Quantum Distributed Computing

François Le Gall

Nagoya University

ADGA 2022

Remark: this talk doesn't require any prior knowledge of quantum computation

Outline of the Talk

1. Brief overview of quantum computation
   - ✓ Basics of quantum computation

2. Overview of quantum distributed computing
   - ✓ Early results about quantum distributed computing
   - ✓ Recent results

3. Quantum distributed algorithms in the CONGEST model

   LG and Magniez. **Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks**. *PODC'18.*

4. Quantum distributed algorithms in the LOCAL model

   LG, Rosmanis and Nishimura. **Quantum Advantage for the LOCAL Model in Distributed Computing**. *STACS'19.*

5. Conclusion and open problems

Outline of the Talk

1. Brief overview of quantum computation
    - ✓ Basics of quantum computation
2. Overview of quantum distributed computing
    - ✓ Early results about quantum distributed computing
    - ✓ Recent results
3. Quantum distributed algorithms in the CONGEST model

    LG and Magniez. **Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks**. *PODC'18.*

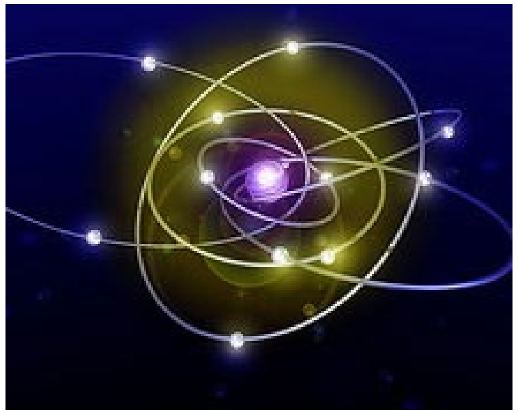
4. Quantum distributed algorithms in the LOCAL model

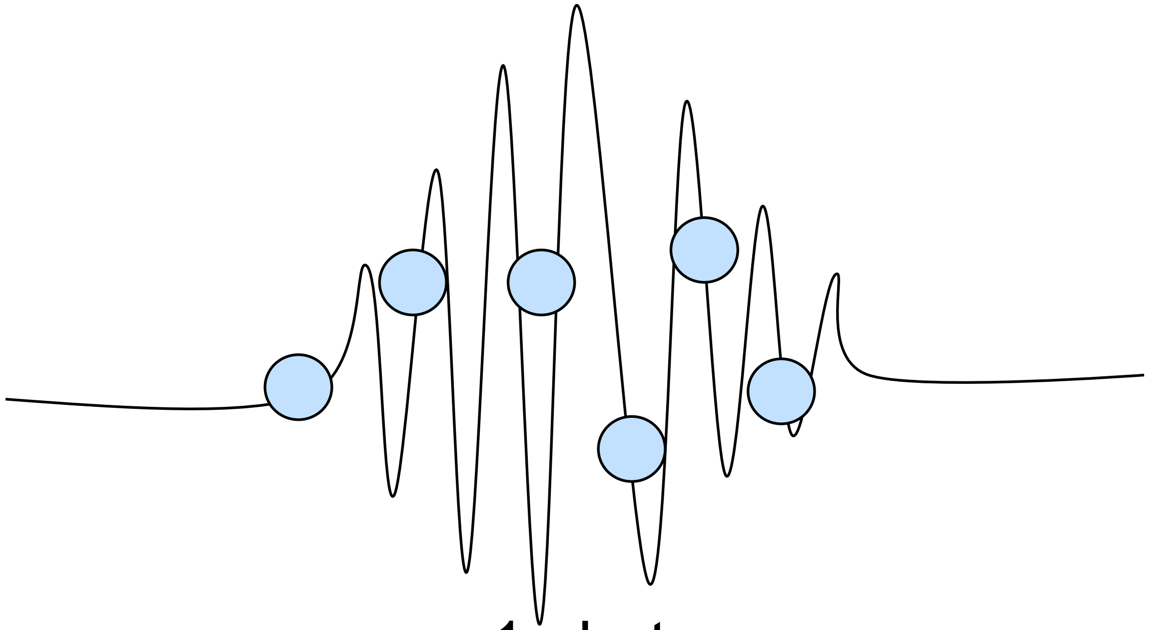
    LG, Rosmanis and Nishimura. **Quantum Advantage for the LOCAL Model in Distributed Computing**. *STACS'19.*

5. Conclusion and open problems

Quantum Computing

✓ Computation paradigm based on the laws of quantum mechanics





1 photon

quantum mechanics:

The position of a photon is described by a <u>wave</u> function (also called <u>quantum state</u>)

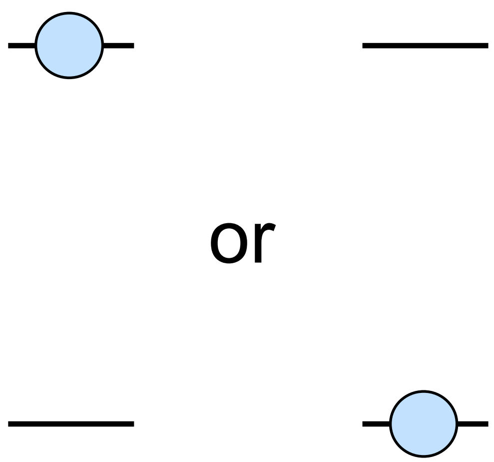
Quantum Mechanics: Discrete Case

two-state physical system

CLASSICAL

QUANTUM

state 1
("excited")



or

state 0
("non-excited")

more generally:

a probability distribution over 0 and 1

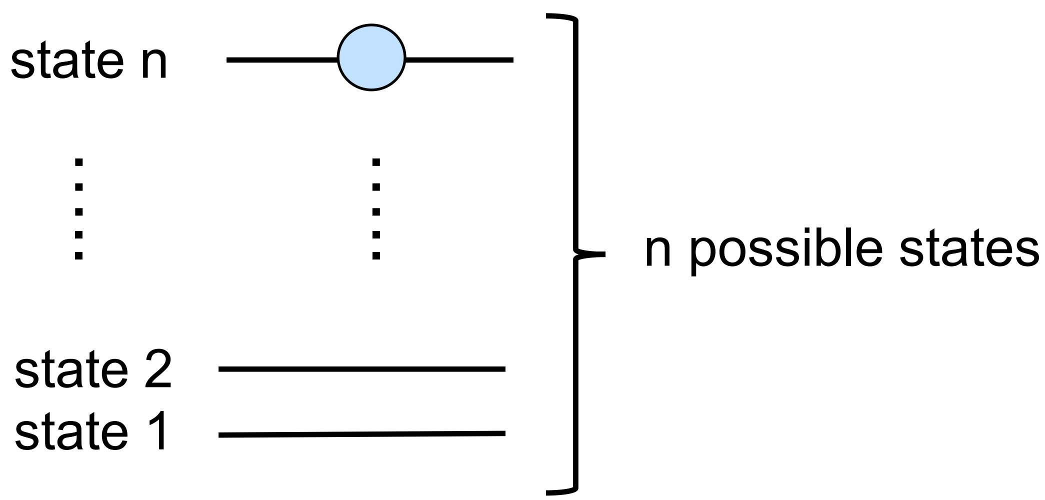
$\binom{p}{q}$ with $p, q \geq 0$ and $p + q = 1$

p is the probability to be at state 0
q is the probability to be at state 1

Quantum Mechanics: Discrete Case

n-state physical system

CLASSICAL



Description of the system:

a probability distribution

$$\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \text{ with } p_i \geq 0 \text{ and } \sum_i p_i = 1$$

