Challenges in Quantum Distributed Computing

François Le Gall

Nagoya University

Workshop on Foundations of Distributed and Parallel Graph Algorithms

Outline of the Talk

1. Brief overview of quantum computing

2. Quantum distributed computing: Three main techniques
   - ✓ Quantum leader election (anonymous networks)
   - ✓ Quantum search (CONGEST model)
   - ✓ Quantum nonlocality (LOCAL model)

3. Open problems and Challenges

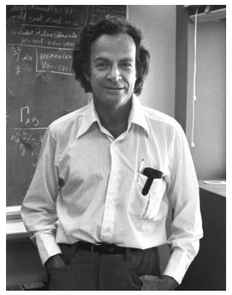
History of Quantum Computing

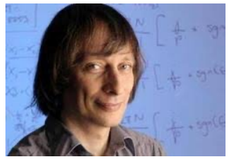
Proposal of QC

First experiments

Discovery of fast quantum algorithms


Manin


Feynman


Deutsch


Wineland Haroche
Nobel Prize in Physics（2012）


Aspect Clauser Zeilinger
Nobel Prize in Physics（2022）


Shor


Grover

1980 1982 1985 1994 1996

integer factoring

quantum search

makes convergence quadratically faster

Description of a classical (probabilistic) system:

a probability distribution

$$\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \quad \text{with } p_i \in [0,1] \text{ and } \sum_i p_i = 1$$

Description of a quantum system:

a wave function

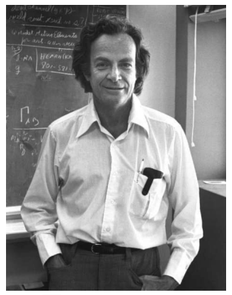
$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \text{with } \alpha_i \in \mathbb{C} \text{ and } \sum_i |\alpha_i|^2 = 1$$

makes inferences possible

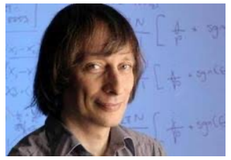
History of Quantum Computing

Proposal of QC

Manin



Feynman



Deutsch

1980

1982

1985

First experiments

Wineland Haroche

Nobel Prize in Physics（2012）

Aspect Clauser Zeilinger

Nobel Prize in Physics（2022）

integer factoring

Discovery of fast quantum algorithms

Shor

Grover

1994

1996

quantum search

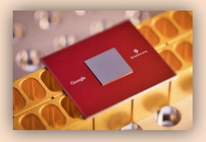
quantum error-correction

1999

First Quantum Computing Boom

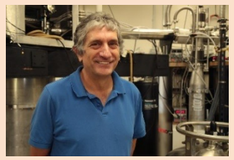
Construction of the first (small) quantum computers

