

Основи квантових обчислень

Лекція 1

“Літня онлайн школа з лінійної алгебри та її застосувань”
Інститут математики НАН України

Данило Якименко

20 липня 2026

Нотація Дірака.

$H = \mathbb{C}^d$ – комплексний гільбертів простір розмірності d .

Стандартний базис:

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

Будь-який вектор (кет вектор):

$$|v\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix}, \quad \alpha_i \in \mathbb{C}.$$

Спряжений вектор (бра вектор):

$$\langle v| = |v\rangle^\dagger = (\overline{\alpha_0} \quad \overline{\alpha_1} \quad \dots \quad \overline{\alpha_{d-1}}).$$

Скалярний добуток: якщо $|w\rangle = \sum_i \beta_i |i\rangle$, то

$$\langle v|w\rangle = \langle v| \cdot |w\rangle = \sum_{i=0}^{d-1} \overline{\alpha_i} \beta_i.$$

Маємо що $\langle v|w\rangle = \overline{\langle w|v\rangle}$.

Норма вектору: $\| |v\rangle \| = \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=0}^{d-1} |\alpha_i|^2}$.

Ортонормований базис $|v_0\rangle, \dots, |v_{d-1}\rangle$:

$$\langle v_i|v_i\rangle = 1, \quad \langle v_i|v_j\rangle = 0, i \neq j.$$

Дія матриць.

Дія матриці на вектор: $A|v\rangle = A \cdot |v\rangle$, $\langle w|A = \langle w| \cdot A$.
Зокрема, $\langle i|A|j\rangle$ це елемент A на місці ij .

Спряжена матриця: $A^\dagger = \overline{A}^T$. Маємо що $(AB)^\dagger = B^\dagger A^\dagger$.

Оператор проєктування на $|v\rangle$: $P_v = |v\rangle\langle v|$. $P_v|w\rangle = |v\rangle\langle v|w\rangle$.

Самоспряжена матриця: $A = A^\dagger$. За спектральною теоремою завжди існує розклад

$$A = \sum_{i=0}^{d-1} \lambda_i |v_i\rangle\langle v_i|,$$

де λ_i власні числа, а $|v_i\rangle$ відповідні власні вектори, що утворюють ортонормований базис.

Унітарні оператори.

Матриця U називається унітарною, якщо вона зберігає скалярні добутки між векторами, зокрема, ортонормований базис переводиться в ортонормований.

Це еквівалентно тому, що $U^\dagger U = I$, тобто її стовпчики утворюють ортонормований базис (так само й рядки). Стовпчики U дорівнюють $U|i\rangle$, тож це є ортонормований базис, в який переходить стандартний під дією U .

Навпаки, будь-який ортонормований базис $|v_i\rangle$ можна отримати зі стандартного унітарним оператором

$$U = \sum_i |v_i\rangle \langle i|.$$

Звідси слідує, що будь-який ОНБ можна перевести в будь-який інший унітарним оператором (причому єдиним чином), і що добуток унітарних операторів є унітарним.

Тензорні добутки.

Для матриць $A = [a_{ij}]_{i=1,j=1}^{k,l}$, $B = [b_{mn}]_{m=1,n=1}^{p,q}$ розмірів $k \times l$ та $p \times q$ відповідно їх тензорним добутком (добутком Кронекера) називають матрицю

$$A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \dots & a_{1,l}B \\ a_{2,1}B & a_{2,2}B & \dots & a_{2,l}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{k,1}B & a_{k,2}B & \dots & a_{k,l}B \end{pmatrix} = [a_{ij}b_{mn}]$$

розміру $kp \times lq$.

Зокрема, для вектор-стовпчиків $|v\rangle$ та $|w\rangle$ розміру k та p їх тензорним добутком буде вектор-стовпчик $|v\rangle \otimes |w\rangle$ розміру kp .

Не важко персвідчитись, що якщо множина

$\{|i\rangle \otimes |m\rangle \mid i = 0, \dots, k-1, m = 0, \dots, p-1\}$ впорядкована лексикографічно, тобто $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, \dots, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle, \dots, |k\rangle \otimes |m-1\rangle, |k\rangle \otimes |m\rangle$, то, вона співпадає зі стандартним базисом в $\mathbb{C}^{kp}$.

