Methods in quantum computing

Mária Kieferová

August 15, 2023

University of Technology Sydney

Announcements

- Problem set 0 (Optional):
  - one more week
  - Question 1 does NOT have a typo
- Problem set 1:
  - Bonus question involves regular addition, not mod 2 $a+b=c$
  - you can use CNOTS, Toff and any single qubit gates
  - it just needs to work
- submit through email/Canvas/Teams
- you can update your solutions before the deadline if you want to

Today

1. More circuits
2. Linear algebra
3. Quantum states
4. Quantum operations
5. No-cloning theorem (if we have time)
6. Measurement (if we have time)

Pauli Z and X

$Z|0\rangle = |0\rangle$

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

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$

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

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

$L_{0,0} = 1$ $\quad L_{0,1} = L_{1,0} = 0$

$L_{1,1} = -1$

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

$$X = |1\rangle\langle 0| + |0\rangle\langle 1|$$

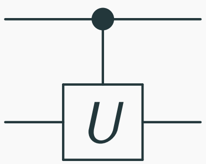
$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

Lecture notes 1

Exercise

Compute XZX and ZXZ

Controlled gates



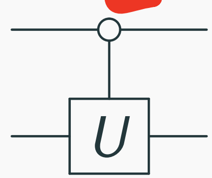
If the first qubit is 1, apply U,

otherwise, apply identity

if it is 0

$$|1\rangle\langle 1| \otimes U + |0\rangle\langle 0| \otimes \mathbb{1}$$
$$\parallel$$
$$C\text{-}U$$

$$\text{CNOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$
$$= |0\rangle\langle 0| \otimes \left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) + |1\rangle\langle 1| \otimes \left(|0\rangle\langle 1| + |1\rangle\langle 0|\right)$$

We also sometimes use 

, meaning If the first qubit is 0, apply U,

$$|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes \mathbb{1}$$

otherwise, apply identity

Linear algebra

finite

A d-dimensional Hilbert space $\mathcal{H}$ is a vector space equipped with an inner product. Let $\{\boldsymbol{e}_i\}_{i=0}^{d-1}$ be the computational basis, where $\boldsymbol{e}_i$ is a column vector of zeros except a '1' at the $(i+1)$-th entry. Any vector $\boldsymbol{v} \in \mathcal{H}$ can be decomposed into basis vectors $\boldsymbol{e}_i$ as

$\langle 1 \rangle$

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

$$\boldsymbol{v} = \sum_{i=0}^{d-1} v_i \boldsymbol{e}_i, \qquad (1)$$

linear comb of basis vectors

for some complex number $v_i \in \mathbb{C}$. The inner product (or dot product) '$\cdot$' of two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ in the same basis in $\mathcal{H}$ is defined as

$$\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{u}^\dagger \boldsymbol{v} = \sum_{i=0}^{d-1} u_i^* v_i, \qquad (2)$$

this is how it's computed

where $\dagger$ denotes transpose and conjugate.

Dirac notation

basis vector

Denote $|i\rangle \equiv \boldsymbol{e}_i$ and write $\boldsymbol{v}$ as $|v\rangle$:

$$|v\rangle = \sum_{i=0}^{d-1} v_i |i\rangle. \tag{3}$$

decomp.

bra $\langle\ |$
ket $|\ \rangle$

The inner product

braket

$$u^\dagger v = \langle u|v\rangle = \sum_{i,j} u_i^* v_j \underbrace{\langle i|j\rangle} = \sum_i u_i^* v_i \tag{4}$$

where $\langle u| \equiv |u\rangle^\dagger$ is now a row vector and $\boxed{\langle i|j\rangle = \delta_{i,j}}$

$i=j \rightarrow \langle i|j\rangle = 1$
$i\neq j \rightarrow \langle i|j\rangle = 0$

Kronecker delta

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i=j \\ 0 & i\neq j \end{cases}$$

Vector space basis

for each $|i\rangle$, $\langle i|i\rangle = 1$
if $i \neq j$ $\langle i|j\rangle = 0$

$\{|i\rangle\}$ set of mutually orthogonal normalized vectors.

For a unitary operator U, $\{U\,|i\rangle\}$ will be also mutually orthogonal and normalized.

