Models of Computation: Quantum Computing

Vladimir Zamdzhiev

Inria, Nancy, France

Crash Course on Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world.

Crash Course on Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world. However, wrong for macro/micro world.

Crash Course on Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world. However, wrong for macro/micro world.
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.)

Crash Course on Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world. However, wrong for macro/micro world.
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.). But wrong for micro world.

Crash Course on Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world. However, wrong for macro/micro world.
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.). But wrong for micro world.
- Quantum Mechanics – describes the micro world (photons, electrons, etc.)

Crash Course on Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world. However, wrong for macro/micro world.
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.). But wrong for micro world.
- Quantum Mechanics – describes the micro world (photons, electrons, etc.). Never proven false.

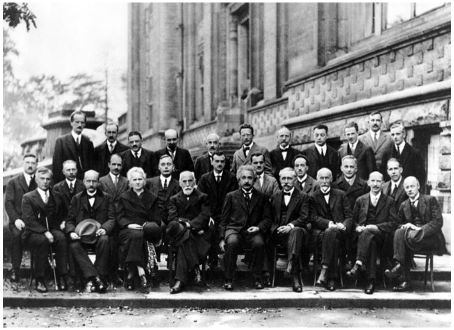


Figure: The 1927 Solvay Conference in Brussels

Computer Design

- Modern computers operate by manipulating electromagnetic processes in electronic circuits.
- However, electronic circuits become smaller and smaller and start exhibiting quantum phenomena.
- What happens when our computational hardware becomes so small that it is fully quantum?

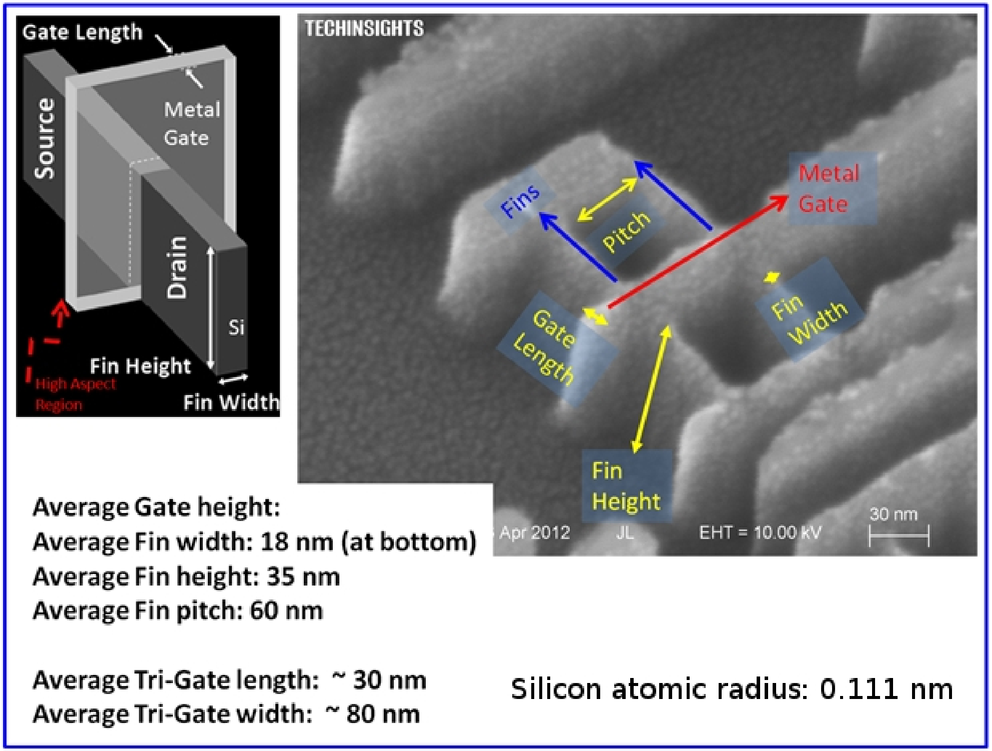


Figure: Intel 22-nm Tri-Gate device

Classical Computing

- Classical computers (laptops, phones, etc.) manipulate classical information (bits) in order to perform computation.
- Classical information is described using classical information theory which is a mathematical model that assumes the world is explained using classical physics.
- This is a perfectly reasonable assumption to make for our current hardware.

Quantum Computing

- Consider a computer so small that it can manipulate simple quantum systems called qubits (quantum bits).
- The underlying mathematical model is now different as it is based on quantum physics.
- Processing of quantum information (qubits) is as a result fundamentally different.
- The speed of certain computations is also faster in some cases.

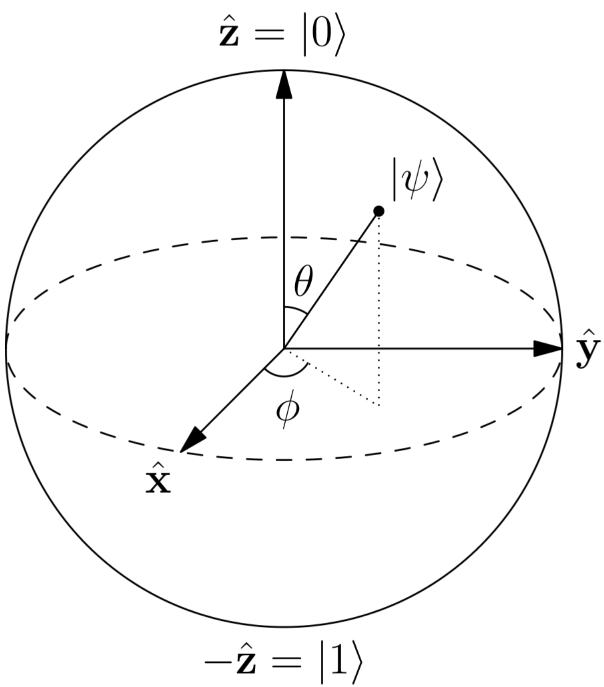


Figure: Bloch-sphere representation of a qubit state.

Quantum Entanglement – important resource

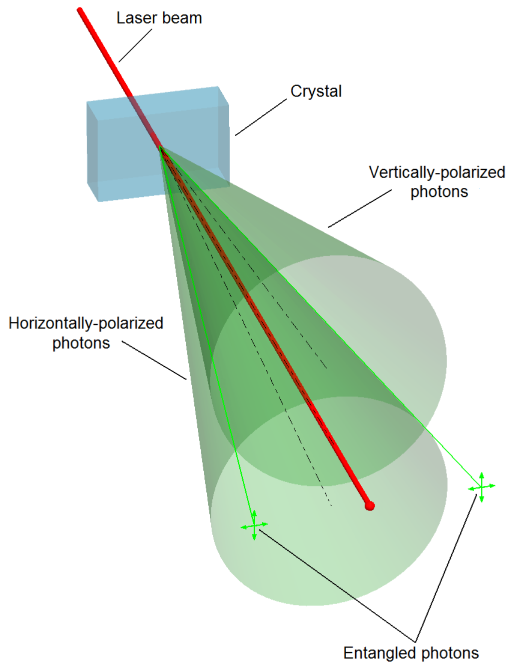
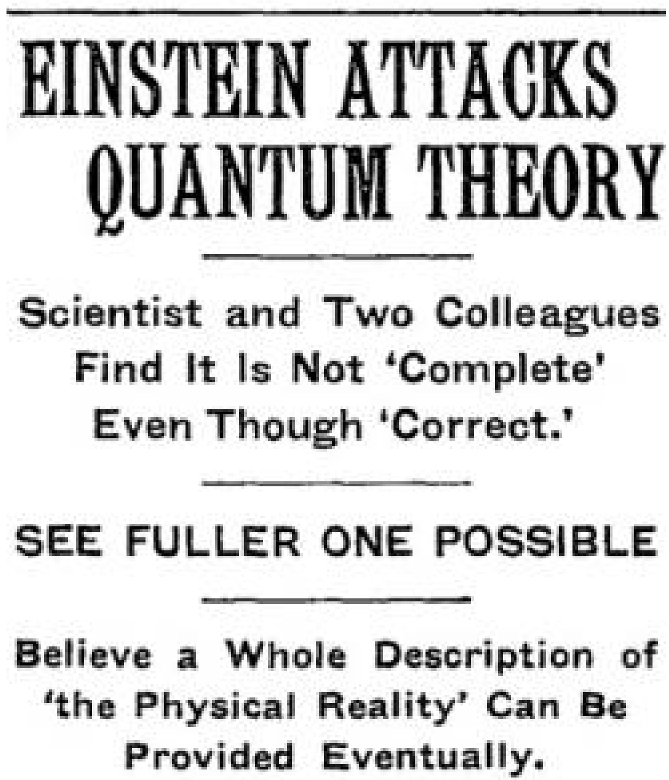


Figure: Illustration of quantum optics experiment which produces entanglement

Quantum Entanglement – important resource



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Figure: May 4, 1935 *New York Times* article headline regarding the imminent EPR paper.

