

# Quantum Systems

(Lecture 3: Quantum states and computation)

Luís Soares Barbosa



Universidade do Minho



UNITED NATIONS  
UNIVERSITY

**UNU-EGOV**

Universidade do Minho

# The principles

Quantum computation explores the laws of quantum theory as computational resources.

Thus, the principles of the former are directly derived from the postulates of the latter.

- The state **space** postulate
- The state **evolution** postulate
- The state **composition** postulate
- The state **measurement** postulate

The underlying maths is that of Hilbert spaces.

# The underlying maths: Hilbert spaces

## Complex, inner-product vector space

A complex vector space with **inner product** which measures how much two vectors **overlap**:

$$\langle - | - \rangle : H \times H \longrightarrow \mathbb{C}$$

such that

$$(1) \quad \langle v | \sum_i \lambda_i \cdot |w_i\rangle \rangle = \sum_i \lambda_i \langle v | w_i \rangle$$

$$(2) \quad \langle v | w \rangle = \overline{\langle w | v \rangle}$$

$$(3) \quad \langle v | v \rangle \geq 0 \text{ (with equality iff } |v\rangle = 0)$$

Note:  $\langle - | - \rangle$  is **conjugate linear** in the first argument:

$$\langle \sum_i \lambda_i \cdot |w_i\rangle | v \rangle = \sum_i \overline{\lambda_i} \langle w_i | v \rangle$$

cinzaNotation:  $\langle v | w \rangle \equiv (|v\rangle, |w\rangle)$

# Dirac's notation

Dirac's bra/ket notation is a handy way to represent elements and constructions on an Hilbert space

- $|u\rangle$  A **ket** stands for a vector in an Hilbert space  $H$ . In  $\mathbb{C}^n$ , it is a column vector of complex entries. Note that the identity for  $+$  (the **zero** vector) is just written 0.
- $\langle u|$  A **bra** is a vector in the **dual** space  $H^*$ , i.e. scalar-valued linear maps in  $H$ . In  $(\mathbb{C}^n)^*$  it is the **adjoint**, i.e. the conjugate transpose, of the corresponding **ket**, therefore a row vector.

There is a bijective correspondence between  $|u\rangle$  and  $\langle u|$

$$|u\rangle = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \Leftrightarrow [\bar{u}_1 \cdots \bar{u}_n] = \langle u|$$

# Inner product: examples

In  $\mathbb{C}$

$$\langle a + bi | c + di \rangle = (a - bi)(c + di) = ac + adi - bci + bd$$

In  $\mathbb{C}^n$ : The dot product

Amost useful example of a **inner product** is the **dot product**

$$\langle u | v \rangle = \underbrace{[\overline{u_1} \quad \overline{u_2} \quad \cdots \quad \overline{u_n}]}_{\langle u |} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \sum_{i=1}^n \overline{u_i} v_i$$

where  $\bar{c} = a - ib$  is the complex conjugate of  $c = a + ib$

.

## Old friends: The dual space

$H^*$

If  $H$  is a Hilbert space,  $H^*$  is the space of **linear maps** from  $H$  to  $\mathbb{C}$ .

Elements of  $H^*$  are denoted by

$$\langle u| : H \longrightarrow \mathbb{C} \text{ and defined as } \langle u|(|v\rangle) = \langle u|v\rangle$$

In a matricial representation  $\langle u|$  is obtained as the **Hermitian conjugate** (i.e. the **transpose** of the vector composed by the **complex conjugate** of each element) of  $|u\rangle$ , therefore the dot product of  $|u\rangle$  and  $|v\rangle$ .

## Old friends: Norms and orthogonality

- The inner product measures the *degree of overlapping*:  $|v\rangle$  and  $|w\rangle$  are **orthogonal** if  $\langle v|w\rangle = 0$
- The "length" of a vector uses the measure of its overlap with itself to yield the (Euclidean) **norm**:

$$\| |v\rangle \| = \sqrt{\langle v|v\rangle}$$

(generalizing the distance between two points)

- $|v\rangle$  is a **unit vector** if  $\| |v\rangle \| = 1$
- **normalization**:  $\frac{|v\rangle}{\| |v\rangle \|}$
- A set of vectors  $\{|i\rangle, |j\rangle, \dots\}$  is **orthonormal** if each  $|i\rangle$  is a unit vector and

$$\langle i|j\rangle = \delta_{i,j} = \begin{cases} i=j & \Rightarrow 1 \\ \text{otherwise} & \Rightarrow 0 \end{cases}$$

# Old friends: Bases

## Orthonormal basis

A orthonormal basis for a Hilbert space  $H$  of dimension  $n$  is a set  $B = \{|i\rangle \mid i \in n - 1\}$  of  $n$  linearly independent elements of  $H$  st

- $\langle i|j\rangle = \delta_{i,j}$  for all  $|i\rangle, |j\rangle \in B$
- and  $B$  **spans**  $H$ , i.e. every  $|v\rangle$  in  $H$  can be written as

$$|v\rangle = \sum_i \alpha_i |i\rangle \quad \text{for some } \alpha_i \in \mathbb{C}$$

Note that the **amplitude** or **coefficient** of  $|v\rangle$  wrt  $|i\rangle$  satisfies

$$\alpha_i = \langle i|v\rangle$$

Why?



