# Quantum One-Way Communication can be Exponentially Stronger than Classical Communication


Bo'az Klartag

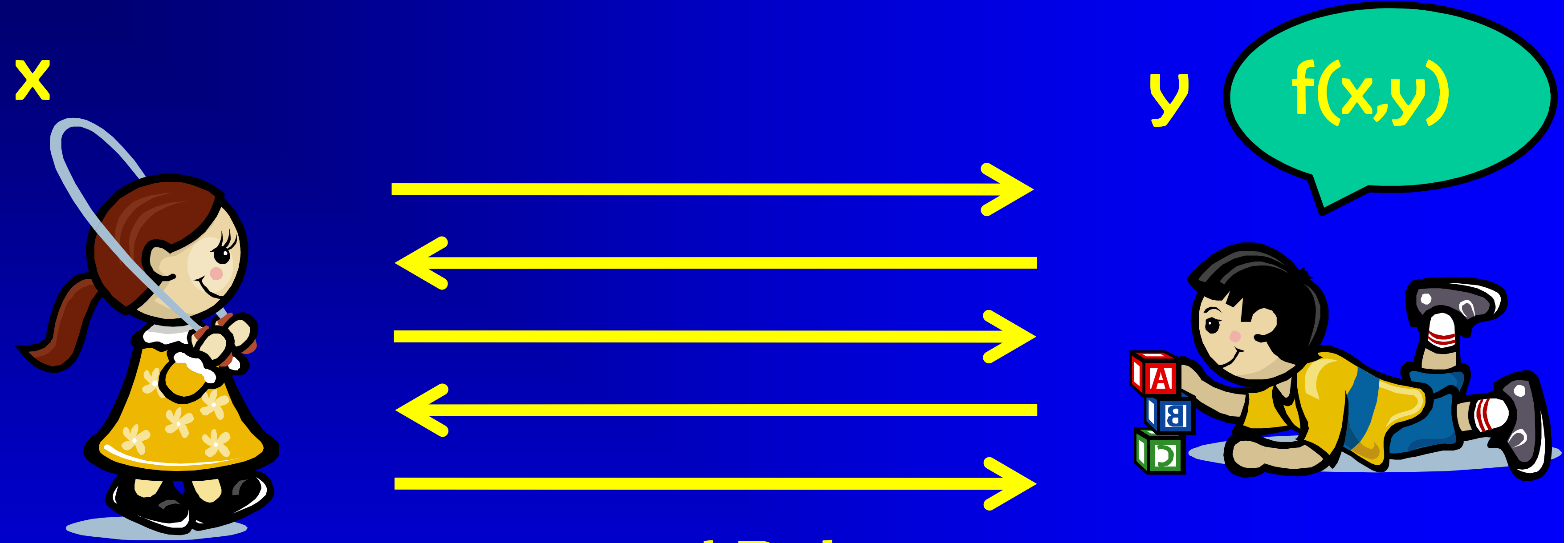
Tel Aviv University

Oded Regev

Tel Aviv University &

CNRS, ENS, Paris

# Communication Complexity




- Alice is given input x and Bob is given y
- Their goal is to compute some (possibly partial) function f(x,y) using the minimum amount of communication
- Two central models:
    1. Classical (randomized bounded-error) communication
    2. Quantum communication

# Relation Between Models

- [Raz'99] presented a function that can be solved using O(logn) qubits of communication, but requires poly(n) bits of randomized communication
- Hence, Raz showed that:

  quantum communication
  can be exponentially stronger than
  classical communication

- This is one of the most fundamental results in the area

# Is One-way Communication Enough?

- Raz's quantum protocol, however, requires two rounds of communication
- This naturally leads to the following fundamental question:

Can quantum one-way communication

be exponentially stronger than

classical communication?