Quantum Entanglement – important resource

- Quantum entanglement is a special kind of correlation between systems which allows them to exhibit similar properties, even when space-time seperated.
- Einstein famously referred to it as: "Spooky action at a distance".
- Schrödinger described it as: "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.".
- Quantum entanglement is a crucial resource for quantum computing and also for many quantum information security protocols.

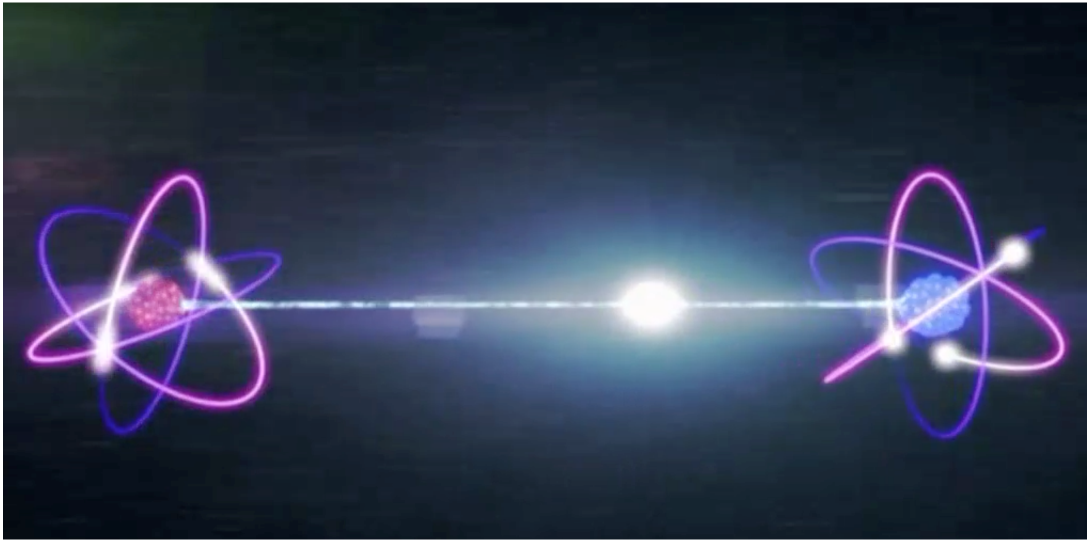


Figure: A most likely inaccurate illustration of quantum entanglement.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security (this is the case for encryption).

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security (this is the case for encryption).
- In the quantum case where all actors have quantum computers and use quantum communication channels, we get unconditional security.

Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution".

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions.
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time.
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is.
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security (this is the case for encryption).
- In the quantum case where all actors have quantum computers and use quantum communication channels, we get unconditional security.
- In the quantum case eavesdropping can be detected, but in the classical case it cannot.

Quantum Superposition – important resource

Very roughly speaking: a quantum system may be in many different states at the same time.

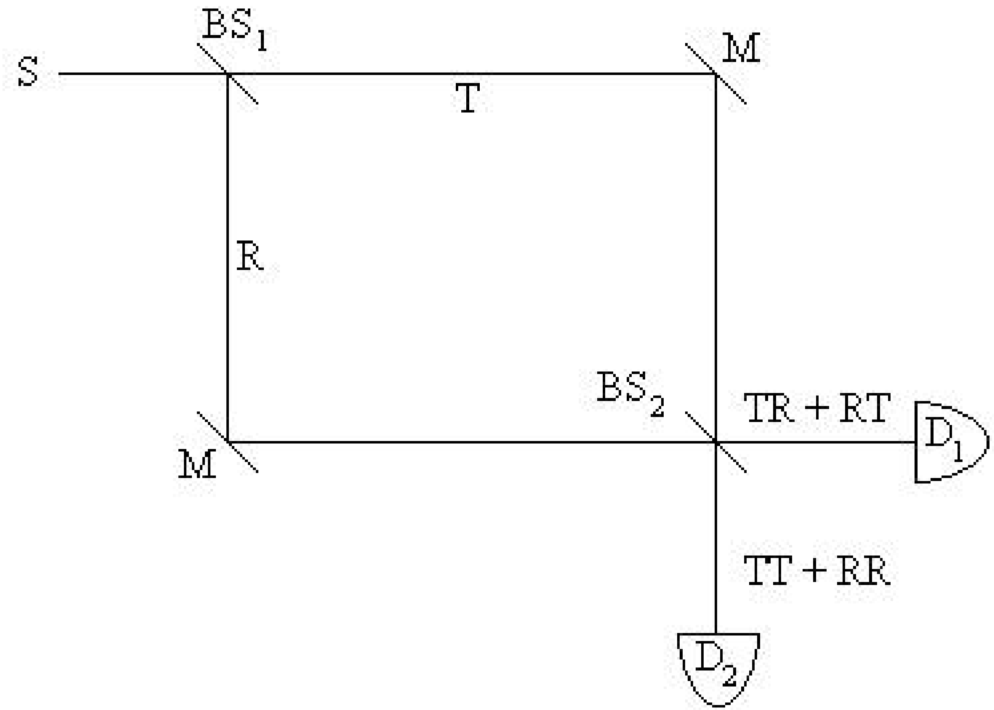


Figure: Single-photon interference performed with a Mach-Zehnder interferometer.

- Very rough analogy: allows for exponential parallelism.
- Crucial for computational speedup.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.
- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
    - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
    - Decent speedup, but not mind-blowing.
    - This results in improved computational complexity for many practical problems.
- Shor's algorithm:
    - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms.
    - This destroys all of the widely used public-key encryption systems.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.
- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms.
  - This destroys all of the widely used public-key encryption systems.
  - Online banking, internet commerce, private communication over the internet – dead.
  - New encryption systems will be needed to solve this problem.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.
- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms.
  - This destroys all of the widely used public-key encryption systems.
  - Online banking, internet commerce, private communication over the internet – dead.
  - New encryption systems will be needed to solve this problem.
- Improved computational complexity for many practical problems.

Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm.
  - Decent speedup, but not mind-blowing.
  - This results in improved computational complexity for many practical problems.
- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms.
  - This destroys all of the widely used public-key encryption systems.
  - Online banking, internet commerce, private communication over the internet – dead.
  - New encryption systems will be needed to solve this problem.
- Improved computational complexity for many practical problems.
- Many other improved algorithms are known, but the above two are the most famous.

About the course

- Required background: some basic linear algebra.
- This course is *not* about quantum physics. We cover quantum *computation*.
  - Example: you do not have to know anything about electromagnetism to study classical computation.
- We will cover only basic concepts, but enough to get you started for more advanced study/research/work.

Some extra material

- Almost all the material you need will be on the slides.
- If you want to learn more:
  - Lecture notes from Bob Coecke: `www.cs.ox.ac.uk/people/bob.coecke/QCS.pdf`. I recommend reading the notes if there are things you do not understand from the slides/lectures.
  - Book: Bob Coecke and Aleks Kissinger: *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press 2017.
  - Book: N.D. Mermin, *Quantum Computer Science*. Cambridge University Press 2007.
  - Book: M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press 2000.

Complex Numbers (Recap)

- Recall that a complex number is a number of the form $z = a + ib$, where $a, b \in \mathbb{R}$.
- The number a is the *real* part of z and the number b is the *imaginary* part of z.
- The *imaginary unit* is the complex number i, which satisfies $i^2 = -1$.
- Every real number a may be seen as a complex number with imaginary part 0.
- The complex numbers admit a geometric representation using cartesian coordinates in the complex plane.
- The absolute value of a complex number $z = a + ib$ is defined as $|z| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$.
- Addition of complex numbers is given by $(a + bi) + (c + di) = (a + c) + (b + d)i$.
- Multiplication of complex numbers is given by $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
- The conjugate complex number of $z = a + bi$ is the number $\overline{z} \stackrel{\text{def}}{=} a - bi$.
- **Euler's formula:** $e^{i\varphi} = \cos\varphi + i\sin\varphi$, for any $\varphi \in \mathbb{R}$.
- Every complex number z can also be expressed as $z = re^{i\varphi}$, where $r = |z| = \sqrt{z\overline{z}}$ and the argument φ is known as the *phase* (geometrically, it is the angle between the positive real axis and the complex number depicted on the complex plane).

