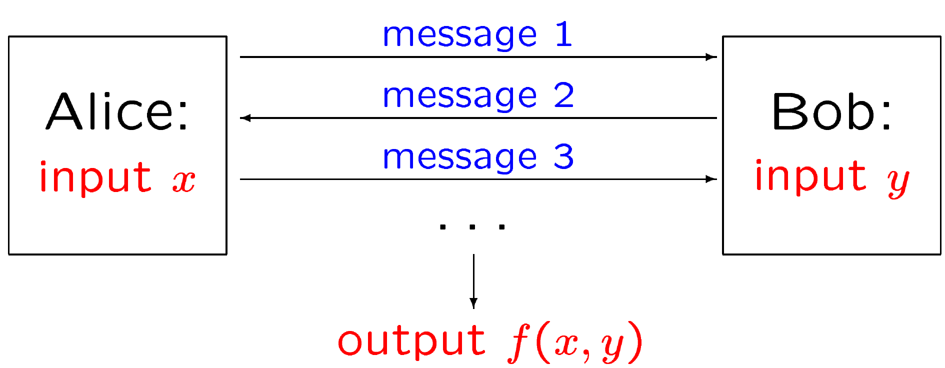
Quantum Communication Complexity

Ronald de Wolf

CWI Amsterdam

Communication Complexity

- Alice receives input $x \in \{0,1\}^n$,
  Bob receives input $y \in \{0,1\}^n$,
  and they want to compute
  $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$
  with minimal communication



- Well-studied classically
  (Yao 79, Kushilevitz & Nisan 97)

Example: Equality

- $\text{EQ}(x, y) = 1$ iff $x = y$

- Deterministic protocols need n bits
  Randomized: need only $O(\log n)$ bits

- Let $p_x(z) = x_1 + x_2 z + \cdots + x_n z^{n-1}$,
  choose field F with $|F| \geq 10n$

  1. Alice picks $z \in_R F$, sends $\underbrace{(z, p_x(z))}_{O(\log n) \text{ bits}}$

  2. Bob outputs whether $p_x(z) = p_y(z)$

  This works because:
  $x = y \Rightarrow p_x(z) = p_y(z)$ for all $z \in F$
  $x \neq y \Rightarrow p_x(z) \neq p_y(z)$ for most $z \in F$

Quantum Communication Complexity

- What if Alice and Bob have a quantum computer and can send each other qubits?

- Holevo's Theorem (73):
  k qubits cannot contain more information than k classical bits

- This suggests that

  quantum communication complexity
  =
  classical communication complexity
  ???

- Wrong!

Why Study Q Communication Complexity?

- For its own sake

- To get lower bounds for other models

- It proves exponential quantum-classical separations in a realistic model, as opposed to

  - Black-box algorithms (not realistic)

  - Factoring (no proven separation because we can't prove factoring $\notin$ P)

Disjointness Problem

- Informally: Alice and Bob want to schedule an appointment, and need to find a day where they are both free

- Formally: find i such that $x_i = y_i = 1$

- Classical protocols need almost n bits, even if we allow some error probability

- We can use Grover's quantum search to search for an intersection (BCW 98):

  $\sqrt{n}$ steps, each step takes $\approx \log n$ qubits of communication $\Longrightarrow \sqrt{n} \cdot \log n$ qubits

- Improved to $\sqrt{n} \cdot f(n)$ (Høyer&dW 02), $f(n)$ grows slower than $\log \log n$

Near-Optimal Lower Bound (Razborov 02)

- Quantum protocols for disjointness need to send at least $\sqrt{n}$ qubits

- Proof (technical):

  1. A q-qubit protocol gives a $2^n \times 2^n$ matrix (with trace norm $\leq 2^{n+2q}$) that is "close" to the communication matrix for disjointness

