

# The Fifth Canadian Summer School on Quantum Information

## Introduction

# Overview

- Hilbert space
- The quantum model: states, measurements and transformations
- Simple algorithms
- Reversible circuits and quantum circuits

# The complex ring (\*)

A complex number has the form  $x = a + bi$  where  $a := \operatorname{Re}(x)$  and  $b := \operatorname{Im}(x)$  are real and  $i = \sqrt{-1}$ .

$$(a_1 + b_1i) + (a_2 + b_2i) = (a_1 + a_2) + (b_1 + b_2)i$$

$$(a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i$$

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

$$(a + bi)^* = (a - bi)$$

$$|a + bi| = \sqrt{(a + bi)(a - bi)} = \sqrt{a^2 + b^2}$$

$$e^{\theta i} = \cos \theta + i \sin \theta$$

$$|x| = 1 \Rightarrow x = e^{i\theta} \qquad e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$$

# Hilbert space

A Hilbert space  $\mathcal{H}$  is a complex vector space. We will only be interested in finite dimensional Hilbert spaces.

We denote a vector  $\psi$  living in an Hilbert space by  $|\psi\rangle$ .

**Definition:**  $\dagger$  is the conjugate transpose operation and it can be applied to a vector or a matrix.

We define  $\langle\psi| = |\psi\rangle^\dagger$ .

# Dagger

$$|\psi\rangle = \begin{pmatrix} 1 \\ i \\ 1+i \\ 1-i \end{pmatrix} \Rightarrow |\psi\rangle^\dagger = \langle\psi| = (1, -i, 1-i, 1+i)$$

$$\begin{pmatrix} 1 & 1+i \\ 2-i & 2 \end{pmatrix}^\dagger = \begin{pmatrix} 1 & 2+i \\ 1-i & 2 \end{pmatrix}$$

# Dagger

$$a^\dagger = a^*$$

$$A^{\dagger\dagger} = A$$

$$(A + B)^\dagger = A^\dagger + B^\dagger$$

$$(AB)^\dagger = B^\dagger A^\dagger$$

# Scalar product

**Definition:** We denote the scalar product on a Hilbert space  $\mathcal{H}$  by  $\langle \psi | \phi \rangle$ .

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \quad |\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$$

$$\langle \psi | \phi \rangle = (a^*, b^*) \begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d$$

**Definition:** We say that  $|x\rangle$  and  $|y\rangle$  are orthogonal if and only if  $\langle x | y \rangle = 0$ .

# Scalar product

**Lemma:** The scalar product has the following properties:

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

$$\langle \psi | \psi \rangle \geq 0,$$

$$\langle \psi | \psi \rangle = 0 \Leftrightarrow |\psi\rangle = 0$$

and

$$\langle \psi | (a |\phi_1\rangle + b |\phi_2\rangle) \rangle = a \langle \psi | \phi_1 \rangle + b \langle \psi | \phi_2 \rangle.$$

# Norm (\*)

**Definition:**  $\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle}$ .

**Lemma:** The norm has the following properties:

$$\| |\psi\rangle \| \geq 0,$$

$$\| |\psi\rangle \| = 0 \Leftrightarrow |\psi\rangle = 0,$$

$$\| a |\psi\rangle \| = |a| \| |\psi\rangle \|,$$

$$\| |\psi\rangle + |\phi\rangle \| \leq \| |\psi\rangle \| + \| |\phi\rangle \|,$$

$$| \langle \psi | \phi \rangle | \leq \| |\psi\rangle \| \| |\phi\rangle \|$$

and

$$\langle \psi | \phi \rangle \langle \phi | \psi \rangle \leq \langle \psi | \psi \rangle \langle \phi | \phi \rangle .$$

# Distance(\*)

**Definition:**  $dist(|\psi\rangle, |\phi\rangle) = \| |\psi\rangle - |\phi\rangle \|$ .

**Lemma:** the distance posses the following properties:

$$dist(|\psi\rangle, |\phi\rangle) = dist(|\phi\rangle, |\psi\rangle),$$

$$dist(|\psi\rangle, |\phi\rangle) \geq 0,$$

$$dist(|\psi\rangle, |\phi\rangle) = 0 \Leftrightarrow |\psi\rangle = |\phi\rangle$$

and

$$dist(|\psi\rangle, |\phi\rangle) \leq dist(|\psi\rangle, |\varphi\rangle) + dist(|\varphi\rangle, |\phi\rangle)$$

# Orthonormal basis

**Definition:** Let  $\mathcal{H}_d$  be an Hilbert space of dimension  $d$ . We say that a set of vectors  $\{|b_0\rangle, |b_1\rangle, \dots, |b_{d-1}\rangle\}$  form an orthonormal basis of  $\mathcal{H}_d$  if and only if

$$\forall i, \langle b_i | b_i \rangle = 1$$

and

$$\forall i, j, i \neq j, \langle b_i | b_j \rangle = 0.$$

# Orthonormal basis(\*)

**Lemma:** The following statements are equivalent.

1.  $\{|b_0\rangle, |b_1\rangle, \dots, |b_{d-1}\rangle\}$  form an orthonormal basis of  $\mathcal{H}_d$ .
2.  $|\phi\rangle = \sum_{i=0}^{d-1} \langle\phi|b_i\rangle |b_i\rangle$ .
3.  $\sum_{i=0}^{d-1} |b_i\rangle \langle b_i| = I_d$ .
4.  $\langle\psi|\psi\rangle = \sum_{i=0}^{d-1} |\langle b_i|\psi\rangle|^2$ .

# Computational basis

**Definition:** In Hilbert space  $\mathcal{H}_d$  of dimension  $d$ , the basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

is the computational basis.

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \dots + \alpha_{d-1} |d-1\rangle$$

$$\forall i, \langle i|i\rangle = 1 \quad \forall i \neq j, \langle i|j\rangle = 0$$

# Other example of basis

A basis for  $\mathcal{H}_4$ .

$$\begin{aligned}|e_1\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\|e_2\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\|e_3\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\|e_4\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle\end{aligned}$$

The four vectors are orthogonal and have norm one. They therefore form a basis of  $\mathcal{H}_4$ .

# Other example of basis (\*)

$|e_1\rangle$  has norm 1.

$$\begin{aligned}\| |e_1\rangle \| &= \sqrt{\langle e_1 | e_1 \rangle} \\ &= \sqrt{\left( \frac{1}{\sqrt{2}} \langle 00| + \frac{1}{\sqrt{2}} \langle 11| \right) \left( \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \right)} \\ &= \sqrt{\frac{1}{2} \langle 00|00\rangle + \frac{1}{2} \langle 00|11\rangle + \frac{1}{2} \langle 11|00\rangle + \frac{1}{2} \langle 11|11\rangle} \\ &= \sqrt{\frac{1}{2} (\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle)} \\ &= \sqrt{\frac{1}{2} (1 + 0 + 0 + 1)} \\ &= 1\end{aligned}$$

## Other example of basis (\*)

$|e_1\rangle$  and  $|e_2\rangle$  are orthogonal.

$$\begin{aligned}\langle e_2|e_1\rangle &= \left(\frac{1}{\sqrt{2}}\langle 01| + \frac{1}{\sqrt{2}}\langle 10|\right)\left(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) \\ &= \frac{1}{2}\langle 01|00\rangle + \frac{1}{2}\langle 01|11\rangle + \frac{1}{2}\langle 10|00\rangle + \frac{1}{2}\langle 10|11\rangle \\ &= \frac{1}{2}(0 + 0 + 0 + 0) \\ &= 0\end{aligned}$$

## Other example of basis (\*)

$|e_1\rangle$  and  $|e_3\rangle$  are orthogonal.

$$\begin{aligned}\langle e_1|e_3\rangle &= \left(\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|\right)\left(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) \\ &= \frac{1}{2}\langle 00|00\rangle - \frac{1}{2}\langle 00|11\rangle + \frac{1}{2}\langle 11|00\rangle - \frac{1}{2}\langle 11|11\rangle \\ &= \frac{1}{2}(1 - 0 + 0 - 1) \\ &= 0\end{aligned}$$

