INTRODUCTION TO QUANTUM INFORMATION SCIENCE

Lecture 2

Quantum Entanglement

ARTUR EKERT

Updated February 12, 2018

The first lecture was about all kinds of weird things we can do with just one qubit. This lecture will be about two or more qubits. Stepping up from one qubit to two or more is a bigger leap than you might expect. In fact, already with two qubits we are in position to see some profound facts about quantum theory that took people decades to understand. Welcome to the world of quantum entanglement.

Before we discuss quantum entanglement let me start with a collection of *separable* qubits. Such a collection can be fully described by specifying the states of the constituent qubits, e.g. $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$. If we want to make it clear that we are looking at a composite quantum system of n qubits we write the state of the total system as

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle,$$

In the lore of quantum computation a collection of n qubits is known as a register of size n.

and say that $|\psi\rangle$ is a tensor product state of n qubits. For example, our standard computational basis for these n qubits is composed of tensor product vectors representing all binary strings of length n. We can manipulate tensor product states by operating on individual qubits. Take a quantum register of size three. It can store individual binary strings such as

$$\begin{aligned} |0\rangle \otimes |1\rangle \otimes |1\rangle &\equiv |011\rangle, \\ |1\rangle \otimes |1\rangle \otimes |1\rangle &\equiv |111\rangle, \end{aligned}$$

but it can also store the two of them simultaneously. For if we take the first qubit and instead of setting it to $|0\rangle$ or $|1\rangle$ we prepare a superposition $1/\sqrt{2}\,(|0\rangle + |1\rangle)$ then we obtain

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle \equiv \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle). \tag{1}$$

In fact we can prepare this register in a superposition of all eight binary strings; it is enough to put each qubit into the superposition $1/\sqrt{2}\,(|0\rangle + |1\rangle)$. This gives

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{2}$$

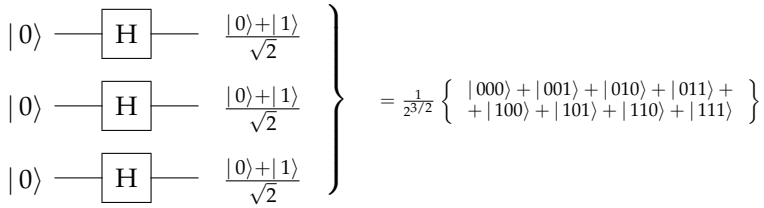
which can also be written as

$$\sum_{x\in\{0,1\}^3} |x\rangle = |000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle. \tag{3}$$

Here we have dropped the normalisation constant $2^{-3/2}$. We will often do it for the clarity of the exposition.

Such superpositions are usually prepared by applying Hadamard gates to individual qubits. The resulting unitary operation is known as the Hadamard Transform on n qubits and it is sufficiently important to deserve special mention.

1.1. **The Hadamard transform.** Most quantum computations start and end with this operation (or with its variant called the Quantum Fourier Transform, about which later). Like the Hadamard gate in the quantum interference circuit, the Hadamard Transform opens and closes a multi-qubit quantum interference. Everything that controls this interference is sandwiched between the Hadamard Transforms. At the very beginning of our quantum computation, if we have no prior information indicating that some inputs are better than other, we prepare an equally weighted superposition of all possible inputs. It makes sense, right, for what else can we do? We usually set all qubits to $|0\rangle$ and apply the Hadamard gate to each qubit, e.g.



This circuit can be fully described by the tensor product of the three Hadamard matrices, $H \otimes H \otimes H$. This is a $2^3 \times 2^3$ matrix. We can start with H, evaluate $H \otimes H$,

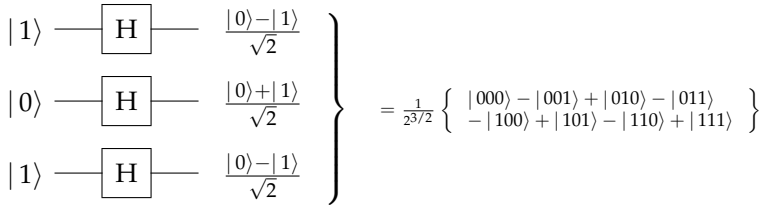
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad H \otimes H = \frac{1}{2} \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right],$$

and once we have this we can tensor it again, $(H \otimes H) \otimes H = H \otimes H \otimes H$,

$$H \otimes H \otimes H = \left(\frac{1}{2}\right)^{\frac{3}{2}} \left[\begin{array}{cc|cc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right].$$

Can you find the entry $(H \otimes H \otimes H)_{010,101}$?

The rows and columns of $H \otimes H \otimes H$ are labelled by the triplets $000, 001, \ldots, 111$. Want to write down $H \otimes H \otimes H \otimes H$? I don't think so. This is an exponentially growing monster so, when it comes to analysing such operations, instead of writing humongous matrices we prefer to start with a specific input and evaluate the corresponding output, e.g. suppose we apply the Hadamard transform to state $|101\rangle$,



The input state $|101\rangle$ evolves into

$$|101\rangle \mapsto \left(\frac{1}{2}\right)^{\frac{3}{2}} (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle). \tag{4}$$

