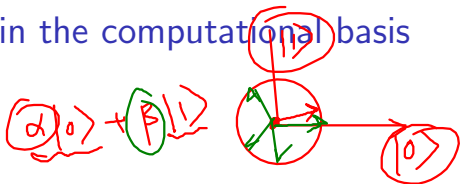


Re-cap: measurement in the computational basis



If we have a state $|\psi\rangle$ which is either $|0\rangle$ or $|1\rangle$, then we can perfectly distinguish which of these it is by measurement in the computational basis:

$$|1\rangle = 0|0\rangle + 1|1\rangle \leftarrow$$

so we measure 1 with probability $|1|^2 = 1$ (and likewise for 0).

Essentially, this is just classical (binary) information.

$$\underline{\underline{1|0\rangle + 0|1\rangle}}$$

Distinguishing any pair of orthogonal states



If we now have a state $|\psi\rangle$ which is either $|\psi_0\rangle = \alpha |0\rangle + \beta |1\rangle$ or $|\psi_1\rangle = \beta^* |0\rangle - \alpha^* |1\rangle$ (where $*$ denotes the complex conjugate), i.e., $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal, then we can still perfectly distinguish which of these it is by first performing the transformation:

$$|\phi\rangle = \begin{bmatrix} \alpha^* & \beta^* \\ \beta & -\alpha \end{bmatrix} |\psi\rangle$$

which sends $|\psi_0\rangle \rightarrow |0\rangle$ and $|\psi_1\rangle \rightarrow |1\rangle$, and then performing the measurement in the computational basis.

In fact, physicists and mathematicians frequently speak not of doing a transformation such that the states are aligned with the computational basis, but rather performing the measurement in the basis $(|\psi_0\rangle, |\psi_1\rangle)$, which amounts to the same thing.

It is not possible to perfectly distinguish non-orthogonal quantum states

check this

If we now have a state $|\psi\rangle$ which is either $|\psi_a\rangle$ or $|\psi_b\rangle$ which are **not orthogonal**, then there is no measurement that can perfectly tell us which of these states $|\psi\rangle$ is.

... but we can perform a measurement that tells us something about the likelihood of whether $|\psi\rangle = |\psi_a\rangle$ or $|\psi\rangle = |\psi_b\rangle$.

Intuitively:

- If we just guess, we will be correct with probability equal to one half, so we expect to be able to do better than this.
- The “closer together” $|\psi_a\rangle$ and $|\psi_b\rangle$ are, the harder they will be to distinguish (i.e., the lower the probability of correctly inferring $|\psi\rangle$)

The Helstrom-Holevo Bound

The intuition in the previous slide turns out to be correct, and is captured by the Helstrom-Holevo bound:

If $|\psi\rangle$ is either $|\psi_a\rangle$ or $|\psi_b\rangle$, where $|\langle\psi_a|\psi_b\rangle| = \cos\theta$, then the probability of correctly inferring the state $|\psi\rangle$ is less than or equal to $\frac{1}{2}(1 + \sin\theta)$.

Furthermore, the bound is tight, it can always be achieved by choosing the measurement basis as the eigenvectors of:

$$|\psi_a\rangle\langle\psi_a| - |\psi_b\rangle\langle\psi_b|$$

Example: distinguishing $|0\rangle$ and $|+\rangle$

First, we note that $|0\rangle$ and $|+\rangle$ are not orthogonal:

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \neq 0$$

therefore we cannot perfectly infer the state of $|\psi\rangle$ if we know it is either $|0\rangle$ or $|+\rangle$. So instead, we must decide a basis to measure in:

$$|0\rangle\langle 0| - |+\rangle\langle +| = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

which has eigenvectors $[0.38 \ 0.92]^T$ and $[-0.92 \ 0.38]^T$. Finally, we can calculate the probability of correctly inferring the state:

$$\frac{1}{2}(1 + \sin(\arccos(1/\sqrt{2}))) = 0.85$$

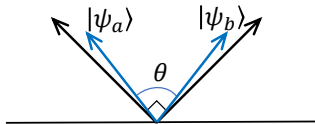
Distinguishing $|0\rangle$ and $|+\rangle$ by measuring in the computational basis

