Chapter 11

The power of entanglement

The violation of the Bell inequalities indicates that entanglement is a genuine quantum feature which has no classical counterpart. Hence, very much like the linear superposition, which also has no classical counterpart, entanglement may prove a powerful resource for communication and computation.

11.1 Quantum dense coding

Suppose that Alice and Bob, who are distantly apart in space, share a pair of qubits in the Bell state $|\psi^-\rangle$. Alice wants to communicate two bits of information to Bob, using her qubit as the carrier of information. We know that for a single qubit (i.e. Bob does not hold an entangled partner) this is not possible. But with entanglement this becomes possible [C.H. Bennett and S.J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992)].

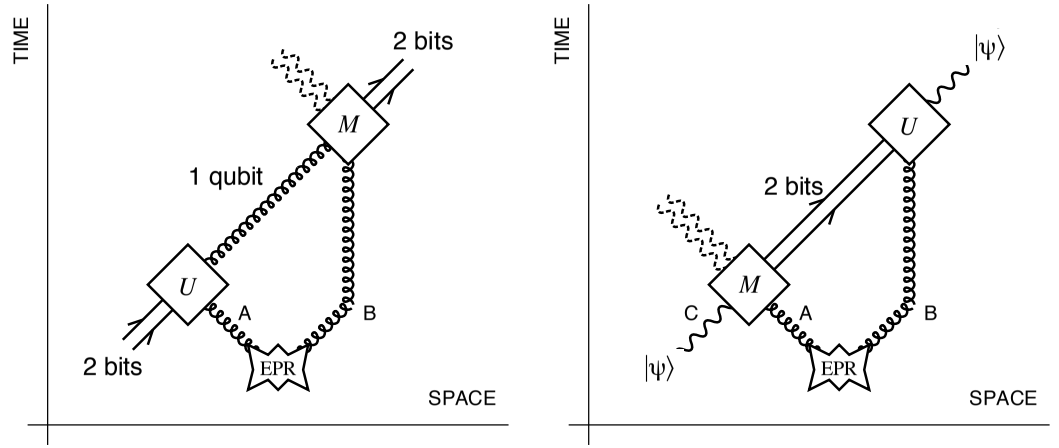

Figure 11.1: The space-time Werner diagrams of quantum dense coding (left) and quantum teleportation (right). The EPR source produces an entangled pair of qubits in the Bell state $|\psi^-\rangle$. One qubit is send to Alice (who is located on the left), the other qubit is send to Bob (who is located on the right). The symbols U and M refer to unitary opertion and measurement, resepctively.

Quantum dense coding, i.e. the cramming of two bits into one qubit, relies on an important feature of the Bell basis: each of the four basis states can be prepared from the singlet state $|\psi^-\rangle$ by Alice *alone* performing purely *local* operations.

Indeed, consider the set of four 1-qubit unitary operations

$$\begin{aligned} \hat{U}_{00} &= \hat{1}\,, & \hat{U}_{01} &= \hat{\sigma}_3\,, \\ \hat{U}_{10} &= -\hat{\sigma}_x\,, & \hat{U}_{11} &= -i\hat{\sigma}_y\,. \end{aligned} \tag{11.1}$$

If Alice applies one of these unitary operations to her qubit, she will induce one of

the transformations

$$\begin{aligned} \hat{U}_{00}|\psi^-\rangle &= |\psi^-\rangle\,, & \hat{U}_{01}|\psi^-\rangle &= |\psi^+\rangle\,, \\ \hat{U}_{10}|\psi^-\rangle &= |\phi^-\rangle\,, & \hat{U}_{11}|\psi^-\rangle &= |\phi^+\rangle\,. \end{aligned} \tag{11.2}$$

Thus to communicate two bits ij to Bob, Alice applies $\hat{U}_{ij}$ to her qubit and sends this *single* qubit to Bob. Upon arrival, Bob performs a Bell measurement on the joint state of the two particles. Since the Bell measurement is a maximal test which distinguishes the four Bell states, he can read out the value of ij with 100 percent reliability.

11.2 Quantum teleportation

Suppose Alice has a qubit in a possibly unknown state $|\psi\rangle$, and she wishes to transfer this state to Bob. One way to achieve this goal is by measuring the state, and sending the data (two real numbers, specifying an orientation of a Stern-Gerlach device) to Bob. But, as we have seen, this is impossible for a single qubit. The other method would be to place the qubit into a box and send the qubit itself across space to Bob. But the box may be opened on the way, and the state thereby being disturbed. However, there is a save way in which the quantum state is transferred to Bob without that any material ingredient is involved – just two bits of information. As this resembles teleportation, the corresponding process has been dubbed "Quantum teleportation" [C.H. Bennett, G. Brassard, C. Crepeau, R. Josza, A. Peres and W.K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993)].

Alice and Bob share an entangled pair of qubits in the Bell state $|\psi^-\rangle$. In addition, Alice also holds the extra qubit, which is in state

$$|\psi\rangle = \alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C \tag{11.3}$$

In what follows, the subscript C labels the extra particle, while subscripts A, B labels the system which comprises $|\psi^-\rangle$.

