Introduction to Quantum Computing

Gerardo Pelosi

Dipartimento di Elettronica, Informazione e Bioingegneria - DEIB
Politecnico di Milano

February 23rd, 2022

Introduction

Quantum mechanics

- Currently, the most accurate and complete description of the laws that govern the physical world
- The mathematical formalism on which it is based and the physical reality it describes are related by some fundamental postulates.

Postulate - 1

- A complex Hilbert space, called the state space, is associated to each isolated physical system.
- An Hilbert complex space is a **vector space** V over $\mathbb{C}$ with a **scalar product** $(\cdot,\cdot) : V \times V \to \mathbb{C}$ which is **complete** w.r.t. the norm $||v|| = \sqrt{(v,v)}$. For us, the space is always **finite**, thus the completeness is always satisfied. $\forall v, w \in V,\ (v,w) = (w,v)^*$
- The system is completely described by its state vector, which is a unit vector ($||v|| = 1$) in the state space.

↳ An isolated system is always described by a state vector.

Dirac notation → used to denote quantum states

In quantum mechanics, bra–ket notation, or Dirac notation, is used ubiquitously to denote quantum states. The notation uses angle brackets, $\langle$ and $\rangle$, and a vertical bar $|$, to construct "bras" and "kets".

Bras and kets

- A ket is of the form $|v\rangle$. It denotes a **column vector**, $\boldsymbol{v}$, in a Hilbert space V, and physically it represents a quantum state.
- A bra is of the form $\langle f|$. It denotes a **linear form** $f : V \to \mathbb{C}$, i.e., a linear map that maps each item in V to an element in $\mathbb{C}$, multiplying each coordinate of the chosen item $|v\rangle$ by a possibly different complex number (collectively denoted by f) and summing up all the partial products. Letting the linear functional $\langle f|$ act on a vector $|v\rangle$ is written as $\langle f \mid v\rangle \in \mathbb{C}$.
- Usually the inner product of an Hilbert space V is denoted as the linear form resulting from the application of a bra to a ket, where the bra is in turn identified with a (row) vector in V such that $\langle w| = (|w\rangle^*)^T$, or with an equivalent notation $\langle w| = |w\rangle^\dagger$.

bras and kets - Examples

$u, v, w, z \in V$, with $V \equiv \mathbb{C}^2$

- $|v\rangle = \begin{bmatrix} v_0 \\ v_1 \end{bmatrix}$, $|w\rangle = \begin{bmatrix} w_0 \\ w_1 \end{bmatrix}$
- $\langle v| = \begin{bmatrix} v_0^* & v_1^* \end{bmatrix}$, $\langle w| = \begin{bmatrix} w_0^* & w_1^* \end{bmatrix}$
- $\langle v \,|\, w\rangle = \langle w \,|\, v\rangle^* \Leftrightarrow v_0^* w_0 + v_1^* w_1 = (w_0^* v_0 + w_1^* v_1)^*$
- $\langle v \,|\, w\rangle = 0$ iif the two vectors are orthogonal.

  E.g., $|v\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, $|w\rangle = \begin{bmatrix} -b^* \\ a^* \end{bmatrix}$
- $\langle v \,|\, \beta_1 w + \beta_2 z\rangle = \beta_1 \langle v \,|\, w\rangle + \beta_2 \langle v \,|\, z\rangle$
- $\langle \alpha_1 v + \alpha_2 u \,|\, w\rangle = \alpha_1^* \langle v \,|\, w\rangle + \alpha_2^* \langle u \,|\, w\rangle$

  α_1, α_2 needs to be coniugated because as a convention everything that is inside a bra should be assumed to be already conjugated.
- the outer product $|v\rangle \langle w|$ equals $\begin{bmatrix} v_0 w_0^* & v_0 w_1^* \\ v_1 w_0^* & v_1 w_1^* \end{bmatrix}$

Global phase invariance

A state in a quantum system is represented by a set of vectors in an Hilbert Space such that any 2 vectors in this set may differ for a multiplicative factor, which is a phase factor

Global phase does not matter as it cannot be measured

- A state in a quantum system is modeled picking a representative element in a *vector equivalent class*.
- The vector equivalent class of a quantum state is a set that includes all vectors which differ among each other for a *multiplicative phase* factor, i.e., the states $e^{i\theta}|\psi\rangle$ and $|\psi\rangle$.
- The states $e^{i\theta}|\psi\rangle$ and $|\psi\rangle$ cannot be distinguished by measuring them in real world thus, we consider them mathematically equivalent.
- θ is called: *global phase factor*.

Quantum bits

State space

An Hilbert complex space is a **vector space** V over $\mathbb{C}$ with a **scalar product** $(\cdot,\cdot) : V \times V \to \mathbb{C}$ which is **complete** w.r.t. the norm $||v|| = \sqrt{(v,v)}$. For us, the space is always **finite**, thus the completeness is always satisfied.