Again we have that $|\psi\rangle$ is either $|0\rangle$ or $|+\rangle$, each with 50% probability. We can tabulate the quantum states and measurement outcomes when measuring in the computational basis:

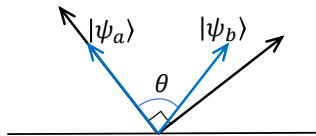
	0	1
$ 0\rangle$	$\frac{1}{2}$	0
$ +\rangle$	$\frac{1}{4}$	$\frac{1}{4}$

- $\frac{1}{4}$ of the time we will measure 1, which means $|\psi\rangle = |+\rangle$.
- $\frac{3}{4}$ of the time we will measure 0, which we should *guess* means $|\psi\rangle = |0\rangle$, but of these $\frac{1}{3}$ will be wrong, and actually $|\psi\rangle = |+\rangle$.
- So we have success probability $1 - \frac{3}{4} \times \frac{1}{3} = \frac{3}{4}$, which is less than the theoretically achievable 0.85, but if we measure 1 then we know $|\psi\rangle = |+\rangle$ with certainty.

Depicting different state discrimination strategies



The optimal strategy is to choose the measurement basis “equally”.



But if one of the measurement basis vectors aligns with one of the states being distinguished, sometimes we get a measurement that we are 100% sure about.

Unambiguous state discrimination

Although detailed analysis is outside the scope of this course, it is worth being aware that there exist schemes (requiring additional ancilla qubits) which *unambiguously* discriminate non-orthogonal quantum states, but only work with some probability less than one. That is if a state $|\psi\rangle$ is either $|\psi_a\rangle$ or $|\psi_b\rangle$, the measurement outputs one of three things:

- $|\psi_a\rangle$ – in which case $|\psi\rangle$ was certainly $|\psi_a\rangle$.
- $|\psi_b\rangle$ – in which case $|\psi\rangle$ was certainly $|\psi_b\rangle$.
- ‘Don’t know’ – in which case we have no information about $|\psi\rangle$ (which has been destroyed in the process).

The no-signalling principle: why it matters

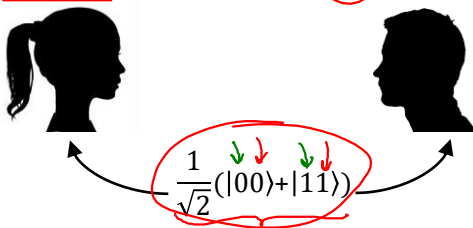
$$|a\rangle \otimes |b\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Handwritten notes: "can't write" with an arrow pointing to the tensor product symbol; "one of the possible entangled states" with an arrow pointing to the right-hand side of the equation; "3 more" with an arrow pointing to the right-hand side of the equation.

In quantum mechanics we accept the reality of entanglement, Einstein's "spooky action at a distance", but can this be used for super-luminal information transfer, that is genuine "action at a distance", or is it merely a non-local stronger than classical correlation?

The answer is, in fact, the latter, and proven by the no-signalling principle.

The no-signalling principle: set-up



- Alice and Bob are at different ends of the universe, but each have one half of a Bell pair: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice can measure her qubit whenever she wants, and this will collapse Bob's to the same state.
- We are interested in whether Bob can infer whether or not Alice has measured her qubit, if he can, then Alice can transfer information to Bob. For example, Alice can measure her qubit when some event occurs, thus signalling this information to Bob.
- But all that Bob can do to infer whether Alice has measured her qubit is to measure his own qubit – therefore, the question reduces to whether the measurement probabilities that Bob sees are altered by virtue of Alice having performed her measurement.

The no-signalling principle: proof

If Alice hasn't measured her qubit, then the state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and so Bob has a $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ probability of measuring each of 0 and 1.

If Alice has measured her qubit, then Bob's qubit has collapsed – it is either in state 0, or state 1 (each with probability $1/2$). However, in the absence of signalling, Bob has no knowledge of which of these measurement outcomes Alice observed, and so all he knows is that he will measure each of $|0\rangle$ and $|1\rangle$ with probability $1/2$. So the no-signalling principle is proved.