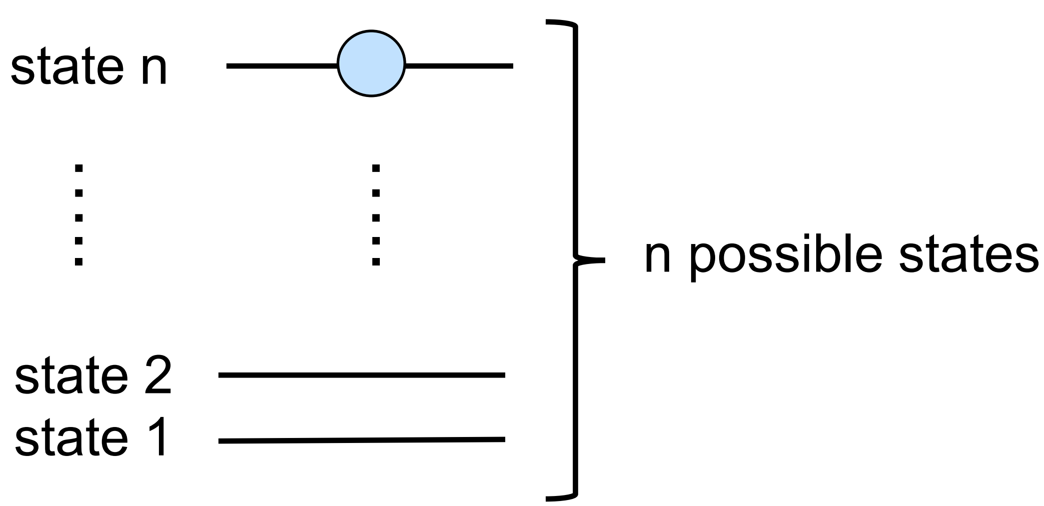
p_i is the probability to be in state i

QUANTUM

Quantum Mechanics: Discrete Case

n-state physical system

CLASSICAL



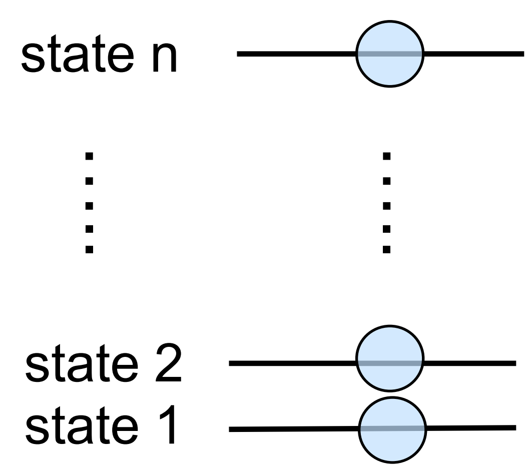
Description of the system:

a probability distribution

$$\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \text{ with } p_i \geq 0 \text{ and } \sum_i p_i = 1$$

p_i is the probability to be in state i

QUANTUM



makes convergence quadratically faster

Description of the system:

a wave function

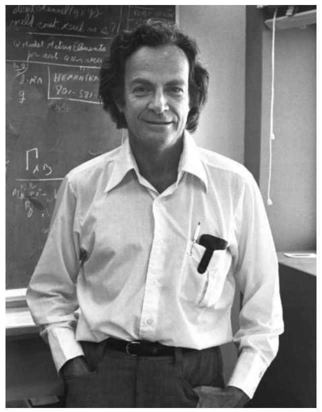
$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \text{ with } \alpha_i \in \mathbb{C} \text{ and } \sum_i |\alpha_i|^2 = 1$$

$|\alpha_i|^2$ is the probability to observe state i

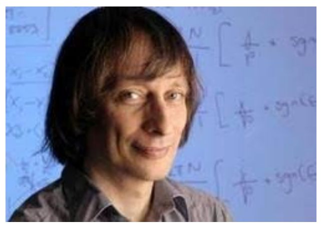
makes inferences possible

History of Quantum Computing

Proposal of QC



Feynman



Deutsch

First experiments

Wineland Haroche

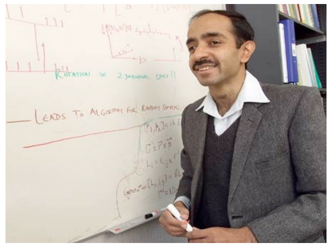
Nobel Prize in Physics (2012)

Aspect Clauser Zeilinger

Nobel Prize in Physics (2022)

Discovery of fast quantum algorithms

Shor



Grover

1982 1985 integer factoring 1994 1996 quantum search

makes convergence quadratically faster

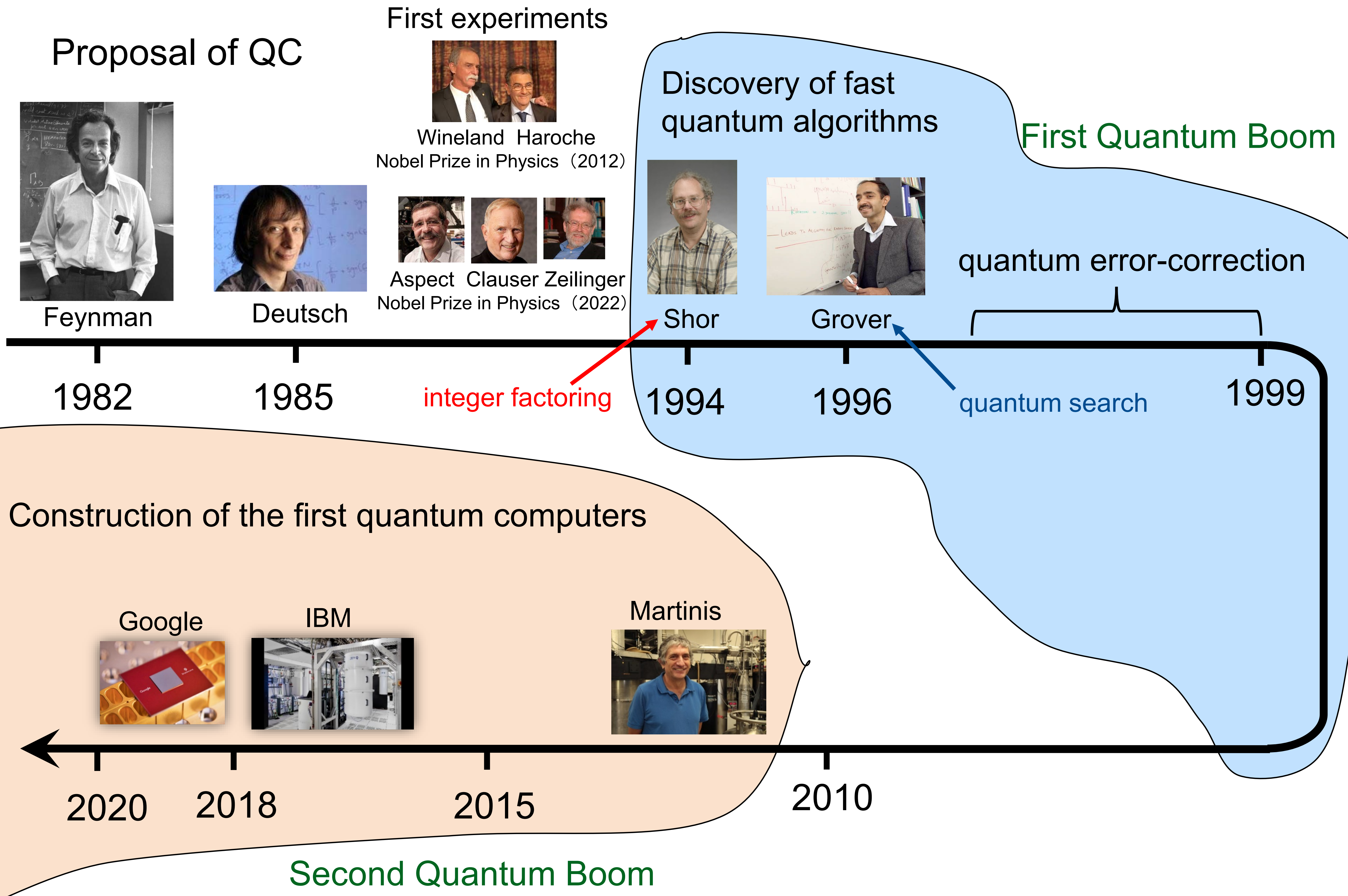
Description of the system:

a <u>wave function</u>

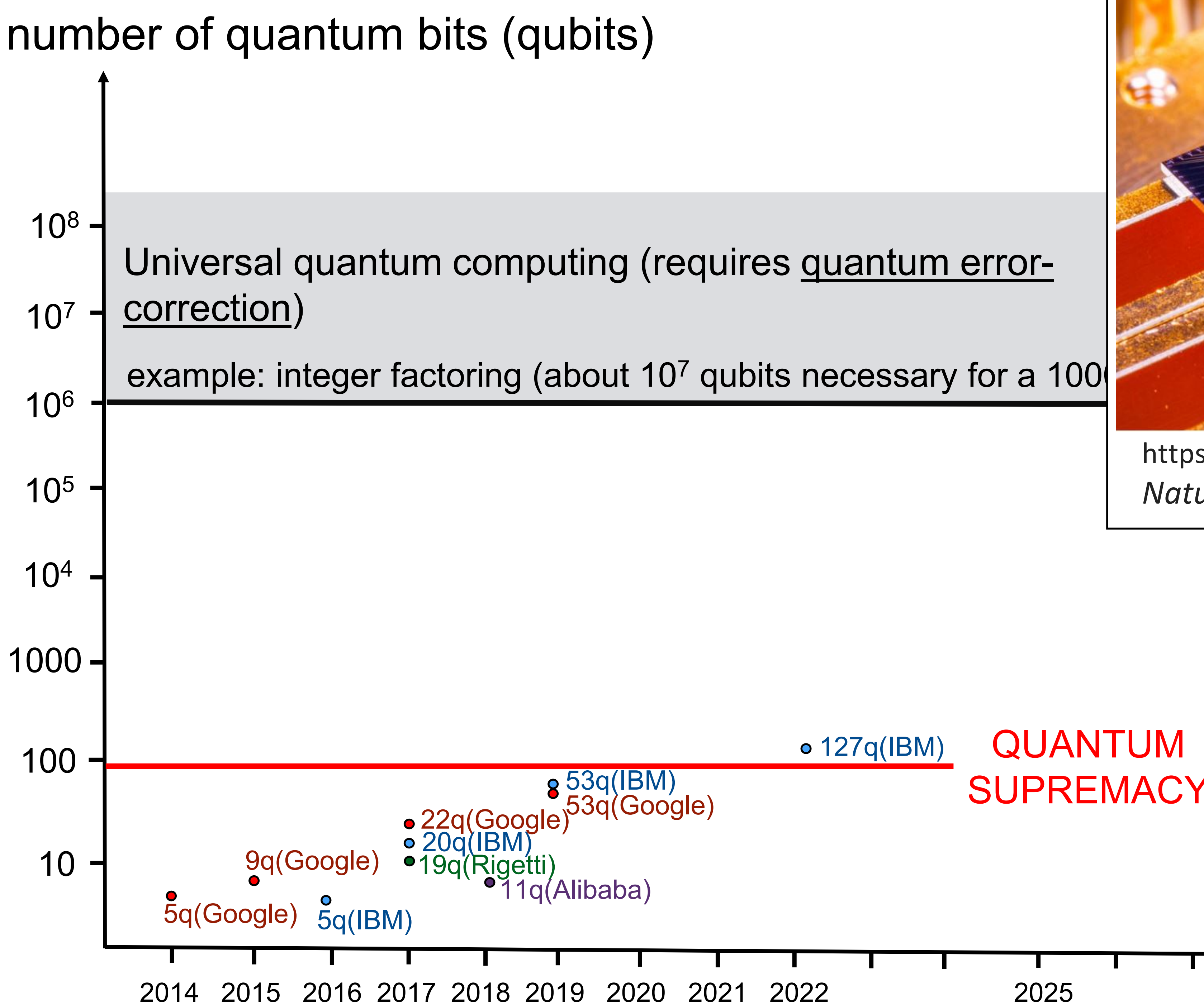
$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \text{ with } \alpha_i \in \mathbb{C} \text{ and } \sum_i |\alpha_i|^2 = 1$$

makes inferences possible

History of Quantum Computing



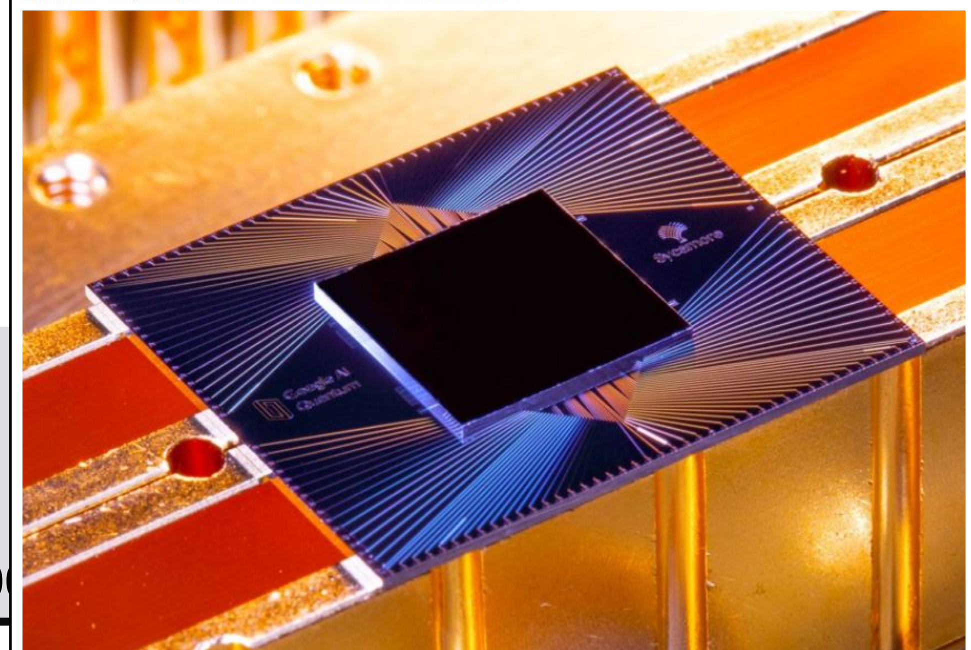
Quantum Moore's Law ?



NEWS · 23 OCTOBER 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.



https://www.nature.com/articles/d41586-019-03213-z

Nature **574**, 461-462 (2019)

- ✓ Task: compute the output of a random quantum circuit acting on 53 qubits
- ✓ Google's claim: it takes 100,000 years for a classical supercomputer

Outline of the Talk

1. Brief overview of quantum computation

   ✓ Basics of quantum computation

2. Overview of quantum distributed computing

   ✓ Early results about quantum distributed computing

   ✓ Recent results

3. Quantum distributed algorithms in the CONGEST model

   LG and Magniez. **Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks**. *PODC'18.*

4. Quantum distributed algorithms in the LOCAL model

   LG, Rosmanis and Nishimura. **Quantum Advantage for the LOCAL Model in Distributed Computing**. *STACS'19.*

5. Conclusion and open problems

Quantum Distributed Computing: History

✓ Mostly been studied in the framework of 2-party communication complexity

seminal result: quantum protocol for the disjointness function
[Cleve, Buhrman and Wigderson STOC'98]

✓ Relatively few results focusing on more than two parties until recently:

- exact quantum protocols for leader election on anonymous networks
[Tani, Kobayashi, Matsumoto PODC'09]

- study of quantum distributed algorithms on non-anonymous networks

[Gavoille, Kosowski, Markiewicz DISC'09] ← LOCAL model

no significant advantage reported

[Elkin, Klauck, Nanongkai, Pandurangan PODC'14] ← CONGEST model

negative results: shows impossibility of quantum distributed computing faster than classical distributed computing for many important problems (shortest paths, MST,…)

Question: can quantum distributed computing be useful?

Two early survey papers asking this question: [Denchev and Pandurangan ACM SIGACT News'08] [Arfaoui and Fraigniaud ACM SIGACT News'14]

Quantum Distributed Computing: Recent Positive Answers

Quantum CONGEST model

CONGEST model where quantum bits can be sent instead of usual bits

[LG, Magniez PODC'18]

The diameter of the network can be computed in $\tilde{\Theta}(\sqrt{n})$ rounds in the quantum CONGEST model (when the diameter is constant) but requires $\Theta(n)$ rounds in the classical CONGEST model.

Quantum CONGEST-CLIQUE model

CONGEST-CLIQUE model where quantum bits can be sent instead of usual bits

[LG, Izumi PODC'19]

The All-Pairs Shortest Path problem can be solved faster in the quantum CONGEST-CLIQUE model (quantum: $\tilde{O}(n^{1/4})$ rounds, classical: $\tilde{O}(n^{1/3})$ rounds [Censor-Hillel et al. PODC'15]).

Quantum LOCAL model

LOCAL model where quantum bits can be sent instead of usual bits

[LG, Nishimura, Rosmanis STACS'19]

There is a computational problem that can be solved in 2 rounds in the quantum LOCAL model but requires $\Theta(n)$ rounds classically.

More Recent Works

Quantum CONGEST model

CONGEST model where quantum bits can be sent instead of usual bits

[LG, Magniez PODC'18] ⇨ The diameter of the network can be computed in $\tilde{\Theta}(\sqrt{n})$ rounds in the quantum CONGEST model (when the diameter is constant) but requires $\Theta(n)$ rounds in the classical CONGEST model.

[Izumi, LG, Magniez STACS'20]

Quantum algorithms for triangle finding

[Magniez, Nayak ICALP'20]

Quantum lower bound for computing the diameter (for arbitrary diameter)

[Censor-Hillel, Fischer, LG, Leitersdorf, Oshman ITCS'22]

Quantum algorithms for

[de Vos, van Apeldoorn PODC'22

Quantum algorithms for

[Wu, Yao PODC'22]

Quantum algorithms for

Another topic: quantum distributed proof systems

(Quantum proofs can be much shorter than classical proofs!)

