Quantum advantage with shallow circuits

Robert König

joint work with Sergey Bravyi and David Gosset (IBM)

QIP 2018

arXiv:1704.00690

Technische Universität München

Are quantum computers more powerful than classical ones?

The development of a scientific field – A familiar cycle of seasons

…but will the progress flourish into a quantum summer?

Justified excitement, or overblown promise?

[…] how realistic are such claims about the future of quantum computing?

[A. Abbott and C. Calude, Limits of Quantum Computing: A Sceptic's View
http://www.quantumforquants.org/quantum-computing/limits-of-quantum-computing/]

"three good reasons for thinking that quantum computers have capabilities surpassing what classical computers can do"

(1) Quantum algorithms for classically intractable problems. First, we know of problems that are believed to be hard for classical computers, but for which quantum algorithms have been discovered that could solve these problems easily. The best known example is the problem of finding the prime factors of a large composite integer [1]. We believe factoring is hard because many smart people have tried for many decades to find better factoring algorithms and haven't succeeded. Perhaps a fast classical factoring algorithm will be discovered in the future, but that would be a big surprise.

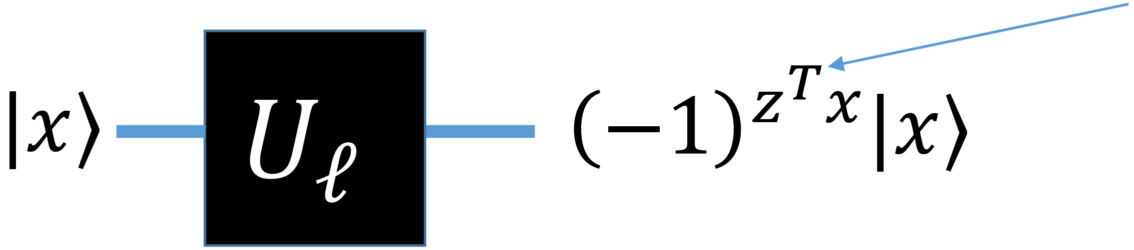
(2) Complexity theory arguments. The theoretical computer scientists have provided arguments, based on complexity theory, showing (under reasonable assumptions) that quantum states which are easy to prepare with a quantum computer have superclassical properties; specifically, if we measure all the qubits in such a state we are sampling from a correlated probability distribution that can't be sampled from by any efficient classical means [2, 3].

(3) No known classical algorithm can simulate a quantum computer. But perhaps the most persuasive argument we have that quantum computing is powerful is simply that we don't know how to simulate a quantum computer using a digital computer; that remains true even after many decades of effort by physicists to find better ways to simulate quantum systems.

[J. Preskill, arXiv:1801.00862 (based on a keynote address at Quantum Computing for Business)]

Bernstein-Vazirani problem (1993)

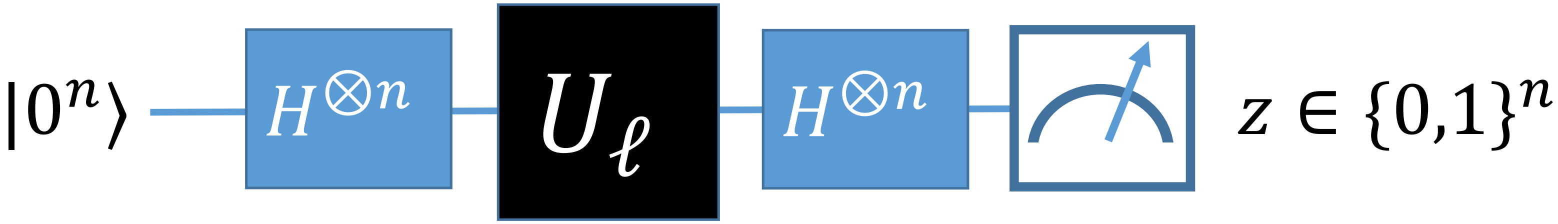
Problem: Find $z \in \{0,1\}^n$ using few queries to an oracle:



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

- The following quantum circuit computes z using only **1 query** to the quantum oracle:

- In contrast, any classical algorithm needs $\boldsymbol{n}$ **queries** to a classical oracle computing ℓ to determine z.

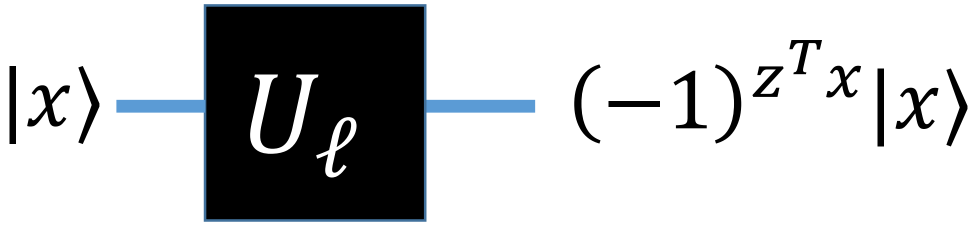


[Bernstein and Vazirani, Quantum complexity theory, SIAM Journal on Computing, 26(5):1411-1473, 1997]

This problem shows a separation between classical and quantum algorithms **in terms of query complexity.**

Potential concerns about query complexity separations

"Where's my black-box?"



"Black-box problems, where one is required to compute a function or property of a classical input by querying a *quantum box*, are easier to prove speedups for because of their extra formal structure. But this also means that they often have a **somewhat artificial flavour and their practical relevance is questionable**."

"One well-known such algorithm is Grover's algorithm, [....] **The cost of constructing the quantum database could negate any advantage of the algorithm**, and in many classical scenarios one could do much better by simply creating (and maintaining) an ordered database."

[A. Abbott and C. Calude, Limits of Quantum Computing: A Sceptic's View http://www.quantumforquants.org/quantum-computing/limits-of-quantum-computing/]

Our result

A **provable**, **non-oracular** quantum speedup,

attainable by a

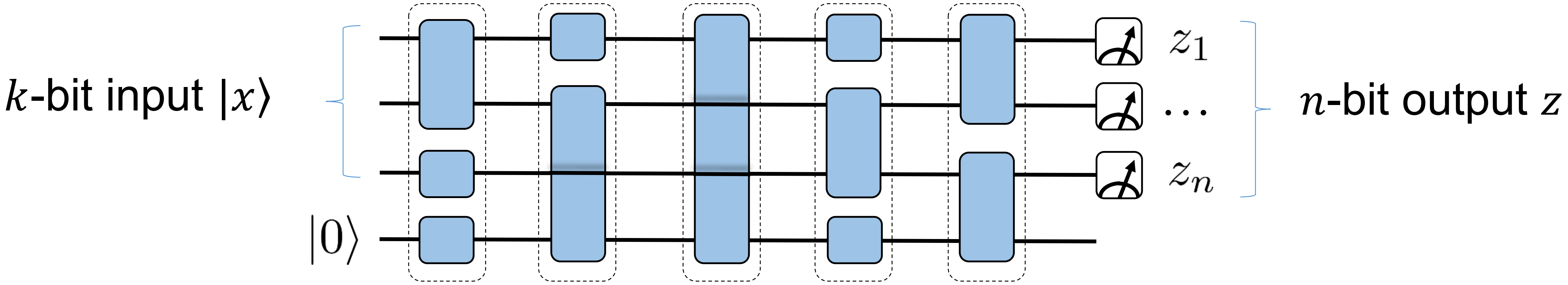
constant-depth

geometrically local (in a 2D),

circuit.

This talk: constant-depth (quantum) circuits

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



Example: depth-5 circuit

$P(z|x)$ output probability distribution for a given input x

Family of circuits $\{U_n\}_n$ with **depth $O(1)$**. Constant-depth or "Shallow"

Fixed set of gates independent of n.

Motivation for considering constant-depth quantum circuits:

The Noisy Intermediate-Scale Quantum (NISQ) Technology Era

[J. Preskill, Quantum Computing in the NISQ era and beyond, arXiv:1801.00862]

Circuit depth in the Noisy Intermediate-Scale Quantum Technology Era

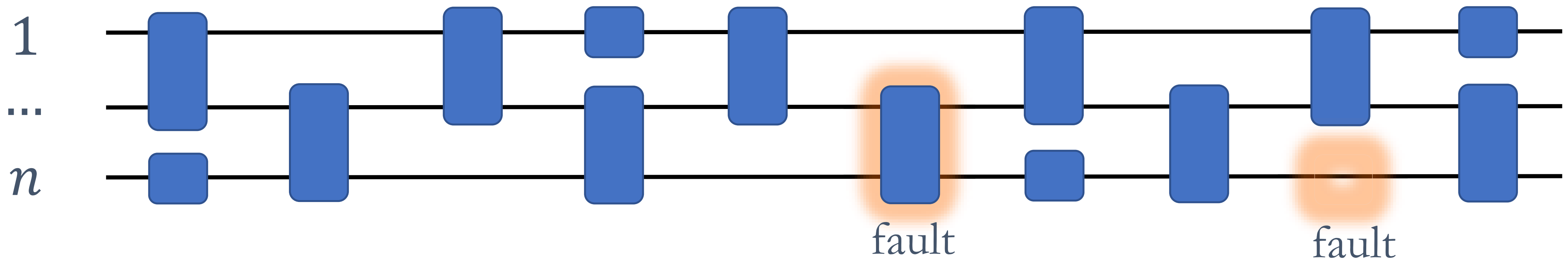
Noise sets a limit on the maximum size of a computation without error correction.

Rough estimate: $nd \ll 1/\epsilon$

n = number of qubits (width)

d = circuit depth

ϵ = error rate



Deep circuits → few qubits → efficient classical simulation.

Shallow circuits → many qubits → potential for a quantum advantage.

Shallow circuits and their potential

$d \leq 2$ | $O(1)$ | $O(\log n)$ | $poly(n)$

$d \leq 2$

efficient classical simulation

Terhal, DiVincenzo 2002

$O(1)$

approximate optimization

variational quantum eigensolver

quantum supremacy ?

Farhi, Goldstone, Gutmann 2014
Peruzzo et al 2014
Boixo et al 2016
Bermejo-Vega et al 2017
Gao, Wang, Duan 2017
Bremner, Montanaro, Shepherd 2016

$O(\log n)$

Shor's algorithm

Clifford circuits

good variational states (MERA)

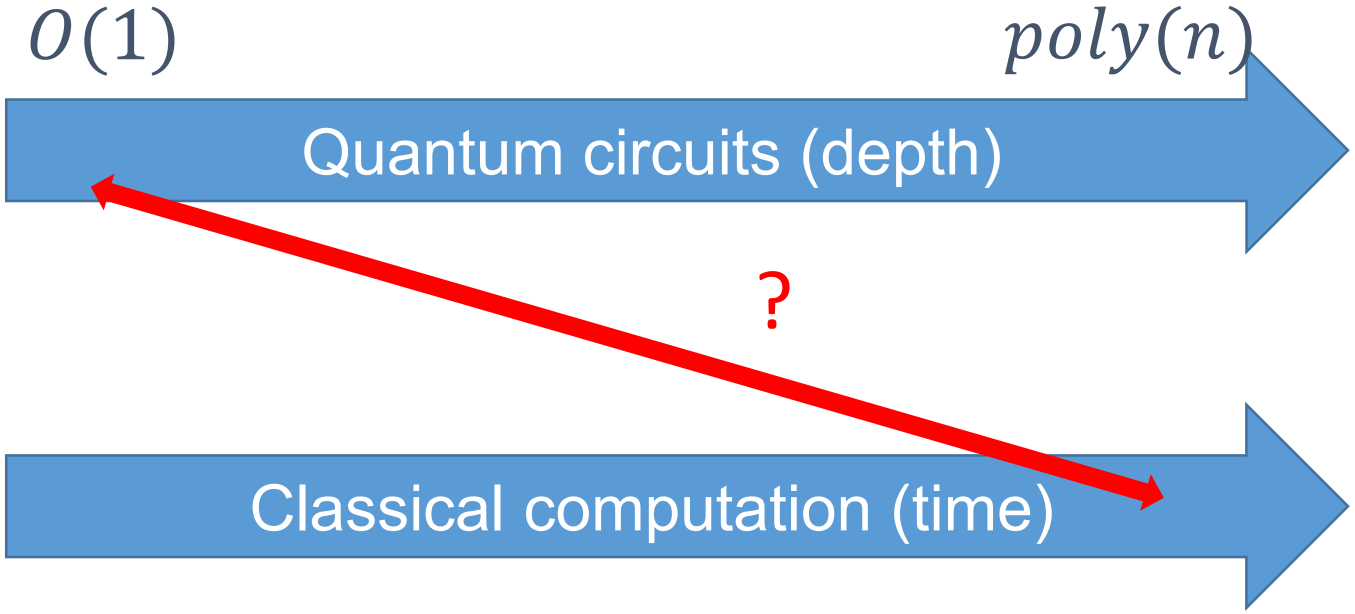
toy models of black holes ?

Cleve, Watrous 2000
Vidal 2007
Moore, Nilsson 2001
Brown, Fawzi 2013

$poly(n)$

BQP complete

Constant-depth quantum circuits versus classical circuits

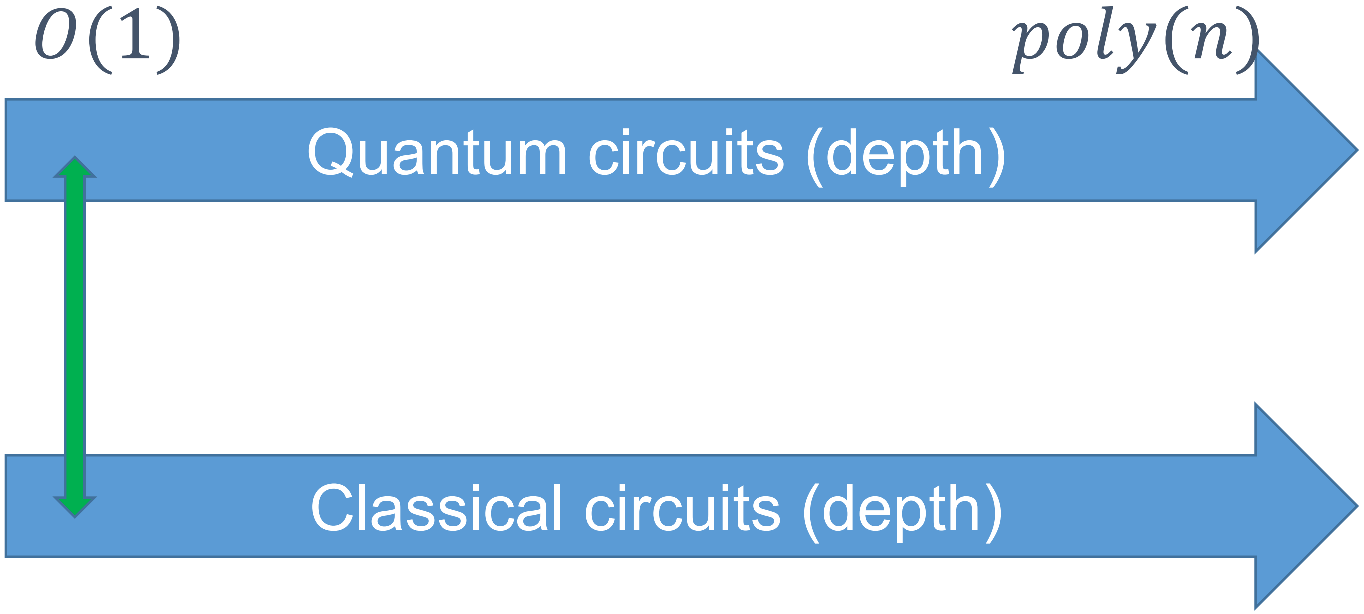


Can **constant-depth quantum** circuits solve a computational problem that **polynomial-time classical computations** cannot?

Too difficult question… No hope for unconditional proof.

Positive answer would imply P≠PSPACE.

Constant-depth quantum versus classical circuits



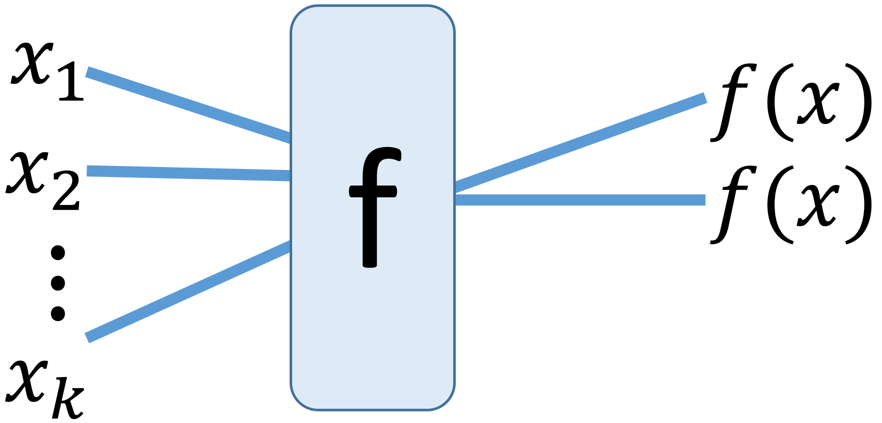
Can **constant-depth quantum** circuits solve a computational problem that **constant-depth classical circuits** cannot?

This talk: The answer is YES.

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**



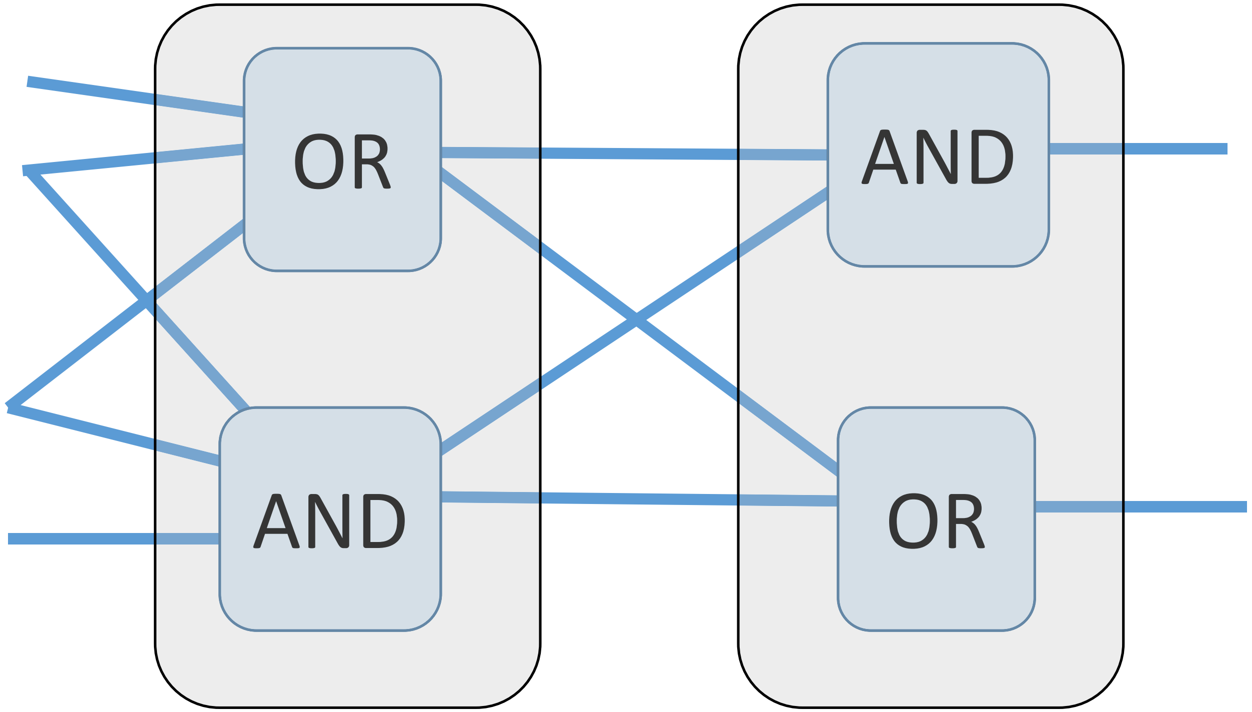
Number of times the output is used is called the **fan-out**

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.

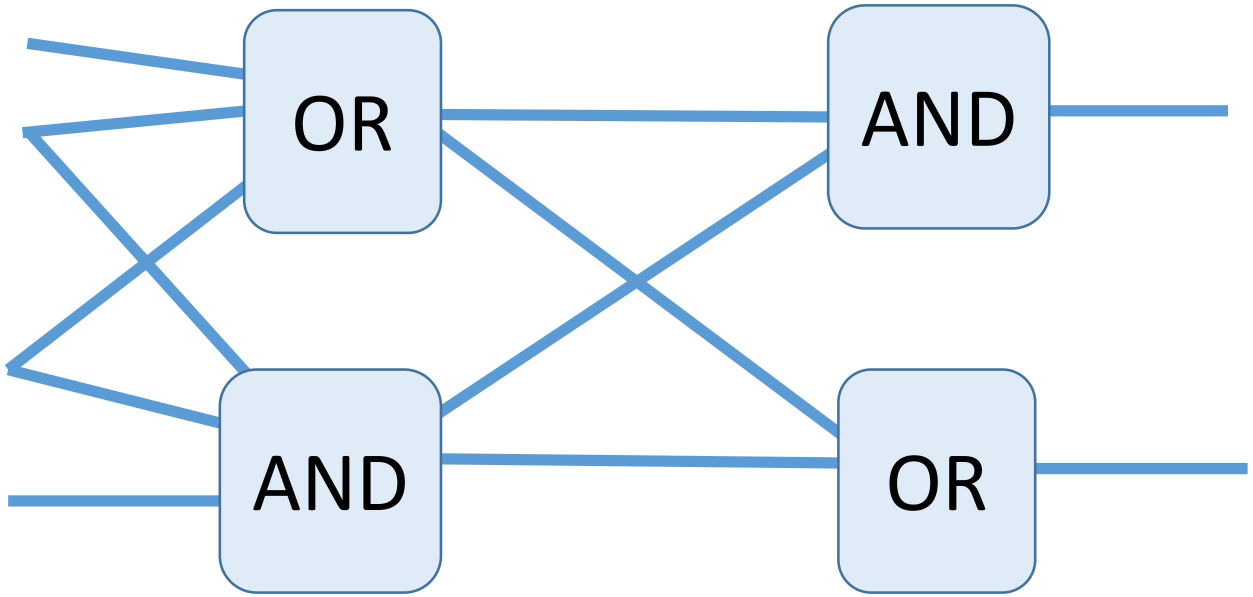


Time step 1

Time step 2

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**.

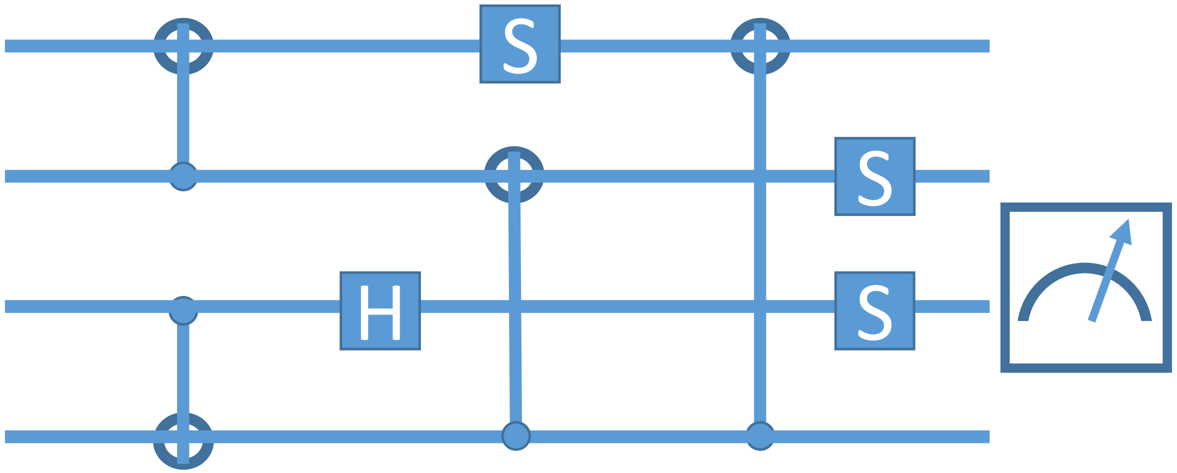
We also allow the circuit to be probabilistic (random input bits are provided).

