1 Introduction

A *qubit* (short form for a *quantum* bit) is a physical object with two "perfectly distinguishable" physical states which are identified with the classical states 0 and 1. Mathematically, these states are represented by two orthonormal vectors in $\mathbb{C}^2$, denoted by $|0\rangle$ and $|1\rangle$ in the Dirac bra-ket notation.

A general qubit state is any linear combination of the two basis states with unit norm: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. Such state is called a *superposition* of the two basis states, and the coefficients α and β are called the *amplitudes* of the corresponding states $|0\rangle$ and $|1\rangle$, respectively.

The state of a qubit may be "read out" by conducting an experiment. In its simplest form, an experiment is captured by an orthonormal basis $|e_i\rangle, i = 0, 1$ for $\mathbb{C}^2$. The outcome of the measurement is i with probability $|\langle e_i|\phi\rangle|^2$, and the state "collapses" to $|e_i\rangle$. Here '$\langle e_y|$' is in the 'bra' notation and may be taken as the conjugate transpose of the ket $|e_y\rangle$ which is viewed as a column vector.

The nature of information carried by a qubit differs from a classical bit in a fundamental sense. The following example of (approximate) *oblivious transfer* due to [Bennett, Brassard, Breidbard, Wiesner '83] illustrates this very well. Note: This scheme was re-discovered as *random access encoding* by [Ambainis, Nayak, Ta-Shma, Vazirani '99].

Oblivious Transfer. Merlin wishes to reveal exactly one of two bits x_1, x_2 to Arthur, who wishes to keep the bit he wants to know secret from Merlin. How can they achieve this?

A quantum solution is to encode the two bits $x_1, x_2 \in \{00, 01, 10, 11\}$ into one qubit in a manner that Arthur can extract with good confidence any one of the two bits. We will see later in the class that such an encoding is necessarily lossy, i.e., does not allow simultaneous decoding of both the bits.

Let

$$\phi_0 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$\phi_1 = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$$

Then we use the following encoding

$$\begin{aligned} 00 &\to |0\rangle + |\phi_0\rangle \\ 01 &\to |0\rangle - |\phi_1\rangle \\ 10 &\to |1\rangle + |\phi_0\rangle \\ 11 &\to |1\rangle + |\phi_1\rangle \end{aligned}$$

where the states on the right are taken to be the proper normalized vectors in the stated direction.

If we measure the encoding of, say, 01 in the standard basis we observe a '0' with probability equal to the amplitude of $|0\rangle$ in the encoding. This probability is:

$$\begin{aligned} \left| \frac{\langle 0|(|0\rangle - |\phi_1\rangle)}{\| \, |0\rangle - |\phi_1\rangle \, \|} \right|^2 &= \frac{(1 + 1/\sqrt{2})^2}{(1 + 2/\sqrt{2} + 1)^2} \\ &= \cos^2 \frac{\pi}{8} = 0.853\ldots \end{aligned}$$

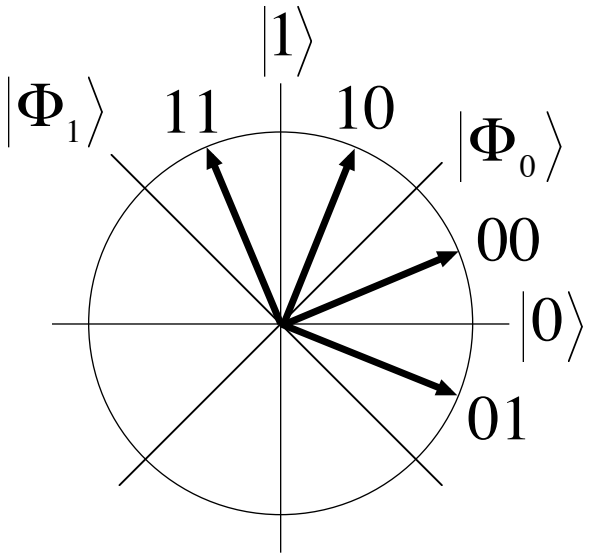

Figure 1: The encoding for oblivious transfer.

