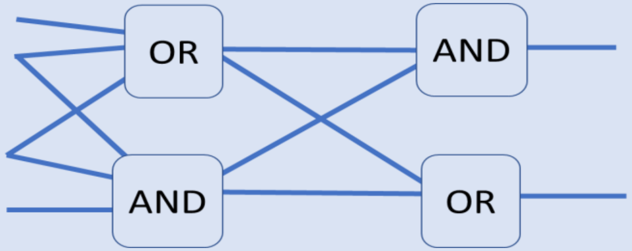
Quantum nonlocality

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

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

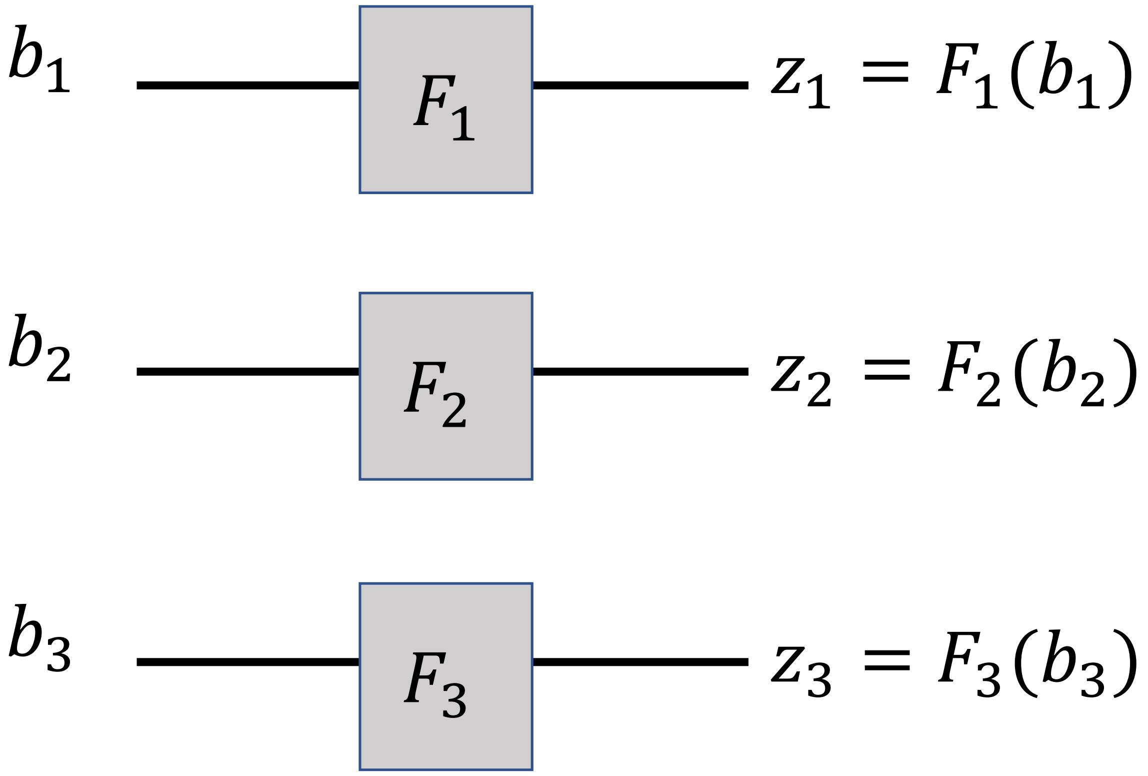
Shallow circuits generalize local hidden variable models

Outputs of constant depth quantum circuits have a strong form of quantum nonlocality

Motivating example

[Greenburger et al. 1990][Mermin 1990]

A **completely local** classical circuit.