- Crucially, in the absence of signalling, Bob's measurement statistics when measuring the uncollapsed quantum state are identical to his lack of knowledge (expressed probabilistically) when measuring the state already collapsed by Alice.
- The no-signalling principle also holds for any type of entanglement, and also any scheme Alice and Bob may come up with involving transformations of their qubits, and measurements in arbitrary bases.

The no-cloning principle: why it matters

- A plethora of physics reasons.
- That we cannot clone makes quantum error-correction harder.
- The possibility of cloning would enable the violation of the no-signalling principle (see exercise sheet).
- Cloning would enable an infinite amount of classical information to be compressed into a single qubit and then recovered afterwards:
 1. Map a classical bit-string to a unique qubit state.
 2. Communicate the single qubit.
 3. Receive the qubit, make an arbitrary number of copies by cloning, and perform quantum state tomography to recover the original classical information.

The no-cloning principle: set-up

$$U = U_k \cdots U_2 U_1$$

(Product of unitary is unitary)

We have a quantum state $|\psi\rangle$ and a register initially set to $|0\rangle$, and we wish to find a cloning unitary, U such that:

$$U |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle$$

All operators are unitary.

We will now prove that no such U exists.

≧

The no-cloning principle: proof

Consider that U must clone all quantum states, so as well as

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

from the previous slide, we have that

$$U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$$

Taking the inner products of the left- and right-hand sides of the above equations, we have that:

$$\begin{aligned}\langle 0|\langle\psi|U^\dagger U|\phi\rangle|0\rangle &= (\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle) \\ \Rightarrow \langle\psi|\phi\rangle\langle 0|0\rangle &= (\langle\psi|\phi\rangle)^2 \\ \Rightarrow \langle\psi|\phi\rangle &= (\langle\psi|\phi\rangle)^2\end{aligned}$$

which is only true if $\psi = \phi$ or ψ and ϕ are orthogonal (so their inner-product is 0). So we have proven that there exists no unitary U that can clone arbitrary quantum states.

The no-deleting principle

Time-reversal of the no-cloning principle yields the no-deleting principle: there does not exist a unitary \tilde{U} that can delete one of two copies of a quantum state, that is:

$$\tilde{U}(|\psi\rangle \underline{|\psi\rangle}) = |\psi\rangle \underline{|0\rangle}$$

Can you delete this?

It is less obvious why this is useful, but the no-deleting principle does arise in quantum information, and so it is worth being aware of.

More generally, quantum computing is reversible (except for measurement), and therefore the (im)possibility of some computation implies the (im)possibility of its reverse.

Summary

In this lecture we have looked at:

- Distinguishing orthogonal and non-orthogonal states.
- Perfectly distinguishing non-orthogonal states, but with probability less than one.
- The no-signalling principle.
- The no-cloning principle.
- The no-deleting principle.

Quantum Computing (CST Part II)

Lecture 5: The Quantum Circuit Model

Information is physical.

Rolf Landauer

Resources for this lecture

Nielsen and Chuang chapter 4 contains a thorough introduction to the quantum circuit model (although this is rather more than is needed for this course).

Quantum circuits: the big picture

This lecture represents a shift in perspective from seeing quantum mechanical events as merely natural phenomena, to instead seeing them as **executable operations in a programmable computer**.

There is, however, a subtlety here: the postulates of quantum mechanics describe what will happen to a *closed* quantum system, however treating quantum phenomena as controllable and executable necessarily implies some opening of the system: we later plug this gap by considering noisy quantum systems.

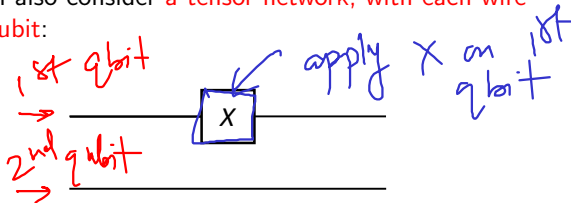
Tensor networks

We have already seen that qubit states can be entangled (not separable), however **we can apply separable operations even to entangled states**.

Consider:

- A two qubit state: $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$
- Performing a Pauli- X on the first qubit only.

