Topics in Quantum Information — **U. Waterloo CO 781, Spring 2004**
Ashwin Nayak (Instructor) — **Kelly Itakura (Scribe)**
Quantum communication (continued) — **May 11th, 2004**

1 Nayak Bound

Suppose Alice encodes n-bit string x into m-qubit $|\phi_x\rangle$. She sends $|\phi_x\rangle$ to Bob, who tries to recover x using a von Neumann measurement on the encoding and some ancillary qubits. Let $\{P_y\}$ be a set of orthogonal projection operators for the measurement. Bob's guess for x will be y, on measurement outcome y.

Theorem 1 (Nayak'99) *If X is chosen uniformly at random, and Y is the random variable corresponding to Bob's outcome, then*

$$Pr(Y = X) \leq \frac{2^m}{2^n}. \tag{1}$$

Corollary 2

1. *If Bob guesses x correctly (with probability 1), $m \geq n$.*
2. *If the error probability is at most $1 - \delta$ (on average), $m \geq n - \log \frac{1}{\delta}$.*

Proof : For (1), if Bob's guess is correct $\Pr[Y = X] = 1 \leq \frac{2^m}{2^n}$. This gives $m \geq n$. For (2), we have $1 - \delta \geq 1 - \frac{2^m}{2^n}$, which gives $m \geq n - \log \frac{1}{\delta}$. □

Note that this bound says that there is absolutely no advantage in using quantum states over classical encoding. The probability of correct decoding is not more than it would be is m bits out of the n were transmitted explicitly.

Before giving a proof of Theorem 1, we state some basic facts about the *trace* of a matrix (or a linear operator).

Definition 3 *The trace of a matrix M, denoted by $\mathrm{Tr}(M)$ is defined as*

$$\mathrm{Tr}(M) = \sum_e \langle e|M|e\rangle, \tag{2}$$

where $\{|e\rangle\}$ is any orthonormal basis.

We can verify that this is a well-defined quantity, since it is basis-independent. In particular, the trace of M is the sum of the diagonal entries of M. Some of its other properties are:

1. $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.
2. Trace is a linear functional on the vector space of linear operators. In particular, $\mathrm{Tr}(M_1 + M_2) = \mathrm{Tr}(M_1) + \mathrm{Tr}(M_2)$.
3. If $A \preceq B$, then $\mathrm{Tr}(PA) \leq \mathrm{Tr}(PB)$ for any positive semi-definite operator P (i.e., $P \succeq 0$).[1]

Using these properties, we now give a proof of Theorem 1.

[1]Here, by $A \preceq B$, we mean that the matrix (or operator) $B - A$ is positive semi-definite.

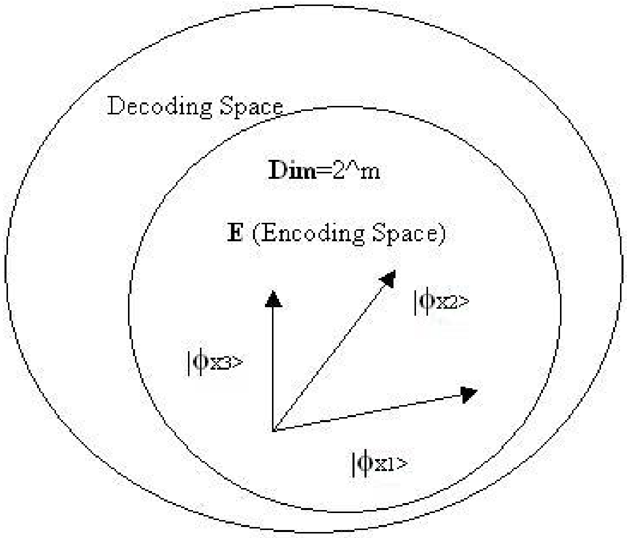

Figure 1: Encoding space inside decoding space

Proof : [Theorem 1] Note that a string x is decoded correctly only if Bob gets outcome x on measuring $|\phi_x\rangle$. Thus,

$$\begin{aligned}
\Pr(Y = X) &= \frac{1}{2^n} \sum_x \| P_x |\phi_x\rangle \|^2 \\
&= \frac{1}{2^n} \sum_x \langle \phi_x | P_x | \phi_x \rangle, \ \text{since} {P_x}^2 = P_x \\
&= \frac{1}{2^n} \sum_x \mathrm{Tr}(P_x |\phi_x\rangle\langle\phi_x|).
\end{aligned}$$

(Here, we have suppressed the ancilla that Bob uses in his measurement, for ease of notation.)