Google



IBM

Martinis



2020

2018

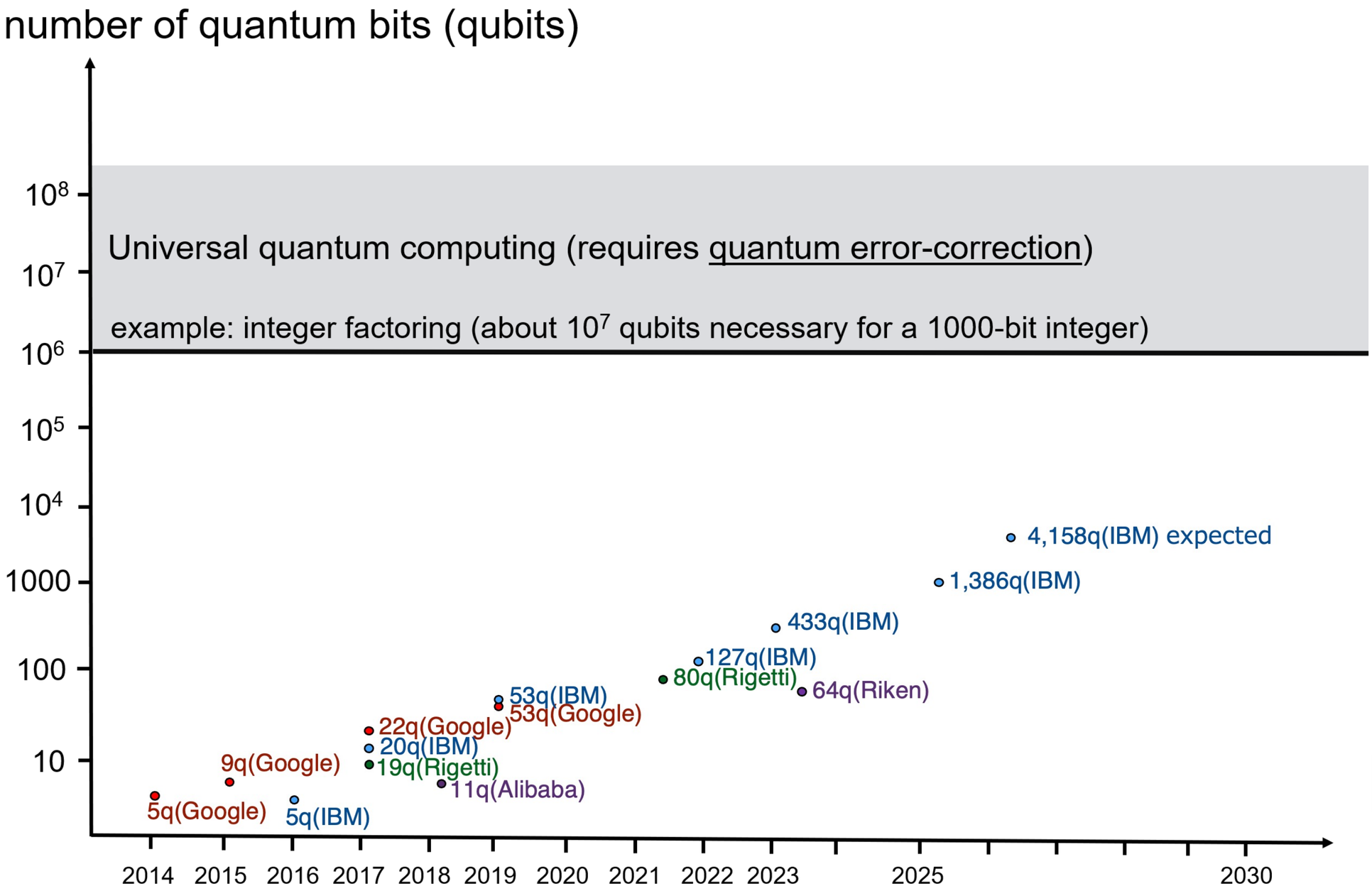
2015

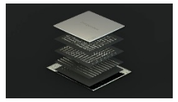
2010

Second Quantum Computing Boom

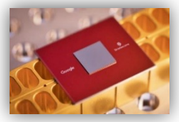
Dark Period

Quantum Moore's Law ?





IBM「Osprey」
（2023, 433 qbits）



Google「Sycamore」
（2019, 53 qbits）

Applications of Quantum Computers

- ✓Integer Factoring (Shor algorithm)
- ✓Quantum search (Grover algorithm)
- ✓Problems with quantum inputs
  (most problems in quantum information theory)
- ✓Distributed quantum algorithms

