Lecture Notes

Quantum Cryptography Week 2: The Power of Entanglement

Contents

We already encountered quantum entanglement in the form of the EPR pair $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This week we will define entanglement more formally and explore some of the reasons that make it such an interesting topic in quantum information. To wet your appetite, let it already be said that in later weeks we will see that entanglement allows us to guarantee the security of communications based only on the laws of nature. We also know that entanglement is a necessary ingredient in the most impressive quantum algorithms, such as Shor's algorithm for factoring, and for quantum error correction.

2.1 Entanglement

If we combine two qubits A and B, each of which is in a pure state, the joint state of the two qubits is given by

$$|\psi\rangle_{AB} = |\psi_1\rangle_A \otimes |\psi_2\rangle_B \ . \tag{2.1}$$

Any two-qubit state that is either directly of this form, or is a mixture of states of this form, is called *separable*. Entangled state are states which are *not* separable. In other words, a pure state $|\psi\rangle$ is entangled if and only if

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \ , \tag{2.2}$$

for any possible choice of $|\psi_1\rangle$ and $|\psi_2\rangle$. A mixed state ρ is entangled if and only if it cannot be written as a convex combination of pure product states of the form in Eq. (2.1).

■ **Example 2.1.1** An example of an entangled state of two qubits is the EPR pair

$$|\text{EPR}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right) \ . \tag{2.3}$$

When we learn more about entanglement later on, we will see that this state is, in a precise sense, the "most entangled" state of two qubits. The EPR pair is thus often referred to as a *maximally entangled* state. (There are other two-qubit states which are different from the EPR pair but have just about the same "amount" of entanglement; we will learn about these other maximally entangled states later.) ■

We have already seen that the EPR pair has the special property that it can be written in many symmetric ways. For instance, in the Hadamard basis

$$\frac{1}{\sqrt{2}}\left(|++\rangle_{AB} + |--\rangle_{AB}\right) \ . \tag{2.4}$$

Thus measurements of both qubits in the standard basis, or the Hadamard basis, always produce the same outcome. In a few weeks we will see that this property can even be used to *characterize* the EPR pair: it is the only two-qubit state having this property!

Exercise 2.1.1 Suppose that ρ_{AB} is a two-qubit separable state. Show that if a measurement of both qubits of ρ_{AB} in the standard basis always yields the same outcome, then a measurement of both qubits in the Hadamard basis necessarily has non-zero probability of giving different outcomes. Deduce a proof that the EPR pair (2.3) is not a separable state. ■

Entanglement has another interesting property which we will see later, called "monogamy". Monogamy states that if two systems are maximally entangled with each other then they cannot have any entanglement with any other system: equivalently, they must be in tensor product with the remainder of the universe.

■ **Example 2.1.2** Consider the state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |11\rangle_{AB}) \ . \tag{2.5}$$

In contrast to the EPR pair in Example 2.1.1 this state is not entangled, since $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |1\rangle_B = |+\rangle_A \otimes |1\rangle_B$. ■

Definition 2.1.1 — Entanglement. Consider two quantum systems A and B. The joint state ρ_{AB} is *separable* if there exists a probability distribution $\{p_i\}_i$, and sets of density matrices $\{\rho_i^A\}_i, \{\rho_i^B\}_i$ such that

$$\rho_{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B. \tag{2.6}$$

If there exists no such decomposition ρ_{AB} is called *entangled*.
If $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$ is a pure state, then $|\Psi\rangle_{AB}$ is separable if and only if there exists $|\psi\rangle_A, |\psi\rangle_B$ such that

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B. \tag{2.7}$$

■ **Example 2.1.3** Consider the density matrix

$$\rho_{AB} = \frac{1}{2}|0\rangle\langle 0|_A \otimes |1\rangle\langle 1|_B + \frac{1}{2}|+\rangle\langle +|_A \otimes |-\rangle\langle -|_B. \tag{2.8}$$

Such a state is in the form of Eq. (2.6), so it is not entangled: it is separable. Note that this does not imply that the systems A and B are necessarily independent: here they are correlated, but not entangled. (We would typically say that they are "classically correlated".) ■

■ **Example 2.1.4** Any cq-state, i.e. a state of the form $\rho_{XQ} = \sum_i p_i |x\rangle\langle x|_X \otimes \rho_x^Q$, is separable. ■

It is important to make the distinction between the two states

$$\rho_{AB} = \frac{1}{2}|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + \frac{1}{2}|1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \qquad \text{and} \qquad \sigma_{AB} = |\text{EPR}\rangle\langle\text{EPR}|_{AB}. \tag{2.9}$$