We drop the normalisation and expand the tensor product to obtain

$$|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle\,.$$

As you can see, this is also an equally weighted superposition of all binary strings of size three, but some terms, exactly half of them in fact, acquired the minus sign. Clearly, the minus signs originate from the Hadamard operation on the first and the third qubit, thus whenever we see 1 in the first or the third location in the binary string we flip the sign in front of this particular term. In fact, there is a simple formula that tells us where to place the minus sign. If we start with a register of size n in some computational basis state $|x\rangle$, where $x \in \{0,1\}^n$, then

$$|\,x\rangle \mapsto \left(\frac{1}{2}\right)^{\frac{n}{2}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}\,|\,y\rangle\,, \tag{5}$$

where the product of the two binary strings $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is taken bit by bit:

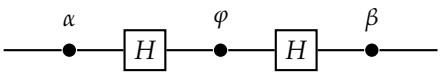
$$x \cdot y = (x_1 y_1 \oplus \ldots \oplus x_n y_n). \tag{6}$$

Binary addition
$0 \oplus 0 = 1 \oplus 1 = 0$
$0 \oplus 1 = 1 \oplus 0 = 1$

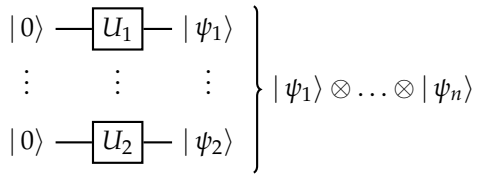
As we vary y, which takes all possible values in $\{0,1\}^n$, the expression $(-1)^{x\cdot y}$ gives as many plus as minus signs, i.e. the expression $x \cdot y$ gives as many zeros as ones.

For any binary strings a, b and c of the same length, we have:
$a \cdot b = b \cdot a$
$(a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c)$.

1.2. **Tensor product operations.** We know that any unitary operation on a qubit (up to an overall multiplicative phase factor) can be implemented by a circuit containing just two Hadamards and three phase gates, with adjustable phase settings,



Thus Hadamard gates and phase gates can be used to transform, for example, the input state $|0\rangle \otimes \ldots \otimes |0\rangle$ of n qubits into any tensor product state of n qubits,



Here we have n independent unitary operations, $U_1, \ldots, U_n$, each can be constructed with just two Hadamards and three phase gates, acting in parallel on n different qubits. The overall action of this circuit is described by the tensor product operator $U_1 \otimes \ldots \otimes U_n$. As we have seen, one useful operation of this type is the Hadamard transform. However, such operations do not explore the whole vastness of the tensor product of Hilbert spaces. Single qubit unitaries acting in parallel leave separable states separable, e.g. for two qubits,

$$(U_1 \otimes U_2)\,|\,\psi_1\rangle \otimes |\,\psi_2\rangle = (U_1\,|\,\psi_1\rangle) \otimes (U_2\,|\,\psi_2\rangle).$$

Restricting our attention to such states is like exploring the tip of the iceberg. Let us go for the full immersion.

1.3. **Quantum entanglement.** I have already mentioned that the most interesting quantum phenomena involve not one but many qubits interacting with each other. Take, for example, two qubits. When they interact they may loose their own identity and get entangled; they cannot be described by a product state anymore. For example, compare the two states,

$$\frac{1}{\sqrt{2}}(|\,00\rangle + |\,01\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle). \tag{7}$$

The first one is separable for we can write it as the tensor product

$$\frac{1}{\sqrt{2}}(|\,00\rangle + |\,01\rangle) = |\,0\rangle \otimes \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle),$$

whilst the second state does not admit such a decomposition,

$$\frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle) \neq |\,\psi_1\rangle \otimes |\,\psi_2\rangle\,, \tag{8}$$

hence we say that it is an entangled state. Any bipartite state that cannot be written as a tensor product of two states pertaining to the constituent subsystems is called entangled. There is lots of interesting physics behind this innocuous mathematical

statement. For example, think again about the state $|00\rangle + |11\rangle$. What happens if you measure just the first qubit? It is equally likely that you get $|00\rangle$ or $|11\rangle$, right? Now, why might that be disturbing? Imagine the second qubit to be light-years away from the first one. It seems that that the measurement of the first qubit affects the second qubit right away, and that implies faster-than-light communication! This is what Einstein called "spooky action at a distance". But can you actually use this effect to send a message faster than light? What would happen if you tried? I hope you can see that it would not work, for the result of the measurement is random — you cannot choose the bit value you want to send. We shall return to this and related phenomena later on.

Spooky action at a distance is a loose translation of the German "spukhafte Fernwirkung", the term Albert Einstein used in his 1947 letter to Max Born.

Now, even though an entangled state cannot be written as a tensor product it can always be written as a linear combination of vectors from the tensor product basis. In fact any state of two qubits $|\psi\rangle$ can be written as

$$\begin{aligned} |\psi\rangle &= c_{00}\,|0\rangle\otimes|0\rangle + c_{01}\,|0\rangle\otimes|1\rangle + c_{10}\,|1\rangle\otimes|0\rangle + c_{11}\,|1\rangle\otimes|1\rangle \\ &\equiv c_{00}\,|00\rangle + c_{01}\,|01\rangle + c_{10}\,|10\rangle + c_{11}\,|11\rangle\,, \end{aligned} \tag{9}$$

but only very few states of two qubits can be written directly as tensor products, $|\psi\rangle = |\psi_1\rangle\otimes|\psi_2\rangle$. Most state vectors simply do not admit such a decomposition. Indeed, taking into account the normalisation condition we need only two real parameters to specify a state vector of a single qubit (up to an overall phase factor), so, we need four real parameters to describe any separable state vector of two qubits. In contrast, we need six real parameters to describe the most general state vector of two qubits (the four complex coefficients c_{ij} are restricted by the normalisation condition and we ignore an overall phase factor). Assuming that all quantum states were created equal (this is not a trivial assumption) if you were to pick up a random state of two qubits your chances of picking up a separable state are of measure zero.