…

https://quantumalgorithmzoo.org/

542 references （May 11th, 2026）

Quantum Algorithm Zoo

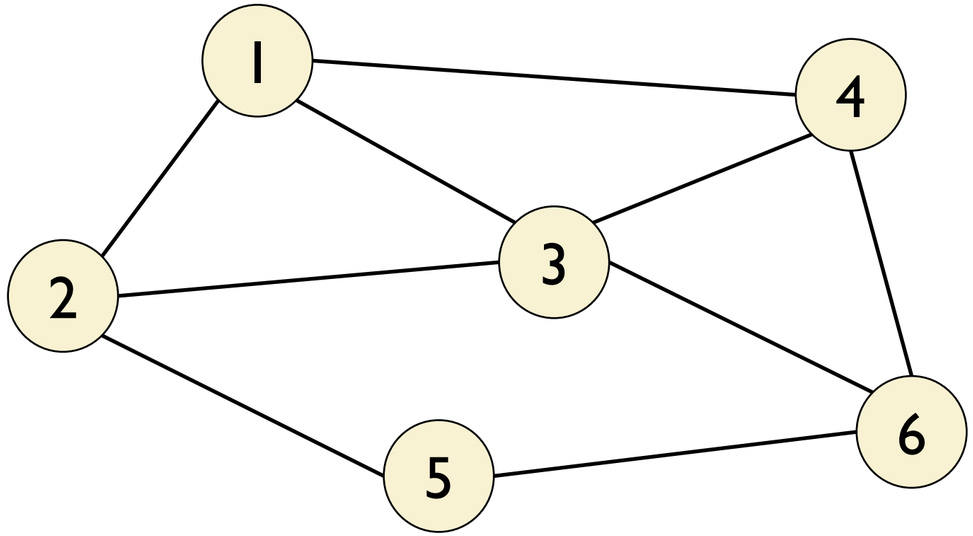
Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Implementation: Classiq, Cirq, PennyLane, Qrisp
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/5+o(1)})$ from [542], improving upon [252, 362]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring “semiprimes”, which are widely used in cryptography, is given in [271]. If small factors exist, Shor's algorithm can be beaten by a quantum algorithm using Grover search to speed up the elliptic curve factorization method [366]. Additional optimized versions of Shor's algorithm are given in [384, 386, 431]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

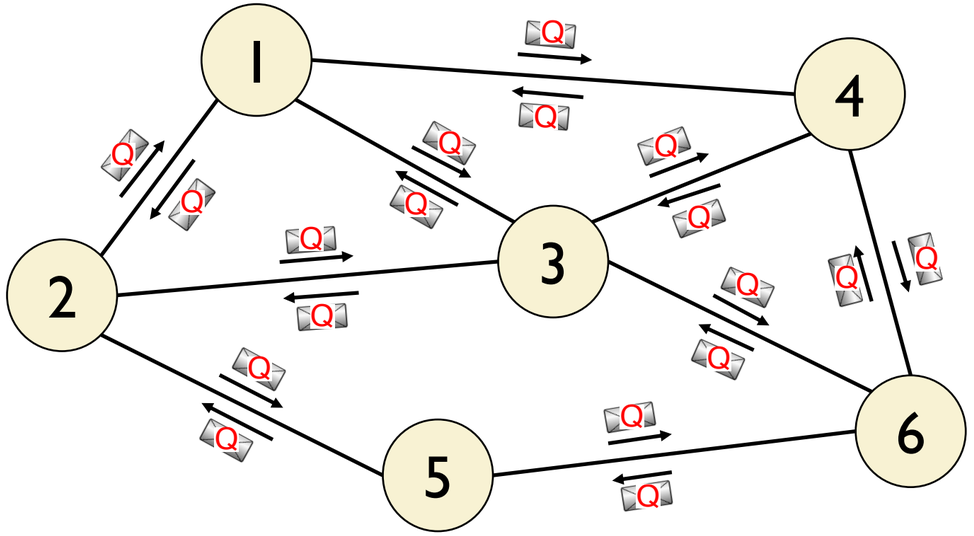
Algorithm: Discrete-log
Speedup: Superpolynomial
Implementation: Classiq, Qrisp
Description: We are given three *n*-bit numbers *a*, *b*, and *N*, with the promise that $b = a^s \mod N$ for some *s*. The task is to find *s*. As shown by Shor [82], this can be achieved on a quantum computer in

Quantum Distributed Computing

CLASSICAL



QUANTUM



Qubits can be sent instead of 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)

Outline of the Talk

1. Brief overview of quantum computing

2. Quantum distributed computing: Three main techniques

   - ✓ Quantum leader election (anonymous networks)
   - ✓ Quantum search (CONGEST model)
   - ✓ Quantum nonlocality (LOCAL model)

3. Open problems and Challenges

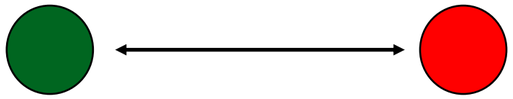
Quantum Leader Election [Tani et al. 05]

Model: anonymous networks

Classically, there is no zero-error bounded-time algorithm for leader election.