Can constant-depth quantum circuits solve a **computational problem** that constant-depth classical circuits cannot?

	Input	Output
✗ Decision problem	Bit-string x	$b_x \in \{0,1\}$

Causality: The marginal distribution of any output bit is determined by $O(1)$ input bits.

Example:



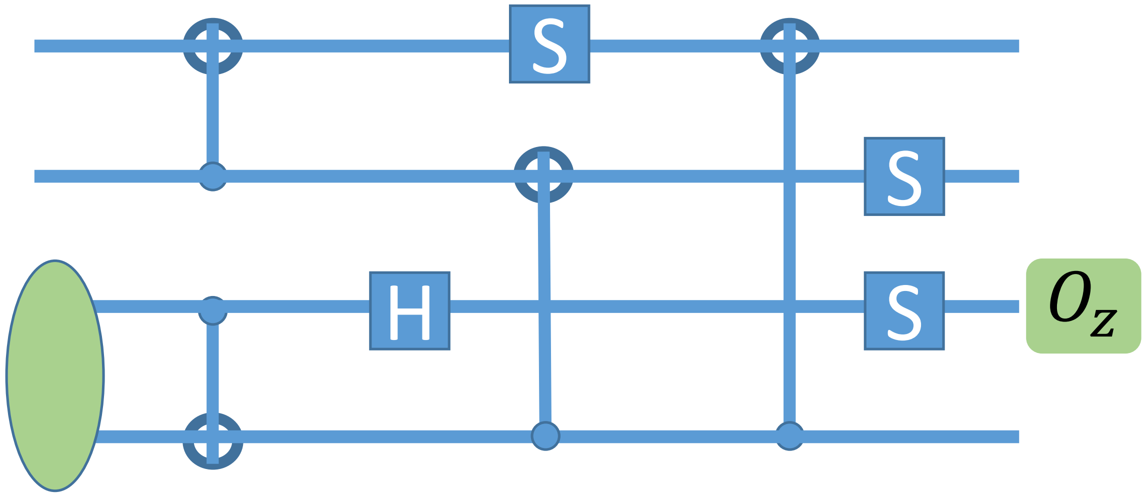
Simulation by a classical circuit of size $O(1)$

Can constant-depth quantum circuits solve a **computational problem** that constant-depth classical circuits cannot?

	Input	Output
✗ Decision problem	Bit-string x	$z \in \{0,1\}$

Causality: The marginal distribution of any output bit is determined by $O(1)$ input bits.

Support of size $2^d = O(1)$



$$P(z|x) = \langle x, 0 | U^\dagger O_z U | x, 0 \rangle$$

O(1)-local operator

Can constant-depth quantum circuits solve a **computational problem** that constant-depth classical circuits cannot?

	Input	Output
✗ **Decision problem**	Bit-string x	$b_x \in \{0,1\}$
✓ **Relation problem**	Bit-string x	$z \in S_x \subseteq \{0,1\}^n$ (non-unique)

Example: combinatorial optimization, say 3-SAT

x { system of equations with binary variables

S_x { set of bit strings satisfying all equations

$z \in S_x$ { a satisfying assignment

Can constant-depth quantum circuits solve a **computational problem** that constant-depth classical circuits cannot?

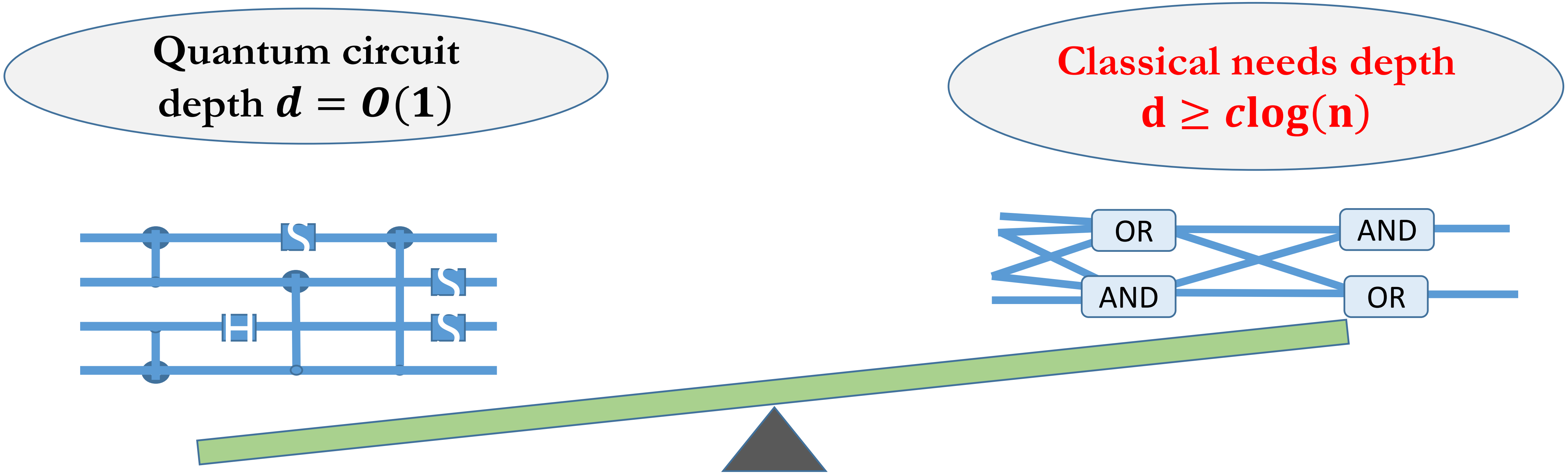
	Input	Output	
✗ **Decision problem**	Bit-string x	$b_x \in \{0,1\}$	
✓ **Relation problem**	Bit-string x	$z \in S_x \subseteq \{0,1\}^n$	(non-unique)

A (quantum) circuit **solves a relation problem** if

for any input x it outputs a valid solution z (with high probability) :

$$\sum_{z \in S_x} P(z|x) \geq 1 - \epsilon \quad \forall x$$

Quantum advantage of constant-depth circuits



Our result: We describe a (relation) problem such that

- The problem is **solved with certainty** $(\epsilon = 0)$ **by a constant-depth quantum circuit** (with geometrically local gates in 2D).

- **Any probabilistic classical circuit** composed of **bounded fan-in gates** (possibly non-local) which **solves the problem with high probability** $(\epsilon < 1/8)$ **must have depth increasing logarithmically with input size**.

The quantum speedup is unconditional:
It is non-oracular and does not rely on complexity-theoretic conjectures.

Note: The problem can be solved in polynomial time classically.

The Hidden Linear Function (HLF) Problem

The Bernstein-Vazirani speedup is relative to an oracle.

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

$$(-1)^{z^T x}|x\rangle$$

Where else can we hide a linear function?

Binary quadratic forms

Suppose A is a symmetric binary matrix of size n

Nullspace: $\mathrm{Ker}(A) = \{x \in \{0,1\}^n \,:\, Ax = 0^n \pmod 2\}$

Quadratic form:
$$q : \{0,1\}^n \to \{0,1,2,3\}$$
$$q(x) = x^T A x \pmod 4 \qquad x \in \{0,1\}^n$$

Example: $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ $\quad Ax = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod 2$ $\quad \mathrm{Ker}(A) = \{000, 111\}$

$$q(x) = x^T A\, x \pmod 4 = x_1 + x_3 + 2x_1x_2 + 2x_2x_3 \pmod 4$$

Real-valued versus binary quadratic forms

x is a real vector: $Ax = 0^n$ implies $x^T Ax = 0$.

x is binary: the restriction of $q(x)$ onto $\mathrm{Ker}(A)$ can be non-zero

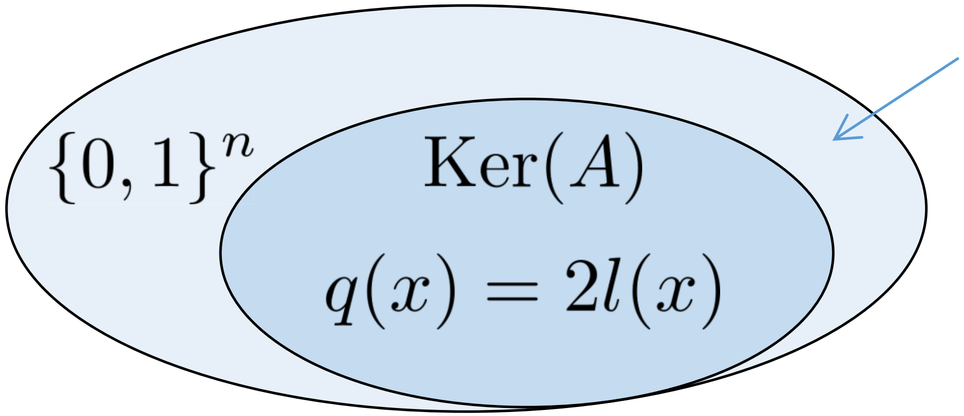
Example: $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ $Ax = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod 2$ $\mathrm{Ker}(A) = \{000, 111\}$

$$q(x) = x^T A\, x \pmod 4 = x_1 + x_3 + 2x_1x_2 + 2x_2x_3 \pmod 4$$

$$q(111) = 1 + 1 + 2 + 2 \pmod 4 = 2$$

Fact:

The restriction of $q(x)$ onto the nullspace of A is a linear function (up to a factor of 2)



$q(x) = x^T A x$

$l : \{0,1\}^n \to \{0,1\}$ Boolean linear function

Proof sketch:

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

for $x \in \mathrm{Ker}(A), y \in \{0,1\}^n$

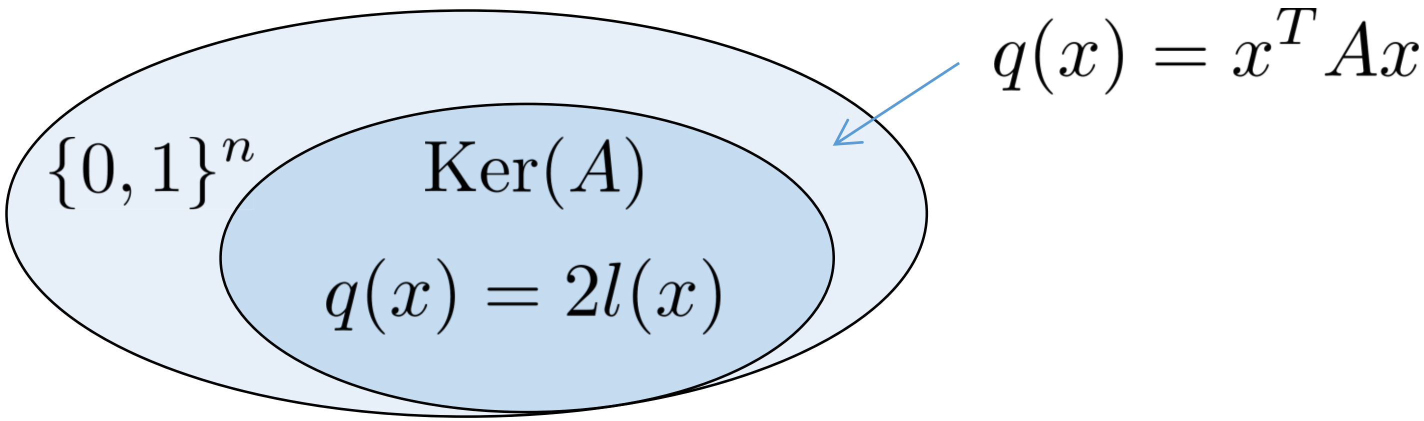
$$= q(x) + y^T (2Ax) + q(y) \mod 4$$

since $Ax = 0^n \mod 2$

$\Rightarrow 2Ax = 0^n \mod 4$

$$= q(x) + q(y) \mod 4$$

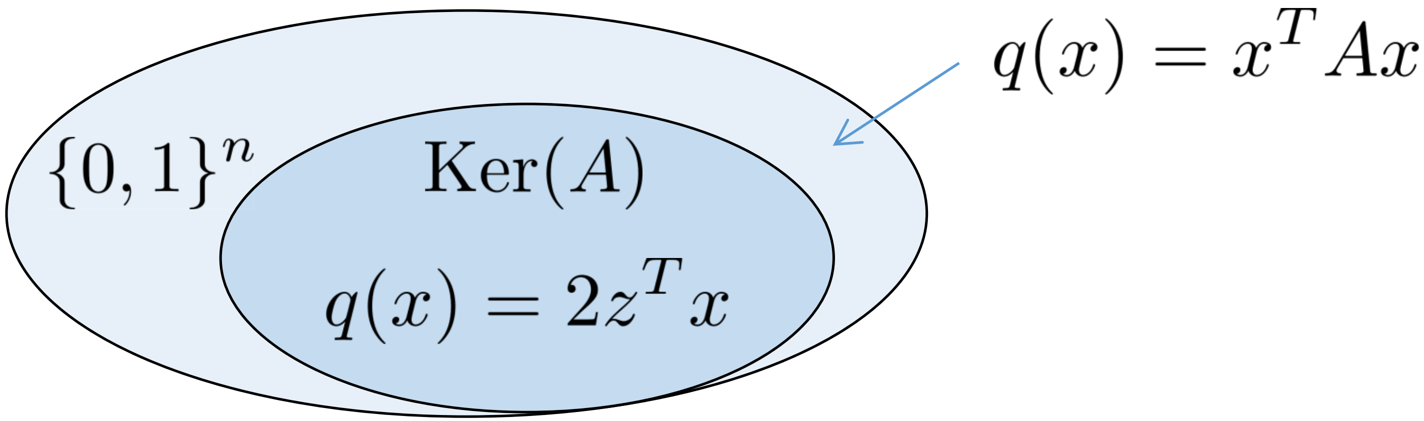
Fact:
The restriction of $q(x)$ onto the nullspace of A is a linear function (up to a factor of 2)



$l \, : \, \{0,1\}^n \to \{0,1\}$ Boolean linear function

A binary quadratic form hides a Boolean linear function (in a non-oracular way)

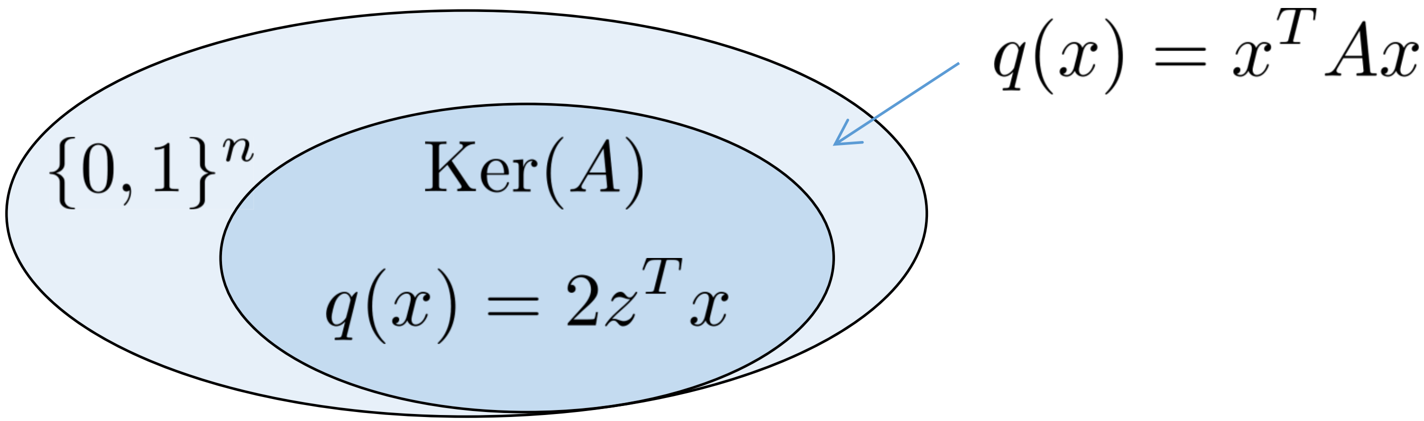
Fact:
The restriction of $q(x)$ onto the nullspace of A is a linear function (up to a factor of 2)



$z \in \{0,1\}^n$ "secret" bit string

A binary quadratic form hides a Boolean linear function (in a non-oracular way)

Fact:
The restriction of $q(x)$ onto the nullspace of A is a linear function (up to a factor of 2)



$z \in \{0,1\}^n$ "secret" bit string

Hidden Linear Function (HLF) problem

Input: binary symmetric matrix A.
Output: bitstring z such that $q(x) = 2z^T x \pmod 4$ for all $x \in \mathrm{Ker}(A)$

Hidden Linear Function (HLF) problem

Input: binary symmetric matrix A.
Output: bitstring z such that $q(x) = 2z^T x \pmod 4$ for all $x \in \mathrm{Ker}(A)$

- This can be viewed as a non-oracular variant of the Bernstein-Vazirani problem.

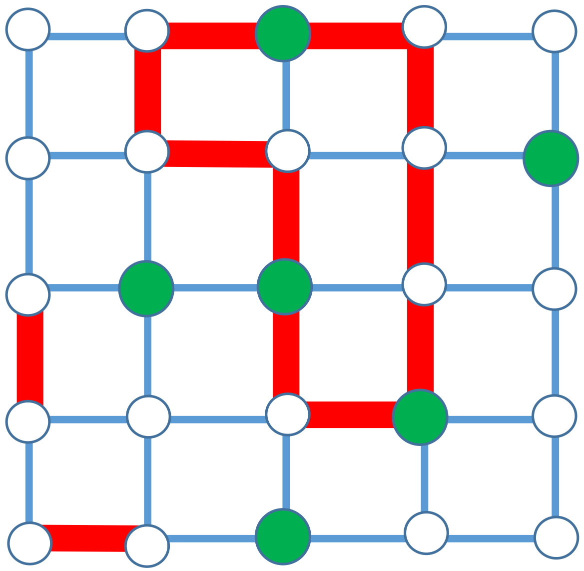
- The solution is non-unique:

  if z is a solution and $y \in \mathrm{Ker}(A)^{\perp}$ then $z \oplus y$ is a solution

- The HLF problem can be solved classically in time $O(n^3)$

  1) Compute a basis $b^1, \ldots, b^k$ of the nullspace $\mathrm{Ker}(A)$
  2) Solve a linear system $2\, z^T b^i = q(b^i), \quad i = 1, \ldots, k$

The 2D HLF: quadratic forms on a square grid



n sites

Consider a square grid of size $\sqrt{n} \times \sqrt{n}$

Variables $x_1, \ldots, x_n$ live at sites

$A_{i,j} = 0$ unless (i, j) are nearest neighbors

i ▬ j $\quad A_{i.j} = 1$

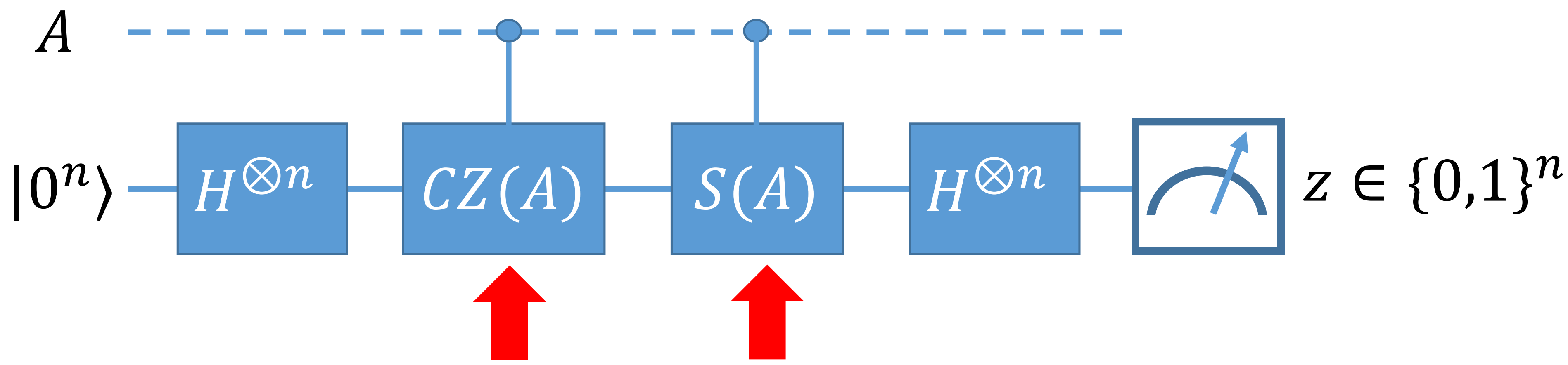
i ● $\quad A_{i.i} = 1$

The **2D HLF problem** is the set of instances where the (off-diagonal part of the) matrix A is the adjacency matrix of a subgraph of the $\sqrt{n} \times \sqrt{n}$ grid graph.

Remainder of the talk

- The hidden linear function (HLF) problem
- A quantum algorithm for the 2D HLF Problem (constant-depth circuit)
- Proof of hardness for constant-depth classical circuits

Solving the 2D HLF by a constant-depth quantum circuit



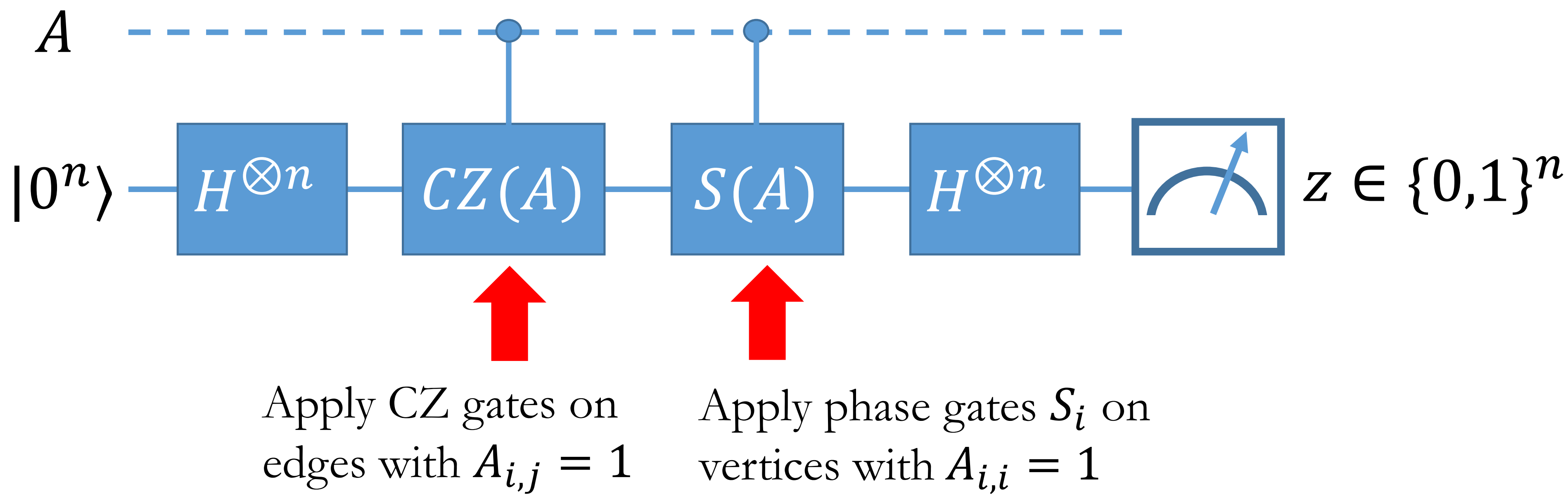
Apply CZ gates on edges with $A_{i,j} = 1$

Apply phase gates S_i on vertices with $A_{i,i} = 1$

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Gate set: Clifford gates H, S, CZ with one (classical) control bit.