Linear maps

$L : U \to V$

Example: Matrix multiplication

Linear operators

Given an linear operator L, there is an equivalent matrix representation $[L_{i,k}]$ in the basis spanned by $\{|i\rangle\langle k|\}$:

$$L = \sum_{i,k=0}^{d-1} L_{i,k}|i\rangle\langle k|, \tag{5}$$

we did this earlier!

where $\boxed{L_{i,k} = \langle i|L|k\rangle.}$

An linear operator $H \in \mathcal{L}(\mathcal{H})$ is called Hermitian iff $H^\dagger = H$. For a Hermitian matrix H, the spectral theorem states that there exists an orthonormal basis $\{|\nu_i\rangle\}$ and real numbers $\{\lambda_i\} \in \mathbb{R}$ so that

$$H = \sum_i \lambda_i|\nu_i\rangle\langle\nu_i|. \tag{6}$$

in the basis of $|\nu_i\rangle$

$$H = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}$$

Equivalently, $\{\lambda_i\}$ and $\{|\nu_i\rangle\}$ are known as eigenvalues and eigenvectors of H, respectively.

Exercise

Verify that Pauli X is a Hermitian operator and compute its eigenvalues and eigenvectors.

Given two vectors $|u\rangle \in \mathcal{H}_A$ and $|v\rangle \in \mathcal{H}_B$, the tensor product '$\otimes$' of them is

$$|u,v\rangle = |u\rangle \otimes |v\rangle = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} u_i v_j |i\rangle \otimes |j\rangle, \tag{7}$$

normalized
mut. orthogonal

a vector of $d_A d_B$-dimension. If $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then $\{|i\rangle_A \otimes |j\rangle_B\}$, $i \in \{0, \cdots, d_A - 1\}$ and $j \in \{0, \cdots, d_B - 1\}$, forms an orthonormal basis in $\mathcal{H}_A \otimes \mathcal{H}_B$. The inner product on the space $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined by

$$\big(\langle u_1|_A \otimes \langle u_2|_B\big)\big(|v_1\rangle_A \otimes |v_1\rangle_B\big) = \langle u_1|v_1\rangle\langle u_2|v_2\rangle. \tag{8}$$

$|01\rangle = |0\rangle \otimes |1\rangle$ $\quad \langle 01 | 11\rangle = \langle 0|1\rangle \cdot \langle 1|1\rangle$

$|11\rangle = |1\rangle \otimes |1\rangle$ $\quad = 0$

Tensor product for operators

Linear operators in $\mathcal{L}(\mathcal{H})$: $\mathcal{H}_A$ $\mathcal{H}_B$

$$\begin{aligned} L \otimes M &= \left(\sum_{i,j=0}^{d_A-1} L_{i,j} |i\rangle\langle j| \right) \otimes \left(\sum_{k,\ell=0}^{d_B-1} M_{k,\ell} |k\rangle\langle \ell|, \right) \\ &= \sum_{i,j=0}^{d_A-1} \sum_{k,\ell=0}^{d_B-1} L_{i,j} M_{k,\ell} \boxed{|i\rangle\langle j| \otimes |k\rangle\langle \ell|.} \end{aligned} \tag{9}$$

Trace

$A = \begin{pmatrix} \ddots \end{pmatrix}$ $\mathrm{Tr}(A) = \sum_i A_{i,i}$

The trace maps is defined as

$$\mathrm{Tr}\, |j\rangle\langle k| = \langle k|j\rangle = \delta_{k,j}. \tag{10}$$

From linearity, the trace of an operator L is

$$\mathrm{Tr}\, L = \sum_{i=0}^{d-1} \langle i|L|i\rangle = \sum_j L_{j,j}. \tag{11}$$

Tr maps operator to a scalar

Exercise

1. • Cyclic property: Show that $\operatorname{Tr} LM = \operatorname{Tr} ML$.

2. • Show that $\operatorname{Tr} A$ is independent of the basis of A.

$|i\rangle \to U|i\rangle$

1. $\operatorname{Tr}(LM) = \sum_i \langle i | LM | i \rangle = \sum_i \langle i | L \left(\sum_j |j\rangle\langle j| \right) M | i \rangle$

$\mathbb{1} = \sum_j |j\rangle\langle j|$

$= \sum_{i,j} \langle i | L | j \rangle \langle j | M | i \rangle = \sum_{i,j} \langle j | M | i \rangle \langle i | L | j \rangle$

scalars

$= \sum_j \langle j | ML | j \rangle = \operatorname{Tr}(ML)$

2. $\operatorname{Tr}(A) = \sum_i \langle i | A | i \rangle \qquad |i\rangle \to U|i\rangle$

$\operatorname{Tr}(A') = \sum_i \langle i | U^\dagger A U | i \rangle = \sum_i \langle i | A \underbrace{U U^\dagger}_{\mathbb{1}} | i \rangle = \sum_i \langle i | A | i \rangle = \operatorname{Tr}(A)$

Partial trace

A generalization of a trace. Partial trace maps an operator to a lower-dimensional operator. Formally, partial trace $\mathrm{Tr}_A : \mathcal{L}(\mathcal{H}_{AB}) \to \mathcal{L}(\mathcal{H}_B)$ is defined by

$$\mathrm{Tr}_A\left(|i\rangle\langle j|_A \otimes |k\rangle\langle \ell|_B\right) = \langle j|i\rangle |k\rangle\langle \ell|_B = \delta_{i,j}|k\rangle\langle \ell|_B. \qquad (12)$$

Tr_B $\quad |i\rangle\langle j|_A \langle \ell|k\rangle$

For a composite system on the space $\mathcal{H}_A \otimes \mathcal{H}_B$, Tr_A gives trace only over the subsystem on $\mathcal{H}_A$ and remains subsystem $\mathcal{H}_A$ intact. We often say that we "trace-over A".