Initially, the state of the three-particle system is given by

$$|\Psi\rangle_{ABC} = |\psi\rangle_C |\psi^-\rangle_{AB} \tag{11.4}$$

This expression is easily rewritten in terms of the Bell states of CA,

$$\begin{aligned}
2|\Psi\rangle_{ABC} = \quad & |\psi^-\rangle_{CA}\,(-\alpha|\uparrow\rangle_B - \beta|\downarrow\rangle_B) && (11.5)\\
+ \; & |\psi^+\rangle_{CA}\,(-\alpha|\uparrow\rangle_B + \beta|\downarrow\rangle_B) && (11.6)\\
+ \; & |\phi^-\rangle_{CA}\,(+\beta|\uparrow\rangle_B + \alpha|\downarrow\rangle_B) && (11.7)\\
+ \; & |\phi^+\rangle_{CA}\,(-\beta|\uparrow\rangle_B - \alpha|\downarrow\rangle_B)\;. && (11.8)
\end{aligned}$$

If Alice performs a Bell measurement on her particles A, C, then regardless of the identity of $|\psi\rangle_C$, each outcome will occur with equal probability 0.25. Depending on the outcome, Bob will hold his particle in one of the four possible states,

$$\begin{aligned}
-\alpha|\uparrow\rangle_B - \beta|\downarrow\rangle_B &= -\hat{U}_{00}|\psi\rangle_B && (11.9)\\
-\alpha|\uparrow\rangle_B + \beta|\downarrow\rangle_B &= -\hat{U}_{01}|\psi\rangle_B && (11.10)\\
\beta|\uparrow\rangle_B + \alpha|\downarrow\rangle_B &= -\hat{U}_{10}|\psi\rangle_B && (11.11)\\
-\beta|\uparrow\rangle_B + \alpha|\downarrow\rangle_B &= \hat{U}_{11}|\psi\rangle_B\,. && (11.12)
\end{aligned}$$

If Alice communicates the outcome of her Bell measurement to Bob, which is easily encoded in two bits ij, Bob can reconstruct $|\psi\rangle$ by just applying $(-1)^{ij+1}\hat{U}_{ij}$ to his particle, restoring it to state $|\psi\rangle_B$ in every case.

Note that neither Alice nor Bob learn anything about ψ. Note also that the initially shared entanglement is destroyed. The "cost" of shipping a (possibly unkown) state from A to B is one (maximally) entangled pair – one *ebit*.

11.3 Quantum public key distribution (E91 protocol)

[A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* **67**(6), pp. 661–663 (1991)]

Given an EPR source which produces pairs of qubits in the Bell state $|\psi^-\rangle$, say. One member of the pair is for Alice, the other is for Bob. Alice and Bob measure the state of their qubit using a Stern-Gerlach magnet. For equally chosen directions, their results will be (i) completely random, but (ii) fully (anti-)correlated. Thus by using the code

$$\text{Alice:} \quad b(|\uparrow_a\rangle) = \mathtt{0}\,, \quad b(|\downarrow_a\rangle) = \mathtt{1}\,, \tag{11.13}$$

$$\text{Bob:} \quad b(|\downarrow_b\rangle) = \mathtt{0}\,, \quad b(|\uparrow_b\rangle) = \mathtt{1}\,, \tag{11.14}$$

and discarding all records where $\vec{a} \neq \vec{b}$, they can establish a key. Public discussion of the discarded records, which essentially consists in checking the CHSH inequality, reveals a potential eavesdropper.

Alice and Bob have three SGM-directions $\vec{a}_i$ and $\vec{b}_i$, $i = 1, 2, 3$ at their disposal. The vectors lie in the $x - y$ plane, and are characterized by azimuthal angles $\varphi_i^A = (i-1)\pi/4$, $\varphi^B = i\pi/4$. For each EPR pair, Alice and Bob choose the direction randomly and independently from each other.

Once they have collected suffiently many measurement data, Alice and Bob broadcast the directions chosen for each qubit measured. Data where the directions match are kept private for later use as a key. Data where the orientations do not match are broadcast for statistical analysis of the CHSH inequality. If the CHSH inequalities are maximally violated (i.e. if $S = 2\sqrt{2}$), they can be sure that no eavesdropper was in the line. In this case they can trust the "privacy"of their key. If, on the

other hand, and eavesdropper was in the line, he (or she) unavoidably must have "classicalized" the correlations, and thus reduced the value of S below its maximum value (which is only assumed for perfect Bell states).

11.4 No Cloning Theorem

It would be nice if one could copy (or clone, like in PCR) arbitrary quantum states. Given a *single* qubit, say, one could then unambiguously determine its state. Doing so, one could, for example, eavesdrop on the BB84 protocol. Yet copying an unknown state is impossible [Wootter and Zurek, *Nature* **299**, 802 (1982); D. Dieks, *Phys. Lett.* A**92**, 271 (1982)].

System A: the "original". System B: the "medium" of the copy, initially in blank state $|0\rangle$ (white paper). Copying on a *universal* copy machine means that for any pair of originals $|\phi\rangle$, $|\chi\rangle$, the following process is possible:

$$|\phi 0\rangle \rightarrow |\phi\phi\rangle = \hat{U}|\phi 0\rangle \tag{11.15}$$
$$|\chi 0\rangle \rightarrow |\chi\chi\rangle = \hat{U}|\chi 0\rangle \tag{11.16}$$

with $\hat{U}$ unitary. The scalar product of these equations yields

$$\langle\chi\chi|\phi\phi\rangle = \langle\chi 0|\hat{U}^\dagger\hat{U}|\phi 0\rangle = \langle\chi 0|\phi 0\rangle \tag{11.17}$$

that is

$$\langle\chi|\phi\rangle^2 = \langle\chi|\phi\rangle\langle 0|0\rangle\,. \tag{11.18}$$

Since by assumption χ is arbitrary, $\langle\chi|\phi\rangle \neq 0$. Thus $\langle\chi|\phi\rangle = \langle 0|0\rangle = 1$, that is $\chi = \phi$, and therefore χ not arbitrary, in contradiction to our assumption.

11.5 Yes Cloning Theorem

If *universal* cloning is impossible – why can one copy classical information *with perfect reliability*? Because any *particular* pair of *orthogonal states* (the alternative representing the classical black/white on the original) can be copied with perfect fidelity!