Let E denote the encoding space, i.e., span$\{|\phi_x\rangle|\bar{0}\rangle\}$. Note that it has dimension at most 2^m. Let $Q = \sum_f |f\rangle\langle f|$, where $\{|f\rangle\}$ is an orthonormal basis for E. We may include $|\phi_x\rangle$ in such basis. Then Q is the orthogonal projection operator onto E, and $Q - |\phi_x\rangle\langle\phi_x|$ is also a projection operator. This is also positive semi-definite, and thus we have $|\phi_x\rangle\langle\phi_x| \preceq Q$. Then, continuing on from the previous equation, we have,

$$\begin{aligned}
\Pr(Y = X) &\leq \frac{1}{2^n} \sum_x \mathrm{Tr}(P_x Q) \quad \text{From property 3 of trace above} \\
&\leq \frac{1}{2^n} \mathrm{Tr}((\sum_x P_x) Q) \quad \text{From property 2 of trace above} \\
&\leq \frac{1}{2^n} \mathrm{Tr}(Q) \quad \text{The sum of the projectors is the identity} \\
&\leq \frac{2^m}{2^n}.
\end{aligned}$$

The last line was obtained because Q is a projector onto E, a space of dimension at most 2^m. □

The bound proved above applies to a passive scenario where Alice sends some qubits to Bob. In fact, it extends to the case of an interactive protocol, where Alice and Bob send messages back and forth, with some intermediate computation. Before we describe how the Nayak bound extends to this kind of protocol as well, we will look at states that occur in the protocol more closely.

2 Bipartite states

Suppose Alice prepares $|\phi_x\rangle$ over $k+m$ qubits and sends m of them to Bob. Note that $|\phi_x\rangle \in \mathbb{C}^{2^k} \otimes \mathbb{C}^{2^m}$. So it may be written as $|\phi_x\rangle = \sum_{e,f} \alpha_{e,f} |e\rangle \otimes |f\rangle$, where $\{|e\rangle\}$ and $\{|f\rangle\}$ form orthonormal bases for the two spaces.

If P is a projection operator from von Neumann measurement that Bob applies,

$$\begin{aligned} \Pr(\text{outcome corresponding to } P) &= \left\| \sum_{e,f} \alpha_{e,f} |e\rangle P |f\rangle \right\|^2 \\ &= \sum_e \left\| \sum_f \alpha_{e,f} P |f\rangle \right\|^2 \end{aligned} \tag{3}$$

What is the probability of Bob obtaining the outcome corresponding to P, if Alice mesasures her qubits first in the basis $\{|e\rangle\}$?

$$\Pr(\text{measurement outcome corresponding to } P) = \sum_e (\sum_f |\alpha_{e,f}|^2) \left\| \frac{\sum_f \alpha_{e,f} |e\rangle \otimes P|f\rangle}{\sum_f |\alpha_{e,f}|^2} \right\|^2 \tag{4}$$

The first term in the product above corresponds to the probability that Alice observes e, and the second part of the product is the probability that Bob observes P given that Alice observed e.

Note that the probability in equation 3 and equation 4 are the same. This means that regardless of whether Alice measures or not, Bob's probability of any measurement outcome is not affected. In fact, the probability remains unchanged even if Alice chooses a different measurement. This suggests that we may treat Bob's part of the joint state as probability distribution over pure states (superpositions).

Definition 4 (Mixed State) *A mixed state is a probability distribution over pure states, and is denoted by* $\{p_i, |\phi_i\rangle\}$, *where* p_i *is the probability with which state* $|\phi_i\rangle$ *is sampled.*

Depending upon Alice's choice of basis to measure her part of the state in, Bob's part of the joint state may collapse to different mixed states. The *Schmidt decomposition* of a bipartite state gives us a special basis for measurement, so that the states in Bob's mixture are all orthogonal.

Fact 5 (Schmidt Decomposition) *A bipartite state* $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ *can be expressed as* $|\psi\rangle = \sum_i \sqrt{\lambda_i} |h_i\rangle |k_i\rangle$, *where* $\{|h_i\rangle\}_i$, *and* $\{|k_i\rangle\}_i$ *are orthonormal bases for* $\mathcal{H}$ *and* $\mathcal{K}$, *respectively, and* $\lambda_i \geq 0$, $\sum_i \lambda_i = 1$.

