Notes for Lecture 21

1 Notation and Formalism

Introducing the following quantum notation/formalism to be used in the last few lectures.

- $|\psi\rangle$ denotes a general quantum state. These are unit norm column vectors in $\mathbb{C}^n$.
- $\langle\psi|$ is the conjugate transpose of $|\psi\rangle$, that is $\langle\psi| = |\psi\rangle^\dagger$.
- $\langle\psi|\phi\rangle$ denotes the inner product of $|\psi\rangle$ and $|\phi\rangle$.
- $|x\rangle$ for $x \in [n]$, denotes the x'th standard basis vector (when using a greek letter, it is usually refers to a general state as above).

The following are the basic quantum operations that we can do:

- Applying a unitary transformation to any quantum state. We say that a transformation $U \in \mathbb{C}^{n\times n}$ is unitary if $U^\dagger U = I$, where $\dagger$ denotes the conjugate transpose of the matrix. Applying a unitary transformation U to a quantum state $|\psi\rangle$ results in the quantum state $U|\psi\rangle$.
- Measure operation. A measurement of a quantum state $|\psi\rangle$ is a probabilistic process where the probability that $|\psi\rangle \mapsto |x\rangle$, that is, the measurement yields $|x\rangle$ is $|\langle x|\psi\rangle|^2$. Note that this is a well defined probability distribution as $|\psi\rangle$ is a vector of unit norm.

We can also consider composite systems, where for $|\psi\rangle \in \mathbb{C}^n$ and $|\varphi\rangle \in \mathbb{C}^m$, the joint state is given by $|\psi\rangle|\varphi\rangle \in \mathbb{C}^{n\times m}$. This is the tensor product of $|\psi\rangle$ and $|\phi\rangle$. If we write

$$|\psi\rangle = \sum_{x\in[n]} \alpha_x |x\rangle \qquad \text{and} \qquad |\phi\rangle = \sum_{y\in[m]} \beta_y |y\rangle$$

then the joint state is

$$|\psi\rangle|\phi\rangle = \sum_{(x,y)\in[n]\times[m]} \alpha_x\beta_y |x\rangle|y\rangle$$

The system we will usually work with is

$$\mathbb{C}^{2^n} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n \text{ times}}$$

each of the systems $\mathbb{C}^2$ will represent a single qubit.

Note. We can also perform partial measurements on composite systems. When doing a right partial measurement on a state $|\psi\rangle = \sum_{x,y} \alpha_{x,y} |x, y\rangle$, an output y_0 is obtained and the state collapses to a sum of states 'compatible' with the measurement of the y_0. That is, after measuring and obtaining y_0 from the state $|\psi\rangle$, we get the collapsed state

$$\frac{1}{\sqrt{\rho_{y_0}}} \sum_x \alpha_{x,y_0} |x, y_0\rangle$$

where ρ_{y_0} is a renormalization constant defined as

$$\rho_{y_0} = \sum_x |\alpha_{x,y_0}|^2$$

and the probability of having measured y_0 is ρ_{y_0}.

Definition 1 (Entanglement)**.** We say that a state $|\tau\rangle \in \mathbb{C}^{n \times m}$ in a composite system is entangled if $|\tau\rangle$ cannot be written as a product state. Explicitly, there do not exist $|\psi\rangle \in \mathbb{C}^n$ and $|\phi\rangle \in \mathbb{C}^m$ such that $|\tau\rangle = |\psi\rangle |\phi\rangle$. For such a state $|\tau\rangle$, we say that it is entangled.

Remark. In general, a state in a larger composite system $|\tau\rangle \in \mathbb{C}^{n \times m}$ cannot be written as $|\psi\rangle |\phi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ (a product state) for $|\psi\rangle \in \mathbb{C}^n$ and $|\phi\rangle \in \mathbb{C}^m$.

This notion of being entangled in the quantum setting is the analogue of correlation in the classical setting.