Qubit: Definition

The simplest isolated physical system is a single **qubit**. It is described by a vector in $\mathbb{C}^2$. In practice, we need to choose a basis to represent it:

- The **computational** basis $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ is orthonormal
- The notation for a qubit is: $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ $(\alpha_0, \alpha_1 \in \mathbb{C})$
- To be a unit vector $|\psi\rangle$ must exhibit the following condition:
  - $|\alpha_0|^2 + |\alpha_1|^2 = 1$ or, equivalently,
  - $(|\psi\rangle, |\psi\rangle) = \langle\psi\,|\,\psi\rangle = 1$, recalling that $\langle\psi| = (|\psi\rangle^*)^T = |\psi\rangle^\dagger$

$|\psi\rangle$ is unitary $\Leftrightarrow$
$||\psi\rangle| = 1 \Leftrightarrow |\langle\psi|\psi\rangle| =$
$= |\alpha_0|^2 + |\alpha_1|^2 = 1$

Relative phase matters, global phase does not

It can be shown that relative phase yields different measurements, while global phase does not

Relative phase

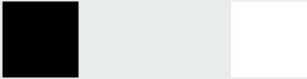
Note that a *relative phase factor* is physically significant, i.e., $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and $|\varphi\rangle = \alpha_0 |0\rangle + \underbrace{e^{i\theta}}_{\text{relative phase factor}}\alpha_1 |1\rangle$ are distinct (not equivalent) qubits.

two quantum states are indistinguishable when it is possible to obtain one of them through a global phase factor. In this slide it is presented a relative phase factor that cannot be used to retrieve the value of another indistinguishable state, therefore it's application yields different qubits.

Information and representation

Classic Bit

A classic bit is deterministically either 0 or 1:



The state of a classical bit is not altered by the process of reading it

Quantum Bit

A qubit allows us to map any linear superposition of 0 and 1 into it

A qubit ψ is defined as: $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle\, ; \alpha_0, \alpha_1 \in \mathbb{C}$, with $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Rightarrow |\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$

Quantum bits

Nature prevents us from directly measuring the values α_0 and α_1 ... we cannot find out the state of a qubit directly!

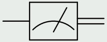
What do α_0 and α_1 actually mean?

Consider a qubit $|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$.

Define the measurement as a function $M(|\psi\rangle)$ with codomain $\{0, 1\}$:

- $\mathrm{Prob}(M(|\psi\rangle) = 0) = |\alpha_0|^2$, $\mathrm{Prob}(M(|\psi\rangle) = 1) = |\alpha_1|^2$

Therefore, it must be $|\alpha_0|^2 + |\alpha_1|^2 = 1$

$|\psi\rangle$  0 *or* 1

- The superposition state is destroyed after measurement! Measurements are irreversible! (continuing to measure after the 1st obs. yields the same result!)
- We cannot directly measure the superposition, we can only get the samples of a binary random variable with a distribution linked to α_0, α_1 (... more on measurements and their actual working in the last part of this lecture...)

Quantum bits

Change of basis

Any basis in $\mathbb{C}^2$ can be used as a computational basis and physical measurement basis.
The qubits $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ are a basis:

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

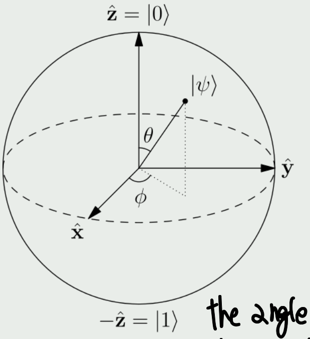
$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_0\left(\tfrac{1}{\sqrt{2}}|+\rangle + \tfrac{1}{\sqrt{2}}|-\rangle\right) + \alpha_1\left(\tfrac{1}{\sqrt{2}}|+\rangle - \tfrac{1}{\sqrt{2}}|-\rangle\right)$$

$$|\psi\rangle = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|+\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|-\rangle$$

Bloch Sphere

It matches the values of a qubit with the points on the surface of a 3D-sphere with a unit radius (it points out how the degrees of freedom in the description of a qubit is equal to two)



$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$

$|\psi\rangle = r_0 e^{i\varphi_0} |0\rangle + r_1 e^{i\varphi_1} |1\rangle$

$r_0, r_1 \in \mathbb{R}, 0 \leq \varphi_0, \varphi_1 < 2\pi$

$r_0^2 + r_1^2 = 1$ denotes a circle, thus assuming

that identifies r_0 as the x axis, r_1 as the y axis

$r_0 = \cos(2\theta), r_1 = \sin(2\theta), 0 \leq \theta < \pi$

the qubit can be rewritten as:

$|\psi\rangle = e^{i\gamma}(\cos(2\theta) |0\rangle + e^{i\phi} \sin(2\theta) |1\rangle)$

where $\gamma = \varphi_0, \phi = \varphi_1 - \varphi_0, 0 \leq \phi < 2\pi$

the angle ϕ represents the rotation of the vector on the plane x-y. Angle θ gives the rotation on the plane z-y.