# Bases

$\alpha_i = \langle i | v \rangle$  because

$$\begin{aligned}\langle i | v \rangle &= \langle i | \sum_j \alpha_j | j \rangle \\ &= \sum_j \alpha_j \langle i | j \rangle \\ &= \sum_j \alpha_j \delta_{i,j} \\ &= \alpha_i\end{aligned}$$

## Note

If  $|v\rangle$  is expressed wrt an orthonormal basis  $\{|i\rangle \mid i \in n\}$ , i.e.

$|v\rangle = \sum_i \alpha_i |i\rangle$ , then

$$\| |v\rangle \| = \sum_i \| \alpha_i \|^2$$

## Example: The Hadamard basis

One of the infinitely many orthonormal bases for a space of dimension 2:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

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

Check, e. g.

$$\langle + | - \rangle = \frac{1}{2}(\langle 0 | + \langle 1 |, |0\rangle - |1\rangle) = \frac{1}{2} \left( \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right) = \frac{1}{2} \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = 0$$

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

# Bases

## A basis for $H^*$

If  $\{|i\rangle \mid i \in n\}$  is an orthonormal basis for  $H$ , then

$$\{\langle i| \mid i \in n\}$$

is an orthonormal basis for  $H^*$ .

# Hilbert spaces

## The complete picture

An **Hilbert space** is an inner-product space  $H$  st the metric defined by its norm turns  $H$  into a **complete metric space**, i.e. any Cauchy sequence

$$|v_1\rangle, |v_2\rangle, \dots$$

$$\forall \epsilon > 0 \exists N \forall m, n > N \quad \| |v_m\rangle - |v_n\rangle \| \leq \epsilon$$

converges

(i.e. there exists an element  $|s\rangle$  in  $H$  st  $\forall \epsilon > 0 \exists N \forall n > N \quad \| |s\rangle - |v_n\rangle \| \leq \epsilon$  )

The completeness condition is trivial in **finite dimensional** vector spaces

# The state space postulate

## Postulate 1

The state space of a quantum system is described by a unit vector in a Hilbert space

- In practice, with finite resources, one cannot distinguish between a **continuous** state space from a **discrete** one with arbitrarily small minimum spacing between adjacent locations.
- One may, then, restrict to **finite-dimensional** (complex) Hilbert spaces.

# The state space postulate

A quantum (binary) state is represented as a **superposition**, i.e. a linear combination of vectors  $|0\rangle$  and  $|1\rangle$  with **complex** coefficients:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

When state  $|\phi\rangle$  is **measured** (i.e. **observed**) one of the two basic states  $|0\rangle, |1\rangle$  is returned with probability

$$\|\alpha\|^2 \quad \text{and} \quad \|\beta\|^2$$

respectively.

Being probabilities, the norm squared of coefficients must satisfy

$$\|\alpha\|^2 + \|\beta\|^2 = 1$$

which enforces quantum states to be represented by **unit** vectors.

# The state space of a qubit

## Global phase

Unit vectors equivalent up to multiplication by a complex number of modulus one, i.e. a **phase factor**  $e^{i\theta}$ , represent the **same** state.

Let

$$|v\rangle = \alpha|u\rangle + \beta|u'\rangle$$

$$\|e^{i\theta}\alpha\|^2 = (\overline{e^{i\theta}\alpha})(e^{i\theta}\alpha) = (e^{-i\theta}\overline{\alpha})(e^{i\theta}\alpha) = \overline{\alpha}\alpha = \|\alpha\|^2$$

and similarly for  $\beta$ .

As the probabilities  $\|\alpha\|^2$  and  $\|\beta\|^2$  are the **only** measurable quantities, **global phase has no physical meaning**.

## Representation redundancy

qubit state space  $\neq$  complex vector space used for representation

# The state space of a qubit

## Relative phase

It is a measure of the angle between the two complex numbers.  
Thus, it cannot be discarded!

## Those are different states

$$\frac{1}{\sqrt{2}}(|u\rangle + |u'\rangle) \quad \frac{1}{\sqrt{2}}(|u\rangle - |u'\rangle) \quad \frac{1}{\sqrt{2}}(e^{i\theta}|u\rangle + |u'\rangle)$$

...