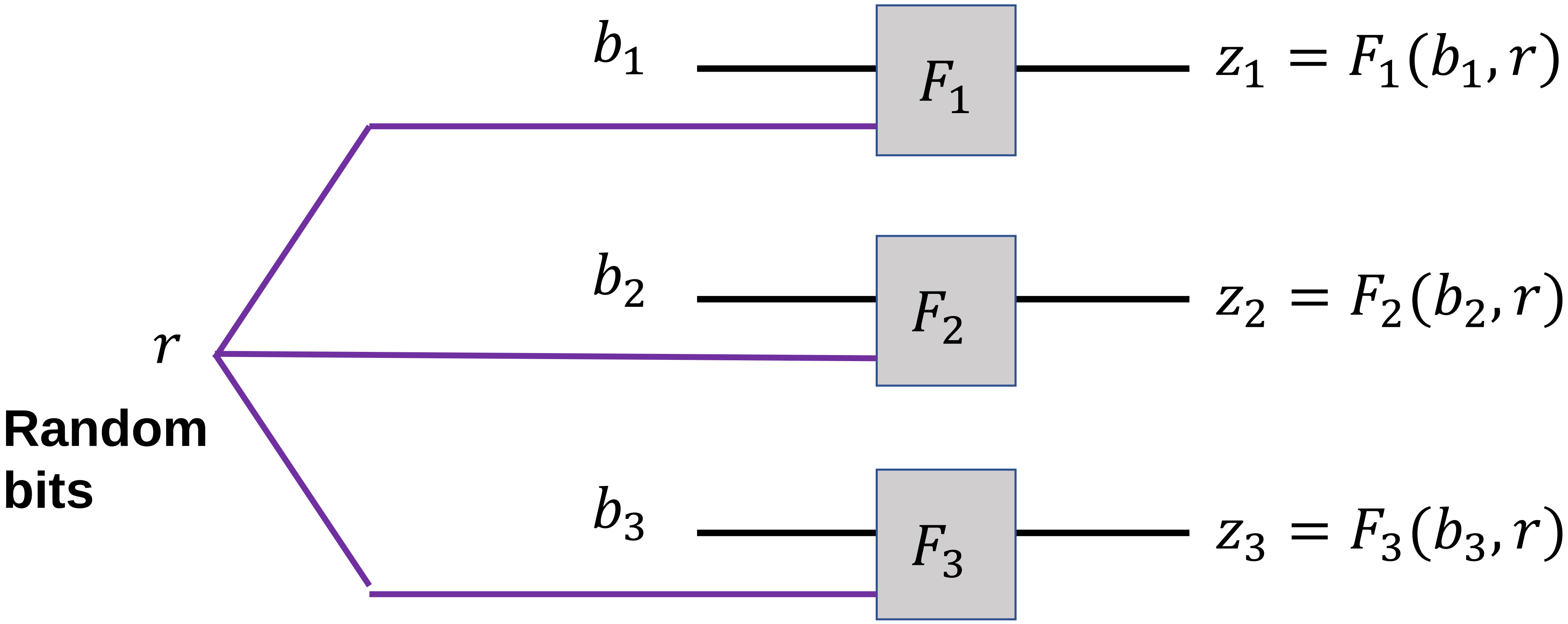
Inputs $\mathbf{b_1, b_2, b_3 \in \{0, 1\}}$

Outputs $\mathbf{z_1, z_2, z_3 \in \{-1, 1\}}$

Motivating example

[Greenburger et al. 1990][Mermin 1990]

A **completely local** probabilistic classical circuit ⟷ Local hidden variable model



Motivating example

[Greenburger et al. 1990][Mermin 1990]

The following input/output relation cannot be realized by a **completely local** probabilistic classical circuit.