Complex Numbers (Recap)

- Recall that a complex number is a number of the form $z = a + ib$, where $a, b \in \mathbb{R}$.
- The number a is the *real* part of z and the number b is the *imaginary* part of z.
- The *imaginary unit* is the complex number i, which satisfies $i^2 = -1$.
- Every real number a may be seen as a complex number with imaginary part 0.
- The complex numbers admit a geometric representation using cartesian coordinates in the complex plane.
- The absolute value of a complex number $z = a + ib$ is defined as $|z| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$.
- Addition of complex numbers is given by $(a + bi) + (c + di) = (a + c) + (b + d)i$.
- Multiplication of complex numbers is given by $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
- The conjugate complex number of $z = a + bi$ is the number $\overline{z} \stackrel{\text{def}}{=} a - bi$.
- **Euler's formula:** $e^{i\varphi} = \cos\varphi + i\sin\varphi$, for any $\varphi \in \mathbb{R}$.
- Every complex number z can also be expressed as $z = re^{i\varphi}$, where $r = |z| = \sqrt{z\overline{z}}$ and the argument φ is known as the *phase* (geometrically, it is the angle between the positive real axis and the complex number depicted on the complex plane).
- $\overline{e^{i\varphi}} =$

Complex Numbers (Recap)

- Recall that a complex number is a number of the form $z = a + ib$, where $a, b \in \mathbb{R}$.
- The number a is the *real* part of z and the number b is the *imaginary* part of z.
- The *imaginary unit* is the complex number i, which satisfies $i^2 = -1$.
- Every real number a may be seen as a complex number with imaginary part 0.
- The complex numbers admit a geometric representation using cartesian coordinates in the complex plane.
- The absolute value of a complex number $z = a + ib$ is defined as $|z| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$.
- Addition of complex numbers is given by $(a + bi) + (c + di) = (a + c) + (b + d)i$.
- Multiplication of complex numbers is given by $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
- The conjugate complex number of $z = a + bi$ is the number $\overline{z} \stackrel{\text{def}}{=} a - bi$.
- **Euler's formula:** $e^{i\varphi} = \cos\varphi + i\sin\varphi$, for any $\varphi \in \mathbb{R}$.
- Every complex number z can also be expressed as $z = re^{i\varphi}$, where $r = |z| = \sqrt{z\overline{z}}$ and the argument φ is known as the *phase* (geometrically, it is the angle between the positive real axis and the complex number depicted on the complex plane).
- $\overline{e^{i\varphi}} = e^{-i\varphi}$.

Complex Numbers (Recap)

- Recall that a complex number is a number of the form $z = a + ib$, where $a, b \in \mathbb{R}$.
- The number a is the *real* part of z and the number b is the *imaginary* part of z.
- The *imaginary unit* is the complex number i, which satisfies $i^2 = -1$.
- Every real number a may be seen as a complex number with imaginary part 0.
- The complex numbers admit a geometric representation using cartesian coordinates in the complex plane.
- The absolute value of a complex number $z = a + ib$ is defined as $|z| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$.
- Addition of complex numbers is given by $(a + bi) + (c + di) = (a + c) + (b + d)i$.
- Multiplication of complex numbers is given by $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
- The conjugate complex number of $z = a + bi$ is the number $\overline{z} \stackrel{\text{def}}{=} a - bi$.
- **Euler's formula:** $e^{i\varphi} = \cos\varphi + i \sin\varphi$, for any $\varphi \in \mathbb{R}$.
- Every complex number z can also be expressed as $z = re^{i\varphi}$, where $r = |z| = \sqrt{z\overline{z}}$ and the argument φ is known as the *phase* (geometrically, it is the angle between the positive real axis and the complex number depicted on the complex plane).
- $\overline{e^{i\varphi}} = e^{-i\varphi}$.
- $|e^{i\varphi}| =$

Complex Numbers (Recap)

- Recall that a complex number is a number of the form $z = a + ib$, where $a, b \in \mathbb{R}$.
- The number a is the *real* part of z and the number b is the *imaginary* part of z.
- The *imaginary unit* is the complex number i, which satisfies $i^2 = -1$.
- Every real number a may be seen as a complex number with imaginary part 0.
- The complex numbers admit a geometric representation using cartesian coordinates in the complex plane.
- The absolute value of a complex number $z = a + ib$ is defined as $|z| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$.
- Addition of complex numbers is given by $(a + bi) + (c + di) = (a + c) + (b + d)i$.
- Multiplication of complex numbers is given by $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
- The conjugate complex number of $z = a + bi$ is the number $\overline{z} \stackrel{\text{def}}{=} a - bi$.
- **Euler's formula:** $e^{i\varphi} = \cos\varphi + i \sin\varphi$, for any $\varphi \in \mathbb{R}$.
- Every complex number z can also be expressed as $z = re^{i\varphi}$, where $r = |z| = \sqrt{z\overline{z}}$ and the argument φ is known as the *phase* (geometrically, it is the angle between the positive real axis and the complex number depicted on the complex plane).
- $\overline{e^{i\varphi}} = e^{-i\varphi}$.
- $|e^{i\varphi}| = 1$.

Vector Spaces (Recap)

Definition

A *vector space* over the field of complex numbers $\mathbb{C}$ is a triple $(V, +, \cdot)$ consisting of a set V (the elements of which we refer to as *vectors*), a binary operation $+ : V \times V \to V$ called *vector addition* and a binary operation $\cdot : \mathbb{C} \times V \to V$ called *scalar multiplication* which satisfy the following axioms:

- **Commutativity.** For all vectors u and v in V, we have $u + v = v + u$.
- **Associativity.** For all vectors u, v and w in V, we have $(u + v) + w = u + (v + w)$.
- **Additive identity.** The set V contains an element, called the *zero vector* and denoted by 0, such that for any vector $v \in V$ we have $v + 0 = v$.
- **Additive inverses.** For any vector $v \in V$, there exists a vector $(-v) \in V$ which has the property that $v + (-v) = 0$.
- **Distributivity w.r.t. vector addition.** For every complex number $c \in \mathbb{C}$ and any vectors $u, v \in V$, we have $c \cdot (u + v) = (c \cdot u) + (c \cdot v)$.
- **Distributivity w.r.t. complex addition.** For every complex numbers $c, d \in \mathbb{C}$ and any vector $v \in V$, we have $(c + d) \cdot v = (c \cdot v) + (d \cdot v)$.
- **Compatability.** For all complex numbers $c, d \in \mathbb{C}$ and any vector $v \in V$, we have $c \cdot (d \cdot v) = (cd) \cdot v$.
- **Unitarity.** For any vector $v \in V$, we have $1 \cdot v = v$.

Remark

A few remarks:

- In this course we only consider finite-dimensional vector spaces over $\mathbb{C}$. From now on, this is implicitly assumed.
- The scalar multiplication $\cdot$ is usually written as juxtaposition, e.g., $3v \stackrel{\text{def}}{=} 3 \cdot v$.
- We write $u - v \stackrel{\text{def}}{=} u + (-v)$.

Vector Spaces (Recap)

Let us consider a few examples and non-examples of vector spaces.

- Any singleton set can be (uniquely) equipped with the structure of a vector space. Why?
- Can the empty set $\emptyset$ be equipped with the structure of a vector space?

Vector Spaces (Recap)

Let us consider a few examples and non-examples of vector spaces.

- Any singleton set can be (uniquely) equipped with the structure of a vector space. Why?
- Can the empty set $\emptyset$ be equipped with the structure of a vector space? No, because it does not contain a zero vector.

Vector Spaces (Recap)

Let us consider a few examples and non-examples of vector spaces.

- Any singleton set can be (uniquely) equipped with the structure of a vector space. Why?
- Can the empty set $\emptyset$ be equipped with the structure of a vector space? No, because it does not contain a zero vector.
- The set of complex numbers $\mathbb{C}$ can be seen as a vector space when we define vector addition to coincide with addition of complex numbers and when we define scalar multiplication to coincide with multiplication of complex numbers.

Vector Spaces (Recap)

Let us consider a few examples and non-examples of vector spaces.

- Any singleton set can be (uniquely) equipped with the structure of a vector space. Why?
- Can the empty set $\emptyset$ be equipped with the structure of a vector space? No, because it does not contain a zero vector.
- The set of complex numbers $\mathbb{C}$ can be seen as a vector space when we define vector addition to coincide with addition of complex numbers and when we define scalar multiplication to coincide with multiplication of complex numbers.
- The set $\mathbb{C}^n$ of n-tuples of complex numbers can be equipped with the structure of a vector space when we define:

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{pmatrix}$$

$$c \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} cu_1 \\ cu_2 \\ \vdots \\ cu_n \end{pmatrix},$$

where $u, v \in \mathbb{C}^n$ and $c \in \mathbb{C}$. **This is the most important example of a vector space in this course! This structure is canonical and we will often implicitly assume it.**

Linear (in)dependence (Recap)

Definition

Given a vector space V and a finite index set I, then a set of vectors $\{v_i\}_{i \in I}$ in V is said to be *linearly dependent* if the equation

$$\sum_{i \in I} a_i v_i = 0$$

has a non-trivial solution, i.e., we can find a set of scalars $a_i \in \mathbb{C}$ which validate the above equation, such that at least one of the scalars a_i is different from 0. If a set of vectors $\{v_i\}_{i \in I}$ is not linearly dependent, then we say that this set of vectors is *linearly independent*.

Questions:

- If a set of vectors contains the zero vector, then is it linearly dependent?
- Let v_1 and v_2 be two vectors. When are these two vectors linearly dependent?
- Is a singleton set of vectors linearly independent?

