Quantum Communication

Ronald de Wolf

Overview of this lecture

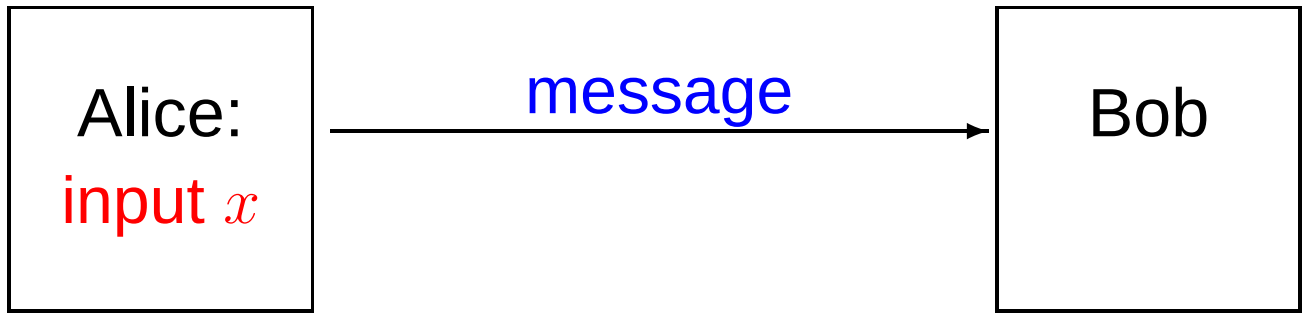
1. Quantum information
   + application to classical codes

2. Quantum communication complexity

3. Quantum cryptography

Quantum communication

- Typical situation: Alice has $x \in \{0,1\}^n$, which she wants to communicate to Bob



- A k-qubit message contains 2^k amplitudes! Can we pack this much classical information into it?
- Holevo's theorem (1973): if Alice sends k qubits, then any measurement that Bob can do gives him at most k bits of mutual information with Alice
- k qubits are no better than k bits (?)

Proof of weaker version

- Suppose you encode $x \in \{0,1\}^n$ in quantum state $|\phi_x\rangle \in \mathbb{C}^d$. With k qubits, $d = 2^k$
- Recover with measurement operators $\{M_x\}$ (probability of outcome x on state ϕ is $\mathsf{Tr}(M_x|\phi\rangle\langle\phi|)$, require $\sum_x M_x = I_d$)
- Success probability to recover x: $p_x = \mathsf{Tr}(M_x|\phi_x\rangle\langle\phi_x|) \leq \mathsf{Tr}(M_x)$
- $$\sum_{x\in\{0,1\}^n} p_x \leq \sum_x \mathsf{Tr}(M_x) = \mathsf{Tr}\left(\sum_x M_x\right) = \mathsf{Tr}(I_d) = d$$
- Average success probability is at most $d/2^n$
- If $d \ll 2^n$, then bad average success probability

Random access codes

- Bob cannot learn all bits of $x \in \{0,1\}^n$ from a k-qubit quantum message if $k < n$
- But could he learn any one bit x_i of his choice?
- Note that a measurement to learn x_i destroys the state
- Can encode 2 bits into 1 qubit:
  $|\phi_\alpha\rangle = \cos(\alpha)|0\rangle + \sin(\alpha)|1\rangle$
  Use $\alpha = \pi/8, 3\pi/8, 5\pi/8, 7\pi/8$ for $00, 10, 11, 01$
  To recover x_1: measure, success prob $\cos(\pi/8)^2 \approx 0.85$
  To recover x_2: rotate and measure, success prob 0.85
- In general there's not much improvement: if Bob can learn any bit x_i with probability $p > 1/2$ then (Nayak'00)

$$k \geq (1 - H(p))n$$

Application: Locally decodable codes

- Error-correcting code: $C : \{0,1\}^n \to \{0,1\}^m$, $m \geq n$

  decoding: $D(w) = x$ if w is "close" to $C(x)$

- Inefficient if you only want to decode a small part of x
- C is q-query locally decodable if there is a decoder D that only looks at q bits of w, and $D(w,i) = x_i$ (w.h.p.)
- Hard question: optimal tradeoff between q and m?
- Using quantum, KW03 show: $q = 2 \Rightarrow m \geq 2^{\Omega(n)}$
- Still the only superpolynomial bound known for LDCs

Exponential bound on 2-query LDC

- Given $C : \{0,1\}^n \to \{0,1\}^m$, 2-query classical decoder
- Can replace 2 classical queries by 1 quantum query!
- Some massaging: make the quantum query uniform
- Consider query-result $|\phi_x\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{C(x)_j} |j\rangle$
- $|\phi_x\rangle$ has $\log m$ qubits, but allows us to predict each of the encoded bits $x_1, \ldots, x_n$
- Random access code bound: $\log m \geq \Omega(n)$