[Fraigniaud, LG, Nishimura, Paz DISC'20 (BA), ITCS'21]

[LG, Miyamoto, Nishimura DISC'22 (BA)] ⇦ Tuesday afternoon

Outline of the Talk

1. Brief overview of quantum computation
   - ✓ Basics of quantum computation
2. Overview of quantum distributed computing
   - ✓ Early results about quantum distributed computing
   - ✓ Recent results
3. Quantum distributed algorithms in the CONGEST model

   LG and Magniez. **Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks**. *PODC'18.*

4. Quantum distributed algorithms in the LOCAL model

   LG, Rosmanis and Nishimura. **Quantum Advantage for the LOCAL Model in Distributed Computing**. *STACS'19.*

5. Conclusion and open problems

Quantum CONGEST model

Quantum CONGEST model

CONGEST model where quantum bits can be sent instead of usual bits

one quantum bit (qubit) = one quantum particle (e.g., one photon)

- ✓ can be created using a laser and sent using optical fibers
- ✓ generalizes the concept of bit (hence quantum distributed computing can trivially simulate classical distributed computing)

“classical” means “non-quantum”

More formally:

- ✓ network G=(V,E) of n nodes (all nodes have distinct identifiers)
- ✓ each node knows the identifiers of all its neighbors
- ✓ synchronous communication between adjacent nodes: one message of O(log n) qubits per round
- ✓ each node is a quantum processor (i.e., a quantum computer)

Complexity: the number of rounds needed for the computation

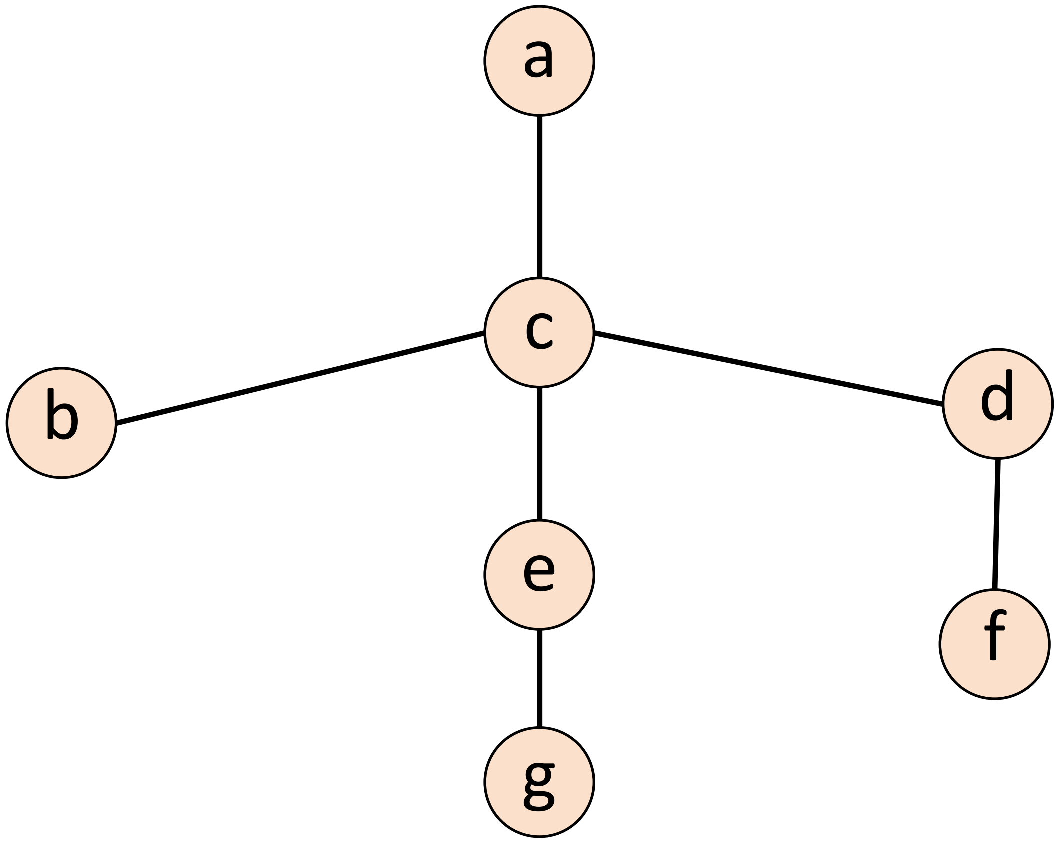
Diameter and Eccentricity

Consider an undirected and unweighted network G = (V,E) with n nodes

The diameter of the graph is the maximum distance between two nodes

$$D = \max_{u,v \in V} \{d(u,v)\}$$

d(u,v) = distance between u and v



Diameter and Eccentricity

Consider an undirected and unweighted network G = (V,E) with n nodes

The <u>diameter</u> of the graph is the maximum distance between two nodes

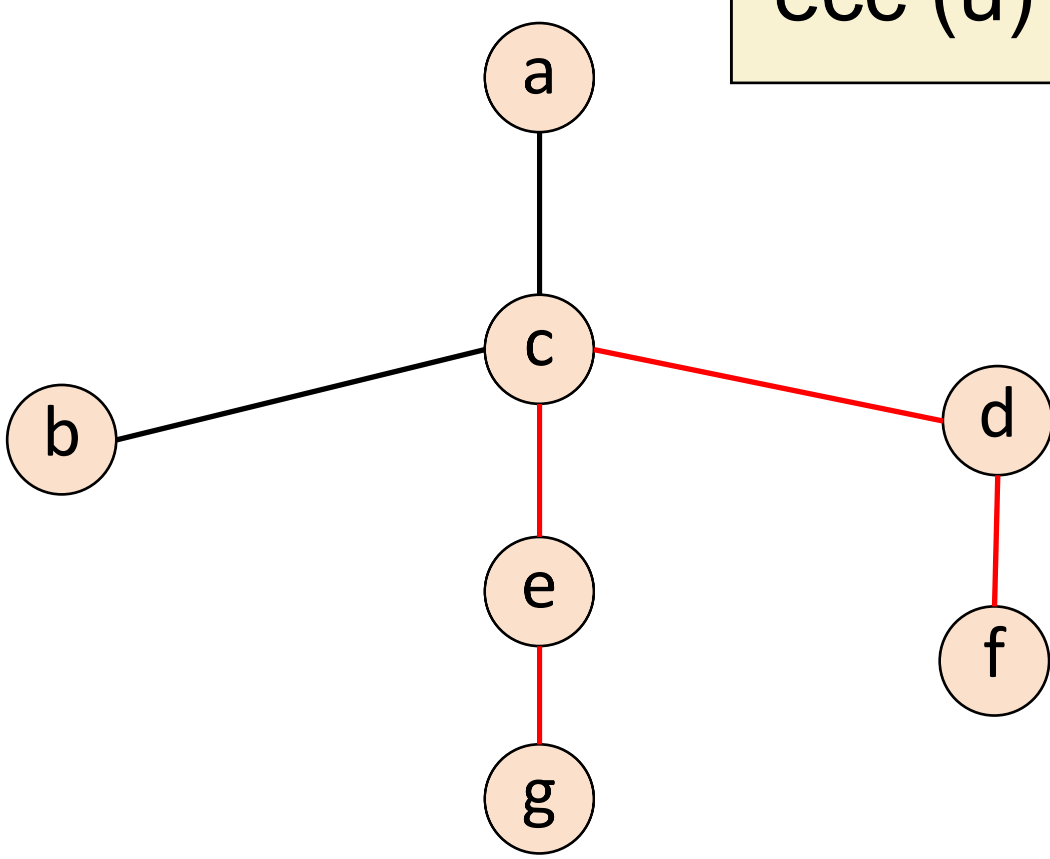
$$D = \max_{u,v \in V} \{d(u,v)\}$$

$$= \max_{u \in V} \{ecc\ (u)\}$$

d(u,v) = distance between u and v

The <u>eccentricity</u> of a node u is defined as

$$ecc\ (u) = \max_{v \in V} \{d(u,v)\}$$



D = 4

ecc (a) = 3
ecc (b) = 3
ecc (c) = 2
ecc (d) = 3
ecc (e) = 3
ecc (f) = 4
ecc (g) = 4

d(a,a) = 0
d(a,b) = 2
d(a,c) = 1
d(a,d) = 2
d(a,e) = 2
d(a, f) = 3
d(a,g) = 3

Diameter and Eccentricity

Consider an undirected and unweighted network G = (V,E) with n nodes

The diameter of the graph is the maximum distance between two nodes

$$D = \max_{u,v \in V} \{d(u,v)\}$$

$$= \max_{u \in V} \{ecc(u)\}$$

d(u,v) = distance between u and v

The eccentricity of a node u is defined as

$$ecc(u) = \max_{v \in V} \{d(u,v)\}$$

In the classical (i.e., non-quantum) CONGEST model:

- ✓ ecc(u) can be computed in O(D) rounds by constructing a Breadth-First Search tree rooted at u
- ✓ computing the diameter (i.e., the maximum eccentricity) requires Θ(n) rounds even for constant D
  [Frischknecht+12, Holzer+12, Peleg+12, Abboud+16]

Computation of the Diameter in the CONGEST model

Main result: sublinear-round quantum computation of the diameter whenever D=o(n)
(this algorithm uses $O((\log n)^2)$ qubits of quantum memory per node)