Тензорний добуток є асоціативною операцією та лінійною по обидвох аргументах, тобто $A \otimes (B \otimes C) = (A \otimes B) \otimes C$ та

$$(\alpha_1 A_1 + \alpha_2 A_2) \otimes B = \alpha_1 (A_1 \otimes B) + \alpha_2 (A_2 \otimes B).$$

Виконуються наступні корисні властивості: $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.
Властивість змішаного добутку:

$$(A \otimes B)(C \otimes D) = AC \otimes BD,$$

якщо розміри узгоджені.

Зокрема, для векторів:

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle.$$

Постулати квантової механіки.

Постулат 1. Квантовій фізичній системі можна поставити у відповідність комплексний гільбертів простір H . Станами системи є вектори $|v\rangle \in H$ однічної довжини, тобто $\langle v|v\rangle = 1$. При цьому вектори, які відрізняються *глобальною фазою* $e^{i\theta}$, $\theta \in \mathbb{R}$, тобто $|u\rangle = e^{i\theta}|v\rangle$, вважаються еквівалентними станами (їх неможливо розрізнити фізично), $|u\rangle \sim |v\rangle$.

$$|v\rangle \sim |v\rangle$$

Найпростішим прикладом є *кубіт* — система розмірності 2, $H = \mathbb{C}^2$. Станами є вектори $|v\rangle = a_0|0\rangle + a_1|1\rangle$, $a_i \in \mathbb{C}$, $|a_0|^2 + |a_1|^2 = 1$. Числа a_i називають *амплітудами*.

$$\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

Кажуть, що стан $|v\rangle = a_0|0\rangle + a_1|1\rangle$ знаходиться у *суперпозиції* відносно стандартного базису, якщо він не еквівалентний до базисного стану, тобто $a_0 \neq 0$, $a_1 \neq 0$. При цьому відносна фаза вже грає роль.

Наприклад, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ та $\frac{1}{\sqrt{2}}(|0\rangle + \underline{e^{i\theta}}|1\rangle)$ це вже різні стани, якщо $e^{i\theta} \neq 1$.

Постулат 2. Вимірювання стану системи.

Нехай $\{|b_0\rangle, \dots, |b_{d-1}\rangle\}$ це ортонормований базис $H = \mathbb{C}^d$.
Вимірюванню фон Неймана відповідає набір ортопроекторів $P_i = |b_i\rangle\langle b_i|$,

$$P_0 + P_1 + \dots + P_{d-1} = I.$$

Результатом вимірювання стану $|v\rangle \in H$ буде індекс i з ймовірністю $p_i = \text{Tr}(P_i |v\rangle\langle v|) = |\langle b_i | v \rangle|^2$. При цьому система переходить у новий стан $P_i |v\rangle / \sqrt{p_i} \sim |b_i\rangle$.

Для кубіту прикладом є вимірювання $|v\rangle = a_0|0\rangle + a_1|1\rangle$ у стандартному базисі. Результатом вимірювання буде 0 з ймовірністю $|a_0|^2$ (при цьому система перейде у стан $|0\rangle$), та 1 з ймовірністю $|a_1|^2$ (при цьому система перейде у стан $|1\rangle$).

Постулат 3. Унітарні перетворення станів.

Фізично стан замкненої квантової системи проходить детерміновану унітарну еволюцію в часі, що описується рівнянням Шредінгера.

В квантових обчисленнях та інформації вважається, що це контрольований процес. Тож вважається, що на стан $|v\rangle \in H$ ми можемо подіяти будь-яким унітарним перетворенням U щоб перевести систему у стан $U|v\rangle$, а сам по собі він не змінюється (якщо не вимірюється).

Процес вимірювання, що відповідає базису $\{|b_0\rangle, \dots, |b_{d-1}\rangle\}$, застосований до стану $|v\rangle$, еквівалентний до вимірювання стану $U^\dagger |v\rangle$ у стандартному базисі, із застосуванням U до кінцевого стану, де $U|i\rangle = |b_i\rangle$, $\forall i$ (тобто $U = \sum_i |b_i\rangle\langle i|$).