# The Bloch sphere

Deterministic, probabilistic and quantum bits

0

•

•

1

0

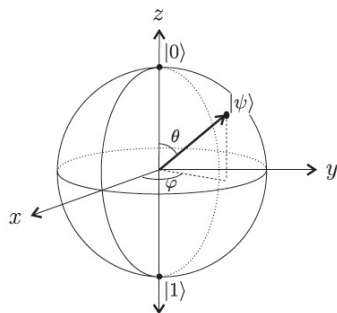
•

 $p_1$ 

×

 $p_0$ 

1



(from [Kaeys et al, 2007])

# The Bloch sphere: Representing $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- Express  $|\psi\rangle$  in **polar** form

$$|\psi\rangle = \rho_1 e^{i\varphi_1} |0\rangle + \rho_2 e^{i\varphi_2} |1\rangle$$

- Eliminate one of the four real parameters multiplying by  $e^{-i\varphi_1}$

$$|\psi\rangle = \rho_1 |0\rangle + \rho_2 e^{i(\varphi_2 - \varphi_1)} |1\rangle = \rho_1 |0\rangle + \rho_2 e^{i\varphi} |1\rangle$$

making  $\varphi = \varphi_2 - \varphi_1$ ,

which is possible because **global phase factors** are **physically meaningless**.

# The Bloch sphere: Representing $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- Switching back the coefficient of  $|1\rangle$  to Cartesian coordinates

$$|\psi\rangle = \rho_1|0\rangle + (a + bi)|1\rangle$$

the normalization constraint

$$\|\rho_1\|^2 + \|a+ib\|^2 = \|\rho_1\|^2 + (a-ib)(a+ib) = \boxed{\|\rho_1\|^2 + a^2 + b^2 = 1}$$

yields the [equation of a unit sphere](#) in the real tridimensional space with Cartesian coordinates:  $(a, b, \rho_1)$ .

# The Bloch sphere: Representing $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- The **polar** coordinates  $(\rho, \theta, \varphi)$  of a point in the surface of a sphere relate to Cartesian ones through the correspondence

$$x = \rho \sin \theta \cos \varphi$$

$$y = \rho \sin \theta \sin \varphi$$

$$z = \rho \cos \theta$$

- Recalling  $\rho = 1$  (cf unit vector),

$$\begin{aligned} |\psi\rangle &= \rho_1|0\rangle + (a + ib)|1\rangle \\ &= \cos \theta |0\rangle + \sin \theta (\cos \varphi + i \sin \varphi) |1\rangle \\ &= \cos \theta |0\rangle + e^{i\varphi} \sin \theta |1\rangle \end{aligned}$$

which, with **two parameters**, defines a **point** in the sphere's surface.

# The Bloch sphere

Actually, one may just focus on the **upper hemisphere** ( $0 \leq \theta' \leq \frac{\pi}{2}$ ) as opposite points in the lower one differ only by a phase factor of  $-1$ , as suggested by

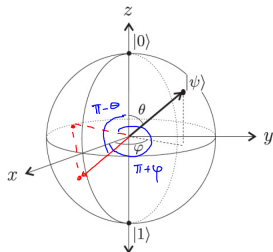
$$\theta' = 0 \Rightarrow |\psi\rangle = \cos 0|0\rangle + e^{i\varphi} \sin 0|1\rangle = |0\rangle$$

$$\theta' = \frac{\pi}{2} \Rightarrow |\psi\rangle = \cos \frac{\pi}{2}|0\rangle + e^{i\varphi} \sin \frac{\pi}{2}|1\rangle = e^{i\varphi}|1\rangle = |1\rangle$$

Note that **longitude** ( $\varphi$ ) is irrelevant in a pole!

# The Bloch sphere

Indeed, let  $|\psi'\rangle$  be the opposite point on the sphere with polar coordinates  $(1, \pi - \theta, \varphi + \pi)$ :



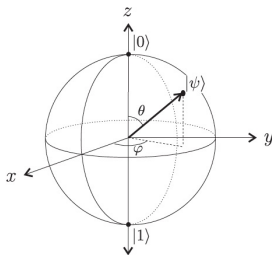
$$\begin{aligned}
 |\psi'\rangle &= \cos(\pi - \theta)|0\rangle + e^{i(\varphi + \pi)} \sin(\pi - \theta)|1\rangle \\
 &= -\cos\theta|0\rangle + e^{i\varphi} e^{i\pi} \sin\theta|1\rangle \\
 &= -\cos\theta|0\rangle + e^{i\varphi} \sin\theta|1\rangle \\
 &= -|\psi\rangle
 \end{aligned}$$

# The Bloch sphere

which leads to

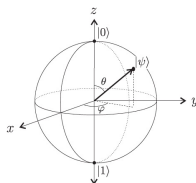
$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

where  $0 \leq \theta \leq \pi$ ,  $0 \leq \varphi \leq 2\pi$



The map  $\frac{\theta}{2} \mapsto \theta$  is **one-to-one** at any point but at  $\frac{\theta}{2}$ :  
all points on the equator are mapped into a single point: the south pole.

# The Bloch sphere



- The poles represent the classical bits. In general, **orthogonal states correspond to antipodal points** and every **diameter** to a **basis** for the single-qubit state space.
- Once measured a qubit collapses to one of the two poles. Which pole depends exactly on the arrow direction: The angle  $\theta$  measures that **probability**: If the arrow points at the equator, there is 50-50 chance to collapse to any of the two poles.
- Rotating a vector wrt the  $z$ -axis results into a **phase change** ( $\varphi$ ), and does not affect which state the arrow will collapse to, when measured.