Example 2. Consider the following system with two qubits.

$$\tfrac{1}{\sqrt{2}} |0\rangle |0\rangle + \tfrac{1}{\sqrt{2}} |0\rangle |1\rangle = |0\rangle \left(\tfrac{1}{\sqrt{2}} |0\rangle + \tfrac{1}{\sqrt{2}} |1\rangle \right)$$

We see that the two qubits are not entangled, as we wrote the state as a product of two states. In this case, we get the quantum analogue of a probability distribution where the first bit is always 0 and the second bit is uniformly random.

However, the state

$$\tfrac{1}{\sqrt{2}} |0\rangle |0\rangle + \tfrac{1}{\sqrt{2}} |1\rangle |1\rangle$$

is entangled. Here we get the quantum analogue of a probability distribution where we take a uniformly random bit and repeat it, as we are guaranteed that the two bits will be equal.

As we are concerned about the involvement of quantum computers in cryptography, we must have a notion of efficiency of such a computer. We defined the notion of an operation by applying a unitary transformation. However there are uncountably many unitary matrices, so there is most certainly no way to compute an arbitrary unitary transformation efficiently. Therefore we take an approach inspired by the classical circuit model. In such case, a function is efficiently computable if there is a circuit of polynomial size that computes the function, using gates from some finite set.

It may be tempting to define efficient computation in the quantum setting as above. Begin by fixing a finite 'gate' set of unitary matrices over 2 qubits and considering all computations that can be represented as polynomial sized circuits using gates from this finite gate set. However, the number of such possible circuits is countable. On the other hand, the number of possible unitary matrices is uncountable. Even by removing the polynomial sized restriction, there are is an uncountable set of unitary transformations that are not computable under this definition, a pitfall which we certainly want to avoid. This motivates the following definition by tolerating approximations to unitary transformations:

Definition 3 (Quantum setting efficient computation)**.** Fix a finite set of unitaries over 2 qubits, this will be the finite 'gate' set Γ. We say that a unitary transformation U is computable if we can approximate U with arbitrary precision with circuits using gates from Γ. Moreover, we say that a unitary transformation U is efficiently computable if it is computable and such approximation to arbitrary precision are with polynomial sized circuits with gates in Γ.

Example 4. Any classical computation can be performed efficiently. We might expect that for a classical function f, we find a unitary matrix U_f representing f that takes a state $|x\rangle$ to $U_f |x\rangle = |f(x)\rangle$. Nonetheless, in general such functions f are information theoretically not invertible, whereas all unitary transformations are.

The model for classical computation does the following. Given a classical function $f : \{0,1\}^n \to \{0,1\}^m$, define U_f a unitary such that

$$U_f |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

where the notation $|x, y\rangle$ denotes $|x\rangle |y\rangle$. It is easy to check that $U_f^\dagger U_f = I$ and hence U_f is in fact a unitary matrix. If f is efficiently computable in the classical setting, then there is a polynomial sized quantum circuit that computes U_f.

Definition 5. The Hadamard gate H acts on a basis vector $|b\rangle$ for $b \in \{0,1\}$ by

$$H |b\rangle = \tfrac{1}{\sqrt{2}} |0\rangle + (-1)^b \cdot \tfrac{1}{\sqrt{2}} |1\rangle$$

the definition is then extended to an arbitrary $|\psi\rangle$ by the bilinearity property. It satisfies $H^2 = I$ the identity.

Similarly for a state in a composite system $|\psi_1, \ldots, \psi_r\rangle$, define

$$H^{\otimes r} |\psi_1, \ldots, \psi_r\rangle = \big(H |\psi_1\rangle\big) \cdots \big(H |\psi_r\rangle\big)$$

Remark. Note that the Hadamard transformation does not have the form of U_f (there is no classical analogue of the Hadamard).

Another example is the phase gate. The gate takes a quantum state $\alpha |0\rangle + \beta |1\rangle \mapsto \alpha |0\rangle + \beta e^{i\theta} |1\rangle$ (this example we will probably not need in this course).

