Quantum Communication

Wim van Dam
HP Labs – MSRI – UC Berkeley

SQUINT 3

June 16, 2003

Introduction

- *Communication complexity* deals with distributed problems.
- Quantum communication allows the use of entangled quantum states and/or the transmission of quantum bits.
- “Quantum properties” can reduce the necessary amount of communication.

Quantum Information

- A quantum bit or qubit: $|x\rangle = \alpha|0\rangle + \beta|1\rangle$
- In general for n qubits: $|x_1 \cdots x_n\rangle = \sum_{z \in \{0,1\}^n} \alpha_z |z\rangle$
- The α_z amplitudes are complex valued and ℓ_2 normalized.
- Probability of observing “z” is $|\alpha_z|^2$.

Entangled Qubits

- Two qubits distributed over parties A and B:

$$\left|\mathrm{EPR}_{AB}\right\rangle = \frac{1}{\sqrt{2}}\left|0_A 0_B\right\rangle + \frac{1}{\sqrt{2}}\left|1_A 1_B\right\rangle$$

- Similar for three parties:

$$\left|\mathrm{GHZ}_{ABC}\right\rangle = \frac{1}{\sqrt{2}}\left|0_A 0_B 0_C\right\rangle + \frac{1}{\sqrt{2}}\left|1_A 1_B 1_C\right\rangle$$

- Such quantum states have nonlocal features that cannot be reproduced with classical correlations.

Operations on Qubits

- Unitary transformation of n qubits is a 2^n dimensional unitary transformation $\in U(2^n)$.

- Three important single-qubit examples:
  - Hadamard H transform:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

  - NOT gate: $\mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

  - ϕ-Phase change: $R_\phi(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta\, e^{i\phi}|1\rangle$

Quantum Communication

- With quantum communication we allow the parties to communicate with qubits and to use the quantum correlations of EPR pairs etc.
- At least as strong as classical communication
- ‘Superdense coding’ and ‘teleportation’ give some quantum advantages, but is there more?

Superdense Coding

Let A and B share an EPR pair $\frac{1}{\sqrt{2}}|0_A 0_B\rangle + \frac{1}{\sqrt{2}}|1_A 1_B\rangle$
A will send 2 bits to B.

1) A applies one of the 4 gates I, NOT, R_π, NOT$\cdot R_\pi$ to her part of the EPR pair and sends it to B.

2) B measures which one of the 'Bell states' it now has, which gives him two bits of information from A.

$$\begin{cases} \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\ \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle \\ \frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|01\rangle \end{cases}$$

"1 qubit+EPR = 2 classical bits"

Teleportation

Let A and B share an EPR pair $\frac{1}{\sqrt{2}}|0_A 0_B\rangle + \frac{1}{\sqrt{2}}|1_A 1_B\rangle$
A will send a qubit $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ to B.

1) A measures x and her part of the EPR pair in the 'Bell basis'. Depending on the outcome, B's part of the EPR pair has now become: x, NOT(x), $R_\pi(x)$, or $\mathrm{NOT}\cdot R_\pi(x)$.

$$\begin{cases} \alpha|0\rangle + \beta|1\rangle \\ \alpha|1\rangle + \beta|0\rangle \\ \alpha|0\rangle - \beta|1\rangle \\ \alpha|1\rangle - \beta|0\rangle \end{cases}$$

2) A tells B the outcome (2 bits), with which B can correct his part to x.

Holevo's and Other Bounds

- If A sends n uncorrelated qubits to B, then B can receive no more than n bits of information.
- If A and B share entanglement, B can get 2n bits of information, but not more than that.

- The teleportation of a qubit requires 2 bits.

- All this suggests that "1 qubit = 2 c-bits" when there is entanglement, and nothing more…

Communication Complexity

Consider two parties A and B, with private inputs $x=x_1 \ldots x_n$ and $y=y_1 \ldots y_n$ of n bits.

How much communication is necessary to compute the distributed function f(x,y)?

The number of bits (as a function of n) is the *communication complexity* CC(f) of the function.
Clearly: $CC(f) \leq n$ for all functions f.

Some Examples

- Equality function: f(x,y) = EQ(x,y) = “x=y”? deterministic complexity is maximal: CC(EQ)=n
- “x+y even or odd?” has one bit complexity.
- If we allow a small error ε: $CC_{\varepsilon}(EQ) = O(1)$.
- Communication complexity is important for parallel computation, understanding of intrinsic complexity of problems, etc.