If we measure the encoding in the basis $\{\phi_0, \phi_1\}$ then we will observe ϕ_1 with the same probability. Similarly, measuring the other states in the first basis reveals the first bit with probability $0.853\ldots$, and measuring in the second basis reveals the second bit.

Such a scheme is not possible with classical encoding.

Theorem 1.1 (ANTV '99) *There does not exist any classical (randomized) encoding of two bits into one bit such that we can decode an arbitrary one of the two bits with probability greater than* $1/2$*.*

(Try to convince yourself of this.)

The following property of qubits ensures that Arthur cannot simultaneously decode both bits.

Theorem 1.2 (Nayak '99) *No measurement on any encoding of two bits into one qubit reveals both encoded bits simultaniously with probability greater than* $1/2$ *(on average over a uniformly random choice of the two bits).*

We will prove a more general version of this theorem in a couple of lectures.

2 Systems with many qubits

In general, the state of an n qubit system can be any unit-norm linear combination of the 2^n basis states in $\{0,1\}^n$. That is, any state can be written as

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$$

where

$$\sum_x |\alpha_x|^2 = 1.$$

A measurement in the standard basis will collapse the state to the probability distribution $\left\{|\alpha_x|^2, x\right\}$. More general measurements are given by orthonormal bases $\{|e_y\rangle\}_y$ for the Hilbert space $\mathbb{C}^{2^n}$. Here the outcome is 'y' with probability $|\langle e_y|\phi\rangle|^2$, and the state collapses to $|e_y\rangle$, a state consistent with the outcome.

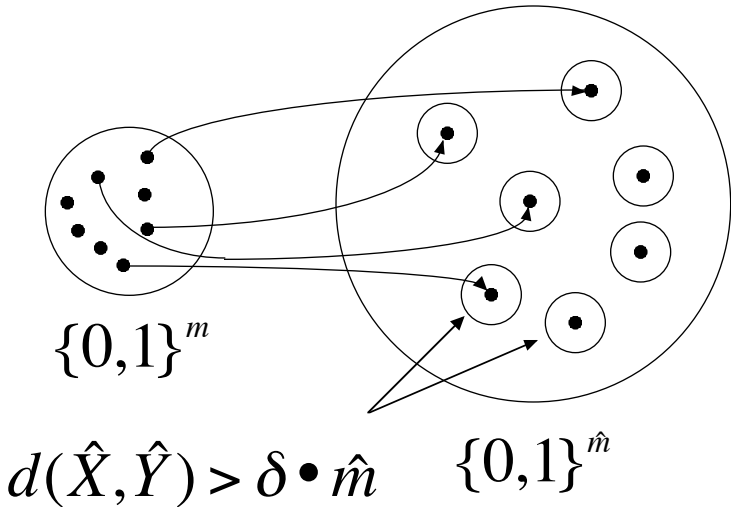

Figure 2: Mapping strings to an error-correcting code.

Given that it takes an exponential number of parameters to specify an arbitrary quantum state of n qubits, it is natural to ask if we can encode as much (an exponential amount) classical information in n qubits. Buhrman, Cleve, Watrous, de Wolf [2001] showed one scenario where this is possible.

Quantum Fingerprints. A quantum fingerprint allows us to encode $2^{O(n)}$ bits into n qubits in a "useful manner".

The encoding, or fingerprint, works as follows. Let $m = 2^{O(n)}$, where we will specify the constants later. Consider any m-bit string x. Map $x \in \{0,1\}^m$ to a longer string $\hat{x} \in \{0,1\}^{\hat{m}}$, where $\hat{m} = O(m)$ and the strings $\hat{x}$ lie in an error-correcting code.

An error-correcting code $C \subset \{0,1\}^{\hat{m}}$ is a set of strings such that every pair of strings differ in at least $\delta\hat{m}$ coordinates, for some parameter $0 \leq \delta \leq 1$. The parameter $d = \delta\hat{m}$ is called the minimum distance of the code. We are interested in codes where $\delta > 0$ is a constant.

Now, we construct the quantum fingerprint for x as:

$$|\phi_x\rangle = \frac{1}{\sqrt{\hat{m}}} \sum_{i=1}^{\hat{m}} |i, x_i\rangle$$

In the next lecture we will see how these fingerprints may be used effectively in a communication protocol.