θ may encode an arbitrary binary string. However, the no. of measurements to recover it is exponential in the string length

The mathematical description of a qubit may correspond to any physical system with at least two physical states that are sufficiently separated

- the two polarization states of a photon (i.e., geometrical direction of oscillation of the electric field in a transverse wave travelling perperdicularly to it)
- the alignment of a nuclear spin in a uniform magnetic field
- two energy levels of an electron orbiting a atom (e.g., H atom)

Crystal of Tourmaline

Qubit: A Real World Example

Crystal of Tourmaline: Classical World (linearly polarized light)

1. Light polarized perpendicularly w.r.t. the crystal axis $\Rightarrow$ goes through
2. Light polarized parallel w.r.t. the crystal axis $\Rightarrow$ filtered
3. Light polarized with angle α w.r.t. the crystal axis $\Rightarrow$ A fraction $(\sin^2 \alpha)$ goes through

Crystal of Tourmaline: Quantum World (single linearly polarized photon)

1. Photon polarized perpendicularly w.r.t. the crystal axis $\Rightarrow$ detected after the crystal
2. Photon polarized parallel w.r.t. the crystal axis $\Rightarrow$ not detected
3. Photon polarized with angle α w.r.t. the crystal axis $\Rightarrow$ A photon perpendicularly polarized is detected after $1/(\sin^2 \alpha)$ trials

Qubit: A Real World Example

* can be put in a 1-to-1 correspondence with

From Physic World to Qubit

Qubit $\overset{*}{\Leftrightarrow}$ the polarization direction of a single photon

$|0\rangle$ photon polarized perpendicular w.r.t. the crystal axis

$|1\rangle$ photon polarized parallel w.r.t. the crystal axis

Superposition state?

A photon polarized with angle α w.r.t. the crystal axis: $|\psi\rangle = \sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle$

Measurement

- The measurement is 0 with prob. $\sin^2\alpha$
- The measurement is 1 with prob. $\cos^2\alpha$
- The photon/qubit is no longer polarized with angle α. What remains is a $|0\rangle$ or $|1\rangle$ photon - NON in superposition → This happens after the measurement.

Quantum registers

tensor product

- A quantum register with n qubits is a unit vector in the Hilbert space $\mathbb{C}^{2^n} = \mathbb{C}^{\otimes n}$ with 2^n dimensions
- the canonical computational base in such a space is described by the 2^n orthonormal unit vectors (labeling the axis of each dimension with a n-bit string)

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

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

$$|000\cdots00\rangle, |000\cdots01\rangle, |000\cdots10\rangle, \dots, |111\cdots1\rangle$$

$$|i_1\, i_2 \cdots i_n\rangle, i_j \in \{0,1\}, 1 \leq j \leq n$$

$|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$

$|i_1\, i_2 \cdots i_n\rangle$ can be derived also as the **tensor product** (right-associative and non-commutative)

$$|i_1\, i_2 \cdots i_n\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle, i_j \in \{0,1\}, 1 \leq j \leq n$$

$|v\rangle, |w\rangle \in \mathbb{C}^2, |v\rangle = \begin{bmatrix}v_0\\v_1\end{bmatrix}, |w\rangle = \begin{bmatrix}w_0\\w_1\end{bmatrix}$

denoted also $|i_1\, i_2 \cdots i_n\rangle = |i_1\rangle\, |i_2\rangle \cdots |i_n\rangle$

$\Rightarrow |v\rangle \otimes |w\rangle = \begin{bmatrix} v_0 \begin{bmatrix}w_0\\w_1\end{bmatrix} \\ v_1 \begin{bmatrix}v_0\\v_1\end{bmatrix} \end{bmatrix} = \begin{bmatrix}v_0 w_0\\v_0 w_1\\v_1 w_0\\v_1 w_1\end{bmatrix}$

Quantum registers

Example

A quantum state $|\psi\rangle$ composed by a pair of qubits $|\psi\rangle = |xy\rangle = |x\rangle \otimes |y\rangle$ can be expressed in the canonical computational basis:

$$|00\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \qquad |01\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|10\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \qquad |11\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$$
$$|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$$

On the tensor product

Properties

- $\forall \ |v\rangle \in V, |w\rangle \in W$:
  $\alpha(|v\rangle \otimes |w\rangle) = (\alpha\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha\,|w\rangle)$ → tensor product is linear w.r.t. the multiplication of a complex number
- $\forall \ |v_1\rangle, |v_2\rangle \in V, |w\rangle \in W$:
  $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$ → tensor product is distributive w.r.t. the sum operation.
- $\forall \ |v_1\rangle, |v_2\rangle \in V, |w\rangle \in W$:
  $|w\rangle \otimes (|v_1\rangle + |v_2\rangle) = |w\rangle \otimes |v_1\rangle + |w\rangle \otimes |v_2\rangle$