# Tensor product

**Definition:** Let

$$A = \begin{pmatrix} a_{0,0} & \cdots & a_{0,d-1} \\ \vdots & \ddots & \vdots \\ a_{d-1,0} & \cdots & a_{d-1,d-1} \end{pmatrix}$$

and

$$B = \begin{pmatrix} b_{0,0} & \cdots & b_{0,d'-1} \\ \vdots & \ddots & \vdots \\ b_{d'-1,0} & \cdots & b_{d'-1,d'-1} \end{pmatrix},$$

then

$$A \otimes B := \begin{pmatrix} a_{0,0}B & \cdots & a_{0,d-1}B \\ \vdots & \ddots & \vdots \\ a_{d-1,0}B & \cdots & a_{d-1,d-1}B \end{pmatrix}.$$

# Tensor product

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \quad B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix}$$

# Tensor Product

$$\mathcal{H}_d \otimes \mathcal{H}'_d := \mathcal{H}_{dd'}$$

$$|\psi\rangle |\phi\rangle := |\psi\rangle \otimes |\phi\rangle$$

$$|1\rangle |0\rangle |1\rangle = |101\rangle = |5\rangle$$

$$(A \otimes B)(|\psi\rangle |\phi\rangle) = (A|\psi\rangle)(B|\phi\rangle)$$

# Tensor product

$$|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle \quad |\Phi\rangle = b_0 |0\rangle + b_1 |1\rangle$$

$$|\Psi\rangle |\Phi\rangle = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$$

If

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B,$$

$$\{|a_i\rangle \mid i = 0 \dots d - 1\}$$

is an orthonormal basis for  $\mathcal{H}_A$  and

$$\{|b_i\rangle \mid i = 0 \dots d' - 1\}$$

is an orthonormal basis for  $\mathcal{H}_B$ , then

$$\{|a_i\rangle |b_j\rangle \mid i = 0 \dots d - 1, j = 0 \dots d' - 1\}$$

is an orthonormal basis for  $\mathcal{H}_{AB}$  having  $dd'$  vectors.

# States and measurements

Any pure quantum state can be represented by a norm 1 vector  $|\psi\rangle \in \mathcal{H}_d$  ( $\langle\psi|\psi\rangle = 1$ ).

In general,  $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$  with  $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$ .

For now, we will only talk of the simplest measurement. When we measure a quantum state  $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$  in the computational basis, we observe  $|i\rangle$  with probability  $|\alpha_i|^2$ . The state then collapses  $|i\rangle$ .

If there is an  $i$  such that  $|\alpha_i|^2 = 1$ , we will say that  $|\psi\rangle$  is in a basis state, otherwise we say that it is in superposition.

# Qubits

A **qubit** lives in  $\mathcal{H}_2$ , and has the form

$$\alpha|0\rangle + \beta|1\rangle,$$

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

A quantum register of  $n$  qubits

$$\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2 = \mathcal{H}_2^{\otimes n} = \mathcal{H}_{2^n}$$

is of the form

$$\sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

with  $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$ .

# Example

$$|\psi\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{6}}|01\rangle - \frac{1}{\sqrt{3}}|10\rangle + \frac{i}{\sqrt{6}}|11\rangle$$

If we measure  $|\psi\rangle$  we will observe

$|00\rangle$  with probability  $|\frac{1}{\sqrt{3}}|^2 = \frac{1}{3}$ ,

$|01\rangle$  with probability  $|\frac{1}{\sqrt{6}}|^2 = \frac{1}{6}$ ,

$|10\rangle$  with probability  $|\frac{-1}{\sqrt{3}}|^2 = \frac{1}{3}$  and

$|11\rangle$  with probability  $|\frac{i}{\sqrt{6}}|^2 = (\sqrt{\frac{i}{\sqrt{6}} \frac{-i}{\sqrt{6}}})^2 = \frac{1}{6}$ .

# Quantum operations

Any quantum operation is reversible, linear and preserves the norm. In fact a linear transformation is a valid quantum operation if and only if it is unitary.

An operator  $U$  is unitary if

$$U U^\dagger = I = U^\dagger U.$$

$U_1$  followed by  $U_2$  is equivalent to

$$U_3 = U_2 U_1.$$

If  $U_1$  acts on  $\mathcal{H}_A$  and  $U_2$  acts on  $\mathcal{H}_B$ , then

$$U_3 = U_1 \otimes U_2,$$

acts on  $\mathcal{H}_{AB}$ .

# Examples of unitary transformations

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$N |0\rangle \rightarrow |1\rangle$$

$$N |1\rangle \rightarrow |0\rangle$$

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$C |00\rangle \rightarrow |00\rangle$$

$$C |01\rangle \rightarrow |01\rangle$$

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

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

# Examples of unitary transformations

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

$$H |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

$$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$S_\theta |0\rangle \rightarrow |0\rangle$$

$$S_\theta |1\rangle \rightarrow e^{i\theta} |1\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z |0\rangle \rightarrow |0\rangle$$

$$Z |1\rangle \rightarrow -|1\rangle$$

# Examples of unitary transformations

$$N' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad \begin{aligned} N' |0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ N' |1\rangle &= \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \end{aligned}$$

$$\begin{aligned} N'(N' |0\rangle) &= N' \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \\ &= \frac{1}{\sqrt{2}}(N' |0\rangle + N' |1\rangle) \\ &= \frac{1}{\sqrt{2}} \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \right) \\ &= \frac{1}{2}(|0\rangle + |1\rangle - |0\rangle + |1\rangle) \\ &= |1\rangle \end{aligned}$$

Could this be the square root of the negation?

# Examples of unitary transformations

$$N' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad \begin{aligned} N' |0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ N' |1\rangle &= \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \end{aligned}$$

$$\begin{aligned} N'(N' |1\rangle) &= N' \left( \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \right) \\ &= \frac{1}{\sqrt{2}}(-N' |0\rangle + N' |1\rangle) \\ &= \frac{1}{\sqrt{2}} \left( -\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \right) \\ &= \frac{1}{2}(-|0\rangle - |1\rangle - |0\rangle + |1\rangle) \\ &= -|0\rangle \end{aligned}$$

**Exercise:** Find  $U$  such that  $U^2 = N$ .

# Ket bra (\*)

For any vector  $|u\rangle$  and  $|v\rangle$  of dimension  $n$ ,  $|u\rangle\langle v|$  is a  $n$  by  $n$  matrix.

Example:

$$|u\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \quad |v\rangle = c|0\rangle + d|1\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$$

$$|u\rangle\langle v| = \begin{pmatrix} a \\ b \end{pmatrix} (c^*, d^*) = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix}$$

$$\begin{aligned} |u\rangle\langle v| &= (a|0\rangle + b|1\rangle)(c^*\langle 0| + d^*\langle 1|) \\ &= ac^*|0\rangle\langle 0| + ad^*|0\rangle\langle 1| + bc^*|1\rangle\langle 0| + bd^*|1\rangle\langle 1| \end{aligned}$$

$$|u\rangle\langle v||x\rangle = \langle v|x\rangle|u\rangle$$

# Ket bra (\*)

An operator  $U$  is unitary if and only if

$$U = \sum_i |a_i\rangle \langle i|,$$

with  $\langle a_i | a_j \rangle = \delta_{ij}$  (an orthonormal basis).

**Proof:**  $\Rightarrow$

$$\begin{aligned} U^\dagger U &= \left( \sum_i |a_i\rangle \langle i| \right)^\dagger \left( \sum_j |a_j\rangle \langle j| \right) \\ &= \sum_{ij} |i\rangle \langle a_i| |a_j\rangle \langle j| \\ &= \sum_i |i\rangle \langle i| \\ &= I \end{aligned}$$

**Theorem:**

Unitary transformations preserve the inner product.