In general, given n qubits we need $2(2^n-1)$ real parameters to describe their state vector, but only $2n$ to describe separable states.

1.4. **The Schmidt decomposition.** In general, an arbitrary vector in the Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$ pertaining to a composite system $\mathcal{A}+\mathcal{B}$ can be expanded as

$$|\psi\rangle = \sum_{ij} c_{ij}\,|a_i\rangle\,|b_j\rangle\,,$$

where $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$ are orthonormal basis for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Moreover, for each particular bipartite state $|\psi\rangle$ we can find orthonormal bases, $\{|\tilde{a}_i\rangle\}$ in $\mathcal{H}_A$ and $\{|\tilde{b}_j\rangle\}$ in $\mathcal{H}_B$ such that $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \sum_{i} d_i\,|\tilde{a}_i\rangle\,|\tilde{b}_i\rangle\,,$$

where the coefficients d_i are nonnegative numbers. This is known as the Schmidt decomposition of the bipartite state $|\psi\rangle$. Any bipartite state can be expressed in this form but remember that the bases used depend on the state being expanded. Given two bipartite states $|\psi\rangle$ and $|\phi\rangle$ we usually cannot perform the Schmidt decomposition using the same orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$. The number of terms in the Schmidt decomposition is, at most, the minimum of $\dim\mathcal{H}_A$ and $\dim\mathcal{H}_A$.

1.5. **Density operators and the like.** The existence of entangled states begs an obvious question: if we cannot attribute a state vectors to an individual qubit then how shall we describe its quantum state? In the next few lectures we will see that when we limit our attention to a part of a larger system, then states are not represented by vectors, measurements are not described by orthogonal projections and evolution is not unitary. As a spoiler, here is a list of few new concepts that will be introduced soon.

$$\begin{array}{rcl} \text{state vectors} & \mapsto & \text{density operators} \\ \text{unitary evolution} & \mapsto & \text{completely positive trace preserving map} \\ \text{orthogonal projectors} & \mapsto & \text{positive operator-valued measure} \end{array}$$

1.6. **A long mileage out of controlled-NOT a.k.a. controlled-X.** In order to generate entanglement we need interactions between qubits. For now we will talk about entangling gates, that is, simple unitary operations that can entangle two qubits, and we will discuss how to implement them in one of the future lectures. The most popular two-qubit gate, and I mean the most popular by far, is the controlled-NOT (C-NOT), also known as the controlled-X gate (here X refers to the Pauli $\sigma_x \equiv X$ operation that effects the bit-flip) or the measurement gate. The gate acts on two qubits — it flips the second (target) qubit if the first (control) qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$. It is represented by the unitary matrix

$$\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

C-NOT gate

$|x\rangle\,|y\rangle \mapsto |x\rangle\,|x \oplus y\rangle$

$$\text{C-NOT} = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right] \qquad \begin{array}{l} |x\rangle \\ |y\rangle \end{array} \!\!\begin{array}{c} \text{---}\bullet\text{---} \\ \text{---}\oplus\text{---} \end{array}\!\! \begin{array}{l} |x\rangle \\ |x \oplus y\rangle \end{array} \tag{10}$$

where $x, y = 0$ or 1 and $\oplus$ denotes XOR or addition modulo 2. We can write this operation as

$$|x\rangle\,|y\rangle \mapsto |x\rangle\,|x \oplus y\rangle\,.$$

The gate is described by the matrix that does not admit any tensor product decomposition, but it can be written as the sum of tensor products

$$|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|),$$

or

$$|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X,$$

where X is the Pauli bit-flip operation. Let me now discuss all kind of interesting things that you can and cannot do with a controlled-NOT gate.

Make sure that you understand how the Dirac notation is used here. Think why the expression $|0\rangle\langle 0| \otimes A + |1\rangle\langle 1| \otimes B$ means "if the first qubit is in state $|0\rangle$ apply A to the second one but if the first qubit is in state $|1\rangle$ apply B to the second one". What happens if the first qubit in a superposition of $|0\rangle$ and $|1\rangle$?

1.7. **Thou shalt not clone.** Let me start with something that controlled-NOT seems to be doing but in fact it doesn't. It is easy to see that the C-NOT can copy the bit value of the first qubit,

$$|x\rangle|0\rangle \mapsto |x\rangle|x\rangle \qquad x = 0, 1. \tag{11}$$

One might suppose that this gate could also be used to copy superpositions such as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, so that

$$|\psi\rangle|0\rangle \mapsto |\psi\rangle|\psi\rangle \tag{12}$$

for any $|\psi\rangle$. This is not so! The unitarity of the C-NOT requires that the gate turns superpositions in the control qubit into *entanglement* of the control and the target. If the control qubit is in a superposition state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $(\alpha, \beta \neq 0)$, and the target in $|0\rangle$ then the C-NOT generates the entangled state

Quantum states cannot be cloned.

$$(\alpha|0\rangle + \beta|1\rangle)\,|0\rangle \mapsto \alpha|00\rangle + \beta|11\rangle. \tag{13}$$

