Aspetti Matematici Nella Computazione Quantistica

Remarks on Hilbert Spaces

Def A **DEFINITE POSITIVE SCALE PRODUCT** on a complex vector space $\mathbb{V}$ is a map $\langle , \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$ with the following properties:

- $\langle \varphi | \psi \rangle = \overline{\langle \psi | \varphi \rangle}$
- $\langle \varphi | \varphi \rangle \geq 0 \quad \forall \varphi \in \mathbb{V}$
- $\langle \varphi | \varphi \rangle = 0 \iff \varphi = 0$
- $\langle \varphi | a\psi_1 + b\psi_2 \rangle = a\langle \varphi | \psi_1 \rangle + b\langle \varphi | \psi_2 \rangle \quad \forall a,b \in \mathbb{C}$

$\forall \varphi, \psi_1, \psi_2 \in \mathbb{V}$

(a consequence is antilinearity on the first argument)

Obs A scale product on $\mathbb{V}$ defines a norm on $\mathbb{V}$ by

$$\|\psi\| := \sqrt{\langle \psi | \psi \rangle}$$

Def A **HILBERT SPACE** is a vector space $\mathbb{H}$ over $\mathbb{C}$ endoned with a definite positive scalar product such that $\mathbb{H}$ is complete with respect to the given norm

Rmk

(1) $\forall a \in \mathbb{C} \quad \forall \psi, \varphi \in \mathbb{H}, \quad \langle a\varphi | \psi \rangle = \bar{a} \langle \varphi | \psi \rangle$

$$\|a\varphi\| = |a| \cdot \|\varphi\|$$

(2) Let $\psi \in \mathbb{H}$, then $\langle \psi | \varphi \rangle = 0 \ \forall \varphi \in \mathbb{H} \iff \psi = 0$

Dim [$\Rightarrow$] $\langle \psi | \psi \rangle = 0 \Rightarrow \psi = 0$

[$\Leftarrow$] $\forall \varphi \in \mathbb{H} \quad \langle 0 | \varphi \rangle = 0$ because of linearity

(3) Complex parallelogram identity

$\forall \varphi, \psi \in \mathbb{H}$ it holds that

$$\langle \psi | \varphi \rangle = \frac{1}{4}\left(\|\psi+\varphi\|^2 - \|\psi-\varphi\|^2 + i\|\psi-i\varphi\|^2 - i\|\psi+i\varphi\|^2 \right)$$

Def
- A vector $\psi \in \mathbb{H}$ is UNITARY (NORMED) if $\|\psi\| = 1$
- $\varphi, \psi \in \mathbb{H}$ are ORTHOGONAL if $\langle \varphi | \psi \rangle = 0$
- Given $\psi \in \mathbb{H}$ the ORTHOGONAL SUBSPACE to ψ is

$$\mathbb{H}_{\psi^\perp} := \{ \varphi \in \mathbb{H} \mid \langle \varphi | \psi \rangle = 0 \}$$

Obs Let $\psi \in \mathbb{H}$, $\psi \neq 0$. For any $\varphi \in \mathbb{H}$, $\varphi - \frac{\langle \psi | \varphi \rangle}{\|\psi\|^2}\psi \in \mathbb{H}_{\psi^\perp}$

Def Let $\mathbb{H}$ be an Hilbert space and I an index set
- The vectors $\{\psi_i\}_{i \in I} \subseteq \mathbb{H}$ are LINEARLY INDEPENDENT if for every finite subset $\{i_1, \dots, i_n\} \subseteq I$ it holds that

$$a_1 \psi_{i_1} + \dots + a_n \psi_{i_n} = 0 \Rightarrow a_1 = \dots = a_n = 0$$

- $\mathbb{H}$ is FINITE-DIMENSIONAL if any set of linearly independant vector is finite
- An ORTHONORMAL BASIS (ONB) for $\mathbb{H}$ is a set of linearly independant vector $\{e_j\}_{j \in I} \subseteq \mathbb{H}$ such that $\langle e_i | e_j \rangle = \delta_{ij}$ and any $\psi \in \mathbb{H}$ can be written as

$$\psi = \sum_j a_j e_j \qquad a_j \in \mathbb{C}$$

Rmk in this equation the a_j's are uniquely defined and are equal to $a_j = \langle e_j | \psi \rangle$

We will only work with SEPARABLE Hilbert spaces (ie: basis have a countable number of elements)

Let $\psi, \varphi \in \mathbb{H}$, $\{e_j\}$ ONB, $\psi = \sum \psi_j e_j$ and $\varphi = \sum \varphi_j e_j$

then $\langle \varphi | \psi \rangle = \sum \overline{\varphi_j} \psi_j$ and $\|\psi\| = \sqrt{\sum |\psi_j|^2}$

If $\langle \varphi | \psi \rangle = 0$ then $\|\psi + \varphi\|^2 = \|\psi\|^2 + \|\varphi\|^2$ because

$$\|\psi + \varphi\|^2 = \langle \psi + \varphi \mid \psi + \varphi \rangle = \|\psi\|^2 + \|\varphi\|^2 + \underbrace{\langle \varphi | \psi \rangle}_{=0} + \underbrace{\langle \psi | \varphi \rangle}_{=0}$$

Th (REISZ REPRESENTATION THEOREM)

All linear continuous map $\mathbb{H} \to \mathbb{C}$ can be written as

$\langle \psi | \cdot \rangle : \mathbb{H} \to \mathbb{C}$ for some $\psi \in \mathbb{H}$

$\varphi \rightsquigarrow \langle \psi | \varphi \rangle$

Def The space of linear continuous maps from $\mathbb{H}$ to $\mathbb{C}$ is called the DUAL SPACE $\mathbb{H}^* = \{ g : \mathbb{H} \to \mathbb{C} \mid g \text{ lin. cont.} \}$ and is (because of the last theorem) in bijection with $\mathbb{H}$

Def (DIRAC NOTATION)

A KET vector is $|\psi\rangle \in \mathbb{H}$

A BRA vector is $\langle \psi | \in \mathbb{H}^*$

If $A : \mathbb{H} \to \mathbb{H}$ is a linear map then $|A\psi\rangle = A|\psi\rangle$

Given an ONB $\{|e_j\rangle\}$ on $\mathbb{H}$ we can write any $|\psi\rangle$ as

$$|\psi\rangle = \sum_j \langle e_j | \psi \rangle |e_j\rangle.$$

Applying A we get $A|\psi\rangle = \sum_j A|e_j\rangle \langle e_j | \psi \rangle$

$$|A\psi\rangle = \sum_j |e_j\rangle \langle e_j | A\psi \rangle =$$

$$= \sum_j |e_j\rangle \langle e_j | A \sum_k |e_k\rangle \langle e_k | \psi \rangle \rangle$$

Thus $A = \sum_{j,k} |e_j\rangle\langle e_j|A e_k\rangle\langle e_k|$ as the operator acting on ψ

Finite-dimensional case

$\mathbb{H} \cong \mathbb{C}^n$ ($\dim \mathbb{H} = n$) with an almost explicit representation

given $\{|e_j\rangle\}_{j=1}^n$ ONB we have $|e_j\rangle \rightsquigarrow \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ (j-th position)

$\mathbb{H}^* \cong (\mathbb{C}^n)^* \cong \mathbb{C}^n$ but $|e_j\rangle \rightsquigarrow (0 \dots 1 \dots 0)$

So given $|\psi\rangle \in \mathbb{H}$ because we can write $|\psi\rangle = \sum_{j=1}^n \psi_j |e_j\rangle$

we have $|\psi\rangle \rightsquigarrow \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix} \in \mathbb{C}^n$

Also given $\langle\psi| \in \mathbb{H}^*$ we can write $\langle\psi| = \sum_{j=1}^n \langle e_j|\overline{\psi_j}$

so we have $\langle\psi| \rightsquigarrow (\overline{\psi_1} \dots \overline{\psi_n})$

It holds $|\psi\rangle\langle\varphi| = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix} (\overline{\varphi_1} \dots \overline{\varphi_n}) = \begin{pmatrix} \psi_1\overline{\varphi_1} & \dots & \psi_1\overline{\varphi_n} \\ \vdots & & \vdots \\ \psi_n\overline{\varphi_1} & \dots & \psi_n\overline{\varphi_n} \end{pmatrix}$

30/09

Es $d = 2$

We have $\mathbb{H} \cong \mathbb{C}^2$. We usually call an ONB for $\mathbb{H}$ as $\{|0\rangle, |1\rangle\}$ and the isomorphism is given by $|0\rangle \to \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle \to \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Elements in $\mathbb{H}$ are $|\psi\rangle = a|0\rangle + b|1\rangle \in \mathbb{H}$

Then $|\psi\rangle \rightsquigarrow \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ and $\langle\psi| = \bar{a}\langle 0| + \bar{b}\langle 0| \rightsquigarrow (\bar{a}, \bar{b}) \in (\mathbb{C}^2)^*$

Given $|\psi\rangle, |\varphi\rangle \in \mathbb{H}$ we can construct the operator

$|\psi\rangle\langle\varphi| : \mathbb{H} \to \mathbb{H}$

With the ONB we get

$|0\rangle\langle 0| \rightsquigarrow \begin{pmatrix}1\\0\end{pmatrix}(1\ 0) = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ the projection on the first coordinate

$|1\rangle\langle 1| \rightsquigarrow \begin{pmatrix}0\\1\end{pmatrix}(0\ 1) = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$ the projection on the second coordinate

$|0\rangle\langle 1| \rightsquigarrow \begin{pmatrix}1\\0\end{pmatrix}(0\ 1) = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, $|1\rangle\langle 0| \rightsquigarrow \begin{pmatrix}0\\1\end{pmatrix}(1\ 0) = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$

By linearity, given $|\psi\rangle = a|0\rangle + b|1\rangle$, $|\varphi\rangle = c|0\rangle + d|1\rangle$

$$|\psi\rangle\langle\varphi| = a\bar{c}|0\rangle\langle 0| + a\bar{d}|0\rangle\langle 1| + b\bar{c}|1\rangle\langle 0| + b\bar{d}|1\rangle\langle 1|$$

$$\rightsquigarrow \begin{pmatrix}a\\b\end{pmatrix}(\bar{c}\ \bar{d}) = \begin{pmatrix}a\bar{c} & b\bar{c}\\ a\bar{d} & b\bar{d}\end{pmatrix}$$

Let $A: \mathbb{H} \to \mathbb{H}$ be a linear operator. We will assume that A is bounded (ie: $\|A\| := \sup\{\|A\psi\| \mid |\psi\rangle \in \mathbb{H}, \|\psi\| = 1\} < +\infty$)

Def The **ADJOINT** of A is an operator $A^*: \mathbb{H} \to \mathbb{H}$ such that $\langle A^*\psi|\varphi\rangle = \langle\psi|A\varphi\rangle$ $\forall |\psi\rangle, |\varphi\rangle \in \mathbb{H}$

We say that A is **SELF-ADJOINT** if $A = A^*$

Properties

(1) $(A^*)^* = A$, because $\forall |\psi\rangle, |\varphi\rangle \in \mathbb{H}$ we have

$$\langle (A^*)^*\psi|\varphi\rangle = \langle\psi|A^*\varphi\rangle = \overline{\langle A^*\varphi|\psi\rangle} = \overline{\langle\varphi|A\psi\rangle} = \langle A\psi|\varphi\rangle$$

(2) $(cA)^* = \bar{c}A^*$ $\forall c \in \mathbb{C}$

because $\langle\psi|cA\varphi\rangle = c\langle\psi|A\varphi\rangle = c\langle A^*\psi|\varphi\rangle = \langle \bar{c}A^*\psi|\varphi\rangle$

!

(3) $(A^*)_{ij} = \overline{A_{ji}}$

because $(A^*)_{ij} = \langle e_i | A^* e_j \rangle = \langle Ae_i | e_j \rangle = \overline{\langle e_j | Ae_i \rangle} = \overline{A_{ji}}$

(4) $\langle A\psi| = \langle \psi | A^*$, where $\langle A\psi| : \mathbb{H} \longrightarrow \mathbb{C}$

$|\varphi\rangle \rightsquigarrow \langle A\psi|\varphi\rangle$

and $\langle \psi | A^* : \mathbb{H} \longrightarrow \mathbb{C}$

$|\varphi\rangle \rightsquigarrow \langle \psi | A^* \varphi \rangle$

(5) $\left(|\psi\rangle\langle\varphi|\right)^* = |\varphi\rangle\langle\psi|$

because for any $|\xi\rangle, |\eta\rangle \in \mathbb{H}$ it holds

$$\langle \eta \,|\, (|\psi\rangle\langle\varphi|)\,\xi \rangle = \langle (|\psi\rangle\langle\varphi|)^* \eta \,|\, \xi \rangle$$

$$\langle \eta | \psi \rangle \cdot \langle \varphi | \xi \rangle = \langle \varphi | \xi \rangle \cdot \langle \eta | \psi \rangle =$$

$$= \overline{\langle \xi | \varphi \rangle} \cdot \overline{\langle \psi | \eta \rangle} =$$

$$= \overline{\langle \xi | \varphi \rangle \langle \psi | \eta \rangle} =$$

$$= \overline{\langle \xi \,|\, (|\varphi\rangle\langle\psi|)\,\eta \rangle} =$$

$$= \langle (|\varphi\rangle\langle\psi|)\,\eta \,|\, \xi \rangle$$

Def We say that $U : \mathbb{H} \longrightarrow \mathbb{H}$ is UNITARY if

$\langle U\psi | U\varphi \rangle = \langle \psi | \varphi \rangle \quad \forall |\psi\rangle, |\varphi\rangle \in \mathbb{H}$

Oss The following are equivalent:

(1) U is unitary

(2) $U^* U = Id$

(3) $\|U\psi\| = \|\psi\| \quad \forall |\psi\rangle \in \mathbb{H}$

Dim [1 => 2] $\langle \psi | \varphi \rangle = \langle U\psi | U\varphi \rangle = \langle U^* U \psi | \varphi \rangle \quad \forall |\psi\rangle, |\varphi\rangle \in \mathbb{H}$

$\Rightarrow U^* U = Id$

⋮

$[1 \Rightarrow 3]$ $\|U\psi\| = \sqrt{\langle U\psi | U\psi\rangle} = \sqrt{\langle \psi|\psi\rangle} = \|\psi\|$

$[* \Rightarrow *]$ left as an exercise to the reader

□

Rmk In finite dimension, if $\{e_j\}_{j\in I}$ is ONB then $\{Ue_j\}_{j\in I}$ is ONB if U is unitary

Def Let A be an operator on $\mathbb{H}$. We say that $|\psi\rangle \in \mathbb{H}$, $|\psi\rangle \neq 0$ is an **EIGENVECTOR** of A with respect to the **EIGENVALUE** $\lambda \in \mathbb{C}$ if $A|\psi\rangle = \lambda|\psi\rangle$

Def $\sigma(A) = \{\lambda \in \mathbb{C} \mid (A - \lambda Id) \text{ is not invertible}\}$ is the **SPECTRUM** of A

Oss λ eigenvalue for $A \Rightarrow \sigma(A)$

Also in the finite dimensional case the viceversa is also true

Let $A = A^*$ and λ eigenvalue of A with eigenvector $|\psi\rangle$

Then $\langle \psi | A\psi\rangle = \langle \psi | \lambda\psi\rangle = \lambda \langle \psi|\psi\rangle = \lambda \|\psi\|$

$\langle A^*\psi | \psi\rangle = \langle A\psi|\psi\rangle = \langle \lambda\psi|\psi\rangle = \bar{\lambda}\|\psi\|$

$\Rightarrow \lambda \in \bar{\lambda} \Rightarrow \lambda \in \mathbb{R}$

Let U be unitary and λ eigenvalue of U with eigenvector $|\psi\rangle$

Then $\|\psi\| = \|U\psi\| = \|\lambda\psi\| = |\lambda|\,\|\psi\| \Rightarrow |\lambda| = 1$

Let A be a compact operator on $\mathbb{H}$ with $A = A^*$. Then A can be diagonalized with respect to an ONB of $\mathbb{H}$

Let $\{\lambda_j\}_{j\in I}$ be the eigenvalues of A, then $A = \sum_{j,\alpha} \lambda_j |e_{j,\alpha}\rangle\langle e_{j,\alpha}|$

Def $P: \mathbb{H} \to \mathbb{H}$ is a **PROJECTION** if $P^2 = P$

⋮

Let $\mathbb{K}$ be a subspace of $\mathbb{H}$, then P is a **PROJECTION ONTO** $\mathbb{K}$ if $P(\mathbb{H}) \subseteq \mathbb{K}$

Es Let $|\psi\rangle \in \mathbb{H}$ with $\|\psi\| = 1$, the operator $|\psi\rangle\langle\psi|$ is the projection over $\mathrm{Span}(|\psi\rangle)$

P is an **ORTHOGONAL** projection if $P^2 = P \wedge P^* = P$

Oss If P is an orthogonal projection then there exists an orthonormal set $\{|\psi_j\rangle\}_{j \in I}$ such that

$$P = \sum |\psi_j\rangle\langle\psi_j|$$

This is a consequence of the property of the possible eigenvalues of a projection (0 and 1) and diagonal representation

Def Given $A, B : \mathbb{H} \to \mathbb{H}$, the **COMMUTATOR** of A and B is $[A,B] = AB - BA$

Oss A and B commute $\iff [A,B] = 0$

Def Given A we say that A is

- **POSITIVE** if $\langle\psi|A\psi\rangle \geq 0 \ \forall |\psi\rangle \in \mathbb{H}$
- **STRICTLY POSITIVE** if it's positive and

$$\langle\psi|A\psi\rangle = 0 \iff |\psi\rangle = 0$$

Oss Given $A, B : \mathbb{H} \to \mathbb{H}$, $(AB)^* = B^* A^*$

In addition, if $A = A^*$ and $B = B^*$, then $(AB)^* = AB$ if and only if they commute

Def The **TRACE** operator is the map

$$A \rightsquigarrow \sum_j \langle e_j | A e_j \rangle = \mathrm{tr}(A)$$

where $\{e_j\}_{j \in I}$ is an ONB. Note that the definition does not depend on the choice of the ONB

Oss $\mathrm{tr}(AB) = \mathrm{tr}(BA) \quad \forall A, B : \mathbb{H} \to \mathbb{H}$

05/10

QUANTUM MECHANICS

Postulates

Quantum Mechanics was initially developed at the beginning of the XX century by Heisenberg, Pauli, Weyl and Schrödinger

For what we're interested in, quantum mechanics gives a set of rules to compute probabilities associated to events related to "measures" which can be something like

- "the electron will be located in some $D \subseteq \mathbb{R}^3$"
- "light will be polarized along some direction $\vec{v}$"

We will use a frequentist approach: every event will be random but by repeating the same experiment a large number of times the fraction of success will approach the probability of success of the single random event

A consequence is that algorithms will only have a high

chance of success, so they'll have to be ran multiple times. Still, in many cases this will be faster than classical algorithms

Probability theory

Given a discrete space of events $\Omega = \{1, \dots, n\}$ and a probability density $(p_j)_{j=1}^n$ st $p_j \in [0,1]$ & $\sum_j p_j = 1$ we can define the expected value of $g : \Omega \to \mathbb{R}$ as

$$\mathbb{E}[g] = \sum_j p_j g(j)$$

We're now going to replace these objects to get a useful theory

First, we note that g can be described as a vector $(g_j)_{j=1}^n$ where $g_j = g(j)$

We can replace the expected value with

$$\mathbb{E}[g] = \sum_j p_j g_j = \left[(\sqrt{p_j})_{j=1}^n \right]^T F \, (\sqrt{p_j})_{j=1}^n$$

where $F = \mathrm{diag}(g_1, \dots, g_n)$

P1 (STATES, OBSERVABLES)

A quantum system is described as a Hilbert space $\mathbb{H}$

Given $\mathbb{H}$:

- an OBSERVABLE is any self-adjoint $A : \mathbb{H} \to \mathbb{H}$

;

- a **PURE STATE** is any $|\psi\rangle \in \mathbb{H}$ s.t. $\|\psi\| = 1$

We say that the physical system is in state $|\psi\rangle$ if for every observable A the quantum expected value of A is $\langle A \rangle_{|\psi\rangle} = \langle \psi | A \psi \rangle$

So physically we're not predicting probabilities as much as expected values, but practically that's the same

More precisely:

- $|\psi\rangle$ is a state vector (also called wave function)
- The physical system S will be identified with its Hilbert space $\mathbb{H}$

Ex $|\langle A \rangle_{|\psi\rangle}| \leq \|A\|$ $\left(\|A\| = \sup\{\langle \psi | A\psi \rangle \mid |\psi\rangle \text{ is a state}\}\right)$

By spectral theorem, given an observable A we can diagonalize it with an ONB $(|e_{j,\alpha}\rangle)_{j,\alpha}$, ie $A = \sum_{j,\alpha} \lambda_j |e_{j,\alpha}\rangle\langle e_{j,\alpha}|$ and we can rewrite the expected value of an observable as

$$\langle A \rangle_{|\psi\rangle} = \sum_{j,\alpha} \lambda_j \langle \psi | e_{j,\alpha} \rangle \langle e_{j,\alpha} | \psi \rangle =$$

$$= \sum_{j,\alpha} \lambda_j |\langle e_{j,\alpha} | \psi \rangle|^2$$

If $A = Id$ (also sometimes written as $\mathbf{1}$) we get

$$\langle Id \rangle_{|\psi\rangle} = \sum_{\alpha} 1 \, |\langle e_\alpha | \psi \rangle|^2 = \|\psi\|^2 = 1$$

Note that if A, B are observables and $\lambda \in \mathbb{R}$ it holds

$$\langle A + \lambda B \rangle_{|\psi\rangle} = \langle A \rangle_{|\psi\rangle} + \lambda \langle B \rangle_{|\psi\rangle}$$

P2 (PROBABILITIES)

Assume that a system is in a state $|\psi\rangle \in \mathbb{H}$ and let A be an observable

The possible outcomes of measuring A are $\sigma(A)$

(This has implications on quantization of outcomes, discrete possible values and discrete levels of energy)

For any $\lambda \in \sigma(A)$ the probabilities of measuring λ is $\mathbb{P}_\psi(\lambda) = \| P_\lambda \psi \|^2$ where $P_\lambda : \mathbb{H} \to \mathbb{H}$ denotes the orthogonal projection on $Eig_A(\lambda) = \{ |\varphi\rangle \in \mathbb{H} \mid |A\varphi\rangle = \lambda |\varphi\rangle \}$

Obs Consider P_λ as an observable (it satisfies the requirements)

Then $\mathbb{P}_\psi(\lambda) = \| P_\lambda \psi \|^2 = \langle P_\lambda \psi | P_\lambda \psi \rangle =$ $\quad P_\lambda^* = P_\lambda$

$= \langle \psi | P_\lambda P_\lambda \psi \rangle =$ $\quad P_\lambda^2 = P_\lambda$

$= \langle \psi | P_\lambda \psi \rangle =$

$= \langle P_\lambda \rangle_{|\psi\rangle}$

One might wonder when two states $|\psi\rangle$ and $|\varphi\rangle$ are "physically" the same, ie: $\langle A \rangle_{|\psi\rangle} = \langle A \rangle_{|\varphi\rangle}$ $\forall A$ observable (that is, they can't be physically distinguished by measurements)

It can be proven that this holds if and only if $|\varphi\rangle = e^{i\alpha} |\psi\rangle$ for some $\alpha \in \mathbb{R}$, called the PHASE

Proof

$[\Rightarrow]$ $\langle A \rangle_{|\psi\rangle} = \langle \psi | A \psi \rangle = e^{-i\alpha} \langle \varphi | A \varphi \rangle e^{i\alpha} = \langle \varphi | A \varphi \rangle$

$[\Leftarrow]$ left as an exercise

□

Def A **RAY** is defined as $R_\psi = \{ e^{i\alpha} |\psi\rangle \mid \alpha \in \mathbb{R} \}$

Let $|\psi\rangle, |\varphi\rangle$ be states and $a, b \in \mathbb{C}$ st $a|\psi\rangle + b|\varphi\rangle$ is also a state (ie such that $\| a|\psi\rangle + b|\varphi\rangle \| = 1$)

Any such combination is called a quantum superposition of $|\psi\rangle$ and $|\varphi\rangle$

Es if $\langle\psi|\varphi\rangle = 0$ then $\| a|\psi\rangle + b|\varphi\rangle \|^2 = \underbrace{|a|^2}_{p} + \underbrace{|b|^2}_{1-p} = 1$ $\quad p \in [0,1]$

$\frac{1}{\sqrt{2}}|\psi\rangle + \frac{1}{\sqrt{2}}|\varphi\rangle$ is an example of a superposition, and one would expect that, once measured, it has ½ of probability of being $|\psi\rangle$ and ½ of being $|\varphi\rangle$

Sadly the expected value isn't always as straightforward

$$\begin{aligned}
\langle A \rangle_{\sqrt{p}|\psi\rangle + \sqrt{1-p}|\varphi\rangle} &= \langle \sqrt{p}\,\psi + \sqrt{1-p}\,\varphi \mid A(\sqrt{p}\,\psi + \sqrt{1-p}\,\varphi)\rangle = \\
&= p\langle\psi|A\psi\rangle + (1-p)\langle\varphi|A\varphi\rangle + \\
&\quad + \sqrt{p(1-p)}\left(\langle\psi|A\varphi\rangle + \overline{\langle\psi|A\varphi\rangle}\right) = \\
&= p\langle A\rangle_{|\psi\rangle} + (1-p)\langle A\rangle_{|\varphi\rangle} + \underbrace{\sqrt{p(1-p)}\,\mathrm{Re}(\langle\psi|A\varphi\rangle)}_{\text{INTERFERENCE}}
\end{aligned}$$

Ex Compute $\langle A \rangle_{\sqrt{p}|\psi\rangle + e^{i\alpha}\sqrt{1-p}|\varphi\rangle}$ and show what happens to the interference

Prop If $|\psi\rangle, |\varphi\rangle \in \mathbb{H}$ are state vectors, then the probability of observing $|\varphi\rangle$ if the system is prepared in the state $|\psi\rangle$ is given by

$$\text{“}P_\psi(|\varphi\rangle)\text{”} = |\langle\varphi|\psi\rangle|^2$$

Proof consider the observable $A = |\varphi \times \varphi|$ ← $|\varphi\rangle\langle\varphi|$???

$$\mathbb{P}_\psi(Id) = \langle A \rangle_{|\psi\rangle} = \langle \psi | A \psi \rangle = \langle \psi | \varphi \rangle \langle \varphi | \psi \rangle$$
$$= |\langle \varphi | \psi \rangle|^2$$

Because we have defined a quantum expectation $\mathbb{E}[\cdot]$ it seems sensible to define a "quantum standard deviaton". The equivalent of the standard deviation will be the uncertainty

Def The **UNCERTAINTY** of an observable A in a state vector $|\psi\rangle$ is defined as

$$\Delta_\psi(A) = \sqrt{\langle (A - \langle A \rangle_{|\psi\rangle} Id)^2 \rangle_{|\psi\rangle}}$$