Linear Spans (Recap)

- **Definition:** Given a vector space $(V, +, \cdot)$, a *linear subspace* of V is a subset $W \subseteq V$, such that $(W, +, \cdot)$ is a vector space.
- This is equivalent to requiring that $c_1 w_1 + c_2 w_2 \in W$ for every two vectors $w_1, w_2 \in W$ and $c_1, c_2 \in \mathbb{C}$.
- **Definition:** Given a vector space V, the span of a set S, denoted $\mathrm{span}(S)$, is defined to be the intersection of all subspaces of V that contain S.
- It follows that $\mathrm{span}(S)$ is a subspace of V and

$$\mathrm{span}(S) = \left\{ \sum_{i=1}^{m} c_i v_i \mid m \in \mathbb{N}, v_i \in S, c_i \in \mathbb{C} \right\}.$$

- In other words, the span of a set S is the linear subspace of V that contains all finite linear combinations of vectors in S.
- **Question:** What is the span of the set

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

when seen as a subspace of $\mathbb{C}^3$ (with its canonical vector space structure)?

Basis (Recap)

- **Definition:** A *basis* of a vector space V is a set B of linearly independent vectors whose span is V.
- **Theorem:** Every vector space has a basis. Furthermore, every two bases of the same vector space have the same cardinality.
- **Definition:** The *dimension* of a vector space V, denoted $\dim(V)$, is the cardinality of a basis of V.
- **Remark:** In this course we only consider vector space over $\mathbb{C}$ which have *finite* dimension.
- If $B = \{v_1, \ldots, v_n\}$ is a basis of V, it follows that every vector $v \in V$ can be *uniquely* expressed as a linear combination of the basis elements:

$$v = c_1 v_1 + \cdots + c_n v_n.$$

- In this situation, the ordered tuple of complex numbers c_i are called the *coordinates* of the vector v with respect to the basis B.
- When a basis is fixed, or implicitly understood, we can simply write

$$v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

to denote this decomposition of v.

The Standard Basis of $\mathbb{C}^n$ (Recap)

- What is the dimension of the vector space $\mathbb{C}^n$?

The Standard Basis of $\mathbb{C}^n$ (Recap)

- What is the dimension of the vector space $\mathbb{C}^n$? $\dim(\mathbb{C}^n) = n$. Why?

The Standard Basis of $\mathbb{C}^n$ (Recap)

- What is the dimension of the vector space $\mathbb{C}^n$? $\dim(\mathbb{C}^n) = n$. Why?
- The *standard basis* of $\mathbb{C}^n$ is given by the set

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}.$$

Linear Maps (Recap)

- **Definition:** A function $f : V \to W$ between vector spaces V and W is said to be *linear* when
  - $f(v_1 + v_2) = f(v_1) + f(v_2)$; and
  - $f(a \cdot v) = a \cdot f(v)$,

  for any possible choice of a scalar $a \in \mathbb{C}$ and vectors $v, v_1, v_2 \in V$. We will also call linear functions by the names *linear maps* and *linear operators*.
- **Proposition:** Any linear map $f : V \to W$ is completely determined by its action on the basis elements. Indeed, writing v_i for the basis vectors of V, observe that:

$$f(v) = f(c_1 v_1 + \cdots + c_n v_n) = c_1 f(v_1) + \cdots + c_n f(v_n).$$

- **Proposition:** Any complex $m \times n$ matrix A determines a linear function $f_A : \mathbb{C}^n \to \mathbb{C}^m$ by setting $f_A(v) := Av$. Hint: recall how matrix multiplication works.
- **Proposition:** Conversely, every linear function $f : \mathbb{C}^n \to \mathbb{C}^m$ is completely determined by a $m \times n$ complex matrix A, such that $f_A(v) = f(v)$.
- Therefore, we may think of complex $m \times n$ matrices and linear functions $f : \mathbb{C}^n \to \mathbb{C}^m$ interchangeably and we will often do so from now on.
- **Proposition:** Any two vector spaces of the same dimension are isomorphic.

Composing Linear Maps and Matrix Multiplication (Recap)

- Let A be an $k \times m$ complex matrix and B an $m \times n$ complex matrix. Then $C = AB$, the matrix obtained via matrix multiplication, is a $k \times n$ matrix.
- Recall that the c_{ij} entry of C is given by the dot product of the i-th row of A and the j-th column of B.
- Matrix multiplication represents composition of linear functions. That is, if $f : W \to U$ is a linear map represented by the matrix A and $g : V \to W$ is a linear map represented by the matrix B, then the composition $f \circ g : V \to U$ is represented by the matrix $C = AB$.
- Composition of linear maps (and therefore multiplication of matrices) is associative, but not commutative, in general.
- **Question:** What is the matrix representation of the identity linear map on $\mathbb{C}^n$?
- **Exercise:** matrix multiplication.

Hilbert Spaces (Recap)

We want to equip vector spaces with some additional structure that will allow us to:

- measure the length of vectors.
- measure the angle between vectors.
- measure distances in the vector space.

We arrive at the concept of a Hilbert space.

Definition

A *finite-dimensional Hilbert space* is a finite-dimensional vector space $\mathcal{H}$ over the complex number field $\mathbb{C}$ which comes equipped with an *inner-product*, i.e., a map

$$\langle -, - \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C},$$

which satisfies the following properties:

- $\langle v, a_1 \cdot w_1 + a_2 \cdot w_2 \rangle = a_1 \langle v, w_1 \rangle + a_2 \langle v, w_2 \rangle$;
- $\langle v, w \rangle = \overline{\langle w, v \rangle}$;
- $\langle v, v \rangle \in \mathbb{R}$ and $\langle v, v \rangle \geq 0$;
- $\langle v, v \rangle = 0$ if and only if $v = \mathbf{0}$,

for any scalars $a_1, a_2 \in \mathbb{C}$ and any vectors $v, w, v_1, v_2, w_1, w_2 \in \mathcal{H}$.

From this definition follows:

$$\langle a_1 \cdot v_1 + a_2 \cdot v_2, w \rangle = \overline{a_1} \langle v_1, w \rangle + \overline{a_2} \langle v_2, w \rangle.$$

In other words, the inner product is linear in the second argument, but antilinear in the first.

Hilbert Spaces (Recap)

Recall that:

- The transpose of a matrix A is the matrix A^T with entries given by $a^T_{ij} \stackrel{\text{def}}{=} a_{ji}$, i.e., by swapping rows and columns.
- The conjugate of a matrix A is the matrix $\overline{A}$ with entries given by $\overline{a_{ij}} \stackrel{\text{def}}{=} \overline{a}_{ij}$, i.e., by entrywise conjugation.
- The conjugate transpose (also known as *adjoint*) of a matrix A is the matrix $A^\dagger$ given by $A^\dagger \stackrel{\text{def}}{=} \overline{A^T} = \overline{A}^T$.
- All of these definitions apply to vectors as special cases.

Proposition

The complex vector space $\mathbb{C}^n$ has the structure of a (finite-dimensional) Hilbert space when we define

$$\langle v, w \rangle := v^\dagger w.$$

Proof.

Exercise. $\square$

The Canonical Norm of a Hilbert Space

- Every Hilbert $\mathcal{H}$ space has a canonical norm $||-|| : \mathcal{H} \to \mathbb{R}_{\geq 0}$ defined by $||v|| \stackrel{\text{def}}{=} \sqrt{\langle v, v \rangle}$.
- The norm can be used to measure the length of vectors.
- This norm satisfies the usual properties of a norm, namely:
  - $||c \cdot v|| = |c|||v||$, where $c \in \mathbb{C}$ and $v \in \mathcal{H}$.
  - $||v + w|| \leq ||v|| + ||w||$, where $v, w \in \mathcal{H}$.
  - $||v|| = 0$ iff $v = 0$.

- **Exercise:** What is the norm of a vector in $\mathbb{C}^n$?

The Canonical Norm of a Hilbert Space

- Every Hilbert $\mathcal{H}$ space has a canonical norm $||-|| : \mathcal{H} \to \mathbb{R}_{\geq 0}$ defined by $||v|| \stackrel{\text{def}}{=} \sqrt{\langle v, v \rangle}$.
- The norm can be used to measure the length of vectors.
- This norm satisfies the usual properties of a norm, namely:
  - $||c \cdot v|| = |c|||v||$, where $c \in \mathbb{C}$ and $v \in \mathcal{H}$.
  - $||v + w|| \leq ||v|| + ||w||$, where $v, w \in \mathcal{H}$.
  - $||v|| = 0$ iff $v = 0$.
- **Exercise:** What is the norm of a vector in $\mathbb{C}^n$? **Answer:** If $v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{C}^n$ then

$$||v|| = \sqrt{\langle v, v \rangle} = \sqrt{v^\dagger v} = \sqrt{\sum_i |v_i|^2}$$

- **Definition:** A vector is said to be normalised whenever $||v|| = 1$.

Orthonormal Basis of a Hilbert Space

- An *orthonormal basis* of a Hilbert space $\mathcal{H}$ is a basis $B = \{v_1, \ldots, v_n\}$ of $\mathcal{H}$ (when seen as a vector space) such that:
$$\langle v_i, v_j \rangle = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$
- From now on, when we speak of a basis of a Hilbert space, we will implicitly assume the basis is orthonormal.
- **Exercise:** what is an orthonormal basis of $\mathbb{C}^n$? Are there more than one such bases? Can you think of a basis which is not orthonormal?