In fact, it is impossible to clone an unknown quantum state. To see this assume that you can build a universal quantum cloner. Take any two normalised states $|\psi_1\rangle$ and $|\psi_2\rangle$ which are non-identical ($|\langle\psi_1|\psi_2\rangle| \neq 1$) and non-orthogonal ($\langle\psi_1|\psi_2\rangle \neq 0$), and run your hypothetical cloning machine,

$$|\psi_1\rangle|0\rangle|W\rangle \mapsto |\psi_1\rangle|\psi_1\rangle|W'\rangle, \tag{14}$$

$$|\psi_2\rangle|0\rangle|W\rangle \mapsto |\psi_2\rangle|\psi_2\rangle|W''\rangle. \tag{15}$$

Here, the third system, initially in state $|W\rangle$, represents everything else (say, the internal state of the cloning machine). For this be a unitary transformation which preserves the inner product hence we must require

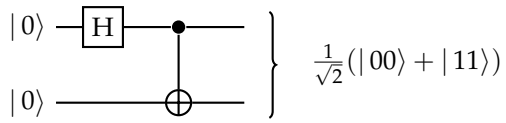
$$\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2\langle W'|W''\rangle, \tag{16}$$

which can only be satisfied when $|\langle\psi_1|\psi_2\rangle| = 0$ or 1, which contradicts our assumptions. Thus states of qubits, unlike states of classical bits, cannot be faithfully cloned. This leads to interesting applications, quantum cryptography being one such.

1.8. **The Bell states and the Bell measurement.** Here is a simple circuit that demonstrates the entangling power of C-NOT

For whom the bell tolls

John Stewart Bell (1928–1990) was a Northern Irish physicist.



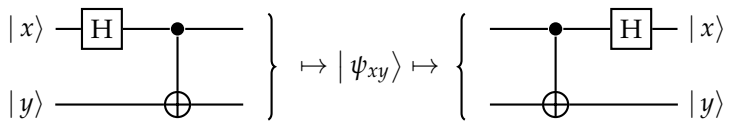
The separable input $|0\rangle|0\rangle$ evolves as

$$\begin{aligned} |0\rangle|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle \quad &= \quad \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle \\ &\xrightarrow{\text{C-NOT}} \quad \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle, \end{aligned} \tag{17}$$

resulting in the entangled output $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. In fact, this circuit implements the unitary operation which maps the standard computation basis into the four entangled states, known as the Bell states,

$$\begin{aligned} |00\rangle &\mapsto |\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |01\rangle &\mapsto |\psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |10\rangle &\mapsto |\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |11\rangle &\mapsto |\psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

The Bell states form an orthonormal basis in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of two qubits. We can perform measurements in the Bell basis. The easiest way to do it in practice is to "rotate" the Bell basis to the standard basis and then perform the measurement in the standard basis.

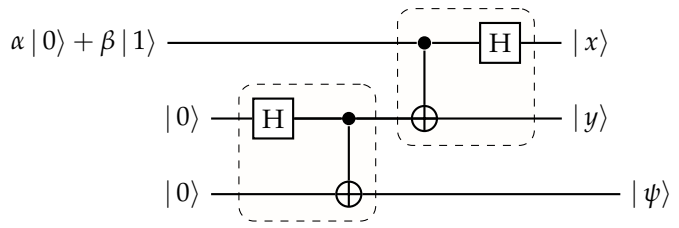


As we have just seen, the circuit on the left maps the standard basis $|x\rangle|y\rangle \equiv |xy\rangle$ into the four Bell states $|\psi_{xy}\rangle$. The circuit on the right, which is the reverse image of the circuit on the left, implements the inverse of this operation and maps the Bell states $|\psi_{xy}\rangle$ into the corresponding states from the standard basis $|xy\rangle$. This unitary mapping allows us to "implement" the projections on the Bell states by applying the circuit (on the right) followed by the regular qubit by qubit measurement in the standard basis.

For any state $|\psi\rangle$ of two qubits the amplitude $\langle\psi_{xy}|\psi\rangle$ can be written as $\langle xy|U^\dagger|\psi\rangle$, where $U^\dagger$ is the compensating unitary, such that $|\psi_{xy}\rangle = U|xy\rangle$.

1.9. **Quantum teleportation.** An unknown quantum state cannot be cloned but it can be teleported. Consider the following circuit

Divide et impera, that is, divide and conquer, a good approach to solving problems in mathematics (and in life). Start with smaller circuits, those surrounded by the dashed boxes.



The first input qubit (counting from the top) is in some arbitrary state. After the action of the circuit in the first dashed box the state of the three qubits reads (we have dropped the normalisation factors),

$$(\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|11\rangle).$$

By regrouping the terms, but keeping the qubits in the same order, this state can be written as the sum

$$\begin{array}{lcl}(|00\rangle+|11\rangle) & \otimes & (\alpha|0\rangle+\beta|1\rangle)+\\ (|01\rangle+|10\rangle) & \otimes & (\alpha|1\rangle+\beta|0\rangle)+\\ (|00\rangle-|11\rangle) & \otimes & (\alpha|0\rangle-\beta|1\rangle)+\\ (|01\rangle-|10\rangle) & \otimes & (\alpha|1\rangle-\beta|0\rangle).\end{array} \tag{18}$$

The second dashed box circuit maps the four Bell states of qubits 1 and 2 to the corresponding states from the computational basis