Exercise

- Denoting with b_i^m, $1 \leq i \leq m$ the unit orthonormal vector in $\mathbb{C}^m$ with the i-th coordinate asserted and the other ones equal to zero, prove that $b_i^m \otimes b_j^k = b_{(i-1)k+j}^{mk}$
- Prove that $\langle v \otimes w \,|\, v' \otimes w' \rangle = \langle v \,|\, v' \rangle \langle w \,|\, w' \rangle$ with $v, v' \in \mathbb{C}^m$ and $w, w' \in \mathbb{C}^k$

On the tensor product

Matrices

- $\forall\ M : \mathbb{C}^m \mapsto \mathbb{C}^m,\ \ N : \mathbb{C}^k \mapsto \mathbb{C}^k$

$$M \otimes N : \mathbb{C}^{mk} \mapsto \mathbb{C}^{mk}, \quad M \otimes N = \begin{bmatrix} M_{11}N & M_{12}N & \dots & M_{1m}N \\ \cdots & \cdots & \cdots & \cdots \\ M_{k1}N & M_{k2}N & \dots & M_{km}N \end{bmatrix}$$

- $M = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$, $N = \begin{bmatrix} 1 & -1 \\ 1 & 2 \end{bmatrix}$, $M \otimes N = \begin{bmatrix} 1 & -1 & 3 & -3 \\ 1 & 2 & 3 & 6 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 2 \end{bmatrix}$

Properties (.. prove them as an exercise)

- $(M \otimes N)(v \otimes w) = (Mv) \otimes (Nw)$
- $(\alpha M + \alpha' M') \otimes (\beta N + \beta' N') = \dots$ $\otimes$ is distributive w.r.t. $+$
- $(M \otimes N)(M' \otimes N') = (MM' \otimes NN')$ and $(M \otimes N)^\dagger = M^\dagger \otimes N^\dagger$
- M, N unit (or invertible) matrices $\Rightarrow$ $M \otimes N$ is a unit (invertible) matrix

Entangled states

- Not every state of a quantum registers with n qubit can be decomposed as the tensor product of single qubit states.
- The states of this type are called **entangled** and enjoy properties that cannot be found in any object of classic physics.
- qubits belonging to a register in an entangled state do not have an individual status but only a shared status.
  - they behave as if they were closely related to each other regardless of the distance that separates them.
  - E.g., a measurement of the state of a qubit belonging to a pair of entangled qubits provides information about the state of the other simultaneously
    [...entanglement is crucial for *teleportation*, that is the transfer of a quantum state from one location (where the qubit is destroyed) to another (where another qubit identical to the former is built)]

Entangled states

Example

The quantum state $|00\rangle + |11\rangle$ cannot be tensor factored in the states of two independent qubits. Indeed, given $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, and $|\varphi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ with $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$

$$|\psi\rangle \otimes |\varphi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) =$$

$$= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$$

Searching for coefficients values such that $|\psi\rangle \otimes |\varphi\rangle = |00\rangle + |11\rangle$ implies that the following set of simultaneous equalities must hold

$$\begin{cases} \alpha_0\beta_0 & = & 1 \\ \alpha_0\beta_1 & = & 0 \\ \alpha_1\beta_0 & = & 0 \\ \alpha_1\beta_1 & = & 1 \end{cases}$$

As it can be easily verified, there is no solution.

Evolution of a closed quantum system

Postulate - 2 - of Quantum Mechanics

The evolution of a closed quantum system is described by a unit transformation: the state of the system $|\psi\rangle$ at time t_1 is linked to the state of the system $|\psi'\rangle$ at time t_2 by means of a unitary operator U that depends only on t_1 and t_2,

$$|\psi'\rangle = U\,|\psi\rangle$$

What is a unit operator in an Hilbert space? ... next slides

 → We need these concepts in order to understand what a unitary operator is

Definition of adjoint linear operator L

Given a linear operator L in an Hilbert space V (i.e., a matrix), there exists a unique linear operator $L^\dagger$ called *adjoint operator of* L such that $\forall\ |v\rangle, |w\rangle \in V$:

$$(|v\rangle, L|w\rangle) = (L^\dagger|v\rangle, |w\rangle) \quad \text{or, in equivalent notation,} \quad \langle v \,|\, Lw\rangle = \langle L^\dagger v \,|\, w\rangle$$

- A linear operator L is Normal (i.e., diagonalizable) iif $LL^\dagger = L^\dagger L$
- A linear operator L is Hermitian iif $L = L^\dagger$ ↗ Since $L^\dagger = (L^T)^* = (L^*)^T$, if $L = L^\dagger \Rightarrow L$ is symmetric (related to the transpose) and all its values are real (related to the conjugate)
  - A Hermitian operator is Normal. Viceversa (Thm), a Normal operator is Hermitian only if it has real eigenvalues
- A unit operator U is such that $U^{-1} = U^\dagger \Leftrightarrow U^\dagger U = I$
  - A unit operator is Normal and preserves the internal products:

$$\langle Uv \,|\, Uw\rangle = \langle U^\dagger Uv \,|\, w\rangle = \langle Iv \,|\, w\rangle = \langle v \,|\, w\rangle$$

This property allows to prove that $||U v\rangle| = 1 \Rightarrow$ For this reason it is called UNITARY operator.

