

## Lecture 5

Maximally entangled states:

Consider the state

$$|\Phi^+\rangle_{AB} = \frac{|0\rangle^A |0\rangle^B + |1\rangle^A |1\rangle^B}{\sqrt{2}}$$

Z measurements on A & B will be perfectly correlated. But in fact, the correlations are stronger than that. One can show that, in the X basis, the state is

$$|\Phi^+\rangle_{AB} = \frac{|++\rangle + |--\rangle}{\sqrt{2}},$$

So X measurements are also perfectly correlated.

This state is entangled - there are no state vectors for A and B. In fact,  $|\Phi^+\rangle$  is an example of what is called a maximally-entangled state. Such states can be used as resources in quantum info protocols. In that context they are often called ebits or EPR pairs.

We've already seen that by using an ebit we can do a joint measurement remotely. We'll see many more tricks you can do with entanglement.

## Resource notation

②

In this course we will often consider protocols that convert some resource or resources into others (or use some resources to simulate others). We will use a special notation to indicate resources, with square or curly brackets.

We represent one shared ebit as  $[qq]$ . The way to read this is as one unit of noiseless shared quantum correlation (entanglement).

A simple protocol is ~~to~~ to measure both halves of the ebit in the  $Z$  (or  $X$ ) basis. The outcome is a perfectly correlated pair of binary random variables  $X_A$  and  $X_B$ :

$$P_{X_A X_B}(x_A, x_B) = \frac{1}{2} \delta_{x_A x_B}.$$

Such a unit of shared randomness is written  $[cc]$  to indicate noiseless classical correlation. This brings us to our first resource inequality:

$$[qq] \geq [cc]$$

So ebits can be used to produce shared randomness, but not necessarily vice versa. (In fact, the reverse is impossible.) Ebits, as we shall see, are a much more powerful resource than shared randomness.

## The CHSH Game

③

Alice and Bob are physically separated and unable to communicate. A referee gives each of them a bit,  $x$  and  $y$  respectively, chosen uniformly at random. A & B must then each send a bit ( $a$  and  $b$ ) to the referee that satisfies  $a \oplus b = x \& y$ .

What is the probability to win this game? The dominant strategy is to always choose  $a = b = 0$ . This wins  $3/4$  of the time (except when  $x = y = 1$ ).

If A & B have shared randomness [cc] it doesn't help them. But if they have an ebit they can improve their probability. On the HW you will show that the following strategy wins w/prob =  $\cos^2(\pi/8) \approx 85\%$ .

① If  $x = 0$ , A measures  $Z$ ; if  $x = 1$ , A measures  $X$ . She returns her answer as  $a$ : ( $+1 \rightarrow 0$ ,  $-1 \rightarrow 1$ ).

② If  $y = 0$ , B measures  $(X+Z)/\sqrt{2}$ ; if  $y = 1$ , B measures  $(Z-X)/\sqrt{2}$ . He returns the answer as  $b$ .

The CHSH is just a disguised version (and not very well disguised) of a Bell inequality violation.

## Bell States

an orthonormal

(4)

One can produce a set of 4 maximally-entangled states starting from the state  $|\Phi^+\rangle$  by applying Pauli operators to one of the two qubits:

$$|\Phi^+\rangle = (I \otimes I) |\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = (Z \otimes I) |\Phi^+\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = (X \otimes I) |\Phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = (\underbrace{ZX}_{iY} \otimes I) |\Phi^+\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

These are the Bell states. They form an orthonormal basis for <sup>the</sup> 2-qubit space  $\mathcal{H}_2 \otimes \mathcal{H}_2$  (the Bell basis).

Keep this procedure for generating the Bell states in mind — it will show up again later when we discuss superdense coding.

## d-dimensional systems

(5)

Everything we've discussed extends straightforwardly to d-dimensional systems:

I: States are vectors in  $\mathcal{H}_d \equiv \mathbb{C}^d$ .

II: Reversible evolution is given by dxd unitary matrices.

III: Measurements are characterized by sets of orthogonal dxd projectors (or, by Hermitian dxd observables).

IV: The space of a composite system of  $d_1$  and  $d_2$ -dimension subsystems is

$$\mathcal{H}_{d_1} \otimes \mathcal{H}_{d_2} = \mathcal{H}_{d_1 d_2}.$$

Note that there are d-dimensional versions of maximally entangled states; for example,

$$\sum_{j=1}^d \frac{1}{\sqrt{d}} |j\rangle^A \otimes |j\rangle^B.$$

This is a special case of what is called a Schmidt decomposition. Given any state