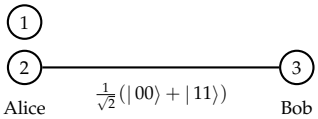
$$\begin{array}{lcl}|00\rangle & \otimes & (\alpha|0\rangle+\beta|1\rangle)+\\ |01\rangle & \otimes & (\alpha|1\rangle+\beta|0\rangle)+\\ |10\rangle & \otimes & (\alpha|0\rangle-\beta|1\rangle)+\\ |11\rangle & \otimes & (\alpha|1\rangle-\beta|0\rangle).\end{array} \tag{19}$$

Upon performing the standard measurement and learning the values of x and y we can choose one of the four transformations,

$$00\to\mathbb{1},\quad 01\to X,\quad 10\to Z,\quad 11\to ZX, \tag{20}$$

(e.g. if $x=0, y=1$ we choose X) and apply it to the third qubit. This restores the original state of the first qubit. If you understand how this circuit works then you are ready for quantum teleportation.

Suppose three qubits, which look very similar, are initially in a possession of an absent-minded Oxford student Alice. The first qubit is in a precious quantum state and this state is needed urgently for an experiment in Cambridge. Alice's colleague, Bob, pops in to collect the qubit. Once he is gone Alice realises that by mistake she gave him not the first but the third qubit, the one which is entangled with the second qubit. The situation seems to be hopeless – Alice does not know the quantum state of the first qubit, Bob is now miles away and her communication with him is limited to few bits. However, Alice and Bob are both very clever and attended the "Introduction to Quantum Information Science" course at Oxford. Can Alice rectify her mistake and save Cambridge science? Hmmm... pause for thought.... Sure she can. Alice can teleport the state of the first qubit. She performs the Bell measurement on the first two qubits, which gives her two binary digits, x and y. She then broadcasts x and y to Bob who chooses one of the four transformations, as in (20), and recovers the original state.



1.10. **Controlled-phase.** Needless to say, it is not all about the controlled-NOT gates. Another common two-qubit gate is the controlled phase shift gate cP_φ defined as

$$cP_\varphi = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{array}\right] \qquad \left.\begin{array}{l} |\,x\rangle \\ |\,y\rangle \end{array}\right\} e^{ixy\varphi}\,|\,x\rangle\,|\,y\rangle\,. \tag{21}$$

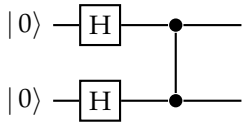
$$\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{array}\right]$$

c-Z gate

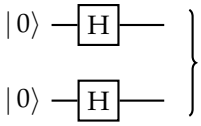
Again, the matrix is written in the computational basis $\{|\,00\rangle\,, |\,01\rangle\,, |\,10\rangle\,, |\,11\rangle\}$ and the diagram on the right shows the structure of the gate. If we do not specify the phase we usually assume that $\varphi = \pi$, in which case we call this operation the controlled-Z gate,

$$|\,0\rangle\,\langle 0\,| \otimes \mathbb{1} + |\,1\rangle\,\langle 1\,| \otimes Z.$$

Here Z refers to the Pauli phase-flip, $\sigma_z \equiv Z$, operation. In order to see its entangling power consider the following circuit

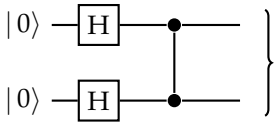


First, the two Hadamard gates prepare the equally weighted superposition of all states from the computational basis



$$\tfrac{1}{2}(|\,00\rangle + |\,01\rangle + |\,10\rangle + |\,11\rangle)$$

and then the controlled-Z operation flips the sign in front of $|\,11\rangle$,



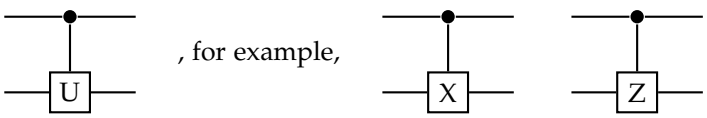
$$\tfrac{1}{2}(|\,00\rangle + |\,01\rangle + |\,10\rangle - |\,11\rangle)$$

which results in the entangled state (see exercises). As you can see, sometimes introducing a tiny relative phase shift can result in entangling two systems.

1.11. **Controlled-U.** More generally, these various 2-qubit controlled gates are all of the form controlled-U, for some single-qubit unitary transformation U,

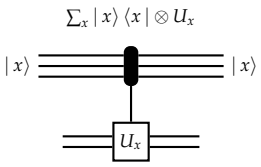
$$|\,0\rangle\,\langle 0\,| \otimes \mathbb{1} + |\,1\rangle\,\langle 1\,| \otimes U.$$

It is graphically represented as



which is an alternative way of representing controlled-X (controlled-NOT) and controlled-Z gates respectively. We can go further and consider a more general unitary operation, namely, an x-controlled-U on two qubits,

$$\sum_x |\,x\rangle\,\langle x\,| \otimes U_x \equiv |\,0\rangle\,\langle 0\,| \otimes U_0 + |\,1\rangle\,\langle 1\,| \otimes U_1,$$



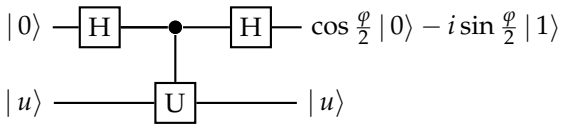
where U_0 and U_1 are unitary transformation applied to the second qubit if the first one is in state $|\,0\rangle$ and $|\,1\rangle$ respectively. In general, an x-controlled-U is a unitary

operation $\sum_x |x\rangle\langle x| \otimes U_x$ on two registers of size n and m; here $x \in \{0,1\}^n$ and U_x is the corresponding $2^m \times 2^m$ unitary matrix acting on the second register.