Постулат 4. Композиції квантових систем.

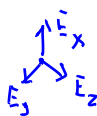
Якщо є дві квантові системи, яким відповідають гільбертові простори H_1 та H_2 , то сукупній системі відповідає гільбертів простір $H_1 \otimes H_2$. При цьому якщо перша система перебуває у стані $|v_1\rangle \in H_1$, а друга у стані $|v_2\rangle \in H_2$, то сукупна система перебуває у стані $|v_1\rangle \otimes |v_2\rangle \in H_1 \otimes H_2$.

Але сукупна система може перебувати і в станах, які не можна виразити як $|v_1\rangle \otimes |v_2\rangle$, а лише як їх лінійні комбінації (суперпозиції). Такі стани називають *заплутаними*.

$$\begin{array}{l} |0\rangle \text{ з \u044e\u043c. } 1/2 \quad |1\rangle \text{ з \u044e\u043c. } 1/2 \end{array} \left| \begin{array}{l} \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\ 1 \cdot |+\rangle\langle +| \end{array} \right.$$
$$|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \in \mathbb{C}^2$$

Приклад однокубітної системи - поляризація світла

(Див. <https://youtube.com/watch?v=DvEdm6a-9Tw>)



$$\vec{E} = (E_x, E_y, E_z)$$

$$(x(t), y(t), z(t))$$

$$\vec{E}(t, z)$$

photon

$$E_x = A_x \cos(\omega t - kz + \varphi_x)$$

$$E_y = A_y \cos(\omega t - kz + \varphi_y)$$

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

$$\begin{pmatrix} E_x \\ E_y \end{pmatrix} = \text{Re} \begin{pmatrix} A_x e^{i\varphi_x} \cdot e^{i(\omega t - kz)} \\ A_y e^{i\varphi_y} \cdot e^{i(\omega t - kz)} \end{pmatrix} = \text{Re} \begin{pmatrix} A_x e^{i\varphi_x} \\ A_y e^{i\varphi_y} \end{pmatrix} \cdot e^{i(\omega t - kz)}$$

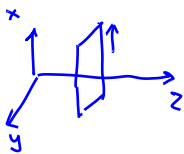
$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |V\rangle$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |H\rangle$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = |D\rangle$$

braket $\|A\| \dots$

$$|\psi\rangle = \alpha_0|V\rangle + \alpha_1|H\rangle, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

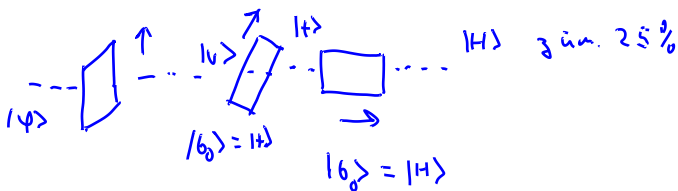


$$|b_0\rangle = |V\rangle$$

$$|b_1\rangle = |H\rangle$$

$$p_0 = |\langle b_0|\psi\rangle|^2 \quad \text{— проїшов і став } |b_0\rangle$$

$$p_1 = |\langle b_1|\psi\rangle|^2$$



Основи квантових обчислень

Лекція 2

“Літня онлайн школа з лінійної алгебри та її застосувань”
Інститут математики НАН України

Данило Якименко

21 липня 2026

Унітарні перетворення кубіту. Матриці Паулі.

Матриці Паулі:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Вони задовольняють

$$X^2 = Y^2 = Z^2 = I, \quad \underline{XYZ = iI}, \quad ZYX = -iI,$$

$$XY = -YX, \quad YZ = -ZY, \quad ZX = -XZ.$$

I, X, Y, Z утворюють базис в просторі матриць 2×2 .

Унітарні перетворення кубіту.