**Proof:**

If  $|u'\rangle = U|u\rangle$ ,  $|v'\rangle = U|v\rangle$ , then

$$\begin{aligned}\langle u'|v'\rangle &= |u'\rangle^\dagger |v'\rangle \\ &= (U|u\rangle)^\dagger (U|v\rangle) \\ &= \langle u|U^\dagger U|v\rangle \\ &= \langle u|v\rangle.\end{aligned}$$

**Note:**

If  $U|u\rangle = \lambda|u\rangle$ , then  $|\lambda| = 1$  and  $\lambda = e^{i\theta}$ .

**Theorem:**

Any unitary transformation  $U$  acting on  $\mathcal{H}_n$  can be written as

$$U = \sum_{i=1}^n \lambda_i |e_i\rangle \langle e_i|,$$

where

1. the  $|e_i\rangle$  form an orthonormal basis and are the eigenvectors of  $U$ ,
2. the  $|\lambda_i| = 1$  are the eigenvalues of  $U$ .

# Distinguishable states

For example:

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

are orthogonal:

$$\begin{aligned} \langle + | - \rangle &= \frac{1}{\sqrt{2}}(\langle 0 | + \langle 1 |) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(\langle 0 | 0 \rangle - \langle 0 | 1 \rangle + \langle 1 | 0 \rangle - \langle 1 | 1 \rangle) \\ &= \frac{1}{2}(1 - 0 + 0 - 1) = 0. \end{aligned}$$

Since

$$H |0\rangle = |+\rangle \quad H |1\rangle = |-\rangle,$$

then

$$H^\dagger |+\rangle = |0\rangle \quad H^\dagger |-\rangle = |1\rangle.$$

# Distinguishable states

**Theorem:**  $k$  states are perfectly distinguishable if and only if they are pairwise orthogonal.

**Proof:**  $\Leftarrow$

Let  $|e_1\rangle, \dots, |e_k\rangle$  be  $k$  orthogonal vectors living in  $\mathcal{H}_n$ . We can complete this set to an orthonormal basis of  $\mathcal{H}_n$  by adding  $n - k$  vectors  $|e_{k+1}\rangle, \dots, |e_n\rangle$ .

Let  $U = \sum_{i=1}^n |e_i\rangle \langle i|$ . Clearly  $U^\dagger |e_i\rangle = |i\rangle$  and the states are therefore perfectly distinguishable.

**Proof:**  $\Rightarrow$

If  $|e_1\rangle, \dots, |e_k\rangle$  are perfectly distinguishable then there exists  $U$  such that  $U |e_i\rangle = |i\rangle$ , where  $|i\rangle$  is in the computational basis. Since unitary transformations preserve the inner product and the  $|i\rangle$  are orthogonal, we conclude that the  $|e_i\rangle$  must also be orthogonal.

# Cloning is impossible

## Theorem:

There is no unitary transformation  $U$  such that

$$U |x\rangle |0\rangle = |x\rangle |x\rangle .$$

## Proof:

Suppose that such a  $U$  exist.

Let  $|u\rangle$  and  $|v\rangle$  be chosen such that  $\langle u|v\rangle = \frac{1}{2}$ .

We have  $U |u\rangle |0\rangle = |u\rangle |u\rangle$  and  $U |v\rangle |0\rangle = |v\rangle |v\rangle$ . Therefore:

$$(\langle u| \langle 0|)(|v\rangle |0\rangle) = (\langle u| \langle u|)(|v\rangle |v\rangle)$$

$$\langle u|v\rangle \langle 0|0\rangle = \langle u|v\rangle \langle u|v\rangle$$

$$\frac{1}{2} \cdot 1 = \frac{1}{2} \cdot \frac{1}{2}.$$

Contradiction!

# Simple algorithms

# Computing a function

To any function  $f : X \rightarrow Y$  we can associate a unitary transformation

$$F |x\rangle |y\rangle := |x\rangle |y \oplus f(x)\rangle .$$

Clearly  $F = F^\dagger$ ,  $FF = I$  and

$$F |x\rangle |0\rangle := |x\rangle |f(x)\rangle .$$

Also, if  $f$  is a binary function, we can define

$$F' |x\rangle := (-1)^{f(x)} |x\rangle .$$

Again  $F' = F'^\dagger$  and  $F'F' = I$ .

We will see later how we actually can implement these transformations using simple operations. For now just assume that the transformations exist.

# Computing a function

From  $F$ , we can compute  $F'$  by using an ancillary qubit in the state.

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

$$\begin{aligned} F |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |\overline{f(x)}\rangle) \\ &= |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= F' |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

# Deutsch algorithm

Deutsch problem (the version of R. Cleve and A. Tapp):  
Let  $f : \{0, 1\} \rightarrow \{0, 1\}$ , decide if  $f(0) = f(1)$ .

Algorithm Deutsch( $f$ )

- $|\psi\rangle = HF'H|0\rangle$
- $m = \text{Measure}(|\psi\rangle)$
- if  $m = 0$  answer CONSTANT else BALANCED

Classically: two evaluations of  $f$ .

Quantum mechanically: one evaluation of  $f$ .

# Recall

$$H |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

$$H = H^\dagger$$

# Deutsch algorithm Analysis

$$\begin{aligned} |\psi\rangle &= HF'H|0\rangle \\ &= HF'\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= H\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \\ &= H(-1)^{f(0)}\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)}(-1)^{f(1)}|1\rangle) \\ &= H(-1)^{f(0)}\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \\ &= (-1)^{f(0)}|f(0)\oplus f(1)\rangle \end{aligned}$$

We thus obtain  $f(0)\oplus f(1)$  with certainty.

# Grover algorithm (simple case)

Let  $f : \{0, 1\}^2 \rightarrow \{0, 1\}$  with the promise that there exists a unique  $x_0$  such that  $f(x_0) = 1$ . Otherwise  $f(x) = 0$ .

Let  $U$  be a unitary transformation define by:

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

# Grover algorithm (simple case)

Grover algorithm

- $|\psi\rangle = U^\dagger F' H^\otimes |00\rangle$
- $m = \text{Measure}(|\psi\rangle)$
- return  $m$

Any classical algorithm requires three evaluations of  $f$ .  
Quantum mechanically: one evaluation is sufficient.

# Grover algorithm (analysis)

$$\begin{aligned} |\psi\rangle &= U^\dagger F' H^{\otimes 2} |00\rangle \\ &= U^\dagger F' \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= U^\dagger \frac{1}{2}((-1)^{f(00)} |00\rangle + (-1)^{f(01)} |01\rangle \\ &\quad + (-1)^{f(10)} |10\rangle + (-1)^{f(11)} |11\rangle) \\ &= |x_0\rangle \end{aligned}$$

# Deutsch-Josza algorithm

Deutsch-Josza problem:

Given  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , decide if  $f$  is constant ( $\forall x, y, f(x) = f(y)$ ) or balanced ( $|f^{-1}(0)| = |f^{-1}(1)|$ ).

Deutsch-Josza algorithm( $f$ )

- $|\psi\rangle = H^{\otimes n} F' H^{\otimes n} |0\rangle$
- $m = \text{Measure}(|\psi\rangle)$
- if  $m = 0$  answer CONSTANT otherwise BALANCED

Deterministic classical algorithm:  $2^{n-1} + 1$  evaluations of  $f$ .

Quantum mechanically: one evaluation of  $f$ .

Unfortunately there exists a probabilistic algorithm that solve the problem with constant probability using a constant number of evaluations of  $f$ . Can you guess it?