Obs
$$\Delta_\psi(A) = \sqrt{\langle (A - \langle A \rangle_{|\psi\rangle} Id)^2 \rangle_{|\psi\rangle}} =$$

$$= \sqrt{\langle \psi | (A - \langle A \rangle_{|\psi\rangle} Id)^2 \psi \rangle} = \quad (A - \langle A \rangle_{|\psi\rangle} Id) \text{ is self-adjoint}$$

$$= \sqrt{\langle (A - \langle A \rangle_{|\psi\rangle} Id)\psi \,|\, (A - \langle A \rangle_{|\psi\rangle} Id)\psi \rangle} =$$

$$= \| (A - \langle A \rangle_{|\psi\rangle} Id)\psi \|$$

Def An observable A is **SHARP** on the state $|\psi\rangle$ if $\Delta_\psi(A) = 0$

Prop. $\Delta_\psi(A) = 0 \iff |\psi\rangle$ is an eigenvector for A
(with eigenvalue $\langle A \rangle_{|\psi\rangle}$)

Proof

$[\Rightarrow]$ $\Delta_\psi(A) = 0 \iff \| (A - \langle A \rangle_{|\psi\rangle} Id)\psi \| = 0$

$$\iff A|\psi\rangle = \langle A \rangle_{|\psi\rangle} |\psi\rangle$$

□

Def A, B observables are **COMPATIBLE** if $[A,B]=0$

Compatible observables can be "measured" at the same time

Th If $[A,B]=0$ then $\exists (e_j)_j$ ONB such that A and B are both diagonal

Oss If A and B are not compatible then $\forall |\psi\rangle$ state

$$\langle i[A,B]\rangle_{|\psi\rangle} \leq 2\,\Delta_\psi(A)\,\Delta_\psi(B)$$

This is the **HEISENBERG UNCERTAINTY PRINCIPLE**

NOTE: if there wasn't the i, it wouldn't be an observable

12/10

Proof Observe that $\forall K: \mathbb{H} \longrightarrow \mathbb{H}$ operator we can get K^*K which is a non-negative operator because

$$\langle \psi | K^*K\psi\rangle = \langle K\psi | K\psi\rangle = \|K\psi\|^2 \geq 0$$

Pick $K = A + iB \Rightarrow K^* = A - iB$

Then $K^*K = (A-iB)(A+iB) =$ A and B do not commute

$$= A^2 + iAB - iBA + B^2 =$$

$$= A^2 + B^2 + i[A,B]$$

We get $0 \leq \langle K^*K\rangle_{|\psi\rangle} = \langle A^2\rangle_{|\psi\rangle} + \langle B^2\rangle_{|\psi\rangle} + \langle i[A,B]\rangle_{|\psi\rangle}$

so $-\langle i[A,B]\rangle_{|\psi\rangle} \leq \langle A^2\rangle_{|\psi\rangle} + \langle B^2\rangle_{|\psi\rangle}$

Now imagine we substitute A with $A - Id\langle A\rangle_{|\psi\rangle}$

then $[A - Id\langle A\rangle_{|\psi\rangle}, B] = [A,B] - \langle A\rangle_{|\psi\rangle}\underbrace{[Id,B]}_{=0}$

so the LHS doesn't change and on the right we get $\Delta_\psi(A)^2$

So far we have $\langle i[A,B]\rangle_{|\psi\rangle} \leq \Delta_\psi(A)^2 + \Delta_\psi(B)^2$

Now we'll replace A with λA and B with $\frac{B}{\lambda}$ for some $\lambda > 0$ so that we get

$$\langle i[A,B]\rangle_{|\psi\rangle} \leq \lambda^2 \Delta_\psi(A)^2 + \frac{1}{\lambda^2}\Delta_\psi(B)^2$$

And if we try to minimize wrt $\lambda > 0$ we have $\lambda^2 = \frac{\Delta_\psi(B)}{\Delta_\psi(A)}$ and the thesis follows from this □

Ex try and see what happens with $K = A + B$

Consider the Heisenberg inequality on $\mathbb{H} = L^2(\mathbb{R})$

We can define Q (position operator) st $(Q\psi)(x) = x \cdot \psi(x)$

P (momentum operator) st $(P\psi)(x) = -i\frac{d}{dx}\psi(x)$

Note it's not clear why every function should be differentiable with derivative in $L^2(\mathbb{R})$. We can define the derivative in a density-way but still we cannot be sure that P takes any function in L^2

One can prove that if $\psi \in C^1_c(\mathbb{R})$ then

$$[Q,P]\psi(x) = QP\psi - PQ\psi = -i\,x\frac{d}{dx}\psi(x) + i\frac{d}{dx}(x\,\psi(x)) =$$

$$= i\psi(x) = i(\mathrm{Id}\,\psi)(x)$$

So in general they do not commute

Following the process in the Heisenberg inequality proof we get $\frac{\langle\psi|\psi\rangle}{2} = \frac{1}{2} \leq \Delta_\psi(P)\,\Delta_\psi(Q)$ $\quad \langle\psi|\psi\rangle = \int_{-\infty}^{+\infty} |\psi(x)|^2 dx = 1$

So we cannot measure sharply both position and momentum

P3 (COLLAPSE OF WAVE FUNCTION)

If $|\psi\rangle$ is the state of a quantum system and the observable A is measured with outcome $\lambda \in \sigma(A)$ then the state after the measurement is described by $\frac{|P_\lambda \psi\rangle}{\|P_\lambda \psi\rangle}$ where P_λ is the orthogonal projection on $Eig(\lambda, A) = \{|\varphi\rangle \in H \mid A|\varphi\rangle = \lambda|\varphi\rangle\}$

P4 (...)

If the system is CLOSED (ie isolated) the evolution of a state $|\psi_t\rangle$ from a time t_0 to a time t_1 is described by a unitary $U(t_0, t_1)$ so that

$$|\psi_{t_1}\rangle = U(t_0, t_1)|\psi_{t_0}\rangle$$

Def An observable H is the HAMILTONIAN of a system if $U(t_0, t_1) = e^{-i(t_1 - t_0)H}$

Assuming that H does not depend on t_0, t_1, one can write $|\psi_t\rangle = e^{-itH}|\psi_0\rangle$, and if we take the derivative we get

$$\frac{\partial}{\partial t}|\psi_t\rangle = -iH|\psi_t\rangle \qquad : \partial_t|\psi_t\rangle = H|\psi_t\rangle$$

Schrödinger equation

Mixed states

We called a state $|\psi\rangle = a|\varphi_0\rangle + b|\varphi_1\rangle$ a quantum superposition (given that $|\psi\rangle, |\varphi_0\rangle, |\varphi_1\rangle$ are all states) and we saw that in the expected value there was some interference.

We'll now try to describe the following system:

Fix $(p_i)_{i=1}^N$ classical probabilities and chose $(|\psi_i\rangle)_{i=1}^N$ state vectors such that the probability of measuring $|\psi_i\rangle$ is p_i

We'll describe this system via the **DENSITY OPERATOR**

$(\rho = \sum p_i \cdot |\psi_i \times \psi_i| \quad \text{if } \langle\psi_i|\psi_j\rangle = \delta_{ij})$

Def A **MIXED STATE** on a system $\mathbb{H}$ is described by any density operator $\rho : \mathbb{H} \to \mathbb{H}$ st

- ρ is self-adjoint $\quad \rho^* = \rho$
- ρ is non-negative $\quad \langle\psi|\rho\psi\rangle \geq 0 \quad \forall |\psi\rangle \in \mathbb{H}$
- ρ has unit trace $\quad Tr(\rho) = 1$

We write $D(\mathbb{H}) = \{\rho : \mathbb{H} \to \mathbb{H} \mid \rho^* = \rho,\ \rho \geq 0,\ Tr(\rho) = 1\}$

Rmk

- $D(\mathbb{H})$ is a convex set, ie $\forall \rho_0, \rho_1 \in D(\mathbb{H}) \quad \forall p \in [0,1]$ then $(1-p)\rho_0 + p\rho_1 \in D(\mathbb{H})$
- If $|\psi\rangle$ is a pure state we can build $\rho = |\psi \times \psi| \in D(\mathbb{H})$ which shows $|\psi\rangle$ as a mixed state

Every state is a mixed state but some mixed state are NOT pure

$|\psi\times\psi| \in \mathcal{D}(\mathbb{H})$, because

- $\langle\varphi|\rho\varphi\rangle = \langle\varphi|\psi\rangle\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle\langle\varphi|\psi\rangle = \langle\rho\varphi|\varphi\rangle$
- $\mathrm{Tr}(\rho) = \ldots = \|\psi\|^2 = 1$

- If $|\varphi\rangle \in R_{|\psi\rangle}$, ie $|\varphi\rangle = e^{i\alpha}|\psi\rangle$ then $|\varphi\times\varphi| = |\psi\times\psi|$
- If U is unitary then $\forall \rho \in \mathcal{D}(\mathbb{H})$ then $U\rho U^*$ is also a state

Th If $\rho \in \mathcal{D}(\mathbb{H})$ then $(\dim \mathbb{H} = n)$

- $\exists (p_i)_i$, $p_i \in [0,1]$ $\sum_i p_i = 1$
  $\exists (|\psi_i\rangle)_i$ ONB of $\mathbb{H}$ st
  $\rho = \sum_i p_i |\psi_i\times\psi_i|$
- $\rho^2 \leq \rho$ (as quadratic forms)
  with equality if and only if ρ is pure $\rho = |\psi\times\psi|$
- $\|\rho\| \leq 1$ with equality iff ρ is pure

Proof We apply the spectral theorem to ρ and we get

- $(|\varphi_{j,\alpha}\rangle)_{j,\alpha}$ ONB st

$$\rho = \sum_j \lambda_j \sum_\alpha |\varphi_{j,\alpha}\times\varphi_{j,\alpha}|, \qquad \{\lambda_j\} = \sigma(\rho)$$

And up to renumbering we can do $|\varphi_{j,\alpha}\rangle \rightsquigarrow |\psi_i\rangle$

$\lambda_j \rightsquigarrow p_i$

Then $1 = \mathrm{Tr}(\rho) = \sum_j \lambda_j \underbrace{m_j}_{\text{multiplicity of } \lambda_j} = \sum_i p_i$

Also $p_i \geq 0$ so $p_i \in [0,1]$

- $\rho = \sum_i p_i |\psi_i \times \psi_i|$

  so $\rho^2 = \left(\sum_i p_i |\psi_i \times \psi_i|\right)\left(\sum_j p_j |\psi_j \times \psi_j|\right) =$ because of orthonormality

  $= \sum_i p_i^2 |\psi_i \times \psi_i| \leqslant$

  $< \sum_i p_i |\psi_i \times \psi_i| = \rho$

  Formally, $\rho - \rho^2 = \sum_i \underbrace{p_i(1-p_i)}_{\geqslant 0} |\psi_i \times \psi_i|$

  We get the equality exactly only if one of the $p_i = 1$ and the others are 0, so iff ρ is pure

- Left as an exercise

□

We will now see the 4 postulets we saw, but for the mixed states

P1 Given an observable A, its expectation on a mixed state ρ is $Tr(A\rho) = \sum_i p_i \langle A \rangle_{|\psi_i\rangle}$

P2 The probability of observing $\lambda \in \sigma(A)$ if the system is in the mixed state ρ is

$$\mathbb{P}_\rho(\lambda) = Tr(P_\lambda \rho) = \sum_i p_i \mathbb{P}_{\psi_i}(\lambda)$$

P3 After measuring $\lambda \in \sigma(A)$ the state ρ collapses to

$$\frac{P_\lambda \rho P_\lambda}{\mathbb{P}_\rho(\lambda)} \in D(\mathcal{H})$$

Note Say that A is measured but the outcome is not given to us, we can still describe the system, as

$$\tilde{\rho} = \sum_{\lambda \in \sigma(A)} \mathbb{P}_{\tilde{\rho}}(\lambda) \cdot \frac{P_\lambda \rho P_\lambda}{\mathbb{P}_{\tilde{\rho}}(\lambda)}$$

This was not possible using only pure states and it doesn't really have a classical correspondent

P4 If the system is closed it evolves from time t_0 to time t_1 according to an unitary operator $U(t_0, t_1)$

$$\rho_{t_0} \rightsquigarrow \rho_{t_1} = U(t_0, t_1)\, \rho\, U(t_0, t_1)^*$$

The Schrödinger equation associated to H is

$$i \partial_t \rho_t = H\rho_t - \rho_t H = [H, \rho_t]$$

The uncertainty of A over ρ is

$$\Delta_\rho(A) = \left(\langle (A - \langle A \rangle_\rho)^2 \rangle_\rho \right)^{1/2}$$

Ex Does the Heisenberg inequality still hold?

If $\rho \in \mathcal{D}(\mathbb{H})$ is represented as $\rho = \sum_{i=1}^{m} q_i |\varphi_i \times \varphi_i|$ with $|\varphi_i\rangle$ state vectors we can still rewrite as $\rho = \sum_{i=1}^{n} p_i |\psi_i \times \psi_i|$ with $(|\psi_i\rangle)_{i=1}^{n}$ ON. Can we relate somehow the two decompositions?

It holds that $m \geq n$ and $\exists U \in \mathbb{C}^{m \times m}$ unitary such that

$$\sqrt{q_i}\, |\varphi_i\rangle = \sum_{j=1}^{n} U_{ij} \sqrt{p_j}\, |\psi_j\rangle$$

Note that because we don't use every entry of the matrix U, U is not unique

Hint of proof

$$U_{ij} = \sqrt{\frac{q_i}{p_j}} \langle \varphi_i | \psi_j \rangle \qquad \text{for } i = 1, \dots, m,\ j = 1, \dots, n$$

And complete it to unitary $m \times m$ matrix

⌟

Ex If $\rho, \rho' \in \mathcal{D}(\mathcal{H})$ such that $\langle A \rangle_\rho = \langle A \rangle_{\rho'}$ $\forall A$ observable then $\rho = \rho'$

Hint $\mathrm{Tr}(A\rho) = \mathrm{Tr}(A\rho') \to \mathrm{Tr}(A(\rho - \rho')) = 0$ ...

14/10

Spin of a vector

Electrons have a property called spin which isn't an actual spinning motion but it's useful to think about it like that (more precisely, the axis of rotation)

Spin is identified with a vector in $\mathbb{R}^3$

We are interested in measuring the components along the three axis with the observables S_x, S_y, S_z

We will work in the Hilbert space $\mathcal{H} \cong \mathbb{C}^2$

From now on Hilbert spaces will always have dim 2

We consider an ONB on $\mathcal{H}$ identified as $|\uparrow_z\rangle, |\downarrow_z\rangle$ (up & down)

We also denote it as $|0\rangle, |1\rangle$

We can now write the observable as matrices

$$S_x = \frac{1}{2}\sigma_x \qquad \sigma_x = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$S_y = \frac{1}{2}\sigma_y \qquad \sigma_y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$S_z = \frac{1}{2}\sigma_z \qquad \sigma_z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

These are also called **PAULI MATRICES**

$|\uparrow_z\rangle$ and $|\downarrow_z\rangle$ are eigenvectors for the observable S_z with eigenvalues $\frac{1}{2}$ and $-\frac{1}{2}$ respectively, which explains the notation

Properties

where $\mathbb{1} = Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(1) $\sigma_j \sigma_k = \delta_{jk}\mathbb{1} + i\varepsilon_{jke}\sigma_e$ where $\varepsilon_{123} = \varepsilon_{231} = \varepsilon_{312} = 1$

where e is the missing index when $j \neq k$, and the value of e doesn't matter when $j = k$ because $\varepsilon_{jj*} = 0$

$\varepsilon_{321} = \varepsilon_{213} = \varepsilon_{132} = -1$

0 otherwhise

(2) $[\sigma_j, \sigma_k] = \sigma_j\sigma_k - \sigma_k\sigma_j = 2i\varepsilon_{jke}\sigma_e$ eg $[\sigma_1, \sigma_2] = 2i\sigma_3$

(3) $\{\sigma_j, \sigma_k\} = \sigma_j\sigma_k + \sigma_k\sigma_j = 2\delta_{jk}\mathbb{1}$

(4) σ_j is unitary and self-adjoint for $j = 1, \ldots, 3$

Suppose a system in state $|o\rangle = |\uparrow_z\rangle$. What happens when we measure σ_z (so "2 · zspin" as in $\sigma_z = 2S_z$)?

From the postulates we expect that:

- the measurement is sharp
- the expected value is 1
- the system stays in state $|o\rangle$ after measurement

$$\langle\sigma_z\rangle_{|o\rangle} = \langle o|\sigma_z|o\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$ expected value ✓

For the uncertainty we get

$$\sigma_z - \langle\sigma_z\rangle_{|0\rangle}\mathbb{1} = \begin{pmatrix}1&0\\0&-1\end{pmatrix} - \begin{pmatrix}1&0\\0&1\end{pmatrix} = \begin{pmatrix}0&0\\0&-2\end{pmatrix}, \quad \text{so}$$

$$\left(\sigma_z - \langle\sigma_z\rangle_{|0\rangle}\mathbb{1}\right)^2 = \begin{pmatrix}0&0\\0&4\end{pmatrix}, \quad \text{so}$$

$$\langle 0|\left(\sigma_z - \langle\sigma_z\rangle_{|0\rangle}\mathbb{1}\right)^2|0\rangle = (1\ 0)\begin{pmatrix}0&0\\0&4\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = 0$$

So the measurement is indeed sharp
Also $|0\rangle$ is an eigenstate so the system remains in state

If we started in state $|1\rangle$ instead of $|0\rangle$ the only thing that would change is the expected value, which would be -1

What happens if we measure σ_x instead of σ_z?
Expected value: $\langle\sigma_x\rangle_{|0\rangle} = (1\ 0)\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = 0$
Uncertainty: $\left(\sigma_x - \langle\sigma_x\rangle_{|0\rangle}\mathbb{1}\right)^2 = \sigma_x^2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$

$$\Rightarrow \langle 0|\left(\sigma_x - \langle\sigma_x\rangle_{|0\rangle}\mathbb{1}\right)^2|0\rangle = (1\ 0)\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = 1$$

The possible outcomes of this measurement are the eigenvalues of σ_x, which are ± 1, each of which has a probability of occurring which we can compute via projection on the eigenspaces
The eigenstates of σ_x are $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ and $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ respectively for the eigenvalues 1 and -1 " $|\uparrow_{\hat{x}}\rangle$ " $|\downarrow_{\hat{x}}\rangle$
We can write these states with respect to the ONB

$$|\uparrow_{\hat{x}}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |\downarrow_{\hat{x}}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

So to get the probability of measuring 1 from state $|0\rangle$

we take its coefficient and square its modulus. The same goes for the probability of measuring -1 from state $|0\rangle$

So we have a probability of $\frac{1}{2}$ of measuring 1, after which the system will be in state $|\uparrow \hat{x}\rangle$, and $\frac{1}{2}$ of measuring -1, after which the system will be in state $|\downarrow \hat{x}\rangle$

What happens if we measure σ_z again after measuring σ_x? Suppose the system was in $|0\rangle$, we measured σ_x and got 1 so the system is now in the state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.
Then the system has a probability of $\frac{1}{2}$ of being $|0\rangle$ and $\frac{1}{2}$ of being $|1\rangle$, while previously the measurament was sharp! Measuring a different property (σ_x) changed one we already measured (σ_z, well we didn't necessarely measure it but if we knew the system was in state $|0\rangle$ that's the same as measuring σ_z and getting 1)

Rmk σ_z and σ_x do NOT commute, so they are not compatible

Qubits

Classical bits have 2 possible states: 0 and 1
We define a QUBIT as a quantum system defined by a 2-dimensional Hilbert space $\mathbb{H}$ with ONB $\{|0\rangle, |1\rangle\}$ and an observable σ_z with $|0\rangle, |1\rangle$ as eigenstates and respective eigenvalues $1, -1$
The states $|0\rangle$ and $|1\rangle$ correspond to the classical states 0 and 1

but we also have all the states of the form

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad \text{where } |a|^2+|b|^2=1, \quad a,b \in \mathbb{C}$$

For this reason a qubit contains much more information than a classical bit, but once you measure it you lose this additional information

Measuring a qubit means measuring σ_z, yeilding either 1 or -1 after which the state will collapse in $|0\rangle$ or $|1\rangle$ respectively

Bloch sphere representation

Since $|a|^2+|b|^2=1$, there exist α, β, ϑ angles such that

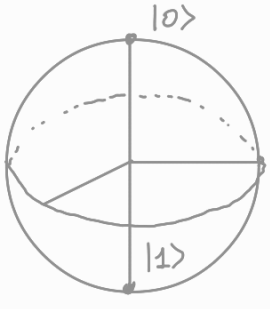
$$a = e^{i\alpha}\cos\tfrac{\vartheta}{2}, \qquad b = e^{i\beta}\sin\tfrac{\vartheta}{2}$$

So, up to global phase, I can write $|\psi\rangle = e^{-i\varphi/2}\cos\tfrac{\vartheta}{2}|0\rangle + e^{i\varphi/2}\sin\tfrac{\vartheta}{2}|1\rangle$ with $0 \le \vartheta \le \pi$, $0 \le \varphi \le 2\pi$

Note that because we're writing it up to a global phase, we can "put all the phase on $|1\rangle$" writing $|\psi\rangle$ as

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

We can represent $|\psi\rangle = |\psi\rangle_{\varphi,\vartheta}$ as the point $\begin{pmatrix}\sin\vartheta\cos\varphi\\ \sin\vartheta\sin\varphi\\ \cos\vartheta\end{pmatrix}$ in $S^2 \subseteq \mathbb{R}^3$. This is called BLOCH SPHERE representation



For $\vartheta = 0$, φ is irrelevant and we get $|0\rangle$, and the same goes for $\vartheta = \pi$ where we get $|1\rangle$

There is a bijetion between the points on the sphere and the possible states up to global phase.

Let's fix a qubit state $|\psi\rangle$. We would like to build an observable which has $|\psi\rangle$ as an eigenvector

Def Let $a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \in \mathbb{R}^3$. We define

$$a \cdot \sigma = \sum_{k=1}^{3} a_k \sigma_k = a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3$$

So $a \in \mathbb{R}^3$ identifies the linear combination of the Pauli matrices given by $a \cdot \sigma = \begin{pmatrix} a_3 & a_1 - ia_2 \\ a_1 + ia_2 & -a_3 \end{pmatrix}$

Oss $(a\cdot\sigma)(b\cdot\sigma) = (a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3)(b_1\sigma_1 + b_2\sigma_2 + b_3\sigma_3) =$

$$= (a_1b_1 + a_2b_2 + a_3b_3)\mathbb{1} + a_1b_2\sigma_1\sigma_2 + a_1b_3\sigma_1\sigma_3 +$$
$$+ a_2b_1\sigma_2\sigma_1 + a_2b_3\sigma_2\sigma_3 + a_3b_1\sigma_3\sigma_1 + a_3b_2\sigma_3\sigma_2 =$$

$$= (a\cdot b)\mathbb{1} + i(a_1b_2\sigma_3 - a_1b_3\sigma_2 - a_2b_1\sigma_3 + a_2b_3\sigma_1$$
$$+ a_3b_1\sigma_2 - a_3b_2\sigma_1) =$$

$$= (a\cdot b)\mathbb{1} + i\left[(a_2b_3 - a_3b_2)\sigma_1 + (a_3b_1 - a_1b_3)\sigma_2 + \right.$$
$$\left. + (a_1b_2 - a_2b_1)\sigma_3\right] =$$

$$= (a\cdot b)\mathbb{1} + i(a\times b)\cdot\sigma$$

Def Given a qubit state $|\psi\rangle$ we define

$$\hat{n}_{|\psi\rangle} = \begin{pmatrix} \sin\vartheta\cos\varphi \\ \sin\vartheta\sin\varphi \\ \cos\vartheta \end{pmatrix} \in \mathbb{R}^3$$ where ϑ, φ are the parameters

that represent $|\psi\rangle$ in Bloch notation

Oss $$\hat{n}_{|\psi\rangle} \cdot \sigma = \begin{pmatrix} \cos\vartheta & \sin\vartheta\cos\varphi - i\sin\vartheta\sin\varphi \\ \sin\vartheta\cos\varphi + i\sin\vartheta\sin\varphi & -\cos\vartheta \end{pmatrix} =$$

$$= \begin{pmatrix} \cos\vartheta & e^{-i\varphi}\sin\vartheta \\ e^{i\varphi}\sin\vartheta & -\cos\vartheta \end{pmatrix}$$

The operator $\hat{n}_{|\psi\rangle}$ is exactly the operator we were looking for, as $|\psi\rangle$ is an eigenvector for $\hat{n}_{|\psi\rangle}$. Let's verify it:

$$\begin{pmatrix} \cos\vartheta & e^{-i\varphi}\sin\vartheta \\ e^{i\varphi}\sin\vartheta & -\cos\vartheta \end{pmatrix} \begin{pmatrix} e^{-i\varphi/2}\cos\vartheta/2 \\ e^{i\varphi/2}\sin\vartheta/2 \end{pmatrix} = \begin{pmatrix} e^{-i\varphi/2}\cos\vartheta\cos\vartheta/2 + e^{-i\varphi/2}\sin\vartheta\sin\vartheta/2 \\ e^{i\varphi/2}\sin\vartheta\cos\vartheta/2 - e^{i\varphi/2}\cos\vartheta\sin\vartheta/2 \end{pmatrix} =$$

$$= \begin{pmatrix} e^{-i\varphi/2}\left(\cos\vartheta\cos\vartheta/2 + \sin\vartheta\sin\vartheta/2\right) \\ e^{i\varphi/2}\left(\cos\vartheta/2\sin\vartheta - \cos\vartheta\sin\vartheta/2\right) \end{pmatrix} =$$

$$= \begin{pmatrix} e^{-i\varphi/2}\cos\left(\vartheta - \vartheta/2\right) \\ e^{i\varphi/2}\sin\left(\vartheta - \vartheta/2\right) \end{pmatrix}$$

$$= |\psi\rangle$$

Analogously, $|\downarrow \hat{n}_{|\psi\rangle}\rangle = \begin{pmatrix} e^{-i\varphi/2}\cos\vartheta/2 \\ -e^{i\varphi/2}\sin\vartheta/2 \end{pmatrix}$ is an eigenvector

with eigenvalue -1

We've discussed pure states in the context of qubits.
We'll discuss now mixed states

A mixed state is given by a density operator ρ, ie:

(i) $\rho^* = \rho$ (ii) $\operatorname{tr}\rho = 1$ (iii) $\rho \geq 0$

In dim = 2 we get $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ so to satisfy (i, ii, iii) we get

(i) $\Rightarrow a, d \in \mathbb{R}$, $b = \bar{c}$ (ii) $\Rightarrow a + d = 1$

So we can describe ρ with three real parameters x_1, x_2, x_3 by

$$a = \frac{1 + x_3}{2} \qquad d = \frac{1 - x_3}{2} \qquad b = \frac{x_1 + ix_2}{2} \qquad c = \frac{x_1 - ix_2}{2}$$

$$\Rightarrow \quad \rho = \frac{1}{2}\begin{pmatrix} 1 + x_3 & x_1 + ix_2 \\ x_1 - ix_2 & 1 - x_3 \end{pmatrix}$$