For the state ρ_{AB}, if A is measured in the standard basis then whenever $|0\rangle_A$ is observed the state on B is $|0\rangle_B$; likewise when $|1\rangle_A$ is observed, the state on B is $|1\rangle_B$. This is also true for σ_{AB}. However, consider measuring system A of ρ_{AB} in the Hadamard basis. The corresponding measurement operators are $|+\rangle\langle +|_A \otimes \mathbb{I}_B, |-\rangle\langle -|_A \otimes \mathbb{I}_B$. The post-measurement state conditioned on obtaining the outcome $|+\rangle_A$ is then

$$\rho_{|+_A}^{AB} = \frac{(|+\rangle\langle +|_A \otimes \mathbb{I}_B)\rho_{AB}(|+\rangle\langle +|_A \otimes \mathbb{I}_B)}{\text{tr}((|+\rangle\langle +|_A \otimes \mathbb{I}_B)\rho_{AB})} \tag{2.10}$$

$$= 2 \cdot \left(\frac{1}{2}\frac{1}{2}|+\rangle\langle +|_A \otimes |0\rangle\langle 0|_B + \frac{1}{2}\frac{1}{2}|+\rangle\langle +|_A \otimes |1\rangle\langle 1|_B\right) \tag{2.11}$$

$$= |+\rangle\langle +|_A \otimes \frac{\mathbb{I}_B}{2}, \tag{2.12}$$

and we see that the reduced state on B, $\rho_{|+_A}^B = \frac{\mathbb{I}_B}{2}$ is maximally mixed. In contrast, using that the state $|\text{EPR}\rangle_{AB}$ can be rewritten as

$$|\text{EPR}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}}(|++\rangle_{AB} + |--\rangle_{AB}), \tag{2.13}$$

when σ_{AB} is measured with respect to the Hadamard basis on system A, conditioned on the outcome $|+\rangle_A$, the reduced state on B is $\sigma_{|+_A}^B = |+\rangle\langle +|_B$. In particular this state is pure: it is very different from the totally mixed state we obtained by performing the same experiment on ρ_{AB}. This is a sense in which the correlations in σ_{AB} are stronger than those in ρ_{AB}.

2.2 Purifications

Last week we learned about the partial trace operation, which provides a way to describe the state of a subsystem when given a description of the state on a larger composite system. Even if the state of the larger system is pure, the reduced state can sometimes be mixed, and this is a signature of entanglement in the larger state.

Is it possible to reverse this process? Suppose given a density matrix ρ_A describing a quantum state on system A. Is it always possible to find a pure state $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$ such that $\mathrm{tr}_B(\rho_{AB}) = \rho_A$? Such a state is called a *purification* of ρ_A.

Definition 2.2.1 — Purification. Given any density matrix ρ_A, a pure state $|\Psi_{AB}\rangle$ is a *purification* of A if $\mathrm{tr}_B(|\Psi\rangle\langle\Psi|_{AB}) = \rho_A$.

Let's see how an arbitrary density matrix ρ_A can be purified. As a first step, diagonalize ρ_A, expressing it as a mixture

$$\rho_A = \sum_{j=1}^{d_A} \lambda_j |\phi_j\rangle\langle\phi_j| \,, \tag{2.14}$$

where λ_j are the (necessarily non-negative) eigenvalues of ρ_A and $|\phi_j\rangle$ the eigenstates. Since ρ_A is a density matrix the λ_j are non-negative and sum to 1. We've seen an interpretation of density matrices before: here we would say that ρ_A describes a quantum system that is in a probabilistic mixture of being in state $|\phi_j\rangle$ with probability λ_j. But who "controls" which part of the mixture A is in?

Let's introduce an imaginary system B which achieves just this. Let $\{|j\rangle_B\}_{j\in\{1,\ldots,d_B\}}$ be the standard basis for a system B of dimension $d_B = d_A$, and consider the pure state

$$|\Psi\rangle_{AB} = \sum_{j=1}^{d_A} \sqrt{\lambda_j} |\phi_j\rangle_A \otimes |j\rangle_B \,, \tag{2.15}$$

where $\{|j\rangle_B\}_j$ is the standard basis on system B. Suppose we were to measure the B system of $|\Psi\rangle_{AB}$ in the standard basis. We know what would happen: we will obtain outcome j with probability $\langle\Psi|_{AB} M_j |\Psi\rangle_{AB}$, where $M_j = \mathbb{I}_A \otimes |j\rangle\langle j|_B$, and a short calculation will convince you this equals λ_j. Since we're using a projective measurement, we can describe the post-measurement state easily as being proportional to $M_j|\Psi\rangle\langle\Psi|_{AB}M_j$, and looking at the A system only we find that it is $|\phi_j\rangle\langle\phi_j|_A$.

To summarize, a measurement of system B gives outcome j with probability λ_j, and the post-measurement state on A is precisely $|\phi_j\rangle\langle\phi_j|$. This implies that $\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{AB}) = \rho_A$, a fact which can be verified directly using the mathematical definition of the partial trace operation.

Are purifications unique? You'll notice that in the above construction we made the choice of the standard basis for system B, but any other basis would have worked just as well. So it seems like we at least have a choice of basis on system B: there is a "unitary degree of freedom". To see that this is the only freedom that we have in choosing a purification, we first need to learn about a very convenient representation of bipartite pure states, the *Schmidt decomposition*.

2.2.1 The Schmidt decomposition

The purification that we constructed in (2.15) has a special form: it is expressed as a sum, with non-negative coefficients whose squares sum to 1, of tensor products of basis states for the A and B systems respectively. As we saw, this particular form is convenient because it lets us compute the reduced states in A and B very easily. Unfortunately, not every state is always given in this way: for example, if we write $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |+\rangle_A|1\rangle_B)$ then the two states $|0\rangle_A, |+\rangle_A$ on A are not orthogonal. But maybe the same state can be written in a more convenient form? The answer is yes, and it is given by the Schmidt decomposition.