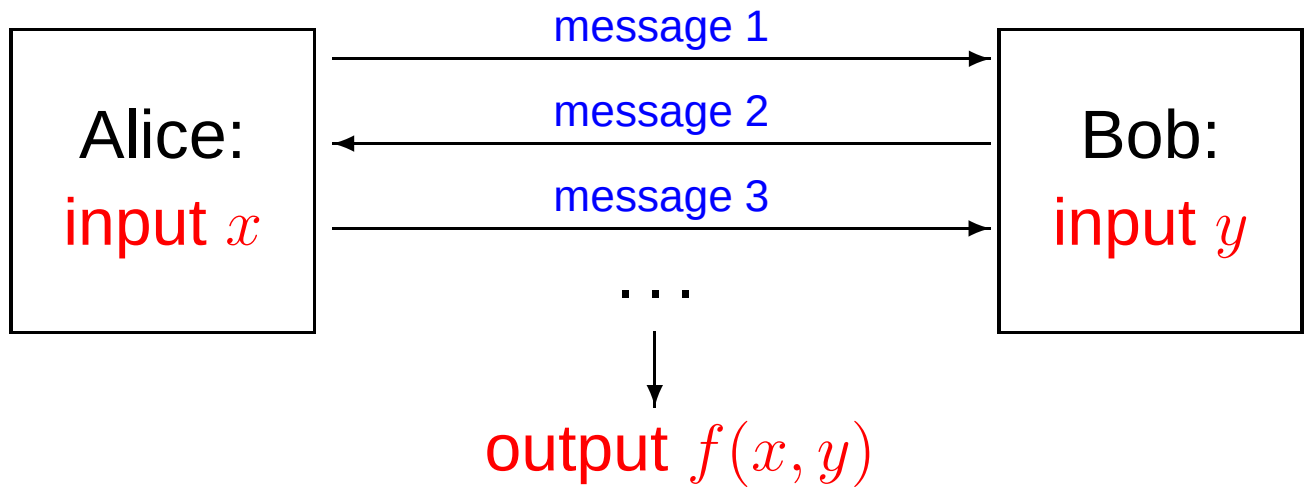
  $\Rightarrow$ 2-query LDCs need exponential length $m \geq 2^{\Omega(n)}$

Part 2:

Quantum communication complexity

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

- EQ$(x, y) = 1$ iff $x = y$
- Deterministic protocols need n bits
  Randomized: need only $O(\log n)$ bits
- Define polynomial $p_x(z) = x_1 + x_2 z + \cdots + x_n z^{n-1}$,
  over field $\mathbb{F}$ with $|\mathbb{F}| \geq 10n$
  1. Alice picks $z \in_R \mathbb{F}$, sends $\underbrace{z \text{ and } p_x(z))}_{O(\log n)\ bits}$
  2. Bob outputs whether $p_x(z) = p_y(z)$
- This works because:
  $x = y \Rightarrow p_x(z) = p_y(z)$ for all $z \in \mathbb{F}$
  $x \neq y \Rightarrow p_x(z) \neq p_y(z)$ for most $z \in \mathbb{F}$, because
  $p_x - p_y$ has degree $< n$, so $< n$ zeroes

Quantum communication complexity

- What if Alice and Bob have a quantum computer and can send each other qubits?
- Holevo's theorem: k qubits cannot contain more information than k classical bits
- This suggests that

$$\text{quantum communication complexity}$$
$$=$$
$$\text{classical communication complexity}$$
$$?$$

- Wrong!

Why study this?

- For its own sake
- To get lower bounds for other models:
  data structures, circuits, streaming algorithms, . . .
- It proves exponential quantum-classical separations
  in a realistic model,
  as opposed to
  - Factoring (Shor doesn't give us a proven separation,
    because we don't know if factoring $\notin$ P)
  - Query algorithms (not realistic)

Example 1: Distributed Deutsch-Jozsa

- Deutsch-Jozsa (black-box problem):
  Is bitstring $z_1 \ldots z_N$ constant or balanced?
- Distributed Deutsch-Jozsa:
  Are x and y equal or at distance $N/2$?
- Efficient quantum protocol (BCW 98):
  1. Alice sends $|\phi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} (-1)^{x_i} |i\rangle$ ($\log N$ qubits)
  2. Bob changes to $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_i (-1)^{x_i + y_i} |i\rangle$,
     measures in a basis containing $|U\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$
  3. If $x = y$: $|\psi\rangle = |U\rangle$

     If $(x, y) = \frac{N}{2}$: $|\psi\rangle$ is orthogonal to $|U\rangle$
- Classical protocols need to send 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 algorithm to search for an intersection (BCW 98):

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

- Improved to $O(\sqrt{N})$ (AA 02), optimal (Razborov 01)