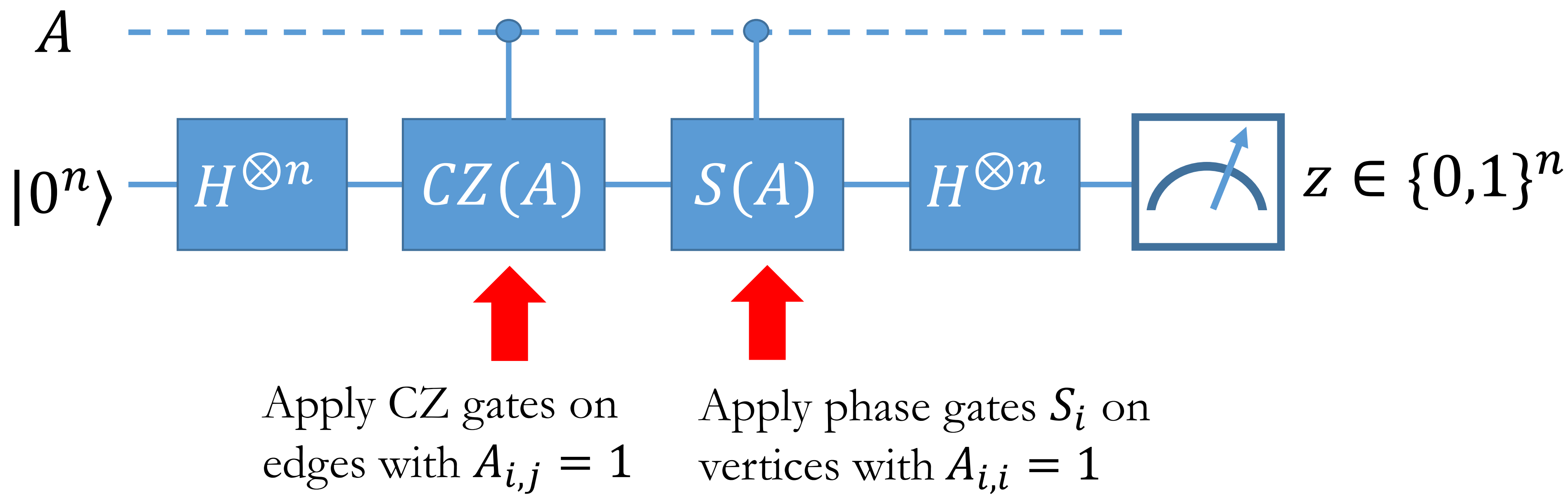
Solving the 2D HLF by a constant-depth quantum circuit



Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.
(The distribution $P(z|A)$ is uniform on the set of all solutions.)

Fact 2: The circuit can be implemented in constant depth.
(with nearest neighbor gates in 2D)

Solving the 2D HLF by a constant-depth quantum circuit



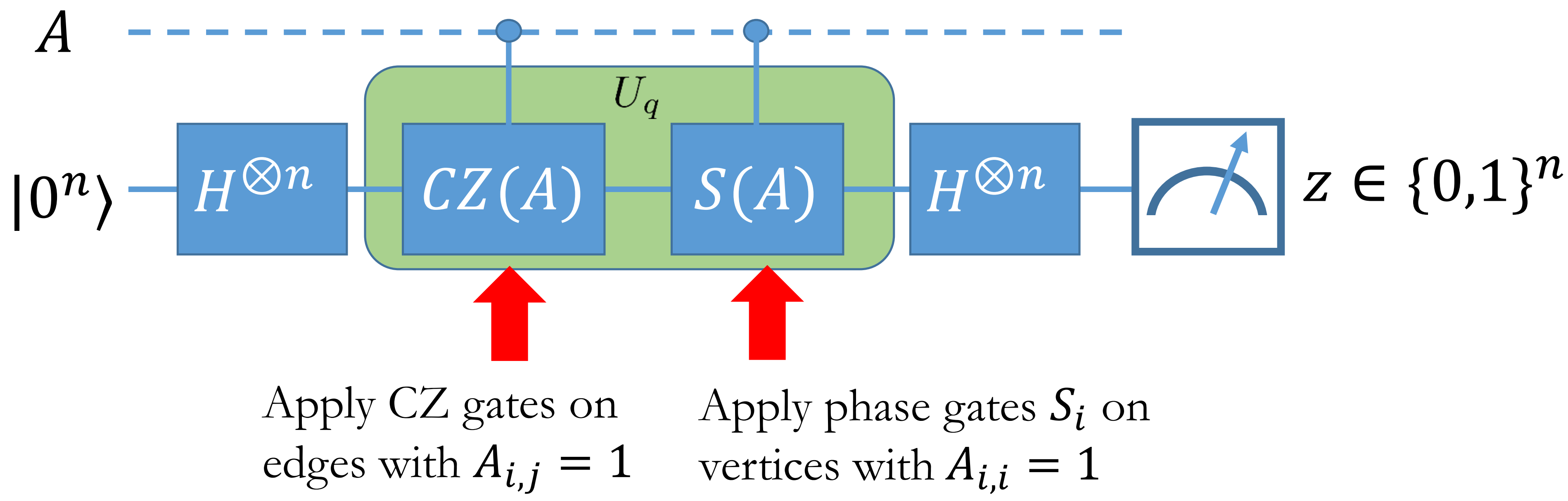
Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.

$$P(z|A) \sim \left| \sum_{x \in \{0,1\}^n} (-1)^{z \cdot x} \cdot i^{q(x)} \right|^2$$

similar to IQP circuits

Bremner, Montanaro, Shepherd 2016

Solving the 2D HLF by a constant-depth quantum circuit



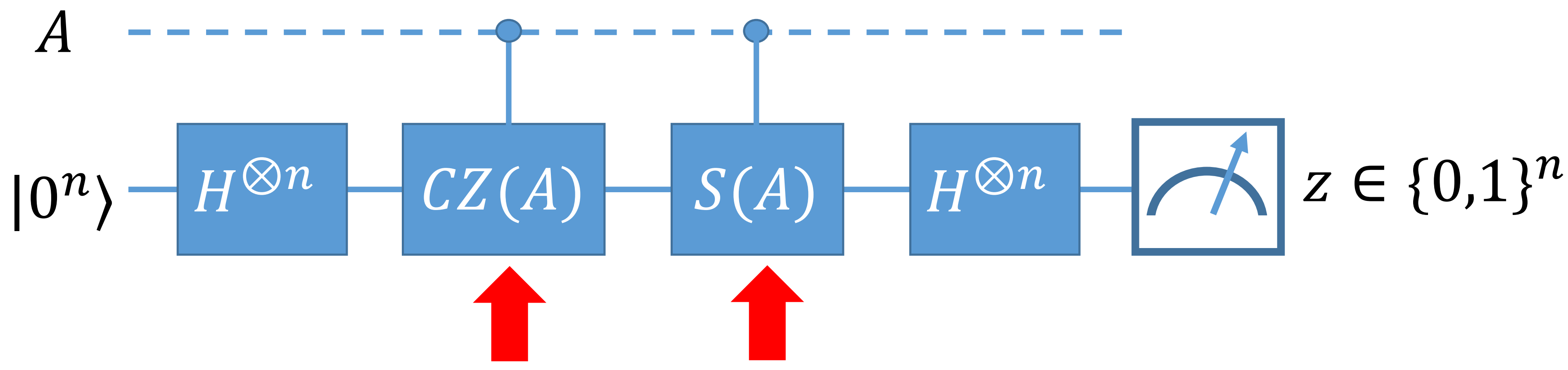
Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.

Relationship to IQP circuits:

The unitary $U_q = S(A)CZ(A)$ is diagonal and satisfies $U_q|x\rangle = i^{q(x)}|x\rangle$ for all $x \in \{0,1\}^n$

This (explicitly realized) unitary takes the place of an oracle in the Bernstein-Vazirani algorithm.

Solving the 2D HLF by a constant-depth quantum circuit



Apply CZ gates on edges with $A_{i,j} = 1$

Apply phase gates S_i on vertices with $A_{i,i} = 1$

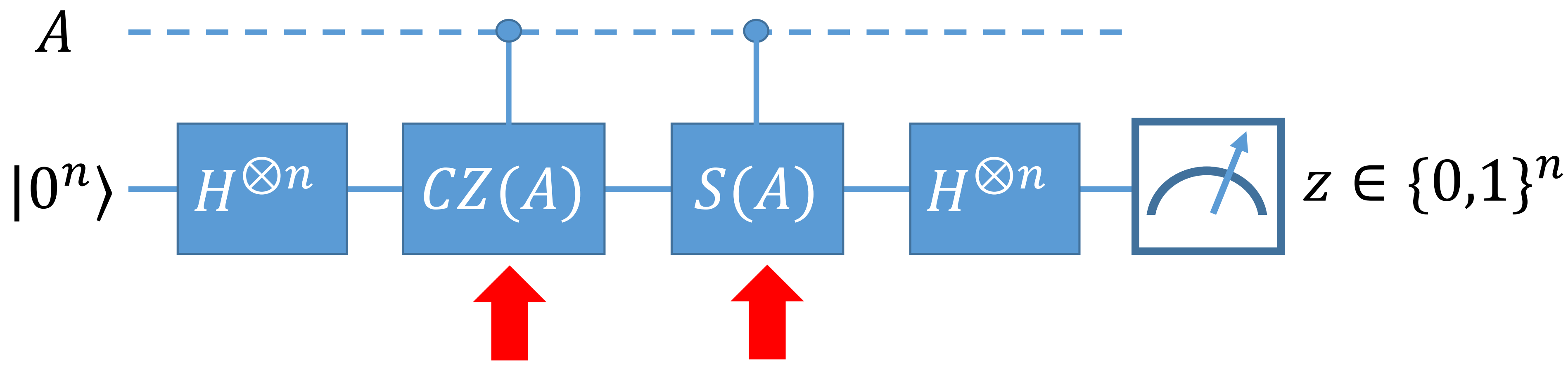
Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.

$$P(z|A) \sim \left| \sum_{x \in \{0,1\}^n} (-1)^{z \cdot x} \cdot i^{q(x)} \right|^2$$

similar to IQP circuits

Bremner, Montanaro,Shepherd 2016

Solving the 2D HLF by a constant-depth quantum circuit



Apply CZ gates on edges with $A_{i,j} = 1$

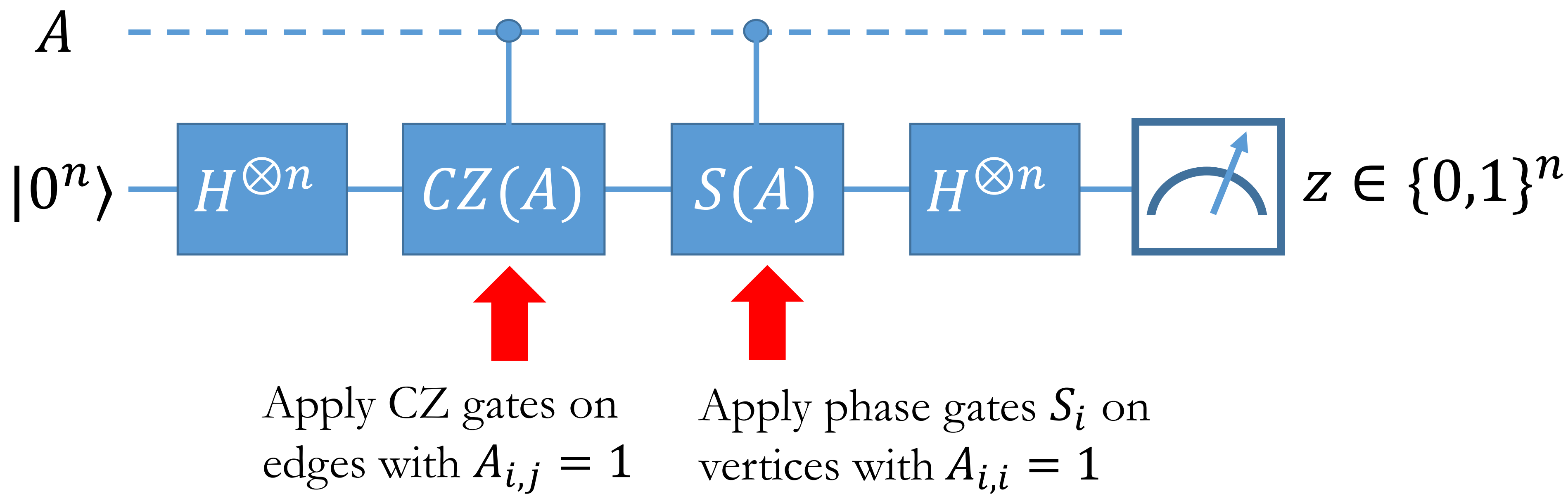
Apply phase gates S_i on vertices with $A_{i,i} = 1$

Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.

$$P(z|A) \sim \left| \sum_{x \in \mathrm{Ker}(A)} (-1)^{z \cdot x} \cdot i^{q(x)} \right|^2$$

use the fact that $q(x)$ is a quadratic form

Solving the 2D HLF by a constant-depth quantum circuit

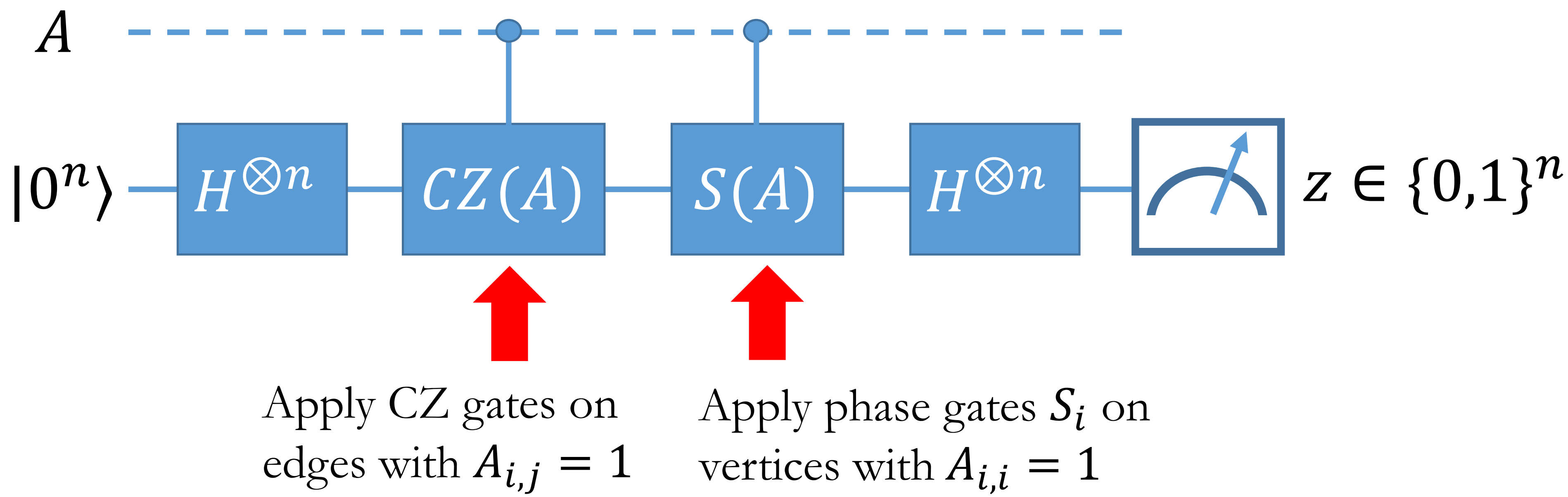


Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.

$$P(z|A) \sim \left| \sum_{x \in \mathrm{Ker}(A)} (-1)^{z \cdot x} \cdot i^{2\ell(x)} \right|^2$$

use the fact that the restriction of $q(x)$ to $\mathrm{Ker}(A)$ is linear

Solving the 2D HLF by a constant-depth quantum circuit

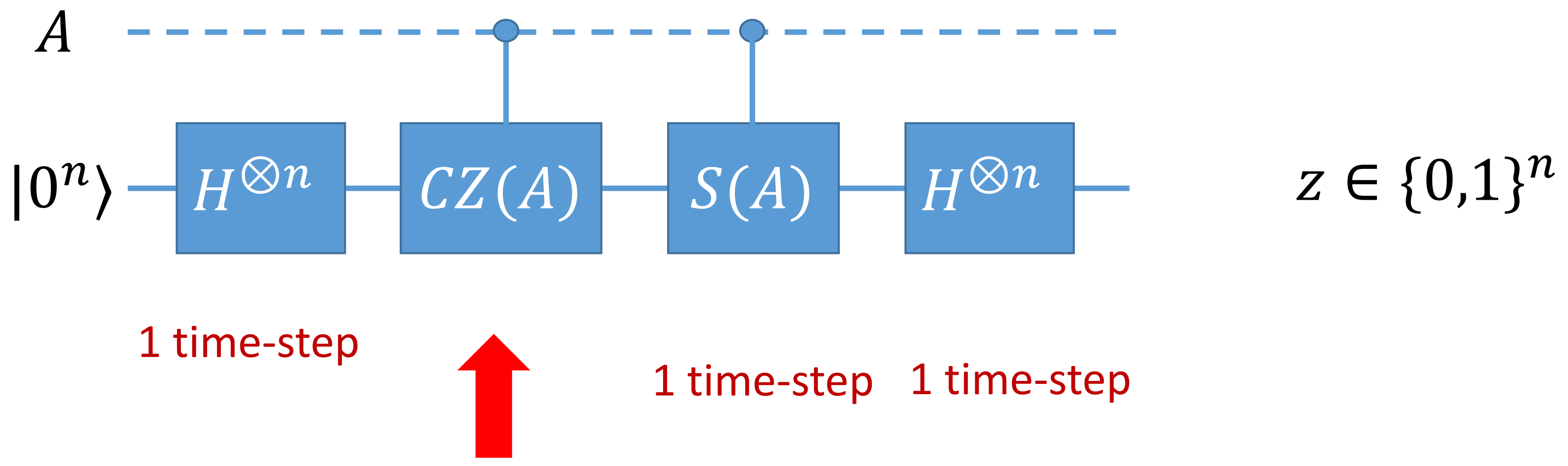


Fact 1: The string of measurement outcomes z is a solution to the 2D HLF Problem.

$$P(z|A) \sim \left| \sum_{x \in \mathrm{Ker}(A)} (-1)^{z \cdot x + l(x)} \right|^2$$

similar to Bernstein-Vazirani

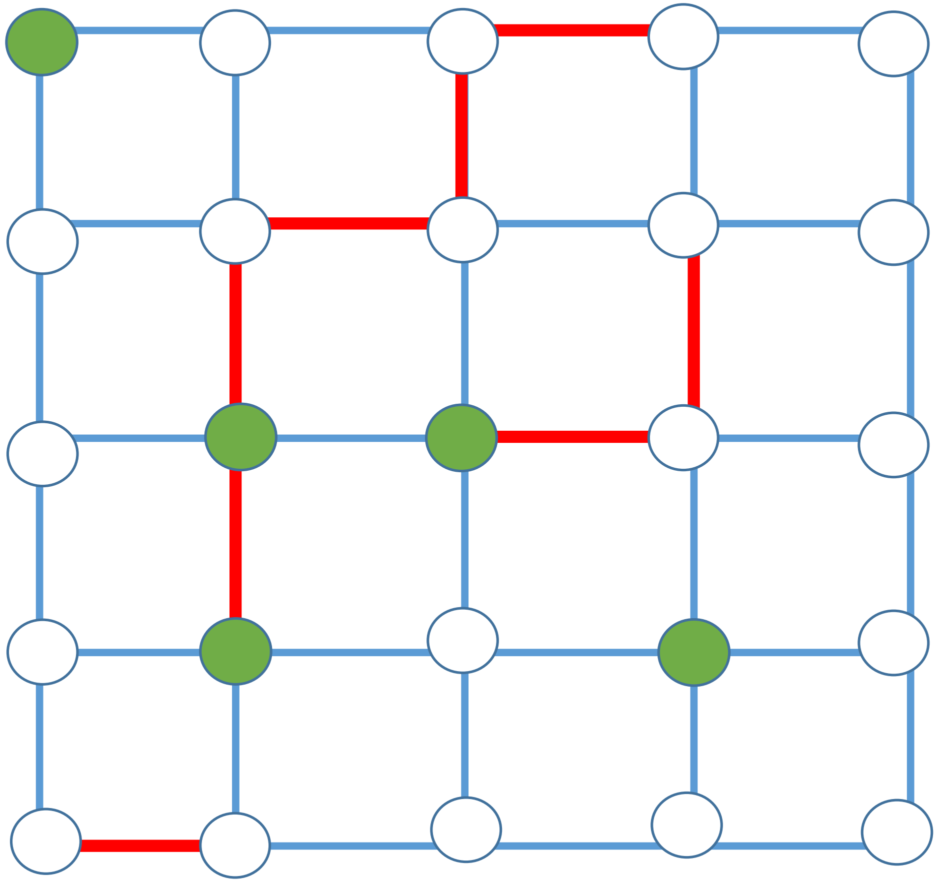
Solving the 2D HLF by a constant-depth quantum circuit



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

Fact 2: The circuit can be implemented in constant depth
(with nearest neighbor gates in 2D)

A constant-depth quantum circuit for 2D HLF



Place a qubit at each vertex in $|0\rangle$

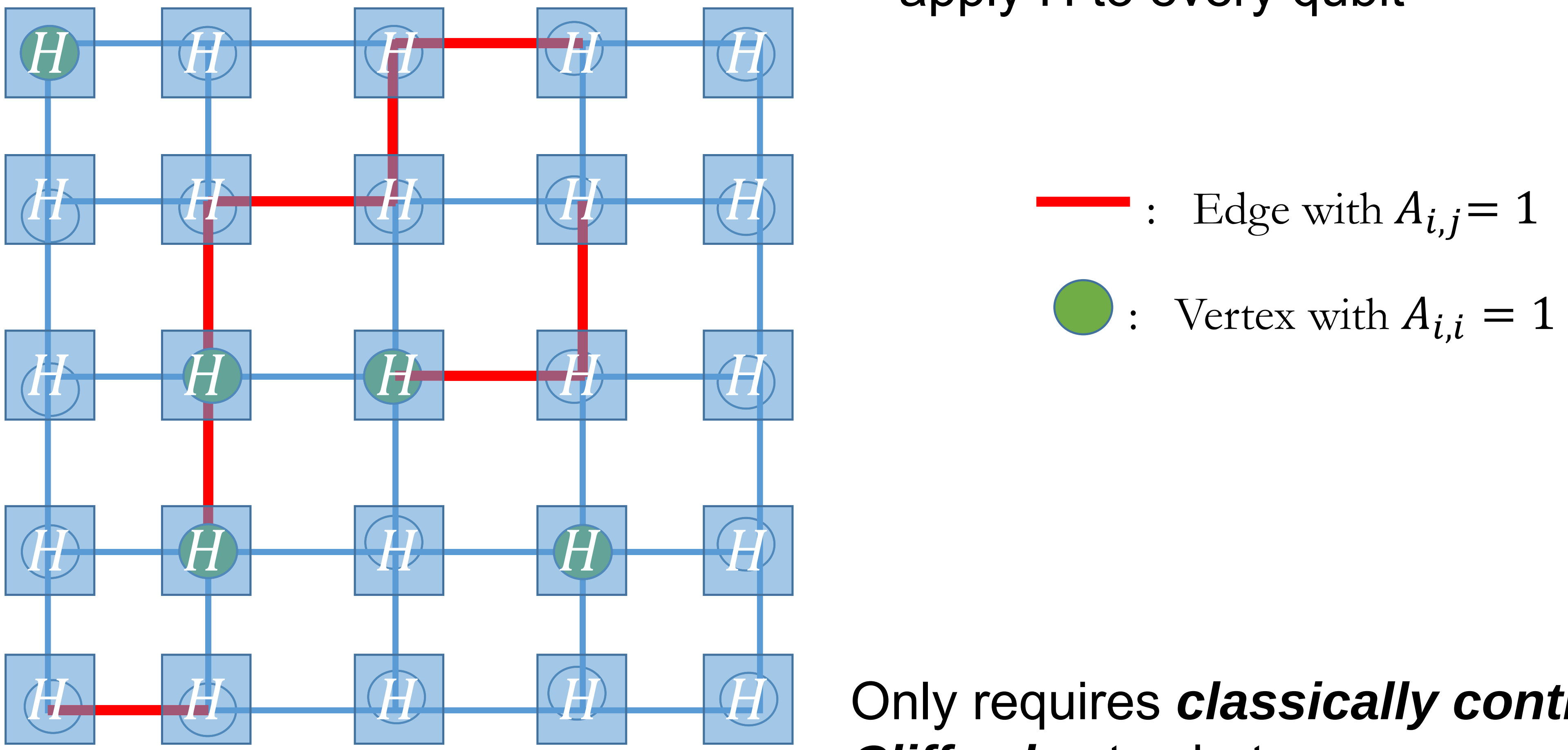
Place input bits on vertices and edges:

(red line) : Edge with $A_{i,j} = 1$

(green circle) : Vertex with $A_{i,i} = 1$

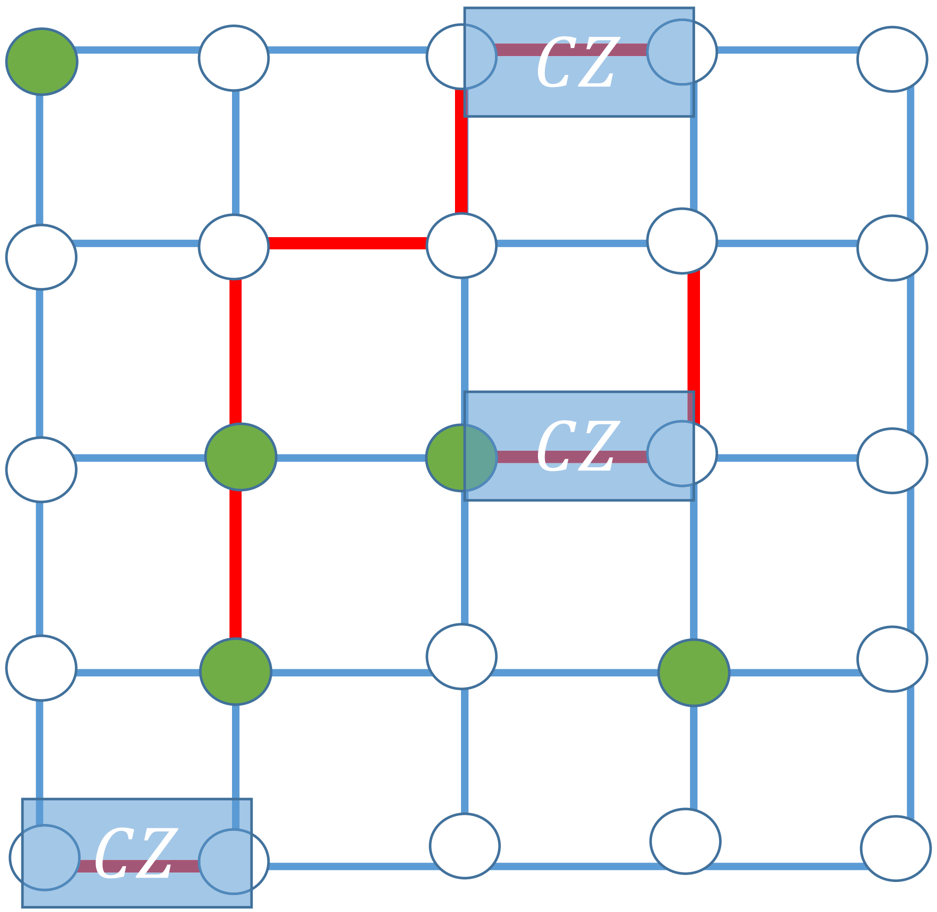
A constant-depth quantum circuit for 2D HLF

apply H to every qubit



Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

A constant-depth quantum circuit for 2D HLF



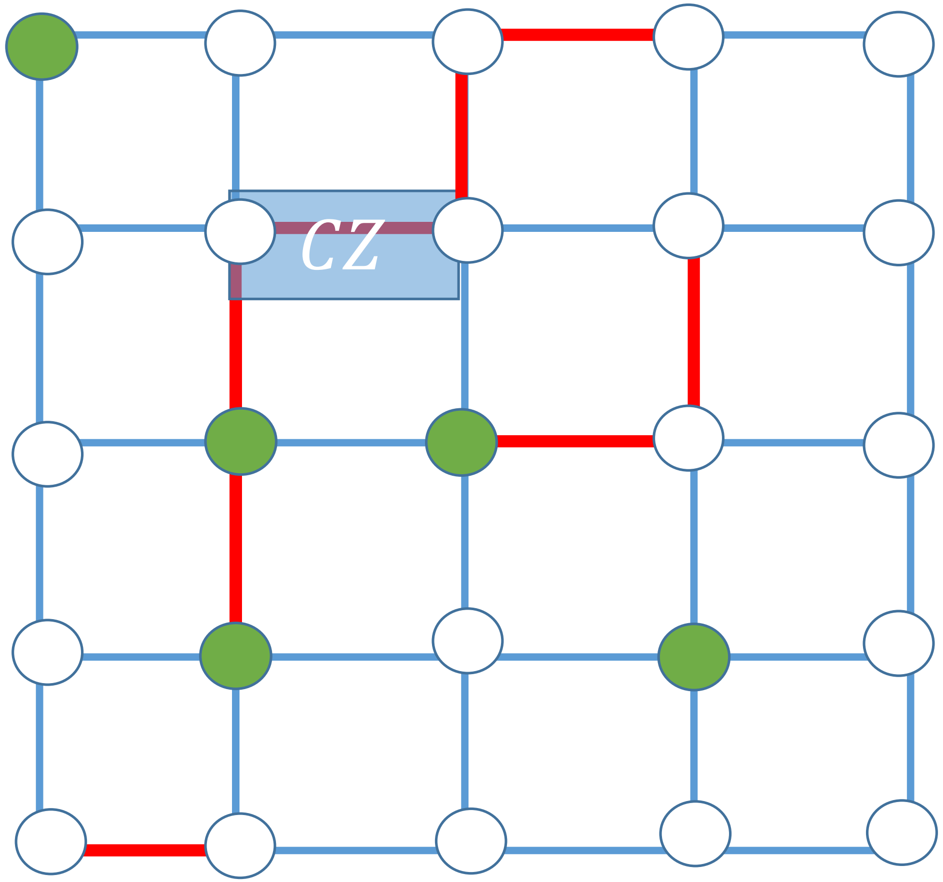
apply a CZ to every pair (i, j) of qubits with $A_{i,j} = 1$

: Edge with $A_{i,j} = 1$

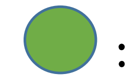
: Vertex with $A_{i,i} = 1$

Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

A constant-depth quantum circuit for 2D HLF

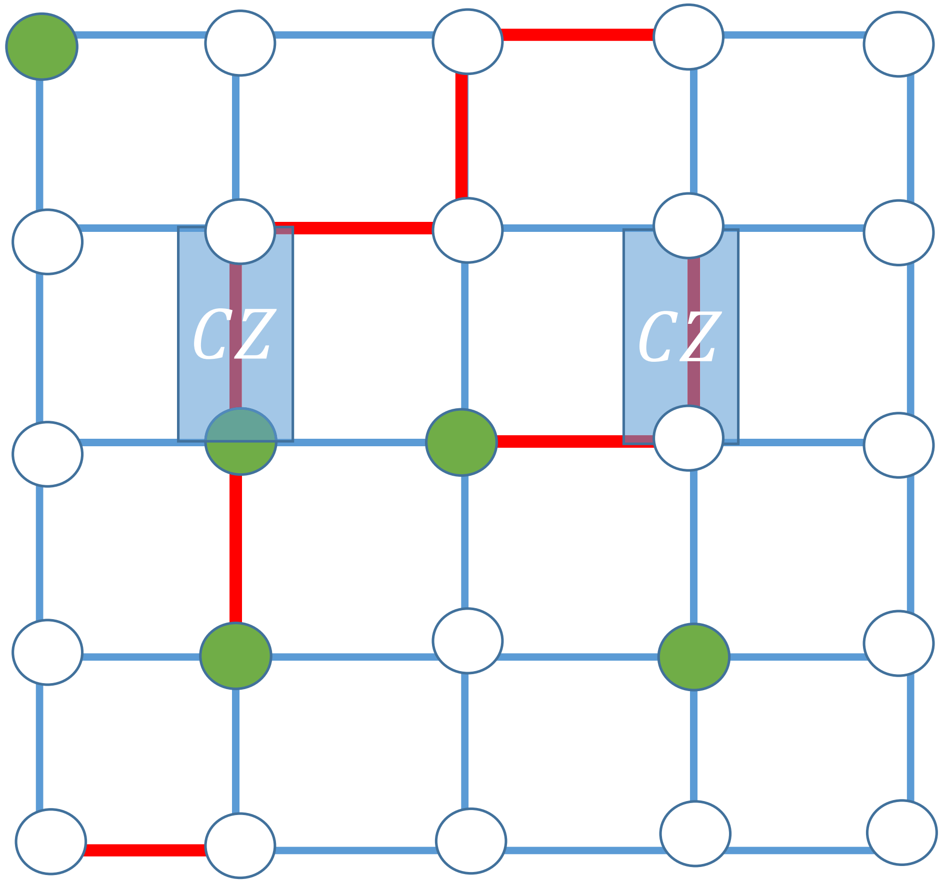


apply a CZ to every pair (i, j) of qubits with $A_{i,j} = 1$



Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

A constant-depth quantum circuit for 2D HLF



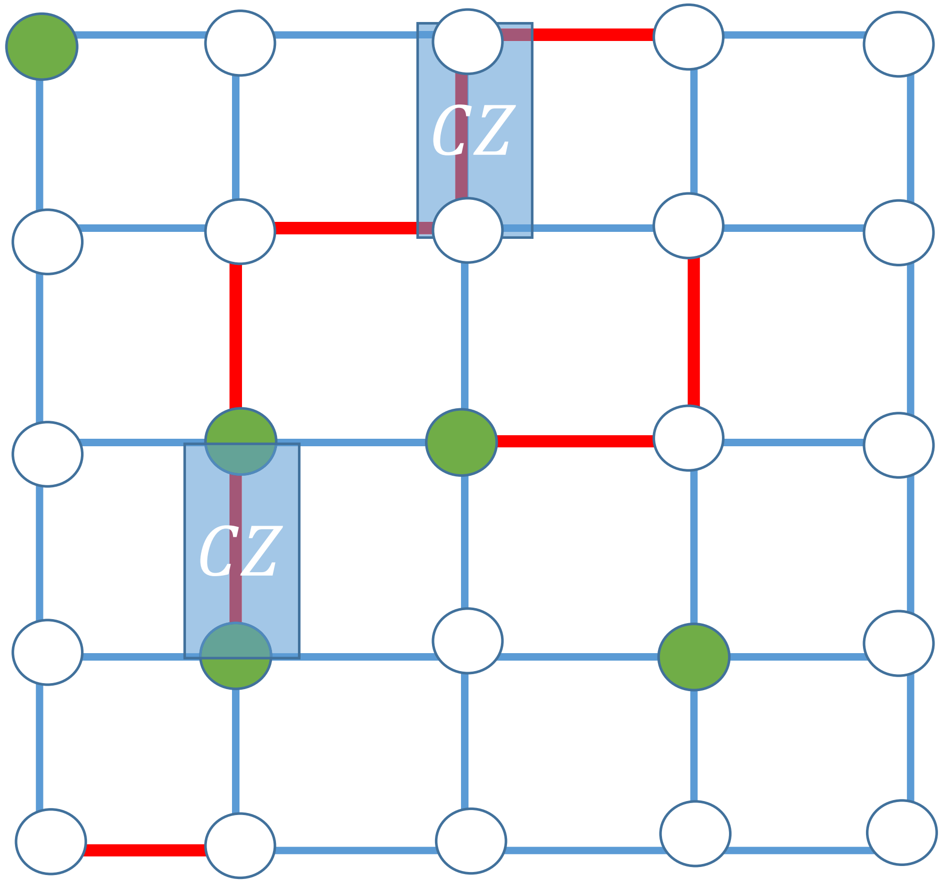
apply a CZ to every pair (i, j) of qubits with $A_{i,j} = 1$

— : Edge with $A_{i,j} = 1$

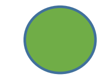
● : Vertex with $A_{i,i} = 1$

Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

A constant-depth quantum circuit for 2D HLF

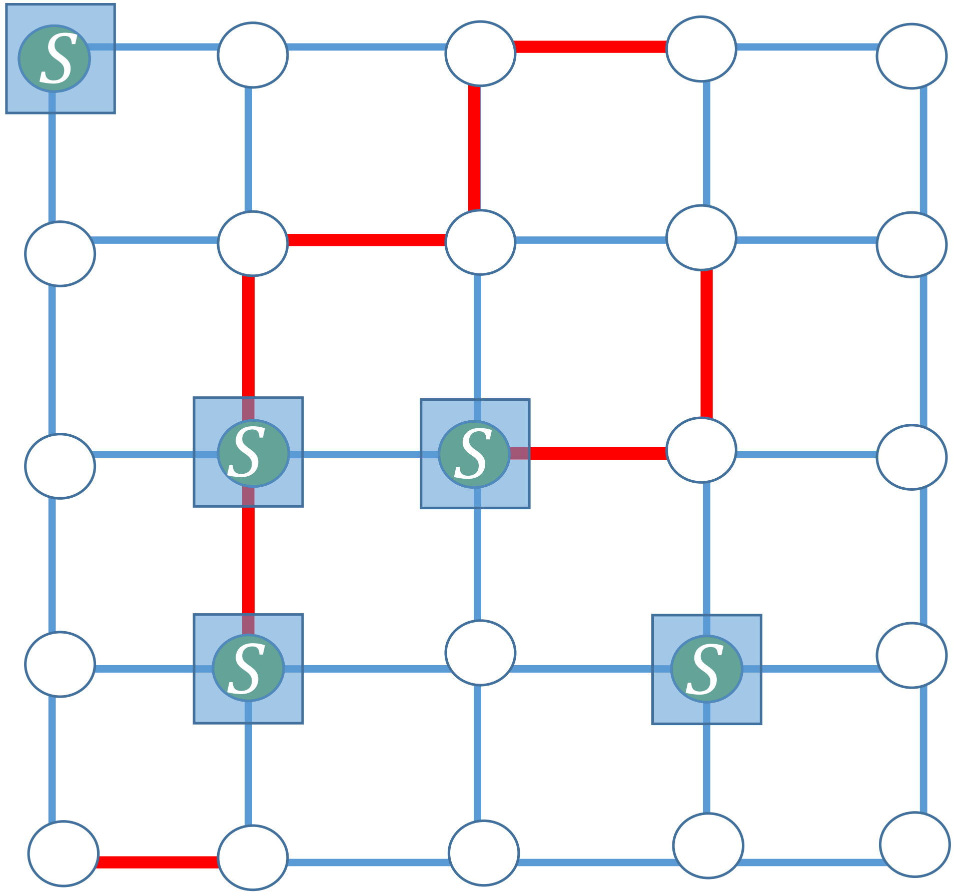


apply a CZ to every pair (i, j) of qubits with $A_{i,j} = 1$

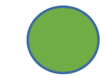


Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

A constant-depth quantum circuit for 2D HLF

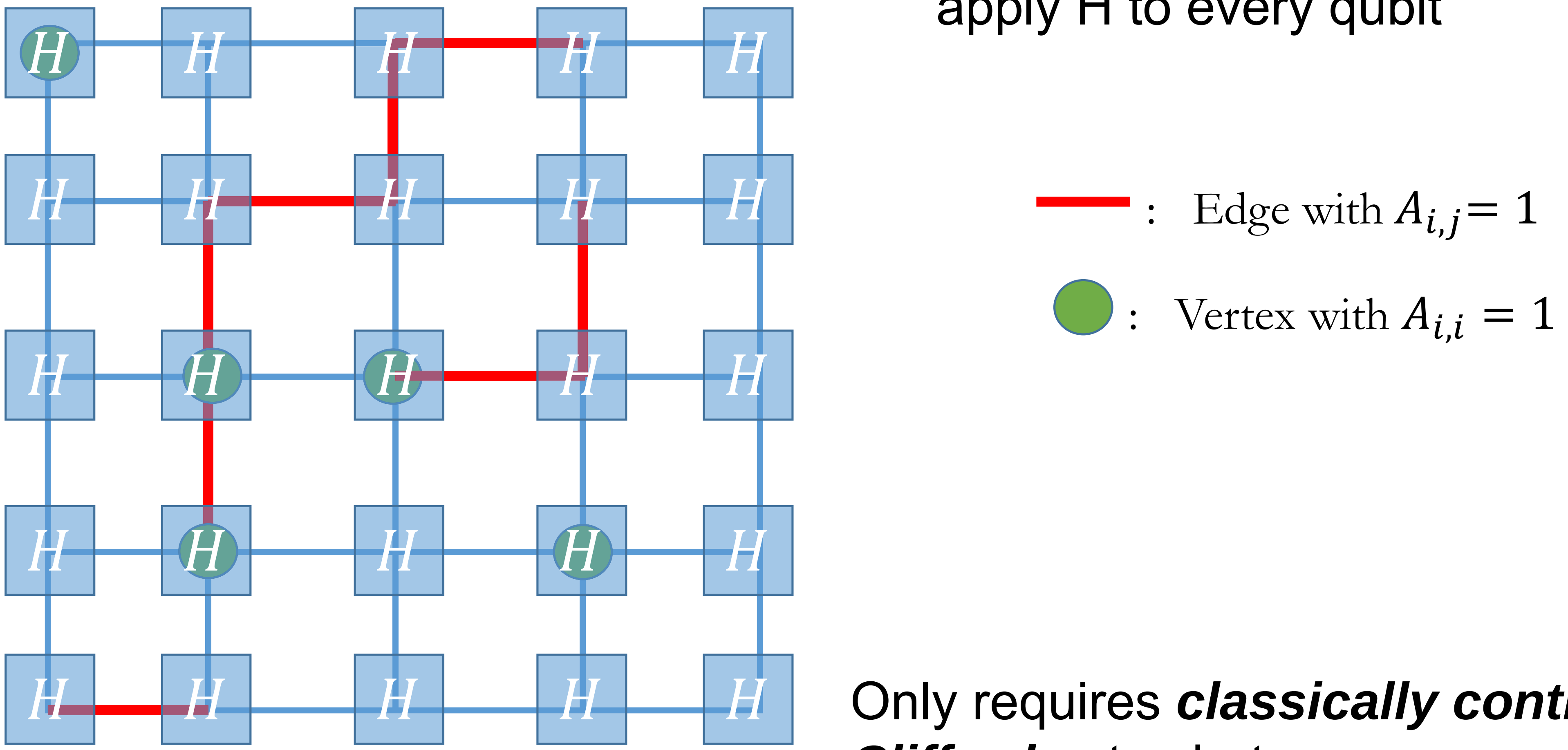


apply S to every qubit i with $A_{i,i} = 1$



Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

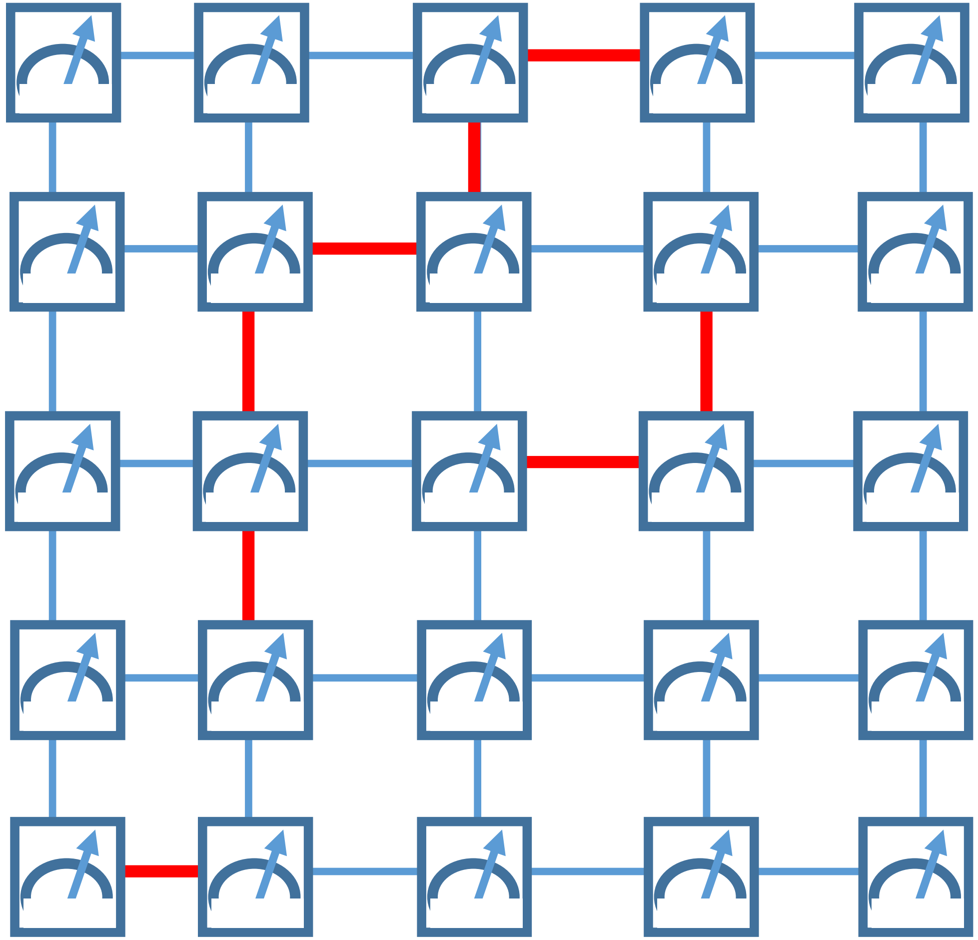
A constant-depth quantum circuit for 2D HLF



apply H to every qubit

Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

A constant-depth quantum circuit for 2D HLF



measure each qubit in the computational basis

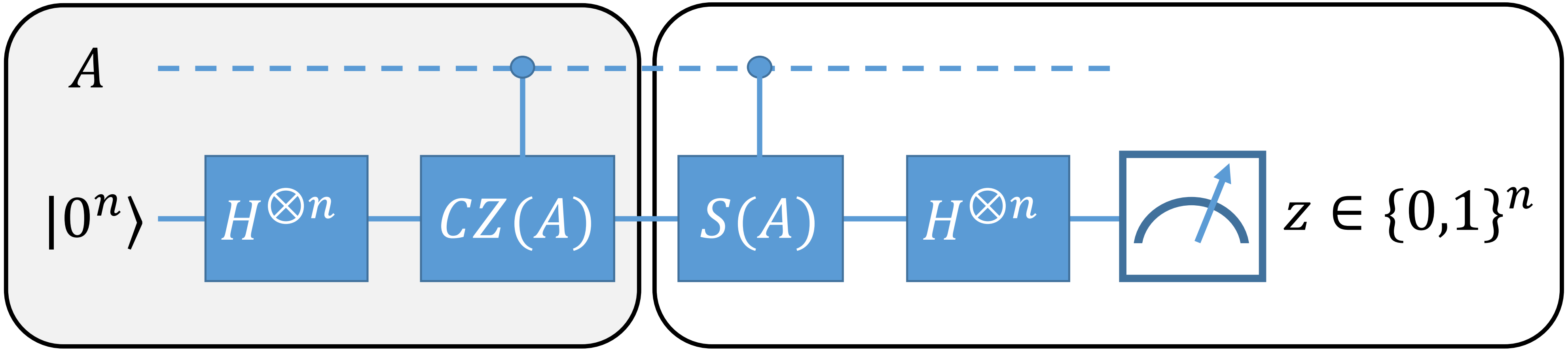
: Edge with $A_{i,j} = 1$

: Vertex with $A_{i,i} = 1$

Only requires ***classically controlled Clifford*** gates between nearest neighbor qubits on a 2D grid.