Theorem 2.2.1 — Schmidt decomposition. Consider quantum systems A and B with dimensions d_A, d_B respectively, and let $d = \min(d_A, d_B)$. Any pure bipartite state $|\Psi\rangle_{AB}$ has a Schmidt decomposition

$$|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{\lambda_i} |u_i\rangle_A |v_i\rangle_B, \tag{2.16}$$

where $\lambda_i \geq 0$ and $\{|u_i\rangle_A\}_i, \{|v_i\rangle_B\}_i$ are orthonormal vector sets. The coefficients $\sqrt{\lambda_i}$ are called the *Schmidt coefficients* and $|u_i\rangle_A, |v_i\rangle_B$ the *Schmidt vectors*.

We discussed the proof of the theorem in the video module; you can also find a detailed proof in Section 2.5 of [NC01]. The main idea is to start by expressing $|\Psi\rangle_{AB} = \sum_{j,k} \alpha_{j,k} |j\rangle_A |k\rangle_B$ using the standard bases of A and B, and then write the singular value decomposition of the $d_A \times d_B$ matrix with coefficients $\alpha_{j,k}$ to recover the $\sqrt{\lambda_i}$ (the singular values) and the $|u_i\rangle_A$ (the left eigenvectors) and the $|v_i\rangle_B$ (the right eigenvectors).

The Schmidt decomposition has many interesting consequences. A first consequence is that it provides a simple recipe for computing the reduced density matrices: given a state of the form (2.16), we immediately get $\rho_A = \sum_i \lambda_i |u_i\rangle\langle u_i|_A$, and $\rho_B = \sum_i \lambda_i |v_i\rangle\langle v_i|_B$. An important observation is that ρ_A and ρ_B have the same eigenvalues, which are precisely the squares of the Schmidt coefficients. As a consequence, given any two density matrices ρ_A and ρ_B, there exists a pure bipartite state $|\Psi\rangle_{AB}$ such that $\rho_A = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{AB})$ and $\rho_B = \mathrm{Tr}_A(|\Psi\rangle\langle\Psi|_{AB})$ if and only if ρ_A and ρ_B have the same spectrum! Without the Schmidt decomposition this is not at all an obvious fact to prove.

The same observation also implies that the Schmidt coefficients are uniquely defined: they are the square roots of the eigenvalues of the reduced density matrix. The Schmidt vectors are also unique, up to degeneracy and choice of phase: if an eigenvalue has an associated eigenspace of dimension 1 only then the associated Schmidt vector must be the corresponding eigenvector. If the eigenspace has dimension more than 1 we can choose as Schmidt vectors any basis for the subspace. And note that in (2.16) we can always multiply $|u_i\rangle$ by $e^{i\theta_i}$, and $|v_i\rangle$ by $e^{-i\theta_i}$, so there is a phase degree of freedom.

Another important consequence of the Schmidt decomposition is that it provides us with a way to measure entanglement between the A and B systems in a pure state $|\Psi_{AB}\rangle$. A first, rather rough but convenient such measure is given by the number of non-zero coefficients $\sqrt{\lambda_j}$. This measure is the so-called *Schmidt rank*. If the Schmidt rank is 1 then the state is a product state, and if it is strictly larger than 1 then the state is entangled.

Definition 2.2.2 — Schmidt rank. For any bipartite pure state with Schmidt decomposition $|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{\lambda_i} |a_i\rangle_A |b_i\rangle_B$, the *Schmidt rank* is defined as the number of non-zero coefficients $\sqrt{\lambda_i}$. It is also equal to $\mathrm{rank}(\rho_A)$ and $\mathrm{rank}(\rho_B)$.

The Schmidt coefficients provide a finer way to measure entanglement than the Schmidt rank. A natural measure, called "entropy of entanglement", consists in taking the entropy of the distribution specified by the squares of the coefficients. If the entropy is 0 then there is only a single coefficient equal to 1, and the state is not entangled. But as soon as the entropy is positive the state is entangled. This measure is finer than the Schmidt rank. For example, it distinguishes the entanglement in the two states

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \qquad \text{and} \qquad |\phi\rangle = \sqrt{1-\varepsilon}|00\rangle + \sqrt{\varepsilon}|11\rangle.$$

For small $0 < \varepsilon < 1/2$ both states have the same Schmidt rank, but the first one has entanglement entropy 1 whereas the second has entanglement entropy $H(\varepsilon)$ (where H is the binary entropy

function) going to 0 as $\varepsilon \to 0$. This is the reason why we call the EPR pair "maximally entangled": its entanglement entropy is maximal among all two-qubit states.

2.2.2 Uhlmann's theorem

Let's return to the topic of the freedom in choosing purifications of a density matrix. We saw that we at least had a unitary degree of freedom by choosing a basis on the purifying system B. Uhlmann's theorem states that this is precisely the only freedom we have.