1.12. **Universality revisited.** We will come across few more gates in this course but at this stage you already know all the elementary unitary operations that are needed to construct any unitary operation on any number of qubits. The Hadamard gate, all phase gates, and the C-NOT, form a *universal set of gates* i.e. if the C-NOT gate as well as the Hadamard and all phase gates are available then any n-qubit unitary operation can be constructed exactly with $O(4^n n)$ such gates. We should mention that there are many universal sets of gates. In fact, almost any gate which can entangle two qubits can be used as a universal gate. We will be in particular interested in a *finite* universal set of gates, such as the one containing the Hadamard, $P_{\frac{\pi}{4}}$ (the T gate) and the C-NOT, can approximate any unitary operation on n qubits with arbitrary precision. The price to pay is the number of gates — better precision requires more gates. We shall elaborate on it later on.

Here and in the following we use asymptotic notation: given a positive function $f(n)$, the symbol $O(f(n))$ means bounded from above by $cf(n)$ for some constant $c > 0$ (for sufficiently large n). For example, $15n^2 + 4n + 7$ is $O(n^2)$.

1.13. **Phase kickback.** Before we conclude this lecture, let me describe a simple "trick", an unusual way of introducing phase shifts, which will be essential for our analysis of quantum algorithms. Consider the following circuit



You recognise, I hope, the interference circuit at the top. Well, almost, instead of a phase gate I have inserted a controlled-U operation but, as you will see in a moment, it will mimic the phase gate. The second qubit is prepared in state $|u\rangle$ which is an eigenstate of U, that is, $U|u\rangle = e^{i\varphi}|u\rangle$. The circuit effects the following sequence of transformations (normalisation factors neglected)

$$\begin{aligned}
|0\rangle|u\rangle &\overset{H}{\mapsto} (|0\rangle + |1\rangle)|u\rangle = |0\rangle|u\rangle + |1\rangle|u\rangle \\
&\overset{cU}{\mapsto} |0\rangle|u\rangle + |1\rangle U|u\rangle = |0\rangle|u\rangle + e^{i\varphi}|1\rangle|u\rangle = (|0\rangle + e^{i\varphi}|1\rangle)|u\rangle \\
&\overset{H}{\mapsto} \left(\cos\frac{\varphi}{2}|0\rangle - i\sin\frac{\varphi}{2}|1\rangle\right)|u\rangle
\end{aligned}$$

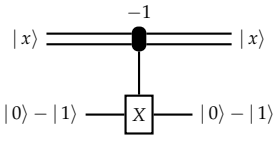
Note that the second qubit does not get entangled with the first one, it retains its original state $|u\rangle$. The interaction between the two qubits, induced by the controlled-U gate, introduces a phase shift on the first qubit. This may look like an unnecessarily complicated way of introducing phase shifts, but, as we shall see soon, this is how quantum computers do it. Let me give you a preview of things to come. Consider the following x-controlled-U operation,

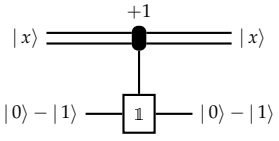
$$|00\rangle\langle 00| \otimes \mathbb{1} + |01\rangle\langle 01| \otimes \mathbb{1} + |10\rangle\langle 10| \otimes \mathbb{1} + |11\rangle\langle 11| \otimes X. \tag{22}$$

$$\left[\begin{array}{c|c|c|c} \mathbb{1} & 0 & 0 & 0 \\ \hline 0 & \mathbb{1} & 0 & 0 \\ \hline 0 & 0 & \mathbb{1} & 0 \\ \hline 0 & 0 & 0 & X \end{array}\right]$$

$|00\rangle\langle 00| \otimes \mathbb{1} + |01\rangle\langle 01| \otimes \mathbb{1} + |10\rangle\langle 10| \otimes \mathbb{1} + |11\rangle\langle 11| \otimes X$

The corresponding matrix is shown in the margin. The first register is of size 2 and the second register is of size 1 (just a single qubit). The expression above tells you that if the first register is prepared in state $|11\rangle$ then the qubit in the second register is flipped (the Pauli bit-flip X operation is applied to the second register) and nothing happens otherwise (the identity $\mathbb{1}$ is applied to the second register whenever the first register is in state $|00\rangle, |01\rangle$ or $|10\rangle$). This unitary operation is a quantum version of the Boolean function evaluation, it corresponds to the Boolean function $f : \{0,1\}^2 \mapsto \{0,1\}$ such that $f(11) = 1$ and $f(00) = f(01) = f(10) = 0$. Whenever $f(x) = 1$ we flip the bit value in the second register (with operation X) and whenever $f(x) = 0$ we do nothing. Now, prepare the qubit in the second register in state $|0\rangle - |1\rangle$. This is the eigenstate of X with eigenvalue -1. Thus, whenever X is applied to the second register the phase factor -1 appears in front of the





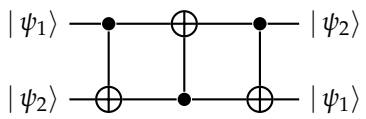
corresponding term in the first register. If we prepare the first register in the superposition $|00\rangle + |01\rangle + |10\rangle + |11\rangle$ then the result of applying the x-controlled-U, given by (22), is the entangled state $|00\rangle + |01\rangle + |10\rangle - |11\rangle$. The phase kickback mechanism introduced a relative phase in the equally weighted superposition of all binary strings of size two. This is how we control quantum interference in quantum computation. We will return to this topic in our next lecture, when we discuss quantum evaluation of Boolean functions and quantum algorithms.

