Open Problems in Quantum Information Processing

John Watrous
Department of Computer Science
University of Calgary

#1 Open Problem

Find new quantum algorithms.

Existing algorithms:

- Shor's Algorithm (+ extensions)

  - algorithms for: finding abelian hidden subgroups, hidden normal subgroups, and order of solvable groups; decomposing abelian groups; computing class numbers of quadratic number fields; solving Pell's equation.

#1 Open Problem

Find new quantum algorithms.

Existing algorithms:

- Grover's Algorithm + Amplitude Amplification.

    - many black box problems admit some polynomial speed-up: counting, finding collisions, searching spatial regions, …

#1 Open Problem

Find new quantum algorithms.

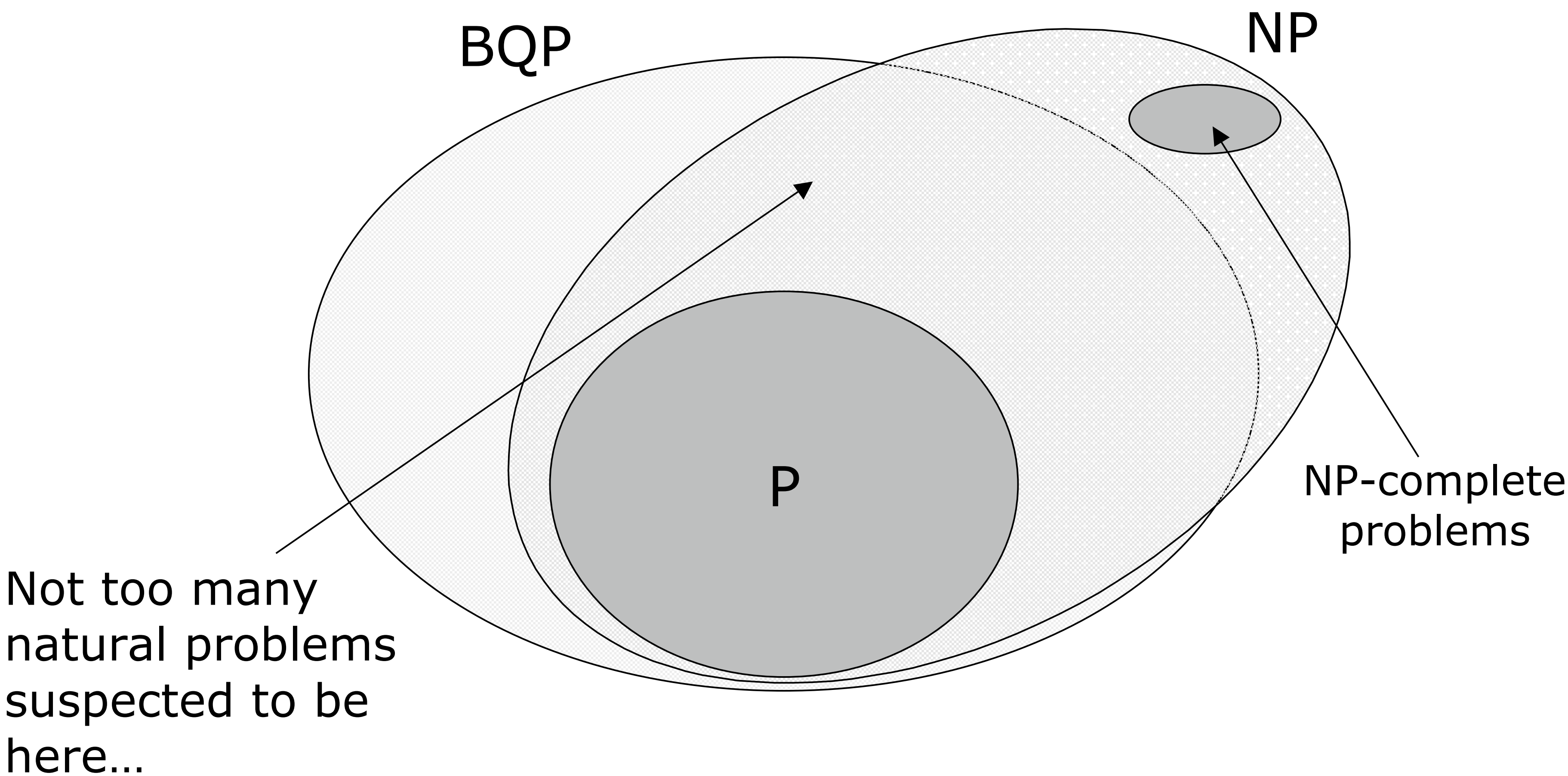
Existing algorithms:

- Graph reachability via quantum walks
  [Childs, Cleve, Deotto, Farhi, Gutmann, Spielman, 2002]

Application to a non-black-box problem?

#1 Open Problem

Find new quantum algorithms.



#1 Open Problem

Find new quantum algorithms.

Candidate problems:

- graph isomorphism
- group-theoretic problems
- lattice problems
- simulating physical systems

Warning: many have tried…

☆ Find new techniques. ☆

Weak Coin-Flipping

Is weak coin flipping with arbitrary bias possible?

Alice and Bob want to flip a fair coin, but one of them might be cheating… Alice wants heads, Bob wants tails.

Bias $\frac{1}{\sqrt{2}} - \frac{1}{2}$ is possible.

Bias ε requires $O\left(\log\log \varepsilon^{-1}\right)$ rounds.

Black-box Problems

Several open problems on black-box complexity:

- Improve the bound $D(f) = O\left(Q(f)^6\right)$ to $D(f) = O\left(Q(f)^2\right)$ for total functions.

- Is there a black box (promise) problem that admits an exponential quantum speed-up where the answer is invariant under permutation of the black box?

- Specific problems: finding triangles in graphs, searching a 2 dimensional region, AND-OR trees, equal or disjoint sets…

QMA

Identify natural problems in QMA.

Problems known to be in QMA:

- Local Hamiltonian problem
- Group Non-membership
- Approximate shortest vector in a lattice.

Is graph non-isomorphism in QMA?

Other complexity questions:

- Is BQP in the polynomial-time hierarchy?
- Is QIP = PSPACE? Is QIP = EXP?

Non-Distillability of NPT States

Do there exist non-distillable NPT states?

Let T denote the linear mapping corresponding to matrix transposition:

$$T(A) = A^T$$

Tensoring with the identity gives the **partial transpose**:

$$(T \otimes I)(A \otimes B) = A^T \otimes B$$

(extend by linearity).

Non-Distillability of NPT States

Do there exist non-distillable NPT states?

If ρ is separable, then $(T \otimes I)(\rho)$ is positive semidefinite.

If ρ is entangled, then $(T \otimes I)(\rho)$ may or may not be positive semidefinite:

$$(T \otimes I)(\rho) \geq 0 \quad \Leftrightarrow \quad \rho \text{ is PPT}$$

$$(T \otimes I)(\rho) \ngeq 0 \quad \Leftrightarrow \quad \rho \text{ is NPT}$$

If ρ is PPT, then $E_D(\rho) = 0$. Is there an NPT state ρ for which $E_D(\rho) = 0$?

Communication Complexity

There are many open questions about quantum communication complexity:

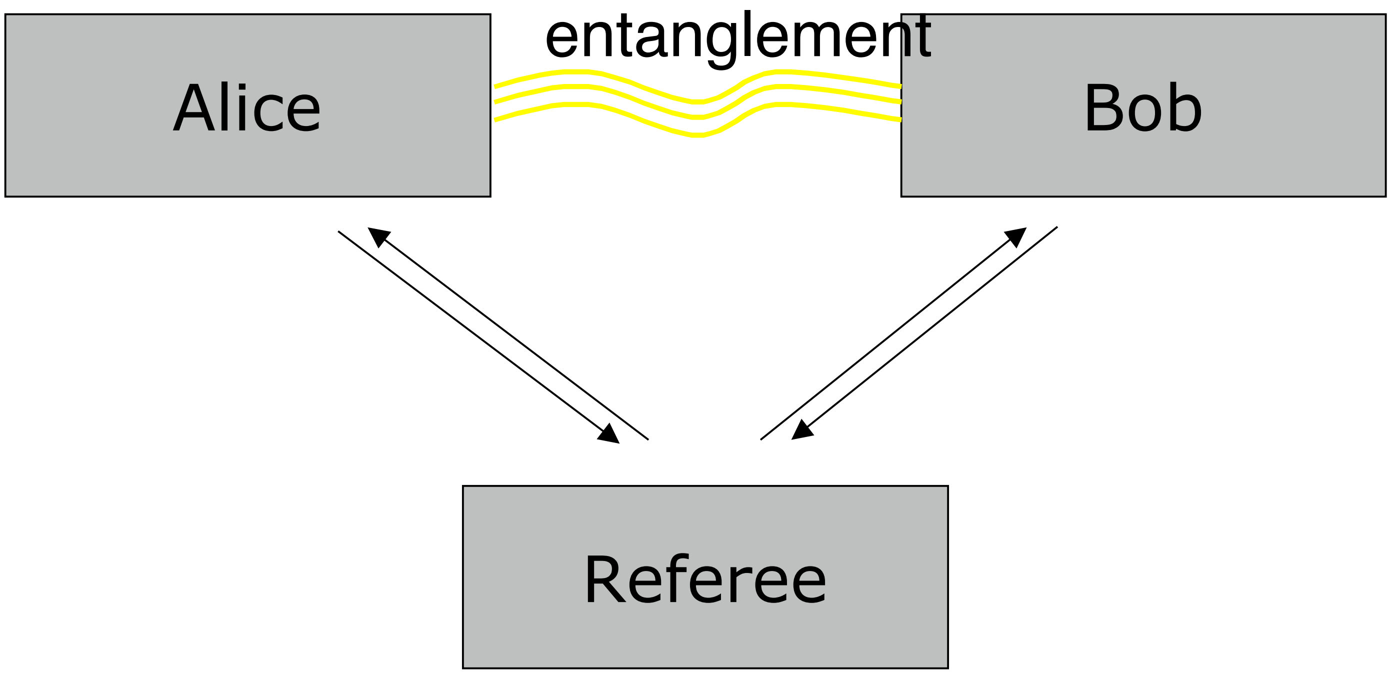
- Is there a total function for which an exponential savings in communication is possible in the quantum setting?

- How powerful is prior entanglement for quantum communication protocols?

- Find a problem for which one-way quantum communication is exponentially more efficient than one-way classical communication.

Non-locality and Multiple Provers

There are many open questions concerning non-locality.



Referee asks classical questions, Alice and Bob give classical answers… we are interested in the possible correlations in their answers.

Non-locality and Multiple Provers

There are many open questions concerning non-locality.

- How much classical communication would be needed for classical players Alice and Bob to “look quantum” to the referee.
- Cooperative games setting: how much entanglement is needed for Alice and Bob to play optimally?
- Does parallel repetition work?
- What is the power of multi-prover quantum interactive proofs.

Quantum Channel Capacities

There are many open questions concerning quantum channel capacities:

Unlike classical channels, quantum channels can have several different capacities (e.g., for sending quantum information or classical information, one-way or two-way communication, prior entanglement).

- Additivity questions.
- Relations between capacities.

Quantum Cryptography

Open questions in quantum cryptography:

- Identify candidate quantum one-way functions. Develop classical cryptographic systems that are secure against quantum attacks.

- Give a cryptographically good definition for quantum zero knowledge.

- Identification and relations among quantum cryptographic primitives.

Physical Implementations

- **Entanglement of spatially separated qubits**: Put two ions into physically separated ion traps into an entangled state. (Or a similar experiment.)

- **Characterize errors in quantum systems**: validate or invalidate error models. Develop methods to efficiently approximate errors.

- **Better fault-tolerant quantum computing schemes**

That’s all for now…