From the previous notes on linear algebra and the postulates of quantum mechanics, we know that this yields a state, $|\psi'\rangle$, equal to $(X \otimes I)|\psi\rangle$. However, we can also consider **a tensor network, with each wire representing a qubit**:



As the Pauli- X is a “not” operation, we immediately get

$$|\psi'\rangle = \alpha|10\rangle + \beta|11\rangle + \gamma|00\rangle + \delta|01\rangle$$

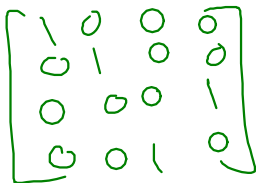
Exercise: prove consistency with the matrix calculation.

Quantum circuits: from matrices to gates

In the tensor network, we have that:

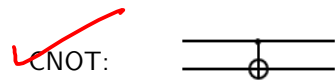
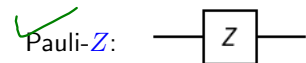
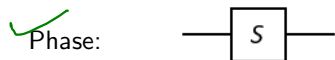
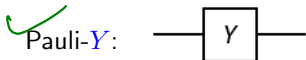
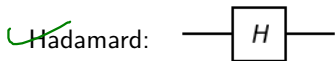
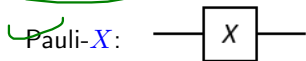
- Wires are qubits (possibly entangled).
- Gates are unitary matrices.

CNOT =



We have already met the Pauli and Hadamard single-qubit unitary matrices as well as the CNOT two-qubit unitary, and the *phase gate*

$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ is also a useful primitive.



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

$|11\rangle \rightarrow |10\rangle$

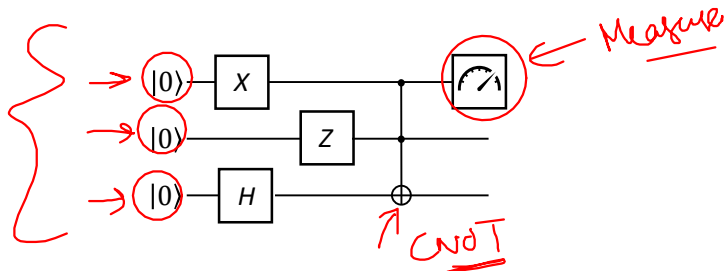
$$|10\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$|10\rangle \rightarrow |11\rangle$

$$|00\rangle \rightarrow |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Quantum circuits



A quantum circuit is a tensor network of n qubits, with three stages:

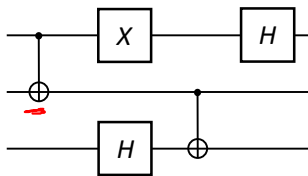
- Initialisation of all qubits in the $|0\rangle$ state (denoted $|0\rangle^{\otimes n}$).
- Some quantum gates, which represent unitary transformations.
- A final layer of measurements in the computational basis, on some or all of the qubits.

The matrix of a quantum circuit

As the quantum circuit (with the initialisation and measurement stages omitted) just represents a unitary evolution, **we can express the whole thing as a matrix**. We must follow the following two rules:

- Composition across wires is achieved by the tensor product.
- Composition along (sets of) wires is achieved by the normal matrix product, but **right to left**.

For example:



Is equal to:

$$(\underline{H} \otimes I_4) \times (I_2 \otimes \text{CNOT}) \times (\underline{X} \otimes I_2 \otimes H) \times (\text{CNOT} \otimes I_2)$$

where I_2 is the 2×2 identity, and $I_4 = I_2 \otimes I_2$ is the 4×4 identity.

Quantum computational power (1/2)

The quantum circuit model completely captures the postulates of quantum mechanics:

- The wires represent the state-space of a composition of 2-level quantum systems (qubits), which can be entangled – postulates 1 and 4.
- The gates are just a convenient way of writing down the unitary evolution – postulate 2.
- Measurement occurs (and it can be shown that this can always be deferred to the end of the circuit) – postulate 3.

Furthermore, there is no loss in generality in assuming that we can prepare the states as $|0\rangle^{\otimes n}$.

It follows that any computation leveraging the quantum nature of some physical system can, in principle, be expressed using the quantum circuit model.