# The state evolution postulate

If a quantum state is a **ray** (i.e. a unit vector in a Hilbert space  $H$  up to a global phase), its evolution is specified a certain kind of **linear** maps  $U : H \longrightarrow H$ .

## Linearity

$$U \left( \sum_j \alpha_j |v_j\rangle \right) = \sum_j \alpha_j U(|v_j\rangle)$$

just by itself has an important consequence: **quantum states cannot be cloned**

# The no-cloning theorem

Linearity implies that quantum states cannot be cloned

Let  $U(|a\rangle|0\rangle) = |a\rangle|a\rangle$  be a 2-qubit operator and  $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$  for  $|a\rangle, |b\rangle$  orthogonal. Then,

$$\begin{aligned}U(|c\rangle|0\rangle) &= \frac{1}{\sqrt{2}}(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)) \\&= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle) \\&\neq \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle) \\&= |c\rangle|c\rangle \\&= U(|c\rangle|0\rangle)\end{aligned}$$

As already seen,  $|x\rangle|y\rangle = |xy\rangle = |x\rangle \otimes |y\rangle$

## But, linearity is not enough ...

... we need to enforce that the norm squared of the new amplitudes still represent a probability distribution

$$\text{If } \sum_j \alpha_j U(|v_j\rangle) = \sum_j \alpha'_j |v_j\rangle \text{ then } \sum_j \|\alpha'_j\|^2 = 1$$

This is achieved by making  $U$  unitary, i.e. such that  $U^{-1} = U^\dagger$ .

# What is $U^\dagger$ ? The adjoint map

Given a linear map  $U : H \longrightarrow H'$ , its **adjoint**  $U^\dagger : H' \longrightarrow H$  is the **unique** linear map such that

$$\langle U^\dagger a | b \rangle = \langle a | U b \rangle$$

or, in the more 'verbose' notation for the inner product

$$(\langle U^\dagger a |, |b\rangle) = (|a\rangle, \langle U b |)$$

Note that  $(UV)^\dagger = V^\dagger U^\dagger$  and  $U^{\dagger\dagger} = U$  because

$$\langle V^\dagger U^\dagger a | b \rangle = \langle U^\dagger a | V b \rangle = \langle a | UV b \rangle$$

and

$$\langle U^{\dagger\dagger} a | b \rangle = \langle a | U^\dagger b \rangle$$

# The state evolution postulate

## Postulate 2

The evolution over time of the state of a closed quantum system is described by a unitary map.

The evolution is **linear**

$$U\left(\sum_j \alpha_j |v_j\rangle\right) = \sum_j \alpha_j U(|v_j\rangle)$$

and preserves the **normalization constraint**

$$\text{If } \sum_j \alpha_j U(|v_j\rangle) = \sum_j \alpha'_j |v_j\rangle \text{ then } \sum_j \|\alpha'_j\|^2 = 1$$

# The state evolution postulate

Preservation of the **normalization constraint** means that unit length vectors (and thus orthogonal subspaces) are mapped by  $U$  to unit length vectors (and thus to orthogonal subspaces).

It also means that applying a transformation followed by a measurement in the transformed basis is equivalent to a measurement followed by a transformation.

This entails a condition on valid quantum operators: they must **preserve** the inner product, i.e.

$$\langle Ua|Ub \rangle = \langle a|U^\dagger Ub \rangle = \langle v|w \rangle$$

which is only the case iff  $U$  is **unitary**, i.e.  $U^\dagger$  is the **inverse** of  $U$ :

$$U^\dagger U = UU^\dagger = I$$

# Unitary maps

- Preserving the inner product means that a unitary operator maps **orthonormal bases** to **orthonormal bases**.
- Conversely, any operator with this property is unitary.
- If given in matrix form, being unitary means that the set of columns of its matrix representation are orthonormal (because the  $j$ th column is the image of  $U|j\rangle$ ). Equivalently, rows are orthonormal (why?)

# Unitary maps

Unitarity is the **only** constraint on quantum operators: Any unitary matrix specifies a valid quantum operator.

This means that there are many non-trivial operators on a single qubit (in contrast with the **classical** case where the only non-trivial operation on a bit is **complement**).

Finally, because the **inverse** of a unitary matrix is also a unitary matrix, a quantum operator can always be inverted by another quantum operator

Unitary transformations are **reversible**



## Representing linear maps

A linear map  $U : H \longrightarrow H'$  is fully characterized by specifying how it acts on a basis of  $H$ . If  $H$  is **finite** this leads to a natural representation of  $U$  as **matrix**.

Let  $\{|j\rangle \mid j \in n-1\}$  be a basis for a  $n$ -dimensional Hilbert space  $H$ , and similarly  $\{|i\rangle \mid i \in m-1\}$  for a  $m$ -dimensional  $H'$ . Then the  $m \times n$  matrix corresponding to  $U$  is defined as

$$[U|0\rangle \quad U|1\rangle \quad \dots \quad U|n-1\rangle]$$

i.e. its  $j^{\text{th}}$ -column corresponds to  $m$ -dimensional vector  $U|j\rangle$ .