Quantumly, there is a zero-error bounded-time algorithm for leader election.

Consider the case of two players:



When each node owns a bit: four states 00, 01, 10, 11

the state of the system is a probability distribution

$$\begin{pmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{pmatrix} \quad \text{with } p_{ij} \geq 0 \text{ and } \sum_{ij} p_{ij} = 1$$

p_{ij} is the probability to be in state ij

When each node owns a quantum bit: from the first principle of Quantum Mechanics,

the state of the system is a wave function

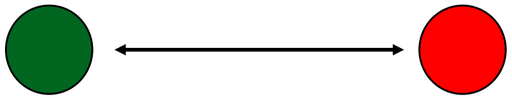
$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \quad \text{with } \alpha_{ij} \in \mathbb{C} \text{ and } \sum_{ij} |\alpha_{ij}|^2 = 1$$

$|\alpha_{ij}|^2$ is the probability to observe state ij

Quantum Leader Election [Tani et al. 05]

Model: anonymous networks

Second principle of Quantum Mechanics: quantum processes correspond to unitary matrices



Theorem ([Tani et al. 05]):

There is a "nice" unitary matrix that maps $\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ to $\begin{pmatrix}0\\1/\sqrt{2}\\1/\sqrt{2}\\0\end{pmatrix}$.
(can be implemented in a distributed way)

Initial state: 00 (symmetric)

Final state: uniform superposition of 01 and 10 (symmetric state)

Measuring it gives 01 w.p. 1/2 and 10 w.p. 1/2 (symmetry broken!)

When each node owns a quantum bit: from the first principle of Quantum Mechanics,

the state of the system is a wave function

$$\begin{pmatrix}\alpha_{00}\\\alpha_{01}\\\alpha_{10}\\\alpha_{11}\end{pmatrix}$$

with $\alpha_{ij} \in \mathbb{C}$ and $\sum_{ij}|\alpha_{ij}|^2 = 1$

$|\alpha_{ij}|^2$ is the probability to observe state ij

Quantum Leader Election [Tani et al. 05]

Model: anonymous networks

Generalizing this idea gives a zero-error quantum algorithm for leader election!
(the number of rounds is poly(n))

Main issue: the notion of zero-error quantum algorithm is problematic

- ✓ in quantum computing there will always be some noise
- ✓ even in the noiseless setting, the quantum algorithm can be implemented without error only if arbitrary (infinite-precision) quantum operations are allowed

Challenge: can a similar technique be useful for bounded-error setting?

Outline of the Talk

1. Brief overview of quantum computing

2. Quantum distributed computing: Three main techniques
   - ✓ Quantum leader election (anonymous networks)
   - ✓ Quantum search (CONGEST model)
   - ✓ Quantum nonlocality (LOCAL model)

3. Open problems and Challenges

Quantum Search (Grover 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 N calls to the black box, where $N = |X|$
("brute force search: try all the elements x")

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

Quantum search
[Grover 1996]

Application: 2-party communication complexity of the disjointness function

(Alice and Bob each has a subset of {1,2,…,N} as input, and they want to decide whether the intersection of the two subsets is empty or not)

Quantum communication complexity: $\Theta(\sqrt{N})$ qubits [Burhman, Cleve, Wigderson 1998]

Classical communication complexity: $\Theta(N)$ bits

Applications of Quantum Search

CONGEST model

[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.

idea (for the decision version): the diameter is at least d iff there is a vertex of eccentricity at least d

use quantum search to try to find such a vertex

Quantum advantage for important/natural problems (more applications in the next slide)

Is a $O(\sqrt{n})$-round quantum algorithm really faster than a $O(n)$-round classical algorithm?