	Classical	Quantum ([LG, Magniez, PODC'18])
Exact computation (upper bounds)	$O(n)$ [Holzer+12, Peleg+12]	$O(\sqrt{nD})$
Exact computation (lower bounds)	$\widetilde{\Omega}(n)$ [Frischknecht+12]	$\widetilde{\Omega}(\sqrt{nD})$ [conditional]

number of rounds needed to compute the diameter (n: number of nodes, D: diameter)

condition: holds for quantum distributed algorithms
using only polylog(n) qubits of memory per node

Upper Bound

Main result: sublinear-round quantum computation of the diameter whenever D=o(n)

(this algorithm uses $O((\log n)^2)$ qubits of quantum memory per node)

	Classical	Quantum ([LG, Magniez, PODC'18])
Exact computation (upper bounds)	$O(n)$ [Holzer+12, Peleg+12]	$O(\sqrt{nD})$

Quantum Distributed Computation of the Diameter

Computation of the diameter (decision version)

$$\text{Given an integer } d\text{, decide if } \underbrace{\text{diameter} \geq d}_{\text{there is a vertex } u \text{ such that ecc }(u) \geq d}$$

This is a search problem

Idea: use the technique called “quantum search”

Centralized Quantum Search: Grover's algorithm

Let f: X → {0,1} be a Boolean function given as a black box

Goal: find an element x ∈ X such that f(x) = 1

Classically this can be done using $O(|X|)$ calls to the black box
("brute force search: try all the elements x")

There is a quantum centralized algorithm solving this problem with $O(\sqrt{|X|})$ calls to the black box

Quantum search
[Grover 96]

Intuition behind Grover's algorithm

Let f: X → {0,1} be a Boolean function given as a black box

$x \longrightarrow \boxed{\text{Classical Algorithm}} \longrightarrow f(x)$

Goal: find an element x ∈ X such that f(x) = 1

Classical sampling strategy:

Convert
$$\begin{pmatrix} 1/|X| \\ \vdots \\ 1/|X| \\ \boxed{1/|X|} \\ 1/|X| \\ \vdots \\ 1/|X| \end{pmatrix} \text{ to } \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \boxed{1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

x ∈ X such that f(x) = 1

$O(|X|)$ calls to the black box are enough

Grover's algorithm:

Convert
$$\begin{pmatrix} 1/\sqrt{|X|} \\ \vdots \\ 1/\sqrt{|X|} \\ \boxed{1/\sqrt{|X|}} \\ 1/\sqrt{|X|} \\ \vdots \\ 1/\sqrt{|X|} \end{pmatrix} \text{ to } \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \boxed{1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

x ∈ X such that f(x) = 1

$O(\sqrt{|X|})$ calls are enough [Grover 96]

CLASSICAL

Description of the system:

a probability distribution

$$\begin{pmatrix} p_1 \\ \vdots \\ p_m \end{pmatrix} \text{ with } p_i \geq 0 \text{ and } \sum_i p_i = 1$$

p_i is the probability to be in state i

QUANTUM

Description of the system:

a wave function

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \text{ with } \alpha_i \in \mathbb{C} \text{ and } \sum_i |\alpha_i|^2 = 1$$

$|\alpha_i|^2$ is the probability to observe state i

Centralized Quantum Search: Grover's algorithm

Let f: X → {0,1} be a Boolean function given as a black box

$$x \longrightarrow \boxed{\text{Classical Algorithm}} \longrightarrow f(x)$$

Goal: find an element x ∈ X such that f(x) = 1

Classically this can be done using $O(|X|)$ calls to the black box
("brute force search: try all the elements x")

> There is a quantum centralized algorithm solving this problem with $O(\sqrt{|X|})$ calls to the black box

Quantum search [Grover 96]

<u>Example of application</u>: quantum algorithm for Boolean satisfiability (SAT)

> SAT: given a Boolean formula f of poly size on M variables, find a satisfying assignment (if such an assignment exists)

Centralized Quantum Search: Grover's algorithm

Let f: X → {0,1} be a Boolean function given as a black box

x → Classical Algorithm → f(x)

Goal: find an element x ∈ X such that f(x) = 1

Classically this can be done using $O(|X|)$ calls to the black box
("brute force search: try all the elements x")

> There is a quantum centralized algorithm solving this problem with $O(\sqrt{|X|})$ calls to the black box

Quantum search
[Grover 96]

<u>Example of application</u>: quantum algorithm for Boolean satisfiability (SAT)

> SAT: given a Boolean formula f of poly size on M variables, find a satisfying assignment (if such an assignment exists)

X = set of all possible assignments ← $|X| = 2^M$

Black box: computes f(x) from x ← poly(M) time

Centralized Quantum Search: Grover's algorithm

Let f: X → {0,1} be a Boolean function given as a black box

Goal: find an element x ∈ X such that f(x) = 1

Classically this can be done using $O(|X|)$ calls to the black box
("brute force search: try all the elements x")

> There is a quantum centralized algorithm solving this problem with $O(\sqrt{|X|})$ calls to the black box

Quantum search
[Grover 96]

<u>Example of application</u>: quantum algorithm for Boolean satisfiability (SAT)

> SAT: given a Boolean formula f of poly size on M variables, find a satisfying assignment (if such an assignment exists)

X = set of all possible assignments ⟵ $|X| = 2^M$

Black box: computes f(x) from x ⟵ poly(M) time

⇨ Quantum search solves SAT in $O(2^{M/2} \times \text{poly}(M))$ time

Quantum Distributed Computation of the Diameter

Define the function f: V → {0,1} such that $f(u) = \begin{cases} 1 \text{ if ecc } (u) \geq d \\ 0 \text{ otherwise} \end{cases}$

Goal: find u such that f(u) = 1 (or report that no such vertex exist)

There is a quantum <u>centralized</u> algorithm for this search problem using $O(\sqrt{n})$ calls to a black box evaluating f

Quantum search [Grover 96]

Computation of the diameter (decision version)

Given an integer d, decide if $\underbrace{\text{diameter} \geq d}_{\text{there is a vertex u such that ecc (u)} \geq d}$

This is a search problem
Idea: use the technique called “quantum search”

Quantum Distributed Computation of the Diameter

Define the function f: V → {0,1} such that $f(u) = \begin{cases} 1 \text{ if } ecc(u) \geq d \\ 0 \text{ otherwise} \end{cases}$

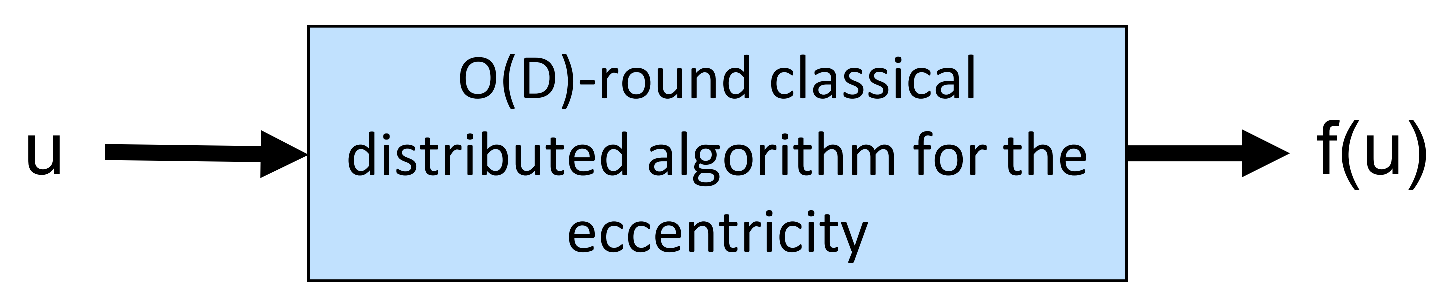
Goal: find u such that f(u) = 1 (or report that no such vertex exist)

There is a quantum centralized algorithm for this search problem using $O(\sqrt{n})$ calls to a black box evaluating f

Quantum search [Grover 96]

Quantum distributed algorithm computing the diameter

- ✓ The network elects a leader
- ✓ The leader locally runs this centralized quantum algorithm for search, in which each call to the black box is implemented by executing the standard O(D)-round classical algorithm computing the eccentricity



Quantum Distributed Computation of the Diameter

Define the function f: V → {0,1} such that f(u) = $\begin{cases} 1 \text{ if ecc (u)} \geq \text{d} \\ 0 \text{ otherwise} \end{cases}$

Goal: find u such that f(u) = 1 (or report that no such vertex exist)

There is a quantum <u>centralized</u> algorithm for this search problem using $O(\sqrt{n})$ calls to a black box evaluating f

Quantum search [Grover 96]

<u>Quantum distributed algorithm computing the diameter</u>

- ✓ The network elects a leader
- ✓ The leader locally runs this centralized quantum algorithm for search, in which each call to the black box is implemented by executing the standard O(D)-round classical algorithm computing the eccentricity

Complexity: $O(\sqrt{n} \times \mathrm{D})$ rounds

u → O(D)-round classical distributed algorithm for the eccentricity → f(u)