Quantum computational power (2/2)

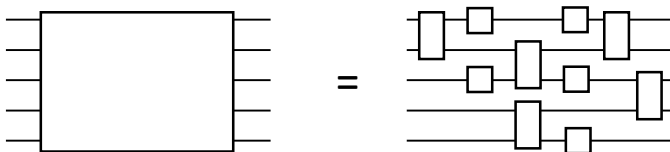
Additionally:

- Quantum computing generalises classical computing, and so any classical computation can be performed on a quantum computer.
- It has been shown that quantum computing does not violate the Church-Turing thesis – there is no problem that is solvable on a quantum computer that is not on a classical computer... what quantum computers give us is a more efficient way to do some computations.

Locality constrains the physical realisation of gates

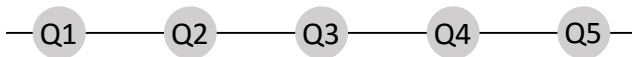
Unitary matrices of all dimensions exist, thus in principle quantum gates of all dimensions exist... however **quantum computers live in physical space**, and so it follows that it is physically unreasonable to assume that we can have an arbitrary number of qubits in a single operation (that is, that we can have gates of any size). In fact, **usually we assume that we are only allowed to use single- and two- qubit gates**.

It has been proven that **two-qubit unitaries are universal**, in the sense that any arbitrary n -qubit unitary can be decomposed as a product of two-qubit unitaries, e.g.:

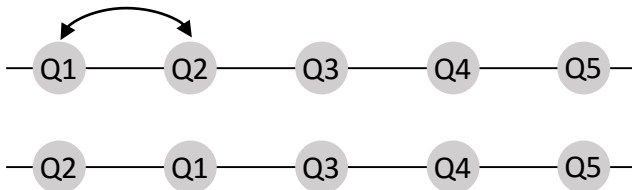


Qubits located in an array

Not only do we assume that we can only perform operations (gates) on one or two qubits, but in physical quantum computers **two qubits that undergo a two-qubit gate must be physically adjacent**. For example, the qubits may be laid out in a linear array:

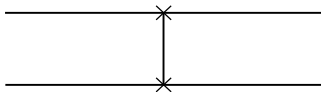


If a gate is to be executed on qubits 1 and 3, it is necessary to *swap* qubits 1 and 2 such that qubits 1 and 3 are adjacent:



The SWAP gate

Fortunately, this swapping can be achieved using the **SWAP** gate, which swaps the states of two qubits:



Let $|\psi_1\psi_2\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, which corresponds to the vector $[\alpha, \beta, \gamma, \delta]^T$, we have that:

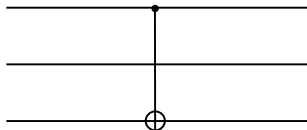
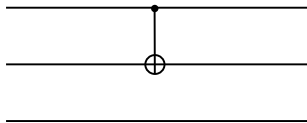
$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{bmatrix} = \text{SWAP} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$

i.e., is equal to $|\psi_2\psi_1\rangle = \alpha|00\rangle + \gamma|01\rangle + \beta|10\rangle + \delta|11\rangle$.

SWAP can be constructed from three **CNOT** gates (**exercise sheet**).

Matrix representation of CNOT on non-adjacent qubits

Even though the existence of the SWAP gate is crucial for practical considerations, we continue to write down two-qubit operations on non-adjacent qubits. This raises the question of how to express them in matrix form. For example, consider the following



We know that we can express the left-hand circuit as $\text{CNOT} \otimes I_2$, but how would we express the right-hand circuit?

...we can just SWAP, do the CNOT on adjacent qubits and then SWAP back:

$$(I_2 \otimes \text{SWAP}) \times (\text{CNOT} \otimes I_2) \times (I_2 \otimes \text{SWAP})$$

How many one- and two-qubit gates do we need?

Previously, it was asserted that an arbitrary unitary operation could be decomposed into a product of one- and two- qubit unitaries. However, as a unitary is a matrix of complex numbers this leaves two possibilities:

- Either we require a continuum of two qubit unitaries (i.e., an infinite number of gates).
- Or we can construct arbitrary one- and two-qubit unitaries from a finite set of unitaries (a finite universal gate-set).