Adjoints

- **Theorem:** Let $f : \mathcal{H}_1 \to \mathcal{H}_2$ be a linear map between Hilbert spaces. Then, there exists a unique linear map $f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1$, such that

$$\langle v, f(w) \rangle = \langle f^\dagger(v), w \rangle$$

  for all vectors $v \in \mathcal{H}_2$ and $w \in \mathcal{H}_1$.
- The map $f^\dagger$ above is called the *adjoint* of f.
- If A is the matrix corresponding to the linear map f, then $A^\dagger$ (the conjugate transpose of A) is the matrix corresponding to the linear map $f^\dagger$.
- Note that $(f^\dagger)^\dagger = f$ and that $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$. **Exercise:** Can you prove these facts without using the matrix representation?

Unitary Maps

- **Definition:** Given a Hilbert space $\mathcal{H}$, a linear map $f : \mathcal{H} \to \mathcal{H}$ is said to be *unitary* if $f \circ f^\dagger = \mathrm{id} = f^\dagger \circ f$, where $\mathrm{id} : \mathcal{H} \to \mathcal{H}$ is the identity linear map.
- The same definition can be used to define a *unitary matrix*. That is, a complex matrix A is said to be unitary if $AA^\dagger = I = A^\dagger A$, where I is the identity matrix.
- **Theorem:** A map $f : \mathcal{H} \to \mathcal{H}$ is unitary iff f and $f^\dagger$ preserve the inner product:

$$\langle f(v), f(w) \rangle = \langle v, w \rangle \qquad \text{and} \qquad \langle f^\dagger(v), f^\dagger(w) \rangle = \langle v, w \rangle$$

- Note that this theorem implies that a unitary map preserves the norm as well.
- Unitary maps can be used to change (orthonormal) bases. That is, if $\{v_1, \ldots, v_n\}$ is an orthonormal basis of $\mathcal{H}$ and $f : \mathcal{H} \to \mathcal{H}$ is a unitary map, then $\{f(v_1), \ldots, f(v_n)\}$ is also an orthonormal basis of $\mathcal{H}$. **Exercise:** prove this.

Quantum Preliminaries

- *"Anyone who is not shocked by quantum theory has not understood it."* – Niels Bohr.
- Quantum theory was given its mathematical formalism mostly by John von Neumann in 1920s–1930s.
- This formalism is known as the "Hilbert Space Formalism" and this is what we introduce.
- We will only consider it for finite-dimensional spaces and we assume that we have full and perfect control of the underlying quantum systems. These are common assumptions in quantum computing.
- Even under those simplifying assumptions, the notion of a *quantum state* is very different from classical states. For example:
  - Quantum states can be combined via **superposition**.
  - Composite quantum systems cannot always be decomposed into simpler parts – a state of a composite system is *not* necessarily determined by the states of its components. In this situation, the state is **entangled**.
  - Quantum states cannot be copied, in general. This is known as the **no cloning theorem**.
  - Quantum states cannot be read off in the same way as classical states. One can only perform **quantum measurements** on quantum states which *change* the state that is being measured.
  - Performing the same measurement on the same state does *not* always produce the same result. The outcomes of quantum measurements are **probabilistic**.
  - Quantum systems may exhibit **non-local correlations** due to the possibility of entanglement, even when space-time separated. The resulting probability distributions *cannot* be explained via classical statistical mechanics.
  - In order to extract (classical) information from a quantum system, we have to perform quantum measurements on it, thereby changing its previous state.

Quantum bits (qubits)

The simplest (and most important) non-trivial quantum system is the *quantum bit*, often abbreviated to *qubit*.

Definition

The *state space of qubits* is given by the finite-dimensional Hilbert space $\mathbb{C}^2$. A *qubit* is described by a vector $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ which is normalised in the sense that $|a|^2 + |b|^2 = 1$. Two unit (i.e. normalised) vectors $\mathbf{q}_1, \mathbf{q}_2 \in \mathbb{C}^2$ represent the same qubit iff they differ by a normalised complex multiple, i.e, if there exists $z \in \mathbb{C}$ with $|z| = 1$ such that $\mathbf{q}_1 = z \cdot \mathbf{q}_2$.

Example

The *zero qubit* is defined to be $|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

The *one qubit* is defined to be $|1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

These two qubits form an (orthonormal) basis of $\mathbb{C}^2$ known as the *computational basis*.

Remark

You can think of $|0\rangle$ and $|1\rangle$ as corresponding to the classical bits 0 and 1.

Exercise

How many states does a bit have? How many states can a qubit have?

Quantum bits (qubits)

The simplest (and most important) non-trivial quantum system is the *quantum bit*, often abbreviated to *qubit*.

Definition

The *state space of qubits* is given by the finite-dimensional Hilbert space $\mathbb{C}^2$. A *qubit* is described by a vector $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ which is normalised in the sense that $|a|^2 + |b|^2 = 1$. Two unit (i.e. normalised) vectors $\mathbf{q}_1, \mathbf{q}_2 \in \mathbb{C}^2$ represent the same qubit iff they differ by a normalised complex multiple, i.e, if there exists $z \in \mathbb{C}$ with $|z| = 1$ such that $\mathbf{q}_1 = z \cdot \mathbf{q}_2$.

Example

The *zero qubit* is defined to be $|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

The *one qubit* is defined to be $|1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

These two qubits form an (orthonormal) basis of $\mathbb{C}^2$ known as the *computational basis*.

Remark

You can think of $|0\rangle$ and $|1\rangle$ as corresponding to the classical bits 0 and 1.

Exercise

How many states does a bit have? How many states can a qubit have?
Answer: A bit has two possible states – 0 or 1. A qubit can be in *uncountably* many states.

Exercise: qubits

Which of the following vectors represent qubits? Which of these vectors represent the same qubit?

- $\begin{pmatrix} i \\ 0 \end{pmatrix}$
- $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$
- $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
- $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$
- $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
- $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
- $\frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\phi} \\ e^{i\phi} \end{pmatrix}$, where $\phi \in [0, 2\pi)$.

Remark

Recall that $e^{i\phi} = \cos\phi + i\sin\phi$.

Superposition

Given an ONB $B = \{v_1, \ldots, v_n\}$ of a Hilbert space $\mathcal{H}$, we say that a vector of v of $\mathcal{H}$ is in *superposition* with respect to B iff the (unique) decomposition

$$v = \sum_{i=1}^{n} a_i v_i$$

has at least two non-zero coefficients a_i. Notice that the notion of superposition is relative to a basis.

Example

The *plus qubit* is defined to be $|+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$.

The *minus qubit* is defined to be $|-\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$.

These two qubits also form an (orthonormal) basis of $\mathbb{C}^2$.
Both of these qubits are a non-trivial linear combination of $|0\rangle$ and $|1\rangle$ (and vice versa). Because of this, we say that $|+\rangle$ (and $|-\rangle$) is in superposition of $|0\rangle$ and $|1\rangle$ (and vice versa).

Exercise

- How can you express $|+\rangle$ in terms of $|0\rangle$ and $|1\rangle$?
- How can you express $|-\rangle$ in terms of $|0\rangle$ and $|1\rangle$?
- How can you express $|0\rangle$ in terms of $|+\rangle$ and $|-\rangle$?
- How can you express $|1\rangle$ in terms of $|+\rangle$ and $|-\rangle$?

Single-qubit unitary operations

- In quantum computer science, we assume that the time evolution of quantum systems are described by unitary operators and that we have full control of it.
- Therefore this evolution is *deterministic* and *reversible*.
- **Example:** Unitary operations on a single qubit are described by unitary matrices acting on $\mathbb{C}^2$.

Exercise

Consider the following matrices:

$$H \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{and} \qquad T \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}.$$

What is $H^\dagger$ and $T^\dagger$? Are these matrices unitary? Describe the action of H and T on the computational basis. Describe the action of H on the $\{|+\rangle, |-\rangle\}$ basis.

Single-qubit unitary operations

Definition

The *Hadamard gate* is a single qubit unitary operation defined by

$$H \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The T *gate* is a single qubit unitary operation defined by

$$T \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}.$$

We then have:

- $H^\dagger = H$.
- $H\left|0\right\rangle = \left|+\right\rangle$ and $H\left|1\right\rangle = \left|-\right\rangle$.
- $H\left|+\right\rangle = \left|0\right\rangle$ and $H\left|-\right\rangle = \left|1\right\rangle$.
- $T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix}$.
- $T\left|0\right\rangle = \left|0\right\rangle$ and $T\left|1\right\rangle = e^{i\frac{\pi}{4}}\left|1\right\rangle$.

These two unitary gates (operations) are perhaps the most important examples of single-qubit deterministic transformations. In fact, any single-qubit unitary operation may be approximated with arbitrary precision by applying a sequence of H and T gates.

Exercise: expressing other quantum operations

Exercise

Consider the following quantum operations:

$$S \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad X \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Which of these operations are unitary? What is their action on the computational basis? What does Z do on the $\{|+\rangle, |-\rangle\}$ basis? Is it possible to express each of them as a combination of H and T? Hint: work from left to right and think in terms of basis states.