With further work, the complexity can be reduced to $O(\sqrt{nD})$ rounds

The Upper Bound

	Classical	Quantum ([LG, Magniez, PODC'18])
Exact computation (upper bounds)	$O(n)$ [Holzer+12, Peleg+12]	$O(\sqrt{nD})$

Lower Bounds

	Classical	Quantum [LG, Magniez PODC'18]
Exact computation (lower bounds)	$\widetilde{\Omega}(n)$ [Frischknecht+12]	$\widetilde{\Omega}(\sqrt{n}+D)$ [unconditional] $\widetilde{\Omega}(\sqrt{nD})$ [conditional]

via two-party communication complexity of the disjointness function (DISJ)

classical lower bound

- ✓ reduce DISJ to the distributed computation of diameter [Frischknecht+12]
- ✓ the (two-party) communication complexity of $DISJ_n$ is $\Omega(n)$ bits [Kalyanasundaram+92]

unconditional quantum lower bound

- ✓ same reduction from DISJ to the distributed computation of diameter
- ✓ the (two-party) communicati

Improvement [Magniez, Nayak ICALP'20]

$$\widetilde{\Omega}(\sqrt{n}+n^{1/3}D^{2/3})$$ [unconditional]

conditional quantum lower

- ✓ Claim: if the quantum distributed algorithm for diameter <u>uses few quantum memory</u> per node, then the reduction can be adjusted to give a two-party protocol for DISJ using few messages (idea: send communication in batches)
- ✓ the (two-party) r-message quantum communication complexity of $DISJ_n$ is $\Omega(\ n/r+r\ )$ qubits [Braverman+15]

Summary on the Quantum CONGEST

Quantum CONGEST model

CONGEST model where quantum bits can be sent instead of usual bits

[LG, Magniez PODC'18]

The diameter of the network can be computed in $\tilde{O}(\sqrt{nD})$ rounds in the quantum CONGEST model, but requires $\Theta(n)$ rounds in the classical CONGEST model.

Useful for problems in distributed computing where the bottleneck is a search problem

"Recipe" to build a quantum distributed algorithm
(even without knowing anything about quantum computation):

If you need to find a good element among N candidates and have a r-round procedure to check if an element is good, there is a $O(r\sqrt{N})$-round quantum algorithm for this search problem.

"Distributed Quantum Search"

Summary on the Quantum CONGEST

Quantum CONGEST model

CONGEST model where quantum bits can be sent instead of usual bits

[LG, Magniez PODC'18]

The diameter of the network can be computed in $\tilde{O}(\sqrt{nD})$ rounds in the quantum CONGEST model, but requires $\Theta(n)$ rounds in the classical CONGEST model.

[Izumi, LG, Magniez STACS'20]

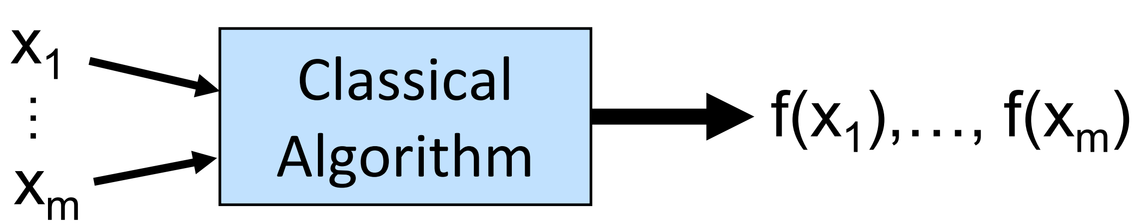
Quantum algorithms for triangle finding using distributed quantum search (quantum: $\tilde{O}(n^{1/4})$ rounds, classical: $\tilde{O}(n^{1/3})$ rounds [Chang and Saranurak PODC'19]).

[Censor-Hillel, Fischer, LG, Leitersdorf, Oshman ITCS'22]

Quantum algorithms for clique detection using nested distributed quantum search (for triangle detection: $\tilde{O}(n^{1/5})$ rounds in the quantum setting).

[de Vos, van Apeldoorn PODC'22]

Quantum algorithms for cycle detection and girth computation using a more general framework for distributed quantum search using parallel queries



[Wu, Yao PODC'22]

Quantum algorithms for weighted diameter and radius using distributed quantum search

Outline of the Talk

1. Brief overview of quantum computation

   ✓ Basics of quantum computation

2. Overview of quantum distributed computing

   ✓ Early results about quantum distributed computing

   ✓ Recent results

3. Quantum distributed algorithms in the CONGEST model

   LG and Magniez. **Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks**. *PODC'18.*

4. Quantum distributed algorithms in the LOCAL model

   LG, Rosmanis and Nishimura. **Quantum Advantage for the LOCAL Model in Distributed Computing**. *STACS'19.*

5. Conclusion and open problems

Quantum distributed computing: Recent Works

Quantum CONGEST model

CONGEST model where quantum bits can be

quantum distributed search

[LG, Magniez PODC'18]

The diameter of the network can be computed in $\tilde{\Theta}(\sqrt{n})$ rounds in the quantum CONGEST model (when the diameter is constant) but requires $\Theta(n)$ rounds in the classical CONGEST model.

Quantum CONGEST-CLIQUE model

CONGEST-CLIQUE model where quantum bits

quantum distributed search

[LG, Izumi PODC'19]

The All-Pairs Shortest Path problem can be solved faster in the quantum CONGEST-CLIQUE model (quantum: $\tilde{O}(n^{1/4})$ rounds, classical: $\tilde{O}(n^{1/3})$ rounds [Censor-Hillel et al. PODC'15]).

Quantum LOCAL model

LOCAL model where quantum bits can be

completely different technique

[LG, Nishimura, Rosmanis STACS'19]

There is a computational problem that can be solved in 2 rounds in the quantum LOCAL model but requires $\Theta(n)$ rounds classically.

Quantum LOCAL model

Messages can now have arbitrary length

Quantum CONGEST model

- ✓ network G=(V,E) of n nodes (all nodes have distinct identifiers)
- ✓ each node knows the identifiers of all its neighbors
- ✓ synchronous communication between adjacent nodes: one message of O(log n) qubits per round
- ✓ each node is a quantum processor (i.e., a quantum computer)

Complexity: the number of rounds needed for the computation

Quantum LOCAL model

- ✓ network G=(V,E) of n nodes (all nodes have distinct identifiers)
- ✓ each node knows the identifiers of all its neighbors
- ✓ synchronous communication between adjacent nodes: one message of arbitrary length per round
- ✓ each node is a quantum processor (i.e., a quantum computer)

Complexity: the number of rounds needed for the computation

Superiority of the Quantum LOCAL model

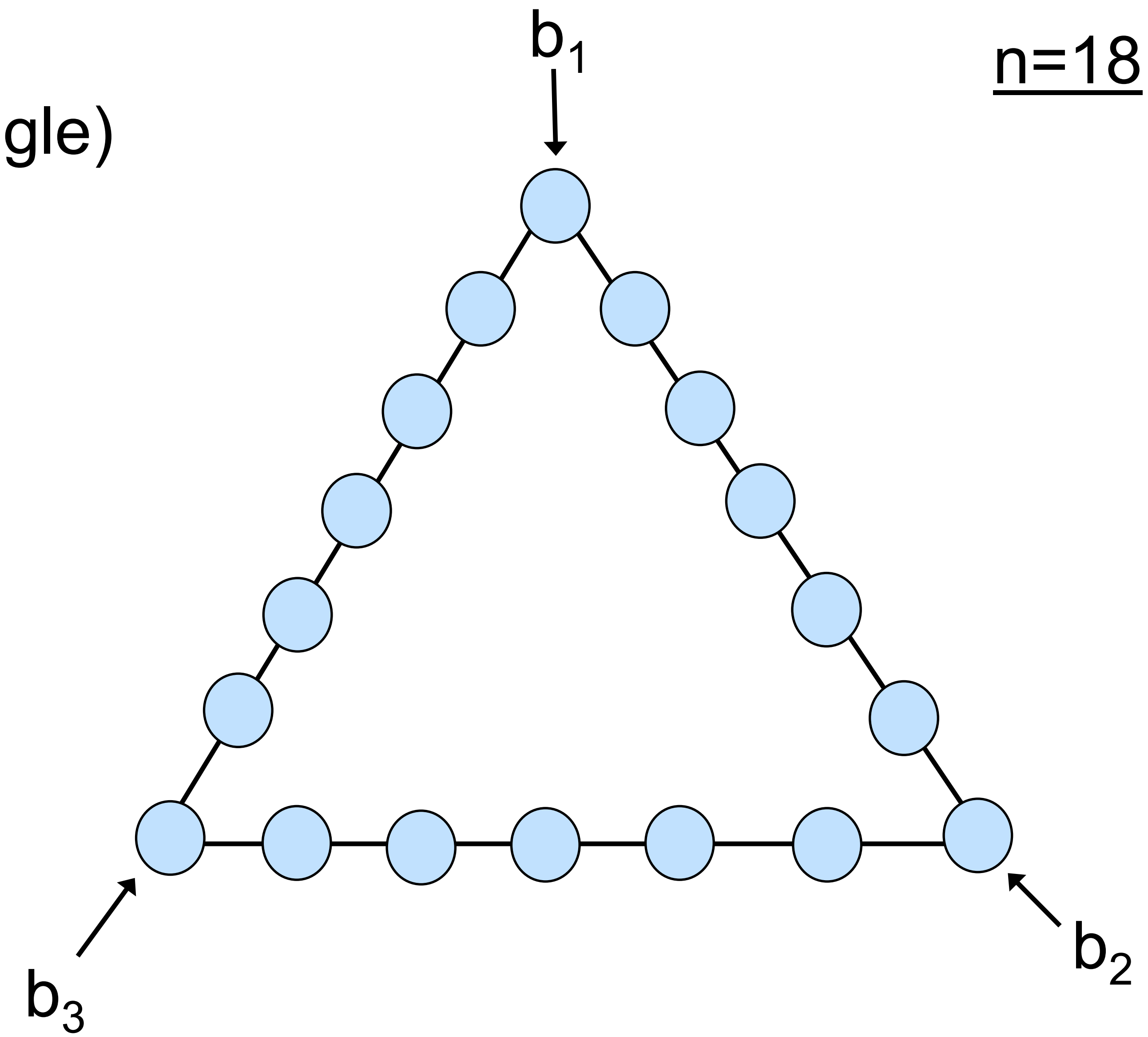
[LG, Rosmanis and Nishimura 2018]