Even/Odd Problem

- Consider three parties A, B and C that have three numbers x, y and z $\in$ R
  - Promise: x+y+z is a natural number
  - Question: is x+y+z even or odd?

- With GHZ entanglement, this can be solved exactly with three classical bits of communication. (The bits are publicly announced and we want everybody to know the answer in the end.)

- Classically, we need 5 bits for this task.

The GHZ Solution (1)

- Start with distributed GHZ state

$$\left|\mathrm{GHZ}_{ABC}\right\rangle = \frac{1}{\sqrt{2}}\left|0_A 0_B 0_C\right\rangle + \frac{1}{\sqrt{2}}\left|1_A 1_B 1_C\right\rangle$$

- Each party applies phase rotation R with angle proportional to x,y and z, which yields:

$$\frac{1}{\sqrt{2}}\left|0_A 0_B 0_C\right\rangle + \frac{1}{\sqrt{2}} e^{i\pi(x+y+z)}\left|1_A 1_B 1_C\right\rangle$$

$$= \begin{cases} \frac{1}{\sqrt{2}}\left(\left|0_A 0_B 0_C\right\rangle + \left|1_A 1_B 1_C\right\rangle\right) & \text{if } x+y+z \text{ is even} \\ \frac{1}{\sqrt{2}}\left(\left|0_A 0_B 0_C\right\rangle - \left|1_A 1_B 1_C\right\rangle\right) & \text{if } x+y+z \text{ is odd} \end{cases}$$

The GHZ Solution (2)

- Next, each party applies the H transform:

$$\begin{cases} \frac{1}{2}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right) & \text{if } x+y+z \text{ is even} \\ \frac{1}{2}\left(|001\rangle + |010\rangle + |100\rangle + |111\rangle\right) & \text{if } x+y+z \text{ is odd} \end{cases}$$

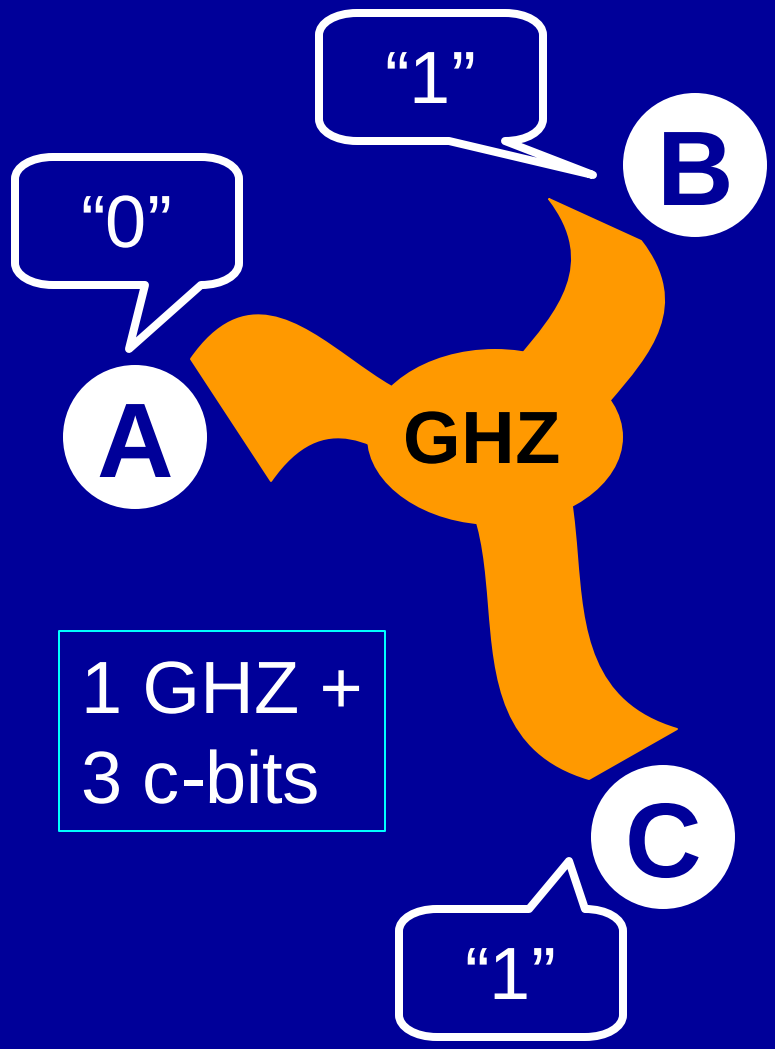
- Parties measure their qubits, and broadcast the observed bit value.