The HLF circuit and graph states

Quantum algorithm solving the HLF :



Prepare the graph state for a graph with adjacency matrix A

Measure qubit i in the X basis if $A_{i,i} = 0$

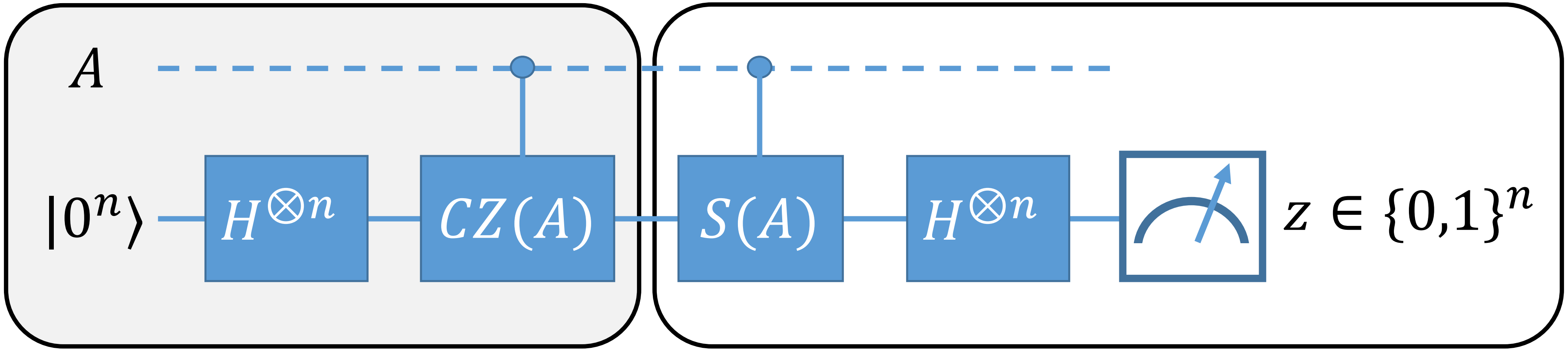
Measure qubit i in the Y basis if $A_{i,i} = 1$

M. Hein, J. Eisert, H.J. Briegel: **Multi-party entanglement in graph states,** Phys. Rev. A 69, 062311 (2004)

R. Raussendorf, D.E. Browne, H.J. Briegel: **Measurement-based quantum computation on cluster states,** Phys. Rev. A 69, 062311 (2004)

The HLF circuit and graph states

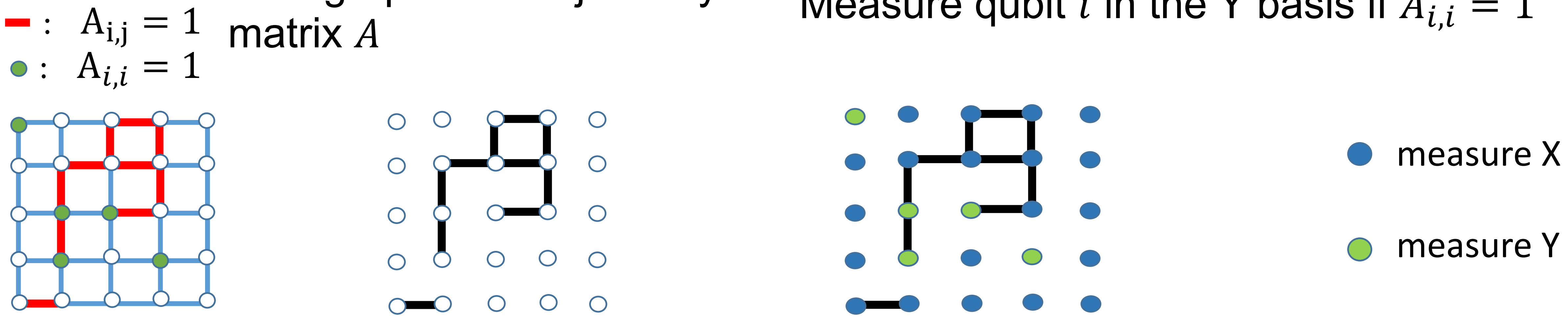
Quantum algorithm solving the HLF :



input:

Prepare the graph state for a graph with adjacency matrix A

Measure qubit i in the X basis if $A_{i,i} = 0$
Measure qubit i in the Y basis if $A_{i,i} = 1$



Remainder of the talk

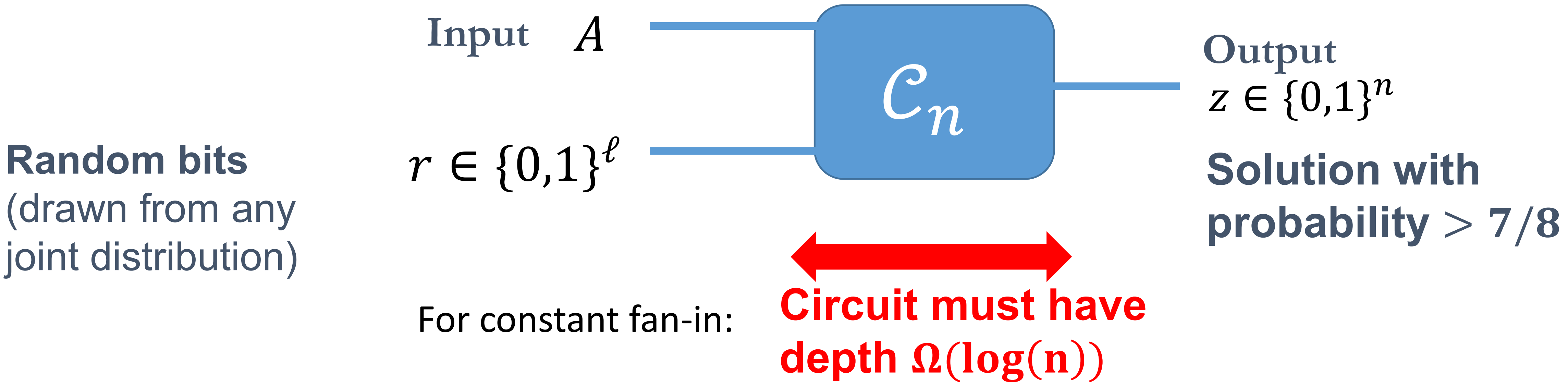
- The hidden linear function (HLF) problem
- A quantum algorithm for the 2D HLF Problem (constant-depth circuit)
- Proof of hardness for constant-depth classical circuits

Main result: A lower bound on classical circuits

Theorem: The following holds for all sufficiently large n.

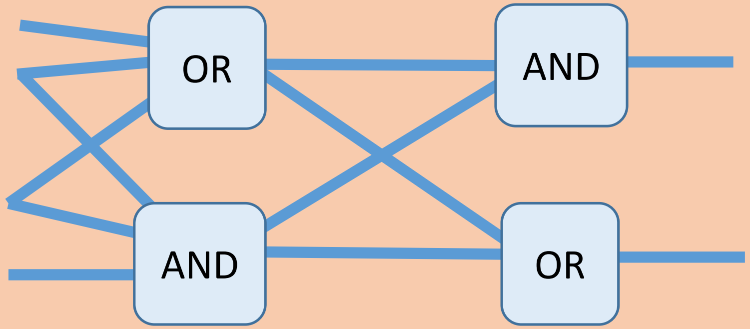
Let $\mathcal{C}_n$ be a classical probabilistic circuit where each gate of $\mathcal{C}_n$ has **fan-in at most K**. Suppose it **solves size-n instances** of the 2D HLF Problem **with probability $> 7/8$**. Then

$$\mathrm{depth}(\mathcal{C}_n) \geq \frac{\log(n)}{16 \log(K)}$$



Proof idea

Locality in shallow classical circuits



versus

Quantum non-locality

John Bell

David Mermin

Each output bit depends only on O(1) input bits.

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

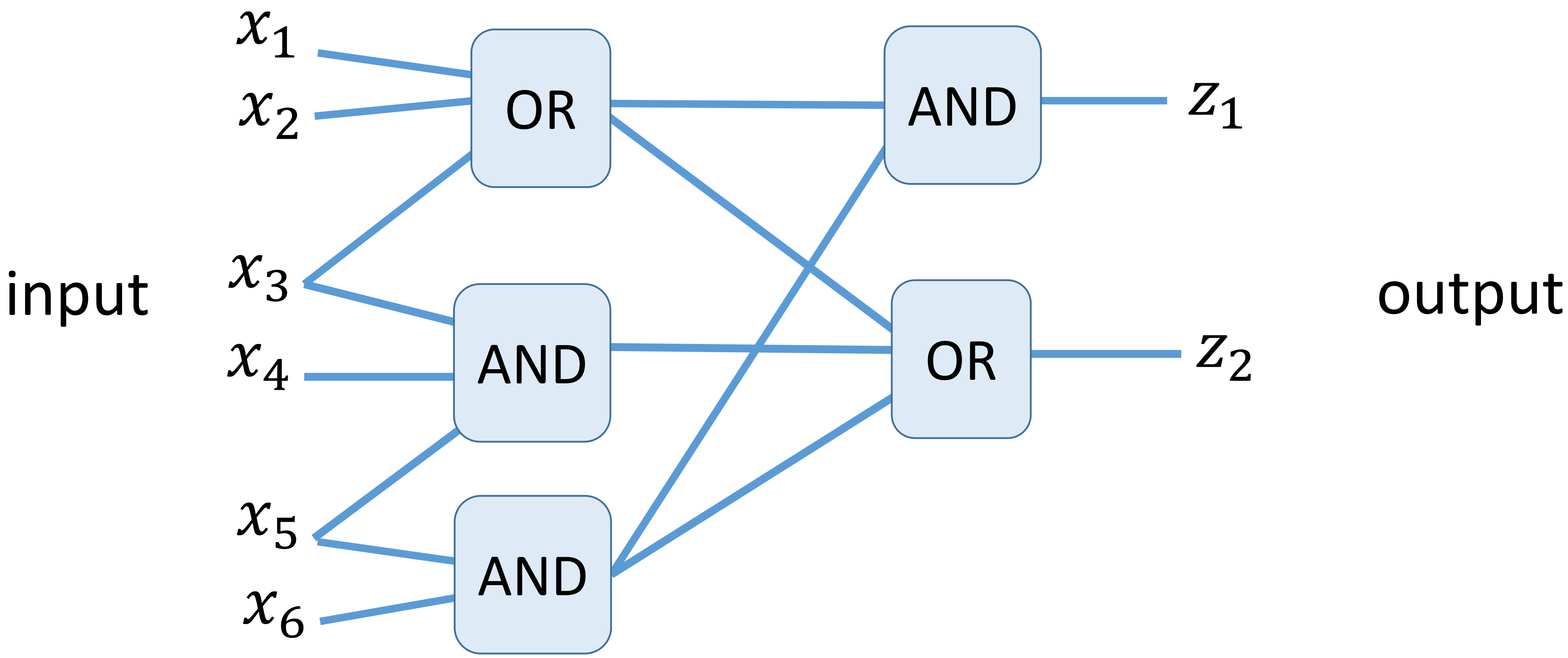
We will show that **quantum nonlocality beats**

(A) Strictly local classical circuits
(local hidden variable models)

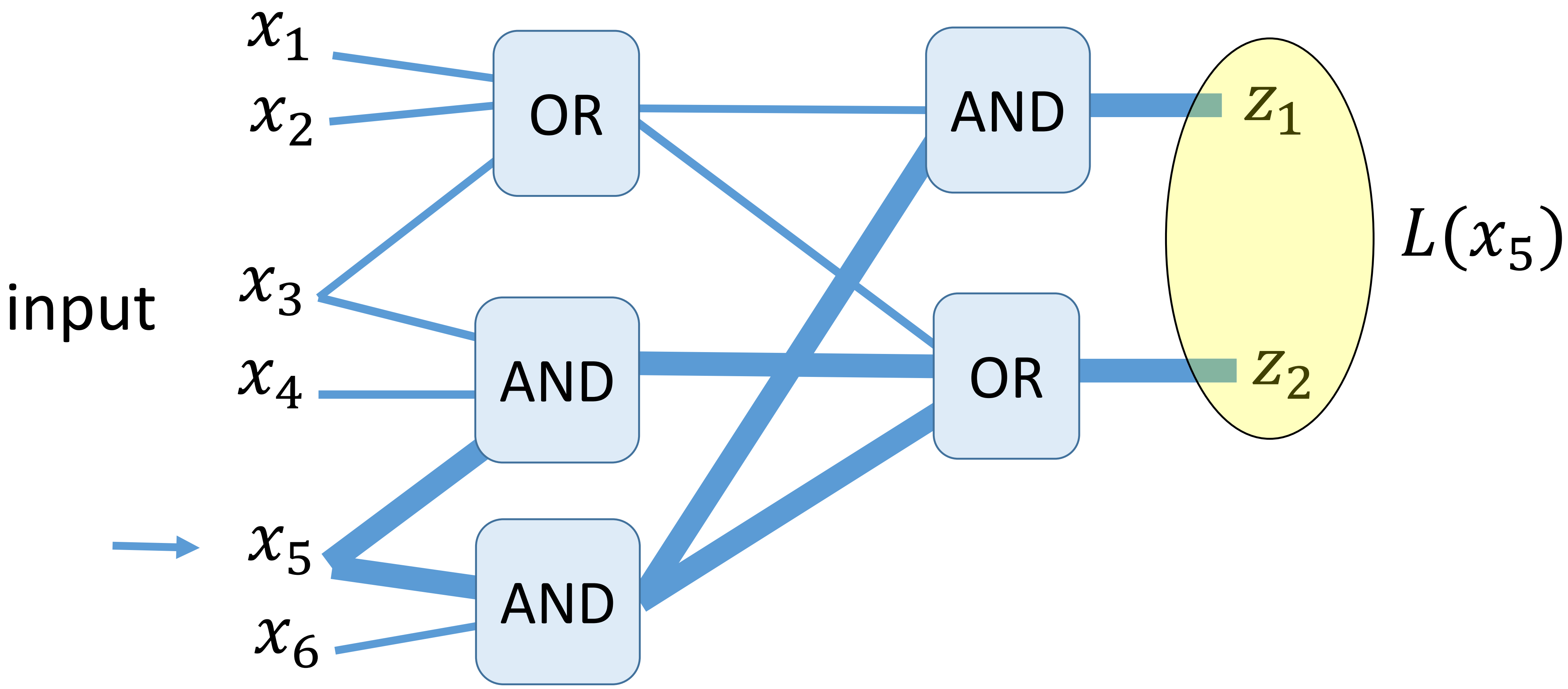
(B) Geometrically local classical circuits in 1D

(C) “Constant-depth local” classical circuits

Locality in classical circuits

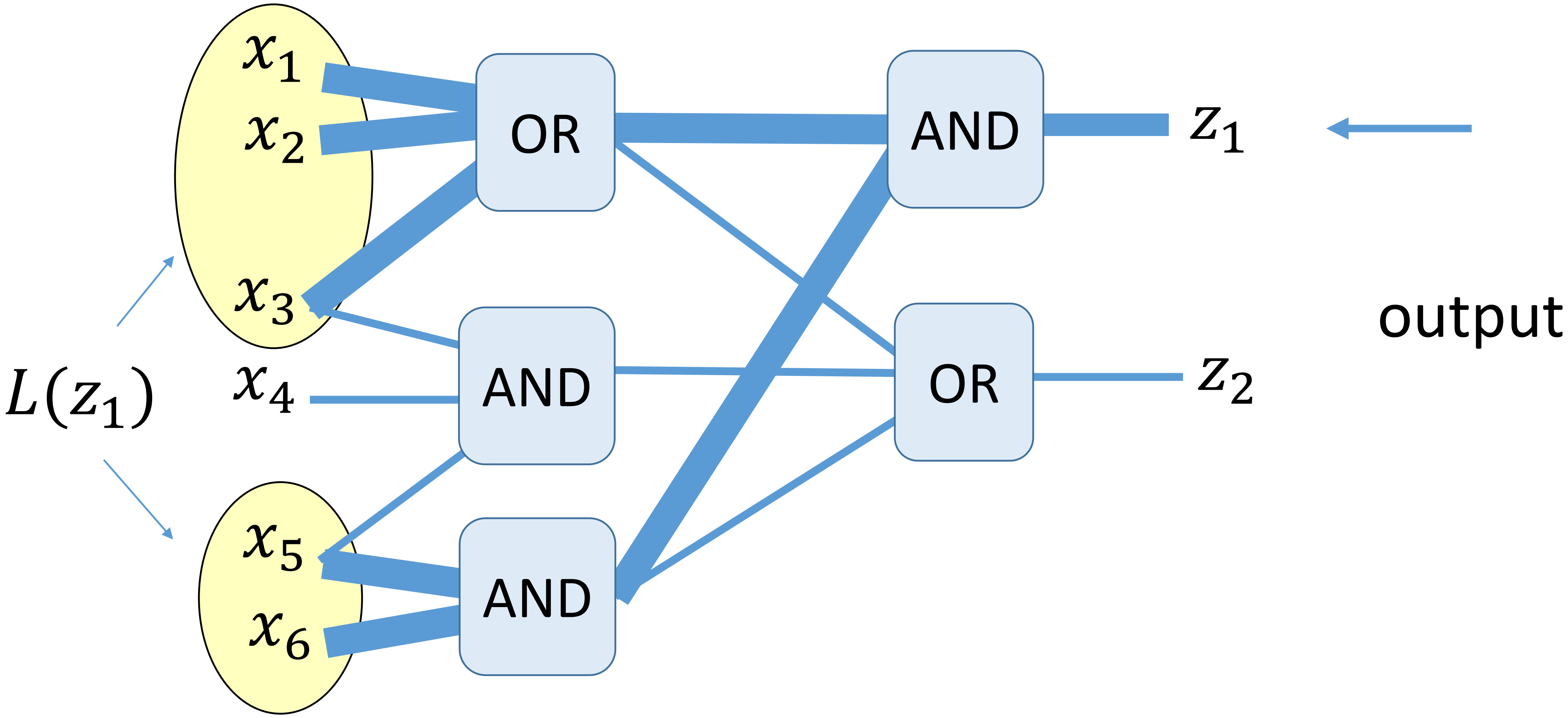


Locality in classical circuits



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

Locality in classical circuits



The (backward) **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.**

We will show that **quantum nonlocality beats**

(A) Strictly local classical circuits
(local hidden variable models)

$L(z_k) = \{x_k\}$ for any output bit z_k

(B) Geometrically local
classical circuits in 1D

$L(x_k) \subset B^D(x_k)$ for any input bit x_k

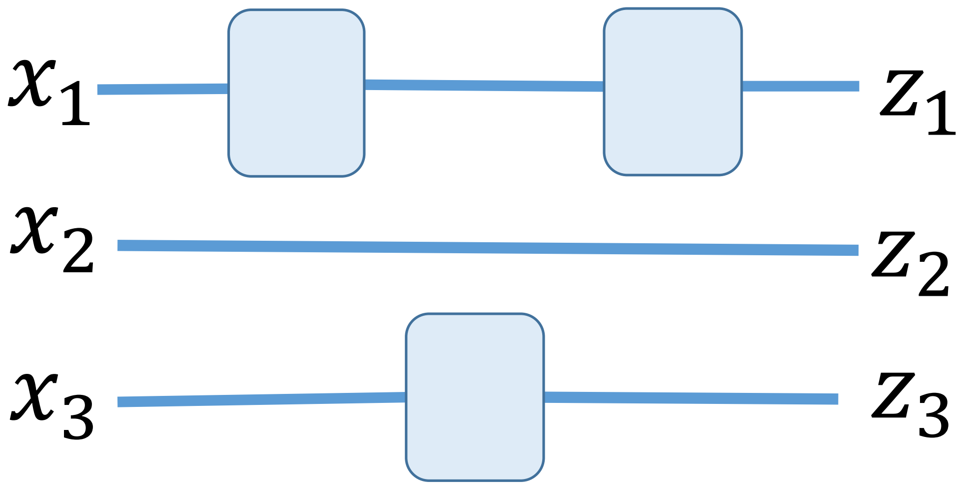
(C) "Constant-depth local"
classical circuits

$|L(z_k)| \leq K^d$ for all output bits z_k

Strictly local classical circuits

A **strictly local circuit** has the property that $L(z_k) = \{x_k\}$ for any output bit z_k

(We assume here that there is a one-to-one correspondence between input- and output bits.)

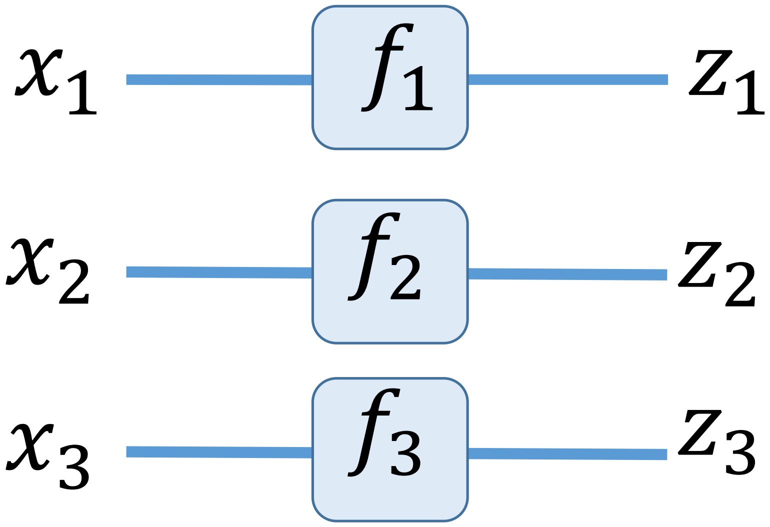


Note: Every output bit z_k is of the form $z_k = f_k(x_k)$

Strictly local classical circuits

A **strictly local circuit** has the property that $L(z_k) = \{x_k\}$ for any output bit z_k

(We assume here that there is a one-to-one correspondence between input- and output bits.)

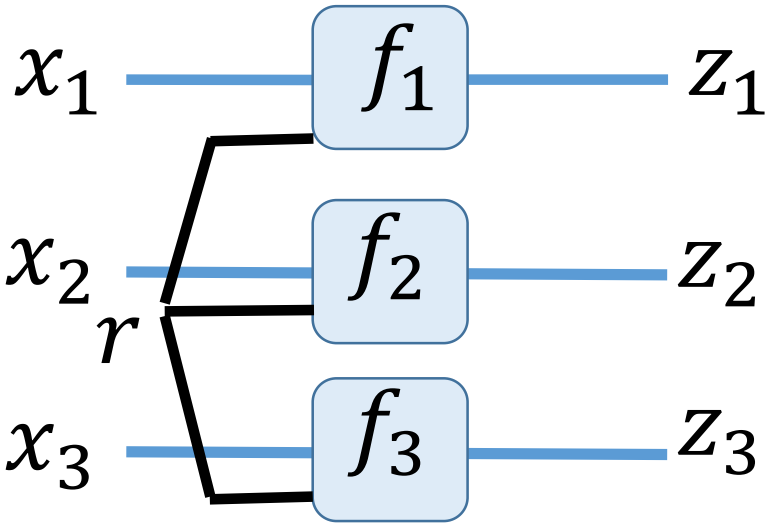


Note: Every output bit z_k is of the form $z_k = f_k(x_k)$

Strictly local classical circuits

A **strictly local circuit** has the property that $L(z_k) = \{x_k\}$ for any output bit z_k

(We assume here that there is a one-to-one correspondence between input- and output bits.)



r = shared random bit string

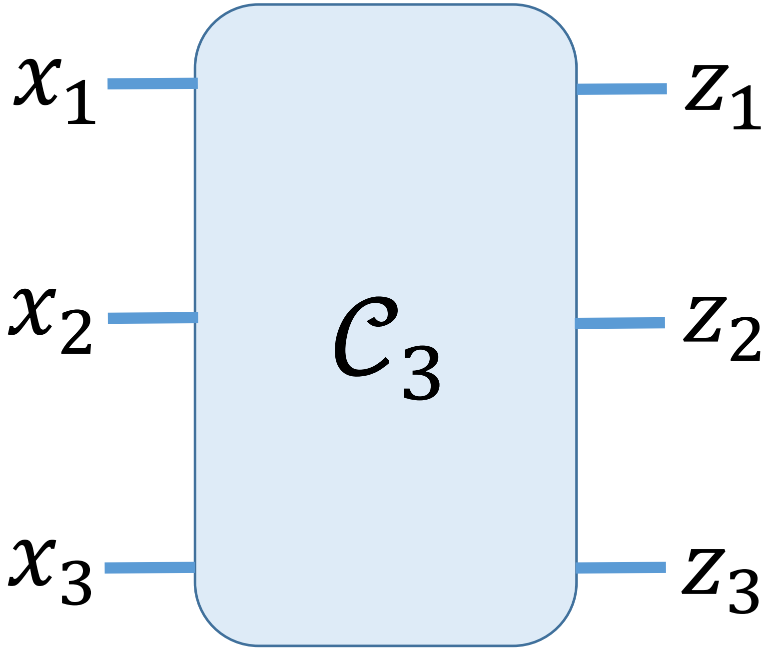
Note: If the circuit is **probabilistic**,

every output bit z_k is of the form $z_k = f_k(x_k, r)$

where r is shared randomness

Circuits and the GHZ relation

[Greenburger et al. 1990][Mermin 1990]



GHZ-relation:

x_1	x_2	x_3	$z_1 z_2 z_3$
0	0	0	1
1	1	0	-1
1	0	1	-1
0	1	1	-1

inputs $x_i \in \{0,1\}$
outputs $z_i \in \{+1,-1\}$

Compact form

$$R(x,z) = i^{x_1+x_2+x_3} z_1 z_2 z_3$$

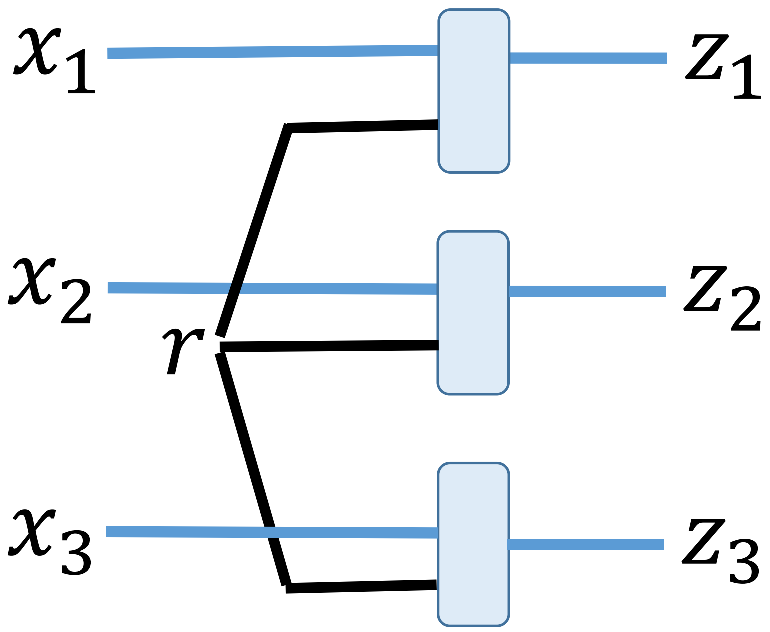
$R(x,z) = 1$
whenever
$x_1 \oplus x_2 \oplus x_3 = 0$

Suppose C obeys the GHZ relation for any input x.