Exercise: expressing other quantum operations

Exercise

Consider the following quantum operations:

$$S \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad X \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

- All of them are unitary.
- $S = TT$; $\qquad S\left|0\right\rangle = \left|0\right\rangle, S\left|1\right\rangle = i\left|1\right\rangle.$
- $Z = SS$; $\qquad Z\left|0\right\rangle = \left|0\right\rangle, Z\left|1\right\rangle = -\left|1\right\rangle;$ $\qquad Z\left|+\right\rangle = \left|-\right\rangle, Z\left|-\right\rangle = \left|+\right\rangle.$
- $X = HZH$; $\qquad X\left|0\right\rangle = \left|1\right\rangle, X\left|1\right\rangle = \left|0\right\rangle.$

Bra-ket notation

Notation

We shall often write $|\psi\rangle \in \mathbb{C}^2$ to refer to arbitrary qubits. We also write $\langle\psi| \stackrel{\text{def}}{=} |\psi\rangle^\dagger$.

Exercise

Write in matrix notation the following expressions:

- $\langle 0|$.
- $\langle 1|$.
- $\langle +|$.
- $\langle -|$.

Are the above expressions qubits in $\mathbb{C}^2$?

Exercise

Write in matrix notation the following expressions:

- $|0\rangle\langle 0|$.
- $|1\rangle\langle 1|$.
- $|0\rangle\langle 0| + |1\rangle\langle 1|$.
- $|0\rangle\langle 1| + |1\rangle\langle 0|$.

Have we seen any of them before?

Inner product of qubits

Let $|\psi\rangle$ and $|\phi\rangle$ be two vectors in a Hilbert space. Observe that their inner product is

$$\langle \psi, \phi \rangle = \langle \psi| \, |\phi\rangle$$

We will therefore often write $\langle \psi|\phi\rangle \stackrel{\text{def}}{=} \langle \psi| \, |\phi\rangle$ for the inner product as well.

Exercise

What are the following inner products? Use linearity to compute most of them.

- $\langle 0|0\rangle$.
- $\langle 0|1\rangle$.
- $\langle 1|1\rangle$.
- $\langle +|-\rangle$.
- $\langle +|+\rangle$.
- $\langle -|-\rangle$.
- $\langle 0|+\rangle$.
- $\langle 1|+\rangle$.
- $\langle 0|-\rangle$.
- $\langle 1|-\rangle$.

Quantum measurement (single-qubit system)

Definition

Let $|\psi\rangle \in \mathbb{C}^2$ be an arbitrary qubit. A *single-qubit measurement in the computational basis* on state $|\psi\rangle$ collapses the state of the system to either $|0\rangle$ or $|1\rangle$ and produces one bit of classical information to the observer performing the measurement.
The probability the state collapses to $|0\rangle$ is $\langle\psi| |0\rangle \langle 0| |\psi\rangle$ and then the observer gets bit 0 as result.
The probability the state collapses to $|1\rangle$ is $\langle\psi| |1\rangle \langle 1| |\psi\rangle$ and then the observer gets bit 1 as result.

Notice: measurements are **probabilistic** and **irreversible**.

Exercise

Assume we are given a qubit $|\psi\rangle \in \mathbb{C}^2$. An observer performs a measurement in the computational basis. Describe the probability distribution of the possible measurement outcomes when:

- $|\psi\rangle = |0\rangle$.
- $|\psi\rangle = |1\rangle$.
- $|\psi\rangle = |+\rangle$.
- $|\psi\rangle = |-\rangle$.

Exercise

Assume we are given a qubit $|\psi\rangle \in \mathbb{C}^2$. We apply a T gate to $|\psi\rangle$. Does this influence the probability of the measurement outcomes? Why? What if we instead apply an H gate?

Exercise

The probability calculation in the above definition can be equivalently expressed in a simpler way. Do you see how?

Quantum measurement (single-qubit system)

Definition

Let $|\psi\rangle \in \mathbb{C}^2$ be an arbitrary qubit. A *single-qubit measurement in the computational basis* on state $|\psi\rangle$ collapses the state of the system to either $|0\rangle$ or $|1\rangle$ and produces one bit of classical information to the observer performing the measurement.
The probability the state collapses to $|0\rangle$ is $\langle\psi| |0\rangle \langle 0| |\psi\rangle$ and then the observer gets bit 0 as result.
The probability the state collapses to $|1\rangle$ is $\langle\psi| |1\rangle \langle 1| |\psi\rangle$ and then the observer gets bit 1 as result.

Notice: measurements are **probabilistic** and **irreversible**.

Exercise

Assume we are given a qubit $|\psi\rangle \in \mathbb{C}^2$. An observer performs a measurement in the computational basis. Describe the probability distribution of the possible measurement outcomes when:

- $|\psi\rangle = |0\rangle$.
- $|\psi\rangle = |1\rangle$.
- $|\psi\rangle = |+\rangle$.
- $|\psi\rangle = |-\rangle$.

Exercise

Assume we are given a qubit $|\psi\rangle \in \mathbb{C}^2$. We apply a T gate to $|\psi\rangle$. Does this influence the probability of the measurement outcomes? Why? What if we instead apply an H gate?

Exercise

The probability calculation in the above definition can be equivalently expressed in a simpler way. Do you see how? **Answer:** If $\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, then outcome 0 occurs with probability $|\alpha|^2$ and outcome 1 occurs with probability $|\beta|^2$.

Composite quantum systems

Definition

The state space of an n-qubit system is given by $\mathbb{C}^{2^n}$. The state of an n-qubit register is a unit vector of $\mathbb{C}^{2^n}$. Two unit vectors $\mathbf{q}_1, \mathbf{q}_2 \in \mathbb{C}^{2^n}$ represent the same state iff they differ by a normalised complex multiple, i.e, if there exists $z \in \mathbb{C}$, with $|z| = 1$ such that $\mathbf{q}_1 = z \cdot \mathbf{q}_2$.

Remark

Recall that a vector $(a_1 \cdots a_n)^T \in \mathbb{C}^n$ is a unit vector when

$$\sum_i |a_i|^2 = 1.$$

Exercise

What is the state space of the smallest possible quantum register?

Composite quantum systems

Definition

The state space of an n-qubit system is given by $\mathbb{C}^{2^n}$. The state of an n-qubit register is a unit vector of $\mathbb{C}^{2^n}$. Two unit vectors $\mathbf{q}_1, \mathbf{q}_2 \in \mathbb{C}^{2^n}$ represent the same state iff they differ by a normalised complex multiple, i.e, if there exists $z \in \mathbb{C}$, with $|z| = 1$ such that $\mathbf{q}_1 = z \cdot \mathbf{q}_2$.

Remark

Recall that a vector $(a_1 \cdots a_n)^T \in \mathbb{C}^n$ is a unit vector when

$$\sum_i |a_i|^2 = 1.$$

Exercise

What is the state space of the smallest possible quantum register? **Answer:** $\mathbb{C}$, when $n = 0$.

Definition

Given an n-qubit state $|\psi\rangle$ and an m-qubit state $|\phi\rangle$, then the *composed system* containing $|\psi\rangle$ and $|\phi\rangle$ is described by the $n+m$-qubit state $|\psi\phi\rangle \stackrel{\text{def}}{=} |\psi\rangle \otimes |\phi\rangle$, where $(- \otimes -)$ denotes the Kronecker product.

Remark

Recall that the Kronecker product of an $n \times m$ matrix $A = (a_{i,j})$ and $p \times r$ matrix B is the $(np \times mr)$ matrix

$$\begin{pmatrix} a_{1,1}B & \cdots & a_{1,m}B \\ a_{2,1}B & \cdots & a_{2,m}B \\ \vdots & \cdots & \vdots \\ a_{n,1}B & \cdots & a_{n,m}B \end{pmatrix}.$$

Properties of the Tensor/Kronecker Product

From linear algebra we know that:

- Tensor product of (finite-dimensional) Hilbert spaces: $\mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{C}^{nm}$.
- The tensor product is a bilinear operation. In particular:
  - $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$.
  - $(A + B) \otimes C = (A \otimes C) + (B \otimes C)$.
  - $(zA) \otimes B = A \otimes (zB) = z(A \otimes B)$.
- The tensor product is associative: $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.
- $\mathbf{0} \otimes B = \mathbf{0} = A \otimes \mathbf{0}$.
- Interchange law: $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.
- Adjoints: $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

where $z \in \mathbb{C}$, $\mathbf{0}$ is a zero matrix and where A, B, C, D are complex matrices (of appropriate dimensions in some of the above equations).

Exercise

Compute $(H \otimes H) |00\rangle$ using the above properties.

Exercise

Simplify the following expression: $(T \otimes H^\dagger)(I \otimes H)(T^\dagger \otimes I)$.

Exercise

Rewrite $A \otimes (\sum_{i=1}^n z_i B_i)$ in another form. Do the same for $(\sum_{j=1}^m y_j A_j) \otimes (\sum_{i=1}^n z_i B_i)$.