Theorem 2.2.2 — Uhlmann's theorem. Suppose given a density matrix ρ_A and a purification of A given by $|\Psi\rangle_{AB}$. Then another state $|\Phi\rangle_{AB}$ is also a purification of A if and only if there exists a unitary U_B such that

$$|\Phi\rangle_{AB} = \mathbb{I}_A \otimes U_B |\psi\rangle_{AB}. \tag{2.17}$$

We already saw a proof of the "if" part of the theorem. To show the converse, i.e. that two purifications must always be related by a unitary, consider the Schmidt decomposition:

$$|\Phi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |u_i\rangle_A |v_i\rangle_B,$$
$$|\Psi\rangle_{AB} = \sum_i \sqrt{\mu_i} |w_i\rangle_A |z_i\rangle_B.$$

As we know the λ_i are uniquely defined: they are the eigenvalues of ρ_A. So if $|\Phi\rangle_{AB}$ and $|\Psi\rangle_{AB}$ are both purifications of the same ρ_A, we must have $\lambda_i = \mu_i$. Now suppose for simplicity that all eigenvalues are non-degenerate. Then the $|u_i\rangle_A$ are also uniquely determined: they are the eigenvectors of ρ_A associated to the λ_i. Therefore $|u_i\rangle_A = |w_i\rangle_A$ as well! Thus we see that the only choice we have left are the $|v_i\rangle_B$, or $|z_i\rangle_B$: since the density matrix ρ_B of the purification is not specified a priori, we may choose any orthonormal basis of the B system. Since any two orthonormal bases of the same space are related by a unitary matrix, this choice of basis is precisely the degree of freedom that is guaranteed by Uhlmann's theorem.

2.3 Secret sharing

Let's discuss a cryptographic application of the notions we just introduced. The application is called *secret sharing*. Imagine a country owns nuclear weapons yet wants to make sure that both the queen (Alice) and king (Bob) have to come together to activate them. One solution would be to give half of the launch codes $s = (s_1, \ldots, s_\ell) \in \{0,1\}^\ell$ to Alice, and the other half to Bob, thereby making sure that they both need to reveal their share of the information in order for the weapons to be activated. A drawback of this scheme is that each of them does have significant information about the launch codes, namely half of the bits. And what if there is only one bit? (Although that wouldn't be very secure, would it...)

The goal in a secret sharing scheme is to divide the information s into shares in such a way that any unauthorized set of parties (in the example, Alice or Bob alone) cannot learn *anything* at all about the secret. Remembering the idea behind the one-time pad, a much better scheme would be to choose a random string $r \in \{0,1\}^\ell$ and give r to Alice and $r \oplus s$ to Bob. In this case neither Alice nor Bob individually has any information about s; their respective secrets appear uniformly random. Yet when they come together they can easily recover s!

From the example above we see that given a random classical bit one can construct a secret sharing scheme between Alice and Bob that shares a single secret bit s. However they can do better if they are each given a qubit instead. Consider the case that Alice and Bob are given one of the

following four states at random:

$$|\psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}), \qquad |\psi_{01}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB}), \tag{2.18}$$

$$|\psi_{10}\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}), \qquad |\psi_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}). \tag{2.19}$$

These states are called the *Bell states*. Observe that they are orthonormal and thus form a basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$. We've already calculated the reduced density on Alice's system of one of those states, the EPR pair $|\psi_{00}\rangle_{AB}$:

$$\begin{aligned}
\rho_{00}^A &= \mathrm{tr}_B(|\psi_{00}\rangle\langle\psi_{00}|_{AB}) \\
&= \frac{1}{2}\big(|0\rangle\langle 0|_A \,\mathrm{tr}_B(|0\rangle\langle 0|_B) + |0\rangle\langle 1|_A \,\mathrm{tr}_B(|0\rangle\langle 1|_B) \\
&\qquad + |1\rangle\langle 0|_A \,\mathrm{tr}_B(|1\rangle\langle 0|_B) + |1\rangle\langle 1|_A \,\mathrm{tr}_B(|1\rangle\langle 1|_B)\big) \\
&= \frac{1}{2}(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A) = \frac{\mathbb{I}_A}{2}.
\end{aligned}$$

Calculating the reduced states on either A or B for each each of these states always gives the same result,

$$\rho_{00}^A = \rho_{01}^A = \rho_{10}^A = \rho_{11}^A = \frac{\mathbb{I}}{2}, \tag{2.20}$$

$$\rho_{00}^B = \rho_{01}^B = \rho_{10}^B = \rho_{11}^B = \frac{\mathbb{I}}{2}. \tag{2.21}$$

We know what this means: since the reduced state on each subsystem is maximally mixed, neither Alice nor Bob can gain any information on which of the states $|\psi_{00}\rangle_{AB}, |\psi_{01}\rangle_{AB}, |\psi_{10}\rangle_{AB}, |\psi_{11}\rangle_{AB}$ they have one qubit of! However, due to the fact that these states together form a basis, when Alice and Bob come together they can perform a measurement in that basis that perfectly distinguishes which state they have, yielding two bits of information.

Exercise 2.3.1 Suppose there are now three parties, Alice, Bob and Charlie (the prime minister is also given a share of the nuclear codes!). Give a secret sharing scheme, based on a tripartite entangled state, such that no individual party has any information about the secret but the three of them together are able to recover the secret. Better: can you give a scheme such that no two of them has any information about the secret. Different: give a scheme such that no individual has any information about the secret, but any group of two can recover it. ∎

Application: Superdense coding

A different application of the usefulness of entanglement is to *superdense coding*. The task in dense coding consists in sending classical bits of information from Alice to Bob by encoding them in a quantum state that is as small as possible. Let's see how using entanglement we can send two classical bits using a single qubit.

Suppose Alice and Bob share the state $|\psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, and that Alice performs a unitary on her qubit as indicated in Table 2.1, depending on which bits $ab \in \{00, 01, 10, 11\}$ she wants to send to Bob.

As we already saw, the four states on the right-hand side in Table 2.1 form the Bell basis, and in particular they are perfectly distinguishable. Hence if Alice sends her qubit over to Bob, he can perform a measurement in the Bell basis and recover both of Alice's classical bits.

