Quantum Communication Complexity

Ronald de Wolf

UC Berkeley

Overview of the Talk

1. The model of communication complexity (classical and quantum)

2. Examples of good quantum protocols

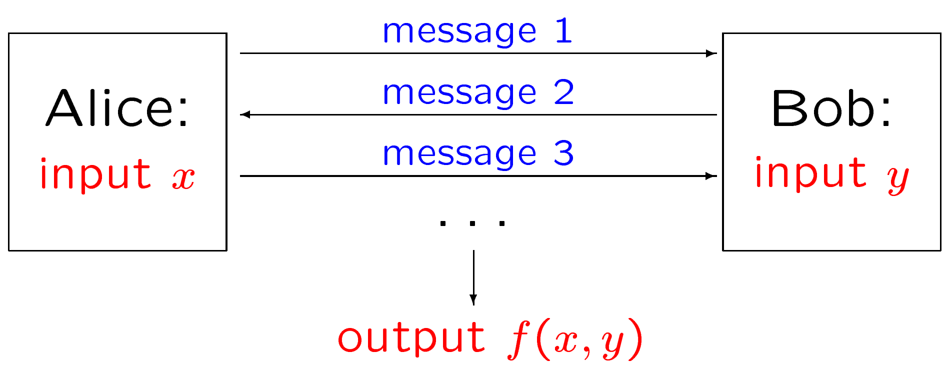
3. Known limitations of qcc

4. Questions you might want to work on

Communication Complexity

- Information theory + complexity theory

- 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

- $\mathrm{EQ}(x, y) = 1$ 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 $\underbrace{(z, p_x(z))}_{O(\log n)\ bits}$

  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)

Example 1: Distributed Deutsch-Jozsa

- Deutsch-Jozsa (black-box problem):
  Is $x_1 \dots x_n$ constant or balanced?

- Distributed Deutsch-Jozsa:
  Are x and y equal or at distance $n/2$?

- Efficient quantum protocol (BCW 98):

  1. Alice sends $|\phi\rangle = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$ (log n qubits)

  2. Bob changes to $|\psi\rangle = \sum_i (-1)^{x_i + y_i} |i\rangle$

  3. If $x = y$: $|\psi\rangle = \sum_i |i\rangle$
     If $d(x,y) = \frac{n}{2}$: $|\psi\rangle$ orthogonal to $\sum_i |i\rangle$

- Classical protocols need almost n bits

Example 2: Disjointness

- Are $x \subseteq [n]$ and $y \subseteq [n]$ disjoint sets?

- 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):

  $O(\sqrt{n})$ steps, each step takes $O(\log n)$ qubits of communication $\Longrightarrow$ $O(\sqrt{n}\log n)$ qubits

- Improved to $O(\sqrt{n}c^{\log^* n})$ (HW 02)

Example 3: Exponential separation (Raz 99)

- Alice gets $v \in \mathbb{R}^n$, orthogonal spaces M_0, M_1
  Bob gets a unitary U

  Promise: Uv is either in M_0 or in M_1
  Question: which one?

- $2 \log n$ qubit protocol:

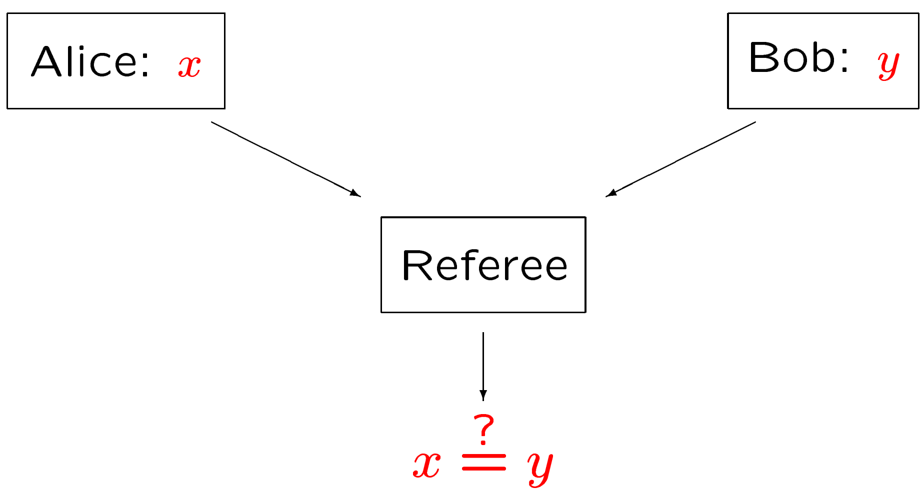
  1. Alice sends $|v\rangle$
  2. Bob sends back $U|v\rangle$
  3. Alice measures if $U|v\rangle \in M_0$ or M_1

- Classical protocols need $\dfrac{n^{1/4}}{\log n}$ bits
  (even if we allow error)

Example 4: Fingerprinting

- Quantum fingerprinting (BCWW 01):
  n-bit $x \Longrightarrow \log n$-qubit $|\phi_x\rangle$, s.t. $\langle \phi_x | \phi_y \rangle$ small

- Simultaneous message passing model:



- Quantum protocol: Alice sends $|\phi_x\rangle$,
  Bob sends $|\phi_y\rangle$, referee tests equality

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

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

Lower Bounds: Inner Product (CDNT 98)

- Inner product problem: $f(x,y) = x{\cdot}y$ mod 2

- Suppose a protocol computes f:
  $|x\rangle|y\rangle \mapsto (-1)^{x \cdot y} \underbrace{|x\rangle}_{\text{Alice}} \underbrace{|y\rangle}_{\text{Bob}}$

- Run the protocol on superposition of all y:
  $|x\rangle \sum_y |y\rangle \mapsto |x\rangle \sum_y (-1)^{x \cdot y} |y\rangle$

- Now a Hadamard transform gives Bob x!

- Then n bits have been communicated (Holevo)
  $\Longrightarrow$ protocol must have sent n qubits

Some General Lower Bounds

1. Protocols without error probability:

   - Consider communication matrix $M_f[x,y] = f(x,y)$, let $rank(M_f)$ be its rank.

     A protocol for f needs $\frac{\log rank(M_f)}{2}$ qubits

   - Equality, disjointness, and most other f: $rank(M_f) = 2^n \Rightarrow$ at least $n/2$ qubits

2. With small error probability:

   - Need log of "approximate rank" of M_f

   - Disjointness needs at least $\sqrt{n}$ qubits (Razborov 02)

Applications to Other Models

General idea: if communication complexity problem A can be embedded in problem B, then lower bounds on A imply lower bounds on B

For example, we can derive lower bounds on:

- Chip size
- Circuit size
- Automata size
- Data structure size

Interesting Open Problems

- Polynomial quantum-classical equivalence for all total functions?

- Exponential separation for 1-round protocols (with only one message)?

- Can EPR-pairs save communication?

  Superdense coding can save a factor of 2; public coin flips can save additive $\log n$ bits of communication. What else?