The Dirac notations provides a handy, alternative description of matrices via **outer products**.

# Representing linear maps

## Outer product

... is computed straightforwardly by matrix multiplication, e.g.

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

In general, for vectors  $|i\rangle, |j\rangle$  in an orthonormal basis,  $|i\rangle\langle j|$  is a square matrix with 1 in position  $(i, j)$  and 0 elsewhere. As an operator,  $|i\rangle\langle j|$  maps  $|j\rangle$  into  $|i\rangle$  because

$$|i\rangle\langle j|j\rangle = |i\rangle\langle j|j\rangle = |i\rangle$$

A linear map  $U : H \longrightarrow H'$  can be represented as a matrix

$$\sum_{i \in m-1, j \in n-1} U_{i,j} |i\rangle\langle j|$$

# Representing linear maps

## Decomposition of the identity (for an orthonormal basis)

$$I_H = \sum_{i \in n-1} |i\rangle\langle i|$$

Thus,

$$\begin{aligned} U &= I_H U I_H = \sum_{i \in m-1} |i\rangle\langle i| U \sum_{j \in n-1} |j\rangle\langle j| \\ &= \sum_{i \in m-1, j \in n-1} |i\rangle\langle i| U |j\rangle\langle j| \\ &= \sum_{i \in m-1, j \in n-1} \langle i|U|j\rangle |i\rangle\langle j| \end{aligned}$$

Clearly,

$$U_{i,j} = \langle i|U|j\rangle$$

# Representing linear maps

because

$$\begin{aligned}\langle i|U|j\rangle &= \langle i|\left(\sum_{i'\in m-1, j'\in n-1} U_{i',j'} |i'\rangle\langle j'|\right)|j\rangle \\ &= \sum_{i'\in m-1, j'\in n-1} U_{i',j'} \langle i|i'\rangle\langle j|j'\rangle \\ &= \sum_{i'\in m-1, j'\in n-1} U_{i',j'} \delta_{ii'}\delta_{jj'} = U_{i,j}\end{aligned}$$

# Representing linear maps

Any orthonormal provides a decomposition of the identity.

Is there a standard way to provide a decomposition for an arbitrary operator  $U$  over a Hilbert  $H$ ?

Yes, if  $U$  is **normal** operator, i.e.  $UU^\dagger = U^\dagger U$ , because of the

## Spectral theorem

Any normal operator on a finite,  $n$ -dimensional Hilbert space  $H$  provides a basis for  $H$  consisting of its **eigenvectors**. Thus,

$$U = \sum_{i \in n-1} \lambda_i |\lambda_i\rangle \langle \lambda_i|$$

where each  $(\lambda_i, |\lambda_i\rangle)$  is a eigenvalue / eigenvector pair.

# Typical quantum gates on 1 qubit

The  $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$  gate



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

As  $X|+\rangle = |+\rangle$  and  $X|-\rangle = -|-\rangle$ , its **spectral decomposition** yields

$$X = |+\rangle\langle +| - |-\rangle\langle -|$$

## Typical quantum gates on 1 qubit

The  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$  gate

Acts as

$$Z|0\rangle = |0\rangle \text{ and } Z|1\rangle = -|1\rangle$$

i.e. leaves  $|0\rangle$  invariant, but injects a phase  $e^{i\pi} = -1$  to  $|0\rangle$ , corresponding to a rotation of  $\pi$  radians around the  $Z$  axis.

Clearly, its spectral decomposition yields:

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

# Typical quantum gates on 1 qubit

## The phase shift gate

$$P_{\phi} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

i.e.  $P_{\phi} |0\rangle = |0\rangle$  and  $P_{\phi} |1\rangle = e^{i\phi} |1\rangle$ .

The probability of measuring a  $|0\rangle$  or  $|1\rangle$  remains unchanged, but it modifies the phase of the quantum state.

This corresponds to a rotation of  $\phi$  radians around the  $Z$  axis (i.e. along a line of latitude on the Bloch sphere) by  $\phi$  radians.



# Typical quantum gates on 1 qubit

## Examples

- $Z = P_\pi$
- $S = P_{\frac{\pi}{2}} = \sqrt{Z} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
- $T = P_{\frac{\pi}{4}} = \sqrt{S}$  ( also called the  $\frac{\pi}{8}$  gate)

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

which, up to a global phase factor  $e^{i\frac{\pi}{8}}$ , is equivalent to

$$\begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix}$$

# Typical quantum gates on 1 qubit

## Pauli gates

$X, Y, Z$  specify a rotation by  $\pi$  radians around the corresponding axes on the Bloch sphere.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$Y = i(-|1\rangle\langle 0| + |0\rangle\langle 1|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