To satisfy (iii) we need to find the eigenvalues of ρ, so

$$(1 + x_3 - 2\lambda)(1 - x_3 - 2\lambda) - (x_1 - ix_2)(x_1 + ix_2) = 0$$

$$(1 - 2\lambda)^2 - x_3^2 = x_1^2 + x_2^2$$

$$(1 - 2\lambda)^2 = \|x\|_2^2$$

$$\lambda = \frac{1 \pm \|x\|_2}{2}$$

So $\rho \geq 0 \iff \lambda \geq 0 \iff \|x\|_2 \leq 1$

So we can represent any mixed state ρ in dim = 2 with a vector $x \in \mathbb{R}^3$ inside the unitary disk

This gives a representation corresponding to the Bloch sphere

representation, and interestingly:

Rmk 1 ρ is pure $\iff$ it is represented by a point on the sphere (ie $\|x\| = 1$)

Rmk 2 $$\rho = \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + x_1\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} + x_2\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} + x_3\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] =$$

$$= \frac{1}{2}\left[\mathbb{1} + x_1\sigma_x + x_2\sigma_y + x_3\sigma_z\right]$$

$$= \frac{1}{2}\left[\mathbb{1} + x\cdot\sigma\right]$$

Proof of rmk 1

We know that ρ is pure if and only if $\rho^2 = \rho$

so $$\rho^2 = \left(\frac{1}{2}\left[\mathbb{1} + x\cdot\sigma\right]\right)^2 = \frac{1}{4}\left(\mathbb{1} + x\cdot\sigma\right)\left(\mathbb{1} + x\cdot\sigma\right) =$$

$$= \frac{1}{4}\left(\mathbb{1} + (x\cdot\sigma)(x\cdot\sigma) + 2x\cdot\sigma\right) =$$

$$= \frac{1}{4}\left(\mathbb{1} + \|x\|_2^2\,\mathbb{1} + 2x\cdot\sigma\right) =$$

$$= \frac{1}{2}\left(\frac{(1 + \|x\|_2^2)}{2}\,\mathbb{1} + x\cdot\sigma\right)$$

$(a\cdot\sigma)(b\cdot\sigma) = (a\cdot b)\mathbb{1} + i(a\times b)\sigma$

So $\rho^2 = \rho \iff \|x\|_2 = 1$

□

Rmk 3 for $j = 1, 2, 3$ $\quad tr(\rho_x\,\sigma_j) = x_j$

Proof $$tr(\rho_x\cdot\sigma_j) = tr\left(\frac{1}{2}\left(\mathbb{1} + x\cdot\sigma\right)\sigma_j\right) =$$

$$= \frac{1}{2}\,tr\left(\sigma_j + (x\cdot\sigma)\sigma_j\right) =$$

$$= \frac{1}{2}\,tr\,\sigma_j + \frac{1}{2}\,tr\left((x\cdot\sigma)(e_j\cdot\sigma)\right) =$$

$$\vdots$$

$$= \frac{1}{2}\,\mathrm{tr}\left(x\cdot e_j\, \mathbb{1} + i(x\times e_j)\cdot\sigma \right) =$$

$$= \frac{1}{2}\,\mathrm{tr}\left(x_j \mathbb{1}\right) + \frac{1}{2} i \sum_{k=1}^{3} \mathrm{tr}\left((x\times e_j)_k \sigma_k\right) =$$

($\mathrm{tr}(x_j \mathbb{1}) = 2x_j$; $\mathrm{tr}((x\times e_j)_k\sigma_k) = 0$)

$$= x_j$$

□

Operators on qubit

We want to study unitary operators on $\mathbb{H}$

Ex let A be an operator on $\mathbb{H}$, then

$$e^A := \sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

Now suppose that $A^2 = \mathbb{1}$

Then $\forall \alpha \in \mathbb{R}$, $e^{i\alpha A} = \mathbb{1} + i\alpha A - \frac{1}{2}\alpha^2 \mathbb{1} - \frac{1}{3!} i\alpha^3 A + \frac{1}{4!}\alpha^4 \mathbb{1} + \dots$

$$= \cos(\alpha)\,\mathbb{1} + i\sin(\alpha) A$$

Def Let $\hat{n} \in \mathbb{R}^3$ be a unit vector (ie $\hat{n} \in S^2$)

and $\alpha \in \mathbb{R}$

We define the rotation around $\hat{n}$ of an angle $\alpha/2$ as

the operator $D_{\hat{n}}(\alpha) = e^{-i\alpha/2\, \hat{n}\cdot\sigma}$ (aka spin operator)

Obs $(\hat{n}\cdot\sigma)^2 = \underbrace{(\hat{n}\cdot\hat{n})}_{=1}\mathbb{1} + i\underbrace{(\hat{n}\times\hat{n})}_{=0}\cdot\sigma = \mathbb{1}$

So we get:

Properties

(1) $D_{\hat{n}}(\alpha) = e^{-i\alpha/2\,\hat{n}\cdot\sigma} = \cos(\alpha/2)\,\mathbb{1} - i\sin(\alpha/2)\,\hat{n}\cdot\sigma$

(from the previous exercise)

(2) $D_{\hat{n}}(\alpha)^* = D_{\hat{n}}(-\alpha)$ (check as an exercise)

(3) $D_{\hat{n}}(\alpha)\, D_{\hat{n}}(\alpha)^* = \mathbb{1}$ so $D_{\hat{n}}(\alpha)$ is unitary

(follows from ② and (④ or common sense))

(4) $D_{\hat{n}}(\alpha)\, D_{\hat{n}}(\beta) = D_{\hat{n}}(\alpha+\beta)$

because $D_{\hat{n}}(\alpha)\, D_{\hat{n}}(\beta) =$

$$= \left[\cos(\alpha/2)\,\mathbb{1} - i\sin(\alpha/2)\,\hat{n}\cdot\sigma\right]\left[\cos(\beta/2)\,\mathbb{1} - i\sin(\beta/2)\,\hat{n}\cdot\sigma\right]$$

$$= \cos(\alpha/2)\cos(\beta/2)\,\mathbb{1} - \sin(\alpha/2)\sin(\beta/2)\,\mathbb{1} -$$
$$- i\left[\cos(\alpha/2)\sin(\beta/2) + \sin(\alpha/2)\cos(\beta/2)\right]\hat{n}\cdot\sigma =$$

$$= \cos\left(\frac{\alpha+\beta}{2}\right)\mathbb{1} - i\sin\left(\frac{\alpha+\beta}{2}\right)\hat{n}\cdot\sigma$$

$$= D_{\hat{n}}(\alpha+\beta)$$

□

Lemma Let U be an unitary operator on $\mathbb{H}$

Then $\exists\, \alpha, \beta, \gamma, \delta \in \mathbb{R}$ st the matrix of U with respect to $\{|0\rangle, |1\rangle\}$ is

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

Idea of proof

Write $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{C}^2$ and impose $UU^* = \mathbb{1}$

ie $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ so

$$\begin{cases} |a|^2 + |b|^2 = 1 \\ a\bar{c} + b\bar{d} = 0 \\ |c|^2 + |d|^2 = 1 \end{cases}$$

and from this you get ☆ a n g l e s ☆

□

Lemma Let U be an unitary operator on $\mathbb{H}$

then $\exists\, \alpha, \beta, \gamma, \delta \in \mathbb{R}$ st

$$U = e^{i\alpha} D_{\hat{z}}(\beta) D_{\hat{y}}(\gamma) D_{\hat{z}}(\delta)$$

ie as rotations around only $\hat{z}$ and $\hat{y}$ (no $\hat{x}$)

Proof

$$D_{\hat{z}}(\beta) = \cos\left(\beta/2\right)\mathbb{1} - i\sin\left(\beta/2\right)\sigma_z = \begin{pmatrix} \cos\beta/2 - i\sin\beta/2 & 0 \\ 0 & \cos\beta/2 + i\sin\beta/2 \end{pmatrix}$$

$$D_{\hat{y}}(\gamma) = \cos\left(\gamma/2\right)\mathbb{1} - i\sin\left(\gamma/2\right)\sigma_y = \begin{pmatrix} \cos\gamma/2 & -\sin\gamma/2 \\ \sin\gamma/2 & \cos\gamma/2 \end{pmatrix}$$

And if you explicit the product $e^{i\alpha} D_{\hat{z}}(\beta) D_{\hat{y}}(\gamma) D_{\hat{z}}(\delta)$ with the matrices we've just found you get the representation given by the first lemma □

Lemma Let U be an unitary operator on $\mathbb{H}$

Then there exist operators A, B, C on $\mathbb{H}$ and $\alpha \in \mathbb{R}$ st

- $ABC = \mathbb{1}$
- $U = e^{i\alpha} A \sigma_x B \sigma_x C$

Idea of proof "just choose the correct operators A, B, C"

we know that $U = e^{i\alpha} D_{\hat{z}}(\beta) \cdot D_{\hat{y}}(\gamma) \cdot D_{\hat{z}}(\delta)$

we now take

$$A = D_{\hat{z}}(\beta) D_{\hat{y}}\left(\gamma/2\right) \qquad C = D_{\hat{z}}\left(\frac{\delta - \beta}{2}\right)$$

$$B = D_{\hat{y}}\left(-\gamma/2\right) D_{\hat{z}}\left(-\frac{\beta+\delta}{2}\right)$$

It's clear that $ABC = \mathbb{1}$ (just look at them angles)

$$A\sigma_x B\sigma_x C = D_{\hat{z}}(\beta) D_{\hat{y}}\left(\gamma/2\right) \sigma_x D_{\hat{y}}\left(-\gamma/2\right) D_{\hat{z}}\left(-\frac{\beta+\delta}{2}\right) \sigma_x D_{\hat{z}}\left(\frac{\delta-\beta}{2}\right)$$

$$\mathbb{1} = \sigma_x \sigma_x$$

$$= D_{\hat{z}}(\beta) D_{\hat{y}}(\gamma/2) \cdot \underbrace{\sigma_x D_{\hat{y}}(-\gamma/2)\sigma_x}_{D_{\hat{y}}(\gamma/2) \longleftrightarrow D_{\hat{z}}\left(\frac{\beta+\delta}{2}\right)} \cdot \underbrace{\sigma_x D_{\hat{z}}\left(-\frac{\beta+\delta}{2}\right)\sigma_x}_{} \cdot D_{\hat{z}}\left(\frac{\delta-\beta}{2}\right)$$

this holds specifically because $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and we're using $D_{\hat{y}}$ and $D_{\hat{z}}$. The full proof is left as an exercise

$$= D_{\hat{z}}(\beta) D_{\hat{y}}(\gamma) D_{\hat{z}}(\delta)$$

□

Lemma Let U be an unitary operator on $\mathbb{H}$

Then $\exists \alpha, \xi \in \mathbb{R}$, $\hat{n} \in \mathbb{R}^3$ unit vector st $U = e^{i\alpha} D_{\hat{n}}(\xi)$

Idea of proof "it's not difficult it's just long"

We use the representation from the first lemma and split that matrix as $U = c_0 \mathbb{1} + c_1 \sigma_x + c_2 \sigma_y + c_3 \sigma_z$ and deduce the coordinates of $\hat{n}$ and ξ from $\{c_i\}_{i=0}^3$

□

Ex Let A be an operator on $\mathbb{H}$

Then $\exists z_0, z_1, z_2, z_3 \in \mathbb{C}$ st $A = z_0 \mathbb{1} + z \cdot \sigma$, where $z = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} \in \mathbb{C}^3$

If A is unitary then $|z_0|^2 + \|z\|_2^2 = 1$

Proof $\mathbb{C}^{2\times 2} \ni A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} z_0 + z_3 & z_1 - i z_2 \\ z_1 + i z_2 & z_0 - z_3 \end{pmatrix}$ from which we get

$$z_0 = \frac{a+d}{2}, \quad z_3 = \frac{a-d}{2}, \quad z_1 = \frac{b+c}{2}, \quad z_2 = i\frac{b-c}{2}$$

If A is unitary $A = e^{i\alpha} D_{\hat{n}}(\xi)$ and deduce $|z_0|^2 + \|z\|_2^2 = 1$

(or use this exercise to prove the lemma ☺)

□

Hadamard Operator

Def The Hadamard operator is $H := \frac{\sigma_x + \sigma_z}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ with respect to $\{|0\rangle, |1\rangle\}$

Obs $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\quad$ $H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$H^2 = \mathbb{1}$

$H = e^{i\frac{3\pi}{2}} D_{\hat{z}}(0) D_{\hat{y}}(\pi/2) D_{\hat{z}}(-\pi)$

21/10

Composite Systems

A classical bit stores information in $\{0,1\}$, and a system of bits represent $\{0,1\}^n = \{(x_{n-1} \dots x_1 x_0) \mid x_i \in \{0,1\}\}$

A qubit is represented by a state in $\mathbb{H} = \mathbb{C}^2$. How should we represent a system of qubits? We'll use the tensor product of $\mathbb{H}$, say $\mathbb{H}^{AB} = \mathbb{H}^A \otimes \mathbb{H}^B$

Given a joint probability on $\mathbb{H}^{AB}$ we would like to be able to compute the marginal probabilities on $\mathbb{H}^A$ and $\mathbb{H}^B$ $\rho^A \in D(\mathbb{H}^A)$, $\rho^B \in D(\mathbb{H}^B)$ given $\rho \in D(\mathbb{H}^{AB})$ (called reduced states)

Def Given $(\mathbb{H}^A, \langle\cdot\rangle^{\mathbb{H}^A})$ and $(\mathbb{H}^B, \langle\cdot\rangle^{\mathbb{H}^B})$ two Hilbert space with the respective scalar products, we define $\forall |\varphi\rangle \in \mathbb{H}^A$, $|\psi\rangle \in \mathbb{H}^B$ the functional $|\varphi\rangle \otimes |\psi\rangle$ given by

$$|\varphi\rangle \otimes |\psi\rangle : \mathcal{H}^A \times \mathcal{H}^B \longrightarrow \mathbb{C}$$
$$(\xi, \eta) \rightsquigarrow \langle \xi | \varphi \rangle^{\mathcal{H}^A} \cdot \langle \psi | \eta \rangle^{\mathcal{H}^B}$$

Properties

- $|\varphi\rangle \otimes |\psi\rangle (\xi + \xi', \eta) = |\varphi\rangle \otimes |\psi\rangle (\xi, \eta) + |\varphi\rangle \otimes |\psi\rangle (\xi', \eta)$
- $|\varphi\rangle \otimes |\psi\rangle (a\xi, \eta) = \bar{a} |\varphi\rangle \otimes |\psi\rangle (\xi, \eta)$

So $|\varphi\rangle \otimes |\psi\rangle$ is a biantilinear functional on $\mathcal{H}^A \times \mathcal{H}^B$

Notation $|\varphi\rangle \otimes |\psi\rangle = |\varphi \otimes \psi\rangle = |\varphi, \psi\rangle = |\varphi\rangle|\psi\rangle = |\varphi\psi\rangle$

We define the tensor product of $\mathcal{H}^A$ and $\mathcal{H}^B$ as

$$\mathcal{H}^A \otimes \mathcal{H}^B = \{ \Phi : \mathcal{H}^A \times \mathcal{H}^B \longrightarrow \mathbb{C} \text{ biantilinear} \}$$

Rmk

(i) $\mathcal{H}^A \otimes \mathcal{H}^B$ is a vector space on $\mathbb{C}$

(ii) If $\{|e_i\rangle\}_{i=1,\dots,n_A}$ and $\{|f_j\rangle\}_{j=1,\dots,n_B}$ ONBs for $\mathcal{H}^A$ and $\mathcal{H}^B$ then $\{|e_i\rangle \otimes |f_j\rangle\}_{\substack{i=1,\dots,n_A \\ j=1,\dots,n_B}}$ is a (orthonormal, but we haven't defined a scalar product yet) basis for $\mathcal{H}^A \otimes \mathcal{H}^B$

$$\forall \Psi \in \mathcal{H}^A \otimes \mathcal{H}^B, \quad \Psi = \sum_{i=1}^{n_A} \sum_{j=1}^{n_B} \Psi_{ij} |e_i\rangle \otimes |e_j\rangle \quad \text{where}$$
$$\Psi_{ij} = \Psi(e_i, f_j)$$

(iii) $\dim \mathcal{H}^A \otimes \mathcal{H}^B = \dim \mathcal{H}^A \cdot \dim \mathcal{H}^B$

Proof

(ii) If $\xi \in \mathcal{H}^A$, $\eta \in \mathcal{H}^B$ then $\xi = \sum_i \langle e_i | \xi \rangle |e_i\rangle$ and $\eta = \sum_j \langle f_j | \eta \rangle |f_j\rangle$

Then $\Psi(\xi, \eta) = \sum_i \sum_j \overline{\xi_i \eta_j} \Psi_{ij}$

And $\overline{\xi_i \eta_j} = \langle \xi | e_i \rangle^{\mathbb{H}^A} \langle \eta | f_j \rangle = |e_i\rangle \otimes |f_j\rangle (\xi, \eta)$

So $\Psi(\xi, \eta) = \sum_i \sum_j \Psi_{ij} |e_i\rangle \otimes |f_j\rangle (\xi, \eta)$

So $\{|e_i\rangle \otimes |f_j\rangle\}_{i,j}$ generate, we have to show that they are linearly independent

Pick $\xi = e_{\bar{i}}$ and $\eta = f_{\bar{j}}$, then

$$|e_i\rangle \otimes |f_j\rangle (e_{\bar{i}}, f_{\bar{j}}) = \begin{cases} 1 & \text{if } i = \bar{i} \wedge j = \bar{j} \\ 0 & \text{otherwise} \end{cases}$$

... which shows the linear independence

Def A scalar product on $\mathbb{H}^A \otimes \mathbb{H}^B$ is defined $\forall \varphi_1, \varphi_2 \in \mathbb{H}^A$ $\forall \psi_1, \psi_2 \in \mathbb{H}^B$ as $\langle \varphi_1 \otimes \psi_1 | \varphi_2 \otimes \psi_2 \rangle^{\mathbb{H}^A \otimes \mathbb{H}^B} = \langle \varphi_1 | \varphi_2 \rangle^{\mathbb{H}^A} \langle \psi_1 | \psi_2 \rangle^{\mathbb{H}^B}$ and extended by linearity, ie:

If $\Psi, \Phi \in \mathbb{H}^A \otimes \mathbb{H}^B$ are written as $\Psi = \sum_k \sum_\ell \Psi_{k\ell} |e_k\rangle \otimes |f_\ell\rangle$ and $\Phi = \sum_i \sum_j \Phi_{ij} |e_i\rangle \otimes |f_j\rangle$, the scalar product is

$$\langle \Psi | \Phi \rangle^{\mathbb{H}^A \otimes \mathbb{H}^B} = \sum_{i,j} \sum_{k,\ell} \overline{\Psi_{ij}} \Phi_{k\ell} \langle e_i | e_k \rangle^{\mathbb{H}^A} \langle f_j | f_\ell \rangle^{\mathbb{H}^B}$$

Ex Show that $\langle | \rangle^{\mathbb{H}^A \otimes \mathbb{H}^B}$ does not depend on the choice for the ONBs $\{|e_i\rangle\}, \{|f_j\rangle\}$

Rmk If $\{|e_i\rangle\}, \{|f_j\rangle\}$ are ONBs on $\mathbb{H}^A$ and $\mathbb{H}^B$ then $\{|e_i\rangle \otimes |f_j\rangle\}$ is an ONB, and the scalar product becomes

$$\langle \Psi | \Phi \rangle^{\mathbb{H}^A \otimes \mathbb{H}^B} = \sum_{i,j} \overline{\Psi_{ij}} \Phi_{ij} = \mathrm{tr}\left(M_\Psi^* M_\Phi\right)$$

where $M_\Psi = (\Psi_{ij})_{ij} \in \mathbb{C}^{n_A \times n_B}$

Rmk $\mathbb{C}^{n_A \times n_B} \simeq \mathbb{C}^{n_A n_B}$ (matrices $\simeq$ long vectors)

$\begin{pmatrix} - r_1 - \\ - r_2 - \\ \vdots \\ - r_{n_A} - \end{pmatrix} \longrightarrow (r_1, r_2, \ldots r_{n_A})^T$

Rmk $\| |\varphi\rangle \otimes |\psi\rangle \|_{\mathbb{H}^A \otimes \mathbb{H}^B} = \|\varphi\|_{\mathbb{H}^A} \|\psi\|_{\mathbb{H}^B}$

We can generalise the definition to n factors $\mathbb{H}^{A_1} \otimes \dots \otimes \mathbb{H}^{A_n}$, where $|\varphi_1\rangle \otimes \dots \otimes |\varphi_n\rangle : \mathbb{H}^{A_1} \times \dots \times \mathbb{H}^{A_n} \longrightarrow \mathbb{C}$

$$(\xi_1, \dots, \xi_n) \rightsquigarrow \prod_{i=1}^{n} \langle \xi_i | \varphi_i \rangle^{\mathbb{H}^{A_i}}$$

Note that set-wise $(\mathbb{H}^A \otimes \mathbb{H}^B) \otimes \mathbb{H}^C \neq \mathbb{H}^A \otimes \mathbb{H}^B \otimes \mathbb{H}^C$ but they're isomorphic as Hilbert spaces

In general $\mathbb{H}^A \otimes \mathbb{H}^B \neq \mathbb{H}^B \otimes \mathbb{H}^A$ (they are isomorphic but with qubits the order will be important)

Example $\mathbb{H}^A = \mathbb{H}^B = \mathbb{C}^2$ with ONBs $\{|0\rangle^{\mathbb{H}^A}, |1\rangle^{\mathbb{H}^A}\}$, $\{|0\rangle^{\mathbb{H}^B}, |1\rangle^{\mathbb{H}^B}\}$

Then $\mathbb{H}^A \otimes \mathbb{H}^B \simeq \mathbb{C}^4$ with ONB given by

$$|0\rangle^{\mathbb{H}^A} \otimes |0\rangle^{\mathbb{H}^B} = |00\rangle = |0\rangle$$
$$|0\rangle^{\mathbb{H}^A} \otimes |1\rangle^{\mathbb{H}^B} = |01\rangle = |1\rangle$$
$$|1\rangle^{\mathbb{H}^A} \otimes |0\rangle^{\mathbb{H}^B} = |10\rangle = |2\rangle$$
$$|1\rangle^{\mathbb{H}^A} \otimes |1\rangle^{\mathbb{H}^B} = |11\rangle = |3\rangle$$

Any $\Psi \in \mathbb{H}^A \otimes \mathbb{H}^B$ can be written as

$$\Psi = \Psi_{00}|00\rangle + \Psi_{01}|01\rangle + \Psi_{10}|10\rangle + \Psi_{11}|11\rangle$$

and we can represent it as a matrix in $\mathbb{C}^{2\times 2}$ or as a vector in $\mathbb{C}^4$

$$\begin{pmatrix} \Psi_{00} & \Psi_{01} \\ \Psi_{10} & \Psi_{11} \end{pmatrix} \rightsquigarrow \begin{pmatrix} \Psi_{00} \\ \Psi_{01} \\ \Psi_{10} \\ \Psi_{11} \end{pmatrix}$$

With this correspondence we have

$$|00\rangle \rightsquigarrow \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |01\rangle \rightsquigarrow \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle \rightsquigarrow \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle \rightsquigarrow \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

So if you read x_1x_0 of $|x_1x_0\rangle$ as a binary number $x = 2x_1 + x_0$ we get $|x_1x_0\rangle \rightsquigarrow e_{(x+1)}$

Def (computational basis of n-fold tensor product of qubit system)

Given $\mathbb{H}^n = \underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ times}}$ with $\dim \mathbb{H}^n = 2^n$

The **COMPUTATIONAL BASIS** of $\mathbb{H}^n$ is defined as

$$\{|s\rangle\}_{s \in \{0,1\}^n} \quad \text{where} \quad s = (x_{n-1} \dots x_1 x_0), \; x_i \in \{0,1\}$$

$$\text{and} \quad |s\rangle = |x_{n-1}\rangle \otimes \dots \otimes |x_1\rangle \otimes |x_0\rangle$$

The computational basis is an ONB (prove it by induction)

Notation Given $s = (x_{n-1} \dots x_1 x_0)$ we let $s_{base\,2} = \sum_{i=0}^{n-1} 2^i x_i$

Given $x \in \{0, 1, \dots, 2^n - 1\}$ we let $|x\rangle^n \in \mathbb{H}^n$

$|x\rangle = |s\rangle$ where $x = s_{base\,2} = \sum_{i=0}^{n-1} 2^i x_i$ (only used to specify the size of the system)

Example $|6\rangle^3 = |110\rangle \in \mathbb{H}^3$

$|6\rangle^4 = |0110\rangle \in \mathbb{H}^4$

Another basis in $\mathbb{H}^2$ is the **BELL BASIS**, given by the following vectors:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Ex Check $\langle \Phi^+ | \Phi^+ \rangle = 1$

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

States and Observables for composite systems

Postulate Given systems represented by $\mathbb{H}^A$, $\mathbb{H}^B$, the composite system is represented by $\mathbb{H}^A \otimes \mathbb{H}^B$

(pure) states are represented by $|\psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ with $\||\psi\rangle\| = 1$

mixed states are $\rho \in \mathcal{D}(\mathbb{H}^A \otimes \mathbb{H}^B)$, ie:

- $\rho : \mathbb{H}^A \otimes \mathbb{H}^B \longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B$ linear
- $\rho = \rho^*$
- $\rho \geq 0$ $\quad (\sigma(\rho) \subseteq [0, +\infty))$
- $\mathrm{Tr}(\rho) = 1$

Example $\rho \in \mathcal{D}(\mathbb{H}^n)$ can be written as $\rho = \sum_{s,s' \in \{0,1\}^n} \rho_{ss'} |s\rangle\langle s'|$ with density matrix $(\rho_{ss'}) \in \mathbb{C}^{2^n \times 2^n}$

$|\psi\rangle = |00\rangle \in \mathbb{H}^2$ is a pure state. In this case the reduced states on each qubit are $|0\rangle$ and $|0\rangle$

If $|\psi\rangle = |\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$, the reduced states are not clear.