Composite quantum systems

Exercise

Write down the following states in vector notation:

- $|00\rangle$.
- $|11\rangle$.
- $|0+\rangle$.
- $|1-\rangle$.
- $|+1\rangle$.
- $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Definition

An *n*-qubit state $|\psi\rangle$ is *entangled* when there exists no non-trivial quantum states $|\phi\rangle$ and $|\tau\rangle$, such that $|\psi\rangle = |\phi\rangle \otimes |\tau\rangle$ (non-trivial means that the two states contain at least one qubit).

Exercise

The *Bell state* is the state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Is this state entangled?

Composite quantum systems

Exercise

Write down the following states in vector notation:

- $|00\rangle$.
- $|11\rangle$.
- $|0+\rangle$.
- $|1-\rangle$.
- $|+1\rangle$.
- $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Definition

An n-qubit state $|\psi\rangle$ is *entangled* when there exists no non-trivial quantum states $|\phi\rangle$ and $|\tau\rangle$, such that $|\psi\rangle = |\phi\rangle \otimes |\tau\rangle$ (non-trivial means that the two states contain at least one qubit).

Exercise

The *Bell state* is the state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Is this state entangled? **Answer:** Yes, it is. A simple algebraic argument shows that it is not the Kronecker product of any two vectors in $\mathbb{C}^2$. The Bell state is the most important example of quantum entanglement.

Composite quantum system dynamics

Definition

Deterministic operations on an n-qubit system are described by unitary matrices acting on $\mathbb{C}^{2^n}$.

Exercise

How do the following quantum states evolve when we apply the $H \otimes X$ operation on them (recall that $(- \otimes -)$ is bilinear)?

- $|01\rangle$.
- $|{+}0\rangle$.
- $|0{+}\rangle$.
- $|0{-}\rangle$.
- $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

How can we manipulate entanglement?

Exercise

Assume that $|\psi\rangle = |\phi\rangle \otimes |\tau\rangle$ is a non-entangled state, where $|\phi\rangle$ is an n-qubit state and $|\tau\rangle$ is an m-qubit state. Assume further that $U_1 : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$ and $U_2 : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ are unitary maps. Is the state $(U_1 \otimes U_2)(|\psi\rangle \otimes |\phi\rangle)$ entangled?

How can we manipulate entanglement?

Exercise

Assume that $|\psi\rangle = |\phi\rangle \otimes |\tau\rangle$ is a non-entangled state, where $|\phi\rangle$ is an n-qubit state and $|\tau\rangle$ is an m-qubit state. Assume further that $U_1 : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$ and $U_2 : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ are unitary maps. Is the state $(U_1 \otimes U_2)(|\psi\rangle \otimes |\phi\rangle)$ entangled?

Answer: No, because $(U_1 \otimes U_2)(|\phi\rangle \otimes |\tau\rangle) = (U_1 |\phi\rangle) \otimes (U_2 |\tau\rangle)$ due to bilinearity of the Kronecker product.

How can we manipulate entanglement?

Exercise

Assume that $|\psi\rangle = |\phi\rangle \otimes |\tau\rangle$ is a non-entangled state, where $|\phi\rangle$ is an n-qubit state and $|\tau\rangle$ is an m-qubit state. Assume further that $U_1 : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$ and $U_2 : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ are unitary maps. Is the state $(U_1 \otimes U_2)(|\psi\rangle \otimes |\phi\rangle)$ entangled?

Answer: No, because $(U_1 \otimes U_2)(|\phi\rangle \otimes |\tau\rangle) = (U_1 |\phi\rangle) \otimes (U_2 |\tau\rangle)$ due to bilinearity of the Kronecker product.

Exercise

Assume that $|\psi\rangle$ is an entangled 2-qubit state. Assume further that $U_1 : \mathbb{C}^2 \to \mathbb{C}^2$ and $U_2 : \mathbb{C}^2 \to \mathbb{C}^2$ are unitary maps. Is the state $(U_1 \otimes U_2) |\psi\rangle$ entangled?

How can we manipulate entanglement?

Exercise

Assume that $|\psi\rangle = |\phi\rangle \otimes |\tau\rangle$ is a non-entangled state, where $|\phi\rangle$ is an n-qubit state and $|\tau\rangle$ is an m-qubit state. Assume further that $U_1 : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$ and $U_2 : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ are unitary maps. Is the state $(U_1 \otimes U_2)(|\psi\rangle \otimes |\phi\rangle)$ entangled?
Answer: No, because $(U_1 \otimes U_2)(|\phi\rangle \otimes |\tau\rangle) = (U_1 |\phi\rangle) \otimes (U_2 |\tau\rangle)$ due to bilinearity of the Kronecker product.

Exercise

Assume that $|\psi\rangle$ is an entangled 2-qubit state. Assume further that $U_1 : \mathbb{C}^2 \to \mathbb{C}^2$ and $U_2 : \mathbb{C}^2 \to \mathbb{C}^2$ are unitary maps. Is the state $(U_1 \otimes U_2) |\psi\rangle$ entangled?
Answer: Yes. Assume for contradiction that it is not entangled. Then by the above exercise it follows that applying $(U_1^\dagger \otimes U_2^\dagger)$ to the non-entangled state would still result in a non-entangled state. But this means

$$(U_1^\dagger \otimes U_2^\dagger)(U_1 \otimes U_2) |\psi\rangle = (U_1^\dagger U_1 \otimes U_2^\dagger U_2) |\psi\rangle = (I \otimes I) |\psi\rangle = |\psi\rangle$$

must be non-entangled which is a contradiction.

- So, how can we change introduce/eliminate entanglement in a quantum system?
- For this we need to consider some additional unitary operations that we have not seen so far.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\mathrm{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\mathrm{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.
- $|01\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.
- $|01\rangle$. **Answer:** $\mathrm{CNOT}\,|01\rangle = |01\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.
- $|01\rangle$. **Answer:** $\mathrm{CNOT}\,|01\rangle = |01\rangle$.
- $|10\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.
- $|01\rangle$. **Answer:** $\mathrm{CNOT}\,|01\rangle = |01\rangle$.
- $|10\rangle$. **Answer:** $\mathrm{CNOT}\,|10\rangle = |11\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.
- $|01\rangle$. **Answer:** $\mathrm{CNOT}\,|01\rangle = |01\rangle$.
- $|10\rangle$. **Answer:** $\mathrm{CNOT}\,|10\rangle = |11\rangle$.
- $|11\rangle$.

The CNOT gate

Definition

The CNOT operation is a 2-qubit unitary map defined by

$$\mathrm{CNOT} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

What is $\mathrm{CNOT}^\dagger$? What is the action of CNOT on the computational basis states:

- $|00\rangle$. **Answer:** $\mathrm{CNOT}\,|00\rangle = |00\rangle$.
- $|01\rangle$. **Answer:** $\mathrm{CNOT}\,|01\rangle = |01\rangle$.
- $|10\rangle$. **Answer:** $\mathrm{CNOT}\,|10\rangle = |11\rangle$.
- $|11\rangle$. **Answer:** $\mathrm{CNOT}\,|11\rangle = |10\rangle$.

Creating Entanglement

Exercise

Consider the 2-qubit state $|00\rangle$. Find two unitary gates which can be applied to $|00\rangle$ resulting in the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Hint: the second one should be CNOT. The first one should create superposition on one of the qubits.

Creating Entanglement

Exercise

Consider the 2-qubit state $|00\rangle$. Find two unitary gates which can be applied to $|00\rangle$ resulting in the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Hint: the second one should be CNOT. The first one should create superposition on one of the qubits.

Answer: Consider the map $\mathrm{CNOT}(H \otimes I)$. Then, we get:

$$\mathrm{CNOT}(H \otimes I)\,|00\rangle = \mathrm{CNOT}\,|{+}0\rangle = \mathrm{CNOT}\frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{\mathrm{CNOT}\,|00\rangle + \mathrm{CNOT}\,|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

This shows that we can use the *combination* of a CNOT and H gates to create entanglement.

Measurement in composite systems

Remark

Every non-zero vector $v \in \mathbb{C}^n$ can be normalised by setting $v' = \frac{v}{||v||}$. Why is this true?

Remark

In this course we only consider measurements in the computational basis and they are given in the following way.

Definition

Assume we are given an n-qubit quantum system $|\psi\rangle \in \mathbb{C}^{2^n}$. A measurement on qubit $1 \leq i \leq n$ is determined by the following process. Let $P_0^i = I \otimes \cdots \otimes I \otimes |0\rangle \langle 0| \otimes I \otimes \cdots \otimes I$ and $P_1^i = I \otimes \cdots \otimes I \otimes |1\rangle \langle 1| \otimes I \otimes \cdots \otimes I$. That is in P_0^i we apply $|0\rangle \langle 0|$ at the i-th position and we tensor with the identity matrix on all other positions. Similarly for P_1^i.

After performing the measurement:

- the state of the system collapses to $\frac{P_0^i|\psi\rangle}{||P_0^i|\psi\rangle||}$ with probability $||P_0^i |\psi\rangle ||^2$.
- the state of the system collapses to $\frac{P_1^i|\psi\rangle}{||P_1^i|\psi\rangle||}$ with probability $||P_1^i |\psi\rangle ||^2$.