Матриці повороту відносно x, y та z :

$$R_x(\theta) = \cos(\theta/2)I - i \sin(\theta/2)X = \begin{pmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ -i \sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$R_y(\theta) = \cos(\theta/2)I - i \sin(\theta/2)Y = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$R_z(\theta) = \cos(\theta/2)I - i \sin(\theta/2)Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \quad \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

Матриця Адамара H та фазові зсуви S та T :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

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

$$1 = |u| = \lambda_1 \lambda_2$$

Унітарні перетворення кубіту.

$$U U^\dagger = I$$

Будь-яку унітарну матрицю $U \in L(H)$ можна зобразити як

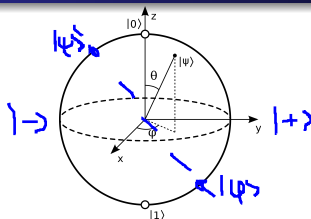
$U = e^{i\alpha} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, де $|a|^2 + |b|^2 = 1$. Звідси можна отримати наступний загальний вигляд

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

Тож будь-яку унітарну матрицю можна записати як

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

Сфера Блоха.



$$U = e^{-i\theta/2} \cdot |\psi\rangle\langle\psi| + e^{i\theta/2} \cdot |\psi\rangle\langle\psi|$$

Кожний чистий стан кубіту можна задати вектором

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

де $0 \leq \theta \leq \pi$, $0 \leq \phi < 2\pi$. Це можна зобразити як точку з координатами

$$\vec{a} = (a_x, a_y, a_z) = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$$

на дійсній трьохвимірній одиничній сфері з центром у $(0, 0, 0)$. Зокрема, $|0\rangle$ це точка $(0, 0, 1)$, а $|1\rangle$ це точка $(0, 0, -1)$.

Інтерактивна сфера Блоха –

<https://javafxpert.github.io/grok-bloch/>

Сфера Блоха.

Також цей же зв'язок можна записати як

$$\frac{1}{2}(|0\rangle\langle 0| + \frac{a_z}{2}|1\rangle\langle 1|) \quad |\psi\rangle\langle\psi| = \frac{1}{2}(I + a_x X + a_y Y + a_z Z). \quad | \cdot \chi$$

Звідси можна отримати, що

$$\underline{a_x = \langle\psi|X|\psi\rangle}, \quad a_y = \langle\psi|Y|\psi\rangle, \quad a_z = \langle\psi|Z|\psi\rangle,$$

де використано циклічність сліду $\text{Tr}(|\psi\rangle\langle\psi|X) = \langle\psi|X|\psi\rangle$.

Дія гейту $R_z(\gamma)$ на $|\psi\rangle$ відповідає повороту на сфері Блоха навколо осі z на кут γ проти годинникової стрілки. Аналогічно для гейтів $R_x(\gamma)$ та $R_y(\gamma)$.

Це по суті задає ізоморфізм між поворотами в $\mathbb{R}^3$ та унітарними однокубітними гейтами:

$$SO(3) \cong SU(2)/\langle -I \rangle$$

$$|u|=1$$

Універсальні набори однокубітних гейтів

Скінченна множина G однокубітних гейтів називається *універсальною*, якщо будь-який унітарний гейт можна отримати як добуток скінченної кількості елементів з G .

Наприклад, усі повороти $\{R_y(\theta), R_z(\theta)\}$ є універсальною множиною.

Скінченна множина G однокубітних гейтів називається *апроксимативно універсальною*, якщо будь-який унітарний гейт можна як завгодно точно наблизити добутком скінченної кількості елементів з G .

Наприклад, пара гейтів $\{H, T\}$ є апроксимативно універсальною. Будь-яка пара поворотів U, V відносно різних осей, і така, що UV є ірраціональним поворотом, є апроксимативно універсальною.

$UV UV UV \dots$



Теорема Соловея-Кітаєва дає оцінку кількості гейтів з універсального набору потрібних для апроксимації.