# Previous Work

- [BarYossef-Jayram-Kerenidis'04] showed a relational problem for which quantum one-way communication is exponentially stronger than classical one-way
- This was improved to a function by [Gavinsky-Kempe-Kerenidis-Raz-deWolf'07]
- [Gavinsky'08] showed a relational problem for which quantum one-way communication is exponentially stronger than classical communication

# Our Result

- We present a function with a O(logn) quantum one-way protocol that requires poly(n) communication classically
- Hence our result shows that:

**quantum one-way communication can be exponentially stronger than classical communication**

- This might be the strongest possible separation between quantum and classical communication

# Vector in Subspace Problem

[Kremer95,Raz99]


- Alice is given a unit vector $v \in \mathbb{R}^n$ and Bob is given an n/2-dimensional subspace $W \subseteq \mathbb{R}^n$
- They are promised that either

  $v$ is in $W$ or $v$ is in $W^\perp$

- Their goal is to decide which is the case using the minimum amount of communication

# Vector in Subspace Problem

- There is an easy logn qubit one-way protocol
  - Alice sends a logn qubit state corresponding to her input and Bob performs the projective measurement specified by his input
- No classical lower bound was known
- We settle the open question by proving:

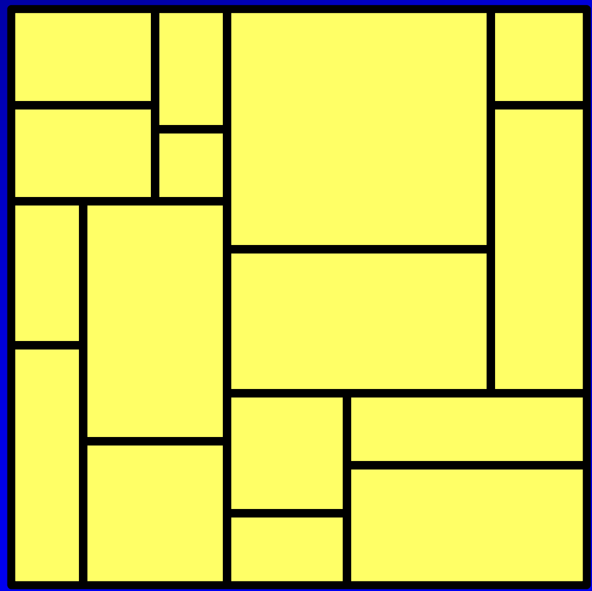
$$R(VIS)=\Omega(n^{1/3})$$

- This is nearly tight as there is an $O(n^{1/2})$ protocol

# The Proof

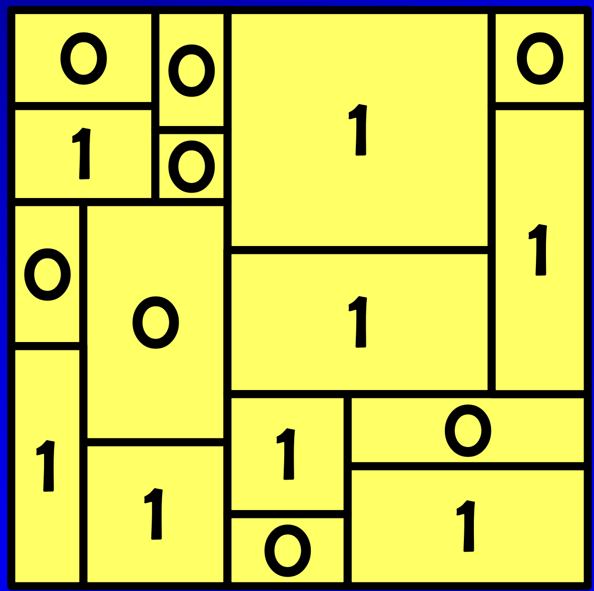
# The Rectangle Bound

- We prove our lower bound using a standard method known as the rectangle bound:



# The Rectangle Bound

- We prove our lower bound using a standard method known as the rectangle bound:




- This reduces the problem to a clean mathematical question, described next…

# Being on the Equator is Great!

# Unfortunately, only 21.3% of the equator is land

Even though 29.2% of earth is land

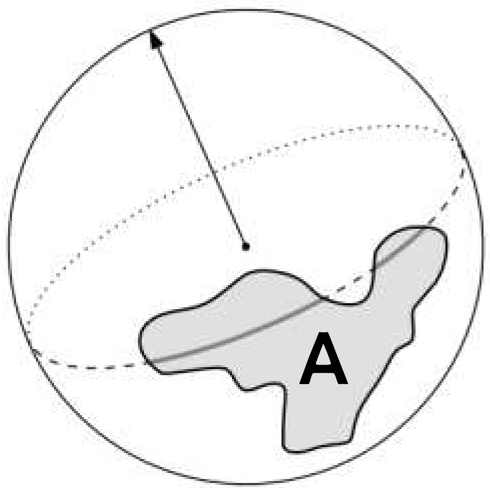
## How can we correct this injustice?