Classical information a,b	Unitary $X_A^a Z_A^b$	Final joint state
00	$\mathbb{I}_A$	$\frac{1}{\sqrt{2}}(\|00\rangle_{AB} + \|11\rangle_{AB})$
01	X_A	$\frac{1}{\sqrt{2}}(\|10\rangle_{AB} + \|01\rangle_{AB})$
10	Z_A	$\frac{1}{\sqrt{2}}(\|00\rangle_{AB} - \|11\rangle_{AB})$
11	$-X_A Z_A$	$\frac{1}{\sqrt{2}}(\|01\rangle_{AB} - \|10\rangle_{AB})$

Table 2.1: Unitary operation performed by Alice in order to encode her two classical bits $ab \in \{0,1\}^2$.

2.4 Bell-Nonlocality

Entanglement has many counter-intuitive properties, many of which we will discover during the course of this lecture series. A very important one is that it allows correlations between two particles — two qubits — that cannot be replicated classically. The very first example of such correlations was demonstrated in [Bel64], where Bell proved that the predictions of quantum theory are incompatible with those of any classical theory satisfying a natural notion of *locality*.

The modern way to understand Bell non-locality is by means of so-called non-local games (see [Bru+14] for a detailed review on Bell non-locality). Let's imagine that we play a game with two players, which we'll again call Alice and Bob. Alice has a system A, and Bob has some system B. In this game, we will ask Alice and Bob questions, and collect answers. Let us denote the possible questions to Alice and Bob x and y, and label the answers a and b. We will play this game many times, and in each round choose the questions to ask with some probability $p(xy)$. As you might have guessed our little game has some rules. We denote these rules using a predicate $V(a,b|x,y)$, which takes the value "1" if a and b are winning answers for questions x and y. To be fair, Alice and Bob know the rules of the game given by $V(a,b|x,y)$, and also the distribution $p(xy)$. They can agree on any strategy before the game starts. However, once we start asking questions they are no longer allowed to communicate. Of interest to us will be the probability that Alice and Bob win the game, maximized over all possible strategies. That is,

$$p_{\text{win}} = \max_{\text{strategy}} \sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y)\, p(a,b|x,y) \ , \tag{2.22}$$

where $p(a,b|x,y)$ is the probability that Alice and Bob produce answers a and b given x and y according to their chosen strategy.

What are these strategies? In a classical world, Alice and Bob can only have a classical strategy. A deterministic classical strategy is simply given by functions $f_A(x) = a$ and $f_B(y) = b$ that take the questions x and y to answers a and b. We then have $p(a,b|x,y) = 1$ whenever $a = f_A(x)$ and $b = f_B(y)$, and $p(a,b|x,y) = 0$ otherwise. Possibly, Alice and Bob also use shared randomness. That is, they have another string r, which they share with probability $p(r)$. In physics, r is also referred to as a hidden variable, but we will take the more operational viewpoint of shared randomness. In a strategy using shared randomness r, classical Alice and Bob can however still only apply functions: $a = f_A(x,r)$ and $b = f_B(y,r)$. In terms of the probabilities we then have $p(a,b|x,y,r) = 1$ if $a = f_A(x,r)$ and $b = f_B(y,r)$ and $p(a,b|x,y,r) = 0$ otherwise. This gives

$$p(a,b|x,y) = \sum_r p(r) p(a,b|x,y,r) \ . \tag{2.23}$$

Does shared randomness help Alice and Bob? Note that for a classical strategy based on shared

randomness we have

$$p_{\text{win}} = \max_{class.strat.} \sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y) \sum_{r} p(r) p(a,b|x,y,r) \tag{2.24}$$

$$= \max_{class.strat.} \sum_{r} p(r) \Big(\sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y)\, p(a,b|x,y,r) \Big) \,. \tag{2.25}$$

Note that the quantity in brackets is largest for some particular value(s) of r. Since Alice and Bob want to maximize their winning probability, they can thus fix the best possible r giving a deterministic strategy $a = f_A(x,r)$ and $b = f_A(y,r)$ where r is now fixed.

Why would we care about this at all? It turns out that for many games, a *quantum* strategy can achieve a higher winning probability. This is of fundamental importance for our understanding of nature. What's more, however, observing a higher winning probability is a signature of entanglement: quantumly, Alice and Bob can achieve a higher winning probability *only* if they are entangled, making such games into *tests* for entanglement. Testing whether the stated shared by Alice and Bob is entangled forms a crucial element in quantum key distribution, as we will see in later weeks.

Specifically, a *quantum strategy* means that Alice and Bob can pick a state ρ_{AB} to share, and agree on measurements to perform depending on their respective questions. That is, x and y will label a choice of measurement, and a and b are the outcomes of that measurement.