$|\Psi\rangle^{AB} = \sum_{ij} t_{ij} |i\rangle^A \otimes |j\rangle^B$  on a 2-party composite system, we can find new bases  $\{|i\rangle^A\}$  and  $\{|j\rangle^B\}$  such that

$$|\Psi\rangle^{AB} = \sum_j \sqrt{\lambda_j} |\tilde{j}\rangle^A \otimes |j\rangle^B \quad (6)$$

i.e., there are no "off-diagonal" terms. The  $\lambda_j$ 's are all real and non-negative, and satisfy

$$\sum_j \lambda_j = 1$$

One can find this decomposition from the svd of the amplitudes  $t_{ij}$ :  $\underline{t} = [\underline{t}_{ij}]$

$$\underline{t} = \underline{U} \underline{D} \underline{V} \quad \underline{U} \& \underline{V} \text{ unitary}$$

$$\Rightarrow |\tilde{i}\rangle^A = \sum_j u_{ij} |j\rangle^A \quad |j\rangle^B = \sum_k v_{jk} |k\rangle^B$$

Two things that do not generalize to  $d > 2$  are the Bloch sphere and the Pauli matrices, at least not completely. One cannot keep all the properties of the Pauli matrices for  $d > 2$ , but one can keep some. For example, consider

$$X(k) |j\rangle \equiv |j+k \bmod d\rangle$$

$$Z(l) |j\rangle \equiv e^{2\pi i l j / d} |j\rangle$$

The set of  $d^2$  matrices

$$Z(l)X(k) \quad 0 \leq l, k \leq d-1$$

have similar properties to the Paulis, including unitarity, but they are not Hermitian.

## No-cloning

(7)

An important fact implied by the postulates of QM is that quantum states cannot be copied. There is no unitary s.t.

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \quad \forall |\psi\rangle$$

Here are two different ways of seeing this.

First  $U|0\rangle|0\rangle = |0\rangle|0\rangle$  and  $U|1\rangle|0\rangle = |1\rangle|1\rangle$ , plus linearity, implies

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|11\rangle \\ \neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

Another is the observation

$$\langle\psi|\phi\rangle\langle 0|0\rangle = \langle\psi|\psi\rangle, \text{ while}$$

$$\langle\psi|\phi\rangle\langle\psi|\phi\rangle = \langle\psi|\psi\rangle^2. \text{ But}$$

$$(\langle\psi|\langle 0|)U^\dagger U(|\psi\rangle|0\rangle) = \langle\psi|\phi\rangle\langle 0|0\rangle \neq \langle\psi|\phi\rangle^2 \text{ in general}$$

The only exceptions are  $\langle\psi|\psi\rangle = 1$  and  $\langle\psi|\psi\rangle = 0$ .

So cloners can only work reliably on orthogonal sets of states.

No-cloning has very important consequences for QIT. Also, if cloning were possible, it would enable FTL signaling, and allow one to measure the state  $|\psi\rangle$  w/o disturbance.

# Noisy QM

⑧

## I. Density matrices.

Suppose that we have incomplete or imperfect knowledge of a Q system's state. We could describe the system, in that case, by a probability distribution over state vectors, or an ensemble:

$$\mathcal{E} = \{ p_{\mathcal{X}}(x), |\psi_x\rangle \} \quad \text{where } x \text{ is an index that labels possible state vectors.}$$

For instance, we could have one of 4 states:

$$\mathcal{E} = \{ (1/4, |0\rangle), (1/4, |1\rangle), (1/4, |+\rangle), (1/4, |-\rangle) \}$$

This gives us an extra layer of classical randomness on top of any Q uncertainty.

It turns out that all observable consequences of an ensemble  $\mathcal{E}$  can be captured by the density matrix  $\rho$ :

$$\rho = \sum_x p_{\mathcal{X}}(x) |\psi_x\rangle \langle \psi_x|$$

← prob. of  $x$        $0 \leq p_{\mathcal{X}}(x) \leq 1$   
 $\sum_x p_{\mathcal{X}}(x) = 1$

↖ projector onto  $|\psi_x\rangle$

Note that while this looks similar to diagonal form, the  $\{|\psi_x\rangle\}$  need not be orthogonal.

Properties of  $\rho$ :

$$\text{Tr}(\rho) = 1, \quad \rho = \rho^\dagger, \quad \rho \geq 0$$

Note that while every ensemble has a unique density matrix, the reverse is NOT true. Many ensembles correspond to a given  $\rho$ .  
 The one exception is a pure state

$$\rho = |\psi\rangle\langle\psi|$$

This is the only density matrix that is also a projector:  $\rho^2 = \rho$ .

Since  $\rho$  is Hermitian we can diagonalize it:

$$\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$$

orthonormal states

$$\lambda_j \geq 0, \sum_j \lambda_j = 1$$

The eigenstates and eigenvalues also form an ensemble decomp. of  $\rho$ .

The most noisy state is the maximally mixed state  $\pi = I/d$ .

For qubits, we can use the Bloch sphere:

$$\rho = \frac{1}{2} (I + r_x X + r_y Y + r_z Z)$$

$$r_x = \sin\theta \cos\phi$$

$$r_y = \sin\theta \sin\phi$$

$$r_z = \cos\theta$$

$$0 \leq \theta \leq \pi, 0 \leq \phi < 2\pi$$

The pure states have  $\|\mathbf{r}\| = 1$ .

They are the surface of the sphere. Mixed states are in the interior.  $\pi$  is ~~at~~ at the center.