QUANTUM INFORMATION AND COMPUTATION

ADAM KELLY – MATHEMATICAL TRIPOS PART II

Contents

1. The No Cloning Theorem

A *cloning process* to clone the state $|\psi\rangle$ is

$$|\psi\rangle_A |0\rangle_B |M_0\rangle_M \longrightarrow |\psi\rangle_A |\psi\rangle_B |M_\psi\rangle_M .$$

Theorem 1.1 (No Cloning Theorem)**.** *Let S be any set of states of A that contains at least one non-orthogonal pair of states. Then no unitary*[1] *cloning process exists that achieves cloning for all states in S.*

Proof. Let $|\xi\rangle \neq |\eta\rangle$ be non-orthogonal states in S. Then our process must have

$$|\xi\rangle_A |0\rangle_B |M_0\rangle_M \longmapsto |\xi\rangle_A |\xi\rangle_B |M_\xi\rangle_M ,$$
$$|\eta\rangle_A |0\rangle_B |M_0\rangle_M \longmapsto |\eta\rangle_A |\eta\rangle_B |M_\eta\rangle_M .$$

Then since unitary operations preserve inner products, taking the inner product of the two above states gives

$$\langle\xi|\eta\rangle \langle 0|0\rangle \langle M_0|M_0\rangle = \langle\xi|\eta\rangle \langle\xi|\eta\rangle \langle M_\xi|M_\eta\rangle ,$$

which, taking absolute values, implies that

$$1 = |\langle\xi|\eta\rangle||\langle M_\xi|M_\eta\rangle|,$$

but $|\langle\xi|\eta\rangle| < 1$ and $|\langle M_\xi|M_\eta\rangle| \leq 1$, so this is a contradiction. $\square$

2. Quantum Dense Coding

Definition 2.1 (Bell States)**.** The Bell states is an orthonormal basis for the state space of two qubits, given by

$$|\varphi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\varphi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$
$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Date: May 26, 2023. Email `ak2316@srcf.net`.

[1] Or process more generally, by the deferred measurement principle and letting M absorb any ancilla.

A notable property of these states is that they can all be achieved from $|\varphi^+\rangle$ by a local operation on the first qubit, with

$$\left|\varphi^-\right\rangle = Z \otimes I \left|\varphi^+\right\rangle, \ \left|\psi^+\right\rangle = X \otimes I \left|\varphi^+\right\rangle, \ \left|\psi^-\right\rangle = Y \otimes I \left|\varphi^+\right\rangle.$$

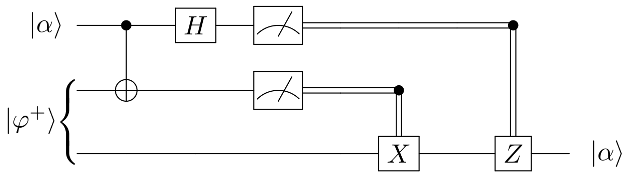
This fact gives us the *quantum dense coding protocol.*

Method 2.1 (Quantum Dense Coding)**.** *Suppose A and B hold one qubit of the state $|\varphi^+\rangle$. Then if A wants to send two bits of classical information, for the messages 00, 01, 10, 11 they can apply the gates I, Z, X, Y to their qubit, making the states $|\varphi^+\rangle, |\varphi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$ respectively. They can then send their qubit to B, who can measure the whole system in the Bell basis to then distinguish the message.*

3. Quantum Teleportation

Suppose A and B, separated in space, hold one qubit of the state $|\varphi^+\rangle$. A also has a single qubit state $|\alpha\rangle$ they would like to send to B by only performing local operations and communicating with classical information. They can do this with *quantum teleportation.*

Method 3.1 (Quantum Teleportation)**.** *The state $|\alpha\rangle$ can be 'teleported' by A and B performing the following operations.*



where A sends the outcome of their measurements B classically so the X and Z gates can be applied if necessary.

4. Oracle Problems

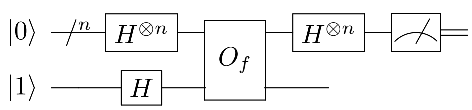
4.1. **Query Complexity.** . We have some 'Oracle' O_f that computes some boolean function $f : B_m \to B_n$ (we might have knowledge or 'promises' about this function). We consider problems about if f has certain properties.

Definition 4.1. The *query complexity* of the algorithm is the number of times that the oracle needs to be used in order to solve the problem. The total time complexity is the total size of the circuit where we count each oracle use as a single gate.

4.2. **Deutsch-Jozsa Algorithm.** We consider a Boolean function $f : B_n \to B_1$ that is either 'constant' or 'balanced' (in the sense that exactly half of its values is zero). The problem is to decide whether c is constant with certainty.

Obviously, classically $2^{n-1}+1$ queries is sufficient and necessary. With a quantum circuit, a single query suffices.

Method 4.1 (Deutsch-Jozsa)**.** *Given an oracle O_f for a Boolean function $f : B_n \to B_1$ (that's constant or balanced), which performs the transformation $|x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$, we perform the following circuit:*



Then if we measure all zeros, the function is constant, otherwise it is balanced.

5. Quantum Fourier Transform

Definition 5.1. Suppose we have a N-dimensional state space with computational basis $\{|n\rangle \mid n \in \mathbb{Z}/N\mathbb{Z}\}$. The quantum Fourier transform modulo N, written QFT_N on the space is the the linear operator which takes the basis state $|a\rangle$ to

$$\frac{1}{\sqrt{N}} \sum_{b \in \mathbb{Z}/N\mathbb{Z}} e^{2\pi i ab/N} |b\rangle .$$