Quantum states

$\langle \ | \ \rangle$

Use the ket notation $|\cdot\rangle$ to denote a column vector of length one, e.g.,

$$|\psi\rangle := \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{13}$$

and use the bra notation $\langle\cdot|$ to denote the hermitian conjugate of $|\cdot\rangle$:

$$\langle\psi| := \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}. \tag{14}$$

An alternative representation of a quantum state is the density matrix.

desity operator

For pure states:

$$\sigma_\psi = |\psi\rangle\langle\psi| \tag{15}$$

projector on $|\psi\rangle$

Joint quantum state

Given $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$, the joint quantum state is $|\varphi\rangle_{AB} \equiv |\psi\rangle_A \otimes |\phi\rangle_B \in \mathcal{H} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$.

If one of the subsystems, say $\mathcal{H}_A$, is lost from $|\varphi\rangle_{AB}$, the residue quantum state can be expressed as

$$\sigma_B = \mathrm{Tr}_A |\varphi\rangle\langle\varphi|. \tag{16}$$

$|\psi\rangle$

σ_B isn't always a pure state but a mixture of states $\sigma_B := \sum_i p_i |\psi_i\rangle\langle\psi_i|$ where $|\psi_i\rangle$ are orthogonal pure states on the subsystem B.

Exercise

There are three necessary and sufficient criteria that a matrix corresponds to a valid description to a quantum state. Show that

In the basis of $|\psi_i\rangle$

$$\rho := \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \rho = \begin{pmatrix} p_0 & & & 0 \\ & p_1 & & \\ & & p_2 & \\ 0 & & & \ddots \end{pmatrix} \tag{17}$$

where $\sum_i p_i = 1$ satisfies all three of them

$\hookrightarrow$ all p_i satisfy $0 \leq p_i \leq 1$ $\swarrow$ real

✓ 1. ρ is Hermitian [1] $\rho^\dagger = \sum_i p_i^* \left(|\psi_i\rangle\langle\psi_i|\right)^\dagger = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

✓ 2. ρ is positive semi-definite [2]

✓ 3. $\mathrm{Tr}[\rho] = 1.$

[1] A hermitian matrix A satisfies $A^\dagger = A$.

[2] Eigenvalues of a positive semi-definitive matrix are real and equal to 0 or positive.

Mixed states

1: $|000\rangle$
2: $|001\rangle$
3: $|010\rangle$
4: $|011\rangle$
5: $|100\rangle$
6: $|101\rangle$

$\frac{1}{6}|000\rangle\langle 000| + \dots$

Not pure states:

- outcome of a random preparation
- part of a larger entangled state

An ensemble of pure states $\mathcal{E} : \{p_i, |\psi_i\rangle\}$ can be denoted by a density operator

τON

$$\sigma := \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{18}$$

where $|\psi_i\rangle$ are individual states that could be prepared and p_i are the corresponding probabilities. We refer to objects σ as **density matrices**.

operator

Pure states

If ρ is pure, it can be written as a projector on the corresponding pure state $|\psi\rangle$

$$\sigma_\psi = |\psi\rangle\langle\psi|. \tag{19}$$

Projectors have the property that $(|\psi\rangle\langle\psi|)^2 = |\psi\rangle\langle\psi|$

$$|\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{1}\langle\psi| = |\psi\rangle\langle\psi|$$

$$a^2 = a \begin{cases} 0 \\ 1 \end{cases}$$

If you show that a normalized σ satisfies $\sigma^2 = \sigma$ then σ is a proj $\Rightarrow$ pure state

Exercise

Let $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$. Compute $\mathrm{Tr}_A(|\Phi\rangle\langle\Phi|_{AB})$ and $\mathrm{Tr}_B(|\Phi\rangle\langle\Phi|_{AB})$. Discuss whether the result could be a pure state (no need to prove it).

