Algorithm Analysis and Design (CS1.301)

Monsoon 2021, IIIT Hyderabad
10 November, Wednesday (Lecture 17)

Quantum Algorithms

The Photon Experiment

Consider the following experiment: place two polarisers in the path of a beam of photons such that no light passes beyond the second. Now, it is possible to place a third polariser in between these two such that some light ends up passing beyond all three – this is not explainable by classical physics.

Qubits

Thus, we describe photons in terms of a new concept – quantum bits or qubits. Qubits are unit vectors in a 2D complex vector space, with the basis conventionally taken as $\{|0\rangle, |1\rangle\}$. Thus a qubit has the form $a|0\rangle + b|1\rangle$, with the additional constraint that $|a|^2 + |b|^2 = 1$.

The values a and b are interpreted as follows: the probability that, when measured, the qubit $a|0\rangle + b|1\rangle$ returns $|0\rangle$ is $|a|^2$, and similarly for $|1\rangle$ and $|b|^2$.

Applying Qubits to the Photon Experiment

Now, we can explain our observation. The first two filters must be placed orthogonal to each other; thus all photons passing through the first one would collapse to $|0\rangle$ (say), and none could then pass through the next one.

However, suppose the filter in the middle is placed halfway between each of these two (at a 45° angle). Then half the photons passing through the first filter could still pass through the second, and similarly for the third.

Quantum Postulates

The following are some fundamental quantum postulates:

- the superposition postulate – quantum systems exist as a superposition of possible configurations, which are represented as state vectors in Hilbert space.
- the measurement and collapse postulate
- the evolution postulate – transformations are unitary matrices and systems evolve according to the Schrödinger equation.

As an example of using transformations, we can see the no-cloning theorem, which states that there is no quantum transformation U such that $U|a0\rangle = |aa\rangle$ for all quantum states $|a\rangle$.

This can be proved by considering a state $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$. Then,

$$\begin{aligned} U|c0\rangle &= \frac{1}{\sqrt{2}}(U|a0\rangle + U|b0\rangle) \\ &= \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle) \end{aligned}$$

But,

$$\begin{aligned} U(|c0\rangle) &= |cc\rangle \\ &= \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle), \end{aligned}$$

which is a contradiction.

Multiple Qubits

Individual state spaces of n classical particles combine with the cartesian product, but quantum states combine through the tensor product.

For example, the basis for a three-qubit system is $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$, and in general an n-qubit system will have 2^n basis vectors.

Thus, nature carries out an extremely complex computation in real time, which we can exploit.

Quantum Entanglement

The state $|00\rangle + |11\rangle$ cannot be described in terms of its components separately, *i.e.*, we cannot find a_1, a_2, b_1, b_2 such that

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle.$$

This means that quantum states can show instantaneous effect at a distance – if the state $|00\rangle + |11\rangle$ is divided and the two bits taken to remote locations, the measurement of either one will lead the immediate collapse of the other.

Quantum Gates and Circuits

Quantum gates are simply unitary transformations (matrices) applied on state vectors.

Quantum circuits are built on such gates.

Quantum Teleportation

The objective of quantum teleportation is to transmit the quantum state of a particle using classical bits and reconstruct the exact quantum state at the receiver. Note that it does not contradict the no-cloning theorem as the original state is destroyed in the process.

Suppose Alice as a qubit $\phi = a\,|0\rangle + b\,|1\rangle$ whose state she doesn't know. It must be teleported to Bob classically.
We will assume that Alice and Bob each possess one qubit of an entagled pair

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Thus, the initial state is

$$\begin{aligned}\phi \otimes \psi_0 &= \frac{1}{\sqrt{2}}(a\,|0\rangle \otimes (|00\rangle + |11\rangle) + b\,|1\rangle \otimes (|00\rangle + |11\rangle)) \\ &= \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle).\end{aligned}$$

Now, Alice applies $C_\neg \otimes I$ and $H \otimes I \otimes I$. Therefore, the state is now

$$\begin{aligned}(H \otimes I \otimes I)(C_\neg \otimes I)(\phi \otimes \psi_0) &= (H \otimes I \otimes I)(C_\neg \otimes I)\frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle) \\ &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle) \\ &= \frac{1}{2}(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\ &= \frac{1}{2}(|00\rangle\,(a\,|0\rangle + b\,|1\rangle) + |01\rangle\,(a\,|1\rangle + b\,|0\rangle) + |10\rangle\,(a\,|0\rangle - b\,|1\rangle) + |11\rangle\,(a\,|1\rangle - b\,|0\end{aligned}$$

Alice measures the first two qubits of her state and sends the result to Bob. According to Alice's results, Bob can find the transformation to apply to his qubit as

bits received	state	decoding
00	$a\,|0\rangle + b\,|1\rangle$	I
01	$a\,|1\rangle + b\,|0\rangle$	X
10	$a\,|0\rangle - b\,|1\rangle$	Z
11	$a\,|1\rangle + b\,|0\rangle$	Y