We're tempted to say that the reduced state is the pure state $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ but the correct interpretation is actually the mixed state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

Consider this special case for an observable on $\mathcal{H}^A \otimes \mathcal{H}^B$

Let $M_A : \mathcal{H}^A \longrightarrow \mathcal{H}^A$ self-adjoint and $M_B : \mathcal{H}^B \longrightarrow \mathcal{H}^B$ self-adjoint

We can define $M_A \otimes M_B : \mathcal{H}^A \otimes \mathcal{H}^B \longrightarrow \mathcal{H}^A \otimes \mathcal{H}^B$

$$|\psi\rangle \otimes |\varphi\rangle \rightsquigarrow |M_A \psi\rangle \otimes |M_B \varphi\rangle$$

We should verify that this is a well defined linear map, which is left as an exercise

Let's check that it is indeed an observable on $\mathcal{H}^A \otimes \mathcal{H}^B$, ie that it's self-adjoint

$$\begin{aligned} \langle \eta \otimes \xi \,|\, M_A \otimes M_B \, \varphi \otimes \psi \rangle^{\mathcal{H}^A \otimes \mathcal{H}^B} &= \langle \eta \,|\, M_A \varphi \rangle^{\mathcal{H}^A} \langle \xi \,|\, M_B \psi \rangle^{\mathcal{H}^B} \\ &= \langle M_A \eta \,|\, \varphi \rangle^{\mathcal{H}^A} \langle M_B \xi \,|\, \psi \rangle^{\mathcal{H}^B} \\ &= \langle M_A \otimes M_B \, \eta \otimes \xi \,|\, \varphi \otimes \psi \rangle^{\mathcal{H}^A \otimes \mathcal{H}^B} \end{aligned}$$

<u>Rmk</u> If $\{|e_i\rangle\}$ ONB for $\mathcal{H}^A$ and $\{|f_j\rangle\}$ ONB for $\mathcal{H}^B$ then $\{|e_i \otimes f_j\rangle\}$ is an ONB for $\mathcal{H}^A \otimes \mathcal{H}^B$

On this basis, $M_A \otimes M_B$ is represented by a matrix in $\mathbb{C}^{(n_A n_B) \times (n_A n_B)}$ given by the Kronecker product of the two matrices representing M_A and M_B

These two matrices are $\left(\langle e_i | M_A e_k \rangle\right)_{i,k=1,\dots,n_A} = \left(M^A_{ik}\right)_{ik} \in \mathbb{C}^{n_A \times n_A}$

$$\left(\langle f_j | M_B f_\ell \rangle\right)_{j,\ell=1,\dots,n_B} = \left(M^B_{j\ell}\right)_{j\ell} \in \mathbb{C}^{n_B \times n_B}$$

and the Kronecker product is defined as

$$\left(\begin{array}{c|c|c} M^A_{11} \cdot M^B & \dots & M^A_{1 n_A} M^B \\ \hline \vdots & & \vdots \\ \hline M^A_{n_A 1} \cdot M^B & \dots & M^A_{n_A n_A} M^B \end{array}\right) \in \mathbb{C}^{(n_A n_B) \times (n_A n_B)}$$

Example let $\mathcal{H}^A = \mathcal{H}^B = \mathbb{C}^2$ $\quad (\mathcal{H}^A \otimes \mathcal{H}^B = \mathbb{C}^2 \otimes \mathbb{C}^2)$

then $\sigma_x \otimes \sigma_x = \left(\begin{array}{cc|cc} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array}\right)$ and it act as

$\sigma_x \otimes \sigma_x |00\rangle \rightsquigarrow |11\rangle$
$\sigma_x \otimes \sigma_x |01\rangle \rightsquigarrow |10\rangle$
$\sigma_x \otimes \sigma_x |10\rangle \rightsquigarrow |01\rangle$
$\sigma_x \otimes \sigma_x |11\rangle \rightsquigarrow |00\rangle$

Also $\sigma_x \otimes \sigma_z = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{array}\right)$ which acts as

$\sigma_x \otimes \sigma_z |00\rangle \rightsquigarrow |10\rangle$
$\sigma_x \otimes \sigma_z |01\rangle \rightsquigarrow -|11\rangle$
$\sigma_x \otimes \sigma_z |10\rangle \rightsquigarrow |00\rangle$
$\sigma_x \otimes \sigma_z |11\rangle \rightsquigarrow -|01\rangle$

In general $\left(M^A \otimes M^B\right)_{(i,j)(k,\ell)} = \langle e_i \otimes f_j \,|\, M_A \otimes M_B \, e_k \otimes f_\ell \rangle$

$= \langle e_i | M^A e_k \rangle \langle f_j | M^B f_\ell \rangle$

$= M^A_{ik} \cdot M^B_{j\ell}$

where these indices are actually meant as $(i-1)n_B + j$, $(k-1)n_B + \ell$

We can check that the two observables $\sigma_x \otimes \sigma_x$ and $\sigma_z \otimes \sigma_z$ commute

$$(\sigma_x \otimes \sigma_x)(\sigma_z \otimes \sigma_z)|\varphi \otimes \psi\rangle = (\sigma_x \otimes \sigma_x)\big|(\sigma_z \varphi) \otimes (\sigma_z \psi)\big\rangle$$
$$= \big|(\sigma_x \sigma_z \varphi) \otimes (\sigma_x \sigma_z \psi)\big\rangle = (\sigma_x \sigma_z) \otimes (\sigma_x \sigma_z)|\varphi \otimes \psi\rangle$$
$$(\sigma_z \otimes \sigma_z)(\sigma_x \otimes \sigma_x)|\varphi \otimes \psi\rangle = (\sigma_z \otimes \sigma_z)\big|(\sigma_x \varphi) \otimes (\sigma_x \psi)\big\rangle$$
$$= \big|(\sigma_z \sigma_x \varphi) \otimes (\sigma_z \sigma_x \psi)\big\rangle = (\sigma_z \sigma_x) \otimes (\sigma_z \sigma_x)|\varphi \otimes \psi\rangle$$

Now $\sigma_x \sigma_z \neq \sigma_z \sigma_x$ but because $\sigma_x \sigma_z = -i\sigma_y$ and $\sigma_z \sigma_x = i\sigma_y$ we get $(\sigma_x \otimes \sigma_x)(\sigma_z \otimes \sigma_z) = (-i\sigma_y) \otimes (-i\sigma_y) = (i\sigma_y) \otimes (i\sigma_y) =$

$$= (\sigma_z \otimes \sigma_z)(\sigma_x \otimes \sigma_x)$$

Because they commute they can be simultaneously diagonalized

and in fact the basis that diagonalizes them both is Bell's basis, which is composed of eigenvectors of both

The eigenvalues are

$$(\sigma_x \otimes \sigma_x)|\Phi^\pm\rangle = \frac{\sigma_x\otimes\sigma_x|00\rangle \pm \sigma_x\otimes\sigma_x|11\rangle}{\sqrt{2}} =$$

$$= \frac{|11\rangle \pm |00\rangle}{\sqrt{2}} = \pm|\Phi^\pm\rangle$$ (meaning + for $|\Phi^+\rangle$ and − for $|\Phi^-\rangle$)

$$(\sigma_z \otimes \sigma_z)|\Phi^\pm\rangle = \frac{\sigma_z\otimes\sigma_z|00\rangle \pm \sigma_z\otimes\sigma_z|11\rangle}{\sqrt{2}} =$$

$$= \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} = |\Phi^\pm\rangle$$

$$(\sigma_x \otimes \sigma_x)|\Psi^\pm\rangle = \frac{\sigma_x\otimes\sigma_x|01\rangle \pm \sigma_x\otimes\sigma_x|10\rangle}{\sqrt{2}} =$$

$$= \frac{|10\rangle \pm |01\rangle}{\sqrt{2}} = \pm|\Psi^\pm\rangle$$ (meaning + for $|\Psi^+\rangle$ and − for $|\Psi^-\rangle$)

$$(\sigma_z \otimes \sigma_z)|\Psi^\pm\rangle = \frac{\sigma_z\otimes\sigma_z|01\rangle \pm \sigma_z\otimes\sigma_z|10\rangle}{\sqrt{2}} =$$

$$= \frac{-|01\rangle \mp |10\rangle}{\sqrt{2}} = -|\Psi^\pm\rangle$$

Basically, by measuring $(\sigma_x \otimes \sigma_x)$ and $(\sigma_z \otimes \sigma_z)$, because they commute, you can determine the state you're in by

$\sigma_z\otimes\sigma_z$ \ $\sigma_x\otimes\sigma_x$	$+1$	-1
$+1$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$
-1	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$

<u>Rmk</u> by the postulates the expectation of $M_A \otimes M_B$ on the mixed state $\rho \in D(\mathcal{H}^A \otimes \mathcal{H}^B)$ is $\mathrm{Tr}((M_A \otimes M_B)\rho)$

If we represent ρ with a density matrix with respect to an ONB $\{|e_i \otimes f_j\rangle\}_{\substack{i=1\dots n_A \\ j=1\dots n_B}}$, then

$$\mathrm{Tr}\left(M_A \otimes M_B \rho\right) = \sum_{\substack{i=1\dots n_A \\ j=1\dots n_B}} \langle e_i \otimes f_j | M_A \otimes M_B \rho\, e_i \otimes f_j \rangle =$$

$$= \sum_{i,j} \langle M_A e_i \otimes M_B f_j \,|\, \sum_{k,\ell} |e_k \otimes f_\ell\rangle \rho_{(k,\ell)(i,j)} \rangle$$

$$= \sum_{i,j,k,\ell} \langle M_A e_i \otimes M_B f_j \,|\, e_k \otimes f_\ell \rangle \rho_{(k,\ell)(i,j)}$$

$$\rho_{(k,\ell)(i,j)} = \langle e_k \otimes f_\ell \,|\, \rho\, e_i \otimes e_j \rangle$$

$$= \sum_{i,j,k,\ell} \langle M_A e_i | e_k \rangle \langle M_B f_j | f_\ell \rangle \rho_{(k,\ell)(i,j)}$$

If for example we take $M_B = \mathbb{1}_B$ (identity on $\mathcal{H}^B$) we get

$$\mathrm{Tr}\left(M_A \otimes \mathbb{1}_B \rho\right) = \sum_{i,j,k,\ell} \langle M_A e_i | e_k \rangle \delta_{j\ell} \rho_{(k,\ell)(i,j)}$$

$$= \sum_{i,k=1}^{n_A} \langle M_A e_i | e_k \rangle \underbrace{\sum_{j=1}^{n_B} \rho_{(k,j)(i,j)}}$$

Notice that $\mathrm{Tr}(\rho) = \sum_{i=1}^{n_A} \sum_{j=1}^{n_B} \rho_{(i,j)(i,j)}$. We can define the partial trace on B as the matrix given by $\left(\mathrm{Tr}^B(\rho)\right)_{i,k} = \sum_{j=1}^{n_B} \rho_{(i,j)(k,j)}$ and analogously $\left(\mathrm{Tr}^A(\rho)\right)_{j,\ell} = \sum_{i=1}^{n_A} \rho_{(i,j)(i,\ell)}$

Def Let $M: \mathcal{H}^A \otimes \mathcal{H}^B \longrightarrow \mathcal{H}^A \otimes \mathcal{H}^B$ linear operator. We define the

PARTIAL TRACE on B, $\mathrm{Tr}^B(M): \mathcal{H}^A \longrightarrow \mathcal{H}^B$ as the only linear operator $L^A: \mathcal{H}^A \longrightarrow \mathcal{H}^A$ that satisfies

$$\mathrm{Tr}(K L^A) = \mathrm{Tr}\left((K \otimes \mathbb{1}_B) M\right) \qquad \forall\, K: \mathcal{H}^A \longrightarrow \mathcal{H}^A$$

Similarly $\mathrm{Tr}^A(M): \mathcal{H}^B \longrightarrow \mathcal{H}^B$

Explicitly, repeating the same calculations we've just done, given $\{|e_i \otimes f_j\rangle\}_{\substack{i=1\dots n_A \\ j=1\dots n_B}}$ ONB we get

$$Tr^A(M) = \sum_{i,k=1}^{n_A} |e_i\rangle\langle e_k| \left(\sum_{j=1}^{n_B} \underbrace{\langle e_i \otimes f_j | M e_k \otimes f_j \rangle}_{= M_{(i,j)(k,j)}} \right)$$

$$Tr^B(M) = \sum_{j,l=1}^{n_B} |f_j\rangle\langle f_l| \left(\sum_{i=1}^{n_A} \langle e_i \otimes f_j | M e_i \otimes f_l \rangle \right)$$

Note that if L^A and $\tilde{L}^A$ are such that $Tr(KL^A) = Tr(K\tilde{L}^A)$ $\forall K$ then $Tr(K(L^A - \tilde{L}^A)) = 0$ $\forall K$.

Because $(K, C) \rightsquigarrow Tr(K \cdot C)$ defines a scalar product (Frobenius)

$Tr(K(L^A - \tilde{L}^A)) = 0$ $\forall K$ $\Rightarrow$ $L^A = \tilde{L}^A$

Properties for Tr^A but equivalently for Tr^B with few changes

(1) Linearity: $Tr^A(M + \lambda N) = Tr^A(M) + \lambda Tr^A(N)$ $\quad \forall M, N \ \forall \lambda \in \mathbb{C}$

More generally $Tr^A((\mathbb{1}_A \otimes K)M) = K\, Tr^A(M)$ $\quad \forall K : \mathcal{H}^B \to \mathcal{H}^B$

(2) If M is self-adjoint and non negative, then $Tr^A(M)$ is also self-adjoint and non negative

(3) $Tr(Tr^A(M)) = Tr(M)$

Proof pick $K = \mathbb{1}_B$, then...

In particular, given $\rho \in \mathcal{D}(\mathcal{H}^A \otimes \mathcal{H}^B)$ we have $Tr^A(\rho) = \rho^B \in \mathcal{D}(\mathcal{H}^B)$ and $Tr^B(\rho) = \rho^A \in \mathcal{D}(\mathcal{H}^A)$, which are called REDUCED density operators (from ρ)

Ex Prove that if $M : \mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C \to \mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C$, then $Tr^{AB}(M) = Tr^A Tr^B(M)$, where $Tr^{AB}(M)$ means interpreting

⋮

$\mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C$ as $(\mathcal{H}^A \otimes \mathcal{H}^B) \otimes \mathcal{H}^C$

Ex Prove that if $U^B : \mathcal{H}^B \longrightarrow \mathcal{H}^B$ is unitary then

$$Tr^B(M) = Tr^B\left((\mathbb{1}_A \otimes U^B) M (\mathbb{1}_A \otimes U^B)^*\right) \quad \forall M$$

Question is $Tr^A(U)$ unitary if $U : \mathcal{H}^A \otimes \mathcal{H}^B \to \mathcal{H}^A \otimes \mathcal{H}^B$ is unitary?

Ex In the same setting as before, ie $\mathcal{H}^A = \mathcal{H}^B = \mathbb{C}^2$

compute $Tr^B(|\Phi^+\rangle\langle\Phi^+|)$

Sol $Tr^B(|\Phi^+\rangle\langle\Phi^+|) = Tr^B\left(\frac{(|00\rangle + |11\rangle)}{\sqrt{2}} \frac{(\langle 00| + \langle 11|)}{\sqrt{2}}\right) =$

$$= \frac{1}{2}\left[Tr^B(|00\rangle\langle 00|) + Tr^B(|00\rangle\langle 11|) + Tr^B(|11\rangle\langle 00|) + Tr^B(|11\rangle\langle 11|)\right] =$$

$$= \frac{1}{2}\left[|0\rangle\langle 0| + |1\rangle\langle 1|\right] = \frac{1}{2}\mathbb{1}_A$$ which is not a pure state !

28/10

Entanglement

As we know, given the systems $\mathcal{H}^A$ and $\mathcal{H}^B$ we can create the composite system $\mathcal{H}^A \otimes \mathcal{H}^B$

If we take two states $|\varphi\rangle \in \mathcal{H}^A$ and $|\psi\rangle \in \mathcal{H}^B$ we can obtain the state $|\varphi\rangle \otimes |\psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ but not every state in $\mathcal{H}^A \otimes \mathcal{H}^B$ can be represented as $|\varphi\rangle \otimes |\psi\rangle$ for some $|\varphi\rangle \in \mathcal{H}^A$ and $|\psi\rangle \in \mathcal{H}^B$

Example Bell's states in a two-qubit system $\mathcal{H}^A \cong \mathcal{H}^B \cong \mathbb{C}^2$

For example take $|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \in \mathcal{H}^A \otimes \mathcal{H}^B$ and suppose $\exists |\varphi\rangle \in \mathcal{H}^A$, $|\psi\rangle \in \mathcal{H}^B$ st $|\varphi\rangle \otimes |\psi\rangle = |\Phi^+\rangle$

We can write with respect to the computational basis and get

$|\varphi\rangle = \varphi_0|0\rangle + \varphi_1|1\rangle, \qquad |\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$

So $|\varphi\rangle \otimes |\psi\rangle$ becomes

$$|\varphi\rangle \otimes |\psi\rangle = \varphi_0\psi_0|00\rangle + \varphi_0\psi_1|01\rangle + \varphi_1\psi_0|10\rangle + \varphi_1\psi_1|11\rangle$$

and impose $|\varphi\rangle \otimes |\psi\rangle = |\Phi^+\rangle$ becomes equivalent to

$$\begin{cases} \varphi_0\psi_0 = \varphi_1\psi_1 = 1/\sqrt{2} \\ \varphi_0\psi_1 = \psi_1\varphi_0 = 0 \end{cases}$$ which has no solution

Def A state in $\mathbb{H}^A \otimes \mathbb{H}^B$ which can be written as $|\varphi\rangle \otimes |\psi\rangle$ with $|\varphi\rangle \in \mathbb{H}^A$, $|\psi\rangle \in \mathbb{H}^B$ is called a **SEPARABLE** state otherwise it is called an **ENTANGLED** state

Rmk If $|\Psi\rangle = |\varphi\rangle \otimes |\psi\rangle$, then (by looking at it as a mixed state) $\rho_\Psi = |\Psi\rangle\langle\Psi| = (|\varphi\rangle \otimes |\psi\rangle)(\langle\varphi| \otimes \langle\psi|) =$

$$= (|\varphi\rangle\langle\varphi|)(|\psi\rangle\langle\psi|)$$

Def Let $\rho \in \mathcal{D}(\mathbb{H}^A \otimes \mathbb{H}^B)$ be a mixed state on a composite system. ρ is called **SEPARABLE** if it can be written as

$$\rho = \sum_{j \in I} p_j \rho_j^{(A)} \otimes \rho_j^{(B)} \qquad \text{with } \sum_{j \in I} p_j = 1, \ \rho_j^{(A)} \in \mathcal{D}(\mathbb{H}^A), \ \rho_j^{(B)} \in \mathcal{D}(\mathbb{H}^B)$$

Otherwise it's called **ENTANGLED**

Th The definitions of separable/entangled for pure states and for mixed states are consistent

Examples (on a two-qubit system)

- Bell's states are entangled

⋮

- $|\Psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ is separable, as it holds $|\Psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Notation If $\rho \in \mathcal{D}(\mathcal{H}^A \otimes \mathcal{H}^B)$ we denote $\rho^B := Tr^A(\rho) \in \mathcal{D}(\mathcal{H}^B)$ and

$$\rho^A := Tr^B(\rho) \in \mathcal{D}(\mathcal{H}^A)$$

Th Let $|\Psi\rangle$ be a pure state on a composite system $\mathcal{H}^A \otimes \mathcal{H}^B$
Then $|\Psi\rangle$ is separable if and only if both $\rho^A(|\Psi\rangle)$ and $\rho^B(|\Psi\rangle)$ are pure states

$\rho^A(|\Psi\rangle)$ meaning "the partial trace on B on the density matrix we get interpreting $|\Psi\rangle$ as a mixed state"

Example We can apply this criteria to $|\Phi^+\rangle$

We saw that $\rho^A(\rho_{\Phi^+}) = Tr^B(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

Recall that if $|\Psi\rangle = \sum_{a,b} \Psi_{a,b} |e_a\rangle \otimes |f_b\rangle$ ONB on $\mathcal{H}^A \otimes \mathcal{H}^B$
Then $\rho^A(|\Psi\rangle) = \sum_{a_1,a_2,b} \Psi_{a_1,b} \overline{\Psi}_{a_2,b} |e_{a_1}\rangle\langle e_{a_2}|$ is a way to compute the trace

So $\rho^A(|\Phi^+\rangle) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}\mathbb{1}$, and we know that a mixed state ρ is pure iff $\rho^2 = \rho$. but $\left(\frac{1}{2}\mathbb{1}\right)^2 = \frac{1}{4}\mathbb{1} \neq \frac{1}{2}\mathbb{1}$

So $\rho^A(|\Phi^+\rangle)$ is not pure which proves (again) that $|\Phi^+\rangle$ is entangled

Consider now the composite system $\mathcal{H}^{ABCD} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C \otimes \mathcal{H}^D$ with $\mathcal{H}^A \cong \mathcal{H}^B \cong \mathcal{H}^C \cong \mathcal{H}^D \cong \mathbb{C}^2$ qubits $\left(\mathcal{H}^{ABCD} \cong \mathbb{C}^{2^4}\right)$

We can prepare $\mathcal{H}^{ABCD}$ in the state $|\Phi\rangle$ defined as

$|\phi\rangle = |\psi^-\rangle^{AB} \otimes |\psi^-\rangle^{CD}$, where $|\psi^-\rangle^{AB} = \frac{|01\rangle^{AB} - |10\rangle^{AB}}{\sqrt{2}}$

$$|\psi^-\rangle^{CD} = \frac{|01\rangle^{CD} - |10\rangle^{CD}}{\sqrt{2}}$$

Ex show that $|\phi\rangle = \frac{1}{2}(|0101\rangle - |1001\rangle - |0110\rangle + |1010\rangle)$

$$= \frac{1}{2}\left(|\psi^+\rangle^{AD} \otimes |\psi^+\rangle^{BC} - |\psi^-\rangle^{AD} \otimes |\psi^-\rangle^{BC} - \right.$$
$$\left. - |\Phi^+\rangle^{AD} \otimes |\Phi^+\rangle^{BC} + |\Phi^-\rangle^{AD} \otimes |\Phi^-\rangle^{BC}\right)$$

For instance $|\psi^+\rangle^{AD} \otimes |\psi^+\rangle^{BC} = \frac{|01\rangle^{AD} + |10\rangle^{AD}}{\sqrt{2}} \otimes \frac{|01\rangle^{BC} + |10\rangle^{BC}}{\sqrt{2}} =$

$$= \frac{1}{2}(|0011\rangle + |0101\rangle + |1010\rangle + |1100\rangle)$$

We can define the two following observables

$$\Sigma_z = \mathbb{1} \otimes \sigma_z \otimes \sigma_z \otimes \mathbb{1}, \quad \Sigma_x = \mathbb{1} \otimes \sigma_x \otimes \sigma_x \otimes \mathbb{1}$$

We saw that on a 2-qubit system $(\sigma_x \otimes \sigma_x)$ and $(\sigma_z \otimes \sigma_z)$ commute so one can strongly trust me when I tell you that Σ_x and Σ_z commute. Recall that measuring $(\sigma_x \otimes \sigma_x)$ and $(\sigma_z \otimes \sigma_z)$ allowed us to prepare one of the Bell's states (depending on which combination of eigenvalue we measured). We can do the same with Σ_x and Σ_z. By measuring Σ_x and Σ_z we can determine whether $\mathcal{H}^{BC}$ is in $|\Phi^\pm\rangle^{BC}$ or $|\psi^\pm\rangle^{BC}$ and given the decomposition of $|\phi\rangle$ given by the exercise this will tell us the state of $\mathcal{H}^{AD}$ For example, if we measure $+1, +1$, we know $\mathcal{H}^{BC}$ is in $|\Phi^+\rangle^{BC}$ so $\mathcal{H}^{ABCD}$ is in $|\Phi^+\rangle^{AD} \otimes |\Phi^+\rangle^{BC}$ (by the decomposition) which means the subsystem $\mathcal{H}^{AD}$ is in the entangled state $|\Phi^+\rangle^{AD}$

We started with an entangled state where the entanglement was between A and B and between C and D. We then measured

a subsistem and produced seemingly out of nowhere an entanglement on the untouched subsystem! This is sometimes called ENTANGLEMENT SWAPPING

Quantum copier

The idea is that we'd like to be able to duplicate qubit values just like we're used to copy bit values.

Formally, a quantum copier is an operator $K: \mathbb{H} \otimes \mathbb{H} \longrightarrow \mathbb{H} \otimes \mathbb{H}$ for a fixed state $|\omega\rangle \in \mathbb{H}$, such that $K|\varphi\rangle \otimes |\omega\rangle = |\varphi\rangle \otimes |\varphi\rangle$ $\forall |\varphi\rangle \in \mathbb{H}$ (ie given a prepared $|\omega\rangle$ and any state $|\varphi\rangle$, it copies $|\varphi\rangle$ on the second subsystem)

Th (no cloning theorem)

There is no quantum copier

Proof On a 2-qubit system ($\mathbb{H} \cong \mathbb{C}^2$) fix $|\omega\rangle \in \mathbb{H}$

PA ↯ $\exists K: \mathbb{H} \otimes \mathbb{H} \longrightarrow \mathbb{H} \otimes \mathbb{H}$ quantum copier

Then we would get

$$K(|0\rangle \otimes |\omega\rangle) = |0\rangle \otimes |0\rangle = |00\rangle$$

$$K(|1\rangle \otimes |\omega\rangle) = |1\rangle \otimes |1\rangle = |11\rangle$$

By applying K on $\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\omega\rangle$ we should get

$$K\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |\omega\rangle\right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

by the copying property, but also

$$K\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |\omega\rangle\right) = \frac{1}{\sqrt{2}}\left(K(|0\rangle \otimes |\omega\rangle) + K(|1\rangle \otimes |\omega\rangle)\right)$$

$$= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad \text{by linearity}$$

So we get inconsistent results, which is absurd

↯

So there exist no quantum copier (on 2-qubit system. The generalisation is left as an exercise)

□

EPR States and Bell telephone

Suppose we have a system $\mathbb{H}^A \otimes \mathbb{H}^B$ given by Alice's qubit and Bob's qubit

Consider $|\Phi^+\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ which can be written as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_{\hat{z}}\rangle \otimes |\uparrow_{\hat{z}}\rangle + |\downarrow_{\hat{z}}\rangle \otimes |\downarrow_{\hat{z}}\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|\uparrow_{\hat{x}}\rangle \otimes |\uparrow_{\hat{x}}\rangle + |\downarrow_{\hat{x}}\rangle \otimes |\downarrow_{\hat{x}}\rangle\right)$$

Suppose Alice measures σ_z (meaning $\sigma_z^A \otimes \mathbb{1}^B$) on her qubit and gets 1. Then her qubit must be in state $|\uparrow_{\hat{z}}\rangle$ so Bob's qubit must be on $|\uparrow_{\hat{z}}\rangle$ even though he took no measurement

The same happens if Alice measures σ_x on her qubit

This concept of sending information instantly is at the base of the EPR paradox

We can use this mechanism to send information (Bell telephone). We can encode classical bits in this way: if Alice wants to send 0, Alice measures σ_z making Bob's qubit either $|0\rangle$ or $|1\rangle$. If Alice wants to send 1, Alice measures σ_x making Bob's qubit either $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ or $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. To distinguish in which case he is, Bob should measure repetedly σ_z to see if he gets always the same

result (meaning Alice also measured σ_z) or random results (meaning Alice measured σ_x), but to do so Bob should have multiple copies of that bit and we proved that that can't happen

Gates

In classical computing, transforming a state means modifying a finite sequence of 0 and 1 into another finite sequence of 0 and 1

Def An elementary classical **GATE** is a function $g: \{0,1\}^n \longrightarrow \{0,1\}$

A classical gate is a function $g: \{0,1\}^n \longrightarrow \{0,1\}^m$ composed of m elementary classical gates

Notation $\oplus$ is the addition mod 2

Ex Some famous examples of gates are:

- NOT,

x_1	out
0	1
1	0

which can be written as $\text{NOT}(x_1) = 1 \oplus x_1$

- AND: $\{0,1\}^2 \longrightarrow \{0,1\}$,

x_1	x_2	0
0	0	0
0	1	0
1	0	0
1	1	1

so $\text{AND}(x_1, x_2) = x_1 x_2$

- XOR: $\{0,1\}^2 \longrightarrow \{0,1\}$

x_1	x_2	0
0	0	0
0	1	1
1	0	1
1	1	0

so $\text{XOR}(x_1, x_2) = x_1 \oplus x_2$

- OR: $\{0,1\}^2 \longrightarrow \{0,1\}$ which is $\text{OR}(x_1, x_2) = x_1 \oplus x_2 \oplus (x_1 \cdot x_2)$