Notes & Exercises

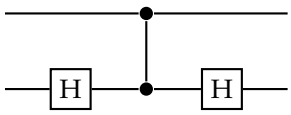
(1) Quantum entanglement appeared first in the early discussions on the meaning of quantum mechanics. Erwin Schrödinger, at the time a fellow of Magdalen College in Oxford, was the first to spot it and to realise its importance. In August 1935, the Cambridge Philosophical Society received a paper written by Schrödinger, and communicated by Max Born, titled "Discussion of probability relations between separated system". The paper was read on the 28th October 1935. In its opening paragraph Schrödinger wrote "I would not call it *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought". Today quantum entanglement is viewed as a physical resource which enables us to communicate with perfect security, build very precise atomic clocks and even teleport small quantum objects!

(2) **Entangled or not?** Prove that the two-qubit state $|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ is entangled iff $\det c_{ij} \neq 0$. Deduce that the state $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + (-1)^k|11\rangle)$ is entangled for $k = 1$ and unentangled for $k = 0$. Express the latter case explicitly as a product state.

(3) **Swap** Show that for any states $|\psi_1\rangle$ and $|\psi_2\rangle$ the circuit below effects the swap operation: $|\psi_1\rangle|\psi_2\rangle \mapsto |\psi_2\rangle|\psi_1\rangle$.



(4) Show that the circuit

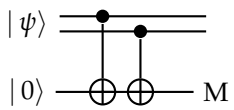


effects the controlled-NOT gate.

(5) The controlled-NOT gate can act as the measurement gate. If you prepare the target in state $|0\rangle$ the gate maps $|x\rangle|0\rangle \mapsto |x\rangle|x\rangle$, thus the target learns the bit value of the control qubit; it acts as a measuring device. If you wish, you can think about a subsequent measurement of the target qubit in the computational basis and and an observer learning about the bit value of the control qubit. Take a look at the circuit below. Here M stands for the measurement in the standard basis. Assume that the two top qubits are in the state

$$\frac{1}{\sqrt{3}}(|01\rangle - |10\rangle + i|11\rangle)$$

The measurement gives two outcomes, 0 and 1. What are the probabilities of the two outcomes and what is the post-measurement state in each case?



What is actually measured here?

(6) **Arbitrary controlled-U on two qubits** Any unitary operation U on a single qubit can be expressed as

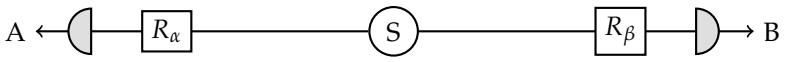
$$U = B^\dagger X B A^\dagger X A,$$

where X is the Pauli σ_x bit-flip operator and A and B are some unitaries. Suppose you can implement any single qubits gate and you have a couple of controlled-NOT gates. How would you implement any controlled-U operation on two qubits?

(7) **Entangled qubits.** Two entangled qubits in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are generated by source S; one qubit is sent to Alice and one to Bob, who perform measurements in the computational basis.

(a) What is the probability that Alice and Bob will register identical results? Can any correlations they observe be used for instantaneous communication?

(b) Prior to the measurements in the computational basis Alice and Bob apply unitary operations R_α and R_β to their respective qubits



The gate R_θ is defined by its action on the basis states

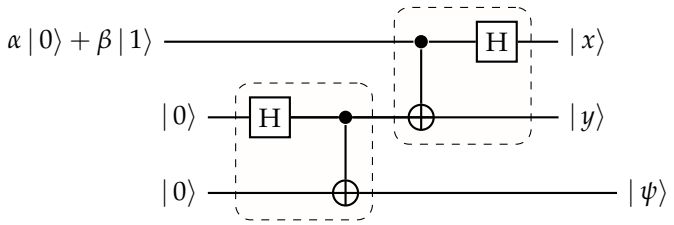
$$\begin{aligned} |0\rangle &\rightarrow \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \\ |1\rangle &\rightarrow -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle\,. \end{aligned}$$

Show that the state of the two qubits prior to the measurements is

$$\cos(\alpha-\beta)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) - \sin(\alpha-\beta)\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

What is the probability that Alice and Bob's outcomes are identical?

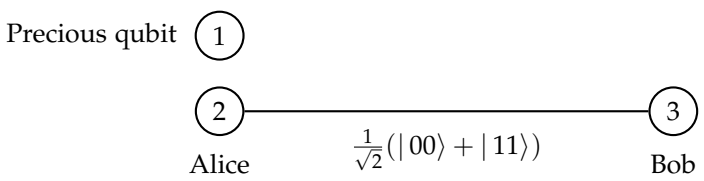
(8) **Quantum teleportation** Consider the following quantum circuit, containing the Hadamard and the controlled-NOT gates,



Divide et impera, that is, divide and conquer, a good approach to solving problems in mathematics (and in life). Start with smaller circuits, those surrounded by the dashed boxes.

The measurement on the first two qubits (counting from the top) gives two binary digits, x and y. The third qubit is not measured. How does the state of the third qubit, $|\psi\rangle$, depend on the values x and y?

