QUANTUM INFORMATION & COMPUTATION

Nilanjana Datta, DAMTP Cambridge

1 Quantum gates and quantum teleportation

Unitary operations on qubits are also called *quantum gates*. Matrices given below are always relative to the standard basis $\{|0\rangle, |1\rangle\}$. The following notations for commonly occurring gates will be used throughout the course, and you should memorise them. *Figures given in class.*

One-qubit gates

$$\textbf{Hadamard gate} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Thus we have $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$ and $HH = I$. As an orthogonal transformation in the real Euclidean plane $\mathbb{R}^2$, H is reflection in the mirror line at angle $\pi/8$ to the x-axis.

Next, introduce the 1-qubit gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Y = ZX = -XZ = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

X is sometimes also called the (quantum) NOT-gate because it interchanges the kets $|0\rangle$ and $|1\rangle$ i.e. effects the classical NOT operation on the label.

Note that $\{|+\rangle, |-\rangle\}$ is the X-eigenbasis and $\{|0\rangle, |1\rangle\}$ is the Z-eigenbasis (in each case corresponding to eigenvalues $+1$ and -1 respectively). We also have the formulas

$$X|k\rangle = |k \oplus 1\rangle \qquad Z|k\rangle = (-1)^k |k\rangle \qquad \text{for } k = 0, 1.$$

Recall that the **Pauli operators (or Pauli matrices)**, introduced previously, are

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = -iY = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

They have elegantly simple multiplicative properties:

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$$
$$\sigma_x\sigma_y = -\sigma_y\sigma_x = i\sigma_z \qquad \sigma_y\sigma_z = -\sigma_z\sigma_y = i\sigma_x \qquad \sigma_z\sigma_x = -\sigma_x\sigma_z = i\sigma_y$$

(noting the cyclic shift of x, y, z labels in the latter set). Note that the matrices $I, \sigma_x, \sigma_y, \sigma_z$ are all Hermitian as well as unitary (which is an unusual coincidence). Finally we have the

$$\textbf{Phase gate} \qquad P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Two-qubit gates

Controlled-X (or controlled-NOT) gate

$$CNOT \equiv CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} (I) & (0) \\ (0) & (X) \end{pmatrix}.$$

For the four basis states we can compactly write $CX\,|i\rangle\,|j\rangle = |i\rangle\,|i \oplus j\rangle$ where $\oplus$ denotes addition modulo 2. Note that for any 1-qubit state $|\alpha\rangle$ we have

$$CX\,|0\rangle\,|\alpha\rangle = |0\rangle\,|\alpha\rangle \qquad CX\,|1\rangle\,|\alpha\rangle = |1\rangle\,X\,|\alpha\rangle$$

i.e CX applies X to the second qubit if the first is set to "1" and acts as the identity if the first is set to "0" (and extends by linearity if the first qubit is in a superposition of the two values etc.) Accordingly the first qubit is called the *control qubit* and the second is called the *target qubit*. Note that we get a different 2-qubit gate if we interchange the qubit roles of control and target. Thus if there is an ambiguity as to which qubit is to be the control and target we introduce labels (say 1 and 2) for the two qubit system, writing CX_{12} or CX_{21} with the first subscript always denoting the control qubit and the second, the target qubit. Thus for example $CX_{12}\,|0\rangle_1\,|1\rangle_2 = |0\rangle_1\,|1\rangle_2$ whereas $CX_{21}\,|0\rangle_1\,|1\rangle_2 = |1\rangle_1\,|1\rangle_2$.

The **controlled-Z gate**:

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} (I) & (0) \\ (0) & (Z) \end{pmatrix}$$

i.e. as for CX, CZ applies Z to the second qubit controlled by the state of the first qubit. Note that despite this asymmetrical description, CZ (unlike CX) is actually symmetric in its action on the two qubits.

Note that

$$CNOT_{21} = (H \otimes H)(CNOT_{12})(H \otimes H) \tag{1}$$

i.e. we can reverse the control/target roles of the two bits by applying H to each bit vector both before and after the $CNOT$ action. This relation is not possible to achieve with any classical 1-bit Boolean operations before and after the $CNOT$s.

The validity of this relation can be readily checked e.g. by computing the actions of the gates on each basis state in turn or by computing the matrices corresponding to either side of eq.(1), and we omit the details here (which you can easily provide). □

1.1 Quantum Teleportation

In superdense coding we used quantum information for transmission of classical information in the presence of prior shared entanglement. Here we study another application of entanglement in which we use classical information to transmit quantum information.

Suppose Alice and Bob who are distantly separated in space, each possesses one qubit of the entangled Bell state

$$\left|\Phi^+\right\rangle_{AB} = \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Alice has the qubit A and Bob has the qubit B. (*Note: here we use the notation in which we write the labels of the subsystems as subscripts outside the ket for later convenience.*) Suppose Alice has another qubit (say, C) which is in a pure state $|\psi\rangle$ unknown to her. She wants to transfer this state (i.e. quantum information) to Bob. How can she achieve this transfer? She may not even know the identity of the state $|\psi\rangle$ and according to quantum measurement theory she is unable to learn more than a small amount of information about it before totally destroying it! She can place the (physical system embodying the) qubit state in a "box" and physically carry it across to Bob. But is there any other way? What if the space region in between Alice and Bob is a hostile and dangerous place? In fact, what if Alice has no means of sending qubits to Bob and is only allowed to communicate with him classically?

The quantum protocol via which Alice can achieve this transfer, by using local operations on the qubits in her possession (C and A), sending classical information to Bob, followed by local operations by Bob on his qubit B, is called *quantum teleportation*.