# Typical quantum gates on 1 qubit

## Rotation gates

Correspond to arbitrary rotations around the three axes of the Bloch sphere

$$R_e(\theta) \hat{=} e^{\frac{-i\theta E}{2}} = \cos\left(\frac{\theta}{2}\right)I - i\sin\frac{\theta}{2}E$$

where  $e \hat{=} x, y, z$  and  $E \hat{=} X, Y, Z$ .

because, for any real number  $\theta$  and matrix  $R$  st  $R^2 = I$ , which is the case for  $X$ ,  $Y$ , and  $Z$ ,

$$e^{i\theta R} = \cos(\theta)I + i\sin(\theta)R$$

# Typical quantum gates on 1 qubit

Rotation gates as matrices in the computational basis

$$R_x(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i \sin\left(\frac{\theta}{2}\right) \\ -i \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$R_y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$R_z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$$

## Typical quantum gates on 1 qubit

Compute  $R_z(\theta)|\psi\rangle$  for  $|\psi\rangle = \cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i\gamma}\sin\left(\frac{\sigma}{2}\right)|1\rangle$

$$\begin{aligned}\begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix} &= \begin{bmatrix} e^{-i\frac{\theta}{2}} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\frac{\theta}{2}} e^{i\gamma} \sin\left(\frac{\sigma}{2}\right) \end{bmatrix} \\ &= e^{-i\frac{\theta}{2}} \begin{bmatrix} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\theta} e^{i\gamma} \sin\left(\frac{\sigma}{2}\right) \end{bmatrix} \\ &= e^{-i\frac{\theta}{2}} \left( \cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i(\gamma+\theta)} \sin\left(\frac{\sigma}{2}\right)|1\rangle \right)\end{aligned}$$

As global phase is insignificant, the angle mapping  $\gamma \mapsto \gamma + \theta$  is a rotation of  $\theta$  around the z-axis of the Bloch sphere.

# Typical quantum gates on 1 qubit

## Theorem

Let  $U$  be a 1-gate, and  $v, w$  any two non-parallel axes of the Bloch sphere. Then there exist real numbers  $\alpha, \beta, \gamma, \delta$  st

$$U = e^{i\alpha} R_v(\beta) R_w(\gamma) R_v(\delta)$$

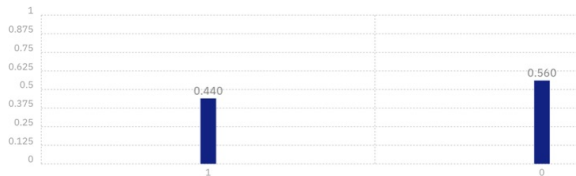
which means that any 1-gate can be expressed as a sequence of **two rotations about an axis** and **one rotation about another non parallel axis**, multiplied by a suitable **phase factor**.

proof hint: Recall  $U$  is unitary and unfold the definition of rotation gate.

# Typical quantum gates on 1 qubit

The Hadamard gate creates superpositions

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



$$\begin{aligned} H|0\rangle &= |+\rangle = \overbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}^{\text{superposition}} \\ H|1\rangle &= |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

# Building larger states from smaller

Operator  $U$  in the no-cloning theorem acts on a 2-dimensional state, i.e. over the composition of two qubits.

What does composition mean?

## Postulate 3

The state space of a combined quantum system is the tensor product  $V \otimes W$  of the state spaces  $V$  and  $W$  of its components.



# Composing quantum states

State spaces in a **quantum** system combine through **tensor**:  $\otimes$

$n$   $m$ -dimensional vectors  $\rightsquigarrow$  a vector in  $m^n$ -dimensional space

i.e. the state space of a quantum system grows exponentially with the number of particles: cf, Feynman's original motivation

## Example

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} \otimes \begin{bmatrix} d \\ e \\ f \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} \begin{bmatrix} d \\ e \\ f \end{bmatrix} = \begin{bmatrix} ad \\ ae \\ af \\ bd \\ be \\ bf \\ cd \\ ce \\ cf \end{bmatrix}$$

# Composing quantum states

## Tensor $V \otimes W$

- $B_{V \otimes W}$  is a set of elements of the form  $|v_i\rangle \otimes |w_j\rangle$ , for each  $|v_i\rangle \in B_V$ ,  $|w_j\rangle \in B_W$  and  $\dim(V \otimes W) = \dim(V) \times \dim(W)$
- $(|u_1\rangle + |u_2\rangle) \otimes |z\rangle = |u_1\rangle \otimes |z\rangle + |u_2\rangle \otimes |z\rangle$
- $|z\rangle \otimes (|u_1\rangle + |u_2\rangle) = |z\rangle \otimes |u_1\rangle + |z\rangle \otimes |u_2\rangle$
- $(\alpha|u\rangle) \otimes |z\rangle = |u\rangle \otimes (\alpha|z\rangle) = \alpha(|u\rangle \otimes |z\rangle)$
- $\langle (|u_2\rangle \otimes |z_2\rangle) | (|u_1\rangle \otimes |z_1\rangle) \rangle = \langle u_2 | u_1 \rangle \langle z_2 | z_1 \rangle$