Definition 6 (Quantum Fourier Transform)**.** As a generalization of the Hadamard gate, the quantum fourier transform (QFT) is defined on the basis vectors $|x\rangle$ for $x \in \{0, \ldots, n-1\}$ by

$$\mathsf{QFT}_n |x\rangle = \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} w_n^{xy} |y\rangle$$

with w_n a primitive n-th root of unity. We may take $w_n = \exp(\frac{2\pi i}{n})$. It is the case that QFT_n is a unitary transformation and the inverse QFT_n^{-1} satisfies

$$\mathsf{QFT}_n^{-1} |x\rangle = \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} w_n^{-xy} |y\rangle$$

where the only difference is the conjugate transpose (in this case equivalent to the inverse) of the primitive roots of unity.

2 Simon's Problem

Suppose we have a function $f : \{0,1\}^n \to \{0,1\}^m$ and given a promise that there exists an $s \in \{0,1\}^n \setminus \{(0, \ldots, 0)\}$ such that

- $f(x) = f(x \oplus s)$ for all $x \in \{0,1\}^n$.
- $f(x) \neq f(y)$ if $y \notin \{x \oplus s, x\}$.

With this setup, the task is to find this binary string s.

We have the following quantum algorithm for the problem.

1. Initialize a system of $n + m$ qubits to $|0^n, 0^m\rangle$.
2. Apply H to each qubit of the left subsystem. This results in a left subsystem as

$$\begin{aligned}(H |0\rangle)^n &= \left(\tfrac{1}{\sqrt{2}} |0\rangle + \tfrac{1}{\sqrt{2}} |1\rangle\right)^n \\ &= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle\end{aligned}$$

where this vector notations represents the system, if $\vec{x} = (b_1, \ldots, b_n)$ with $b_i \in \{0, 1\}$ then $|\vec{x}\rangle = |b_1, \ldots, b_n\rangle$.

3. Apply U_f to the resulting state, where U_f is the unitary for the classical function f. This produces the state

$$\left(\frac{1}{\sqrt{2}}\right)^n \sum_{\vec{x}\in\{0,1\}^n} |\vec{x}, f(\vec{x})\rangle$$

4. Measure the right subsystem (partial measurement). This gives some $f(\vec{x}_0) = y_0$ and the left subsystem state collapses to

$$\tfrac{1}{\sqrt{2}} \left(|x_0\rangle + |x_0 \oplus s\rangle\right)$$

where we get this y_0 uniformly at random (we get y with probability $\frac{1}{2^{n-1}}$ if the y is in the range of f).

5. Apply H to each qubit of the left subsystem state. In its most general form, this transformation yields

$$H^{\otimes n} |x\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_y (-1)^{x\cdot y} |y\rangle$$

Where above we interpret the x, y as vectors instead of scalars. In our case we get

$$\begin{aligned} H^{\otimes n} \left(\tfrac{1}{\sqrt{2}} |x_0\rangle + \tfrac{1}{\sqrt{2}} |x_0 \oplus s\rangle\right) &= \left(\tfrac{1}{\sqrt{2}}\right)^n \cdot \left(\sum_y (-1)^{x_0\cdot y} |y\rangle + \sum_y (-1)^{(x_0\oplus s)\cdot y} |y\rangle\right) \\ &= \left(\tfrac{1}{\sqrt{2}}\right)^n \sum_y [(-1)^{x_0\cdot y} + (-1)^{(x_0\oplus s)\cdot y}] |y\rangle \\ &= \left(\tfrac{1}{\sqrt{2}}\right)^n \sum_y (-1)^{x_0\cdot y} [1 + (-1)^{s\cdot y}] |y\rangle \end{aligned}$$

where we have that the coefficient of $|y\rangle$ is

$$(-1)^{x_0\cdot y}[1 + (-1)^{s\cdot y}] = \begin{cases} 2(-1)^{x_0\cdot y} & \text{if } s\cdot y \equiv 0 \mod 2 \\ 0 & \text{if } s\cdot y \equiv 1 \mod 2 \end{cases}$$

thus, our state becomes

$$\frac{2}{(\sqrt{2})^n} \cdot \sum_{\{y | y\cdot s \equiv 0\ (2)\}} (-1)^{x_0\cdot y} |y\rangle$$

and measuring this state, we get a uniformly random y such that $s \cdot y \equiv 0 \mod 2$.