Основи квантових обчислень

Лекція 3

“Літня онлайн школа з лінійної алгебри та її застосувань”
Інститут математики НАН України

Данило Якименко

22 липня 2026

Багато-кубітна система

Система кубітів моделюється комплексним гільбертовим простором, що є тензорним добутком просторів для одиночних кубітів. Тобто, для n кубітів це простір розмірності 2^n :

$$H = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}.$$

Стандартний базис такої системи це усі можливі тензорні добутки стандартних базисів $\{|0\rangle, |1\rangle\}$ по кожному з кубітів, тобто

$$|b_1 b_2 \dots b_n\rangle := |b_1\rangle |b_2\rangle \dots |b_n\rangle := |b_1\rangle \otimes |b_2\rangle \otimes \dots \otimes |b_n\rangle$$

для всіх можливих значень бітів b_i (всього буде 2^n комбінацій). Наприклад, для двох кубітів стандартним базисом буде

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

Порядок базисних елементів відповідає порядку чисел $(b_1 b_2 \dots b_n)_2$ (тобто якщо розуміти це як двійковий запис). Також цей порядок узгоджений з добутком Кронекера.

Заплутаність

Якщо кожен окремий кубіт перебуває у стані $|v_i\rangle \in \mathbb{C}^2$, то загальна система перебуває у стані, що є тензорним добутком:

$$|v\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \dots \otimes |v_n\rangle.$$

Такий стан також називають *станом-добутком*.

Але ж будь-яка лінійна комбінація векторів (суперпозиція) також є вектором у $(\mathbb{C}^2)^{\otimes n}$.

Лінійні комбінації, взагалі кажучи, не є тензорними добутками.

Типовий приклад – це *стан Белла* двох кубітів:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &\neq |v_1\rangle|v_2\rangle = (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \\ &= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle. \end{aligned}$$

Стан, який не є станом-добутком, називають *заплутаним*.

Результатом вимірювання у стандартному базисі стану

$$|v\rangle = \sum_{\mathbf{b}=b_1b_2\dots b_n}^{2^n} \alpha_{\mathbf{b}} |b_1b_2\dots b_n\rangle, \quad \sum_{\mathbf{b}} |\alpha_{\mathbf{b}}|^2 = 1,$$

$$2 \cdot 2^n - 2$$

буде індекс $\mathbf{b} = b_1b_2\dots b_n$ з ймовірністю $|\alpha_{\mathbf{b}}|^2 = |\langle b_1b_2\dots b_n | v \rangle|^2$,
при цьому система перейде у новий стан $|b_1b_2\dots b_n\rangle$.

Аналогічно для вимірювань в інших базисах.

Наприклад, ймовірності при вимірюванні стану Белла $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ будуть

$$p_{00} = \frac{1}{2}, \quad p_{01} = 0, \quad p_{10} = 0, \quad p_{11} = \frac{1}{2}.$$

Унітарні перетворення. Добутки унітарних.

Унітарні перетворення на $(\mathbb{C}^2)^{\otimes n}$ це матриці U , що задовольняють $U^\dagger U = I$, тобто $U^{-1} = U^\dagger$. Наприклад, добуток

$$U = U_1 \otimes U_2 \otimes \dots \otimes U_n$$

є унітарним, де U_i це однокубітні унітарні матриці.

Результатом дії такої операції на стан-добуток $|v_1\rangle|v_2\rangle\dots|v_n\rangle$ буде стан-добуток $U_1|v_1\rangle \otimes U_2|v_2\rangle \otimes \dots \otimes U_n|v_n\rangle$.

Звідси випливає, що дія такої операції на заплутаному стані завжди буде заплутаний стан (оскільки обернене перетворення до унітарного є унітарним).

Оскільки

$$\begin{aligned} U_1 \otimes U_2 \otimes \dots \otimes U_n &= \\ U_1 \otimes I \otimes \dots \otimes I &\cdot \\ \cdot I \otimes U_2 \otimes \dots \otimes I &\cdot \\ \cdot I \otimes I \otimes \dots \otimes U_n & \end{aligned} \tag{1}$$

то таку унітарну операцію можна розуміти як послідовність однокубітних перетворень (причому порядок не важливий).

$$\begin{aligned} |u\rangle &= \sum_i a_i |i\rangle \\ U|u\rangle &= \sum_i a_i U|i\rangle \end{aligned}$$

Унітарні перетворення. Перестановки базису.