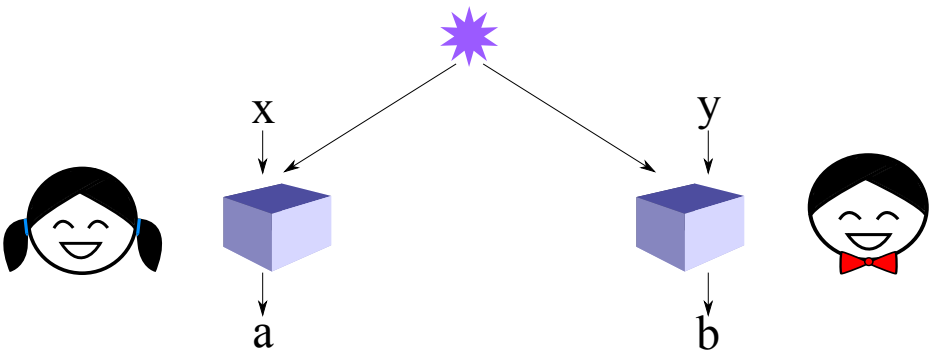

Figure 2.1: A non-local game. Alice and Bob are given questions x and y, and must return answers a and b. If Alice and Bob are quantum, then x and y label measurement settings and a and b are measurement outcomes.

2.4.1 Example of a non-local game: CHSH

Let us have a look at a very simple game based on the famous CHSH inequality. It will turn out to be extremely useful for quantum cryptography. At the start of the game, we send two bits x and y to Alice and Bob respectively, where we choose x with uniform probabilities $p(x=0) = p(x=1) = 1/2$ and y with probabilities $p(y=0) = p(y=1) = 1/2$. In turn, Alice and Bob will return answer bits a and b. Alice and Bob win the game if and only if

$$x \cdot y = a + b \mod 2 \,. \tag{2.26}$$

In terms of the predicate $V(a,b|x,y)$ this means that $V(a,b|x,y) = 1$ if $x \cdot y = a + b \mod 2$ and $V(a,b|x,y) = 0$ otherwise. We are interested in the probability that Alice and Bob win the game. This probability can be written as

$$p_{\text{win}}^{\text{CHSH}} = \frac{1}{4} \sum_{x,y \in \{0,1\}} \sum_{\substack{a,b \\ a+b \mod 2 = x \cdot y}} p(a,b|x,y) \,, \tag{2.27}$$

where $p(a,b|x,y)$ is the probability that Alice and Bob answer a and b given questions x and y. What can Alice and Bob do to win this game?

Classical winning probability

Classically, a is simply a function of x. For example, if $x=0$, then Alice and Bob could agree as part of their strategy that Alice will then always answer $a=0$. We see that as long as $x=0$ or $y=0$, then $x\cdot y=0$. In this case, Alice and Bob want to achieve $a+b \mod 2=0$. However, if $x=y=1$ then they would like to give answers such that $a+b \mod 2=1$. What makes this difficult for Alice and Bob is that they cannot communicate during the game. This means in particular that Alice's answer a can only depend on x (but not on y) and similarly Bob's answer b can only depend on y (but not on x).

It it not difficult to see (you may wish to check!) by trying out all possible strategies for Alice and Bob, that classically the maximum winning probability that can be achieved is

$$p_{\text{win}}^{\text{CHSH}}=\frac{3}{4}\,. \tag{2.28}$$

Alice and Bob can achieve this winning probability with the strategy of answering $a=b=0$ always, which means $a+b \mod 2=0$, which is correct in 3 out of the 4 possible cases. Only when $x=y=1$ will Alice and Bob make a mistake.

Quantum winning probability

It turns out that Alice and Bob can do significantly better with a quantum strategy, using shared entanglement. Indeed, suppose that Alice and Bob share an EPR pair, where we label the qubit held by Alice (A) and the one held by Bob (B).

$$|\Psi\rangle_{AB}=\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\right). \tag{2.29}$$

Suppose now that when $x=0$, Alice measures her qubit in the basis $\{|0\rangle,|1\rangle\}$. Otherwise when $x=1$, she measures in the basis $\{|+\rangle,|-\rangle\}$. Suppose furthermore that when $y=0$, Bob measures his qubit in the basis $|v_1\rangle,|v_2\rangle$ where

$$|v_1\rangle=\cos(\pi/8)|0\rangle+\sin(\pi/8)|1\rangle,\qquad |v_2\rangle=-\sin(\pi/8)|0\rangle+\cos(\pi/8)|1\rangle, \tag{2.30}$$

and when $y=1$, he measures in the basis $|w_1\rangle,|w_2\rangle$, where

$$|w_1\rangle=\cos(\pi/8)|0\rangle-\sin(\pi/8)|1\rangle,\qquad |w_2\rangle=\sin(\pi/8)|0\rangle+\cos(\pi/8)|1\rangle. \tag{2.31}$$

Consider the case where $x=0,y=0$. This means Alice measures in the basis $\{|0\rangle,|1\rangle\}$ and Bob in the basis $\{|v_1\rangle,|v_2\rangle\}$. The probability of winning, conditioned on $x=0,y=0$ is given by

$$\begin{aligned} p_{\text{win}|x=0,y=0} &= p(a=0,b=0|x=0,y=0)+p(a=1,b=1|x=0,y=0) && (2.32)\\ &= |\langle 0_A v_{1B}|\Psi_{AB}\rangle|^2+|\langle 1_A v_{2B}|\Psi_{AB}\rangle|^2 && (2.33)\\ &= 2\left|\frac{1}{\sqrt{2}}\cos\frac{\pi}{8}\right|^2=\cos^2\frac{\pi}{8}. && (2.34)\end{aligned}$$