Quantum CONGEST: Recent Developments

[Izumi, LG, Magniez STACS'20]

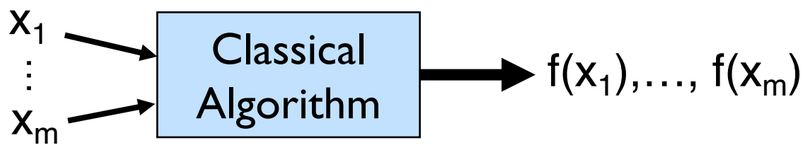
Quantum algorithms for triangle finding using distributed quantum search
(quantum: $\tilde{O}(n^{1/4})$ rounds, classical: $\tilde{O}(n^{1/3})$ rounds [Chang and Saranurak PODC'19]).

[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

[Fraigniaud, Luce, Magniez, Todinca PODC'24]

Quantum algorithms for cycle detection using distributed amplitude amplification

[Dufoulon, Magniez, Pandurangan PODC'25]

Quantum message complexity (i.e., communication complexity) for leader election and agreement using distributed quantum counting and quantum walks

Outline of the Talk

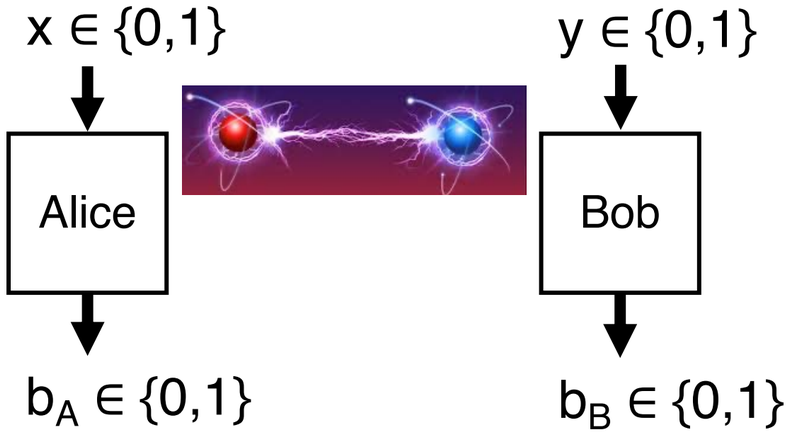
1. Brief overview of quantum computing

2. Quantum distributed computing: Three main techniques
   - ✓ Quantum leader election (anonymous networks)
   - ✓ Quantum search (CONGEST model)
   - ✓ Quantum nonlocality (LOCAL model)

3. Open problems and Challenges

Quantum Nonlocality

CHSH game [Clauser, Horne, Shimony, Holt 1969]



winning condition: $b_A \oplus b_B = xy$

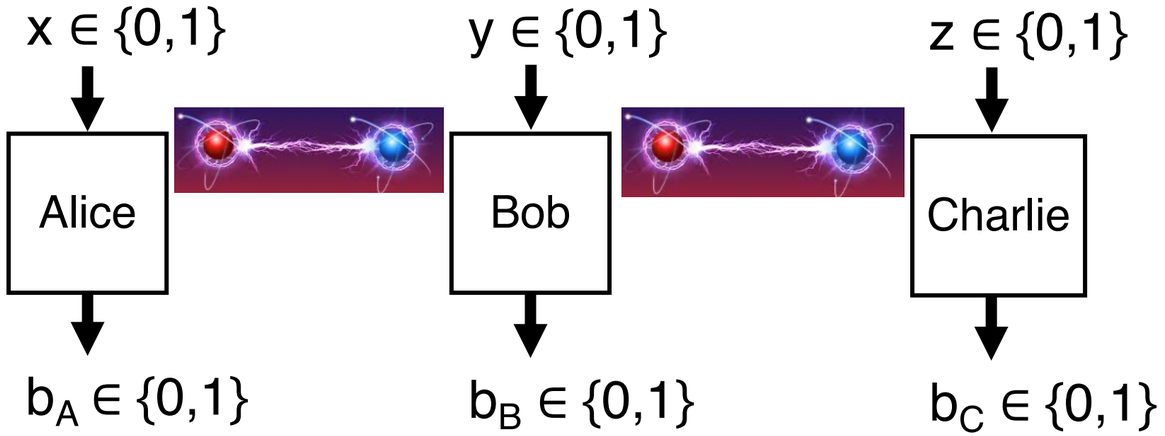
classically: cannot win with probability (when x,y are taken randomly) greater than 3/4
(this holds also if Alice and Bob have prior shared randomness)