multiple of 3

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

Each "corner" gets a bit as input

Each node will output one bit



Superiority of the Quantum LOCAL model

[LG, Rosmanis and Nishimura 2018]

Consider a ring of size n (seen as a triangle) ← multiple of 3

Each “corner” gets a bit as input

Each node will output one bit

Define the following four bits:

$$m_R = z_2 \oplus z_4 \oplus z_6$$

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

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

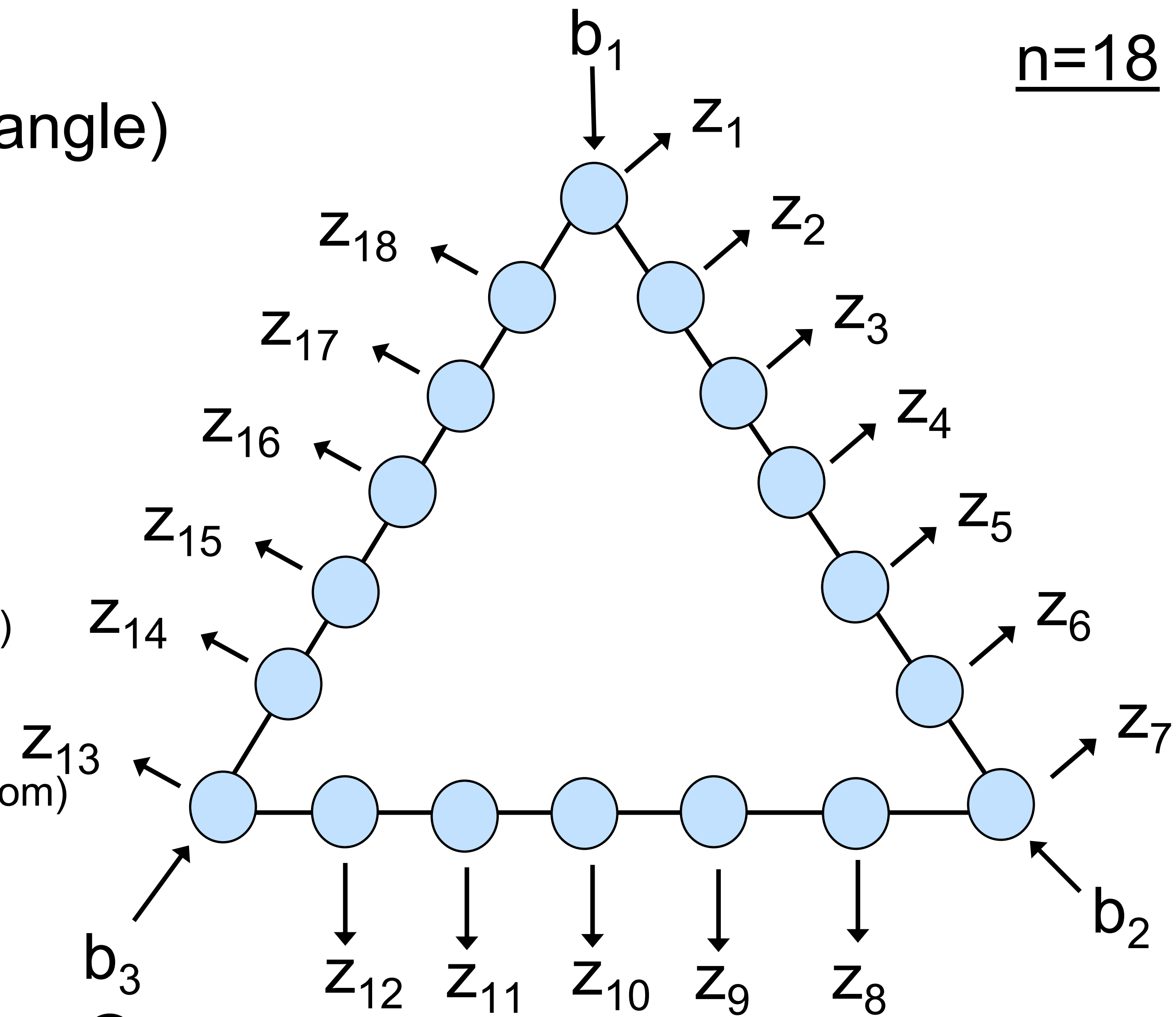
(parity of the outputs of the nodes of even index on the bottom)

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

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

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

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



018]

18

C

E

E

1. Each node creates 1 qubit
2. Each node makes its qubit interact with its two neighbors (2 rounds)
3. Each non-corner node makes a “standard measurement” to its qubit, and outputs the bit corresponding to the measurement outcome
4. Each corner node makes a “standard measurement” to its qubit if its input bit is 0, or makes a “projective measurement” to its qubit if its input bit is 1, and outputs the bit corresponding to the measurement outcome

Define the following four bits:

$$m_R = z_2 \oplus z_4 \oplus z_6$$

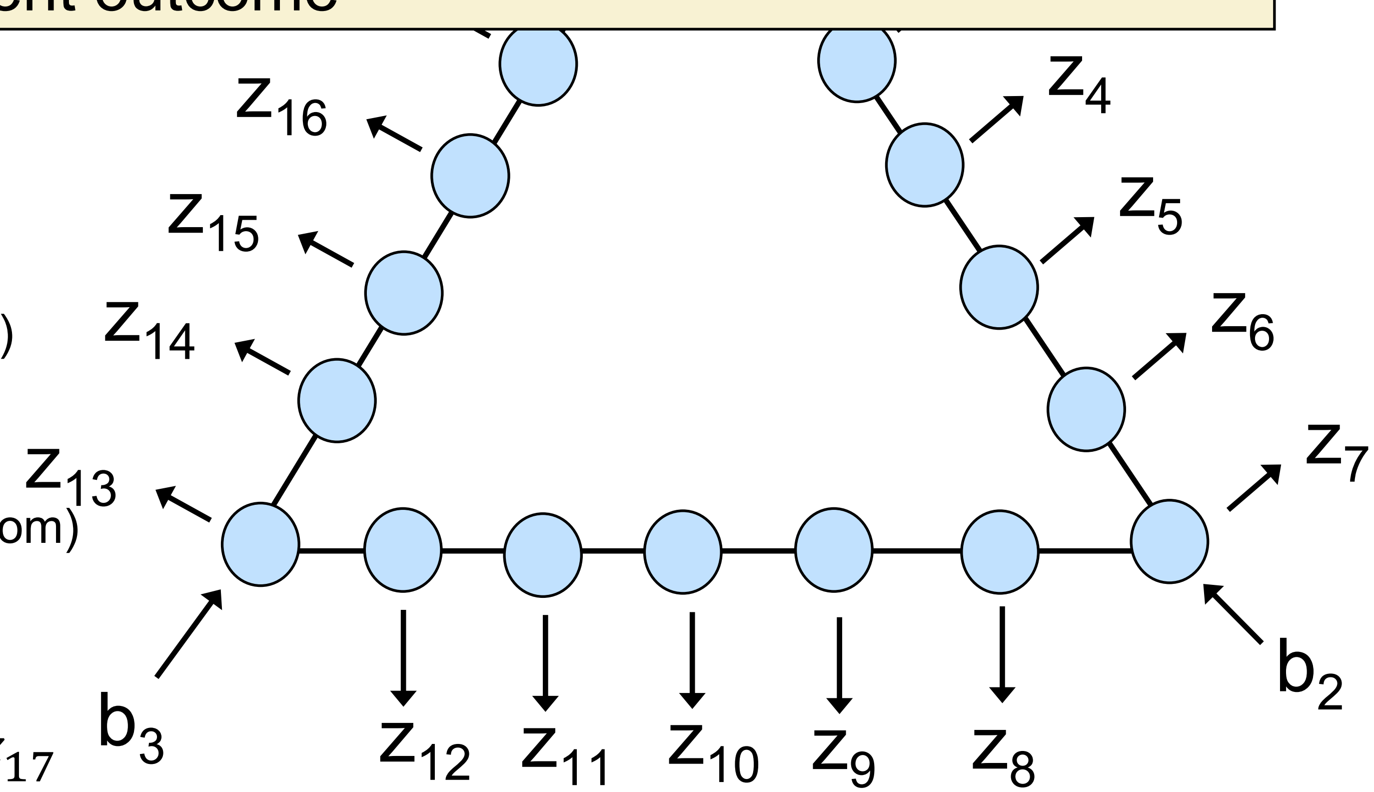
(parity of the outputs of the nodes of even index on the right)