What can be said about its locality ?

Strictly local circuits and the GHZ relation

[Greenburger et al. 1990][Mermin 1990]



r = shared random bit string

GHZ-relation:

x_1	x_2	x_3	$z_1 z_2 z_3$
0	0	0	1
1	1	0	-1
1	0	1	-1
0	1	1	-1

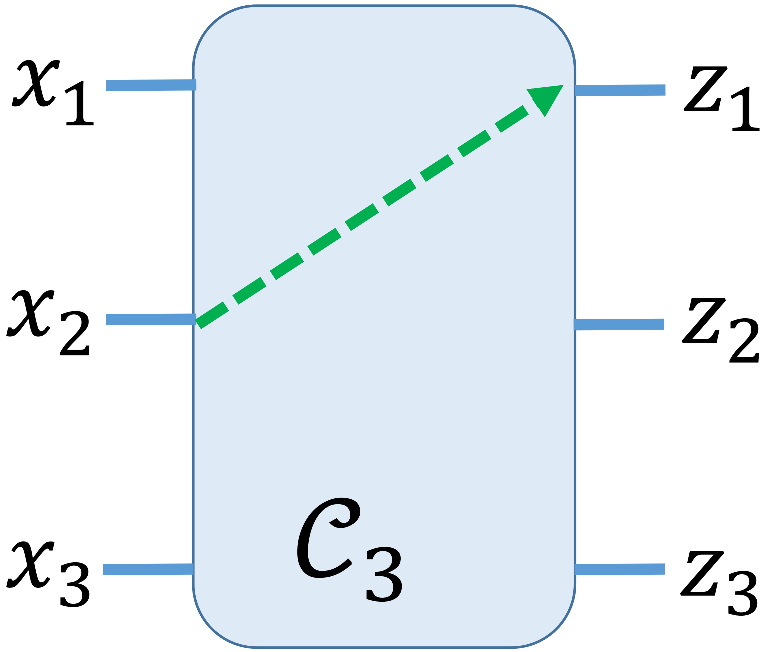
inputs $x_i \in \{0,1\}$
outputs $z_i \in \{+1,-1\}$

Impossible for Local Hidden Variable Models!

reinterpeted as
a **limitation of strictly local circuits:**

Corollary: There is **no strictly local classical circuit** outputting z satisfying the GHZ relation on all inputs x.

Circuits and the GHZ relation

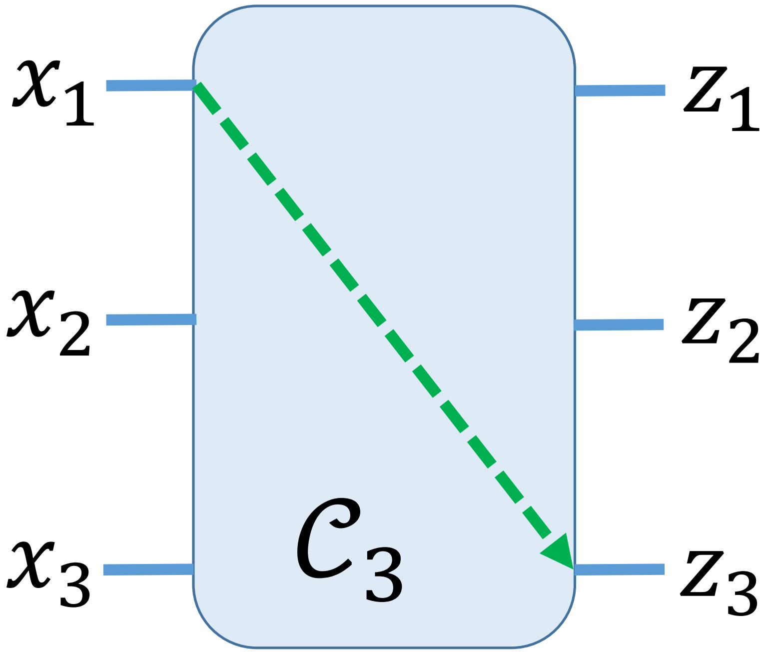


Lemma: Suppose a classical probabilistic circuit satisfies the GHZ relation with probability $> 7/8$.

Then the lightcone $L(x_i)$ of some input bit x_i contains a **distinct output bit** z_k, that is, $i \neq k$

Corollary: There is **no strictly local classical circuit** outputting z satisfying the GHZ relation on all inputs x.

Circuits and the GHZ relation



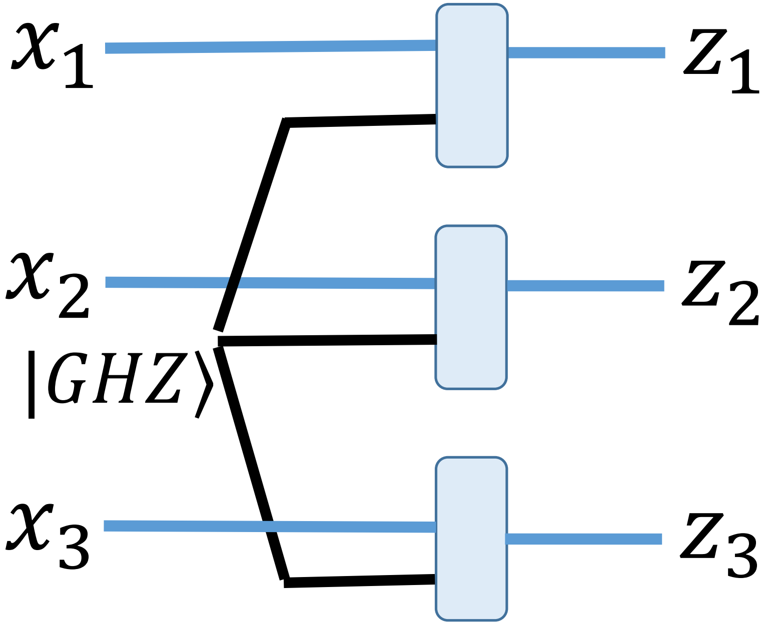
Lemma: Suppose a classical probabilistic circuit satisfies the GHZ relation with probability $> 7/8$.

Then the lightcone $L(x_i)$ of some input bit x_i contains a **distinct output bit** z_k, that is, $i \neq k$

Corollary: There is **no strictly local classical circuit** outputting z satisfying the GHZ relation on all inputs x.

[Greenburger et al. 1990][Mermin 1990]

Satisfying the GHZ relation with quantum non-locality



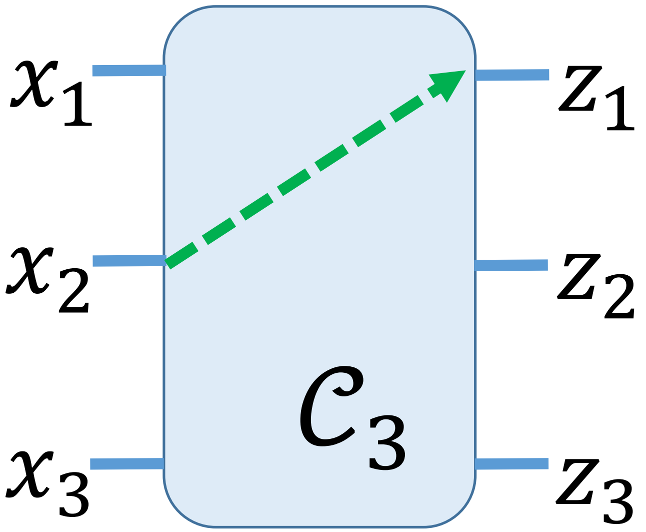
$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

1) Prepare $|\mathrm{GHZ}\rangle$

2) Measure each qubit of $|\mathrm{GHZ}\rangle$ in either the X basis (if $x_j = 0$) or the Y basis (if $x_j = 1$).

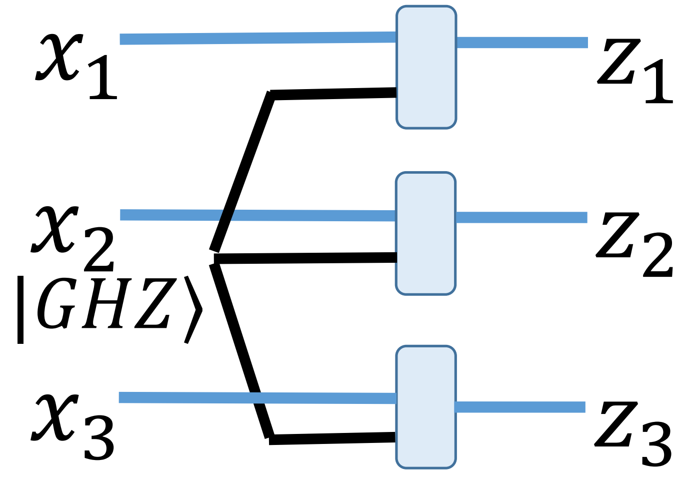
Outcomes $z_j \in \{-1, +1\}$ satisfy the GHZ relation

Quantum nonlocality beats strictly local circuits



GHZ-relation:

x_1	x_2	x_3	$z_1 z_2 z_3$
0	0	0	1
1	1	0	−1
1	0	1	−1
0	1	1	−1



Lemma: Suppose a classical probabilistic circuit satisfies the GHZ relation with probability $> 7/8$.

Then the lightcone $L(x_i)$ of some input bit x_i contains a **distinct output bit** z_k, that is, $i \neq k$

Lemma: This quantum algorithm produces an element z satisfying the GHZ relation with probability 1:

1) Prepare $|\mathrm{GHZ}\rangle$
2) Measure each qubit of $|\mathrm{GHZ}\rangle$ in either the X basis (if $x_j = 0$) or the Y basis (if $x_j = 1$).

We will show that **quantum nonlocality beats**

(A) Strictly local classical circuits
(local hidden variable models)

$L(z_k) = \{x_k\}$ for any output bit z_k

(B) Geometrically local classical circuits in 1D

$L(x_k) \subset B^D(x_k)$ for any input bit x_k

(C) "Constant-depth local" classical circuits

$|L(z_k)| \leq K^d$ for all output bits z_k

Geometrically local circuits

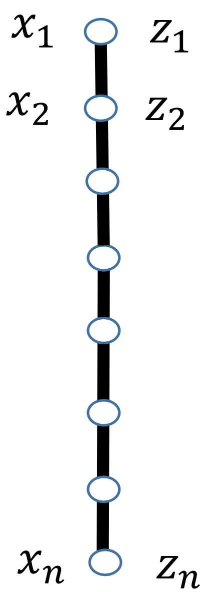
Assumption: Input- and Output bits are associated with vertices of a graph

$\delta(x, y) :=$ Graph distance between x und y

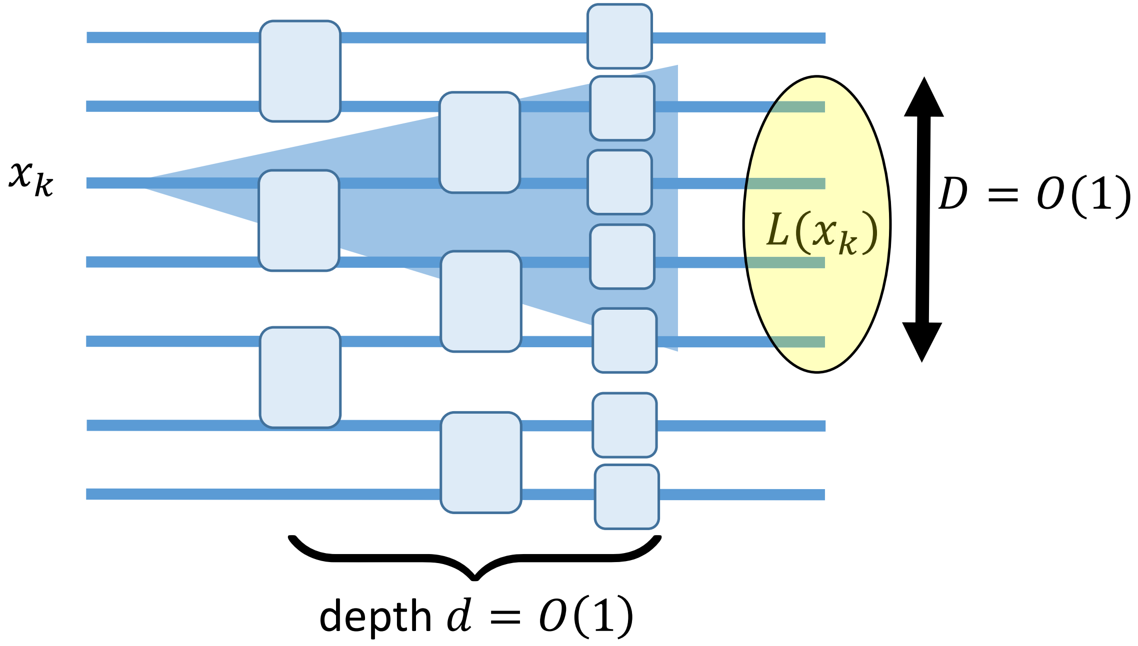
$B^D(x) := \{y \mid \delta(x, y) \leq D\}$

A **geometrically D –local circuit** satisfies $L(x_k) \subset B^D(x_k)$ for any input bit x_k

Example: **geometric locality in 1 dimension**



Shallow circuit
with nearest-neighbor gates in 1D



Quantum nonlocality beats geometrically local circuits

J. Barret, C. Caves, B. Eastin, M. Elliot, S. Pironio: **Modeling Pauli measurements on graph states with nearest-neighbor classical communication**, PRA 75, 012103, 2007.

Simulating the measurement statistics resulting from a graph state cannot be achieved with **limited-distance classical communication** between nodes

Here we reinterpret this result as a **limitation of geometrically local circuits.**

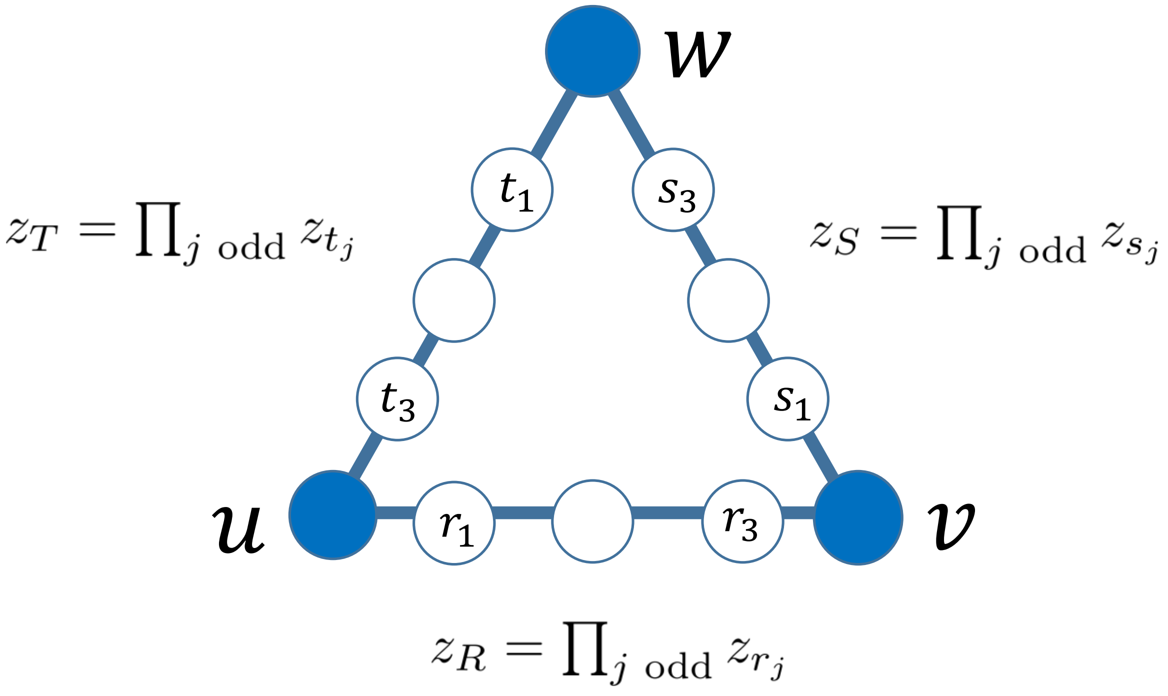
GHZ generalized: the cycle relation

[Barrett et al. 2007]

n even. Consider the n-cycle and u, v, w on the even sublattice

"Input": $x = (x_u, x_v, x_w) \in \{0,1\}^3$

"Output": $z \in \{-1,1\}^{|V|} = \{-1,1\}^n$



$$R(x, z) = i^{x_u + x_v + x_w} z_u z_v z_w z_R^{x_u} z_S^{x_v} z_T^{x_w}$$

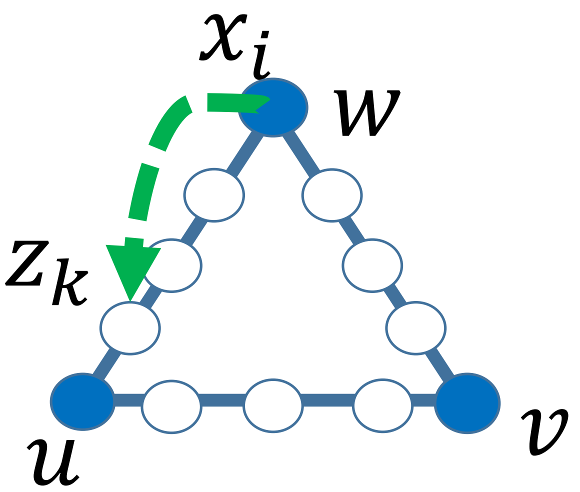
Define the "cycle relation": $R(x, z) = 1$ whenever $x_u \oplus x_v \oplus x_w = 0$

Fact: Satisfying the cycle relation (classically) requires communication.

Fact: The cycle relation is satisfied when (appropriately) measuring the cycle graph state.

(Geometrically local) circuits and the cycle relation

Lemma: Suppose a classical circuit satisfies the cycle relation with probability $> 7/8$ for each input. Then the lightcone $L(x_i)$ of some input bit x_i , $i \in \{u, v, w\}$ contains a **distant output bit** z_k.

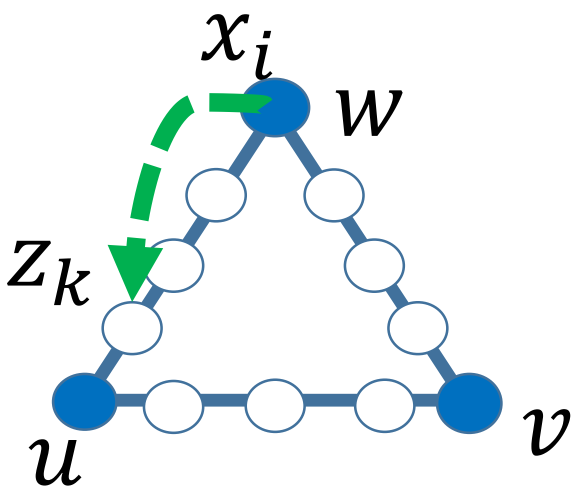


More precisely: $\delta(x_i, z_k) > D,$ $D = \min\{\delta(u,v), \delta(v,w), \delta(w,v)\}/2$

Corollary: There is **no geometrically *D*-local (probabilistic) classical circuit** giving an output z satisfying the cycle relation $\mathrm{R}(x,z) = 1$ for all inputs $x \in \{0,1\}^3$.

(Geometrically local) circuits and the cycle relation

Lemma: Suppose a classical circuit satisfies the cycle relation with probability $> 7/8$ for each input. Then the lightcone $L(x_i)$ of some input bit x_i , $i \in \{u, v, w\}$ contains a **distant output bit** z_k.