As we will see below, state transfer from Alice to Bob is achieved "without the state having to pass through the space in between" in the following sense: the transference is unaffected by any physical process whatsoever that takes place in the intervening space. Note that this is also a feature of the entanglement of $|\Phi^+\rangle$: although quantum theory appears to imply the existence of some kind of "non-local connection" between entangled particles (e.g. reflected in correlations between local measurement results, cf Exercise Sheet 1), the entanglement ("non-local connection") itself remains entirely unaffected by any physical process occurring in the space in between; it can change only by physical actions on the particles themselves.

Let the state to be transferred be given by

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

for some $a, b \in \mathbb{C}$ sch that $|a|^2 + |b|^2 = 1$. The tripartite state initially shared between Alice and Bob is then given by

$$\begin{aligned} |\psi\rangle_C \otimes \left|\Phi^+\right\rangle_{AB} &= (a\,|0\rangle_C + b\,|1\rangle_c) \otimes \frac{1}{\sqrt{2}}((|00\rangle_{AB} + |11\rangle_{AB}) \\ &= \frac{1}{\sqrt{2}}\left[a\,|00\rangle_{CAB} + a\,|011\rangle_{CAB} + b\,|100\rangle_{CAB} + b\,|111\rangle_{CAB}\right] \end{aligned} \quad (2)$$

Henceforth, for notational simplicity, we will suppress the subscripts on the kets (denoting the systems), and keep in mind that the first two kets are with Alice, while the third ket is with Bob. The desired state transfer is achieved through the following steps.

(i) Alice sends her qubits (CA) through a $CNOT$ gate, obtaining

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}\left[a\,|0\rangle\,(|00\rangle + |11\rangle) + b\,|1\rangle\,(|10\rangle + |01\rangle)\right]. \quad (3)$$

(ii) She then sends the first qubit (C) through a Hadamard gate, obtaining

$$|\varphi_2\rangle = \frac{1}{2}\left[|00\rangle\left(a|0\rangle + b|1\rangle\right) + |01\rangle\left(a|1\rangle + b|0\rangle\right) + |10\rangle\left(a|0\rangle - b|1\rangle\right) + |11\rangle\left(a|1\rangle - b|0\rangle\right)\right] \tag{4}$$

The above expression can be rewritten as

$$|\varphi_2\rangle = \frac{1}{2}\left[|00\rangle|\psi\rangle + |01\rangle\left(X|\psi\rangle\right) + |10\rangle\left(Z|\psi\rangle\right) + |11\rangle\left(-Y|\psi\rangle\right)\right] \tag{5}$$

(iii) Alice then measures her qubits relative to the computational basis to obtain a 2-bit string 00, 01, 10 or 11.

Note that the sequence (i), (ii), (iii) is equivalent to Alice just performing a Bell measurement on her two qubits – indeed the unitary operations in (i) and (ii) simply serve to rotate the Bell basis into the computational basis of the two qubits (as is easily checked). *(Figure and Exercise given in class.)*

By calculating the effect of these three operations on the initial state eq. (2) we see that each 2-bit string is obtained with equal probability of 1/4 (irrespective of the values of a and b, recalling that $|a|^2 + |b|^2 = 1$). Furthermore after the measurements in (iii) we have the following post-measurement states (as you should calculate):

mmt outcome	post-mmt state
00	$\|00\rangle \otimes |\psi\rangle$
01	$\|01\rangle \otimes (X|\psi\rangle)$
10	$\|10\rangle \otimes (Z|\psi\rangle)$
11	$\|11\rangle \otimes (XZ|\psi\rangle)$

i.e. Bob's qubit B is now disentangled from CA and it is in a state that is a fixed transform of $|\psi\rangle$, the choice of transform depending only on the measurement outcome and not on the identity of $|\psi\rangle$ (i.e. not on the a, b values). In fact if the measurement outcome is ij then Bob's qubit will be "collapsed" into the state $X^j Z^i |\psi\rangle$. *(In the above, we have made use of the relation $-Y = XZ$.)*

(iv) Alice sends the 2-bit measurement outcome ij to Bob (i.e. she sends him 2 bits of classical information).

(v) On receiving ij Bob applies the unitary operation $Z^i X^j$ (i.e. the inverse of $X^j Z^i$) to his qubit which is then guaranteed to be in state $|\psi\rangle$.

This completes the teleportation of $|\psi\rangle$ from Alice to Bob.

Note that no remnant of any information about $|\psi\rangle$ remains with Alice. After step (iii) she is left with only a 2-bit string that has always been chosen uniformly at random (independent of $|\psi\rangle$) and the 'original' state $|\psi\rangle$ is always totally destroyed. Thus the teleportation process is fully consistent with the no-cloning theorem, as indeed it must be.

The figure (given in class) gives a depiction of the protocol as a network of quantum gates is.

We conclude this section with a few further remarks about the teleportation process.

• Unlike "star-trek" teleportation, the physical system embodying $|\psi\rangle$ is not transferred from Alice to Bob. Only the "information" of the state's identity is transferred, residing finally in a new physical system i.e. the qubit B which was initially with Bob.

• Before Alice's measurements in (iii) Bob's qubit has preparation: "the right half of $|\Phi^+\rangle$". After A's measurement Bob's qubit has preparation: " one of the four states $|\psi\rangle$, $Z|\psi\rangle$, $X|\psi\rangle$ or $XZ|\psi\rangle$ chosen uniformly at random". It can be shown (see Exercise Sheet 1) that for any measurement process on Bob's qubit, these two preparations give identical probability distributions of outcomes so Bob cannot notice any change at all in his qubit's behaviour as a result of Alice's measurements. This is just another example of the no-signalling principle in action. Bob can reliably create the qubit state $|\psi\rangle$ only after receiving the ij message from Alice.