Suppose the three qubits, which look very similar, are initially in a possession of an absent-minded Oxford student Alice. The first qubit is in a precious quantum state and this state is needed urgently for an experiment in Cambridge. Alice's colleague, Bob, pops in to collect the qubit. Once he is gone Alice realises that by mistake she gave him not the first but the third qubit, the one which is entangled with the second qubit (see the figure below).



The situation seems to be hopeless – Alice does not know the quantum state of the first qubit, Bob is now miles away and her communication with him is limited to at most one tweet. However, Alice and Bob are both very clever

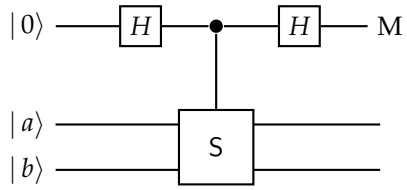
and attended the "Introduction to Quantum Information Science" course at Oxford. Can Alice rectify her mistake and save Cambridge science?

(9) **Playing with conditional unitaries** The swap gate S on two qubits is defined first on product vectors, $S : |a\rangle\,|b\rangle \mapsto |b\rangle\,|a\rangle$ and then extended to sums of products vectors by linearity.

(a) Show that the four Bell states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are eignevectors of S which form the orthonormal basis in the Hilbert space associated with two qubits. Which Bell states span the symmetric subspace (all eigenvectors of S with eigenvalue 1) and which the antisymmetric one (all eigenvectors of S with eigenvalue -1)? Can S have any other eigenvalues except ± 1?

(b) Show that $P_\pm = \frac{1}{2}(\mathbb{1} \pm S)$ are two orthogonal projectors which form the decomposition of the identity and project on the symmetric and the antisymmetric subspaces. Decompose the state vector $|a\rangle\,|b\rangle$ of two qubits into symmetric and antisymmetric components.

(c) Consider the following quantum network composed of the two Hadamard gates, one controlled-S operation (also known as the controlled-swap or the Fredkin gate) and the measurement M in the computational basis,



The state vectors $|a\rangle$ and $|b\rangle$ are normalised but not orthogonal to each other. Step through the execution of this network, writing down quantum states of the three qubits after each computational step. What are the probabilities of observing 0 or 1 when the measurement M is performed?

(d) Explain why this quantum network implements projections on the symmetric and the antisymmetric subspaces of the two qubits.

(e) Two qubits are transmitted through a quantum channel which applies the same, randomly chosen, unitary operation U to each of them. Show that $U \otimes U$ leaves the symmetric and antisymmetric subspaces invariant.

(f) Polarised photons are transmitted through an optical fibre. Due to the variation of the refractive index along the fibre the polarisation of each photon is rotated by the same unknown angle. This makes communication based on polarisation encoding unreliable. However, if you can prepare any polarisation state of two photons you can still use the channel and communicate without any errors. How can this be achieved?

Complement 1

Why qubits? Why subsystems? Why entanglement?

One question that I hear over and over again is this: if entanglement is so fragile and so difficult to control then why bother, why not perform the whole computation in one physical system with sufficiently many quantum states which we can label in the same way we label states of qubits and give them the same computational meaning? It will not work for this is a very inefficient way of representing data (unary encoding). For serious computations we do need subsystems. Here is why.

Suppose you have n physical objects and each object has k distinguishable states. If you can access each object *separately* and put it into any of the k states then with only n operations you can prepare any of the k^n different configurations of the combined systems. Without any loss of generality let us put $k = 2$ and refer to each object of this type as a physical bit. We label the two states of the physical bit as 0 and 1. Any collection of n physical bits can be prepared in 2^n different configurations which can be used to store up to 2^n messages, or binary strings or 2^n different numbers. In order to represent numbers from 0 to $N-1$ we just have to choose n such that $N \leq 2^n$. Suppose the two states in the physical bit are separated by the energy difference ΔE then a preparation of any particular configuration will cost not more than $E = n\Delta E$ or $\log N \ \Delta E$ units of energy (the log is taken to the base 2).

In contrast if we choose to encode N configurations into one chunk of matter, say into the first N energy states of a single harmonic oscillator with the energy separation ΔE then, in the worst case, one has to use $E = N \ \Delta E$ units of energy (e.g. to go from the ground state labelled as 0 to the most excited state labelled as N). For large N this gives an exponieential gap in the energy expenditure between the binary encoding using physical bits and the so-called unary encoding using energy levels of harmonic oscillators.

One can, of course, try to switch from harmonic oscillators to quantum systems which have a finite spread in the energy spectrum. For example, by operating on the energy states of the hydrogen atom one can encode any number from 0 to $N-1$ and one is guaranteed not to spend more than $E_{max} = 13.6$ eV (otherwise the hydrogen atom is ionised). The snag is that in this case some of the electronic states will be separated by the energy difference of the order of E_{max}/N and to drive the system selectively from one state to another one has to tune into the frequency $E_{max}/\hbar N$ which requires a sufficiently long wavepacket (so that the frequency is well defined) and consequently the interaction time of the order $N(\hbar/E_{max})$. Thus we have to trade energy for time. It turns out that whichever way we try to represent the number N using the unary encoding, i.e. using N different states of a single chunk of matter, we end up depleting our physical resources, such as energy, time, space, at a much greater rate than in the case when we use subsystems. This plausibility argument indicates that for efficient processing of information the system must be divided into subsystems, for example, into physical bits.