The probability of winning, conditioned on $x=0,y=1$ is given by a similar expression

$$\begin{aligned} p_{\text{win}|x=1,y=0} &= p(a=0,b=0|x=1,y=0)+p(a=1,b=1|x=1,y=0) && (2.35)\\ &= |\langle 0_A w_{1B}|\Psi_{AB}\rangle|^2+|\langle 1_A w_{2B}|\Psi_{AB}\rangle|^2 && (2.36)\\ &= 2\left|\frac{1}{\sqrt{2}}\cos\frac{\pi}{8}\right|^2=\cos^2\frac{\pi}{8}. && (2.37)\end{aligned}$$

On the other hand,

$$p_{\text{win}|x=0,y=1} = p(a=0,b=0|x=0,y=1) + p(a=1,b=1|x=0,y=1) \tag{2.38}$$
$$= |\langle +_A v_{1B}|\Psi_{AB}\rangle|^2 + |\langle -_A v_{2B}|\Psi_{AB}\rangle|^2 \tag{2.39}$$
$$= \frac{1}{2}\left(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8} + \frac{1}{\sqrt{2}}\sin\frac{\pi}{8}\right)^2 + \frac{1}{2}\left(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8} + \frac{1}{\sqrt{2}}\sin\frac{\pi}{8}\right)^2 \tag{2.40}$$
$$= \frac{1}{2}\left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)^2. \tag{2.41}$$

Finally, you may easily verify that for $x = y = 1$, $p_{\text{win}|x=1,y=1} = p_{\text{win}|x=1,y=0} = \frac{1}{2}\left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)^2$. Also, convince yourself that $\frac{1}{2}\left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)^2 = \cos^2\frac{\pi}{8}$. This implies that

$$p_{\text{win}} = \frac{1}{4}\sum_{x,y} p_{\text{win}|x,y} = \cos^2\frac{\pi}{8} \approx 0.85. \tag{2.42}$$

2.4.2 Implications

This counterintuitive effect of entanglement has far reaching consequences. The first is of a rather conceptual nature, as you may have started wondering what actually happens if we "measure" a quantum particle. Could it be that every particle has a local classical "cheat sheet" attached to it, which specifies the outcome it will give for any possible measurement that we can make on it? Such a cheat sheet would correspond precisely to a classical strategy in the game above: For every x, Alice's qubit has some outcome a attached. In physics, such cheat sheets are also called local hidden variables.

The fact that quantum strategies can beat classical strategies in this game, however, implies that nature does not work that way! There are no classical cheat sheets, but nature is inherently quantum. Many experiments of ever increasing accuracy have been performed that verify that Alice and Bob can indeed achieve a higher winning probability in the CHSH game than the classical world would allow. Recently, an experiment has even proved this, by closing all possible loopholes (caused by experimental imperfections)[Hen+15]. This tells us that the world is not classical, but we need more sophisticated tools to describe it - such as quantum mechanics. It also means that when trying to build the ultimate computing and communication devices, we should make full use of what nature allows and go quantum.

We will later see how to use this simple game to verify the presence of entanglement, test unknown quantum devices, and even create secure encryption keys.

2.5 The monogamy of entanglement

Let's get back to the property mentioned in the very beginning of this lecture: that entanglement is monogamous. We know that two systems A and B can be in a joint pure state that is entangled, such as the "maximally entangled" EPR pair $|\text{EPR}\rangle_{AB}$. All our examples, however, had to do with entanglement between two systems A and B. But what about a third system, call it C for Charlie? Of course we could always consider three EPR pairs, $|\text{EPR}\rangle_{AB}$, $|\text{EPR}\rangle_{BC}$ and $|\text{EPR}\rangle_{AC}$. If this is the state of the three systems however we don't really want to talk about tripartite entanglement, because the correlations are always between any two of the three parties. Is it possible to create a joint state $|\Psi\rangle_{ABC}$ in which the strong correlations of the EPR pair are shared simultaneously between all three systems?

Let's first argue that, if we require that A and B are strictly in an EPR pair, then it is impossible for C to share any correlation with the qubits that form the EPR pair.

■ **Example 2.5.1** Let $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$. Then ρ_{AB} is pure, and in particular its only nonzero eigenvalue is $\lambda_1 = 1$. Thus by Uhlmann's theorem any purification of ρ_{AB} must have the form $\rho_{ABC} = |\Psi\rangle\langle\Psi|_{AB} \otimes |\Phi\rangle\langle\Phi|_C$ for an arbitrary state $|\Phi\rangle_C$ of system C. But this is a pure state with Schmidt rank across $AB : C$ equal to 1: it is not entangled! In fact you can see that the same consequence would hold as soon as AB is required to be in a pure state. In our example, you can further compute that $\rho_{AC} = \frac{\mathbb{I}}{2} \otimes \rho_C$, meaning that not only C is uncorrelated with A, but from the point of view of C A looks maximally mixed, i.e. it completely random. The same holds for ρ_{BC}. ■

2.5.1 Quantifying monogamy

The previous example demonstrates monogamy of the maximally entangled EPR pair. What about more general states, could they demonstrate entanglement across three different parties? This is possible to some extent, as is shown by the example of the GHZ state $|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. But the correlations in that state are weaker than those of a maximally entangled state. How do we make this statement precise?