This is a very useful property of bipartite pure states; we will revisit it in several different contexts later in the course.

3 Bound for interactive communication

Now we sketch how the Nayak Bound applies to general communication protocols.

Step 1 We first observe that encoding a string x in a mixed state does not increase the probability of correctness of the protocol. This is because one of the states in the mixed state has the maximum probability of being decoded correctly, and this pure state may be used instead.

Step 2 Next, we invoke Yao's lemma to infer that in any m-qubit quantum protocol, Bob's state is a mixed state in a fixed subspace (independent of Alice's string x) of dimension at most 2^m.

Step 3 Finally, we point out that the bound in Theorem 1 depends only on the dimension of the encoding subspace.

This completes the proof, except for step 2, which follows from Yao's lemma for quantum communication.

In a general distributed computing scenario, an interactive communication protocol may be described as follows. Each party is given an input x, y, repectively. They start with an arbitrarily large supply of private qubits in some fixed basis state, say $|\bar{0}\rangle$. First, Alice applies a unitary transformation U_x (that depends only on her string x) to her qubits and sends m_1 of these qubits to Bob. Bob now applies a transformation V_y that depends only on his string y, to his qubits (that now include Alice's previous message), and then sends m_2 of these to Alice, and so forth. At the end of the protocol, one of the two parties measures his or her qubits to get the outcome of the protocol. The communication cost of the protocol is the sum $m = m_1 + m_2 + m_3 + \cdots$.

Lemma 6 (Yao '93) *In any quantum communication protocol, the final joint state of Alice and Bob can be written as*

$$\sum_{c \in \{0,1\}^m} |a_c(x)\rangle \otimes |b_c(y)\rangle, \tag{5}$$

where m is the total number of qubits exchanged, and $|a_c(x)\rangle$ and $|b_c(y)\rangle$ are (unnormalised and not necessarily orthogonal) states over Alice's and Bob's qubits respectively, that depend only on their separate inputs.

Proof : We prove this by induction on the number qubits exchanged, m.

The base case is $m = 0$: the joint state is $|\bar{0}\rangle \otimes |\bar{0}\rangle$, where $|\bar{0}\rangle$ denotes a verctor with all the entries initialized to 0.

Suppose $m = 1$: Alice sends a qubit to Bob. Let $|\phi_x\rangle = U_x|\bar{0}\rangle = |\phi_{x,0}\rangle \otimes |0\rangle + |\phi_{x,1}\rangle \otimes |1\rangle$, and suppose Alice sends the last qubit to Bob. Then see that the lemma holds with

$$\begin{aligned} a_0(x) &= |\phi_{x,0}\rangle \\ a_1(x) &= |\phi_{x,1}\rangle \\ b_0(x) &= |0\rangle \otimes |\bar{0}\rangle \\ b_1(x) &= |1\rangle \otimes |\bar{0}\rangle \end{aligned}$$

Now, you may complete the induction step on your own. □

In our setting, only Alice is given an input (the n-bit input x). Using Yao's lemma, we see that no matter what Alice's input is, Bob's part of the state is equivalent to a mixed state that lies in the subspace spanned by the vectors $|b_c(y)\rangle$. Since there are at most 2^m such vectors, the subspace has dimension less than or equal to 2^m. This proves step 2 of the Nayak bound.

4 Protocol for Set disjointness

In the set disjointness problem, Alice and Bob are each given one subset, of a universe of size n, represented by their charectisitic vectors $x, y \in \{0,1\}^n$. I.e., x_i tells us whether i is in the subset x or not. The question they wish to answer is: $x \cap y = \emptyset$?