# Hadamard transform (\*)

Lemma:

$$(H = H^\dagger) \quad H^{\otimes n} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |x\rangle,$$

where  $x \cdot y = x_1y_1 \oplus x_2y_2 \oplus \dots \oplus x_ny_n$  and in particular

$$H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

# Deutsch-Josza algorithm Analysis (\*)

$$\begin{aligned} |\psi\rangle &= H^{\otimes n} F' H^{\otimes n} |0\rangle \\ &= H^{\otimes n} F' \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \\ &= H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \left( \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} |j\rangle \right) \\ &= \sum_{j=0}^{2^n-1} \left( \sum_{i=0}^{2^n-1} \frac{(-1)^{f(i)+i \cdot j}}{2^n} \right) |j\rangle \end{aligned}$$

# Deutsch-Josza algorithm Analysis (\*)

The probability of observing  $|0\rangle$  is given by

$$\left| \sum_{i=0}^{2^n-1} \frac{(-1)^{f(i)+i \cdot 0}}{2^n} \right|^2 = \left| \sum_{i=0}^{2^n-1} \frac{(-1)^{f(i)}}{2^n} \right|^2.$$

If  $f$  is constant, then

$$\left| \sum_{i=0}^{2^n-1} \frac{(-1)^{f(i)}}{2^n} \right|^2 = \left| (-1)^{f(0)} \sum_{i=0}^{2^n-1} \frac{1}{2^n} \right|^2 = 1.$$

If  $f$  is balanced, then

$$\left| \sum_{i=0}^{2^n-1} \frac{(-1)^{f(i)}}{2^n} \right|^2 = \left| \frac{2^{n-1}}{2^n} - \frac{2^{n-1}}{2^n} \right|^2 = 0.$$

# Simon Algorithm

Given  $f : \{0, 1\}^n \rightarrow \{0, 1\}^{n-1}$  with the promise that there exists  $s$  (non zero) such that  $\forall x \neq y : f(x) = f(y) \Leftrightarrow x = y \oplus s$ , find  $s$ .

Simon(f)

- $S = \{\}$
- while  $|S| < n - 1$
- $|\psi\rangle = (H^{\otimes n} \otimes I_{2^{n-1}})F(H^{\otimes n} \otimes I_{2^{n-1}}) |0\rangle$
- $(m, y) = \text{Measure}(|\psi\rangle)$
- if  $m$  is independent of  $S$  then  $S \leftarrow S \cup \{m\}$
- end of while
- deduce  $s$  of  $S$ .

**Classically:**  $\Omega(2^{(1/2-\epsilon)n})$  evaluations of  $f$  are required. Even to have a constant success probability.

**Quantum mechanically:** An expected  $O(n)$  evaluations of  $f$  are sufficient.

# Simon algorithm: analysis (\*)

Let  $X$  be such that  $|X| = 2^{(n-1)}$  and  $X \cup (s \oplus X) = \{0, 1\}^n$ .

$$\begin{aligned}
 |\psi\rangle &= (H^{\otimes n} \otimes I_{2^n}) F (H^{\otimes n} \otimes I_{2^n}) |0\rangle |0\rangle \\
 &= (H^{\otimes n} \otimes I_{2^n}) F \left( \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |0\rangle \right) \\
 &= (H^{\otimes n} \otimes I_{2^n}) \left( \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |f(x)\rangle \right) \\
 &= \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left( \sum_{y \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} (-1)^{x \cdot y} |y\rangle \right) |f(x)\rangle \\
 &= \sum_{x,y \in \{0,1\}^n} \frac{(-1)^{x \cdot y}}{2^n} |y\rangle |f(x)\rangle \\
 &= \sum_{x \in X, y \in \{0,1\}^n} \frac{(-1)^{x \cdot y}}{2^n} |y\rangle |f(x)\rangle + \frac{(-1)^{(x \oplus s) \cdot y}}{2^n} |y\rangle |f(x \oplus s)\rangle \\
 &= \sum_{x \in X, y \in \{0,1\}^n} \frac{(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}}{2^n} |y\rangle |f(x)\rangle
 \end{aligned}$$

# Simon algorithm: analysis (\*)

$$|\psi\rangle = \sum_{x \in X, y \in \{0,1\}^n} \frac{(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}}{2^n} |y\rangle |f(x)\rangle$$

If  $s \cdot y = 0$ , then

$$x \cdot y = x \cdot y + s \cdot y = (x \oplus s) \cdot y.$$

Therefore the amplitude of  $|y\rangle |f(x)\rangle = 2^{-n+1}$ .

Otherwise if  $s \cdot y = 1$ , then

$$x \cdot y = x \cdot y + s \cdot y + 1 = (x \oplus s) \cdot y + 1.$$

Therefore the amplitude of  $|y\rangle |f(x)\rangle$  is 0.

# Simon algorithm: analysis (\*)

We thus obtain  $y$  uniformly distributed such that  $y \cdot s = 0$ .

By repeating, we will eventually obtain  $n$  such values and we will be able to compute  $s$ .

# Reversible circuits

# Calculation of functions

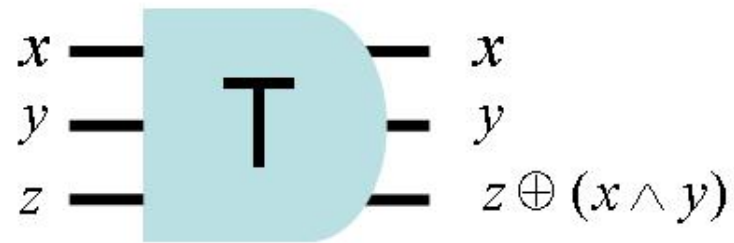
Any quantum transformation is unitary and therefore reversible. In this section we will see the basis of reversible computation.

# Classical circuits

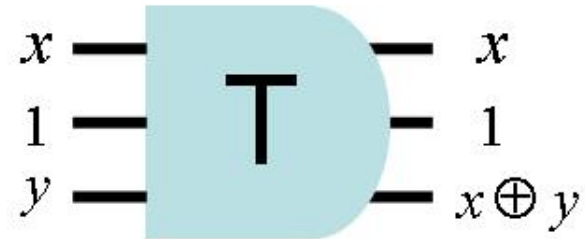
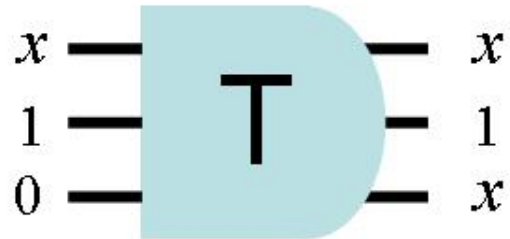
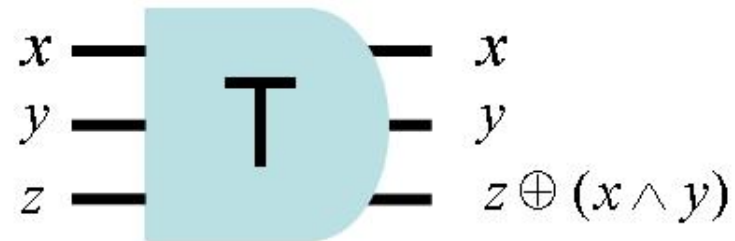
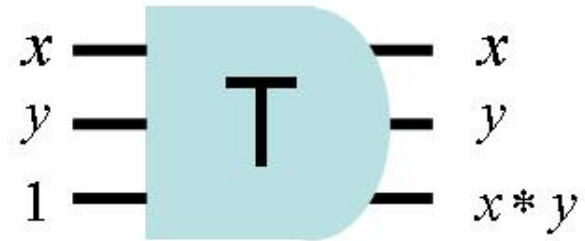
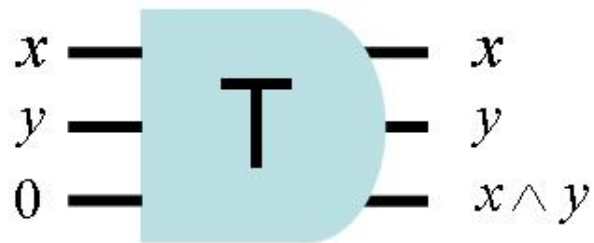
In a regular circuit we might see the following gates:



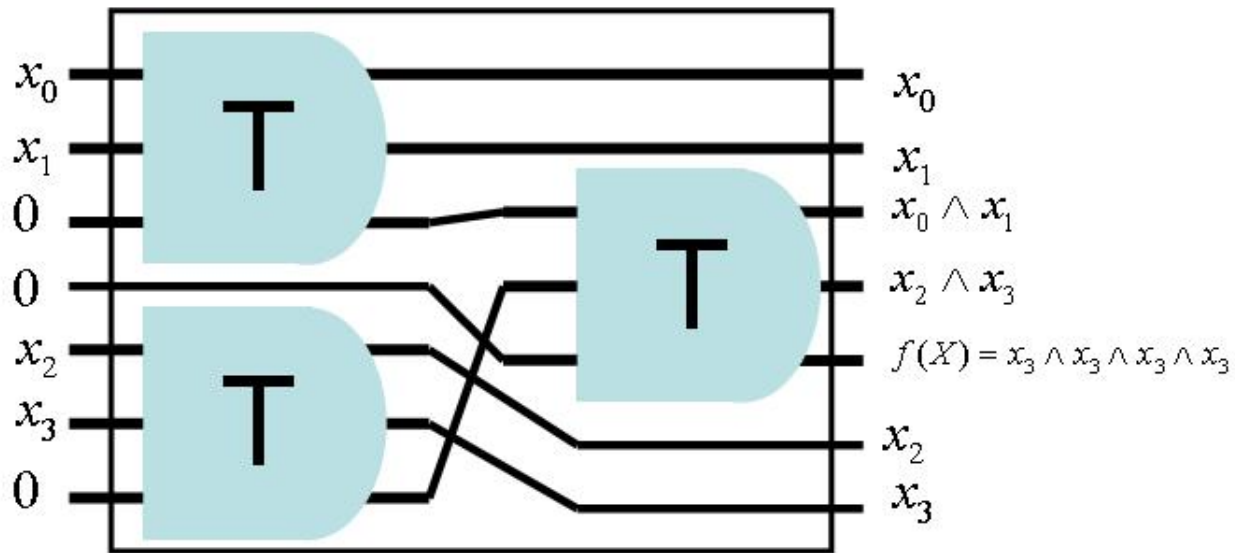
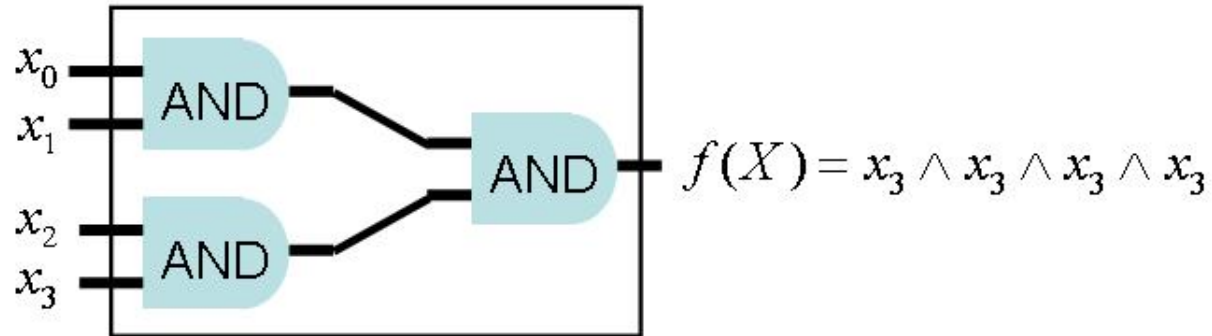
# Reversible circuits



# Simulating regular circuits



# Regular circuits versus reversible circuits



# Minimizing the width of a circuit

Using the literal translation of a regular circuit into a reversible circuits, the size and depth are preserved, but the width increases significantly.

There exists some techniques to construct a reversible circuit from a regular circuit that are more efficient in term of the width, but the price to pay is a small increase in depth.

**Theorem [LS90]** Let  $\mathcal{F}$  be a family of circuit of size  $t(n)$  and of width  $l(n)$ . For any  $\epsilon$ , there exists a family of reversible circuit of size  $\Omega(t(n)^{1+\epsilon})$  and width  $\Omega(l(n)(1 + \log(\frac{t(n)}{l(n)})))$ .

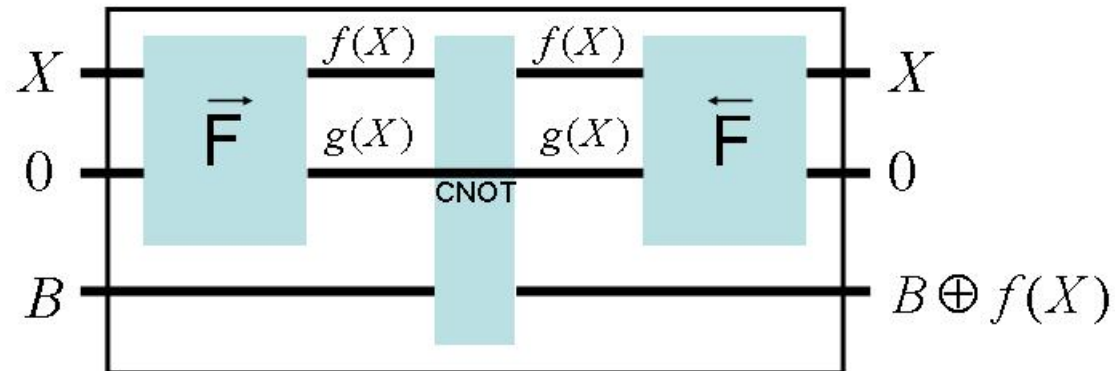
# Clean reversible circuits

The algorithms I have presented earlier required that the unitary transformations preserve the input and compute the function without garbage bits hanging around.

A reversible circuit with that property will be called clean.

**Theorem** If  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  is computable reversibly with a circuit of  $p$  gates of width  $w$ , then it is computable by a clean reversible circuit with  $2p + m$  gates and width  $w + m$ .

# Clean reversible circuits



# Quantum circuits

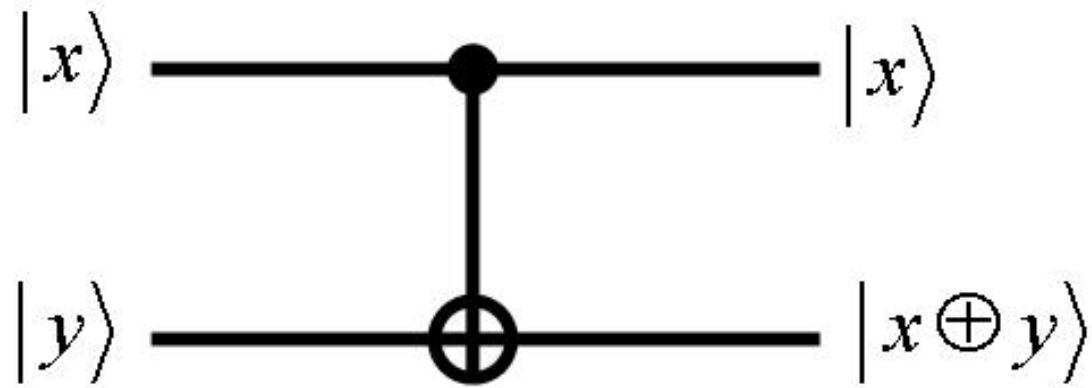
# Calculation of functions

Any algorithm must be decomposed into simple operations that can be implemented. We will see that if one can implement any operation acting on a single qubit and a special operation call the **controlled-not**, then one can implement any quantum transformation.