- The parity of these three bits is the correct answer to the “even/odd?” question

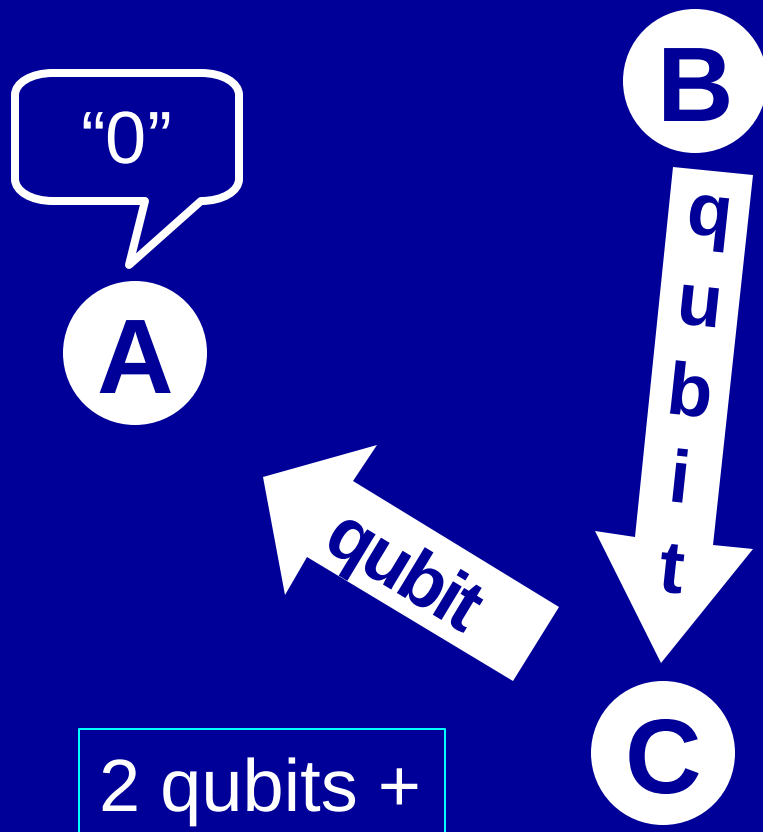
Complexity of Even/Odd

- Not hard to see that the classical, deterministic 3-party complexity is 5 bits.
- In general for k parties: QCC(E/O) = k, whereas classical CC(E/O) = $\Omega(k \log(k))$.
- This was the GHZ–Mermin nonlocality proof in disguise of a communication task.
- *Without entanglement*, the parties can also do it by passing on qubits $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}} e^{i\pi x}|1\rangle$.

The Two Ways of Solving E/O



1 GHZ +
3 c-bits



2 qubits +
1 c-bit

The Appointment Problem

- Two diaries with n days: $x_1 \ldots x_n$ and $y_1 \ldots y_n$
- Is there a day j such that $x_j = y_j =$ “free”?

- Buhrman, Cleve and Wigderson showed:

$$QCC_{\varepsilon}(APP_n) = O(\log n \cdot \sqrt{n})$$

- While we have the classical lower bound

$$CC_{\varepsilon}(APP_n) = \Omega(n)$$

log n·Ön Protocol for APP_n

A and B do a quantum search among the n days, which requires $\sqrt{n}$ rounds of log n qubits:

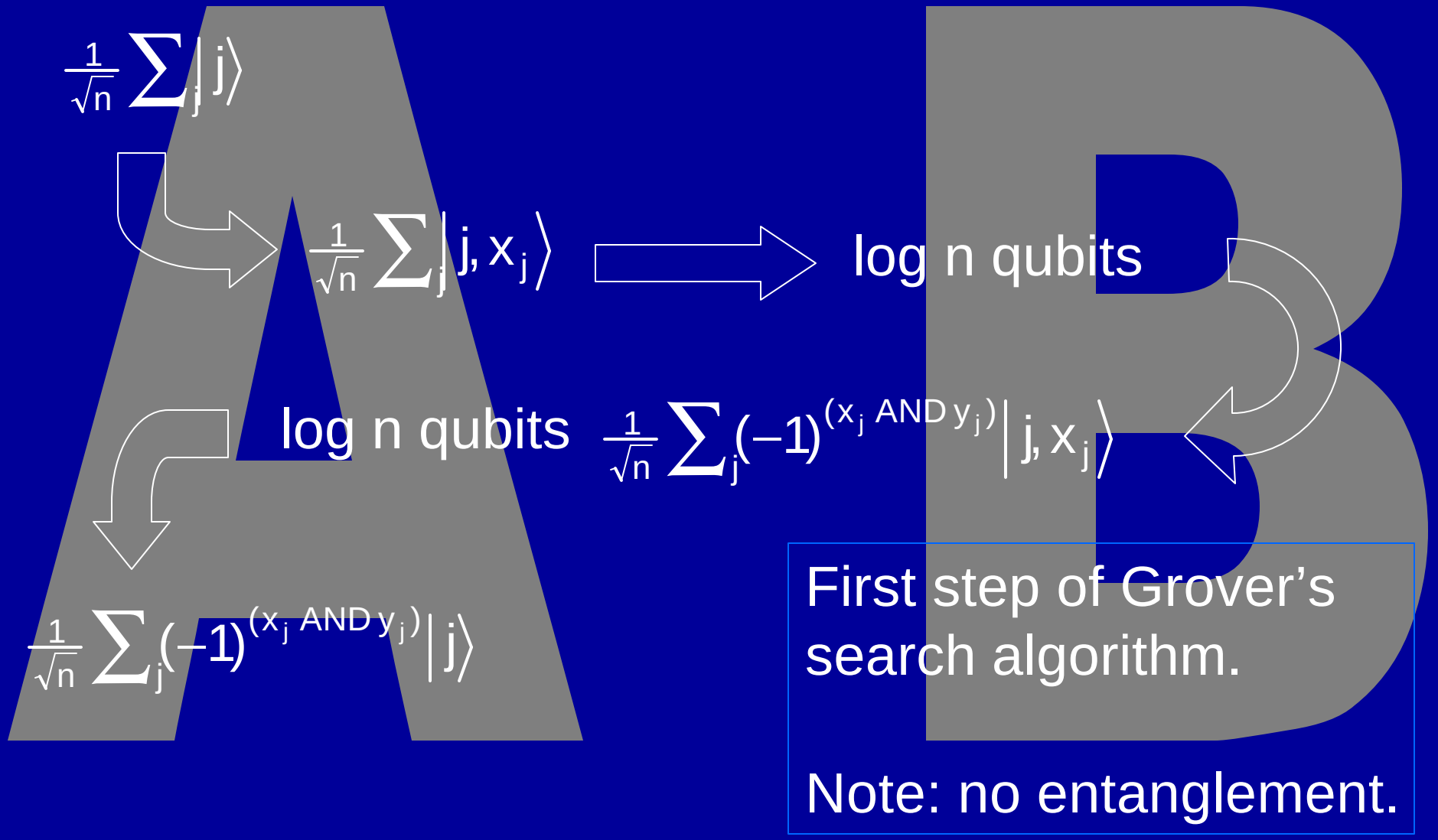
$$\sum_{j=1}^{n} \alpha_j |j\rangle \quad \mapsto \quad \sum_{j=1}^{n} (-1)^{(x_j \text{ AND } y_j)} \cdot \alpha_j |j\rangle$$

First A sends the log n qubits of $\sum_j \alpha_j |j, x_j\rangle$ to B.

Next, B changes this to $\sum_j (-1)^{(x_j \text{ AND } y_j)} \cdot \alpha_j |j, x_j\rangle$ and returns it to A.

A uncomputes x_j to get $\mapsto \sum_j (-1)^{(x_j \text{ AND } y_j)} \cdot \alpha_j |j\rangle$

The 1st Round for APP_n



First step of Grover's search algorithm.

Note: no entanglement.

More on Appointment Problem

- Ambainis and Aaronson improved it to

$$QCC_{\varepsilon}(APP_n) = O(\sqrt{n})$$

- Razborov proved that this is optimal.

- The Appointment Problem is an important, natural task (without a promise like even/odd?) that has a quadratic quantum speed-up.

- What is the power of quantum communication?
- What is the difference between CC_{ε} and QCC?