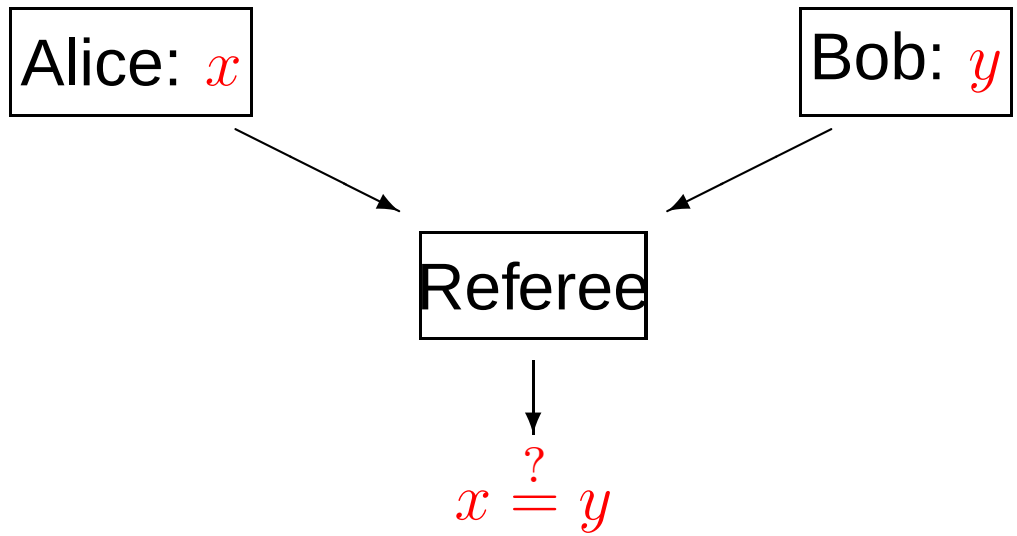
Example 3: Exponential separation

- 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 applies U and sends back $U|v\rangle$
  3. Alice measures if $U|v\rangle \in M_0$ or M_1
- Raz 99: Classical protocols need to send $\approx \sqrt{n}$ 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 ("Swap test")
- Classical lower bound: $\sqrt{n}$ bits (NS 96)

Lower bounds: Inner product

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

$$|x\rangle \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle \mapsto |x\rangle \underbrace{\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle}_{H|x\rangle}$$

- Now a Hadamard transform gives Bob x!
- Then n bits have been communicated $\Longrightarrow$
  protocol must have sent n qubits (CDNT'98, via Holevo)

Teleportation (BBCJPW'93)

- Power of entanglement: using an EPR-pair, we can send an unknown qubit over a classical channel
- Start with $(\alpha|0\rangle_A + \beta|1\rangle_A)\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
- Alice applies $(H \otimes I)C$. Result:

  $\frac{1}{2}|00\rangle_A(\alpha|0\rangle_B + \beta|1\rangle_B)+$
  $\frac{1}{2}|01\rangle_A(\alpha|1\rangle_B + \beta|0\rangle_B)+$
  $\frac{1}{2}|10\rangle_A(\alpha|0\rangle_B - \beta|1\rangle_B)+$
  $\frac{1}{2}|11\rangle_A(\alpha|1\rangle_B - \beta|0\rangle_B)$
- Alice measures her two qubits and sends Bob result (2 classical bits!)
- Bob then knows how to change his qubit to $\alpha|0\rangle + \beta|1\rangle$ e.g., if he received 01 then he applies an X

Part 3:

Quantum cryptography

Cryptography

- Alice wants to send message $M \in \{0,1\}^n$ to Bob
- The goal is not minimal communication, but secrecy: a third party (Eve) tapping the channel should not get information about the message
- If Alice and Bob share a secret key $K \in \{0,1\}^n$ then Alice can send $C = M \oplus K$ over the channel
- Bob learns M, but Eve learns nothing about M from C
- How can we make Alice and Bob share a secret key?
- Classically this is impossible, but with quantum communication it can be done

Quantum key distribution (BB 84)

- Basis 0: $\{|0\rangle, |1\rangle\}$, Basis 1: $\{|+\rangle, |-\rangle\}$
- Alice chooses n random bits $a_1, \ldots, a_n$ and n random bases $b_1, \ldots, b_n$. She sends a_i to Bob in basis b_i
- Bob chooses random bases $b'_1, \ldots, b'_n$ and measures the qubits he received, yielding bits $a'_1, \ldots, a'_n$
- Alice sends Bob all b_i
- $\approx n/2$ i's: $b_i = b'_i$ hence $a_i = a'_i$ (unless Eve tampered)
- Use half of those bits to check for tampering/noise: information vs disturbance tradeoff
- Rest: key of roughly $n/4$ shared bits
- Classical postprocessing: reconcilliation, privacy amplification

Building quantum computers?

- The main problem: quantum systems are very fragile. We need to simultaneously
  - Isolate them from the environment
  - Operate on them very precisely
- Strong effort going on around the world. Approaches:
  - Nuclear magnetic resonance (factored $15 = 3 \times 5$ on a 7-qubit computer in 2001)
  - Electron spins
  - Ion traps
  - Solid state
  - Optics (quantum crypto)
- Hard to predict if/when a QC will be built. . .

Summary: quantum communication

- Holevo's theorem:
  k qubits contain at most k bits of information

- Still, we can sometimes exponentially improve communication complexity with a quantum channel

- Quantum cryptography allows Alice and Bob
  to obtain a secret shared key

Summary of the whole course

- The world is quantum, so the strongest computers that nature allows us are quantum computers
- This is fundamental for the theory of computation, but could also have big practical consequences
- Computation: strong algorithms, like Shor and Grover
- Communication: reduce communication complexity, quantum key distribution

- Much more that I didn't talk about...