- TOFFOLI: $\{0,1\}^3 \longrightarrow \{0,1\}^3$

$$(x_1, x_2, x_3) \rightsquigarrow (x_1, x_2, x_1 x_2 \oplus x_3)$$

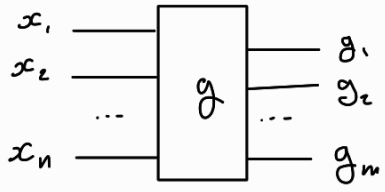
⋮

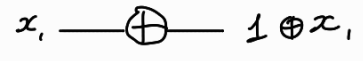
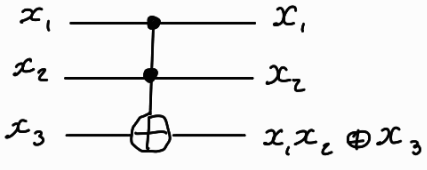
So with a truth table

x_1	x_2	x_3	o_1	o_2	o_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Interpreting $\{0,1\}^3$ as $\{0,\dots,7\}$ (ie as binary numbers), the TOFFOLI gate is the permutation $(6\ 7)$

Graphically we express a gate $g: \{0,1\}^n \to \{0,1\}^m$ as



but there are some special notations: the NOT gate is often written as  and the TOFFOLI gate is written as  where the black dot

means that we are applying the identity on that bit but also we're using it as a control bit to decide whether to apply the NOT gate on x_3: in fact, TOF is basically the NOT gate with control on x_1 and x_2

Def A gate is REVERSIBLE if the associated function is a bijection

Ex NOT and TOF are reversible but AND, XOR & OR aren't reversible

The notion of reversibility is particularly important in quantum computation because we know we can only apply unitary operators, so we cannot apply (for example) the AND gate
What we can do is add more auxiliary bits to get similar gates

Rmk $TOF(x_1, x_2, 0) = (x_1, x_2, x_1 x_2 \oplus 0) = (x_1, x_2, x_1 \text{ AND } x_2)$

$TOF(1, x_2, x_3) = (1, x_2, x_2 \oplus x_3) = (1, x_2, x_2 \text{ XOR } x_3)$

$TOF(1, 1, x_3) = (1, 1, 1 \oplus x_3) = (1, 1, \text{NOT } x_3)$

Other useful gates are:

- ID: $x_1 \rightsquigarrow x_1$
- FALSE: $x_1 \rightsquigarrow 0$
- TRUE: $x_1 \rightsquigarrow 1$
- COPY: $x_1 \rightsquigarrow (x_1, x_1)$

Let $g_1, \dots, g_k$ gates. We define $F(g_1, \dots, g_k)$ the set of gates that can be built using $g_1, \dots, g_k$ as building blocks, according to the following rules:

(1) $g_1, \dots, g_k \in F(g_1, \dots, g_k)$

(2) PADDING is allowed, where padding is defined as:

$$P^{(n)}_{y_1 \dots y_\ell, j_1, \dots, j_\ell} : \{0,1\}^n \longrightarrow \{0,1\}^{n+\ell}$$

$$(x_1, \dots, x_n) \rightsquigarrow (x_1, \dots, x_{j_1 - 1}, y_1, x_{j_1 + 1}, \dots)$$

ie: we insert y_1 in position j_1
y_2 in position j_2
$\vdots$

(3) restrictions and reorderings are allowed

$$r^{(n)}_{j_1 \dots j_\ell} : \{0,1\}^n \longrightarrow \{0,1\}^\ell \qquad \text{with } \ell \leq n \text{ and}$$
$$(x_1, \dots, x_n) \rightsquigarrow (x_{j_1}, \dots, x_{j_\ell}) \qquad j_1, \dots, j_\ell \text{ distinct}$$

(4) composition of gates is allowed

$$h_1, h_2 \in F(g_1, \dots, g_k) \Rightarrow h_1 \circ h_2 \in F(g_1, \dots, g_k)$$

(5) Cartesian products are allowed

$$\left.\begin{aligned} h_1 &: \{0,1\}^n \longrightarrow \{0,1\}^m \\ h_2 &: \{0,1\}^p \longrightarrow \{0,1\}^q \end{aligned}\right\} \in F(g_1, \dots, g_k)$$

$$\Rightarrow h_1 \times h_2 : \{0,1\}^{n+p} \longrightarrow \{0,1\}^{m+q} \in F(g_1, \dots, g_k)$$
$$(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+p}) \rightsquigarrow (h_1(x_1, \dots, x_n), h_2(x_{n+1}, \dots, x_{n+p}))$$

Ex $(ID \times ID \times XOR) \circ (ID \times ID \times AND \times ID) \circ r^{(5)}_{13245} \circ (COPY \times COPY \times ID)(x_1, x_2, x_3) =$

$= (ID \times ID \times XOR) \circ (ID \times ID \times AND \times ID) \circ r^{(5)}_{13245} (x_1, x_1, x_2, x_2, x_3) =$

$= (ID \times ID \times XOR) \circ (ID \times ID \times AND \times ID)(x_1, x_2, x_1, x_2, x_3) =$

$= (ID \times ID \times XOR)(x_1, x_2, x_1 \cdot x_2, x_3)$

$= (x_1, x_2, x_1 \cdot x_2 \oplus x_3)$

$= TOF(x_1, x_2, x_3)$

Def A set of gate $g_1, \dots, g_k$ is UNIVERSAL if $\forall g$ gate, $g \in F(g_1, \dots, g_k)$

Th The (classical) TOFFOLI gate is reversible and $\{TOFFOLI\}$ is universal

Def A **QUANTUM n-GATE** is a unitary operator

$$U : \mathbb{H}^{\otimes n} \longrightarrow \mathbb{H}^{\otimes n}$$

where $\mathbb{H} \cong \mathbb{C}^2$ is the Hilbert space of a single qubit

The n qubits on which we apply quantum gates form a **QUANTUM REGISTER**

Some examples of quantum gates on a qubit (unary) are:

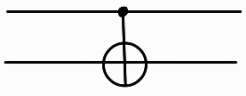
- ID — $\mathbb{1}$ — $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- Phase factor — M(α) — $e^{i\alpha}\mathbb{1}$ — $e^{i\alpha}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- Phase shift — P(α) — $|0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|$ — $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$
- QNOT (Paul: X) — X or ⊕ — $X = \sigma_x$ — $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

  This behaves "like a NOT" because $\sigma_x|0\rangle = |1\rangle$, $\sigma_x|1\rangle = |0\rangle$
- Pauli Y — Y — $Y = \sigma_y$ — $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
- Pauli Z — Z — $Z = \sigma_z$ — $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Hadamard — H — $H = \frac{\sigma_x + \sigma_z}{\sqrt{2}}$ — $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- Spin rotation — $D_{\hat{n}}(\alpha)$ — $D_{\hat{n}}(\alpha)$ — $\begin{pmatrix} \cdots & \cdots \\ \cdots & \cdots \end{pmatrix}$
- Measurement of observable A — A — λ

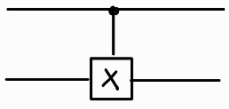
where λ indicates the measured value

Some examples of binary quantum gates are:

- CNOT (controlled not)



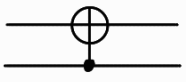
or



$$\Lambda^1(X) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$

as a matrix CNOT becomes $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

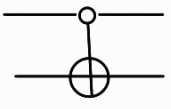
- quantum NOT controlled on the second qubit



$$\Lambda_1(X) = \mathbb{1} \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|$$

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

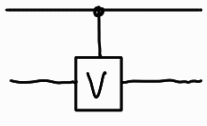
- CNOT controlling $|0\rangle$ instead of $|1\rangle$



$$\Lambda^{|0\rangle}(X) = |0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes \mathbb{1}$$

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

- In general if V is a unary gate we can write controlled-V as

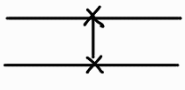


$$\Lambda^1(V) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes V$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & v_{11} & v_{12} \\ 0 & 0 & v_{12} & v_{22} \end{pmatrix} \quad \text{assuming } V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}$$

often used: controlled Hadamard, controlled phase multiplication, ...

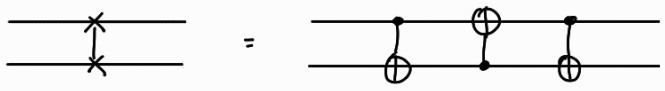
- SWAP



$$S = |00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|$$

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

The swap gate can be written as a composition of 3 CNOT



We can define rules for combining quantum gates:
given $U_1, \dots, U_k$ unitary, the set $F(U_1, \dots, U_k)$ of gates that can be obtained from $U_1, \dots, U_k$ is generated by:

(1) $U_1, \dots, U_k \in F(U_1, \dots, U_k)$

(2) $\mathbb{1}^{\otimes n} \in F(U_1, \dots, U_k)$

(3) $V_1, V_2 \in F(U_1, \dots, U_k) \Rightarrow V_1 V_2 \in F(U_1, \dots, U_k)$

(4) If $V_1, V_2 \in F(U_1, \dots, U_k)$ with $V_1 \in \mathcal{U}(\mathbb{H}^{\otimes n_1})$
$V_2 \in \mathcal{U}(\mathbb{H}^{\otimes n_2})$

$\Rightarrow \quad V_1 \otimes V_2 \in F(U_1, \dots, U_k)$

As before, $\{U_1, \dots, U_k\}$ is universal if any unitary operator on $\mathbb{H}^{\otimes n}$ belongs to $F(U_1, \dots, U_k)$

4/11

Th $\{ M(\alpha), D_{\hat{y}}(\beta), D_{\hat{z}}(\gamma), \Lambda^1(X) \}_{\alpha, \beta, \gamma \in \mathbb{R}}$ is universal

Ex Let's write $\Lambda^1(U)$ with $U \in \mathcal{U}(\mathbb{C}^2)$, and Q-TOFFOLI, in terms of the operators in the theorem

(i) Recall that any U can be decomposed as

$U = e^{i\alpha} A \sigma_x B \sigma_x C$ with $A = D_{\hat{z}}(\beta) D_{\hat{y}}(\gamma/2)$

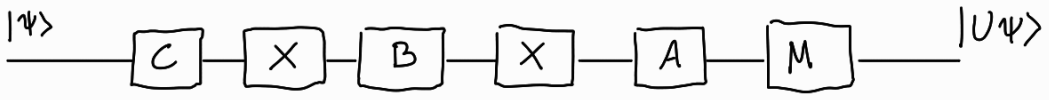
$B = D_{\hat{y}}(-\gamma/2) D_{\hat{z}}(-\frac{\delta+\beta}{2})$

$ABC = \mathrm{Id}$

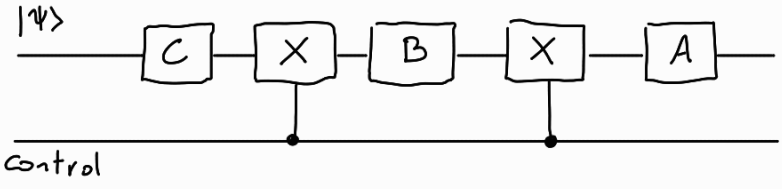
$C = D_{\hat{z}}(\frac{\delta-\beta}{2})$

Note that we can also build σ_x using a global phase so $\sigma_x \in F(\{M, D_{\hat{y}}, D_{\hat{z}}\})$, hence $\forall U \in \mathcal{U}(\mathbb{C}^2)$, $U \in F(M, D_{\hat{y}}, D_{\hat{z}})$

We have

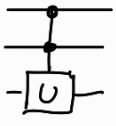


and we can modify the circuit as (ignoring the global phase given by M)



This acts as a controlled U because of the controlled X: if the control is 0, $ABC = Id$ so the target is unchanged if the control is 1, we get $|U\psi\rangle$. To get the correct phase we need a gate of partial phase $P(\alpha)$ which is explained in the book

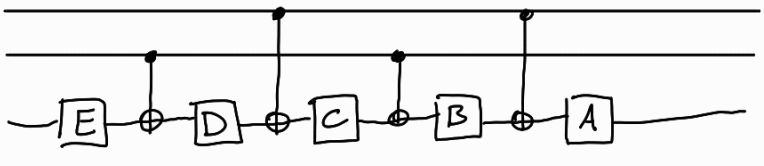
(ii) For the quantum toffoli, let's write any general controlled-controlled-U with $U \in \mathcal{U}(\mathbb{C}^2)$



One way is to generalise the decomposition of U as

$$U = E \times D \times C \times B \times A \quad \text{with} \quad \begin{aligned} EDXCBXA &= Id \\ EXDCXBA &= Id \\ EDCBA &= Id \end{aligned}$$

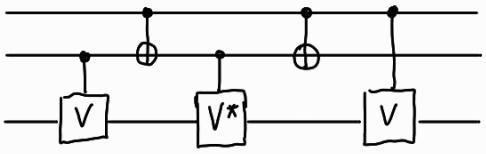
Then we can build



which would work for our case, but it relies on that decomposition which is complicated to prove. Another approach

is to find $V \in \mathcal{U}(\mathbb{C}^2)$ st $V^2 = U$ (which always exists for U unitary)

Then we can build



One can prove as an exercise that this circuit works as a Controlled-controlled-U

Circuits

There are three types of circuits

(i) a plain circuit is a circuit where the used register is composed only of input/output register $\mathbb{H}^{\otimes n} = \mathbb{H}^{I/O}$

(ii) a circuit with ancilla is a circuit where the register has some I/o qubits and some auxillary qubits $\mathbb{H}^{\otimes n} = \mathbb{H}^{I/O} \otimes \mathbb{H}^{\otimes m}$

(iii) composition of quantum circuits and classical operations

Def A **PLAIN CIRCUIT** is a composition of L "elementary" gates $U_1, \dots, U_L \in \mathcal{U}(\mathbb{H}^{I/O})$, which acts as $U = U_L \dots U_2 U_1$. It's said to be of **DEPTH** L and if the system is initially in state $\rho \in \mathcal{D}(\mathbb{H}^{I/O})$, after applying U we are in the state $U\rho U^*$

(pure state $|\psi\rangle$ becomes $U|\psi\rangle$)

Th Let $\mathbb{H}^{I/O}$, $\mathbb{H}^{W}$ be Hilbert spaces. Let $|\omega_i\rangle$, $|\omega_f\rangle$ be states in $\mathbb{H}^{W}$ and let $\hat{U} \in \mathcal{U}(\mathbb{H}^{I/O} \otimes \mathbb{H}^{W})$ st

$$\forall |\psi\rangle \in \mathbb{H}^{I/O} \quad \hat{U}(|\psi\rangle \otimes |\omega_i\rangle) = (U|\psi\rangle) \otimes |\omega_f\rangle$$

Then $|\psi\rangle \rightsquigarrow U|\psi\rangle$ is unitary on $\mathbb{H}^{I/O}$ and if $\rho \in \mathcal{D}(\mathbb{H}^{I/O})$

we have $U\rho U^* = Tr^W\left(\hat{U}\left(\rho \otimes (|w_i\rangle\langle w_i|)\right)\hat{U}^*\right)$

Ex: $M_A \in \mathcal{D}(\mathbb{H}^A)$, $M_B \in \mathcal{D}(\mathbb{H}^B)$
$\Rightarrow M_A \otimes M_B \in \mathcal{D}(\mathbb{H}^A \otimes \mathbb{H}^B)$

Dim $U(|\psi_1\rangle + |\psi_2\rangle) \longleftarrow \hat{U}(|\psi_1\rangle + |\psi_2\rangle) \otimes |w_i\rangle$

$= \hat{U}|\psi_1\rangle \otimes |w_i\rangle + \hat{U}|\psi_2\rangle \otimes |w_F\rangle$

$= (U|\psi_1\rangle) \otimes |w_F\rangle + (U|\psi_2\rangle) \otimes |w_F\rangle$

$U|\psi_1\rangle + U|\psi_2\rangle \longleftarrow (U|\psi_1\rangle + U|\psi_2\rangle) \otimes |w_F\rangle$

so U is a linear operator

$\|\hat{U}|\psi\rangle \otimes |w_i\rangle\|_{\mathbb{H}^{I/O} \otimes \mathbb{H}^W} = \|(U|\psi\rangle) \otimes |w_F\rangle\|_{\mathbb{H}^{I/O} \otimes \mathbb{H}^W}$

$= \|U|\psi\rangle\|_{\mathbb{H}^{I/O}} \underbrace{\||w_F\rangle\|_{\mathbb{H}^W}}_{=1}$

$= \||\psi\rangle \otimes |w_i\rangle\|_{\mathbb{H}^{I/O} \otimes \mathbb{H}^W}$

$= \||\psi\rangle\|_{\mathbb{H}^{I/O}} \cdot \underbrace{\||w_i\rangle\|_{\mathbb{H}^W}}_{=1}$

$= \||\psi\rangle\|_{\mathbb{H}^{I/O}}$

$= \|U|\psi\rangle\|_{\mathbb{H}^{I/O}}$

so U is also unitary

Finally given $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ with $p_j \geq 0$, $\sum p_j = 1$
and $\{\psi_j\}$ ONB, by linearity we have

$Tr^W\left(\hat{U}(\rho \otimes |w_i\rangle\langle w_i|)\hat{U}^*\right) = \sum_j p_j Tr^W\left(\hat{U}(|\psi_j\rangle\langle\psi_j| \otimes |w_i\rangle\langle w_i|)\hat{U}^*\right)$

so we need to prove the identity only on pure states

$Tr^W\left(\hat{U}\underbrace{(|\psi\rangle\langle\psi| \otimes |w_i\rangle\langle w_i|)}_{= (|\psi\rangle \otimes |w_i\rangle)(\langle\psi| \otimes \langle w_i|)}\hat{U}^*\right) =$ because $\hat{U}|\psi\rangle \otimes |w_i\rangle = (U|\psi\rangle) \otimes |w_F\rangle$

$= Tr^W\left(\left[(U|\psi\rangle) \otimes |w_F\rangle\right] \cdot \left[(\langle\psi|U^*) \otimes \langle w_F|\right]\right) =$

$\vdots$

$$= \mathrm{Tr}^{W}\left((U|\psi\rangle\langle\psi|U^*) \otimes |w_f\rangle\langle w_f| \right) =$$

$$= U|\psi\rangle\langle\psi|U^*$$

where in the last step we used the following general fact

Ex $\mathrm{Tr}^{B}(\rho_A \otimes \rho_B) = \rho_A$

so we get the identity we needed

□

Def A unitary $U \in \mathcal{U}(\mathbb{H}^{I/O})$ $(\mathbb{H}^{I/O} = \mathbb{H}^{\otimes n})$ is implemented by a quantum circuit **WITH ANCILLA SYSTEM** $\mathbb{H}^{W}$ and states $|w_i\rangle, |w_f\rangle \in \mathbb{H}^{W}$ if $\exists \hat{U}$ plain circuit on $\mathbb{H}^{I/O} \otimes \mathbb{H}^{W}$ such that $\forall |\psi\rangle \in \mathbb{H}^{I/O}$ $\hat{U}|\psi\rangle \otimes |w_i\rangle = (U|\psi\rangle) \otimes |w_f\rangle$

(or equivalently $U\rho U^* = \mathrm{Tr}\left(\hat{U}(\rho \otimes |w_i\rangle\langle w_i|)\hat{U}^* \right)$

Def Given $f : \mathbb{N} \to \mathbb{N}$ we write (for $n \geq 1$)

$$U_f : \mathbb{H}^n \otimes \mathbb{H}^n \longrightarrow \mathbb{H}^n \otimes \mathbb{H}^n$$
$$|x\rangle^n \otimes |y\rangle^n \rightsquigarrow |x\rangle^n \otimes |y \boxplus f(x)\rangle^n$$

where the n above the ket means we're interpreting x and y as string of bits and $\boxplus$ is the bitwise addition modulo 2

Formally, we map $y \rightsquigarrow s(y) \in \{0,1\}^n$

and for $a, b \in \{0,1\}^n$, $a \boxplus b = (a_i \oplus b_i)_{i=1}^{n}$

Ex if $f(x) = x$ we get $U_f = U_{\boxplus}$ which behaves as

$$|x\rangle \otimes |y\rangle \rightsquigarrow |x\rangle \otimes |x \boxplus y\rangle$$

We'll describe now a general structure for quantum algorithms:

1] Prepare the input $|\psi\rangle \in \mathbb{H}^{I/O}$ (usually with some entanglement)

2] Implement U_f for some (problem dependant) $f: \mathbb{N} \to \mathbb{N}$

3] Do some "clever transformations"

4] Measure/observe the output

Example

(1) Possible basic initialization: Input state: $|0\ldots0\rangle = |0\rangle^n$

Ancilla state: $|0\ldots0\rangle = |0\rangle^m$

Other possible initialization

entangled state (commonly used): $|\psi_0\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle^n$

we can generate this state by applying $H^{\otimes n}$ (tensor product of the Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$) to $|0\rangle^n$, because

$$H \otimes \ldots \otimes H \left(|0\rangle \otimes \ldots \otimes |0\rangle\right) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \ldots \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) =$$

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

If we then apply U_f that implements $f: \mathbb{N} \to \mathbb{N}$ we get

$$U_f\left(|\psi_0\rangle \otimes |0^n\rangle\right) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \boxplus |f(x)\rangle$$

so somehow we encoded (calculated) all the possible outputs of f at once, the problem is that it's not clear how to retrieve this information from this superposition

(4) An example of observable we can measure is

$\Sigma_z^j = \mathbb{1} \otimes \dots \otimes \mathbb{1} \otimes \sigma_z \otimes \mathbb{1} \otimes \dots \otimes \mathbb{1}$ which behaves as the identity on all cubits except on the j-th

if we have $j \neq j'$ we get $[\Sigma_z^j, \Sigma_z^{j'}] = 0$, ie they commute, so we can measure on a state $\rho \in \mathcal{D}(\mathcal{H}^n)$ all the Σ_z^j, $j = 1, \dots, n$ in any order and obtain a "binary" string in $\{1, -1\}^n$, which becomes an actual binary string with the mapping $1 \rightsquigarrow 0$, $-1 \rightsquigarrow 1$

By doing so we get a binary string s which represent a number $x \in \{0, \dots, 2^n - 1\}$ which tells us that the system is currently in state $|x\rangle^n$

9/11

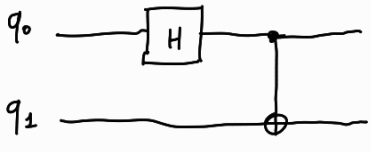
Corrections on 1

(1) Usually the state is initialized to $|0\rangle^n \in \mathcal{H}^{I/O}$ $|0\rangle^m \in \mathcal{H}^W$

We sometimes use the state $|\varphi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle^n$ which is NOT entangled, as it is separable

Ex] Let's produce an entangled state

Consider the following circuit U



Note: there's a bit of convention issue on which is the first q-bit and which is the second. We use the first q-bit on the top (same convention as qiskit)

Compute $U|00\rangle$, $U|01\rangle$, $U|10\rangle$

Sol $U|00\rangle = \Lambda^1(X)\, I \otimes H\, |00\rangle = \Lambda^1(X) \left(|0\rangle \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \right) =$

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

(2) We're looking for a unitary map $U_f : \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n} \longrightarrow \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$

$|a\rangle \otimes |b\rangle \rightsquigarrow |a\rangle \otimes |b \boxplus f(a)\rangle$

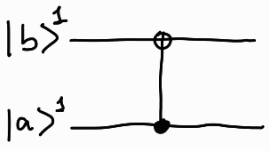
where $f : \mathbb{N} \to \mathbb{N}$

If we consider the special case $f = id$ we get

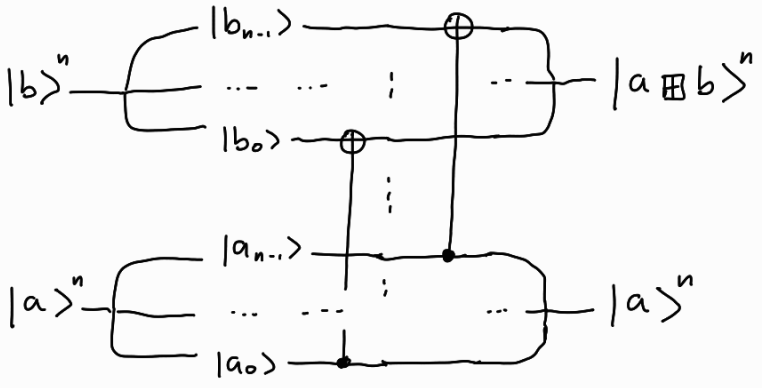
$U_{\boxplus} |a\rangle \otimes |b\rangle = |a\rangle \otimes |a \boxplus b\rangle$.