Evolution of a closed quantum system

- A unit operator U admits an inverse $U^\dagger \implies$ the evolution of a qubit can go forth and back ... the effect of an operator can be always reverted
- Applying a unit operator to a unit vector ($\langle v \mid v \rangle = 1$) yields another vector $w = Uv$ that is also a unit ($\langle w \mid w \rangle = 1$)

Exercise

Prove that the following *Pauli* matrices[a]

$$\text{NOT operator} \leftarrow \mathtt{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \mathtt{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \mathtt{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

are unit matrices (here, i denotes the imaginary unit, i.e.: $i = \sqrt{-1}$) and verify that $\mathtt{Y} = i\mathtt{XZ}$.

[a] they describe the projections of the spin of an electron along the axes x, y, z, respectively

Evolution of a closed quantum system

Unit operator

It can be proved that a unit operator in the Hilbert space $\mathbb{C}^2$ is in one-to-one correspondence with the following:

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

Evolution of a closed quantum system

On linear operators

Any linear operator A in an Hilbert space $V = \mathbb{C}^{\otimes m}$ may be written as

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

$$A = \sum_{i,j \in \{0,\ldots,2^m-1\}} \left(a_{i,j} \left|i\right\rangle \left\langle j\right| \right)$$

where $|i\rangle, |j\rangle$ denote the i-th and j-th orthonormal vector in the canonical computation basis of V (i.e., $|i\rangle = |\texttt{bin(i)}\rangle$) E.g., if $m = 2$, $V = \mathbb{C}^{2^2}$ then $|0\rangle = |00\rangle, |1\rangle = |01\rangle, |2\rangle = |10\rangle, |3\rangle = |11\rangle$.

E.g., if $m = 1$, $V = \mathbb{C}^2$ then $A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} = a_{00}\,|0\rangle\langle 0| + a_{01}\,|0\rangle\langle 1| + a_{10}\,|1\rangle\langle 0| + a_{11}\,|1\rangle\langle 1|$

Linear operator corresponding to a change of basis

Assume $|\psi_1\rangle$ and $|\psi_2\rangle$ be a basis for the space $\mathbb{C}^2$. If $|0\rangle = b_{11}\,|\psi_1\rangle + b_{21}\,|\psi_2\rangle$ and $|1\rangle = b_{12}\,|\psi_1\rangle + b_{22}\,|\psi_2\rangle$, then the matrix to apply a basis change is: $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, and a state $(\alpha, \beta)^T$ in the canonical basis is transformed into a state in the basis $|\psi_1\rangle$, $|\psi_2\rangle$ by performing $B(\alpha, \beta)^T$.

Quantum Gates acting on a single qubit

Unit operators in a finite Hilbert space are also called Quantum Gates. They allow to modify the state of a quantum register, giving rise to quantum computations.

- Similar to classic computers, a quantum computer is formed by quantum circuits consisting of *elementary quantum gates*.

The $\mathtt{X}$ Gate

- The classic `NOT` gate is fed with a single bit and yields a bit value that is the opposite of the input value
- To define an analogous quantum operation, we cannot limit ourselves to establish its action on basic states $|0\rangle$ and $|1\rangle$, but we must specify also how it acts on a qubit in a superposition state

Intuitively, a quantum `NOT` gate should exchange the two fundamental states of a qubit and transform $\alpha|0\rangle + \beta|1\rangle$ into $\beta|0\rangle + \alpha|1\rangle$

- this also fulfill the condition $|\alpha|^2| + |\beta|^2 = 1$ before and after the gate
- $\mathtt{X}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ fits the purpose $\mathtt{X}^{-1}=\frac{1}{\det(X)}\begin{bmatrix}0 & -1\\ -1 & 0\end{bmatrix}$, $\det=-1$; $\mathtt{X}^{\dagger}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \Rightarrow \mathtt{X}^{-1}=\mathtt{X}^{\dagger}$

Requirement for X to be a unitary operator

Quantum Gates acting on a single qubit

The Z Gate

The gate $\mathtt{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ acts only on the $|1\rangle$ component of a qubit $|\psi\rangle$ changing its sign. Thus, if $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ then $\mathtt{Z}|\psi\rangle = \alpha_0 |0\rangle - \alpha_1 |1\rangle$

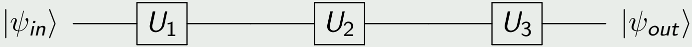
The H Gate

↳ Perfect Random Number Generator

The Hadamard gate $\mathtt{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is used quite often in quantum computing. It has the effect to transform a fundamental state $|0\rangle$ or $|1\rangle$ in a superimposition of states such that proceeding with a measurement, the chances to get a 0 or a 1 are 50% (i.e., perfectly balanced)