In fact, the latter is true, indeed we can *efficiently* approximate any circuit consisting of CNOT gates and single qubit unitaries to a desired accuracy ϵ :

The Solovay-Kitaev theorem implies that any circuit containing m CNOTs and arbitrary single qubit unitaries can be approximated to an accuracy ϵ by a circuit using a universal finite gate-set with $O(\log^c(m/\epsilon))$ gates, where $c \approx 2$.

A universal gate-set

Perhaps surprisingly, **only three gates are needed to form a universal gate-set**, two we have met: **CNOT** and **H**, and the third is:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

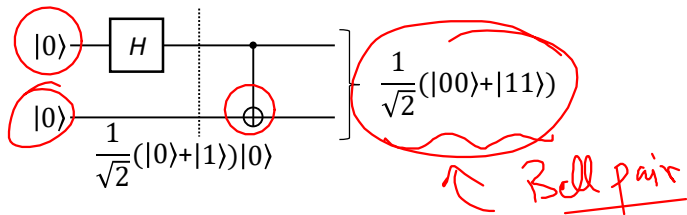
Gates

The introduction of this **T** gate is, however, crucial, and the famous Gottesman-Knill theorem holds that any circuit consisting of just the gates we have met thus far ~~XXX~~ **CNOT** can be efficiently simulated on a classical computer.

We can see that the single-qubit gates we have met so far can be expressed in terms of **H** and **T** as follows:

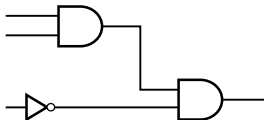
- $S = T^2$
- $Z = S^2$
- $X = H$
- $Y = XZ$

Quantum circuit example 1: entangling two qubits



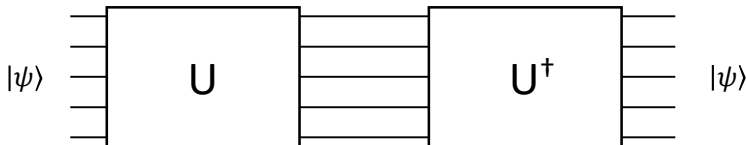
Comparison with classical logic circuits

By expressing quantum evolutions in circuit form, we can express physical phenomena in a manner that can be recognised as similar to classical logic circuits, with which we are all very familiar.



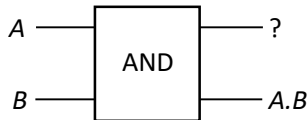
There are, however, two important distinctions:

- Quantum gates have exactly the same number of outputs as they have inputs.
- Moreover, **as the gates represent unitary matrices, they are invertible.**



An invertible AND gate?

Consider the classical logic gate the “AND” gate. Clearly it is not invertible, as one input leads to two outputs. However, if we give the “AND” gate a second output, can we make it invertible? That is:



In fact we cannot – we have three occasions when the second output is zero (~~$A=0, B=0$~~) ; (~~$A=0, B=1$~~) ; (~~$A=1, B=0$~~) , and only one bit with which to distinguish them, so we can never reconstruct the inputs A and B from two outputs of which one is B .

The Toffoli gate

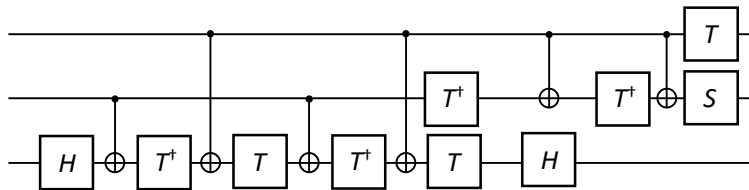
The Toffoli gate *does* provide a quantum generalisation of the classical **AND** gate, with three inputs and outputs.