Other QCC Results

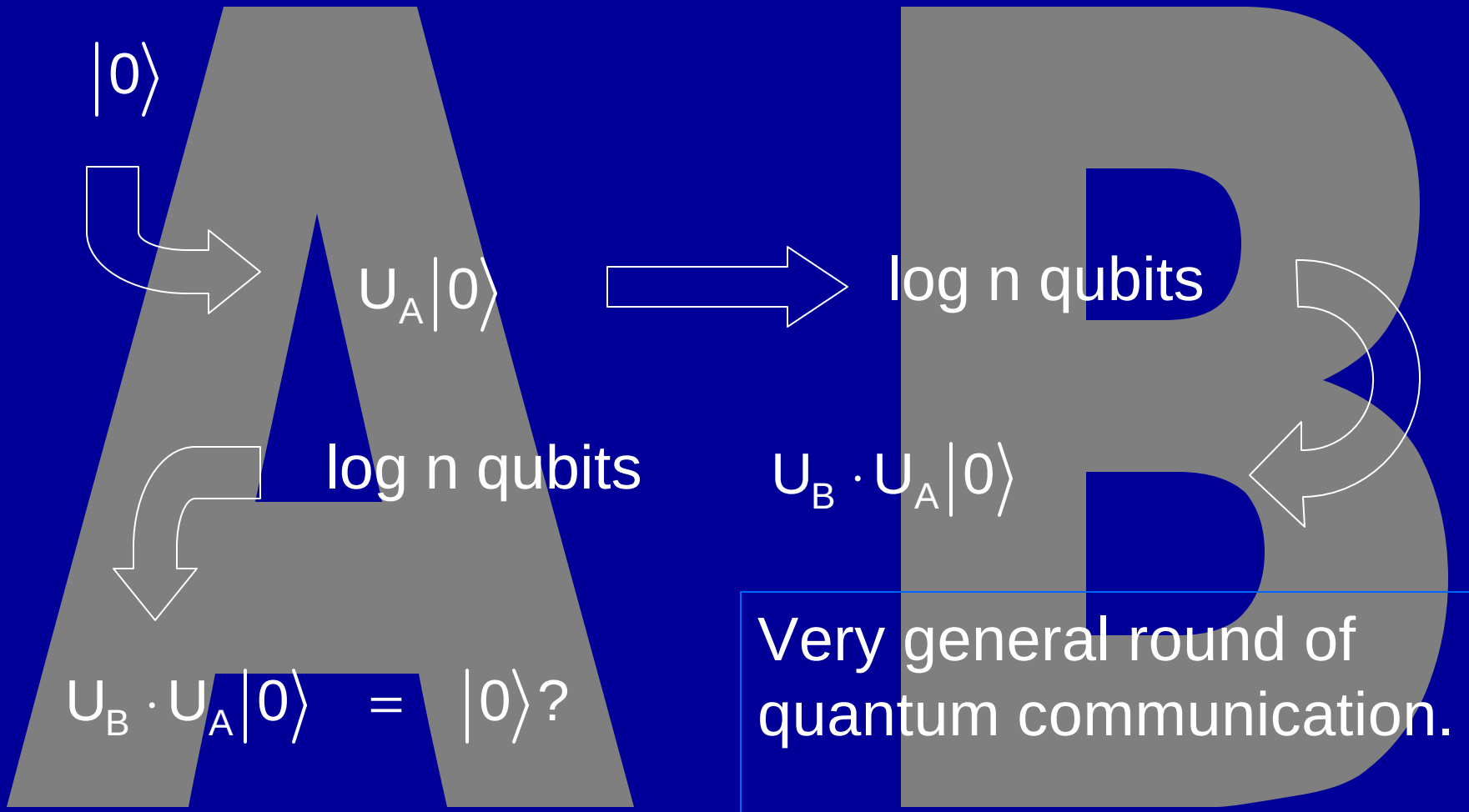
- Certain functions do not allow a quantum reduction in the communication complexity

$$\text{Inner Product}(x,y) = \sum_j x_j y_j \bmod 2$$

(Proof uses Holevo's bound.)

- [Raz]: There is a promised task with an exponential gap between classical and quantum complexity: "Is the unitary rotated vector $U_B \cdot U_A |0\rangle$ close to $|0\rangle$ or not?"

The Round for Raz's Problem



Very general round of quantum communication.

Again: no entanglement.

Open Problems

- Are there better than quadratic quantum improvements for natural problems?

- Is “classical communication+entanglement” more powerful than “quantum communication without (initial) entanglement”?
  No known example thus far…

- Who will be the first to implement a truly efficient quantum communication protocol?