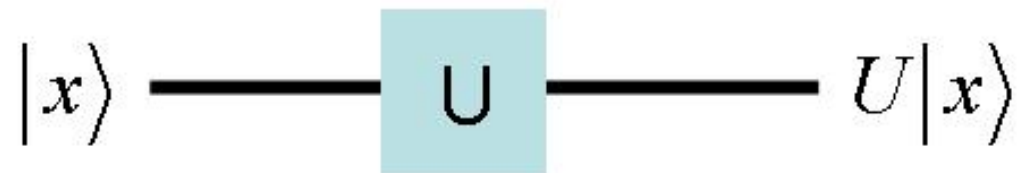
Furthermore, any efficient classical computation can also be implemented efficiently using those quantum operations.

# Our tools

C=CNOT



U, un qubit



# One-qubit gates

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

$$H |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

$$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$S_\theta |0\rangle \rightarrow |0\rangle$$

$$S_\theta |1\rangle \rightarrow e^{i\theta} |1\rangle$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$S |0\rangle \rightarrow |0\rangle$$

$$S |1\rangle \rightarrow i |1\rangle$$

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

$$T |0\rangle \rightarrow |0\rangle$$

$$T |1\rangle \rightarrow e^{i\pi/4} |1\rangle$$

# One-qubit gates

$$S_x S_y = S_{x+y}$$

$$S = S_{\pi/2}$$

$$T = S_{\pi/4}$$

$$T^2 = S$$

$$H = (X + Z)/\sqrt{2}$$

# The Pauli operators

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X |0\rangle \rightarrow |1\rangle$$

$$X |1\rangle \rightarrow |0\rangle$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Y |0\rangle \rightarrow i |1\rangle$$

$$Y |1\rangle \rightarrow -i |0\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z |0\rangle \rightarrow |0\rangle$$

$$Z |1\rangle \rightarrow -|1\rangle$$

# The Pauli operators

$$X = X^\dagger \quad Y = Y^\dagger \quad Z = Z^\dagger$$

$$X = iZY$$

$$Y = iXZ$$

$$Z = iYX$$

$$HXH = Z \quad HYH = -Y \quad HZH = X$$

# Rotations

$$R_x(\theta) = e^{-i\theta X/2} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X = \begin{pmatrix} \cos(\theta/2) & i \sin(\theta/2) \\ i \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_z(\theta) = e^{-i\theta Z/2} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

For  $x, y$  and  $z$ , we have  $R(a)R(b) = R(a + b)$ .

$$R_x(0) = R_y(0) = R_z(0) = I$$

$$X R_y(\theta) X = R_y(-\theta)$$

# Operator decomposition

**Theorem:** For all unitary operators  $U$  on  $\mathcal{H}_2$ , there exists  $\alpha, \beta, \delta$  and  $\gamma$  such that

$$U = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma).$$

**Proof:**

Any two dimensional unitary transformation can be written as

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)} \sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)} \sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)} \cos(\gamma/2). \end{pmatrix}$$

Therefore

$$U = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma).$$

# Operator decomposition

## Theorem:

For any  $U$  acting on  $\mathcal{H}_2$  there exists  $A_1, A_2$  et  $A_3$  and  $\alpha$  such that

$$A_1 A_2 A_3 = I \quad U = e^{i\alpha} A_1 X A_2 X A_3.$$

## Proof:

Let  $\alpha, \beta, \delta$  and  $\gamma$  be such that  $U = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma)$ . Then

$$\begin{aligned} A_1 &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) \\ A_2 &= R_y\left(\frac{-\gamma}{2}\right) R_z\left(\frac{-\delta - \beta}{2}\right) \\ A_3 &= R_z\left(\frac{\delta - \beta}{2}\right) \end{aligned}$$

will do the job.

# Operator decomposition (\*)

$$\begin{aligned}A_1 A_2 A_3 &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(\frac{-\gamma}{2}\right) R_z\left(\frac{-\delta - \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\&= R_z(\beta) R_y(0) R_z\left(\frac{-\delta - \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\&= R_z(\beta) R_z\left(\frac{-\delta - \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\&= R_z(0) \\&= I\end{aligned}$$

# Operator decomposition (\*)

Since  $XX = I$  and  $XR_y(a)X = R_y(-a)$ , we have

$$A_1 X A_2 X A_3$$

$$\begin{aligned} &= A_1 X R_y\left(\frac{-\gamma}{2}\right) R_z\left(\frac{-\delta - \beta}{2}\right) X A_3 \\ &= A_1 X R_y\left(\frac{-\gamma}{2}\right) X X R_z\left(\frac{-\delta - \beta}{2}\right) X A_3 \\ &= A_1 R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta + \beta}{2}\right) A_3 \\ &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta + \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\ &= R_z(\beta) R_y(\delta) R_z(\gamma). \end{aligned}$$

Therefore

$$e^{i\alpha} A_1 X A_2 X A_3 = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma) = U.$$

**QED**

# CNOT

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$C |00\rangle \rightarrow |00\rangle$$

$$C |01\rangle \rightarrow |01\rangle$$

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

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

$$C |a\rangle |b\rangle = |a\rangle |a \oplus b\rangle \quad C'_{[2,1]} |a\rangle |b\rangle = |a \oplus b\rangle |b\rangle$$

$$C = C^\dagger$$

$$\forall |\psi\rangle \in \mathcal{H}_2, C |0\rangle |\psi\rangle = |0\rangle |\psi\rangle$$

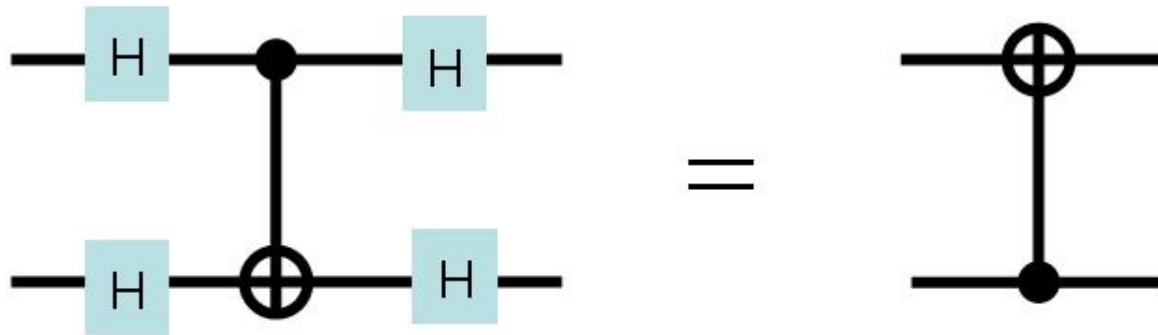
$$\forall |\psi\rangle \in \mathcal{H}_2, C |1\rangle |\psi\rangle = |1\rangle (X |\psi\rangle)$$

$$C |1\rangle (H |0\rangle) = |1\rangle (H |0\rangle)$$

$$C |1\rangle (H |1\rangle) = - |1\rangle (H |1\rangle)$$

# CNOT

$$C' = H^{\otimes 2}CH^{\otimes 2}$$



# CNOT (\*)

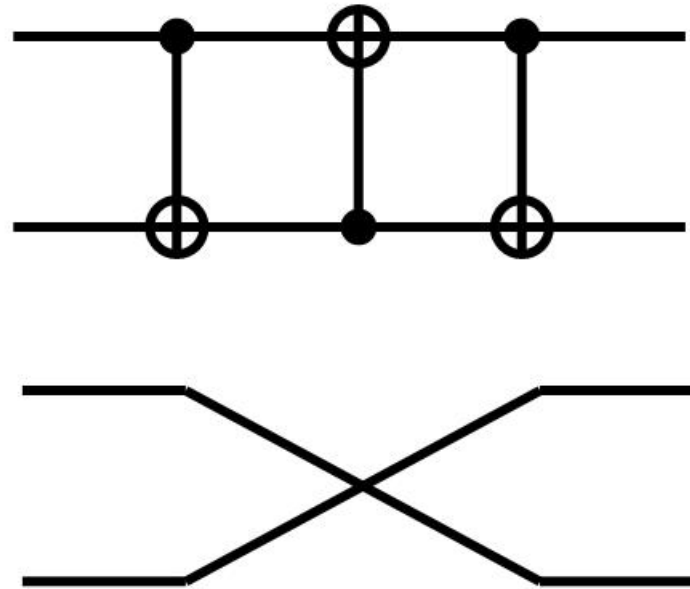
$$H |a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a |1\rangle)$$