Church of the larger Hilbert space

Suppose that the person, say Alice, who prepares this ensemble can keep track of 'which state' she prepared. In other words, she has the additional classical label $|x\rangle\langle x|$ attached to the state $\sigma_x \in \mathcal{D}(\mathcal{H}_B)$, where $\{|x\rangle\}$ forms an orthonormal basis of $\mathcal{H}_X$. Such a hybrid classical-quantum system can be described as

$$\sigma_{XB} = \sum_{x \in \mathcal{X}} p_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|. \tag{20}$$

purification - adding another system to represent a density operator as a part of a pure state

Unitary evolution

$$|\psi\rangle \to U|\psi\rangle\,. \tag{21}$$

For a general quantum state described by a density matrix (21) takes form

$$\rho \to U\rho U^\dagger = \sum_i U|\psi_i\rangle\langle\psi_i|U^\dagger\,. \tag{22}$$

conjugation

unitary sandwich

Schrödinger equation

operator

$$|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle$$

matrix exponential

$$\overset{1}{\overset{\shortparallel}{i\hbar}} \frac{d}{dt}|\psi\rangle = H|\psi\rangle \tag{23}$$

where $\hbar$ is the Planck constant and H is the system Hamiltonian. ← hermitian

Eigenvalues of Hamiltonian define the allowed energies of a system.

Physicists and chemists really care about this!!

e^{-iHt} is unitary

Exercise

Define purity of a quantum state as $\mathrm{Tr}[\rho^2]$. Show that unitary operations preserve purity, i.e. a pure state never gets mapped onto a mixed state and vice versa.

If ρ is pure then $\rho^2 = \rho$ (projector)

so $\mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho) = 1$

$0 < \mathrm{Tr}[\rho^2] < 1$ for mixed

CPTP maps

Channels are the most general operation of quantum states. They must be always map quantum states onto quantum states, even if if we apply the channel only on a subset of qubits. Any such channel can be written as

$$\Phi(\sigma) = \sum_i B_i \sigma B_i^\dagger \quad \text{where} \quad \cancel{\sum_i B_i B_i^\dagger = \mathbb{1}}. \tag{24}$$

Kraus decomposition $\sum_i B_i^\dagger B_i = \mathbb{1}$

No cloning theorem

Theorem (No-Cloning theorem)
There is no unitary operation U_{copy} on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that for all

$|\psi\rangle_A \in \mathcal{H}_A$ *and* $|0\rangle_B \in \mathcal{H}_B$

$|\phi\rangle_A$

$$U_{\text{copy}}(|\phi\rangle_A \otimes |0\rangle_B) = e^{if(\phi)}|\phi\rangle_A \otimes |\phi\rangle_B \tag{25}$$

for some number $f(\phi)$ that depends on the initial state $|\phi\rangle$.

Exercise

Prove the no-cloning theorem by contradiction.

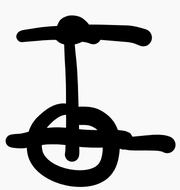
a Assuming U_{copy} exists, take two states $\overbrace{|\phi\rangle \text{ and } |\psi\rangle}^{\text{on 4}}$. Now apply U_{copy} on both of them and compute the resulting inner product $(\langle\phi|_A \otimes \langle 0|_B) U_{\text{copy}}^{\dagger} U_{\text{copy}} (|\psi\rangle_A \otimes |0\rangle_B)$.

b Explain how (a) leads to a contradiction.

THE END

$|\phi\rangle \in |0\rangle$ or $|1\rangle$

$|\phi\rangle$



$|0\rangle$

$|0\rangle|0\rangle \to |00\rangle$

$|1\rangle|0\rangle \to |11\rangle$

Quantum measurement

Obtain classical information from a quantum state. It can destroy the superposition property of a quantum state.

Observe this qubit in state $|0\rangle$ with probability $|\alpha|^2$ and in state $|1\rangle$ with probability $|\beta|^2$. Furthermore, after the measurement, the qubit state $|b\rangle$ will disappear and collapse to the observed state $|0\rangle$ or $|1\rangle$.

General quantum measurement

A collection of $\Upsilon := \{M_i\}$, where each measurement operator $M_i \in \mathcal{L}(\mathcal{H})$ satisfies

$$\sum_i M_i = I \tag{26}$$

and each M_i is positive semi-definite operator. We call this measurements positive operator-valued measure (POVM). The probability of obtaining an outcome i on a quantum state ρ is

$$p_i := \mathrm{Tr}(M_i \rho). \tag{27}$$

The state after measurement will be altered as

$$\rho_i := \frac{M_i \rho}{p_i}.$$

Projective measurement

Each M_i is a projector

$$p_j := \operatorname{Tr}\left(P_j|\phi\rangle\langle\phi|\right)$$

and the resulting state

$$\frac{P_j|\phi\rangle}{\sqrt{p_j}}.$$