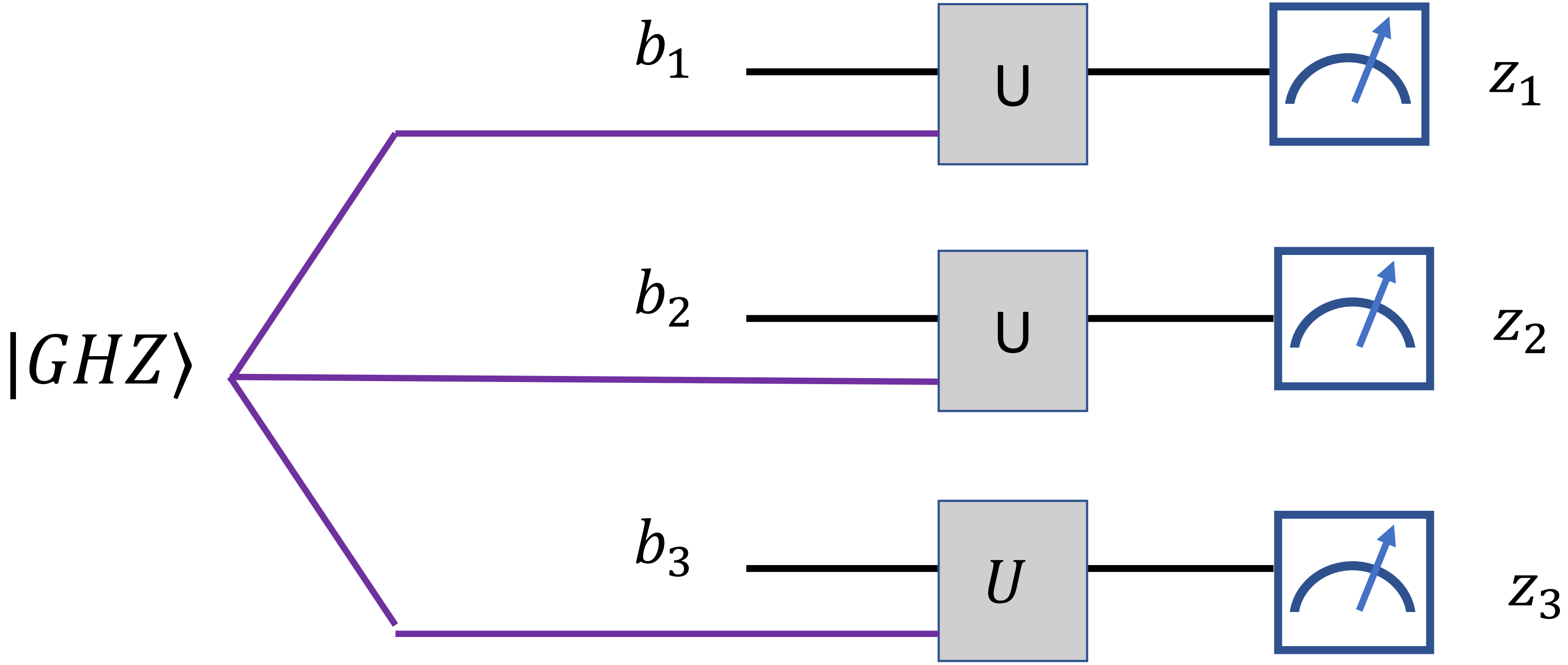
b_1	b_2	b_3	$z_1 z_2 z_3$
0	0	0	1
1	1	0	-1
0	1	1	-1
1	0	1	-1

"GHZ relation"

Motivating example

[Greenburger et al. 1990][Mermin 1990]

However the GHZ relation can be realized by a quantum circuit with the same structure:

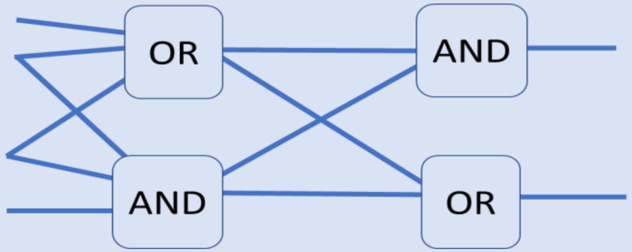


$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Proof ideas

Locality in shallow classical circuits

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



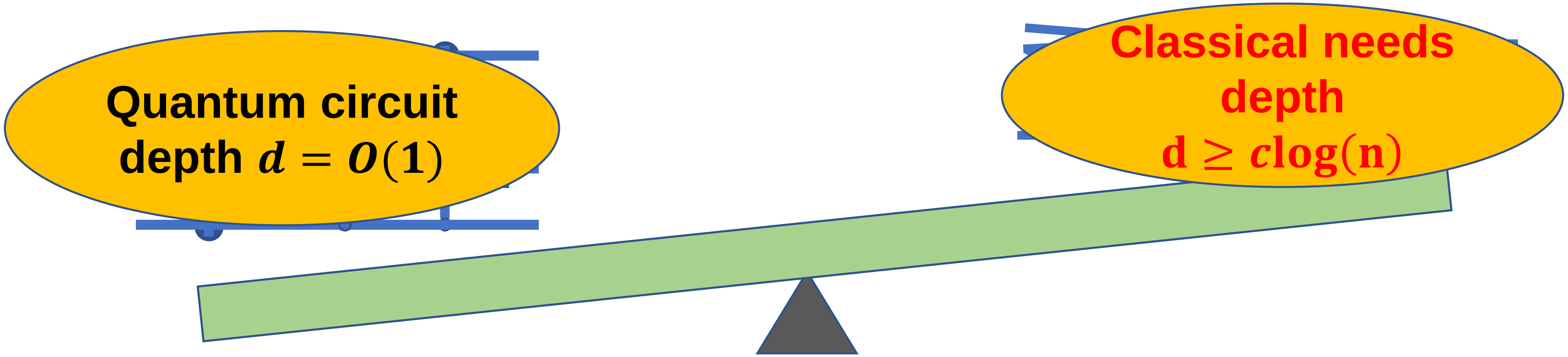
Vs.

Quantum nonlocality

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

Shallow circuits generalize completely local circuits (local hidden variable models)

Outputs of constant depth quantum circuits have a strong form of quantum nonlocality



What else can we do with constant depth quantum circuits?