- Its effect can be thought as the one deriving from a "half-application" of an X gate ...
- on the Bloch sphere, its application corresponds to a 90° rotation around the *y*-axis, followed by a reflection through the plane (x, y)

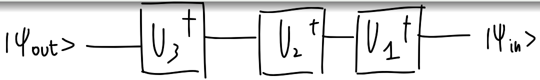
From Gates to Circuits



$$|\psi_{out}\rangle = U_3 U_2 U_1 |\psi_{in}\rangle$$

Reversibility: The way back!

$$|\psi_{in}\rangle = U_1^\dagger U_2^\dagger U_3^\dagger |\psi_{out}\rangle$$



Examples. Assume to work in $\mathbb{C}^2$

$$|0\rangle \;\text{—}\boxed{H}\text{—}\boxed{Z}\text{—}\boxed{H}\text{—} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}$$

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

$\Rightarrow HZH = X$

$$= \frac{1}{2}\begin{bmatrix}0 & 2\\ 2 & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = X\,|0\rangle = |1\rangle$$

$$|1\rangle \;\text{—}\boxed{H}\text{—}\boxed{X}\text{—}\boxed{H}\text{—} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}$$

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

$\Rightarrow HXH = Z$

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

$$= -\,|1\rangle$$

Quantum Circuits with a single qubit

Examples...(this notation we'll be useful to work in a generic $\mathbb{C}^{\otimes n}$, assuming $H^{\otimes n}$ etc...)

Note that in the fundamental computational basis:

- $X|0\rangle = |1\rangle$, and $X|1\rangle = |0\rangle$
- $Z|0\rangle = |0\rangle$, and $Z|1\rangle = -|1\rangle$
- $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

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

Therefore:

$$|0\rangle \;—\boxed{H}—\boxed{Z}—\boxed{H}—$$

$$H\left(Z\left(H|0\rangle\right)\right) = H\left(Z\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right) = H\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \left[\frac{|0\rangle+|1\rangle}{2}\right] - \left[\frac{|0\rangle-|1\rangle}{2}\right] = |1\rangle$$

$$|1\rangle \;—\boxed{H}—\boxed{X}—\boxed{H}—$$

$$H\left(X\left(H|1\rangle\right)\right) = H\left(X\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right) = H\left(\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle\right) = \left[\frac{|0\rangle-|1\rangle}{2}\right] - \left[\frac{|0\rangle+|1\rangle}{2}\right] = -|1\rangle$$

Interlude: eigenvalues and eigenvectors

Definition

- Given a linear transform T on a vector space V over a field K, an *eigenvector* of T is a non null vector $v \in V$ such that $T(v) = \lambda v$ for $\lambda \in K$. λ is the eigenvalue associated to v
- In our case V is finite-dimensional: $Tv = \lambda v$, where T is a matrix representation of the transform
- For a n-dimensional linear operator T we will denote its eigenvectors as $|\ell_{0,T}\rangle, |\ell_{1,T}\rangle, \ldots, |\ell_{n-1,T}\rangle$ and the corresponding eigenvalues as $\lambda_{0,T}, \lambda_{1,T}, \ldots, \lambda_{n-1,T}$

Computing eigenvalues and eigenvectors

- We compute $\lambda_{0,T}, \lambda_{1,T}, \ldots, \lambda_{n-1,T}$ solving $\det(T - \lambda I) = 0$ for λ
- We compute $|\ell_{0,T}\rangle, |\ell_{1,T}\rangle, \ldots, |\ell_{n-1,T}\rangle$ solving $\forall i\{0, \ldots, n-1\}\ T|\ell_{i,T}\rangle = \lambda_{i,T}|\ell_{i,T}\rangle$

Measurements

- The **set of possible outcomes** of a measure depends only on the nature of the measurement apparatus
- The **possible outcomes** of the measurement are the **eigenvalues** $\lambda_{i,M}$ of the measurement operator M
- After measurement the qubit state collapses to one of $|\ell_{i,M}\rangle$ of the measurement operator M even if before it could only be described with a superimposition of $|\ell_{i,M}\rangle$
- The **measurement** is described by a **linear operator** which can be shown to be **Hermitian**
  - It makes sense, given that its eigenvalues are real-valued

Outcome of a measurement: Born rule

Born measurement rule

Given a measurement operator M, a measure $\textsc{Meas}(|\psi\rangle, M)$ on $|\psi\rangle \in \mathbb{C}^{\otimes n}$ yields:

$$\text{For any } i \in \{0, \ldots, 2^n - 1\} \;\; \lambda_{i,M}, \text{ with probability } \langle \psi | \ell_{i,M} \rangle \langle \ell_{i,M} | \psi \rangle = |\langle \ell_{i,M} | \psi \rangle|^2$$

