Quantum Information and Computation

Afiq Hatta

March 14, 2019

Contents

1 Quantum states as information carriers

We can use quantum processes to our advantage in transmitting information between several parties. However, nothing comes for free in life and this also applies to quantum computation - there are restrictions to what we can do. We start by mentioning what is possible and what is not.

1.1 Possible moves allowed on quantum states

Our allowed actions on quantum states boil down to three things. We call these moves Ancilla (A), Unitary (U), and Measure (M).

- **Ancilla:** we can increase the dimensionality of our state space by attaching (via a tensor product) another state to states in the state space.

  $$|\psi\rangle \to |A\rangle\,|\psi\rangle$$

  The effect of this is that we've increased the dimensionality of our state state space from m to mn where n is the dimension of the state space which $|A\rangle$ belongs to.

- **Unitary:** we can operate on states with some unitary operator U. Recall earlier that we can also compose tensor products of unitary operators to operate on tensor products of state spaces. An important feature of unitary operators that we shall use later is that they preserve inner products.

- **Measure:** this is when we perform a complete measurement (a projection on to the basis states of our state space), or an incomplete measurement (when we project onto orthogonal subspaces of a statespace).

1.2 The No-cloning principle

We can now apply the above to prove the simple principle that we cannot arbitrarily "clone" quantum states with some machine. That is to say, given a state space S, there is no arbitrary process $|M\rangle$ which, for all $|\psi\rangle \in S$, we have the process

$$|M\rangle\,|\psi\rangle\,|0\rangle \to |M_\psi\rangle\,|\psi\rangle\,|\psi\rangle\,.$$

This is for state spaces where at least one non-orthogonal pair exists. We can prove this by working first with the restriction that the process consists of just one unitary move. Assume that cloning is possible, and examine two non-orthogonal states.

$$|M\rangle |\psi\rangle |0\rangle \rightarrow |M_\psi\rangle |\psi\rangle |\psi\rangle$$
$$|M\rangle |\phi\rangle |0\rangle \rightarrow |M_\phi\rangle |\phi\rangle |\phi\rangle$$

By preservation of inner products, assuming that all states are properlu normalised, we have that

$$1 =| \langle M_\psi | M_\phi \rangle |^2 | \langle \psi | \phi \rangle |^2$$

However, by non-orthogonality of $|\phi\rangle$ and $|\psi\rangle$, their inner product is between 0 and 1, which is a contradiction since the first modulus is bounded by 1.

1.3 The impossibility of superluminal signalling

1.4 Distinguishing between non-orthogonal states

Computing

Computing concerns taking strings of bits and operating on them to solve a problem. We define a an n-bit string as a sequence $b_n = x_0 x_1 \dots x_n$ where $x_i \in \{0, 1\}$. We denote the set of n-bit strings as B_n, and set the set of all finite length bit strings as $B^* = \bigcup_n B_n$.