$$H^{\otimes 2} C H^{\otimes 2} |a\rangle |b\rangle$$

$$\begin{aligned} &= H^{\otimes 2} C \frac{1}{2} (|0\rangle + (-1)^a |1\rangle) (|0\rangle + (-1)^b |1\rangle) \\ &= H^{\otimes 2} C \frac{1}{2} (|00\rangle + (-1)^b |01\rangle + (-1)^a |10\rangle + (-1)^{a+b} |11\rangle) \\ &= H^{\otimes 2} \frac{1}{2} (|00\rangle + (-1)^b |01\rangle + (-1)^a |11\rangle + (-1)^{a+b} |10\rangle) \\ &= H^{\otimes 2} \frac{1}{2} (|0\rangle + (-1)^{a+b} |1\rangle) (|0\rangle + (-1)^b |1\rangle) \\ &= |a \oplus b\rangle |b\rangle \\ &= C_{[2,1]} |a\rangle |b\rangle \end{aligned}$$

# SWAP

$$P_{12} = CC'C$$

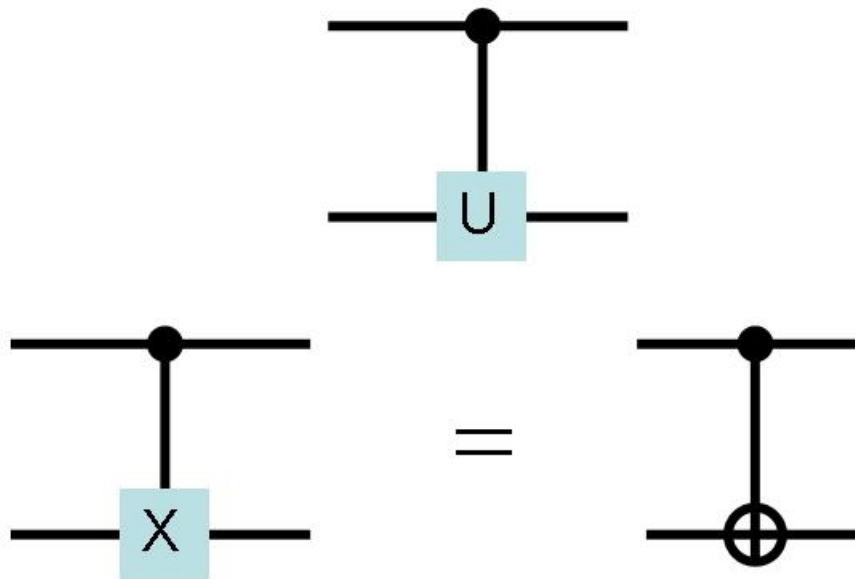


# SWAP (\*)

$$P_{12} |\psi\rangle |\phi\rangle$$

$$\begin{aligned} &= P_{12} (\alpha |0\rangle + \beta |1\rangle)(\delta |0\rangle + \gamma |1\rangle) \\ &= CC_{[2,1]} C (\alpha |0\rangle + \beta |1\rangle)(\delta |0\rangle + \gamma |1\rangle) \\ &= CC_{[2,1]} C (\alpha\delta |00\rangle + \alpha\gamma |01\rangle + \beta\delta |10\rangle + \beta\gamma |11\rangle) \\ &= CC_{[2,1]} (\alpha\delta |00\rangle + \alpha\gamma |01\rangle + \beta\delta |11\rangle + \beta\gamma |10\rangle) \\ &= C (\alpha\delta |00\rangle + \alpha\gamma |11\rangle + \beta\delta |01\rangle + \beta\gamma |10\rangle) \\ &= (\alpha\delta |00\rangle + \alpha\gamma |10\rangle + \beta\delta |01\rangle + \beta\gamma |11\rangle) \\ &= (\delta\alpha |00\rangle + \delta\beta |01\rangle + \gamma\alpha |10\rangle + \gamma\beta |11\rangle) \\ &= |\phi\rangle |\psi\rangle \end{aligned}$$

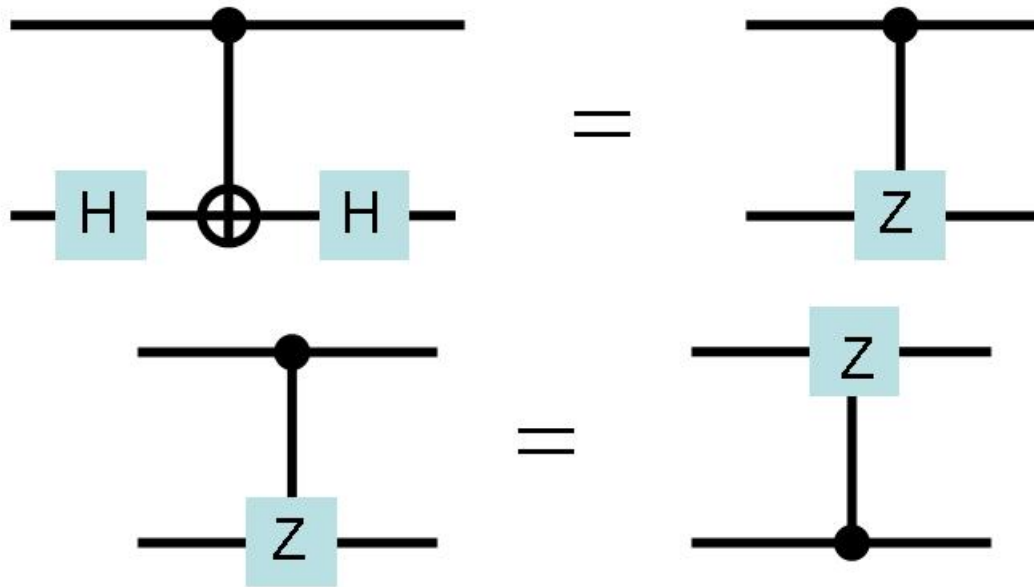
$C-U$



$$C-U |a\rangle |b\rangle = |a\rangle (U^a |b\rangle)$$

$$C-X = C$$

$C-Z$

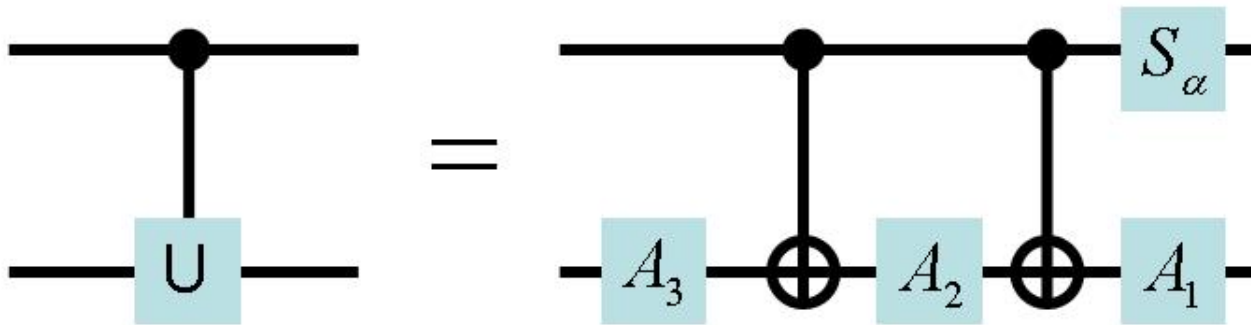


$$\begin{aligned}
 H_{[2]} C H_{[2]} |0\rangle |b\rangle &= H_{[2]} C |0\rangle (H |b\rangle) \\
 &= H_{[2]} |0\rangle (H |b\rangle) \\
 &= |0\rangle |b\rangle
 \end{aligned}$$

$$\begin{aligned}
 H_{[2]} C H_{[2]} |1\rangle |b\rangle &= H_{[2]} C |0\rangle (H |b\rangle) \\
 &= H_{[2]} |0\rangle (X H |b\rangle) \\
 &= |0\rangle (H X H |b\rangle) \\
 &= |0\rangle (Z |b\rangle)
 \end{aligned}$$