Let's see how we can implement this

$n = 1$



$n > 1$



Let's find $U_+ : \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n+1} \longrightarrow \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n+1}$ $\quad \forall a, b \in \{0, \dots, 2^n - 1\}$

$|a\rangle^n \otimes |b\rangle^{n+1} \rightsquigarrow |a\rangle^n \otimes |a + b\rangle^{n+1}$

Note that b could be bigger than $2^n - 1$ given the domain, but we ask that this holds only for $b \in \{0, \dots, 2^n - 1\}$

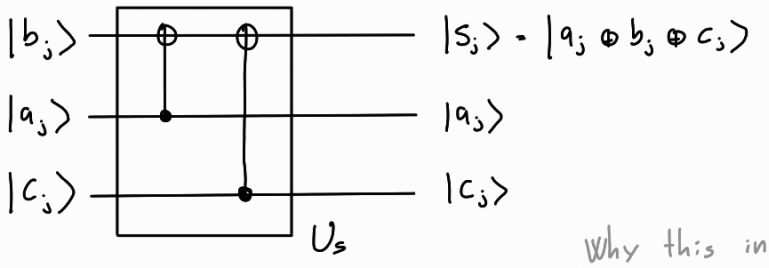
Let $a = \sum_{j=0}^{n-1} 2^j a_j$, $\quad b = \sum_{j=0}^{n-1} 2^j b_j$ with $a_j, b_j \in \{0, 1\}$

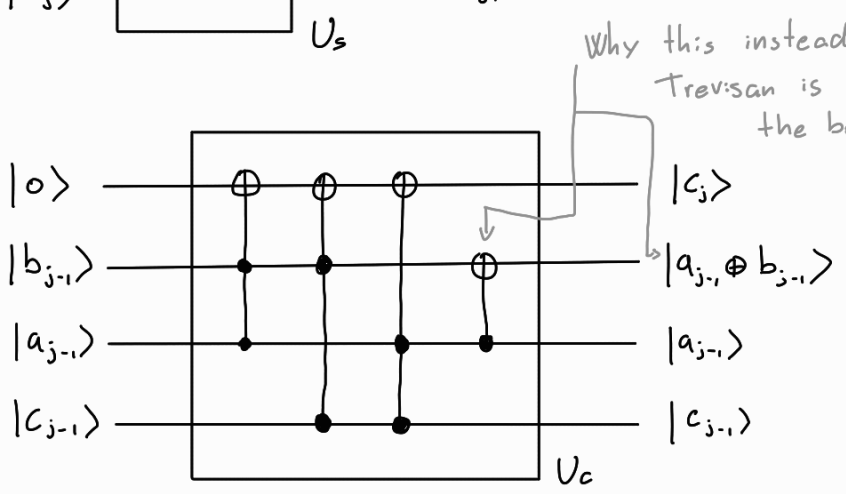
then $a + b = \sum_{j=0}^{n-1} 2^j s_j + 2^n c_n$ $\quad$ c_n is the carry digit

where $c_j = \begin{cases} 0 & \text{if } j = 0 \\ (a_{j-1} b_{j-1}) \oplus (a_{j-1} c_{j-1}) \oplus (b_{j-1} c_{j-1}) \end{cases}$ $\quad$ summation mod 2

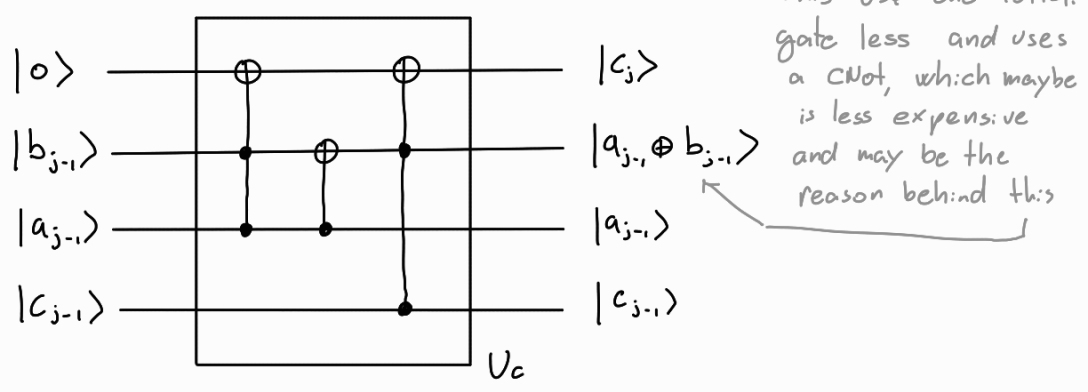
$s_j = a_j \oplus b_j \oplus c_j$

Let's implement this as a circuit



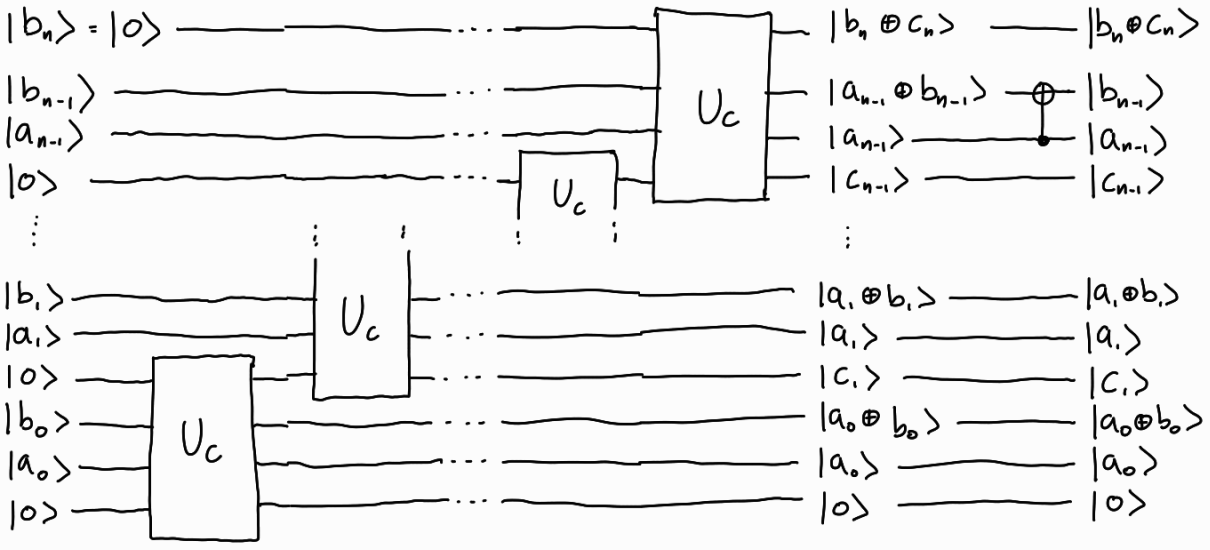


Alternative:

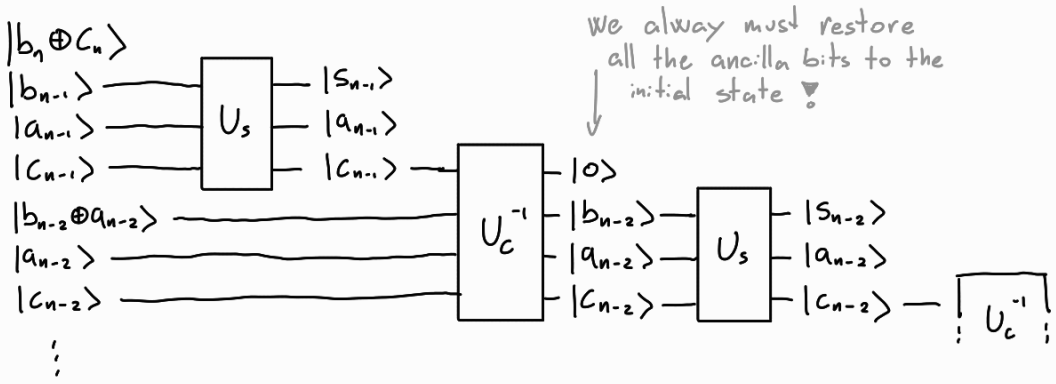


The whole circuit will become. The initial state will be $|b\rangle^{n+1} \otimes |a\rangle^n \otimes |0\rangle^n$ where $|0\rangle^n$ is an ancilla, but sorted this way

1st step



2nd step



The construction requires $O(n)$ elementary gates

Extensions

- $U_{+ \% N} \equiv U_{+ \bmod N} : \mathbb{H}^n \otimes \mathbb{H}^n \longrightarrow \mathbb{H}^n \otimes \mathbb{H}^n$
  $|a\rangle \otimes |b\rangle \rightsquigarrow |a\rangle^n \otimes |a+b \bmod N\rangle$

  $\forall a, b \in \{0, .., N-1\}$ provided that $2^n \geq N$

We can define $\mathbb{H}^{<N} \subseteq \mathbb{H}^{\otimes n}$ as $\mathrm{Span}\{|a\rangle^n : a \in \{0, \dots, N-1\}\}$
then $U_{+ \bmod N} : \mathbb{H}^{<N} \otimes \mathbb{H}^{<N} \longrightarrow \mathbb{H}^{<N} \otimes \mathbb{H}^{<N}$

- $U_{- \bmod N} = U_{+ \bmod N}^*$
- $U_{\cdot c \bmod N} : |a\rangle \otimes |b\rangle \rightsquigarrow |a\rangle \otimes |b + a \cdot c \bmod N\rangle$
- $U_{b^{\cdot} \bmod N} : |a\rangle \rightsquigarrow |b^a \bmod N\rangle$

Quantum Fourier Transform [se chapter 5.5.5]

Recall the Discrete/Finite Fourier Transform

$$F : \underset{\mathbb{C}^N}{(c_x)_{x=0}^{N-1}} \rightsquigarrow (c_\xi)_{\xi=0}^{N-1} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \xi x / N} c_x$$

Note that $F \cdot F^* = \mathrm{Id}_{\mathbb{C}^N}$

The fastest classical algorithm for the DFT is the FFT with complexity of $O(N \log N)$

From now on we'll fix $N = 2^n$ so $F: \mathbb{C}^{2^n} = H^{\otimes n} \longrightarrow H^{\otimes n}$

We want to build it efficiently as a quantum circuit

Let $c_y = \begin{cases} 1 \text{ if } x = y \\ 0 \text{ otherwise} \end{cases}$ then

$$F|x\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{\xi=0}^{2^n-1} e^{2\pi i x \xi / 2^n} \quad |\xi\rangle$$

We can also write it in $2^n \times 2^n$ matrix form $F = \left(F_{\xi x}\right)_{\xi, x=0}^{2^n-1}$

where $F_{\xi x} = \frac{1}{\sqrt{2^n}} e^{2\pi i x \xi}$

<u>Lemma</u> For $|x\rangle^n \in H^n$ with $x = \sum_{j=0}^{n-1} 2^j x_j$ we have

$$F|x\rangle^n = \frac{1}{\sqrt{2^n}} \left[\bigotimes_{j=0}^{n-1} \left(|0\rangle + e^{2\pi i [0.x_j x_{j-1} - x_0]} |1\rangle \right) \right]$$

where $0.x_j x_{j-1} - x_0 = \frac{1}{2} x_j + \frac{1}{2^2} x_{j-1} + \ldots + \frac{1}{2^{j+1}} x_0$

so that $0.x_j \_ x_0$ is the <u>actual</u> decimal representation

<u>Proof</u>

$$F|x\rangle^n = \frac{1}{2^{n/2}} \sum_{\xi=0}^{2^n-1} e^{2\pi i x \xi / 2^n} |\xi\rangle^n \qquad \left[\text{decompose } \xi = \sum_{j=0}^{n-1} 2^j \xi_j \right]$$

$$= \frac{1}{2^{n/2}} \sum_{\xi=0}^{2^n-1} \prod_{j=0}^{n-1} e^{2\pi i x 2^j \xi_j 2^{-n}} \cdot \bigotimes_{j=0}^{n-1} |\xi_j\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\xi=0}^{2^n-1} \bigotimes_{j=0}^{n-1} e^{2\pi i x 2^{j-n} \xi_j} |\xi_j\rangle =$$

$$= \frac{1}{2^{n/2}} \bigotimes_{j=0}^{n-1} \left(|0\rangle + e^{2\pi i x 2^{j-n}} |1\rangle \right)$$

To conclude we notice that $x = \sum_{k=0}^{n-1} x_k 2^k$ so $2^{j-n} x = \sum_{k=0}^{n-1} x_k 2^{k+j-n}$ but since it's multiplying $2\pi i$ in an exponent $e^{\cdot}$, we only care about the decimal part, that is the initial part of the sum, namely until $k = j-n$ (excluded)

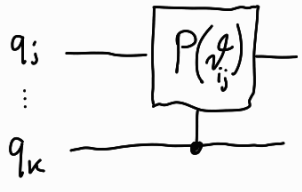
This gives the result up to some confusion in the indices, because the book uses a different convention

□

Now that we have $F|x\rangle^n = \frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \left(|0\rangle + \underbrace{e^{2\pi i \, 0.x_j x_{j-1} - x_0}}_{\prod_{k=0}^{j} e^{2\pi i x_k 2^{j-k-1}}} |1\rangle \right)$

so on each bit we're doing a controlled phase operation

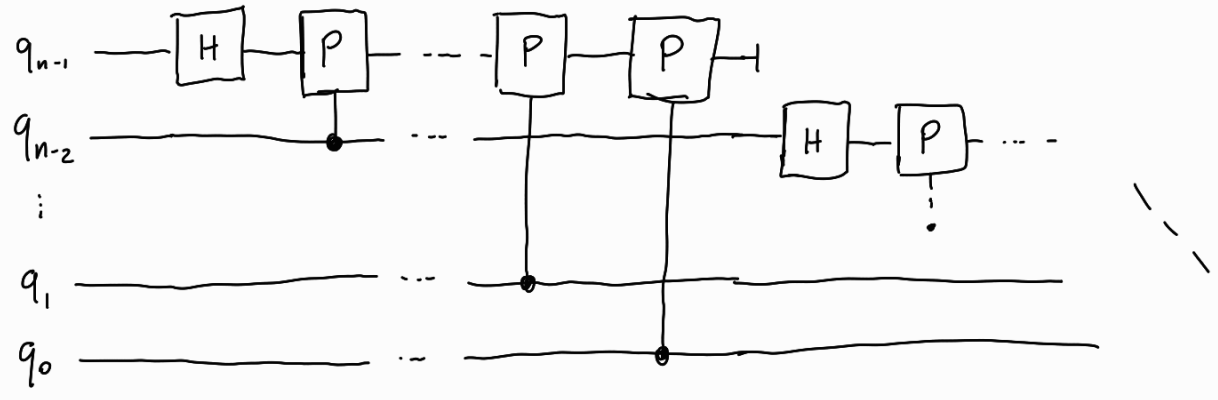
Def P_{kj} "controlled phase shift by $\vartheta_{jk} = \frac{\pi}{2^{j-k}}$ with control at qubit k, acting on qubit j"



where $P(\vartheta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}$

swap operation — which is because of the different notation and basically just reverses the order of all the qubits

Then $F = S^{(n)} \prod_{j=0}^{n-1} \left(\prod_{k=0}^{j-1} P_{kj} \right) H_j$



Deutsch's Problem

Suppose we have a function $f: \{0,1\}^n \longrightarrow \{0,1\}$, as in we have a way to compute it but no analytical representation

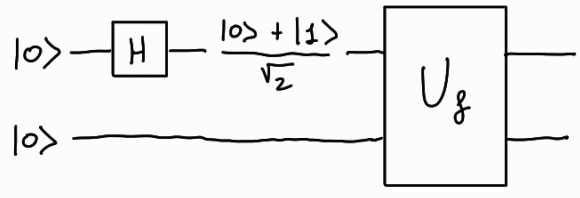
Suppose f is either constant (either $f \equiv 0$ or $f \equiv 1$) or f balanced, that is f assumes value 0 half of the times and 1 the other half

The problem we want to solve is to determine with certainty wether f is constant or balance, with the least number of evaluations possible

In a classical setting, the only solution that gives certainty requires $2^{n-1} + 1$ evaluations in the worst case

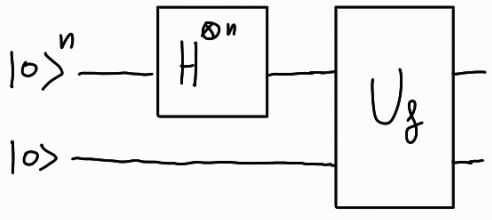
We'll now see how in the quantum setting, the Deutsch-Jozsa algorithm solves this problem in only 1 evaluation !

Consider the following circuit, where $f: \{0,1\} \longrightarrow \{0,1\}$



What's the final state? $U_f\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle}{\sqrt{2}}$

In a way, we evaluated f on multiple inputs (both 0 and 1) with only one U_f gate. This phenomenon is called Quantum parallelism. We can expand the circuit for $f: \{0,1\}^n \longrightarrow \{0,1\}$



with final state $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle$

We can also choose to start with a state different from $|0\rangle^n \otimes |0\rangle$

Prop. Prove that $H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$ where

$x \cdot y = \sum x_i y_i$

Proof by induction

$n=1$ the thesis is $H|x\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - (-1)^x |1\rangle \right)$ for $x \in \{0,1\}$

which is trivially checked manually for $x=0$ and $x=1$

$n \to n+1$ Let $\tilde{x} \in \{0,1\}^{n+1}$, then $H^{\otimes n+1} |\tilde{x}\rangle^{n+1}$ can be rewritten as

$$H^{\otimes n+1} |\tilde{x}\rangle = \left(H \otimes H^{\otimes n} \right) |x_n\rangle \otimes |x\rangle^n \qquad \text{where } x_n \in \{0,1\},\ x \in \{0,1\}^n$$

$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_{y \in \{0,1\}^n} \left((-1)^{x \cdot y} |0\rangle|y\rangle + (-1)^{x \cdot y + x_n} |1\rangle|y\rangle \right) =$$

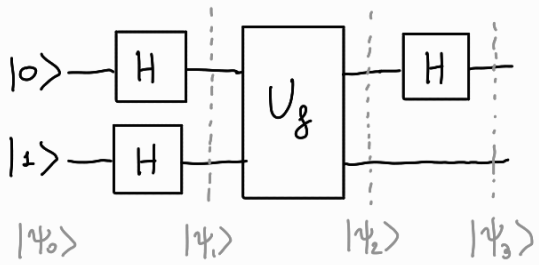
$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_{y \in \{0,1\}^n} \left((-1)^{x \cdot y + x_n \cdot 0} |0\rangle|y\rangle + (-1)^{x \cdot y + x_n \cdot 1} |1\rangle|y\rangle \right)$$

$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_{\tilde{y} \in \{0,1\}^{n+1}} (-1)^{\tilde{x} \cdot \tilde{y}} |\tilde{y}\rangle$$

Deutsch-Jozsa algorithm

Case $n=1$ $f : \{0,1\} \to \{0,1\}$ which means either $f(0) = f(1)$ (constant) or $f(0) \neq f(1)$ (balanced)

We can build the following circuit



Let's analyse the intermediate states

- $|\psi_0\rangle = |0\rangle \otimes |1\rangle$
- $|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Note that $U_g\left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{|x\rangle \otimes |g(x)\rangle - |x\rangle \otimes |1+g(x)\rangle}{\sqrt{2}}$

  so if $g(x)=0$ we get $\frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}}$

  if $g(x)=1$ we get $\frac{|x,1\rangle - |x,0\rangle}{\sqrt{2}}$

  so we can write $U_g\left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{g(x)} \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}}$

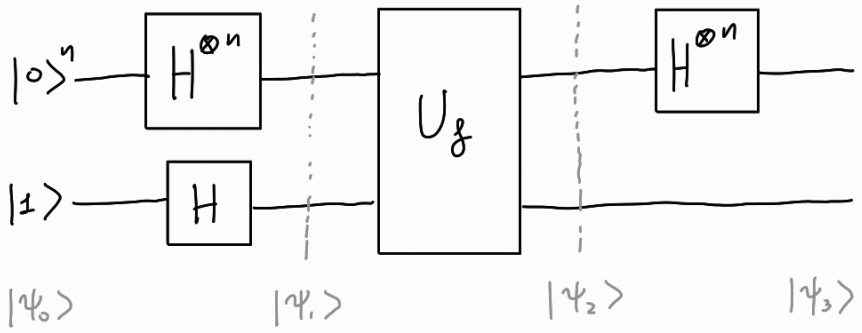
$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } g(0) = g(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } g(0) \neq g(1) \end{cases}$$

so $g(0)$ being different to $g(1)$ "puts a minus sign on the first qubit"

- $$|\psi_3\rangle = \begin{cases} |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } g(0) = g(1) \\ |1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } g(0) \neq g(1) \end{cases}$$

So by measuring the first qubit we can detect wether g is constant or balanced !

Case $n>1$



Similarly we have

- $|\psi_0\rangle = |0\rangle^n \otimes |1\rangle$
- $|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\psi_3\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y + f(x)} |y\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

  The amplitude of the state $|y\rangle = |0\rangle^n$ in the first part $\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$ which is ± 1 if f is constant and 0 if f is balanced

So if we measure the observable $|0\rangle^n\langle 0|^n$ we can detect wether f is constant or balanced !

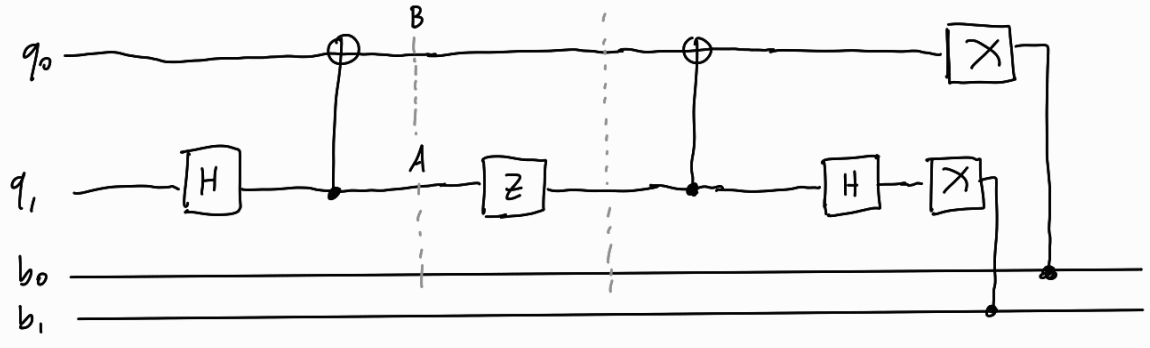
Super dense coding

Suppose we have a two qubit system in state $\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
We give the first qubit to Alice and the second one to Bob.
Alice then performs "some operation" to her qubit and sends it back to Bob

Consider the following table

Classical bits	Alice's operator	Global state
0 0	Id	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
0 1	Z	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
1 0	X	$\frac{\|10\rangle + \|01\rangle}{\sqrt{2}}$
1 1	ZX	$\frac{-\|10\rangle + \|01\rangle}{\sqrt{2}}$

Depending on the bits Alice wants to encode she performs a different operation on her qubit, changing the global state



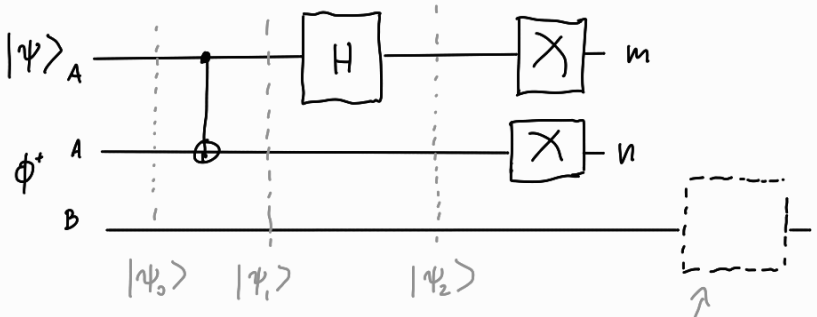
With the given global modifications and measurements, we get

State	After CNOT	After H
$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle + \|10\rangle}{\sqrt{2}}$	$\|00\rangle$
$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle - \|10\rangle}{\sqrt{2}}$	$\|10\rangle$
$\frac{\|10\rangle + \|01\rangle}{\sqrt{2}}$	$\frac{\|11\rangle + \|01\rangle}{\sqrt{2}}$	$\|01\rangle$
$\frac{-\|10\rangle + \|01\rangle}{\sqrt{2}}$	$\frac{-\|11\rangle + \|01\rangle}{\sqrt{2}}$	$\|11\rangle$

Ex7 What is the reduced density matrix with Alice's qubit?
It should be the same for all the cases, so if someone eavesdrop, they won't get any information

Teleportation

Alice has a quantum bit in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (not known to Alice?)
We assume that Alice and Bob also have each one qubit of an entangled pair (say in state $\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$)



$$|\psi_0\rangle = |\psi\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(\alpha|0\rangle\big(|00\rangle + |11\rangle\big) + \beta|1\rangle\big(|10\rangle + |01\rangle\big)\Big)$$

$$|\psi_2\rangle = \frac{1}{2}\Big(|00\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |01\rangle\big(\alpha|1\rangle + \beta|0\rangle\big) + |10\rangle\big(\alpha|0\rangle - \beta|1\rangle\big) + |11\rangle\big(\alpha|1\rangle - \beta|0\rangle\big)\Big)$$

Bob then sees the measurements $(m,n) \in \{0,1\}^2$ and applies the operation $X^n Z^m$ to his qubit, obtaining $|\psi\rangle$. In fact, if $(n,m) = (0,0)$ then Bob's qubit was in state $\alpha|0\rangle + \beta|1\rangle$, if $(n,m) = (0,1)$ then it is in state $\alpha|1\rangle + \beta|0\rangle$ so to obtain $|\psi\rangle$ he must apply Z (or X? check the actual order of m and n plz)

18/11

Shor's Algorithm

The problem we're trying to solve is to give a non-trivial factorization of a composite number.

We usually consider a (big) number $N = pq$ where $p \neq q$ are primes

Note: this an important problem for the RSA cryptographic protocol

The current best classical algorithm is the Numbered Field Sieve algorithm which costs $O(e^{c(\log N)^{1/3} \log\log N})$ (it's expressed in terms of $\log N$ because that's the number of binary digits of N, which is what we're interested in when calculating a cost for such a problem)

The Shor's Algorithm proposed in 1994 requires only $O((\log N)^3 \log\log N)$ of classical AND quantum elementary operations, and $O(\log N)$ qubits

By comparison, to check whether $b|N$ for some $b < N$ requires $O(\log N)$ steps
Computing $GCD(b, N)$ by Euclid's Algorithm, requires $O((\log N)^2)$ steps

Shor's algorithm is probabilistic but $\forall \varepsilon \in (0,1)$ using $O(c_\varepsilon \log^3 N \log\log N)$ we can obtain the factorization with probability $\geq 1 - \varepsilon$

We will always assume that N is odd, that is $p, q \neq 2$, because that case is trivial and can be checked in constant time

The key idea is to reduce the factorization problem to that of determining the period r of some periodic function $f : \mathbb{N} \longrightarrow \mathbb{N}$.
This second problem is in fact very simple with quantum algorithms

The actual function f will be of the form $f_{b,N}(n) = b^n \bmod N$ for some $b < N$. The function $f_{b,N}$ is periodic $r = \text{ord}_N(b)$ ie the order of b in $(\mathbb{Z}/N\mathbb{Z})^*$, so clearly we have to impose $GCD(b,N) = 1$

Note that the classical method to compute _a_ period (not even the smallest) requires $O(N)$ steps. On the other side, Shor's algorithm part for _the_ period calculation requires $O((\log N)^3 \log\log N)$ (it's the most expensive part) so here we have an exponential improvement!

Notice that $f_{b,N}$ restricted to an interval of length $\text{ord}_N(b)$ is injective, which is a nice property apparently

We'll now describe the full Shor's algorithm

Input N odd composite number divided by at least two different primes

Output non-trivial factorization of N

Steps 1] Choose b:

$O((\log N)^2)$

pick b randomly and compute $GCD(b,N)$ efficiently with Euclid's algorithm. If $GCD(b,N) \neq 1$ we're done because this GCD will give us a factorization.

Otherwise continue to step 2

2] Quantum routine $O((\log N)^3 \log\log N)$ with high probability

Use a quantum computer to compute the period $r = \text{ord}_N(b)$ of $f_{b,N}$.

If r is odd, go back to step 1

Otherwise, continue to step 3

3] Compute $GCD\left(b^{r/2}+1, N\right)$ (mod N?)

If GCD = N we go back to step 1

Otherwise we're done, because for sure it can't be GCD = 1 so if GCD ≠ N then it gives us a non trivial factor

Note: the other factor will be $GCD\left(b^{r/2}-1, N\right)$

Why does step 3 work?