# Choose a random equator!

# The Main Sampling Statement

- A routine application of the rectangle bound (omitted), shows that the following implies the $\Omega(n^{1/3})$ lower bound:

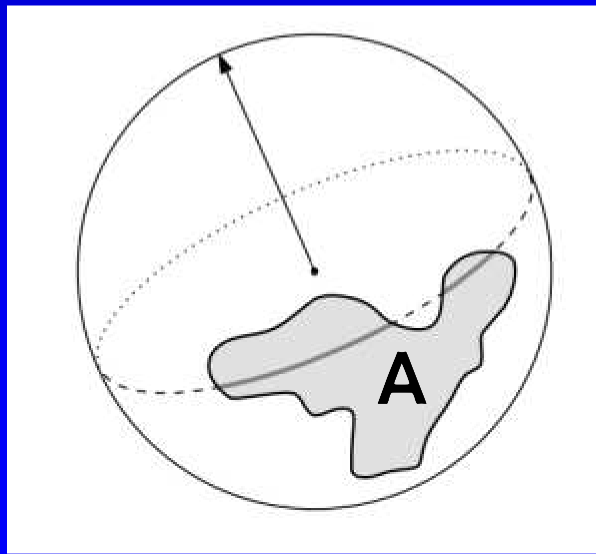
- Thm 1: Let $A \subseteq S^{n-1}$ be an arbitrary set of measure at least $\exp(-n^{1/3})$. Let H be a uniform n/2 dimensional subspace. Then, the measure of $A \cap H$ is $1 \pm 0.1$ that of A except with probability at most $\exp(-n^{1/3})$.