## Composing quantum states

Clearly, every element of  $V \otimes W$  can be written as

$$\alpha_1(|v_1\rangle \otimes |w_1\rangle) + \alpha_2(|v_2\rangle \otimes |w_1\rangle) + \cdots + \alpha_{nm}(|v_n\rangle \otimes |w_m\rangle)$$

### Example

The basis of  $V \otimes W$ , for  $V, W$  qubits with the computational basis is

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$$

Thus, the tensor of  $\alpha_1|0\rangle + \alpha_2|1\rangle$  and  $\beta_1|0\rangle + \beta_2|1\rangle$  is

$$\alpha_1\beta_1|0\rangle \otimes |0\rangle + \alpha_1\beta_2|0\rangle \otimes |1\rangle + \alpha_2\beta_1|1\rangle \otimes |0\rangle + \alpha_2\beta_2|1\rangle \otimes |1\rangle$$

i.e., in a simplified notation,

$$\alpha_1\beta_1|00\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle + \alpha_2\beta_2|11\rangle$$

# Bases

The computational basis for a vector space

$$\underbrace{V \otimes V \otimes \dots \otimes V}_n$$

corresponding to the composition of  $n$  qubits (each living in  $V$ ) is the set

$$\begin{aligned} & \{ \underbrace{|0\rangle \dots |0\rangle}_n |0\rangle, \underbrace{|0\rangle \dots |0\rangle}_n |1\rangle, \underbrace{|0\rangle \dots |1\rangle}_n |0\rangle, \dots, \underbrace{|1\rangle \dots |1\rangle}_n |1\rangle \} \\ \stackrel{\text{abv}}{=} & \{ \underbrace{|0 \dots 00\rangle}_n, \underbrace{|0 \dots 01\rangle}_n, \underbrace{|0 \dots 10\rangle}_n, \dots, \underbrace{|1 \dots 11\rangle}_n \} \end{aligned}$$

which may be written in a compressed (decimal) way as

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, \dots, |2^n - 1\rangle\}$$

# Bases

The **computational basis** for a two qubit system would be

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$$

with

$$|0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |1\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |2\rangle = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |3\rangle = |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

# Bases

There are of course other bases ... besides the **standard** one, e.g.

## The Bell basis

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Compare with the Hadamard basis for the single qubit systems

# Representing multi-qubit states

Any unit vector in a  $2^n$  Hilbert space represents a possible  $n$ -qubit state, but for

... a certain level of redundancy

- As before, vectors that differ only in a **global phase** represent the **same** quantum state
- but also the **same phase factor in different qubits** of a tensor product represent the **same** state:

$$|u\rangle \otimes (e^{i\phi}|z\rangle) = e^{i\phi}(|u\rangle \otimes |z\rangle) = (e^{i\phi}|u\rangle) \otimes |z\rangle$$

Actually, phase factors in qubits of a single term of a superposition can always be factored out into a coefficient for that term, i.e. **phase factors distribute over tensors**

# Representing multi-qubit states

## Representation

- Relative phases still matter (of course!)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ differs from } \frac{1}{\sqrt{2}}(e^{i\phi}|00\rangle + |11\rangle)$$

even if

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(e^{i\phi}|00\rangle + e^{i\phi}|11\rangle) = \frac{e^{i\phi}}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- The complex **projective space** of dimension 1 (depicted in the **Block sphere**) generalises to higher dimensions, although in practice linearity makes Hilbert spaces easier to use.



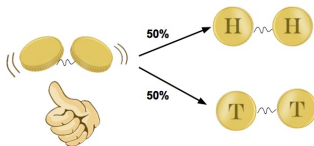
# Entanglement

Most states in  $V \otimes W$  cannot be written as  $|u\rangle \otimes |z\rangle$

For example, the **Bell state**

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

is **entangled**



# Entanglement

Actually, to make  $|\Phi^+\rangle$  equal to

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

would require that  $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$  which implies that either

$$\alpha_1\alpha_2 = 0 \text{ or } \beta_1\beta_2 = 0$$

## Note

Entanglement can also be observed in simpler structures, e.g. **relations**:

$$\{(a, a), (b, b)\} \subseteq A \times A$$

cannot be **separated**, i.e. written as a Cartesian product of subsets of  $A$ .

## 2-gates: *CNOT*

Acts on the standard basis for a 2-qubit system, flipping the second bit if the first bit is 1 and leaving it unchanged otherwise.

$$\begin{aligned}CNOT &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\&= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\&= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\end{aligned}$$

*CNOT* is unitary and is its own inverse, and **cannot be decomposed into a tensor product of two 1-qubit transformations**

## 2-gates: *CNOT*

The importance of *CNOT* is its ability to **change the entanglement** between two qubits, e.g.