In step 2 we've found $b^r \equiv 1 \bmod N$, and since r is even

so $\left(b^{r/2}\right)^2 - 1 \equiv 0 \bmod N \Rightarrow \left(b^{r/2}+1\right)\left(b^{r/2}-1\right) \equiv 0 \bmod N$

so $N \mid (b^r - 1)$ but $b^{r/2} - 1 \not\equiv 0 \bmod N$ so it can't be $N \mid (b^{r/2} - 1)$, so at least some factors of N go into $(b^{r/2}+1)$

if $N \nmid \left(b^{r/2}+1\right)$ this gives a non trivial factorization.

if $N \mid \left(b^{r/2}+1\right)$ then tough luck

There are a lot of "ifs" in this algorithm. There's a theorem that shows that these condition happen often

<u>Theorem</u> let $N = \prod_{j=1}^{J} p_j^{v_j}$ with $\{p_j\}$ distinct odd primes, $J \geq 2$, $v_j \geq 1$

and $\Omega = \{c \in \{0, \ldots, N-1\} \mid GCD(N, c) = 1\}$

Then we have

- $\#\Omega = \phi(N) = \prod_{j=1}^{J} p_j^{v_j - 1}(p_j - 1)$ (not useful in our case)
- $\#\left\{b \in \Omega \mid \text{ord}_N(b) \text{ is even} \wedge N \nmid \left(b^{r/2}+1\right)\right\} \geq \phi(N) \cdot \left(1 - \frac{1}{2^{J-1}}\right)$

Fact $\exists c > 0 \quad \frac{\phi(n)}{n} \geq \frac{c}{\log\log n}$ definitely in n

Let's now focus on Step 2. We'll generalize a bit the problem we're considering

Problem given $f: \mathbb{N} \to \mathbb{N}$ periodic with (unknown) period r, find r

assuming that

i) $\exists L \geq 2 \quad r < 2^{L/2}$ (that is we have an upper boud for r, in our case $L = \lfloor 2 \log_2 N \rfloor + 1$)

ii) f restricted to one period is injective and $\exists k \geq 1$ s.t. $f(n) < 2^k$ (so you can store $f(n)$ in k qubits)

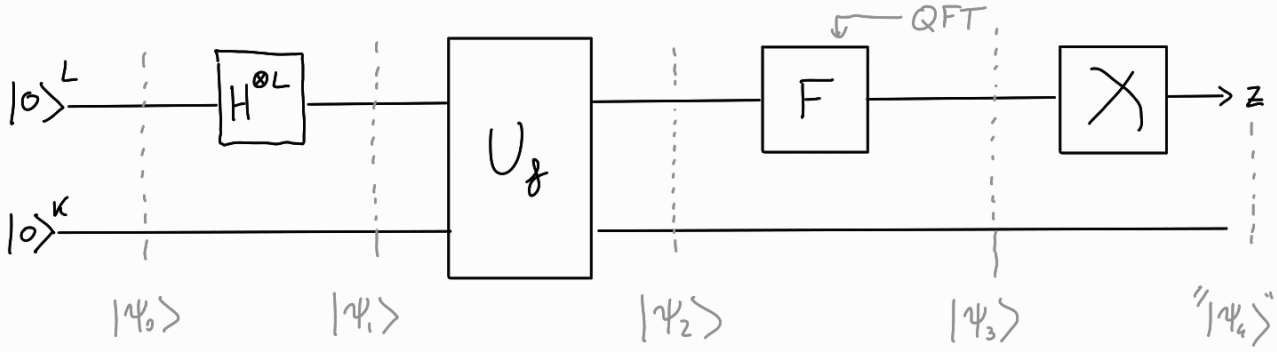
iii) $U_f : H^{\otimes L} \otimes H^{\otimes k} \longrightarrow H^{\otimes L} \otimes H^{\otimes k}$ is implementable with

↳ note, this much much bigger than the period!

$\mathcal{O}(L^c)$ elementary gates (in our case $f_{b,N}$ requires $\mathcal{O}((\log N)^3)$)

We'll show that we can find the period r with probability of at least $\frac{c'}{\log L}$ with at most $\mathcal{O}(L^{\max\{c,3\}})$ elementary gates
(where c' is a constant that depends on nothing, most likely $c' = \frac{1}{10}$)
To find r with probability at least $1/2$ we repeat until $\left(1 - \frac{c'}{\log L}\right)^s \leq 1/2$ where s is the number of times we repeat
As L grows, s needs to be proportional to $\log L$. This repetition gives us the factor $\log\log N$ in the cost

Let's build the circuit for this routine



This circuit gives partial states

$$|\psi_0\rangle = |0\rangle^L \otimes |0\rangle^K$$

$$|\psi_1\rangle = \frac{1}{2^{L/2}} \sum_{x=0}^{2^L-1} |x\rangle^L \otimes |0\rangle^K$$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{2^{L/2}} \sum_{x=0}^{2^L-1} |x\rangle^L \otimes |f(x)\rangle$$

same as the Deutsch-Jozsa

Since f is periodic we can rewrite $|\psi_2\rangle = \frac{1}{2^{L/2}} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} |k + j\cdot r\rangle \otimes |f(k)\rangle$ ($x = k + j\cdot r$)

where $J = \left\lfloor \frac{2^L-1}{r} \right\rfloor$ which is the total number of periods in $\{0, \dots, 2^L-1\}$, $R \equiv 2^L - 1 \bmod r$ and $J_k = \begin{cases} J+1 & \text{if } k \leq R \\ J & \text{if } k > R \end{cases}$

is the number of values of the same "class" of k in $\{0, \dots, 2^L-1\}$.

The discrepancy of the -1 is given by the fact that the last period is not "full", only the first R values of the last period are present in $\{0, \dots, 2^L-1\}$ so the values of class bigger than R are missing their representative in the last period.

For step 3 remember that $F|x\rangle^L = \frac{1}{2^{L/2}} \sum_{l=0}^{2^L-1} e^{2\pi i \frac{lx}{2^L}} |l\rangle^L$ so

$$|\psi_3\rangle = F \otimes 1_K |\psi_2\rangle = \frac{1}{2^L} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} \sum_{l=0}^{2^L-1} e^{2\pi i \frac{l\cdot(k+jr)}{2^L}} |l\rangle \otimes |f(k)\rangle$$

Note: the biggest number factorized this way is $21 = 7 \cdot 3$

When we measure H^L we will get a number $z \in \{0, \dots, 2^L - 1\}$ with probability $P(z) = (A_z)_{|\psi_3\rangle} = \| A_z |\psi_3\rangle \|^2$

"because it's a projection" ↓

Note that the observable here is $A_z = |z\rangle\langle z| \otimes 1_K = A_z^2$

$$A_z |\psi_3\rangle = \frac{1}{2^L} \sum_{k=0}^{r-1} \left(\sum_{j=0}^{J_k} e^{2\pi i \left(\frac{z \cdot (k+jr)}{2^L} \right)} \right) |z\rangle \otimes |g(k)\rangle$$

$$\| A_z |\psi_3\rangle \|^2 = \frac{1}{2^{2L}} \sum_{k=0}^{r-1} \left| \sum_{j=0}^{J_k} e^{2\pi i \left(\frac{z \cdot (k+jr)}{2^L} \right)} \right|^2$$

↑ the $g(k)$ are all different

$= \sum_{j=0}^{J_k} a^j$ where $a = e^{2\pi i \frac{zj}{2^L}}$ because the phase k cancels out (?)

We find

$$P(z) = \begin{cases} \frac{1}{2^{2L}} \sum_{k=0}^{r-1} (J_k + 1)^2 & \text{if } \frac{zr}{2^L} \text{ is an integer, ie } a = 1 \\ \frac{1}{2^{2L}} \sum_{k=0}^{r-1} \left| \frac{e^{2\pi i \frac{zr}{2^L}(J_k+1)} - 1}{e^{2\pi i \frac{zr}{2^L}} - 1} \right|^2 \end{cases}$$

We can prove that in the first case $P(z) \gtrsim \frac{1}{2^{2L}} \cdot r \left(\frac{2^L}{r} \right) \approx \frac{1}{r}$

in the second case, if z is st $\left| \frac{zr}{2^L} - \ell \right| \leq \frac{r}{2^{L+1}}$ for some integer ℓ, that is $\frac{zr}{2^L}$ is "close to be an integer", the same bound $P(z) \gtrsim \frac{c}{r}$ for some constant c that does not depend on anything

To extract r from this we actually need a Step 5 which we will not see in detail but broadly speaking, from continuous fraction theory we know that if $\left| \frac{zr}{2^L} - \ell \right| \leq \frac{r}{2^{L+1}}$ ⊛ for some integer ℓ (which a posteriori will be unique) then the number $\frac{\ell}{r}$ will appear in the fractional approximations of $\frac{z}{2^L}$ given by its continuous fraction representation, provided that $GCD(\ell, r) = 1$ (**)

Lemma $\sum_{z \text{ such that } \circledast \text{ and } \ast\ast} P(z) \geq \frac{c}{\log L}$ (mysterious lemma, we will not prove it)

23/11

Quantum Phase Estimation

Consider the following problem

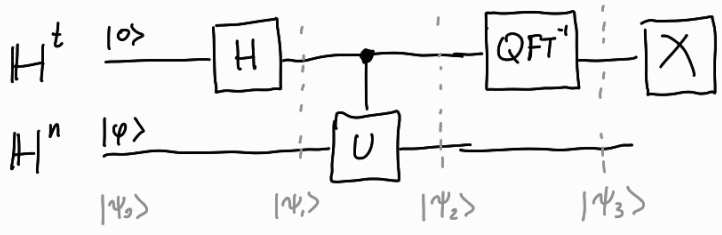
Problem assume we have an eigenstate $|\varphi\rangle \in \mathbb{H}^n$ for a unitary U, ie $U|\psi\rangle = e^{2\pi i \vartheta}|\varphi\rangle$.

Can we extimate or ϑ with high precision using a quantum circuit?

Remember that $|\varphi\rangle$ and $e^{2\pi i \vartheta}|\varphi\rangle$ belong to the same ray so they give the same density operator $\rho = |\varphi\rangle\langle\varphi|$

We'll see that only using U, this is not possible, but if we can build a controlled-U, then we can solve this problem. The solution will apply several times this CU (or a controlled version of powers of U depending on which is cheaper and easier to build) to t additional qubits in order to obtain ϑ up to t binary digits, ie with high probability we will find $\lfloor 2^t \vartheta \rfloor$

Example ($t=1$) (in this case, $|\psi\rangle$ is the ancilla and we assume to have it)



$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\varphi\rangle$$

$$|\psi_2\rangle = \frac{|0\rangle \otimes |\varphi\rangle}{\sqrt{2}} + \frac{e^{2\pi i \vartheta}|1\rangle \otimes |\varphi\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i \vartheta}|1\rangle}{\sqrt{2}} \otimes |\varphi\rangle$$

Notice that for $t=1$, $QFT^{-1} = H$ so

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\varphi\rangle + \frac{e^{2\pi i \vartheta}}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |\varphi\rangle =$$

$$= \left[\frac{1}{2}\left(1 + e^{2\pi i \vartheta}\right)|0\rangle + \frac{1}{2}\left(1 - e^{2\pi i \vartheta}\right)|1\rangle \right] \otimes |\varphi\rangle$$

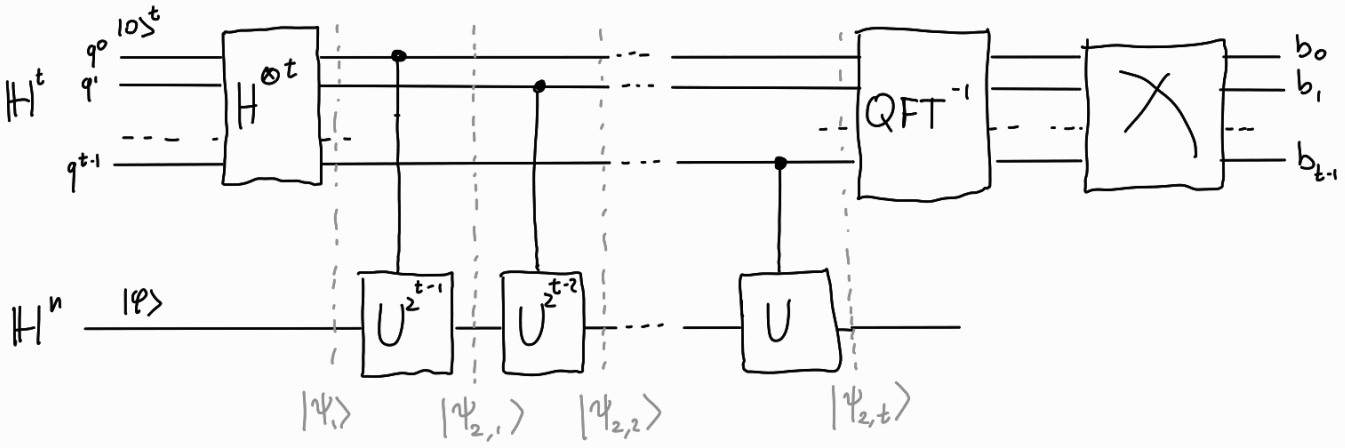
Therefor when we measure the first qubit we obtain 0 with probability $P(0) = \left| \frac{1 + e^{2\pi i \vartheta}}{2} \right|^2 = \cos^2(\pi\vartheta)$

and 1 with probability $P(1) = \left| \frac{1 - e^{2\pi i \vartheta}}{2} \right|^2 = \sin^2(\pi\vartheta)$

Note that $P(0) > P(1) \iff \vartheta \in \left[0, \frac{1}{4}\right] \cup \left[\frac{3}{4}, 1\right)$.

So we can obtain exactly ϑ if $\vartheta \in \{0, 1/2\}$, that is ϑ only has 1 binary digit

For a general t we have



This circuit gives the following state

$$|\psi_1\rangle = \frac{1}{2^{t/2}} \underbrace{\left(|0\rangle + |1\rangle\right)}_{q^{t-1}} \otimes \ldots \otimes \underbrace{\left(|0\rangle + |1\rangle\right)}_{q^0} \otimes |\varphi\rangle$$

$$|\psi_{2,1}\rangle = \frac{1}{2^{t/2}} \underbrace{\left(|0\rangle + |1\rangle\right)}_{q^{t-1}} \otimes \ldots \otimes \underbrace{\left(|0\rangle + |1\rangle\right)}_{q^1} \otimes \underbrace{\left(|0\rangle + e^{2\pi i \vartheta 2^{t-1}}|1\rangle\right)}_{q^0} \otimes |\varphi\rangle$$

$$|\psi_{2,2}\rangle = \frac{1}{2^{t/2}} \underbrace{\left(|0\rangle + |1\rangle\right)}_{q^{t-1}} \otimes \ldots \otimes \underbrace{\left(|0\rangle + e^{2\pi i \vartheta 2^{t-2}}|1\rangle\right)}_{q^1} \otimes \underbrace{\left(|0\rangle + e^{2\pi i \vartheta 2^{t-1}}\right)}_{q^0} \otimes |\varphi\rangle$$

$$|\psi_{2,t}\rangle = \frac{1}{2^{t/2}} \bigotimes_{j=t}^{1} \left(|0\rangle + e^{2\pi i \vartheta 2^{t-j}} |1\rangle\right) \otimes |\varphi\rangle$$

Now recall that $F|x\rangle^t = \frac{1}{2^{t/2}} \sum_{\xi=0}^{2^t-1} e^{2\pi i \xi \cdot x/2^t} |\xi\rangle$

$$F^{-1}|x\rangle^t = \frac{1}{2^{t/2}} \sum_{\xi=0}^{2^t-1} e^{-2\pi i \xi \cdot x/2^t} |\xi\rangle$$

but also we had an alternative representation

$$F|x\rangle^t = \left(|0\rangle + e^{2\pi i \frac{x}{2}} |1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{2\pi i \frac{x}{2^t}} |1\rangle\right)$$

Check the RHS is $\sum_{s \in \{0,1\}^t} \bigotimes_{j=t-1}^{0} e^{2\pi i \frac{x}{2^{t-j}} s_j} |s_j\rangle$ ∎

If we rewrite $|\psi_{2,t}\rangle$ as

$$|\psi_{2,t}\rangle = \frac{1}{2^{t/2}} \bigotimes_{j=t}^{1} \left(|0\rangle + e^{2\pi i \frac{\vartheta 2^t}{2^j}} |1\rangle\right) \otimes |\varphi\rangle$$

and reverse the order of the first t qubits, it becomes clear that if $2^t\vartheta =: x$ is an integer, then

$$(F^{-1} \otimes Id)|\psi_{2,t}\rangle = |2^t\vartheta\rangle \otimes |\varphi\rangle$$

and we can measure $2^t\vartheta$ and get ϑ

If $2^t\vartheta$ is not an integer we get

$$|\psi_3\rangle = \frac{1}{2^t} \sum_{x=0}^{2^t-1} \sum_{\xi=0}^{2^t-1} e^{2\pi i \frac{(2^t\vartheta)}{2^t}\xi} \cdot e^{-2\pi i \frac{x \cdot \xi}{2^t}} |x\rangle^t \otimes |\varphi\rangle$$

Then the probability of measuring a certain number x is

$$P(x) = \frac{1}{2^{2t}} \left| \sum_{\xi=0}^{2^t-1} e^{2\pi i \frac{\xi}{2^t}(2^t\vartheta - x)} \right|^2$$

and this probability has a peak for $\bar{x}$ st $\left|\frac{\bar{x}}{2^t} - \vartheta\right| \leq \frac{1}{2}\cdot\frac{1}{2^t}$,

in particular $P(\bar{x}) \gtrsim c$ universal constant $(40\%?)$

We can now show Shor's Algorithm to find a period $f: \mathbb{N} \to \mathbb{N}$

where
- $r < 2^{L/2}$
- f is injective over a period
- $f(n) < 2^K$

Consider $|\varphi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |f(k)\rangle \in \mathcal{H}^K$, which is an eigenstate

for U that behaves like $U|f(x)\rangle = |f(x+1)\rangle$

(in Shor's factorization algorithm it's $U|x\rangle = |xb\rangle$ $\quad f(r) = f(0)$

Then $U|\varphi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |f(k+1)\rangle = \frac{1}{\sqrt{r}} \sum_{k=1}^{r} |f(k)\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |f(k)\rangle$

Ok so instead consider $|\varphi_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i \frac{s\cdot k}{r}} |f(k)\rangle$ then

$s \in \{0, \dots, r-1\}$

$$U|\varphi_s\rangle = e^{2\pi i \frac{s}{r}} |\varphi_s\rangle$$

We can hope to estimate with high probability $\frac{s}{r}$ with phase estimation

obtaining $\vartheta = \frac{s}{r}$ and get $r = \frac{s}{\vartheta}$

Actually, we want the state $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\varphi_s\rangle = \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{-2\pi i \frac{s\cdot k}{r}} |f(k)\rangle$

$$= \frac{1}{r} \sum_{k=0}^{r-1} \underbrace{\sum_{s=0}^{r-1} e^{-2\pi i \frac{s\cdot k}{r}}}_{= r\,\delta_{s0}} |f(k)\rangle = |f(0)\rangle$$

And in our case $f(0) = 1$ so the state is $|1\rangle$

So $|1\rangle$ is a superposition of the eigenstates $|\varphi_s\rangle$ so if we apply the QPE to $|1\rangle$ we will get some $\frac{s}{r}$ for some random s. If we're lucky s is coprime with r and we can get r

25/11

Grover's Algorithm (1996)

The problem that this algorithm solves is an unstructured search problem

Suppose you have a set X with a subset $S \subset X$ that satisfies a certain easily verifiable property. We want to find an element that satisfies the property, that is we want to find an element in S

The classical approach (given $N = |X|$) is to bruteforce until we find one, which is $O(N)$. Groover's algorithm is $O(\sqrt{N})$, although it is probabilistic, but it is provably optimal (asymptotically) (# of queries of the oracle)

There's been a physical implementation with 3 qubits, so $N = 2^3$ (2017)

We will assume $N = 2^n$. and that we know $m = |S|$ (if we know the solution is unique, we know $m = 1$)

I/O space: $H^{\otimes n}$, ancilla space: H

Suppose we can enumerate X (in any arbitray way), that is find a bijection between $\{0,1\}^n$ and X. We'll use this as an identification of X

Suppose we also have an oracle, ie a boolean function $g: \{0,1\}^n \longrightarrow \{0,1\}$ st $g(x) = \mathbb{1}_S(x)$. We'll call $S^+ = X \setminus S$

We also suppose to have a gate $U_g : H^{\otimes n} \otimes H \longrightarrow H^{\otimes n} \otimes H$

$$|x\rangle \otimes |y\rangle \rightsquigarrow |x\rangle \otimes |y + g(x)\rangle$$

In this case the initial state of the ancilla qubit will be $\frac{|0\rangle - |1\rangle}{\sqrt{2}} = H|1\rangle$

Note that if $x \in \{0,1\}^n$ $\quad U_g\left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{g(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

More generally, for a (non-basis) state $|\varphi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle$ we get

$$U_g\left(|\varphi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \sum_{x=0}^{2^n-1} (-1)^{g(x)} \alpha_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

(*) future abuse of notation

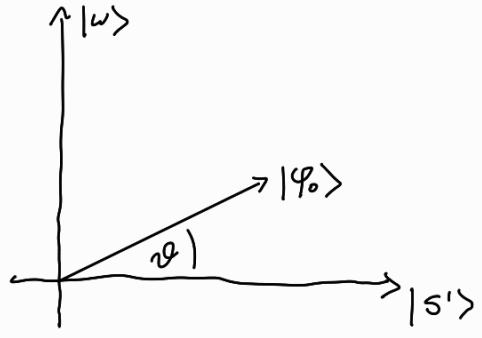
So U_g reverses the phase of the items that belong to the solution set

The I/O initial state will be $H^{\otimes n}|0\rangle^n$, so actually we can start with $|0\rangle^n \otimes |1\rangle$ global state and then apply $H^{\otimes n+1}$

We'll first consider the case $\underline{m=1}$, (just to give an intuition) and let $\omega \in S$ the unique solution

then $|\psi_0\rangle|_{IO} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$. In this state, the probability obtaining ω with a measure is $1/2^n$. Our goal is to increase this probability with a process called amplitude amplification

Let's represent $|\varphi_0\rangle$ as its component in $\text{span}|\omega\rangle$ and $|\omega\rangle^\perp$



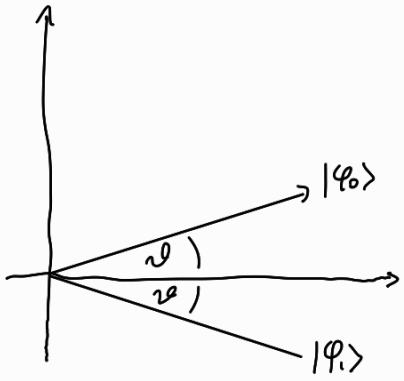
Note that is multidimensional, but to represent this we can simplify to 1-dimensional. Formally, $|\varphi_0\rangle$ belongs to the plane generated by $|\omega\rangle$ and

$$|s'\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{\substack{x=0 \\ x \neq \omega}}^{2^n-1} |x\rangle$$

We can write $|\varphi_0\rangle = \cos\vartheta\,|s'\rangle + \sin\vartheta\,|w\rangle$

If we apply the oracle U_g to $|\varphi_0\rangle$ (and ofcourse the ancilla part)

we get $|\varphi_1\rangle = \cos\vartheta\,|s'\rangle - \sin\vartheta\,|w\rangle = \cos(-\vartheta)\,|s'\rangle + \sin(-\vartheta)\,|w\rangle$

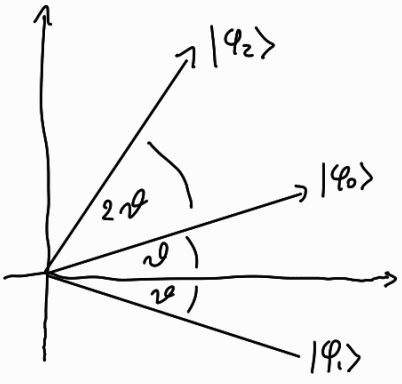


So U_g reflects with respect to $|s'\rangle$!

Now we will perform a reflection wtr $|\varphi_0\rangle$, and the result will be a state with an amplitude of $|w\rangle$ greater than $|\varphi_0\rangle$'s

We can apply this second reflection with the operator $U_{\varphi_0} = 2|\varphi_0\rangle\langle\varphi_0| - \mathbb{1}^{\otimes n}$

so $|\varphi_2\rangle = U_{|\varphi_0\rangle} U_g |\varphi_0\rangle$ will be



so if the amplitude of $|w\rangle$ in $|\varphi_0\rangle$ was ϑ

the amplitude of $|w\rangle$ in $|\varphi_2\rangle$ is 3ϑ

If we repeat this a sufficient number of times we can get the amplitude close to $\pi/2$

so we can get $|w\rangle$ with high probability !

The operator $U_{|\varphi_0\rangle} U_g$ is called Groover's operator and it applies a rotation of 2ϑ

In general, we have a set S of solutions and $S^\perp$ of non-solutions.