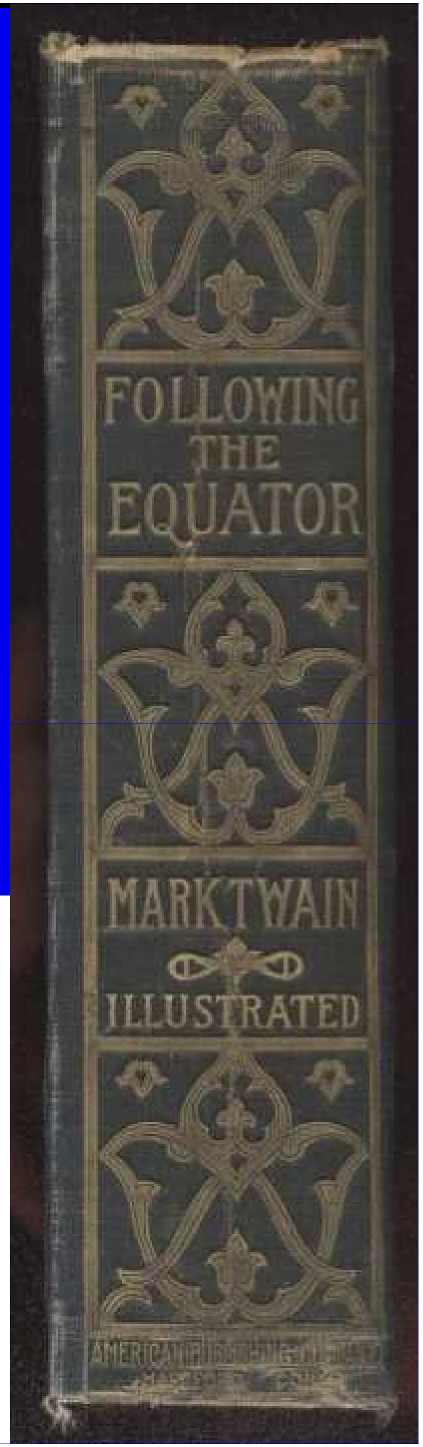



- Remark: this is tight

# Sampling Statement for Equators

- Thm 1 is proven by a recursive application of the following:
- Thm 2: Let $A \subseteq S^{n-1}$ be an arbitrary set of measure at least $\exp(-n^{1/3})$. Let H be a uniform n-1 dimensional subspace. Then, the measure of $A \cap H$ is $1 \pm t$ that of A except with probability at most $\exp(-t\, n^{2/3})$.
- So the error is typically $1 \pm n^{-2/3}$ and has exponential tail



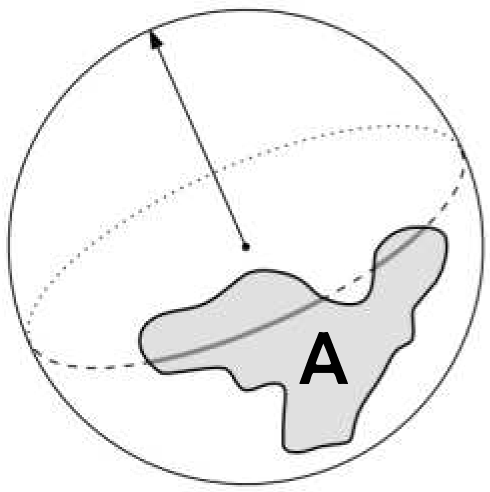



# Thm 1 from Thm 2

- Here is an equivalent way to choose a uniform n/2 dimensional subspace:
  - First choose a uniform n-1 dimensional subspace, then choose inside it a uniform n-2 dimensional subspace, etc.
- Thm 2 shows that at each step we get an extra multiplicative error of $1 \pm n^{-2/3}$. Hence, after n/2 steps, the error becomes $1 \pm n^{1/2} \cdot n^{-2/3} = 1 \pm n^{-1/6}$
- Assuming a normal behavior, this means probability of deviating by more than $1 \pm 0.1$ is at most $\exp(-n^{1/3})$
- (Actually proving all of this requires a very delicate martingale argument...)

# Proof of Theorem 2

- The proof of Theorem 2 is based on:
  - the Radon transform,
  - spherical harmonics,
  - the hypercontractive inequality on the sphere
- Concentration of measure doesn't seem to help
- See paper for an analogous statement for the hypercube $\{0,1\}^n$



# Proof of Thm 2

- Thm 2: Let $A \subseteq S^{n-1}$ be an arbitrary set of measure at least $\exp(-n^{1/3})$. Let x be a uniform point in $S^{n-1}$. Then, the measure of $A \cap x^{\perp}$ is $1 \pm n^{-1/3}$ that of A except with probability at most $\exp(-n^{1/3})$.

- Equivalently, our goal is to prove that for all $A,B \subseteq S^{n-1}$ of measure at least $\exp(-n^{1/3})$,

$$\mathop{\mathbb{E}}_{x \sim B, y \sim x^{\perp}} [1_{y \in A}] \in (1 \pm n^{-1/3}) \mu(A)$$

# Radon Transform

- For a function f:$S^{n-1} \to \mathbb{R}$, define its Radon transform R(f):$S^{n-1} \to \mathbb{R}$ as

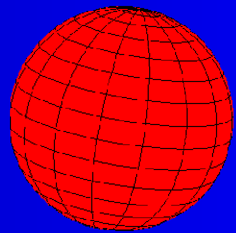
$$R(f)(x) := \mathbb{E}_{y \sim x^\perp}[f(y)]$$

- Define $f = 1_A/\mu(A)$ and $g = 1_B/\mu(B)$
- Then our goal is to prove

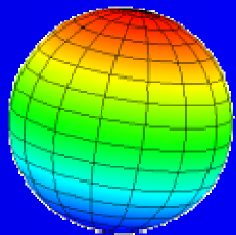
$$\langle g, R(f) \rangle = \mathbb{E}_x[g(x)R(f)(x)] \in 1 \pm n^{-1/3}$$