We then repeat the steps (1) to (6) many times ($\sim n$ times) to obtain multiple random y's such that $y \cdot s \equiv 0 \mod 2$. With high probability on drawing random vectors $y_1, \ldots, y_r$ such that $y_i \cdot s \equiv 0 \mod 2$, we can solve for a unique vector s using linear algebra.

One might ask if there is a classical algorithm to solve this problem. If f is given as a circuit, then in some sense it is hopeless to prove anything. However, if the classical algorithm is given only oracle access to f, then except with $\mathsf{negl}(n)$ probability, it is impossible to find s. The idea of the proof centers on taking random f that satisfy the promise, and under classical queries, outputs of f are random and independent unless the query occurs on x and $x \oplus s$.

On the other hand, Simon's algorithm (the algorithm presented above in the quantum setting) only requires "oracle access" to U_f. Here, quantum setting oracle access means we get to only apply U_f. Thus we have found a separation between what is achievable in the quantum setting and what is achievable in the classical setting.

3 Attacks on Crypto Problems

Simon's problem is a special case of period finding, sometimes also referred to as hidden (abelian) subgroup problem which we now explain. If we have an additive group $(\mathbb{G}, +)$ with some subgroup $H \leq \mathbb{G}$ and a function $f : \mathbb{G} \to \{0,1\}^m$ such that

1. $f(g + h) = f(g)$ for all $h \in H$
2. $f(g + y) \neq f(g)$ if $y \notin H$

The goal is to find this subgroup H.

Note. This is a generalization of Simon's problem. We can view Simon's problem as the hidden abelian subgroup problem with $\mathbb{G} = \mathbb{Z}_2^n$ and $H = \{0, s\}$.

We can solve this problem following the steps in Simon's algorithm described above, however we replace the Hadamard gate H by an appropriate QFT_n and a bit of extra work on a few details.

The relevance to cryptography comes in when we realize factoring and the discrete log as period finding problems.

For factoring, given g and N to factor, we let $\mathbb{G} = \mathbb{Z}/N\mathbb{Z}$ and define the function $f_g(a) = g^a \mod N$. The key comes in when we realize that, for g a quadratic residue, the period of the function f_g is even, and $g^{\frac{1}{2}\text{period}(f_g)} \mod N$ is a square root of 1. With high probability, we get that this square root is not the trivial pair of square roots $\pm 1 \mod N$. If we get such a nontrivial square root u, then we can see by the Chinese Remainder Theorem that $\gcd(u - 1, N)$ is a nontrivial factor of N.

Explicitly with $N = p_1^{r_1} \cdots p_k^{r_k}$, under the CRT, a non-trivial square root u of 1 is ($u_1 \mod p_1^{r_1}, \ldots, u_k \mod p_k^{r_k}$) where u_i are not all equal to 1 or -1. That is, some u_i are 1, some are -1. Hence $u - 1$ is divisible by only by a nontrivial factor of N.

For the discrete log, given g and $h = g^a$ both in some group $\mathbb{G}$ of order p, define the function

$$f_{gh}(r, s) = g^r h^{-s}$$

here the period finding will happen in the group $\mathbb{Z}_p^2$, hence (r, s) are elements in $\mathbb{Z}_p^2$. The subgroup for this function in the period finding problem is

$$H = \{(ax, x) \mid x \in \mathbb{Z}_p\}$$

Hence if we solve the problem and have any nonzero element of H, we can recover a by dividing the left coordinate by the right coordinate.

4 Next time

Next time we will discuss a little more on quantum attacks on cryptography and later move on to the final part of the course, where we use quantum mechanics to do new cryptographic constructions.