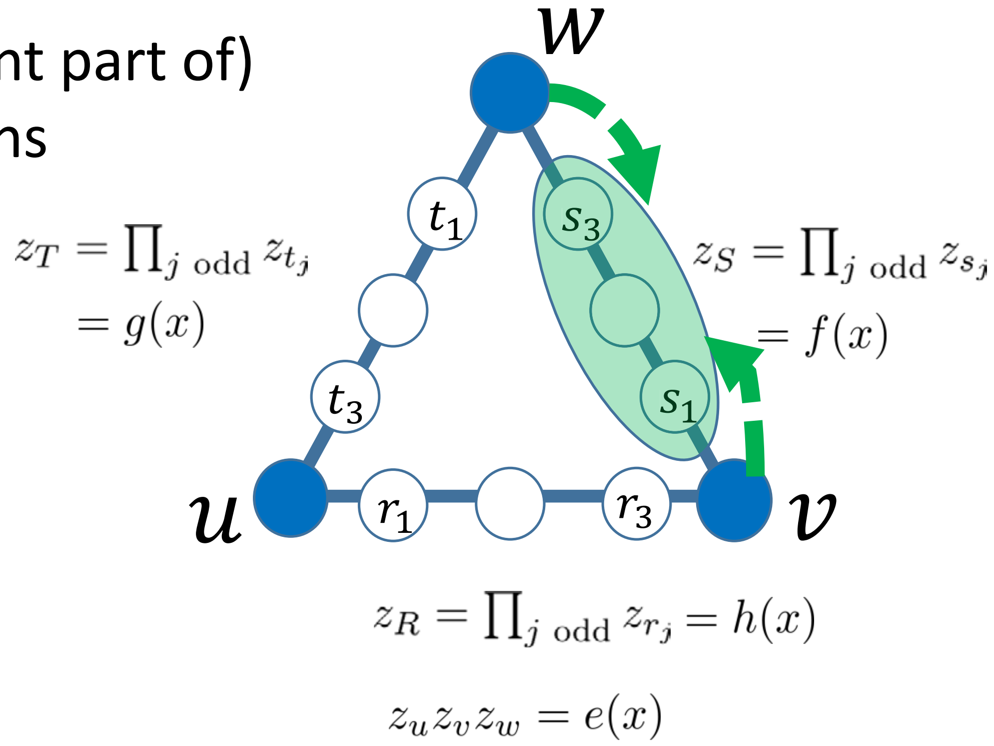
More precisely: $\delta(x_i, z_k) > D,$ $D = \min\{\delta(u,v), \delta(v,w), \delta(w,v)\}/2$

Proof idea: Assume this is not the case. Then the (relevant part of) the output of the circuit can be described by four functions

$$e, f, g, h : \{0,1\}^3 \to \{-1,1\}$$

such that

$f(x)$	does not depend on	x_u
$g(x)$	does not depend on	x_v
$h(x)$	does not depend on	x_w



Satisfying the cycle relation with quantum non-locality

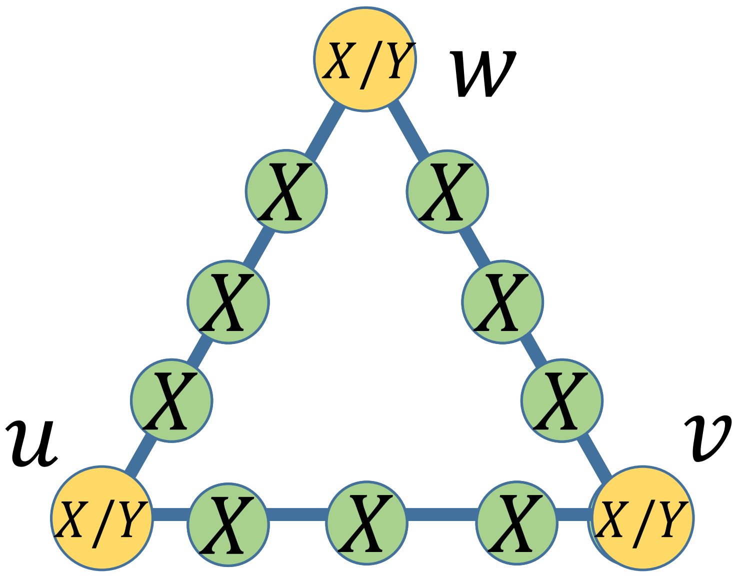
[Barrett et al. 2007]

1) Prepare the graph state associated with the cyle $|\Phi_n\rangle = \left(\prod_{j=1}^{n} CZ_{j,j+1}\right) H^{\otimes n}|0^n\rangle$

2) For each qubit $j \in \{u, v, w\}$ measure $\begin{cases} X & \text{if } x_j = 0 \\ Y & \text{if } x_j = 1 \end{cases}$

for any other qubit measure X

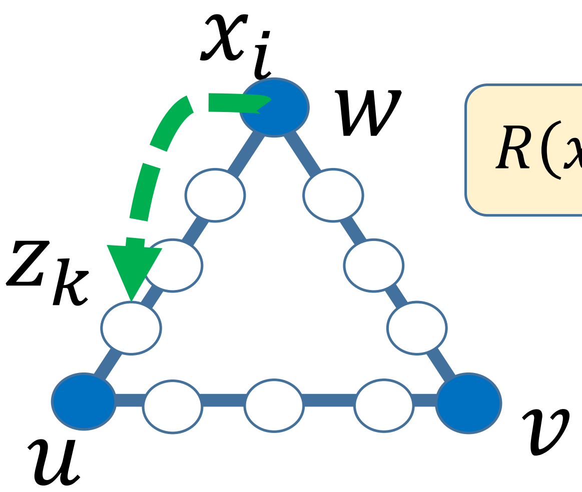
Call z_j the measurement outcome for qubit j.



Fact: This quantum algorithm produces outcomes z satisfying the cycle relation $R(x, z) = 1$

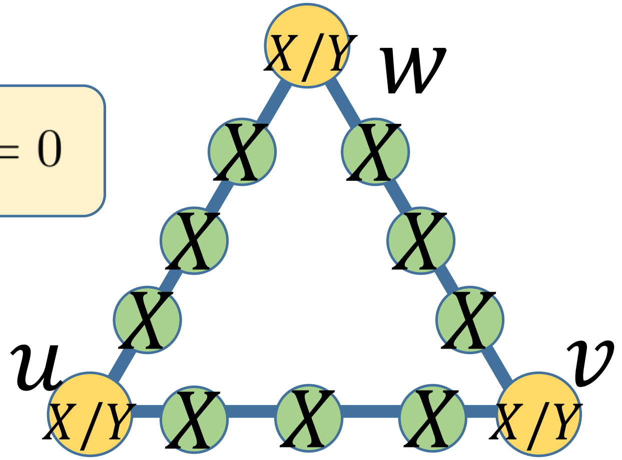
Intuition: the reduced state of uvw (after all green qubits are measured) is the GHZ state modulo a Pauli correction that depends on the measurement outcomes.

Quantum nonlocality beats geometrically local circuits



Cycle-relation

$R(x,z) = 1$ whenever $x_u \oplus x_v \oplus x_w = 0$



Lemma: Suppose a classical circuit satisfies the cycle relation with probability $> 7/8$ for each input.

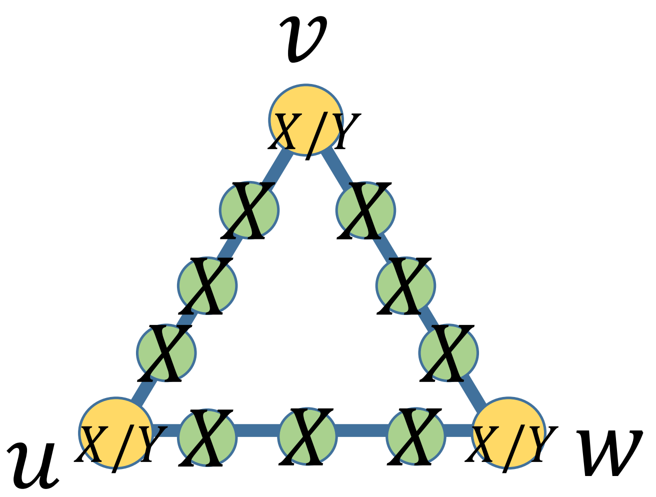
Then the lightcone $L(x_i)$ of some input bit x_i contains a **distant output bit** z_k.

Lemma: This quantum algorithm produces an element z satisfying the cycle relation with probability 1:

1) Prepare the cycle graph state
2) Measure each qubit

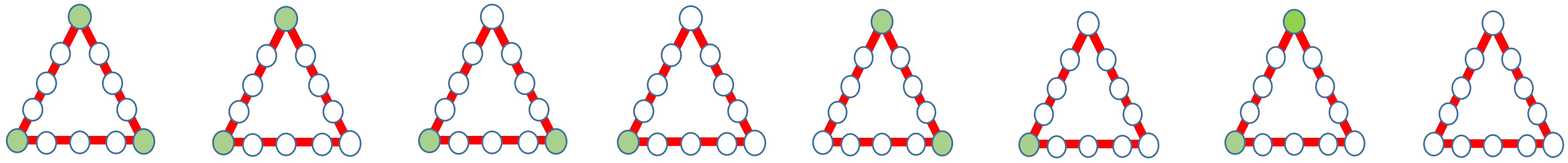
- in the Y basis if $j \in \{u, v, w\}$ and $x_j = 1$
- in the X basis otherwise

The cycle relation and the HLF problem associated with a cycle



The measurement pattern of the quantum algorithm is identical to that used when solving one of 8 special instances of the HLF

(A=adjacency matrix of cycle graph)



In fact: **Satisfying the cycle relation on input** $x = (x_u, x_v, x_w) \in \{0,1\}^3$ **amounts to solving the associated HLF** with $A_{j,j} = x_j$ for $j \in \{u, v, w\}$

We will show that **quantum nonlocality beats**

(A) Strictly local classical circuits
(local hidden variable models)

$L(z_k) = \{x_k\}$ for any output bit z_k

(B) Geometrically local
classical circuits in 1D

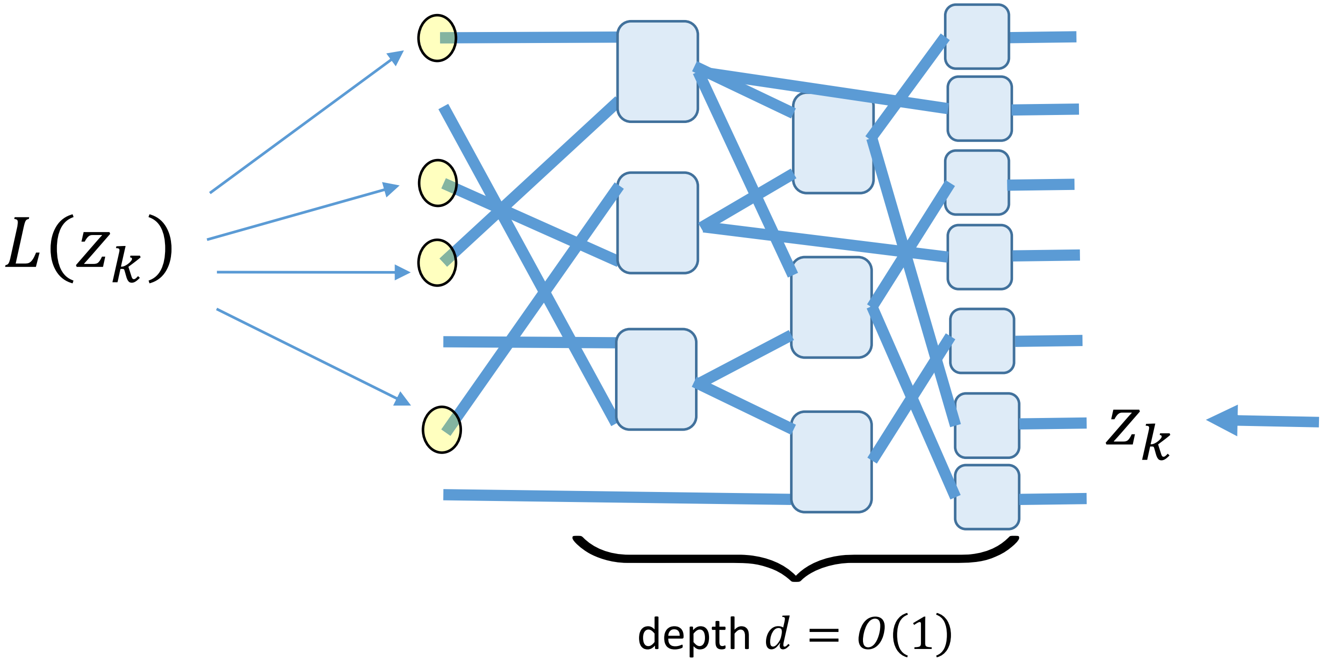
$L(x_k) \subset B^D(x_k)$ for any input bit x_k

(C) "Constant-depth local"
classical circuits

$|L(z_k)| \leq K^d$ for all output bits z_k

Locality in constant-depth classical circuits

general shallow circuit

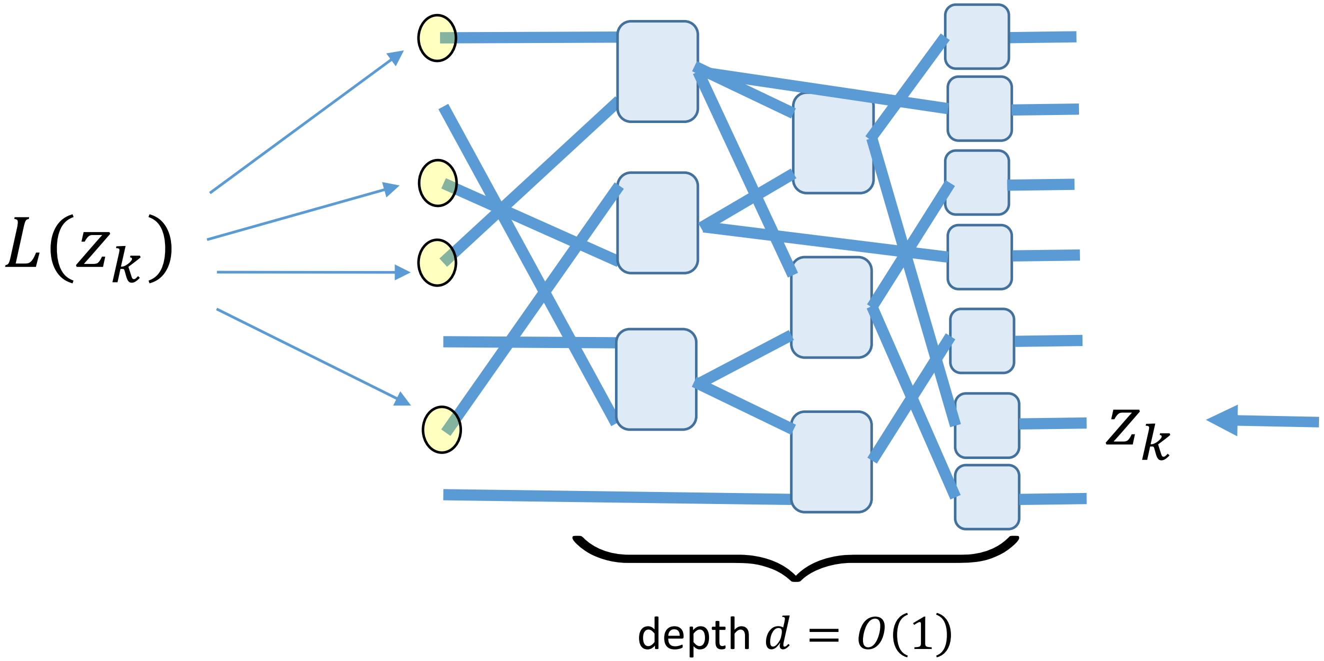


Locality in constant-depth classical circuits

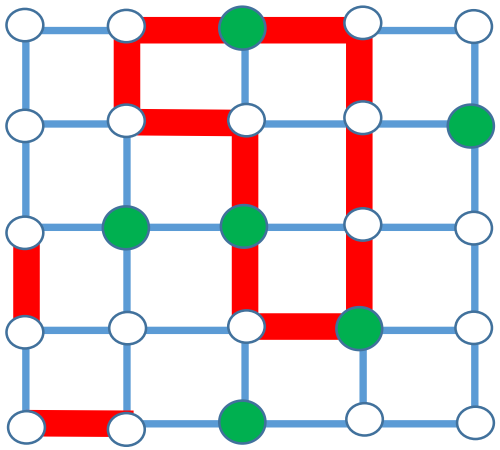
"Constant-depth locality"

$|L(z_k)| \leq K^d$ for all output bits z_k

Example: Any circuit whose depth is d whose gates have fan-in $\leq K$.



Classical circuits solving the 2D HLF



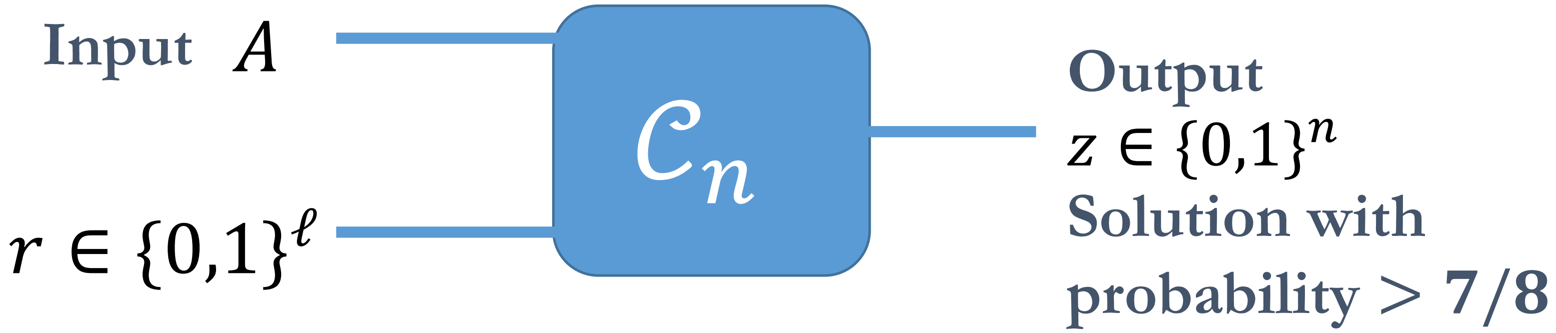
n sites

$A_{i,j} = 0$ unless (i, j) are nearest neighbors

i —— j $A_{i.j} = 1$

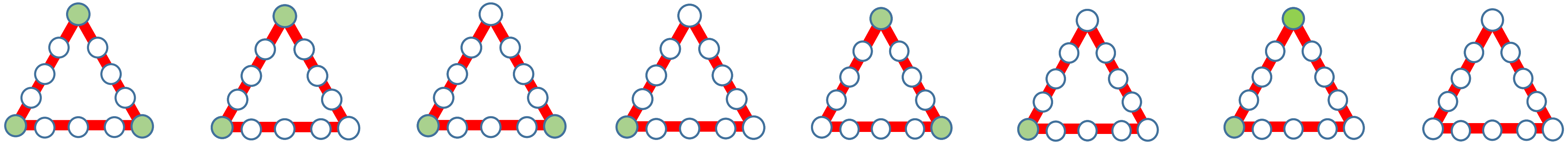
i ● $A_{i.i} = 1$

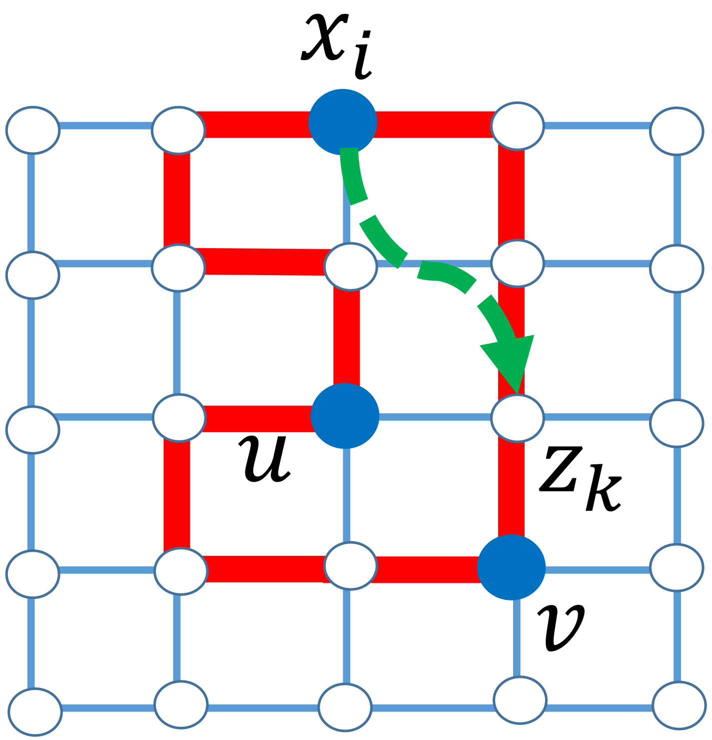
Recall:
The 2D HLF problem is the set of instances where the matrix A is the adjacency matrix of a subgraph of the $\sqrt{n} \times \sqrt{n}$ grid graph.



Suppose C solves every instance of the 2D HLF problem with probability >7/8. What can be said about its locality ?

Cycle relations contained in the 2D HLF





i —— j $\quad A_{i.j} = 1$

i ● $\quad A_{i.i} = x_i$

Choose A to describe the adjacency matrix of a cycle (subgraph of the gridgraph)

Choose $A_{i,i} = x_i$ for $i \in \{u, v, w\}$ to specify X or Y measurement and $A_{j,j} = 0$ for all other j

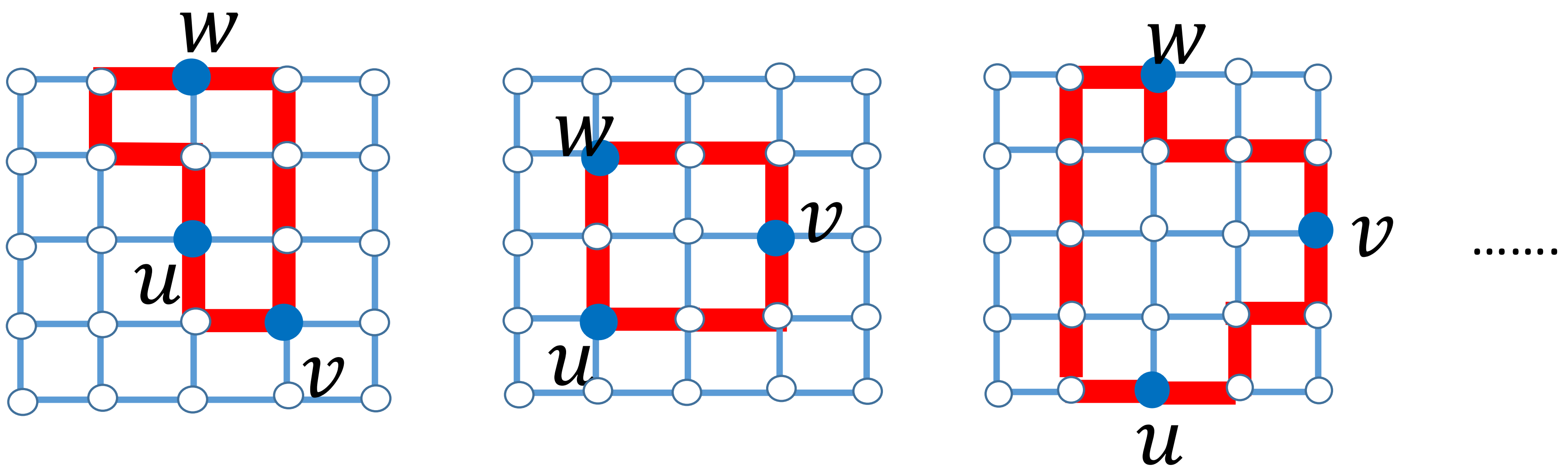
We infer (from Barrett et al.) a cycle relation satisfied by input/output:

Lemma

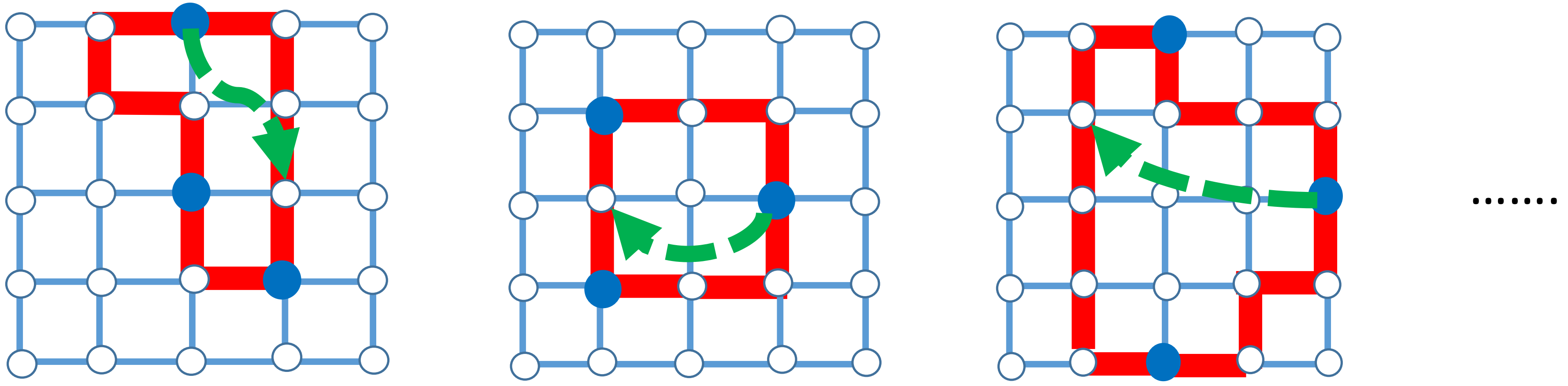
$\Rightarrow$ There is an input bit x_i such that $L(x_i)$ contains a distant output bit z_k

Many locality constraints on 2D HLF-solving circuits

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



…and thus satisfies constraints on the lightcones of certain input bits



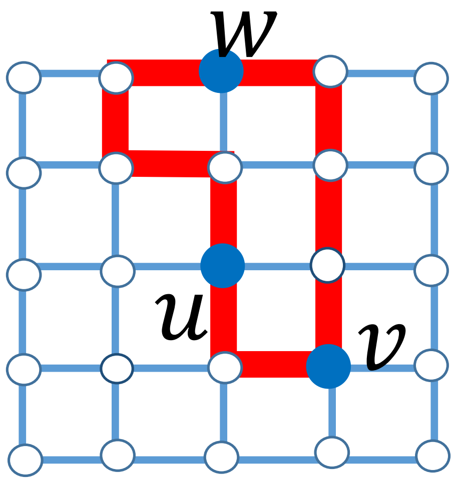
We show that constant-depth locality is incompatible with these constraints.