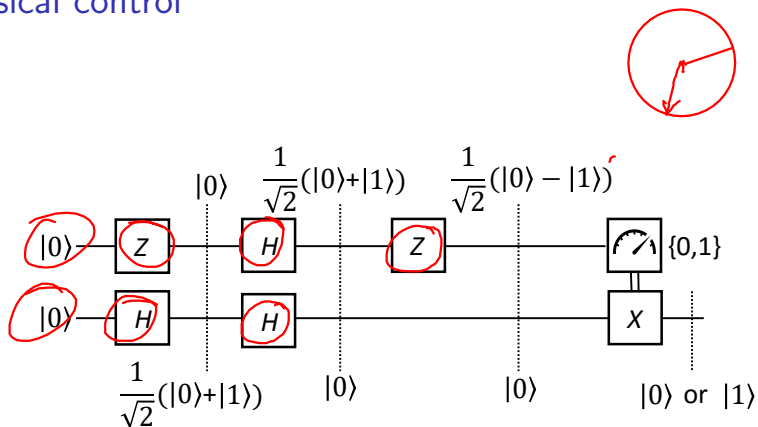
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

When the first two inputs are classical bits ($|0\rangle$ or $|1\rangle$), and the third is $|0\rangle$ the third output is the AND of the first two inputs.

Quantum circuit example 2: decomposing the Toffoli gate into two-qubit unitaries



Quantum circuit example 3: self-inverse nature of H and classical control



Summary

For the remainder of the course, it is crucial to be comfortable with manipulating quantum circuits. The main points to remember from this lecture are:

- Quantum circuits are tensor networks where the wires are qubits and the gates are one- or two- qubit unitary operations.
- Quantum circuits can be used to completely represent quantum computation, and the class of problems solvable on a quantum computer is exactly equal to that on a classical computer.
- CNOT , H is a universal gate-set, but for convenience we include X and S as primitives.
- Quantum gates are reversible, and the Toffoli gate generalises the classical AND gate.

Quantum Computing (CST Part II)

Lecture 6: Some Applications of Quantum Information

Beam me up, Scotty
Captain Kirk

Resources for this lecture

Nielsen and Chuang gives a concise and clear explanation of teleportation (**p26-27**) and superdense coding (**p97**). Nielsen and Chuang also covers QKD quite comprehensively (**p587-591**), this is rather more than is required for this course, but is an interesting read for those who are interested in understanding it with more information theoretic rigour.

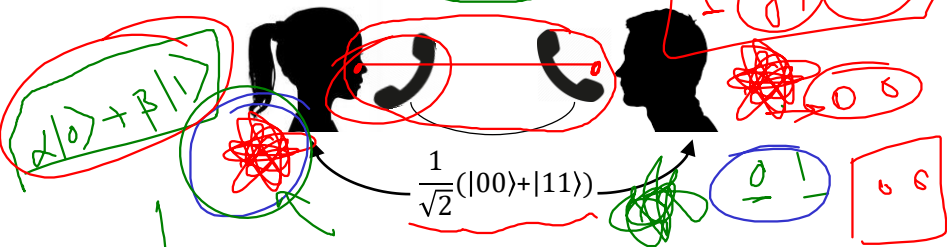
Why look at “some applications of quantum information”?

Before getting into the details of quantum computing proper, we will look at some other aspects of quantum information processing, which have remarkable results that cannot be achieved classically, even in principle. Specifically, we will look at:

- Using entanglement as a resource, in teleportation and superdense coding.
- Using quantum phenomena to achieve information theoretically (rather than computationally) secure communications.

Alice and Bob revisited

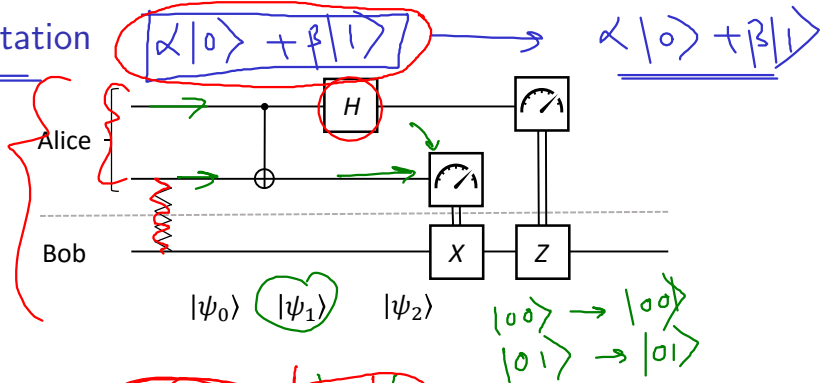
Alice and Bob once again share an entangled pair ($(1/\sqrt{2})(|00\rangle + |11\rangle)$). Previously we saw that they couldn't use this alone for signalling, so we will also give them a communication channel.