- The measured state $|\psi\rangle$ collapses to the $|\ell_{i,M}\rangle$ corresponding to the eigenvalue $\lambda_{i,M}$ obtained as the measurement outcome
  - The previous fact implies that taking further measurements with M, without disturbing the quantum state, yields the same outcome!
- A measurement gives an output with certainty iff the state being measured is an eigenvector of the measurement operator
  - $\textsc{Meas}(|\ell_{i,M}\rangle, M)$ is obtained with Pr$= |\langle \ell_{i,M} | \ell_{i,M} \rangle|^2 = |1|^2 = 1$, without changes to the measured state

Measuring in the computational basis

Pulling back out our classical bits

- We chose to encode a classic 0 as $|0\rangle$ and a classic 1 as $|1\rangle$
- We would like to build a measurement apparatus which measures coherently with that
- We need M s.t. $\lambda_{0,M} = 0$ with $|\ell_{0,M}\rangle = |0\rangle$ and $\lambda_{1,M} = 1$ with $|\ell_{1,M}\rangle = |1\rangle$

$$\begin{bmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow M = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

- Testing if it works:
  - $\textsc{Meas}(|0\rangle, M)$ yields 0 with $\Pr = \langle 0 \,|\, 0 \rangle \langle 0 \,|\, 0 \rangle = 1$, and 1 with $\Pr = \langle 0 \,|\, 1 \rangle \langle 1 \,|\, 0 \rangle = 0$
  - $\textsc{Meas}(|1\rangle, M)$ yields 0 with $\Pr = \langle 1 \,|\, 0 \rangle \langle 0 \,|\, 1 \rangle = 0$, and 1 with $\Pr = \langle 1 \,|\, 1 \rangle \langle 1 \,|\, 1 \rangle = 1$
- $\textsc{Meas}(|\psi\rangle, M)$, with $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, yields 0 with $\Pr = \langle \psi | 0 \rangle \langle 0 | \psi \rangle = \alpha_0^* \alpha_0$

Using a lin.op. with the computational basis as eigenvectors

- Consider $|\psi\rangle = H|0\rangle = |+\rangle$ which is in the following state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$
- What is the result of $\textsc{Meas}(|\psi\rangle, M_{comp})$,

  $M_{comp} = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$, $\lambda_{0,M_{comp}} = 0, \lambda_{1,M_{comp}} = 1, |\ell_{0,M_{comp}}\rangle = |0\rangle, |\ell_{1,M_{comp}}\rangle = |1\rangle$?

  $$\textsc{Meas}(|\psi\rangle, M_{comp}) = \begin{cases} 0 & \text{with Pr} = \langle\psi\,|\,0\rangle\langle 0\,|\,\psi\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} = \frac{1}{2}, \text{ leaving } |\psi\rangle \text{ as } |0\rangle \\ 1 & \text{with Pr} = \langle\psi\,|\,1\rangle\langle 1\,|\,\psi\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} = \frac{1}{2}, \text{ leaving } |\psi\rangle \text{ as } |1\rangle \end{cases}$$
- Basically, we've just built a perfect random number generator!

Measuring in the polar basis

Using a lin.op. with the polar basis as eigenvectors

- Consider still $|\psi\rangle = H|0\rangle = |+\rangle$ which is in the following state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$
- What is the result of $\textsc{Meas}(|\psi\rangle, M_{pol})$,

  $M_{pol} = \begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$, $\lambda_{0,M_{pol}} = 1, \lambda_{1,M_{pol}} = -1, |\ell_{0,M_{pol}}\rangle = |+\rangle, |\ell_{1,M_{pol}}\rangle = |-\rangle$?

$$\textsc{Meas}(|\psi\rangle, M_{pol}) = \begin{cases} 1 & \text{with Pr} = \langle\psi|+\rangle\langle+|\psi\rangle = \langle+|+\rangle\langle+|+\rangle = 1 \\ -1 & \text{with Pr} = \langle\psi|-\rangle\langle-|\psi\rangle = \langle+|-\rangle\langle-|+\rangle = 0 \end{cases}$$

- Measuring with M yields with certainty $\lambda_{0,M_{pol}} = 1$ when $|\psi\rangle = |+\rangle$, and yields $\lambda_{0,M_{pol}} = 1$ with $\Pr < 1$ when $|\psi\rangle \neq |+\rangle$
  - and yields with certainty $\lambda_{1,M_{pol}} = -1$ when $|\psi\rangle = |-\rangle$, and yields $\lambda_{1,M_{pol}} = -1$ with $\Pr < 1$ when $|\psi\rangle \neq |-\rangle$

Avoiding a common misconception

- Measuring according to a given Hermitian operator M is different from applying it to the quantum state: $\textsc{Meas}(|\psi\rangle, M) \neq M|\psi\rangle$

$\textsc{Meas}(|\psi\rangle, M)$

- M only needs to be Hermitian
- After $\textsc{Meas}(|\psi\rangle, M)$ yields $\lambda_{i,M}$, we have that $|\psi\rangle$ collapses to $|\ell_{i,M}\rangle$
- (Generally) irreversible procedure

$M|\psi\rangle$

- M must be Hermitian and unitary
- After $M|\psi\rangle$, we have ... $|M\psi\rangle$
- Reversible procedure

Generalized Born rule

Skipped

What if we measure a single qubit out of a multi-qubit state?