One possibility is to use so-called *entanglement measures* $E(A : B)$. An entanglement measure is any function of bipartite density matrices that satisfies certain desirable properties. We already saw such a measure, the Schmidt rank; however it only applies to pure bipartite states. For states that are not pure the situation is much more complicated, and there is no standard entanglement measure that satisfies all the properties that we would like. Among these properties, there is one which expresses monogamy as follows: for any tripartite density matrix ρ_{ABC} it requires that

$$E(A : B) + E(A : C) \leq E(A : BC). \tag{2.43}$$

One way to interpret this inequality is that, whatever the *total* entanglement that A has with B and C (right-hand side), this entanglement must split additively between entanglement with B and with C (left-hand side). You may think this is obvious — but in fact very few entanglement measures are known to satisfy the monogamy inequality (2.43)!

2.5.2 A three-player CHSH game

Another, more intuitive way of measuring monogamy is through the use of nonlocal games, such as the CHSH game that we discussed in Section 2.4. First consider a three-player variant of this game where Alice would be required to successfully play the CHSH game simultaneously with two different partners, Bob and Charlie. That is, Alice would be sent a random x, Bob a random y and Charlie a random z; they would have to provide answers a, b and c respectively such that $xy = a + b \mod 2$ *and* $xz = a + c \mod 2$. Can they do it? The fact, discussed in Example 2.5.1, that the EPR pair has no entangled extension to three parties should give you a hint that things are going to be difficult for Alice!

In fact it is possible to make an even stronger statement. Consider now the following three-player variant of the CHSH game:

- The referee selects two of the three players at random, and sends each of them the message "You've been selected!".
- The referee plays the CHSH game with the selected players, sending each of them a random question and checking their answers for the CHSH condition. The third player is completely ignored.

Now, what do you think is the players' maximum success probability in this game? For the case of classical players the answer should be clear: $3/4$. Indeed, there is nothing more or less they can do in this variant than in the original two-player CHSH. (Make sure you are convinced of this fact. What is an optimal strategy for the three players?)

What about quantum players? Can they win with probability $\cos^2(\pi/8)$? Why not? Let's think of a possible extension of the two-player strategy we saw in Section 2.4.1. First of all we need the

three players, Alice, Bob and Charlie, to decide on an entangled state to share. Given they know two of them are going to be asked to play CHSH, it is natural to set things up with three EPR pairs, one between Alice and Bob, another between Bob and Charlie, and the third between Alice and Charlie.

Now the game starts, and two players are told they are to play the game. However, the crucial point to observe is that each of the selected players is not told with whom they are to play the game! So, for instance Alice will know she has been selected, but will not be told who is the other lucky winner — Bob or Charlie. Which EPR pair is she going to use to implement her strategy?

It turns out there is no answer to this question: Alice is stuck! Although we won't do it here, it is possible to show that the optimal winning probability in the three-player CHSH game described above, for quantum players, is no larger than the classical optimum: $3/4$. (See [Ton09] for more details if you are interested in seeing how to show this.) This is a powerful demonstration of monogamy of entanglement, showing in particular that there is no nice extension of the EPR pair to a tripartite state — at least not one that allows any two of them to win the CHSH game! We will return to a similar manifestation of monogamy by analyzing a "tripartite guessing game" next week.

Acknowledgements

 The lecture notes are written by Nelly Ng, Thomas Vidick and Stephanie Wehner. We thank David Elkouss, Kenneth Goodenough, Jonas Helsen, Jérémy Ribeiro, and Charles Xu for proofreading.

Important identities for calculations

Purification of states

Given any density matrix diagonalized as $\rho_A = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|_A$, a purification of A is

$$|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_A |w_i\rangle_B, \tag{2.44}$$

for any set of orthonormal vectors $\{|w_i\rangle_B\}_i$.

Schmidt decomposition of bipartite pure states

Any bipartite pure state $|\Psi\rangle_{AB}$ can be written into the form

$$|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{\lambda_i} |a_i\rangle_A |b_i\rangle_B, \tag{2.45}$$

where $\{|a_i\rangle_A\}_i, \{|b_i\rangle_B\}_i$ are orthonormal vector sets, and $\sum_{i=1}^{d} \lambda_i = 1$.

CHSH game winning probability

Consider Alice and Bob playing in a game, where questions $x, y \in \{0,1\}$ are sent to them, and they respond with answers $a, b \in \{0,1\}$ respectively. Alice and Bob win the game if $a + b \pmod 2 = x \cdot y$. The winning probability is given by

$$p_{\text{win}}^{\text{CHSH}} = \frac{1}{4} \sum_{x,y \in \{0,1\}} \sum_{\substack{a,b \\ a+b \\ \text{mod } 2 = x \cdot y}} p(a,b|x,y) \ . \tag{2.46}$$

For any classical strategy, $p_{\text{win}}^{\text{CHSH}} = \frac{3}{4}$.
If Alice and Bob shares an EPR pair, then $p_{\text{win}}^{\text{CHSH}} = \cos^2 \frac{\pi}{8} \approx 0.85$.

Bibliography

[Bel64] John S Bell. *On the Einstein Podolsky Rosen Paradox*. 1964 (cited on page 9).

[Bru+14] Nicolas Brunner et al. "Bell nonlocality". In: *Reviews of Modern Physics* 86.2 (2014), page 419 (cited on page 9).

[Hen+15] Bas Hensen et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". In: *Nature* 526.7575 (2015), pages 682–686 (cited on page 12).

[NC01] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2001 (cited on page 6).

[Ton09] Ben Toner. "Monogamy of non-local quantum correlations". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. Volume 465. 2101. The Royal Society. 2009, pages 59–69 (cited on page 14).