# $C-U$

If  $U = e^{i\alpha} A_1 X A_2 X A_3$  and  $A_1 A_2 A_3 = I$ , then

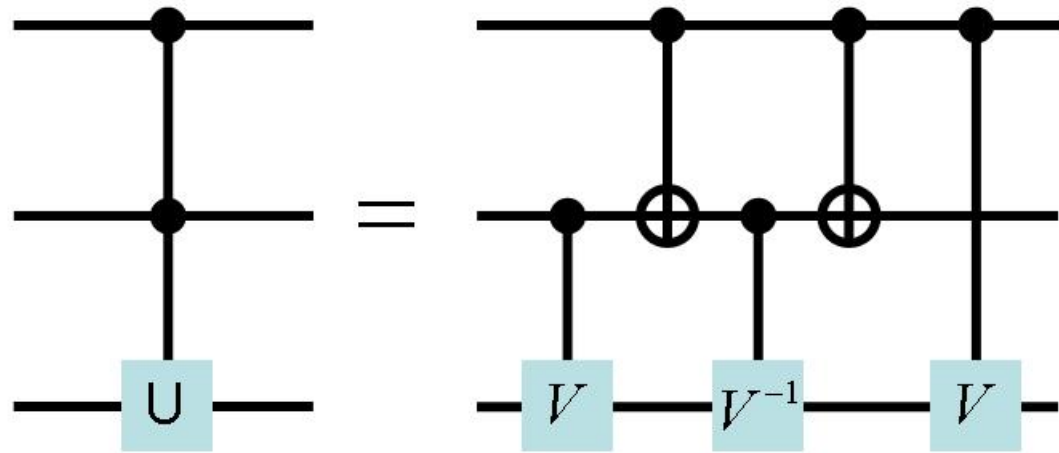


$$S_{\alpha[1]} A_{1[2]} C A_{2[2]} C A_{3[2]} |0\rangle |b\rangle = |0\rangle (A_1 A_2 A_3 |b\rangle) = |0\rangle |b\rangle$$

$$S_{\alpha[1]} A_{1[2]} C A_{2[2]} C A_{3[2]} |1\rangle |b\rangle = e^{i\alpha} |1\rangle (A_1 X A_2 X A_3 |b\rangle) = |1\rangle (U |b\rangle).$$

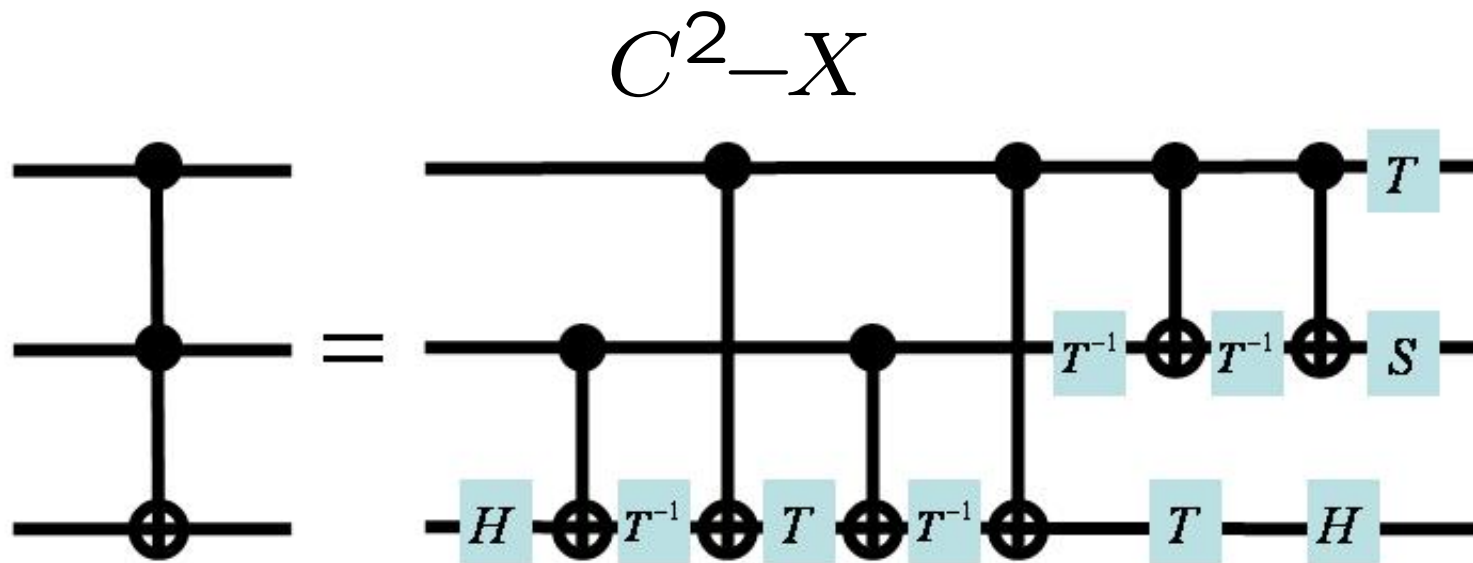
$$C^2-U$$

$$C^2-U |a\rangle |b\rangle |c\rangle = |a\rangle |b\rangle (U^{ab} |c\rangle) \quad V^2 = U$$



$$\begin{aligned}
 &|00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \\
 &|01\rangle |a\rangle \rightarrow |01\rangle (V |a\rangle) \rightarrow |01\rangle (V |a\rangle) \rightarrow |01\rangle |a\rangle \rightarrow |01\rangle |a\rangle \rightarrow |01\rangle |a\rangle \\
 &|10\rangle |a\rangle \rightarrow |10\rangle |a\rangle \rightarrow |11\rangle |a\rangle \rightarrow |11\rangle (V^\dagger |a\rangle) \rightarrow |10\rangle (V^\dagger |a\rangle) \rightarrow |10\rangle |a\rangle \\
 &|11\rangle |a\rangle \rightarrow |11\rangle (V |a\rangle) \rightarrow |10\rangle (V |a\rangle) \rightarrow |10\rangle (V |a\rangle) \rightarrow |11\rangle (V |a\rangle) \rightarrow |11\rangle (V^2 |a\rangle)
 \end{aligned}$$

Using this technique, the Toffoli gate can be implemented using 8 controlled-not and 12 one-qubit gates.



Using this circuit, one can implement the Toffoli gate ( $C^2-X$ ) using 6 controlled-not ( $C$ ) and 10 one-qubit gate.

# Classical computation

Any classical computation can be performed by a classical circuit.

Any classical circuit can be implemented using the Toffoli gate.

Any reversible circuit can be made clean.

Any clean reversible circuit using Toffoli gates can be implemented using controlled-not and one-qubit gates.

# Several identities (\*)

$$CX_{[1]}C = X_{[1]}X_{[2]}$$

$$CY_{[1]}C = Y_{[1]}X_{[2]}$$

$$CZ_{[1]}C = Z_{[1]}$$

$$CX_{[2]}C = X_{[2]}$$

$$CY_{[2]}C = Z_{[1]}Y_{[2]}$$

$$CZ_{[2]}C = Z_{[1]}Z_{[2]}$$

$$R_z[1]C = CR_z[1]$$

$$R_x[2]C = CR_x[1]$$