Again we start with $|\varphi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$. We will call

$$|\varphi_S\rangle = \frac{1}{\sqrt{m}} \sum_{x \in S} |x\rangle \quad \text{and} \quad |\varphi_{S^\perp}\rangle = \frac{1}{\sqrt{N-m}} \sum_{x \in S^\perp} |x\rangle$$

We can define a projection on S, namely $P_S = \sum_{x \in S} |x\rangle\langle x|$

and similarly $P_{S^\perp} = \sum_{x \in S^\perp} |x\rangle\langle x|$

If we call $R_{S^\perp}$ the reflection wrt $S^\perp$, then $\hat{U}_g$ behaves like $R_{S^\perp} \otimes \mathbb{1}$. Note $R_{S^\perp} = 2P_{S^\perp} - \mathbb{1}^{\otimes n}$ (sometimes called the diffusion operator) and $R_{|\varphi_0\rangle} = 2|\varphi_0\rangle\langle\varphi_0| - \mathbb{1}^{\otimes n}$

So again we start $|\varphi_0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ and apply repetedly the Grover operator $\hat{G} = (R_{|\varphi_0\rangle} \otimes \mathbb{1})\hat{U}_g$

Note that $|\varphi_0\rangle = \frac{\sqrt{m}}{\sqrt{N}}|\varphi_S\rangle + \frac{\sqrt{N-m}}{\sqrt{N}}|\varphi_{S^\perp}\rangle$

If we call $\vartheta_0 = \arcsin\sqrt{\frac{m}{N}}$ we get $|\varphi_0\rangle = \cos\vartheta_0 |\varphi_{S^\perp}\rangle + \sin\vartheta_0 |\varphi_S\rangle$

Prop. Let $|\hat{\varphi}_j\rangle = \left[\overbrace{(R_{|\varphi_0\rangle} \otimes \mathbb{1})\hat{U}_g}^{\hat{G}}\right]^j |\hat{\varphi}_0\rangle$, then it holds

$|\hat{\varphi}_j\rangle = |\varphi_j\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ where $|\varphi_j\rangle = \cos\vartheta_j |\varphi_{S^\perp}\rangle + \sin\vartheta_j |\varphi_S\rangle$

and $\vartheta_j = (2j+1)\vartheta_0$

Proof by induction on j

$j = 0$ $|\varphi_0\rangle = \cos\vartheta_0 |\varphi_{S^\perp}\rangle + \sin\vartheta_0 |\varphi_S\rangle$ which is clearly true

$j \to j+1$ $|\hat{\varphi}_{j+1}\rangle = (R_{|\varphi_0\rangle} \otimes \mathbb{1})\hat{U}_g |\hat{\varphi}_j\rangle$

left as an exercise

□

If the current state is $|\varphi_j\rangle$, the probability of measuring an element of S is $P(S) = \sin^2\vartheta_j$, so to maximise this we want to choose j st $\vartheta_j \simeq \frac{\pi}{2}$

Lemma let $j_N = \left\lfloor \frac{\pi}{4 \arcsin\sqrt{\frac{m}{N}}} \right\rfloor$, if we perform j_N iterations of Groover we get an element of S with probability $\geq 1 - \frac{m}{N}$

Proof by definition $j_N \leq \frac{\pi}{4\vartheta_0} < j_N + 1$ so

$$2\vartheta_0 j_N \leq \frac{\pi}{2} < 2\vartheta_0 j_N + 2\vartheta_0 = \vartheta_{j_N} + \vartheta_0$$

$$\hookrightarrow \quad \vartheta_{j_N} \leq \frac{\pi}{2} + \vartheta_0$$

$$\Rightarrow \quad \frac{\pi}{2} - \vartheta_0 < \vartheta_j \leq \frac{\pi}{2} + \vartheta_0$$

Since $P(S) = \sin^2 \vartheta_j$, since $\vartheta_j > \frac{\pi}{2} - \vartheta_0$ we get

$$P(S) = \sin^2 \vartheta_j \geq \sin^2\left(\frac{\pi}{2} - \vartheta_0\right) = \cos^2(\vartheta_0) = 1 - \sin^2(\vartheta_0)$$

$$= 1 - \frac{m}{N}$$

Notice that after j_N iterations, any additional iteration worsens the result as ϑ_j is getting further from $\pi/2$

In particular we get $j_N = \mathcal{O}\left(\sqrt{\frac{N}{m}}\right)$ with a simple Taylor expansion so for the algorithm we have to do $\mathcal{O}\left(\sqrt{\frac{N}{m}}\right)$ calls to Grover operator

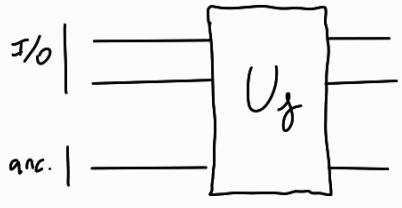
Notice that $\hat{G} = \left(R_{\varphi_0} \otimes \mathbb{1}\right)\hat{U}_g$. An important fact is that $R_{\varphi_0} = H^{\otimes n} R_{|0\rangle} H^{\otimes n}$ so it actually costs $2n+1$ elementary gates, where $n = \log N$, so the cost of the algorithm in elementary gate, is $\mathcal{O}\left(\sqrt{\frac{N}{m}} \log N\right)$ (assuming the oracle is constant)

30/11

We'll now implement Grover for $N = 4$ $\overset{m:1}{\checkmark}$ (ie $I/O = H^{\otimes 2}$)

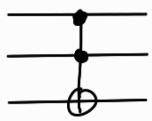
First method in this case we consider an oracle that needs an ancilla qubit

(Ref: Nielsen & Chuang chpt 6)

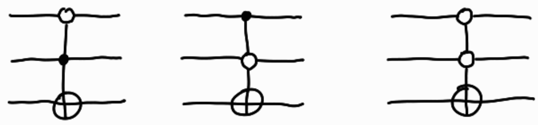


The search set is formed by the basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

To build an actual circuit, we need to build an oracle that recognizes one of these states. For example, if the target item is $|11\rangle$, the oracle would be

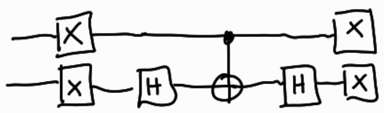


If we want to target a different value we just need to add some X, that is having a CCNOT that control on 0 instead of 1, and we usually indicate them as

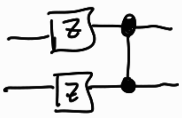


Instead of the reflection $2|\varphi_0\rangle\langle\varphi_0| - \mathbb{1}$ we will use the equivalent $H^{\otimes 2}(2|00\rangle\langle 00| - \mathbb{1})H^{\otimes 2}$ which is easier to build

To build $2|00\rangle\langle 00| - \mathbb{1}$ we can use the following circuit



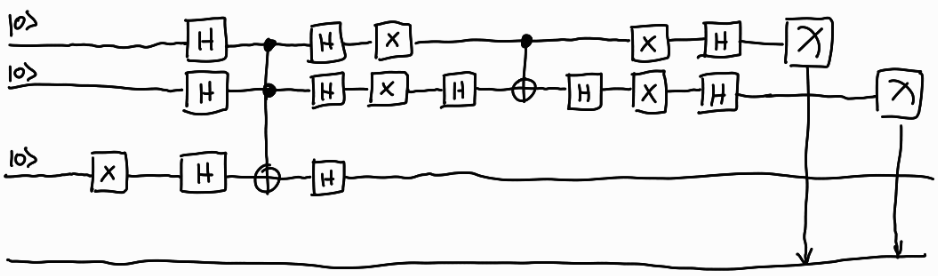
Another option is



which behaves the same up to a global phase (all is multiplied by -1)

In this case $\vartheta = \arcsin \frac{1}{2^{n/2}} = \arcsin \sqrt{\frac{1}{4}} = \frac{\pi}{6}$ so after only $j_4 = 1$ iteration we get an amplitude of $3\vartheta = \pi/2$ so we obtain the result with certainty ! (note: this is always true for $m = \frac{N}{4}$)

The circuit will be

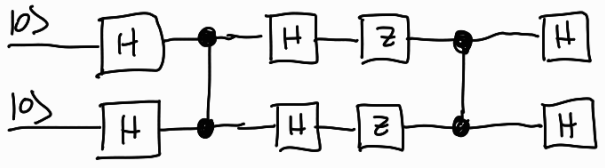


Second method We will consider the following case with an oracle that does not need an ancilla

If the target state is $|11\rangle$ we need an oracle with a matrix

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$ which is the CZ gate !

Then the circuit becomes (with also the "smart" $|0\rangle$ reflection)



Much simpler !

Let's implement the case for $N=8$ $(n=3)$, $m=2$

Quantum Counting

We saw that Grover's operato acts as a rotation of angle 2ϑ in the plane spanned by $|w\rangle$, $|\varphi_0\rangle$, so it acts as a matrix

$$\begin{pmatrix} \cos 2\vartheta & -\sin 2\vartheta \\ \sin 2\vartheta & \cos 2\vartheta \end{pmatrix}$$ which is unitary with eigenvectors $\begin{pmatrix} i \\ 1 \end{pmatrix}$ and $\begin{pmatrix} -i \\ 1 \end{pmatrix}$ and eigenvalues

$e^{i2\vartheta}$, $e^{-i2\vartheta}$

We've also seen the QPE which estimates phases of eigenvalue of a unitary matrix, given the corresponding eigenvector

Suppose we have the oracle but do not know m. Before

applying Grover we need to estimate m, and for this purpose we can use quantum counting. The idea is as follows

Idea Apply QPE to Grover's matrix with an eigenvector, say $\begin{pmatrix} i \\ 1 \end{pmatrix}$

we will get an estimate of $2^t\varphi$ where $e^{2\pi i\varphi}$ is the eigenvalue, and we can deduce a value of ϑ

Since we know $\sqrt{\frac{m}{N}} = \sin\vartheta$ we get $m = N\sin^2\vartheta$

02/12

Remarks on QPE

For the QPE setting we know $|\varphi\rangle$ eigenvector of U and we want to estimate ϑ st $U|\varphi\rangle = e^{2\pi i\vartheta}|\varphi\rangle$

The hypotesys of being able to build $|\varphi\rangle$ is quite strong, so let's see what we can do about it

In the first step of shor we prepare

$$|\psi_0\rangle\otimes|\varphi\rangle = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}|k\rangle\otimes|\varphi\rangle$$

and after applying $\Lambda^i\left(U^{2^*}\right)$ we get the state

$$|\psi_1\rangle\otimes|\varphi\rangle = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi i\vartheta k}|k\rangle\otimes|\varphi\rangle$$

Finally we apply QFT^{-1} to the I/O register to get

$$|\psi_2\rangle\otimes|\varphi\rangle = \frac{1}{2^t}\sum_{l=0}^{2^t-1}\sum_{k=0}^{2^t-1}e^{2\pi i\vartheta k}\,e^{-2\pi i\frac{lk}{2^t}}|l\rangle\otimes|\varphi\rangle$$

Then we measure I/O and obtain $l\in\{0,\dots,2^t-1\}$ with probability

$$P(\ell) = \frac{1}{2^t}\left|\sum_{k=0}^{2^t-1} e^{2\pi i k\cdot\left(\vartheta-\frac{\ell}{2^t}\right)}\right|^2$$ which is exactly 1 if $2^t\vartheta$ is an integer and $\ell = 2^t\vartheta$. Otherwise it's reasonably high ($\geq 40\%$) for $\ell = \lfloor 2^t\vartheta \rfloor$

If we don't know $|\varphi\rangle$ or we can't build it, let's see what we can do

Consider (not an eigenvector) $|\varphi\rangle = \alpha_0|\varphi_0\rangle + \alpha_1|\varphi_1\rangle$ with $|\varphi_0\rangle, |\varphi_1\rangle$ eigenstates with $U|\varphi_0\rangle = e^{2\pi i\vartheta_0}|\varphi_0\rangle$ and $U|\varphi_1\rangle = e^{2\pi i\vartheta_1}|\varphi_1\rangle$

Then $$|\psi_1\rangle\otimes|\varphi\rangle = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}\alpha_0 e^{2\pi i\vartheta_0}|k\rangle\otimes|\varphi_0\rangle + \alpha_1 e^{2\pi i\vartheta_1}|k\rangle\otimes|\varphi_1\rangle$$

and $$|\psi_2\rangle\otimes|\varphi\rangle = \frac{1}{2^t}\sum_{\ell=0}^{2^t-1}\sum_{k=0}^{2^t-1} e^{2\pi i\left(\vartheta_0-\frac{\ell}{2^t}\right)k}\alpha_0|\ell\rangle\otimes|\varphi_0\rangle + \\ + e^{2\pi i\left(\vartheta_1-\frac{\ell}{2^t}\right)}\alpha_1|\ell\rangle\otimes|\varphi_1\rangle$$

Then the probability of obtaining a value ℓ is

$$P(\ell) = \left\| \frac{1}{2^t}\sum_{k=0}^{2^t-1} e^{2\pi i\left(\vartheta_0-\frac{\ell}{2^t}\right)\cdot k}\alpha_0|\varphi_0\rangle + e^{2\pi i\left(\vartheta_1-\frac{\ell}{2^t}\right)\cdot k}\alpha_1|\varphi_1\rangle\right\|^2 =$$

because they're orthogonal, $|\varphi_0\rangle$ and $|\varphi_1\rangle$

$$= \frac{1}{2^t}\left|\sum_{k=0}^{2^t-1} e^{2\pi i\left(\vartheta_0-\frac{\ell}{2^t}\right)k}\right|^2\cdot|\alpha_0|^2 + \frac{1}{2^t}\left|\sum_{k=0}^{2^t-1} e^{2\pi i\left(\vartheta_1-\frac{\ell}{2^t}\right)k}\right|^2\cdot|\alpha_1|^2 =$$

$$= |\alpha_0|^2 P_{\vartheta_0}(\ell) + |\alpha_1|^2 P_{\vartheta_1}(\ell)$$

In the extreme case where both $\vartheta_0 = \ell_0\cdot 2^t$ and $\vartheta_1 = \ell_1\cdot 2^t$ then by measuring we get ℓ_0 with probability $|\alpha_0|^2$ and ℓ_1 with prob $|\alpha_1|^2$

(ever if this doesn't happen, we do get two peaks)

<u>Exercise</u> In quantum counting we had $|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \sqrt{\frac{m}{N}}|S\rangle + \sqrt{\frac{N-m}{N}}|S'\rangle$

G behaved like a rotation of 2ϑ on the plane $\mathrm{Span}(|S\rangle, |S'\rangle)$

we can find eigenvectors $|\varphi_0\rangle, |\varphi_1\rangle$ in this plane with eigenvalues $e^{i2\vartheta}, e^{-i2\vartheta}$ so that we can write $|\psi_0\rangle = \alpha_0|\varphi_0\rangle + \alpha_1|\varphi_1\rangle$

... ok

Harrow - Hassidim - Lloyd algorithm (2008)

This algorithm solves linear systems of equations

Problem given $A \in \mathbb{C}^{N\times N}$, $b \in \mathbb{C}^N$ find $x \in \mathbb{C}^N$ st $Ax = b$

The classical Gaussian algorithm takes $O(N^3)$ steps

Recall that the conditioning number of A is $\kappa(A) = \|A\| \cdot \|A^{-1}\|$ if you fix a norm $\|\cdot\|$. If A is hermitian and positive, we consider $\kappa(A) = \frac{\lambda_{max}}{\lambda_{min}}$

A is s-sparse if every row of A contains at most s non-zero elements

To solve the linear problem $Ax = b$ with A positive hermitian s-sparse we can use the conjugate gradient algorithm with $O(N \cdot s \cdot \kappa(A) \cdot \log 1/\varepsilon)$ to get a solution closer than ε to a solution

The HHL algorithm, for A pos. herm. s-sparse takes $O(\log N \cdot s^2 (\kappa(A))^2/\varepsilon)$ which looks like an exponential improvement, but you don't actually get x but "expectations" of x (a quantum state that encodes x, usually x up to a phase)

We will get $\frac{1}{\|x\|}|x\rangle$ so we can measure for any observable $M \in \mathbb{C}^{N\times N}$ the quantity $\left(M\right)_{\frac{|x\rangle}{\|x\|}} = \frac{\langle x|Mx\rangle}{\|x\|^2}$

A recent result (Wossing, 2018) shows that A is not s-sparse you can solve on a quantum device with $O(\sqrt{N}\log N \kappa^2)$

The first physical implementation for (simplified) HHL was in 2013

There are two main ideas for the HHL algorithm

1] We use QPE on $U = e^{2\pi i A}$, so we need an efficient implementation of U (actually controlled U)

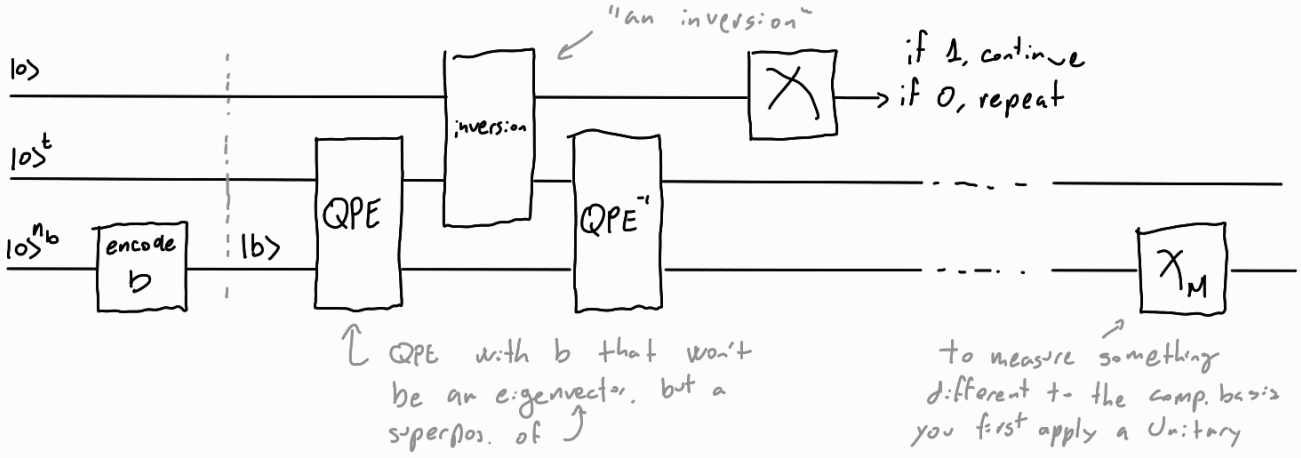
this part is called Hamiltonian Simulation, and we'll take it for granted

2] "branch selection step"

we measure the ancilla and according to the outcome we perform quantum operations on the I/O

Registers $\underbrace{H^{n_b}}_{I/O} \otimes \underbrace{H^t \otimes H}_{\text{ancilla}}$

QPE measure



Let's see the inversion gate. It acts on $H^t \otimes H$ on the basis

$$|\ell\rangle \otimes |0\rangle \rightsquigarrow |\ell\rangle \otimes \left(g(\ell)|1\rangle + \sqrt{1-g^2(\ell)}\,|0\rangle\right)$$

$$|\ell\rangle \otimes |1\rangle \rightsquigarrow |\ell\rangle \otimes \left(-\sqrt{1-g^2(\ell)}\,|1\rangle + g(\ell)|0\rangle\right)$$

where

$$g(\ell) = \begin{cases} \frac{\lambda_{min}}{\ell/2^t} \approx \frac{1}{\ell}\cdot C & \text{if } \ell > C \\ 0 & \text{otherwise} \end{cases}$$

We assume that $N = 2^{n_b}$ so if we let $b = (b_j)_{j=0}^{N-1}$ the encoding will be $|b\rangle := \sum_{j=0}^{N-1} b_j |j\rangle$ assuming $\|b\| = 1$

After the encoding the state is $|b\rangle \otimes |0\rangle^t \otimes |0\rangle$

If we perform QPE on $|b\rangle$ with $U = e^{2\pi i A}$, by Bertrand's theorem we get $A = \sum_{k=0}^{N-1} \lambda_k |\varphi_k\rangle\langle\varphi_k|$, $|b\rangle = \sum_{k=0}^{N-1} b_k |\varphi_k\rangle$

↑ ... non gli stessi b_j no?

Then $U|\varphi_k\rangle = e^{2\pi i \lambda_k} |\varphi_k\rangle$ and the $\{|\varphi_k\rangle\}$ are an orthonorm. basis

After the QPE we get $\sum_{k=0}^{N-1} \sum_{\ell=0}^{N-1} \beta(\ell, \lambda_k) b_k |\varphi_k\rangle^{n_b} \otimes |\ell\rangle^t \otimes |0\rangle$

where $\beta(\ell, \lambda_k) = \frac{1}{2^t} \sum_{j=0}^{2^t-1} e^{2\pi i (\lambda_k - \frac{\ell}{2^t}) j}$

To simplify let us assume that all the eigenvalues λ_k can be written as $\lambda_k = \frac{\ell_k}{2^t}$ for some $\ell_k \in \{0, \dots, 2^t - 1\}$

In this case the state is simply

$$\sum_{k=0}^{N-1} b_k |\varphi_k\rangle \otimes |2^t \lambda_k\rangle^t \otimes |0\rangle$$

When we apply the inversion we get

$$\sum_{k=0}^{N-1} b_k |\varphi_k\rangle \otimes |2^t \lambda_k\rangle^t \otimes \left(\frac{c}{2^t \lambda_k} |1\rangle + \sqrt{1 - \left(\frac{c}{2^t \lambda_k}\right)^2} |0\rangle \right)$$

Then we apply QPE^{-1} we get (we're kind of restoring the H^t register)

$$\sum_{k=0}^{N-1} \frac{c}{2^t \lambda_k} b_k |\varphi_k\rangle \otimes |0\rangle^t \otimes |1\rangle + \sqrt{1 - \left(\frac{c}{2^t \lambda_k}\right)^2} b_k |\varphi_k\rangle \otimes |0\rangle^t \otimes |1\rangle$$

If we measure the ancilla we get 1 with probability

$$P(1) = \left\| \sum_{k=0}^{N-1} b_k |\varphi_k\rangle \otimes |0\rangle^t \frac{c}{2^t \lambda_k} \right\|^2 = \left\| \sum_{k=0}^{N-1} b_k |\varphi_k\rangle \otimes |0\rangle^t \frac{\lambda_{min}}{\lambda_k} \right\|^2 =$$

by orthogonality ↳ $= \sum_{k=0}^{N-1} |b_k|^2 \left(\frac{\lambda_{min}}{\lambda_k}\right)^2 \geq \left(\frac{\lambda_{min}}{\lambda_{max}}\right)^2 = \kappa(A)^{-2}$

If we get 1 after measuring, the state is

$$\underbrace{\frac{c}{2^t} \underbrace{\sum_{k=0}^{N-1} \frac{b_k}{\lambda_k} |\varphi_k\rangle}_{|A^{-1}b\rangle} \otimes |0\rangle^t \otimes |1\rangle}_{\frac{|A^{-1}b\rangle}{\|A^{-1}b\|}}$$

So the final state is: $\frac{|x\rangle}{\|x\|} \otimes |0\rangle^t \otimes |1\rangle$

9/12

Quantum Walks

Suppose we have $G = (V, E)$ undirected, connected graph with no multiple edges, no loops (from a node to itself)

V is the set of nodes labeled from 0 to $N-1$

E is the set of edges

Every graph has an associated matrix, the adjacency matrix $A = (A_{ij})$

where $A_{ij} = \begin{cases} 1 & \text{if } v_i \text{ and } v_j \text{ are connected} \\ 0 & \text{otherwise} \end{cases}$

A classic random walk on G is a stocastic process without memory (Markov chain) where for each node i we have a discrete probability function yielding $\text{prob}(i \to j)$ for j neighbor of i:
The natural way to represent these probability distributions is by the Transition matrix $P = (p_{ij})$ which can be done either by rows or by columns, being respectively row-stocastic or column-stocastic

We'll work with d-regular graphs, that is each node has exactly d neighbors

<u>ex</u> cycles are 2-regular

n-dimensional hypercubes are n-regular

Note that in an undirected graph, A is symmetric but P isn't necessarily.
If the graph is d-regular and all the probability functions are uniform, then P is symmetric and $P = \frac{1}{d}A$

A position vector v is a vector the rappresents where the current position is. It can be a vector of the canonical basis if we know exactly the current position/node, or a linear combination of those if we're in a superposition of nodes
By applying P we get the position vector after 1 step

Iterating walk steps _typically_ converge to a stationary distribution (that will be the uniform distribution on all the nodes). We will assume that this is always the case, although clearly there are cases where this doesn't happen

We want to transpose the idea of random walks in a quantum setting.

There are mainly two ways to formalize this:

- coined quantum walks (Aharonov, 1993, well suited for d-reg graphs)
- Szegedy quantum walks (Szegedy, 2004, more general)

So far we've discussed discrete random walks, but we could also consider continuous walks, both classical and quantum

Coined quantum walks

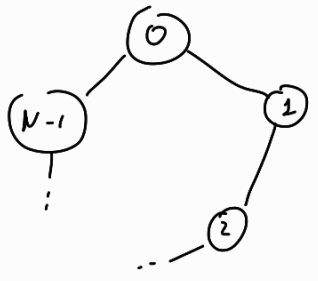
$G=(V,E)$ with all the hypotesis, $|V| = N = 2^n$

The space we will work on is $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$ that is a product of a "coin" space and a "position" space

A state in $\mathcal{H}$ is $|k,p\rangle := |k\rangle \otimes |p\rangle$ which represents being at node $p \in \{0,\dots,N-1\}$ with the coin-toss resulting in k

For a cycle graph

$$\mathcal{H} = \underbrace{\mathcal{H}_c}_{1 \text{ qubit}} \otimes \underbrace{\mathcal{H}_p}_{n \text{ qubits}} =$$



The typical choice for the coin operator is an operator that gives each state equal probability, namely the Hadamard gate, so

$$C : \mathcal{H} \longrightarrow \mathcal{H}$$
$$|k,p\rangle \rightsquigarrow |Hk,p\rangle$$

This models a balanced coin. We then perform a shift operator which models the "jump to the next node"

$$S: \mathcal{H} \longrightarrow \mathcal{H}$$
$$|k,p\rangle \rightsquigarrow |k,\ p + (-1)^k\rangle \quad (\text{mod } N)$$

some authors also impose that the shift operator flips the coin, so it also sends $|k\rangle$ to $|k \oplus 1\rangle$

The walk operator is given by the composition $W = SC$, and each application of W models a single Quantum Walk step
This is sometimes referred as "flip-flop quantum walks"

The reason why we need to add the coin space is so that the resulting operator is Unitary

Let's see a Quantum Walk algorithm

QW Algorithm

1] Prepare the state

2] repeat T times

- apply C
- apply S

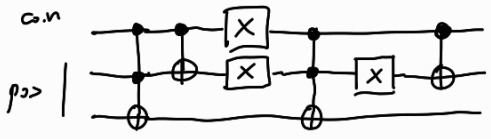
3] measure

Note that there is no randomness in this algorithm, step 2 is deterministic ! the randomness comes only from the measure
Also, because the step is unitary, in this case there is no limit stationary distribution (unitary keep distances so you cant get closer)
There is instead the notion of "limiting distributions" (limit of partial time averages)

Ex in a 4-cycle $\mathcal{H} = \underbrace{\mathcal{H}_c}_{1 \text{ qubit}} \otimes \underbrace{\mathcal{H}_q}_{2 \text{ qubit}}$

The coin operator is $C = H \otimes \mathbb{1}$

One way to implement the shift operator is the following circuit



eg. on $|0\rangle \otimes |00\rangle$ we get

$$|0\rangle\otimes|00\rangle \to |0\rangle\otimes|00\rangle \to |0\rangle\otimes|00\rangle \to |1\rangle\otimes|10\rangle \to |1\rangle\otimes|11\rangle \to |1\rangle\otimes|01\rangle \to |1\rangle\otimes|11\rangle$$

Quantum walks on an n-dimensional hypercube

The definition of n-dimensional hypercube we're going to use is the following

Def An n-dimension hypercube is a graph who's vertices are labeled with binary strings of length n and where two nodes are adjacient if they have Hamming-distance 1

$N = 2^n$ nodes, $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$ with basis $\left\{ |a, v\rangle \;\middle|\; 0 \le a \le n-1,\ v \in \{0,1\}^n \right\}$

The meaning of the coin value a is which digit in the label should be changed to get to the neighbor (0-indexed)

The shift operator acts as $S|a, v\rangle = |a, v \oplus e_a\rangle$ where e_a is the a^{th} elementh of the canonical basis of $\{0,1\}^n$

The coin operator will be a Grover reflection $G = \frac{2}{n} UU^T - I$, where $U = (1, \dots, 1)^T$. Then $W = SG$

Surprise, this is actually the Szegedy formalism, but it just so happens that in the d-regular case, Szegedy formalism becomes a coined Grover walk, which is why we used Grover. In general for this, Szegedy works better

Now we want to use QW to implement a search algorithm on the hypercube.

let M be a set of marked nodes, and $m = |M|$

We start QW on a "suitable" state (a node or a superposition) and we perform QW steps "until" we reach a marked node.

Turns out that we can estimate a priori how many steps we have to take

In this formalism we represent position as edges instead of nodes, so we need 2 registers: one for the current node and one for the previous. Together they identify an edge

$$|G\rangle = \frac{1}{\sqrt{m}} \sum_{x \in M} |x\rangle \otimes |p_x\rangle$$

is a superposition of all the "good" states

with $|p_x\rangle = \sum_y \sqrt{p_{xy}}\, |y\rangle$

is a uniform superposition of neighbors of x

$$|B\rangle = \frac{1}{\sqrt{N-m}} \sum_{x \notin M} |x\rangle \otimes |p_x\rangle$$

We now set $\varepsilon = \frac{m}{N}$, $\vartheta = \arcsin\sqrt{\varepsilon}$, then a uniform superposition of all the edges is $|U\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes |p_x\rangle = \sin\vartheta\, |G\rangle + \cos\vartheta\, |B\rangle$

In the first step of the algorithm, we set the state to $|U\rangle$

In the second step we repeat $O\left(\frac{1}{\sqrt{\varepsilon}}\right)$ (much like Grover) the following routine:

- apply reflection wrt $|B\rangle$
- apply reflection wrt $|U\rangle$

Finally, we measure

To apply the reflection wrt $|B\rangle$ we can use a phase oracle which will do this for us