Exercise

Describe the probability distributions that result from measuring the first qubit of the following states:

- $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
- $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$, $|{-}{-}\rangle$.
- $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. After we measure the first qubit here, what happens if you measure the second one?

Measurement in composite systems

- Measuring several qubits of a composite system simultaneously is the same as measuring individual qubits one after the other (in any order).
- We describe the special case where we measure all qubits simultaneously. This is usually what is done.

Definition

Assume we are given an n-qubit quantum system $|\psi\rangle \in \mathbb{C}^{2^n}$. Measuring all qubits of $|\psi\rangle$ in the computational basis is determined by the following process. Let

$$P_{i_1,\ldots,i_n} = |i_1\rangle\langle i_1| \otimes \cdots \otimes |i_n\rangle\langle i_n| \in \mathbb{C}^{2^n \times 2^n}$$

where $i_j \in \{0,1\}$. After performing the measurement:

- the state of the system collapses to $|i_1 i_2 \cdots i_n\rangle$ with probability $||P_{i_1 i_2 \cdots i_n} |\psi\rangle ||^2$.

Exercise

Describe the probability distributions that result from measuring all qubits of the following states:

- $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
- $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$, $|{-}{-}\rangle$.
- $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Exercise

The above formula for the probability computation can be simplified. How?

Measurements of entangled states

- Consider the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. This is arguably the most important entangled state.
- We just determined that measuring any one qubit would produce measurement outcome 0 or 1 with equal probability.
- However, we also determined that measuring both qubits produces outcomes 00 or 11 with equal probability.
- That is, if we measure one qubit first and consider the outcome, then with probability 100% we know the outcome of the measurement on the second qubit.
- These correlations *cannot* be explained by classical statistical mechanics.

No cloning

- Quantum information cannot be copied, in general.

Proposition

There exists no unitary operation $C : \mathbb{C}^4 \to \mathbb{C}^4$, such that for an arbitrary qubit $|\psi\rangle$:

$$C(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle .$$

Proof.

Exercise:

No cloning

- Quantum information cannot be copied, in general.

Proposition

There exists no unitary operation $C : \mathbb{C}^4 \to \mathbb{C}^4$*, such that for an arbitrary qubit* $|\psi\rangle$ *:*

$$C(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle .$$

Proof.

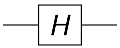
Exercise: Assume that such C exists. Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary qubits. Then:

$$\begin{aligned}\langle\psi|\phi\rangle &= \langle\psi|\phi\rangle \cdot 1 = \langle\psi|\phi\rangle \cdot \langle 0|0\rangle = (\langle\psi| \otimes \langle 0|)(|\phi\rangle \otimes |0\rangle) = \\ &= (\langle\psi| \otimes \langle 0|)I(|\phi\rangle \otimes |0\rangle) = (\langle\psi| \otimes \langle 0|)C^\dagger C(|\phi\rangle \otimes |0\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) \\ &= \langle\psi|\phi\rangle \cdot \langle\psi|\phi\rangle\end{aligned}$$

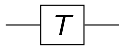
With this, we can now easily reach a contradiction by choosing appropriate $|\psi\rangle$ and $|\phi\rangle$. Example: choose $|\psi\rangle = |0\rangle$ and $|\phi\rangle = |+\rangle$. □

Quantum circuits

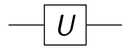
Quantum operations admit a diagrammatic representation in the form of *quantum circuit diagrams*.



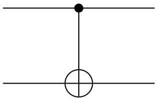
H unitary operator



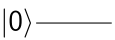
T unitary operator



U unitary operator

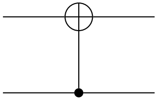


$CNOT$ unitary operator

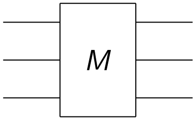


Prepare a new qubit in state $|0\rangle$

Measure a qubit in the computational basis



$CNOT$ unitary operator with swapped inputs



A three qubit unitary operator called M

Remark

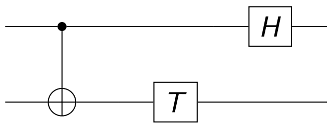
In the literature, authors often use other notations for measurement.

Quantum circuits

- Circuits should be read left-to-right and top-to-bottom.
- Left-to-right direction corresponds to sequential composition (matrix multiplication).
- Topt-to-bottom corresponds to spatial composition (kronecker product/tensor product).

Example

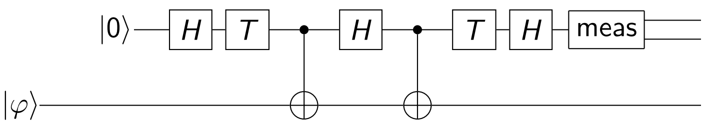
The following circuit:



describes the unitary operator $(H \otimes I)(I \otimes T)CNOT$.

Example

The following circuit:



describes the following quantum algorithm:

1. Input: an arbitrary qubit (abstracted to state $|\varphi\rangle$ above).
2. Prepare a new qubit in state $|0\rangle$. The new state is now $|0\rangle \otimes |\varphi\rangle$.
3. Apply the unitary operator $(H \otimes I)(T \otimes I)CNOT(H \otimes I)CNOT(T \otimes I)(H \otimes I)$.
4. Measure the first (auxiliary, i.e., non-input) qubit.

Quantum teleportation

- Quantum teleportation is an interesting protocol which allows (possibly separated) parties to move quantum information from one place to another.
- In the protocol, there are two parties – Alice and Bob.
- Alice has some qubit $|\psi\rangle$ which she wishes to send to Bob.
- How can this be done? Remember, we cannot copy quantum information.

Quantum teleportation

The protocol is described as follows:

1. Alice has an input qubit $|\psi\rangle$ in her possession.
2. Alice and Bob prepare the Bell state together.
3. After preparing the Bell state, Alice controls one qubit and Bob controls the other.
4. Alice applies a CNOT operation on her two qubits with $|\psi\rangle$ being the control qubit.
5. Alice applies a Hadamard operation on her first qubit.
6. Alice measures her two qubits in the computational basis and reads the measurement outcome (b_1, b_2), which indicates to what state her subsystem has collapsed.
7. Alice sends the two classical bits (b_1, b_2) to Bob.
8. Bob now applies the unitary operation $Z^{b_1} \circ X^{b_2}$ on his qubit. This means, he applies X iff $b_2 = 1$ and he applies Z iff $b_1 = 1$.
9. Bob's qubit is now in state $|\psi\rangle$.

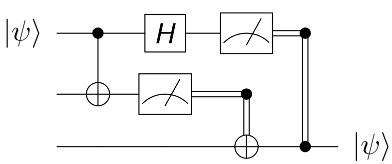


Figure: Quantum circuit representation of quantum teleportation (as seen in the literature).

Quantum teleportation

- **Exercise:** verify the quantum teleportation protocol.

Quantum teleportation

- **Exercise:** verify the quantum teleportation protocol.
- So what can we learn from this?
- 2 bits of classsical information + entanglement = quantum teleportation.
- But a qubit can be in uncountably many states and the shared entangled state is always the Bell state.
- Does it seems counter-intuitive?
- Experimentally confirmed many times, so this does indeed work.

Shor's algorithm

- Problem: Given an integer N, find a non-trivial integer divisor of N.
- Classical results from number theory: it suffices to solve the period finding problem.
- Period finding: Given a function $f(x) = a^x \mod N$, where a and N are positive integers, $a < N$ and such that a and N have no common factors, find the smallest integer $r > 0$, such that $a^r \mod N = 1$.
- Shor's algorithm can solve this problem in polynomial time on a quantum computer. The best known classical algorithms need exponential time.
- For the setup of the algorithm, let us assume that $N^2 \leq 2^q = Q$.
- In the description of the algorithm, for an integer $k < N$, we shall write $|k\rangle = |k_1\rangle \otimes \cdots \otimes |k_n\rangle$, where $k_1 \cdots k_n$ is the bit representation of k.

Shor's algorithm

1. Initialise the state to $|0^{2q}\rangle$.
2. Apply H^q to the first q qubits. The new state is now

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle \otimes |0^q\rangle$$

3. Implement the quantum oracle U_f which realises the classical function f. It has action $U_f(|x\rangle \otimes |0^q\rangle) = |x\rangle \otimes |f(x)\rangle$.
4. Apply the quantum oracle to the current state. The new state is then

$$U_f\left(\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle \otimes |0^q\rangle\right) = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle \otimes |f(x)\rangle$$

5. Apply the quantum Fourier transform to the first q qubits. The QFT unitary is given by

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{Q}}\sum_{y=0}^{Q-1}\omega^{xy}\,|y\rangle$$

where $\omega = e^{2\pi i/Q}$ is the Q-th root of unity. After applying QFT to the previous state, we get

$$(QFT \otimes I)\left(\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle \otimes |f(x)\rangle\right) = \frac{1}{Q}\sum_{x=0}^{Q-1}\sum_{y=0}^{Q-1}\omega^{xy}\,|y\rangle \otimes |f(x)\rangle$$

6. Measure in the computational basis. Now, with high probability and some classical computation, the period is found. If it is not found, then repeat the process until we find it.