quantumly: can win with probability ≈ 0.85 if Alice and Bob share entanglement
would like probability 1

entanglement: quantum version of shared randomness

Quantum Nonlocality

GHZ game



promise: $x + y + z \in \{0,2\}$

winning condition: $b_A \oplus b_B \oplus b_C = \frac{x+y+z}{2}$

To match the performance of the quantum model, we need at least 1 round of communication

classically: cannot win with probability greater than 3/4

quantumly: can win with probability 1 if Alice and Bob share entanglement

Application of Quantum Nonlocality

LOCAL model

Theorem [Balliu, Brandt, Coiteux-Roy, d'Amore, Equi, LG, Lievonen, Modanese, Olivetti, Renou, Suomela, Tendick, Veeren STOC'25]

In the LOCAL model, for any $\Delta \lesssim \log n$ there is a locally-checkable problem (based on the GHZ game) defined on a graph of degree Δ that can be solved in 1 round by a quantum algorithm but requires $\Theta(\Delta)$ rounds for any classical algorithm.

Idea: using 1 round, a quantum algorithm can share entanglement between any adjacent nodes, and then no communication is needed for playing the GHZ games

Main open question: can we show a similar quantum advantage on a bounded-degree graph (LCL problem)?

Recent result [Balliu, Casagrande, d'Amore, Keller, Lievonen, Olivetti, Schmid, Suomela SODA'26]

In the LOCAL model, there is a locally-checkable problem defined on a bounded-degree graph that can be solved in $O(\log n)$ rounds by a quantum algorithm but requires $\Omega(\log n \log^{0.99} \log n)$ rounds for any classical algorithm.

Question: can we get $O(1)$ vs. $\omega(1)$ for a bounded-degree graph?

Conclusions and Open Questions

- ✓ For anonymous networks, quantum advantage for zero-error leader election
- ✓ In the CONGEST model, several polynomial speedups for important graph-theoretic problems: diameter, clique detection, cycle detection, computing the girth…
- ✓ In the LOCAL model, quantum distributed algorithms can also be faster (even when considering locally-checkable problems!) for some “artificial” computational tasks

<u>Open problems:</u>

- ✓ Find other applications of quantum distributed algorithms in the CONGEST model
  - Other applications of the “distributed quantum search” recipe
  - New techniques (e.g., quantum walks)
- ✓ Find one “useful” application of quantum distributed algorithms in the LOCAL model
- ✓ Consider other models (e.g., MPC, asynchronous computation, faulty communication,..)

⇨ find a “killer application” of quantum distributed computing

Conclusions and Open Questions

- ✓ For anonymous networks, quantu
- ✓ In the CONGEST model, several
  diameter, clique detection, cycle c
- ✓ In the LOCAL model, quantum dis
  locally-checkable problems!) for s

Other topics: quantum local certification

(quantum certificates can be much shorter than classical certificates!)

[Fraigniaud, LG, Nishimura, Paz ITCS'21]

[LG, Miyamoto, Nishimura STACS'23]

[Hasegawa, Kundu, Nishimura PODC'24]

quantum Byzantine agreement

[Ben-Or and Hassidim STOC'05]

[Hajiaghayi, Kowalski, Olkowski ICALP'24]

Open problems:

- ✓ Find other applications of quantum distributed algorithms in the CONGEST model
  - Other applications of the "distributed quantum search" recipe
  - New techniques (e.g., quantum walks)
- ✓ Find one "useful" application of quantum distributed algorithms in the LOCAL model
- ✓ Consider other models (e.g., MPC, asynchronous computation, faulty communication,..)

⇨ find a "killer application" of quantum distributed computing