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

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

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

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



Claim 1: There is a 2-round quantum algorithm that outputs the uniform distribution over all binary strings $(z_1, z_2, \dots, z_n) \in \{0,1\}^n$ satisfying the following condition:

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

Claim 2: In the LOCAL model, any classical algorithm that outputs the same distribution must use at least n/6 rounds.

- ✓ In any classical protocol using less than n/6 rounds:

  m_R is an affine function of b_1 and b_2

  m_B is an affine function of b_2 and b_3

  m_L is an affine function of b_1 and b_3

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

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

$m_R = z_2 \oplus z_4 \oplus z_6$

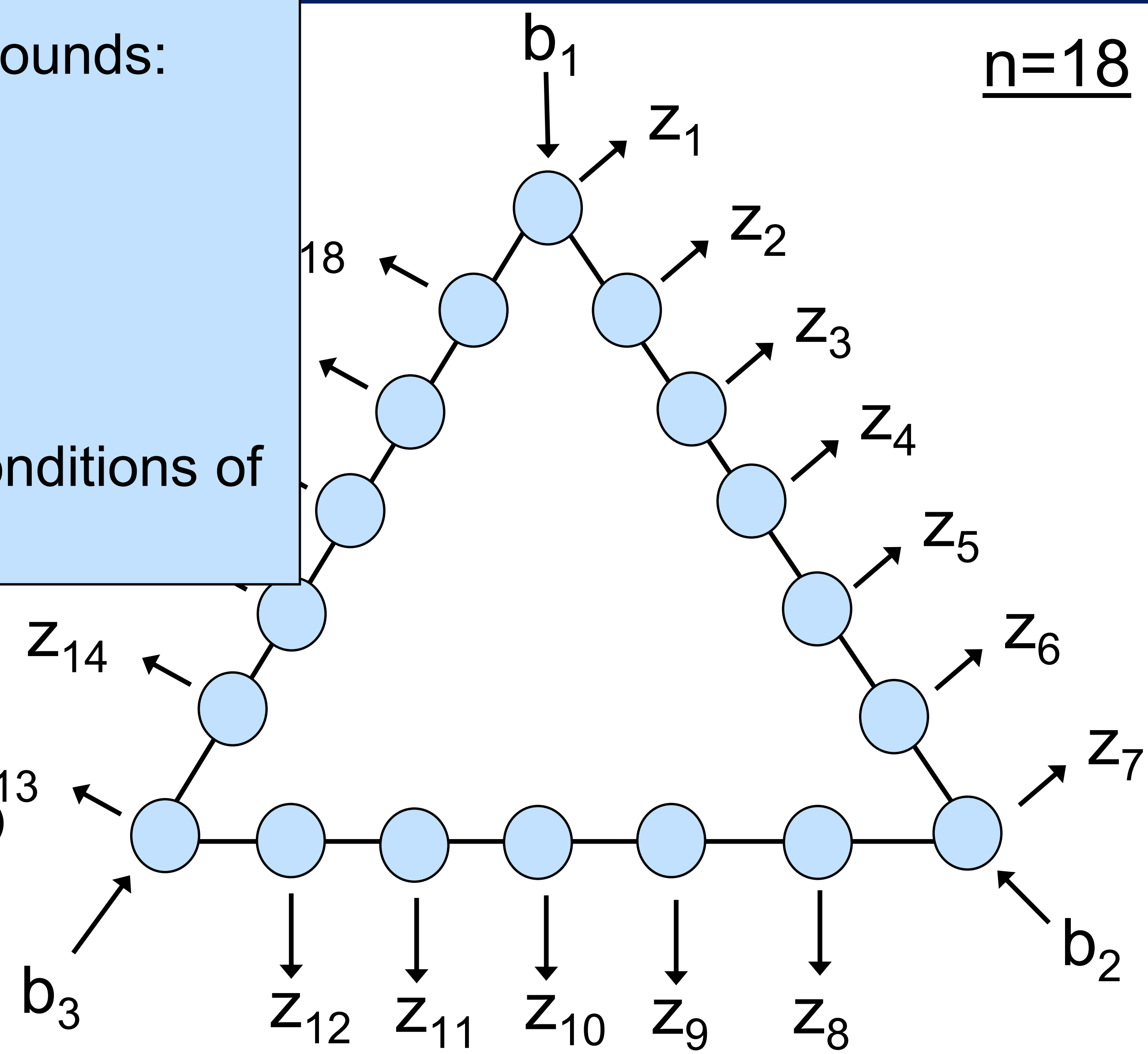
(parity of the outputs of the nodes of even index on the right)

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

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

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

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

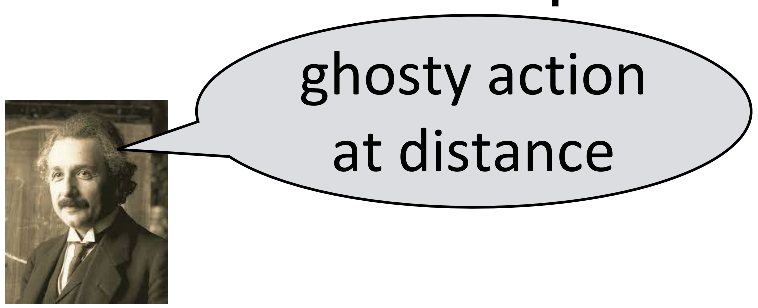


Claim 1: There is a 2-round quantum algorithm that outputs the uniform distribution over all binary strings $(z_1, z_2, \dots, z_n) \in \{0,1\}^n$ satisfying the following condition:

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

Quantum LOCAL model: Summary

- ✓ Huge separation (2 rounds quantumly vs. $\Theta(n)$ rounds classically),
- ✓ This significantly improves the only known previous separation "1 round quantumly vs. 2 rounds classically" from [Gavoille, Kosowski, Markiewicz DISC'09]
- ✓ This separation is another example of quantum non-locality (phenomenon where "quantum correlations are highly non-local")



experimental verification (1980s)

Aspect Clauser Zeilinger
Nobel Prize in Physics（2022）

- ✓ Unfortunately, this separation is for a very artificial problem (as the separation in [Gavoille, Kosowski, Markiewicz DISC'09])

Quantum LOCAL model

LOCAL model where quantum bits can be sent instead of usual bits

[LG, Nishimura, Rosmanis STACS'19]

There is a computational problem that can be solved in 2 rounds in the quantum LOCAL model but requires $\Theta(n)$ rounds classically.

Conclusions and Open Problems

quantum distributed search

✓ In the CONGEST and CONGEST-CLIQUE models, several important graph-theoretic problems can be solved faster using quantum distributed algorithms: diameter, clique detection, cycle detection, computing the girth…

✓ In the LOCAL model, quantum distributed algorithms can also be faster for some (artificial) computational tasks

quantum non-locality

Open problems:

✓ Find other applications of quantum distributed algorithms in the CONGEST or CONGEST-CLIQUE models

- Other applications of the "distributed quantum search" recipe
- New techniques (e.g., quantum walks)

✓ Consider other models (e.g., asynchronous computation, faulty communication,..) in the quantum setting

✓ Find one interesting application of quantum distributed computing in the LOCAL model

[LG and Rosmanis, in preparation]
On a ring, one round is not enough for 3-coloring.

- Can we get a quantum advantage for a locally-checkable problem (LCP)?
- What is the quantum complexity of 3-coloring on the ring? Can we prove an $\Omega(\log^* n)$ lower bound? (Already asked in [Arfaoui and Fraigniaud ACM SIGACT News'14])