Будь-якій перестановці 2^n елементів стандартного базису відповідає перестановочна матриця. Такі матриці є унітарними. Для одного кубіту існує єдина нетотожна перестановочна матриця, це $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Для двох кубітів перестановочних матриць буде вже $4! = 24$. Особливою серед них виділяють матрицю CNOT (або ж CX):

$(2^n)!$

$I \otimes I \otimes \text{CNOT} \otimes \dots \otimes I$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

d_{00}
 d_{01}
 d_{10}
 d_{11}

2

k

$|b_1 b_2 \dots b_k \dots b_n\rangle$
 $\rightarrow |b_1 b_2 \dots b_k \oplus b_k \dots b_n\rangle$

яка діє за правилом $\text{CNOT}|00\rangle = |00\rangle$, $\text{CNOT}|01\rangle = |01\rangle$,
 $\text{CNOT}|10\rangle = |11\rangle$, $\text{CNOT}|11\rangle = |10\rangle$.

Також її можна записати як

$$\text{CNOT}(v) = \sum_i \alpha_i \text{CNOT} |b_i\rangle$$

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

Унітарні перетворення. Перестановки базису.

Матрицю CNOT неможливо представити як тензорний добуток двох унітарних, тобто

$$\text{CNOT} \neq U_1 \otimes U_2$$

Подіємо матрицею CNOT на стан-добуток $|+\rangle|0\rangle$. Отримаємо

$$\text{CNOT}|+\rangle|0\rangle = \frac{1}{\sqrt{2}}\text{CNOT}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

тобто стан Белла, який є заплутаним.

Також окремо виділяють SWAP матрицю

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$|01\rangle \leftrightarrow |10\rangle$

що міняє місцями значення бітів у двійковому позначенні базису. Більше того, для будь-яких станів-добутків вона міняє місцями стани кубітів, тобто $\text{SWAP}|v\rangle|u\rangle = |u\rangle|v\rangle$.

Але вона також не є тензорним добутком двох унітарних.

Унітарні перетворення. Перестановки базису.

Для трьох кубітів серед перестановочних матриць виділяють матрицю Тоффолі, яку позначають CCNOT або ж CCX:

$$\text{CCNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

CCNOT $\neq$ CNOT

Вона змінює значення третього біту лише коли перші два одинички, тобто

$$\text{CCNOT}|110\rangle = |111\rangle, \text{CCNOT}|111\rangle = |110\rangle.$$

Унітарні перетворення. Перестановки кубітів.

Для перестановки π чисел $\{1, 2, \dots, n\}$ можна визначити SWAP_π , що діє на просторі n кубітів, через

$$\text{SWAP}_\pi |b_1 b_2 \dots b_n\rangle = |b_{\pi(1)} b_{\pi(2)} \dots b_{\pi(n)}\rangle$$

по всіх наборах значень бітів b_i .

Для неї також виконується

$$\text{SWAP}_\pi |v_1\rangle |v_2\rangle \dots |v_n\rangle = |v_{\pi(1)}\rangle |v_{\pi(2)}\rangle \dots |v_{\pi(n)}\rangle$$

для будь-яких однокубітних станів $|v_i\rangle$.

$$\pi = \rho \sigma$$

$$\text{SWAP}_\pi = \text{SWAP}_\rho \cdot \text{SWAP}_\sigma$$

Унітарні перетворення. Діагональні матриці.

Також в деяких задачах зручно оперувати діагональними унітарними матрицями, що мають вигляд

$$U = V D V^\dagger$$

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & u_{2,2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & u_{2^n, 2^n} \end{pmatrix}$$

де $|u_{i,i}| = 1$.

І хоча їх дія на базисні стани фізично не відчутна, бо

$$U|b_1 b_2 \dots b_n\rangle = u_{\mathbf{b}, \mathbf{b}} |b_1 b_2 \dots b_n\rangle,$$

але дія на суперпозицію базисних векторів вже є суттєвою, загалом.