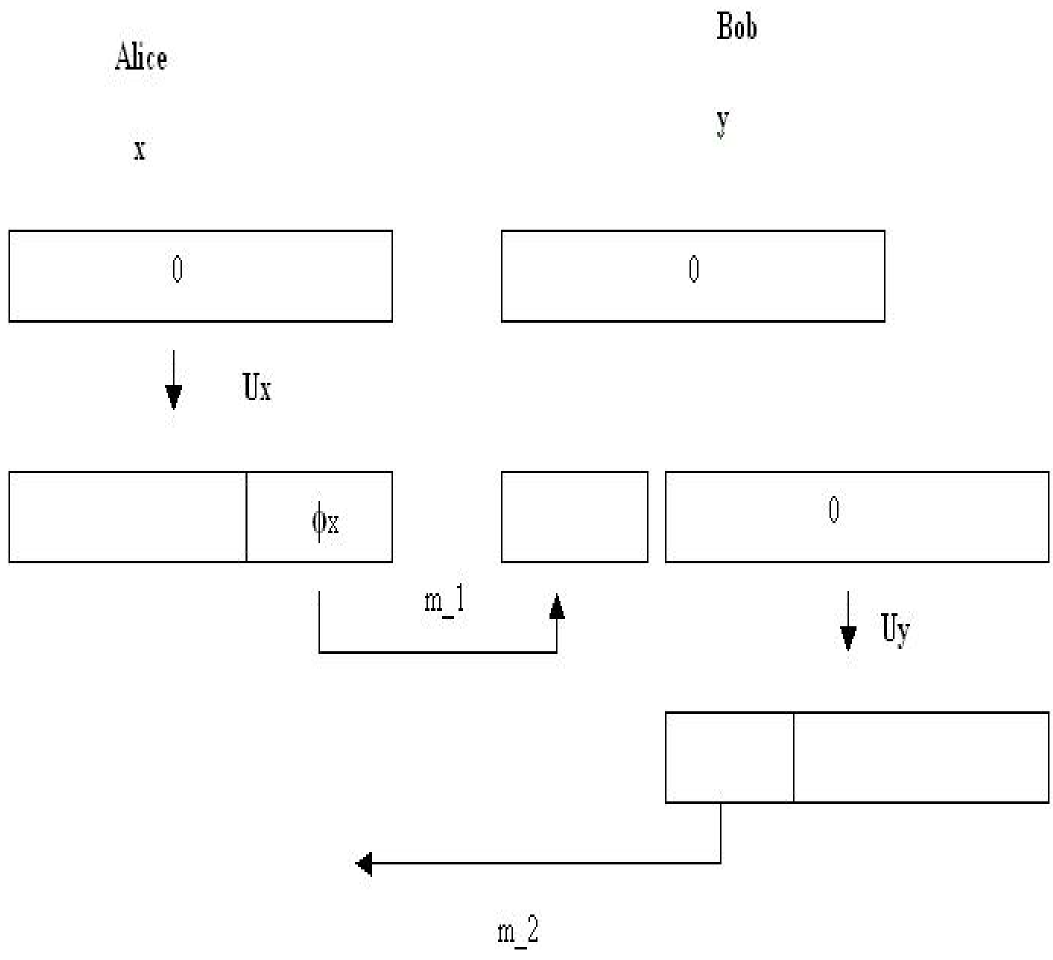

Figure 2: Model for Yao's Lemma

A quantum protocol devised by Buhrman, Cleve, and Wigderson in 1998[BCW98] provides an $O(\sqrt{n}\log n)$ protocol. The upper bound for this problem has been improved by Aaronson and Ambainis [2003] to $O(\sqrt{n})$. This matches the (quantum) lower bound of $\Omega(\sqrt{n})$ given by Razborov [2003]. On the other hand, classical lower bound for this problem was shown to be $\Omega(n)$ by Kalayanasundaram and Schnitger [1987].

The BCW protocol is a natural application of the Grover search algorithm to communication complexity. Since $x \cap y \neq \emptyset \Leftrightarrow \vee_{i=1}^{n}(x_i \wedge y_i)$, Alice and Bob need only locate an index i such that $x_i = 1 = y_i$. They do this by simulating the algorithm and the oracle respectively. At each step, Alice holds a state $|\phi\rangle = \sum_i \alpha_i |i\rangle$. She writes the bit of x corresponding to the index in the superposition, and sends the entire state to Bob. Bob, who now has the appropriate bit of x as well as all the information about y, simulates an oracle for $x_i \wedge y_i$, and returns the state to Alice. Alice can now erase x_i, and perform the transformation in the search algorithm. The communication complexity for this protocol is $\sqrt{n}\log n$, since there are $\sqrt{n}$ iterations, and at each iteration, $2(\log n + 1) = O(\log n)$ qubits are exchanged.

References

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 63–68, 1998.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 369–376, 1999.

[Yao93] A.C.-C. Yao. Quantum circuit complexity. In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, pages 352–361, 1993.