  2. Any such approximating matrix needs trace norm $\geq 2^{n+\sqrt{n}}$

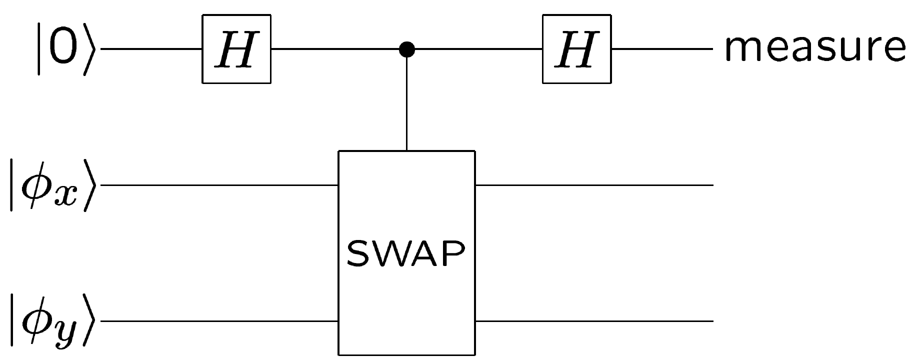
- Also holds if Alice and Bob start with fixed prior entanglement (such as EPR-pairs)

Quantum Fingerprinting (BCWW 01)

- $\underbrace{x}_{n \text{ bits}} \mapsto$ quantum fingerprint $\underbrace{|\phi_x\rangle}_{m \text{ qubits}}$

- If $|\phi_x\rangle, |\phi_y\rangle$ orthogonal, then we need $m = n$
  If almost orthogonal, $m \approx \log n$ suffices

- Equality test:



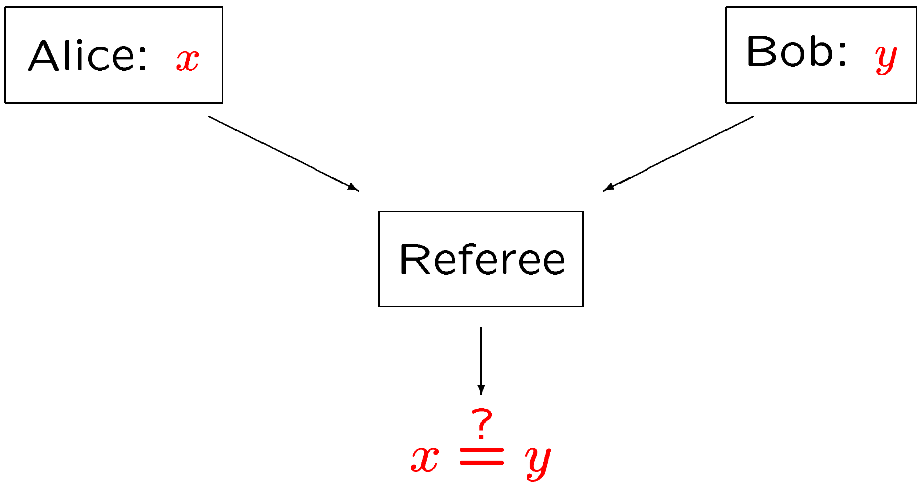
$|\phi_x\rangle = |\phi_y\rangle \Rightarrow$ measure 0
$|\phi_x\rangle \perp |\phi_y\rangle \Rightarrow$ measure random bit

How to Get Almost-Orthogonal $|\phi_x\rangle$

- $p_x(z) = x_1 + x_2 z + \cdots + x_n z^{n-1}$, $|F| = n/\varepsilon$
- $|\phi_x\rangle = \frac{1}{\sqrt{|F|}} \sum_{z \in F} |z\rangle |p_x(z)\rangle$
- $|\langle \phi_x | \phi_y \rangle| \leq \varepsilon$ if $x \neq y$
- $2 \log(n/\varepsilon) = 2 \log n + 2 \log(1/\varepsilon)$ qubits

Application: Simultaneous messages

- Constrained model of communication:



- We can solve this with $\approx 4 \log n$ qubits by sending fingerprints $|\phi_x\rangle$ and $|\phi_y\rangle$

- Classical lower bound: $\sqrt{n}$ bits (NS 96)

- Exponential separation!

Summary

- Communication complexity:
  how much communication do Alice and Bob need to compute $f(x, y)$?

- Two examples of quantum advantages:

  1. Disjointness (appointment scheduling):
     can be computed with $\approx \sqrt{n}$ qubits,
     classical protocols need $\approx n$ bits

  2. Equality (in 3-party model):
     can be computed with $\approx \log n$ qubits,
     classical protocols need $\approx \sqrt{n}$ bits