Consider $|\psi\rangle \in \mathbb{C}^{\otimes(n+1)}$, we can rewrite it as $|\psi\rangle = \alpha_0 |0\rangle |\phi_0\rangle + \alpha_1 |1\rangle |\phi_1\rangle$, with proper $|\phi_0\rangle, |\phi_1\rangle \in \mathbb{C}^{\otimes n}$ and $|\alpha_0|^2 + |\alpha_1|^2 = 1$ (these are possibly unknown to us, but the writing is legit!)

- We rewrite further, in the $(n+1)$-qubit comp. basis as $|\psi\rangle = \sum_{a=0}^{2^{n+1}-1} \gamma_a |\mathtt{bin}(a)\rangle$
- We can thus express $|\phi_0\rangle, |\phi_1\rangle$ as normalized, (but not necessarily orthogonal) vectors:

$$|0\rangle |\phi_0\rangle = \frac{1}{\alpha_0} \sum_{a=0}^{2^n-1} \gamma_a |0\mathtt{bin}(a)\rangle \text{ and } |1\rangle |\phi_1\rangle = \frac{1}{\alpha_1} \sum_{b=0}^{2^n-1} \gamma_b |1\mathtt{bin}(b)\rangle$$

- We obtain $\alpha_0^2 = \sum_{a=0}^{2^n-1} |\gamma_a|^2$, $\alpha_1^2 = \sum_{b=0}^{2^n-1} |\gamma_b|^2$

Generalized Born rule

Outcome of the measure and state collapse

Consider $|\psi\rangle \in \mathbb{C}^{\otimes(n+1)}$, and measure its most-significant (leftmost) qubit with M_{comp}.

- The measurement yields 0 with $\Pr = \alpha_0^2$ leaving $|\psi\rangle$ in $|0\rangle|\phi_0\rangle$
- The measurement yields 1 with $\Pr = \alpha_1^2$ leaving $|\psi\rangle$ in $|1\rangle|\phi_1\rangle$

Observations

- The effects and outcomes of measuring more than one qubit of $|\psi\rangle$ are equivalent to the ones of measuring the qubits separately, in any order, without other operations done in between

if the qubit is in a non-entangled state, which means that we can distinguish 2 factors in a tensor product

- If $|\psi\rangle = \alpha_0|0\rangle|\phi_0\rangle + \alpha_1|1\rangle|\phi_1\rangle$ with $|\phi_0\rangle = |\phi_1\rangle$, i.e., $|\psi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |\phi_0\rangle$, then $|\phi_0\rangle$ is immutated, regardless of the measurement outcome

↳ After the measurement of the first bit, the rest of the quantum bit string ($|\phi_0\rangle$) is not altered, regardless of the measurement outcome.

A two-qubit example

SKIPPED - LEFT TO US

A generic two-qubit system

Consider $|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$, $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$

Measuring the leftmost qubit with M_{comp}

- yields 0 with $\Pr = \sum_{a=0}^{1} |\gamma_a|^2 = |\alpha_0|^2 + |\alpha_1|^2$ leaving $|\psi\rangle$ as $|0\rangle \otimes \frac{1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}(\alpha_0 |0\rangle + \alpha_1 |1\rangle)$
- yields 1 with $\Pr = \sum_{b=0}^{1} |\gamma_b|^2 = |\alpha_2|^2 + |\alpha_3|^2$ leaving $|\psi\rangle$ as $|1\rangle \otimes \frac{1}{\sqrt{|\alpha_2|^2+|\alpha_3|^2}}(\alpha_2 |0\rangle + \alpha_3 |1\rangle)$

Measuring the other qubit from $|\psi\rangle$ as $|0\rangle \otimes \frac{1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}(\alpha_0 |0\rangle + \alpha_1 |1\rangle)$ with M_{comp}

yields 0 with $\Pr = \left|\frac{\alpha_0}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}\right|^2$ leaving $|\psi\rangle$ as $|00\rangle$, and 1 with $\Pr = \left|\frac{\alpha_1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}\right|^2$ leaving $|\psi\rangle$ as $|01\rangle$

Initializing a quantum register

Goal

- After being activated, a quantum computer will be in an unknown (to us) state
- In our computations, we need to set it up in a well defined state, before starting
  - Essentially, we need to initialize the quantum register to a known (superimposition) value
- We now consider the initialization of each qubit in either $|0\rangle$ or $|1\rangle$ (=encode classic bit)

Solution

- We know that measuring a qubit in M_{comp} will leave it in either exactly $|0\rangle$ or $|1\rangle$
  - and, from the outcome of the measurement, we know which one

To initialize a qubit, we simply measure it: if it matches our desired state, we leave it as-is, otherwise, we apply an X gate to it

Bibliographic references

- N. David Mermin - Chapter 1 (+Appendix A)