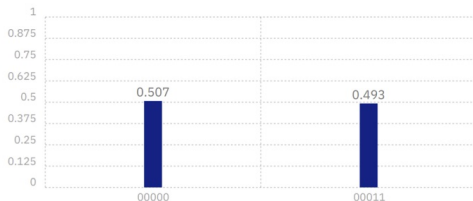
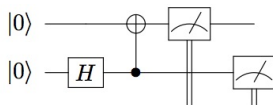
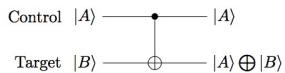
$$\begin{aligned} \text{CNOT} \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \right) &= \text{CNOT} \left( \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \right) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned}$$

Being its own inverse, also takes an entangled state to an unentangled one.

Note that **entanglement** is not a local property in the sense that transformations that act separately on two or more subsystems cannot affect the entanglement between those subsystems:

$$(U \otimes V) |v\rangle \text{ is entangled iff } |v\rangle \text{ is}$$

## 2-gates: *CNOT*

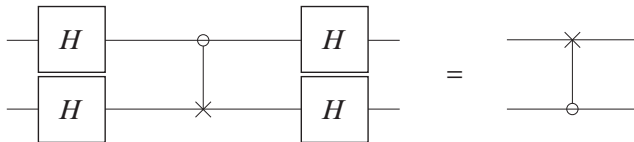


## 2-gates: *CNOT*

The notions of control/target bit in *CNOT* are **arbitrary**: they depend on what basis is considered. The standard behaviour is obtained in the computational basis. However, roles are interchanged in the Hadamard basis in which the effect of *CNOT* is

$$|++\rangle \mapsto |++\rangle \quad |+-\rangle \mapsto |--\rangle \quad |-+\rangle \mapsto |-+\rangle \quad |--\rangle \mapsto |+-\rangle$$

### Exercise



# The proof

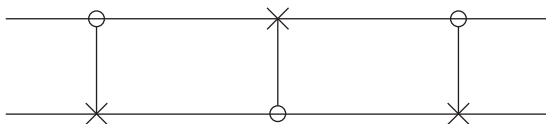
$$\begin{aligned}
 \text{LHS} &= \frac{1}{2} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{\text{CNOT}} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
 &= \frac{1}{2} \begin{bmatrix} H & HX \\ H & -HX \end{bmatrix} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
 &= \frac{1}{2} \begin{bmatrix} I + HXH & I - HXH \\ I - HXH & I + HXH \end{bmatrix} = \frac{1}{2} \begin{bmatrix} I + Z & I - Z \\ I - Z & I + Z \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \\
 &= I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| = \text{RHS}
 \end{aligned}$$

noting that

$$H \otimes H = (I \otimes H)(H \otimes I) = \frac{1}{\sqrt{2}} \begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

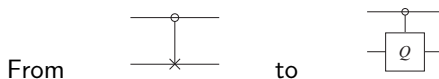
# Exercise

Discuss





# Controlled Q-gates



$$C_Q|0\rangle|\varphi\rangle = |0\rangle|\varphi\rangle$$

$$C_Q|1\rangle|\varphi\rangle = |1\rangle Q|\varphi\rangle$$

$$C_Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q$$

corresponding to the following matrix in the standard basis:

$$C_Q = \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}$$

## Controlled phase shift gate

$$C_{e^{i\theta}} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta}|10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$$

$$C_{e^{i\theta}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$$

### Transforming a global into a local phase

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$$

Actually, a unitary transformation is completely determined by its action on a basis, but **not** by specifying what states the states corresponding to basis states are sent to.

**Example:**  $e^{i\theta}$  takes the four quantum states to themselves (because e.g.  $|10\rangle$  and  $e^{i\theta}|10\rangle$  represent the same state), but a global phase can be transformed into a local one, as above

## *CCNOT* or Toffoli gate

A 3-bit gate corresponding to **controlled *CNOT***. If the first two bits are in the state  $|1\rangle$  applies  $X$  the third bit, else it does nothing:

$$|q_1 q_2 q_3\rangle \mapsto |q_1 q_2, q_3 \oplus (q_1 \wedge q_2)\rangle$$

In matrix form,

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

# Universal set of gates?

## Is there a universal set of quantum gates?

In general **no**: there are uncountably many quantum transformations, and a finite set of generators can only generate countably many elements. However, it is possible for **finite sets of gates** to generate **arbitrarily close approximations to all unitary transformations**.

## Definitions

- The **error** in approximating  $U$  by  $V$  is

$$Er(U, V) = \max_{|\phi\rangle} \|(U - V)|\phi\rangle\|$$

- An operator  $U$  can be **approximated to arbitrary accuracy** if for any positive  $\epsilon$  there exists another unitary transformation  $V$  st  $Er(U, V) \leq \epsilon$ .
- A set of gates is **universal** if for any integer  $n \geq 1$ , any  $n$ -qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set.

# Universal set of gates?

## Some examples

- The set  $\{H, T\}$  is universal for 1-gates.
- The set  $\{H, T, CNOT\}$  is a universal set of gates.

## How efficient is an approximation?

To approximate an unitary transformation encoding some specific computation, one would expect to use a number of gates from the universal set which is **polynomial** in the number of qubits and the inverse of the quality factor  $\epsilon$ .

Main result: theorem of **Solovay-Kitaev**