$|L(z_k)| \leq K^d$ for all output bits z_k

Quantum non-locality beats "constant-depth local" circuits

Suppose a classical circuit has

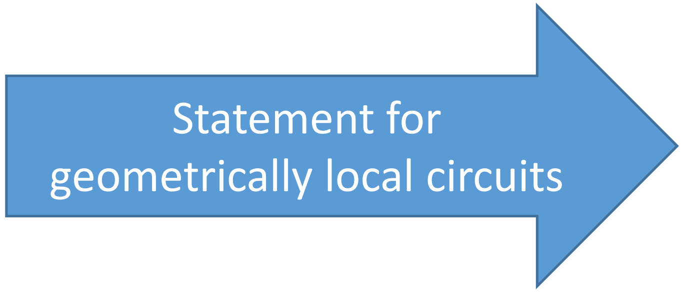
fan-in $\leq K$ and depth $< \frac{\log(n)}{16 \log(K)}$.



Lemma: There are vertices u, v, w on the even sublattice and a cycle Γ passing through them such that
the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v, w\}$
do not contain any distant output bits $z_j \in \Gamma$.

Corollary (Main result): Any classical circuit which solves the 2D HLF problem with probability $> \frac{7}{8}$ must have depth $> \frac{\log(n)}{16 \log(K)}$.

Proof of Corollary: Suppose the depth is smaller. Let Γ be as in the Lemma.



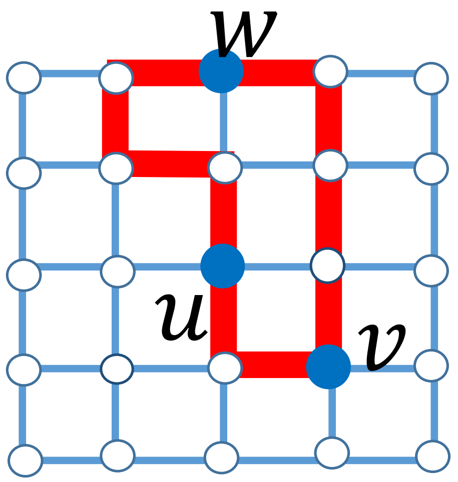
The circuit does not w.h.p solve all instances of 2D HLF problem where A is the adjacency matrix of Γ.

Contradiction!

Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

fan-in $\leq K$ and depth $< \frac{\log(n)}{16 \log(K)}$.



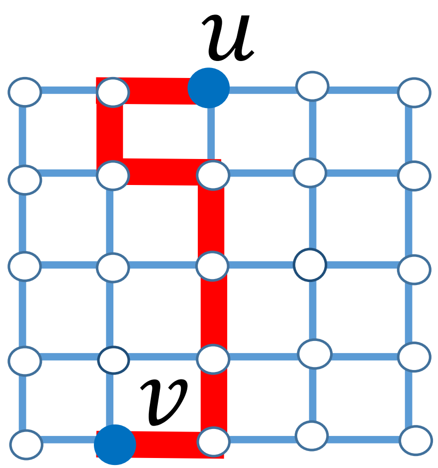
Lemma: There are vertices u, v, w on the even sublattice and a cycle Γ passing through them such that
the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v, w\}$
do not contain any distant output bits $z_j \in \Gamma$.

Proof: Based on a probabilistic argument.

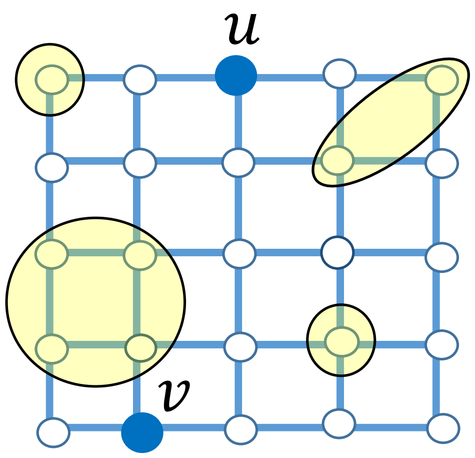
Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

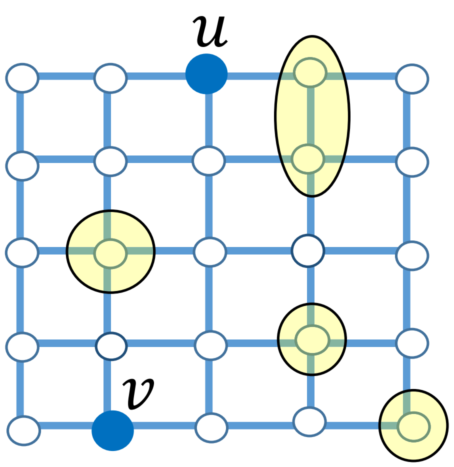
fan-out $\leq K$ and depth $< \frac{\log(n)}{16\log(K)}$.



Lemma: There are vertices u, v on the even sublattice and a ***path*** Γ connecting them such that
the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v\}$
do not contain any distant output bits $z_j \in \Gamma$.



$L(x_u)$



$L(x_v)$

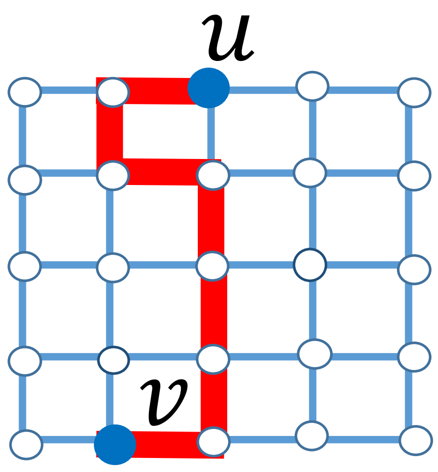
$|L(x_u)| \leq K^d$ and $|L(x_v)| \leq K^d$

(bounded fan-out)

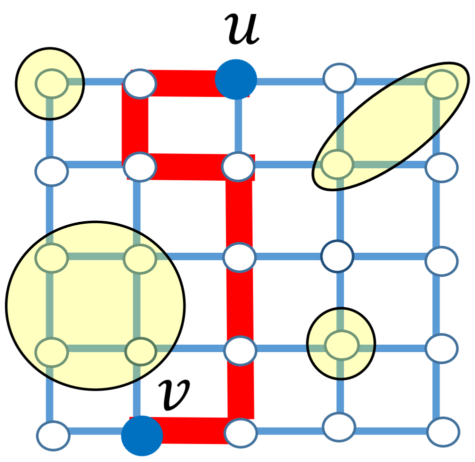
Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

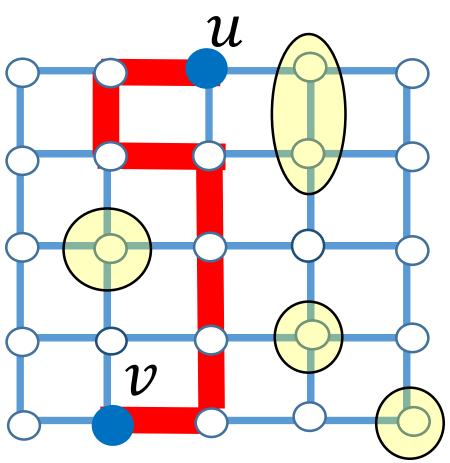
fan-out $\leq K$ and depth $< \frac{\log(n)}{16\log(K)}$.



Lemma: There are vertices u, v on the even sublattice and a **path Γ** connecting them such that the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v\}$ **do not contain any distant output bits $z_j \in \Gamma$.**



$L(x_u)$



$L(x_v)$

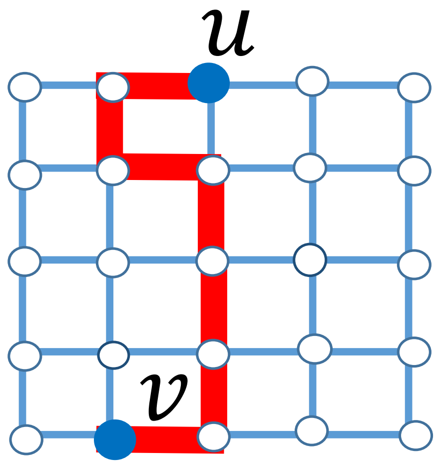
Example of a "good" **path Γ**:

no distant output bits in lightcones on path

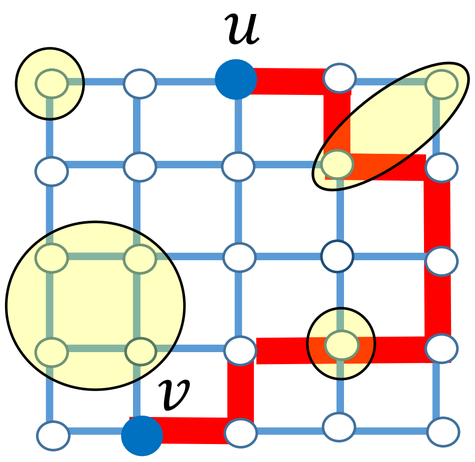
Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

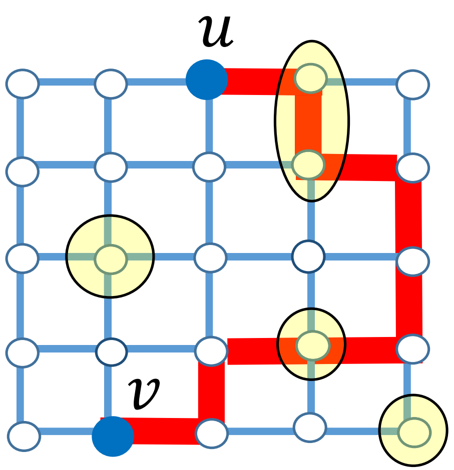
fan-out $\leq K$ and depth $< \frac{\log(n)}{16\log(K)}$.



Lemma: There are vertices u, v on the even sublattice and a **path Γ** connecting them such that
the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v\}$
do not contain any distant output bits $z_j \in \Gamma$.



$L(x_u)$



$L(x_v)$

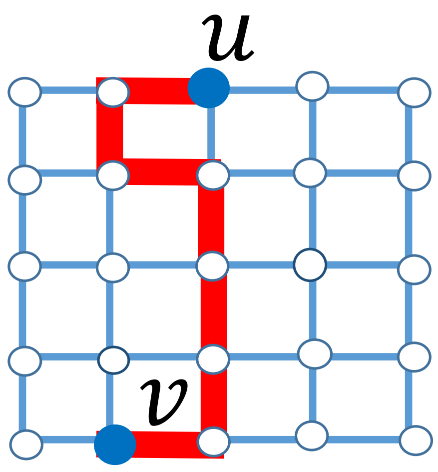
Example of a "bad" **path Γ**:

distant output bits in lightcones on path!

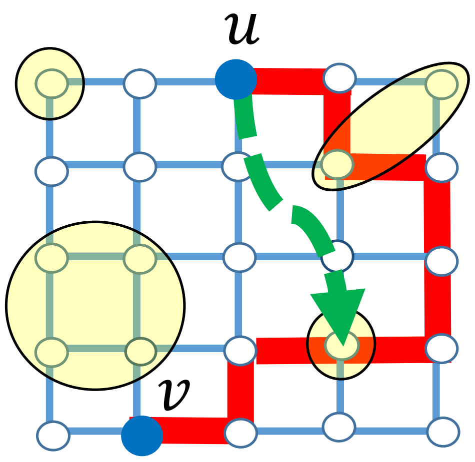
Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

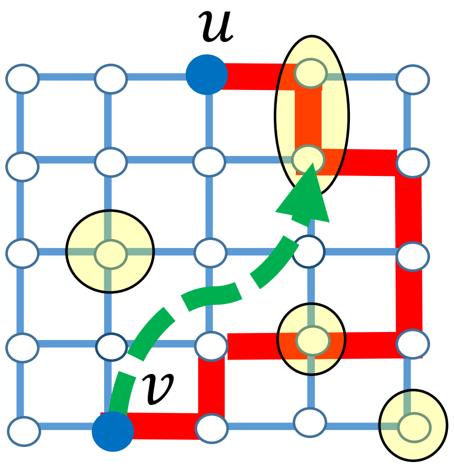
fan-out $\leq K$ and depth $< \frac{\log(n)}{16\log(K)}$.



Lemma: There are vertices u, v on the even sublattice and a **path Γ** connecting them such that
the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v\}$
do not contain any distant output bits $z_j \in \Gamma$.



$L(x_u)$



$L(x_v)$

Example of a "bad" **path Γ**:

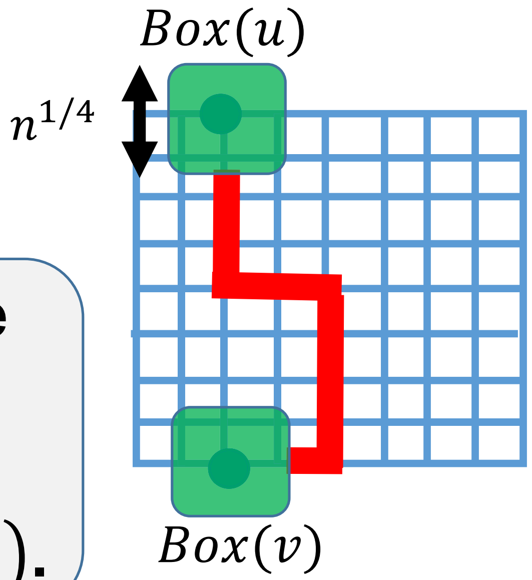
distant output bits on path!

Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

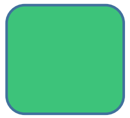
fan-out $\leq K$ and depth $< \frac{\log(n)}{16\log(K)}$.

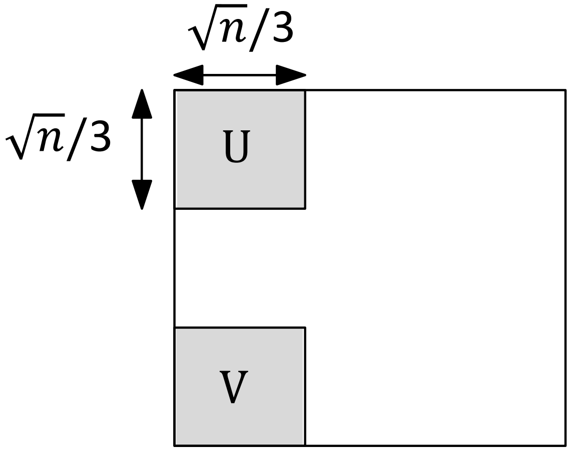
Lemma: Suppose $u \in \mathrm{U}, \mathrm{v} \in \mathrm{V}$ are on the even sublattice. Then there is a **path** Γ connecting them such that the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v\}$ **do not contain any distant output bits** $\boldsymbol{z_j \in \Gamma \setminus \left(Box(u) \cup Box(v)\right)}$.



Pick u, v from certain regions:

and exclude square-shaped boxes of size $n^{1/4} \times n^{1/4}$ around u, v

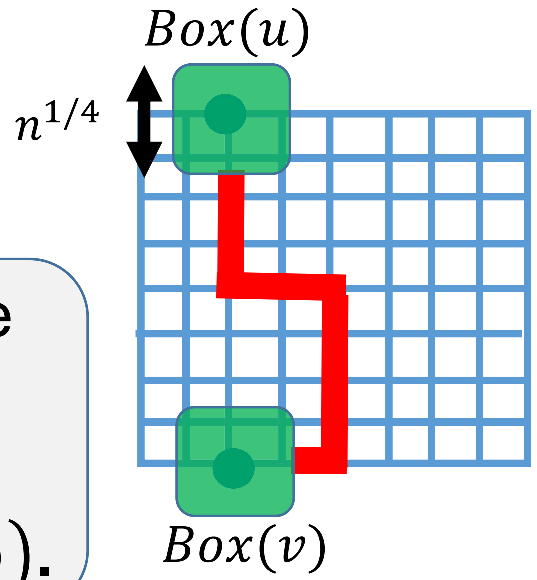




Proving existence of a suitable cycle: some ingredients

Suppose a classical circuit has

fan-out $\leq K$ and depth $< \frac{\log(n)}{16\log(K)}$.

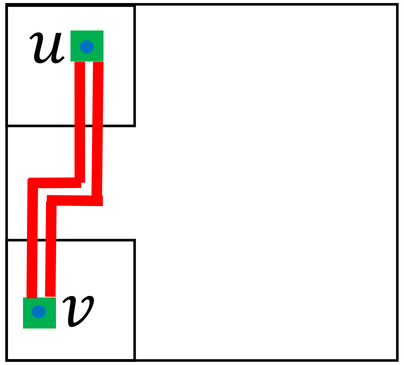


Lemma: Suppose $u \in \mathrm{U}, \mathrm{v} \in \mathrm{V}$ are on the even sublattice. Then there is a **path** Γ connecting them such that the light cones of the input bits $x_i \equiv A_{i,i}$ with $i \in \{u, v\}$ **do not contain any distant output bits** $\boldsymbol{z_j \in \Gamma \setminus \left(Box(u) \cup Box(v)\right)}$.

Proof sketch: Boxes are of size $n^{1/4} \times n^{1/4}$ $\Rightarrow$ Any pair of boxes can be connected by $n^{1/4}$ pairwise disjoint paths

Picking a random path Γ gives

$$\Pr[L(x_u) \cap \Gamma \neq \emptyset] \leq \frac{K^d}{n^{1/4}} \rightarrow 0 \qquad \text{for n large}$$



since $\boldsymbol{L(x_u)}$ intersects at most $\boldsymbol{K^d}$ paths.

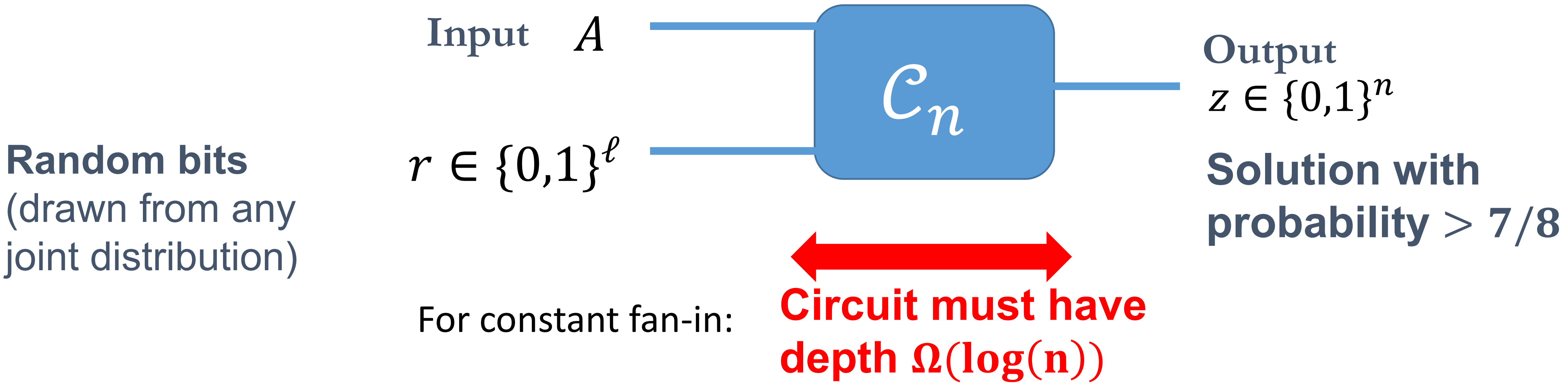
$\Rightarrow$ There is a path Γ which does not intersect $L(x_u)$ outside of $Box(u) \cup Box(v)$.

Main result: A lower bound on classical circuits

Theorem: The following holds for all sufficiently large n.

Let $\mathcal{C}_n$ be a classical probabilistic circuit where each gate of $\mathcal{C}_n$ has **fan-in at most K**. Suppose it **solves size-n instances** of the 2D HLF Problem **with probability $> 7/8$**. Then

$$\text{depth}(\mathcal{C}_n) \geq \frac{\log(n)}{16\log(K)}$$



On the (classical) time complexity of the HLF

Hidden Linear Function (HLF) problem

Input: binary symmetric matrix A

Output: bit string z such that $q(x) = 2z^T x \pmod 4$ for all $x \in \mathrm{Ker}(A)$

The general HLF problem can be solved classically **in time $\mathbf{O(n^3)}$**

1) Compute a basis $b^1, \dots, b^k$ of the nullspace $\mathrm{Ker}(A)$

2) Solve the linear system
$$2\, z^T b^i = q(b^i), \quad i = 1, \dots, k$$

Algorithm for general HLF: use Gottesman-Knill Theorem to simulate the quantum algorithm **in time $\mathbf{O(n^3)}$**

	# used in circuit (general HLF)	Simulation cost (each)
measurement	n	$O(n^2)$
Clifford gate	$\leq \binom{n}{2}$	$O(n)$

Improved algorithm for **2D HLF**: simulate the quantum algorithm **in time $\mathbf{O(n^2)}$**

# used in circuit (2D HLF)	improved simulation cost (each)
n	$O(n)$
n	$O(\sqrt{n})$

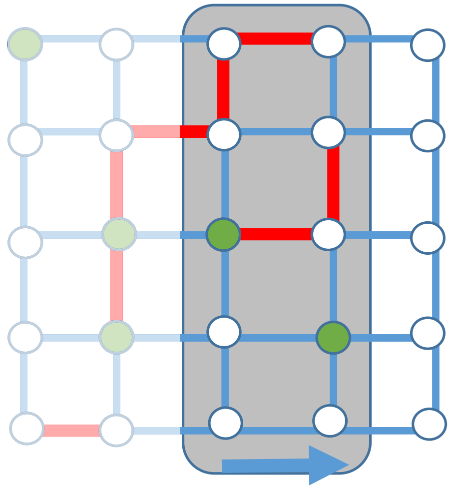
[S. Aaronson and D. Gottesman,PRA 70, 052328 (2004)]

On the (classical) time complexity of the HLF

Hidden Linear Function (HLF) problem

Input: binary symmetric matrix A

Output: bit string z such that $q(x) = 2z^T x \pmod 4$ for all $x \in \mathrm{Ker}(A)$



"sliding window" of size $O(1) \times \sqrt{n}$

Algorithm for general HLF: use

... quantum algorithm

in time $O(n^3)$

	# used in circuit (general HLF)	Simulation cost (each)
measurement	n	$O(n^2)$
Clifford gate	$\leq \binom{n}{2}$	$O(n)$

Improved algorithm for **2D HLF**: simulate the quantum algorithm **in time $O(n^2)$**

# used in circuit (2D HLF)	improved simulation cost (each)
n	$O(n)$
n	$O(\sqrt{n})$

[S. Aaronson and D. Gottesman,PRA 70, 052328 (2004)]

Some open problems

Is this a polynomial quantum (time) speedup with constant-depth circuits?

- The quantum algorithm solves the 2D HLF Problem in time $O(n)$.
- The best-known classical algorithm takes time $O(n^2)$.

Does the advantage persist if we permit stronger classical circuits?

- Can the 2D HLF be solved by AC^0 circuits? (constant depth unbounded fan-in)

Can the quantum advantage be made robust to noise?

- Different computational problems related to the HLF?

Thank you!

arXiv:1704.00690