We will now see how they can:

1. Use the shared entanglement and **two bits** of classical information to **transfer one qubit** (teleportation).
2. Use the shared entanglement and **one qubit** of quantum information to **transfer two classical bits** (superdense coding).

Teleportation



$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}} (|0\rangle(|00\rangle + |11\rangle) + |1\rangle(|00\rangle + |11\rangle)) \end{aligned}$$

$$|1\rangle = \frac{1}{2} (|0\rangle(|00\rangle + |11\rangle) + |1\rangle(|10\rangle + |01\rangle))$$

$$|2\rangle = \frac{1}{2} (|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + (|0\rangle - |1\rangle)(|10\rangle + |01\rangle)$$

after CNOT

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$


$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Teleportation (cont.)



A Bloch sphere diagram is shown with a blue circle and a blue arrow pointing to the state $|0\rangle$. To the right, a red circle contains the expression $\alpha|0\rangle + \beta|1\rangle$ written in green.

The equation for the state $|2\rangle$ is shown with red annotations:

$$|2\rangle = \frac{1}{2} (|00\rangle (|0\rangle + |1\rangle) - |01\rangle (|1\rangle + |0\rangle) + |10\rangle (|0\rangle - |1\rangle) + |11\rangle (|1\rangle - |0\rangle))$$

Alice now measures her two qubits, and sends the results to Bob, who uses this classical information to apply a correction to his qubit (qubit 3):

Measurement	Qubit 3 before	Correction	Qubit 3 after
00	$ 0\rangle + 1\rangle$	I	$ 0\rangle + 1\rangle$ ←
01	$ 1\rangle + 0\rangle$	X	$ 0\rangle + 1\rangle$ ←
10	$ 0\rangle - 1\rangle$	Z	$ 0\rangle + 1\rangle$
11	$ 1\rangle - 0\rangle$	ZX	$ 0\rangle + 1\rangle$ ←

So we can see that, regardless of the measurement outcomes, Alice's qubit state has now been realised on qubit 3 (i.e., in Bob's possession). Note that teleportation does not violate the no-cloning principle, as Alice's original qubit has been destroyed in the process.

Teleportation (cont.)

Einstein:

No information can travel faster than speed of light?

$$| \psi \rangle = \frac{1}{2} (|00\rangle (|0\rangle + |1\rangle) + |01\rangle (|1\rangle + |0\rangle) + |10\rangle (|0\rangle - |1\rangle) + |11\rangle (|1\rangle - |0\rangle))$$

Alice now measures her two qubits, and sends the results to Bob, who uses this classical information to apply a correction to his qubit (qubit 3):

Measurement	Qubit 3 before	Correction	Qubit 3 after
00	$ 0\rangle + 1\rangle$	I	$ 0\rangle + 1\rangle$
01	$ 1\rangle + 0\rangle$	X	$ 0\rangle + 1\rangle$
10	$ 0\rangle - 1\rangle$	Z	$ 0\rangle + 1\rangle$
11	$ 1\rangle - 0\rangle$	ZX	$ 0\rangle + 1\rangle$

So we can see that, regardless of the measurement outcomes, Alice's qubit state has now been realised on qubit 3 (i.e., in Bob's possession). Note that teleportation does not violate the no-cloning principle, as Alice's original qubit has been destroyed in the process.

History of quantum teleportation

- Discovered in 1993
- Experimentally realised in 1997
- The latest reported record distance for quantum teleportation is 1,400 km (870 miles) using the Micius satellite for space-based quantum teleportation



Micius Satellite



Superdense coding: Alice's transmission

Superdense coding was discovered in 1992, and experimentally realised in 1996, it goes as follows:

Alice and Bob share an entangled pair, Alice wants to send two bits, i.e., one of 00, 01, 10 or 11. To do so, she applies a single-qubit unitary to her qubit:

Initial state	Alice's bitstring	Operation	Final state
$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$	00	I	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$	01	X	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$	10	Z	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$	11	XZ	$\frac{1}{\sqrt{2}}(10\rangle - 01\rangle)$

Alice then sends her qubit to Bob.