# Spherical Harmonics

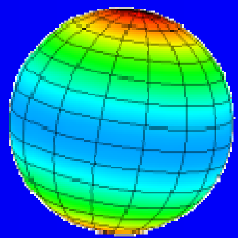
- We can decompose $L^2(S^{n-1})$ into orthogonal subspaces $S_k$ known as the spherical harmonics
- Level k=0:
  - constant functions, dimension=1



- Level k=1:
  - linear functions (e.g., $x_1$), dimension=n



- Level k=2:
  - quadratic functions, dimension=$(n^2+n-2)/2$, e.g., $x_1^2-1/n$



- So any function f can be written as $f=f_0+f_1+f_2+\ldots$ and $\langle f,g\rangle = \langle f_0,g_0\rangle + \langle f_1,g_1\rangle + \langle f_2,g_2\rangle + \ldots$

# Spherical Harmonics and Radon

- The subspaces $S_k$ are eigenspaces of the Radon transform
- The associated eigenvalues $\lambda_k$ are:
  - $\lambda_0=1$, $\lambda_1=0$, $\lambda_2=-1/n$, $\lambda_3=0$, $\lambda_4=1/n^2$, $\lambda_5=0$,…
- Hence, our goal is to prove that

$$\langle R(f), g\rangle = \langle f_0, g_0\rangle - \frac{1}{n}\langle f_2, g_2\rangle + \frac{1}{n^2}\langle f_4, g_4\rangle + \cdots \in 1 \pm n^{-1/3}$$

1

$\leq \frac{1}{n}\|f_2\|_2\|g_2\|_2$

Similarly…

- It remains to show that for all sets A of measure at least $\exp(-n^{1/3})$ and $f=1_A/\mu(A)$,

$$\|f_2\|_2 \leq n^{1/3}$$

# Bounding the Weight in a Level

- A bit more generally, we will show that for all sets A, $f=1_A/\mu(A)$, and $k\geq 1$,

$$\|f_k\|_2 \leq (\log(1/\mu(A)))^{k/2}$$

  - The analogous bound for $\{0,1\}^n$ was used in [Gavinsky-Kempe-Kerenidis-Raz-deWolf'07]
- This is essentially equivalent to:
  - If p is a level k polynomial with $\|p\|_2=1$,

$$\mathbb{P}_x[p(x) > t] \leq \exp(-t^{2/k})$$

  - Proof of sufficiency:

$$\|f_k\|_2^2 = \langle f_k, f_k\rangle = \langle f, f_k\rangle = \mathbb{E}_{x\in A}[f_k]$$

    and so,

$$\|f_k\|_2 = \mathbb{E}_{x\in A}[f_k/\|f_k\|_2]$$

- For k=1 this is easy (enough to consider $x_1$)
  - What about general k?

# The Hypercontractive Inequality

- We prove it is using the hypercontractive inequality for the sphere [Bakry-Émery'85, Rothaus'86, Gross'75,...]
  - Our proof follows [Kahn-Kalai-Linial'88] who worked in $\{0,1\}^n$
- It says that for all q there is a time t s.t. if $U_t$ is the heat flow operator for time t , then for any function $f:S^{n-1}\to\mathbb{R}$,

$$\|U_t(f)\|_q \le \|f\|_2$$

$$\|f\|_q := \mathbb{E}[|f|^q]^{1/q}$$

# The Hypercontractive Inequality

- The subspaces $S_k$ are eigenspaces of $U_t$, and hence $U_t p = \mu_{t,k} p$ where $\mu_{t,k}$ is the eigenvalue
- Plugging in the parameters, we get that for any level k polynomial p with $||p||_2=1$,

$$\|p\|_q \leq q^{k/2} \|p\|_2 = q^{k/2}$$

which implies the desired tail bound by a simple Markov inequality

# Open Questions

- Improve the lower bound to a tight $n^{1/2}$
  - Should be possible using the "smooth rectangle bound" [Klauck10]
- Improve to a functional separation between quantum SMP and classical
  - Seems very challenging, and maybe even impossible?
- What about total functions?