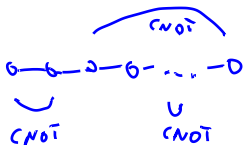
$$U|v\rangle = \sum u_{\mathbf{b}, \mathbf{b}} |b\rangle \neq |v\rangle$$

$$n \text{ bit} \rightarrow n \text{ bit}$$

Будь-яку унітарну матрицю U на n кубітах можна реалізувати як добуток

$$U = U_1 U_2 \dots U_k \quad k \approx O(4^n)$$

де кожне U_i це або однокубітна операція, або $CNOT$.



$$SWAP_{1,2} = CNOT_{1,2} \cdot CNOT_{2,1} \cdot CNOT_{1,2}$$

$$k \approx O(\log(n))$$

- 1 Маємо доступ до n кубітів у стані $|init\rangle = |00\dots 0\rangle$
- 2 Можемо подіяти унітарним перетворенням U
- 3 Після чого виміряти стан $|final\rangle = U|init\rangle$ у стандартному базисі

Як це використати?

Змішані стани та матриця (оператор) густини

Змішаним станом на системі H називається ймовірнісний розподіл на (чистих) станах на H . Наприклад, для дискретного розподілу це буде множина пар $\{(|v_i\rangle, p_i)\}$, де $|v_i\rangle \in H$ це деякі чисті стани, а p_i це відповідні ймовірності, $p_i \geq 0$, $\sum_i p_i = 1$.

Результат вимірювання змішаного стану задовільняє правило повної ймовірності. Тобто, при вимірюванні у базисі $\{|u_j\rangle\}$ результатом буде мітка u_j з ймовірністю

$$r_j = \sum_i p_i |\langle v_i | u_j \rangle|^2,$$

при цьому змішаний стан перейде у чистий стан $|u_j\rangle$.

Змішані стани та матриця (оператор) густини

Для змішаного стану вводять поняття *матриці густини*:

$$p \geq 0$$

$$\text{Tr}(\rho) = 1$$

$$\rho = \sum_i p_i |v_i\rangle\langle v_i|.$$

Виявляється, що змішані стани неможливо відрізнити фізично, якщо у них однакові матриці густини. При цьому матриця густини повністю описує змішаний стан. Наприклад, при вимірюванні ρ у базисі $\{|u_j\rangle\}$ результатом буде мітка u_j з ймовірністю

$$r_j = \text{Tr}(\rho |u_j\rangle\langle u_j|) = \langle u_j | \rho | u_j \rangle.$$

Унітарна ж дія U переводить ρ у матрицю густини $U\rho U^\dagger$.

$$\frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1| = \frac{1}{2} I \quad - \text{макс. зміш.}$$

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

Для тензорного добутку двох гільбертових просторів $H_1 \otimes H_2$ існує поняття часткового сліду.

Частковий слід по другій системі це лінійний оператор $\text{Tr}_2 : L(H_1 \otimes H_2) \rightarrow L(H_1)$, який на матрицях виду $A \otimes B$ діє як

$$\text{Tr}_2(A \otimes B) = A \text{Tr}(B),$$

а на всіх інших матрицях – по лінійності. Альтернативно, його дію на матрицю $M \in L(H_1 \otimes H_2)$ можна записати як

$$\text{Tr}_2(M) = \sum_i I \otimes \langle i | \cdot M \cdot I \otimes | i \rangle,$$

де $\{|i\rangle\}$ це базис H_2 .

$$\begin{aligned} \text{Tr}(M) &= \\ &= \sum \langle i | M | i \rangle \end{aligned}$$

Частковий слід від матриці густини описує *редукований* стан системи. Тобто, якщо ρ це матриця густини на $H_1 \otimes H_2$, то $\text{Tr}_2(\rho)$ це буде якась матриця густини на H_1 , яка повністю описує стан на першій підсистемі.

Зауважимо, що взагалі кажучи,

$$\rho \neq \text{Tr}_2(\rho) \otimes \text{Tr}_1(\rho).$$

> 1

$$\text{Rank } \rho = 1$$

— чистий

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

< 1 — змішаний

