Квантові обчислення

Лекція 3

Київський академічний університет

24 лютого 2025

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:

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

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

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

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 віповідає порядку чисел $(b_1 b_2 ... b_n)_2$ (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:

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

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:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |v_1\rangle|v_2\rangle = (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle)$$

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

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

Вимірювання

Результатом вимірювання у стандартному базисі стану

$$|v\rangle = \sum_{\mathbf{b}=b_1 b_2 \ldots b_n}^{2^n} \alpha_{\mathbf{b}} |b_1 b_2 \ldots b_n\rangle, \quad \sum_{\mathbf{b}} |\alpha_{\mathbf{b}}|^2 = 1,$$

буде індекс $\mathbf{b} = b_1 b_2 \ldots b_n$ з ймовірністю $|\alpha_{\mathbf{b}}|^2 = |\langle b_1 b_2 \ldots b_n | v\rangle|^2$, при цьому система перейде у новий стан $|b_1 b_2 \ldots b_n\rangle$.
Аналогічно для вимірювань в інших базисах.

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

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

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

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

є унітарним, де U_i це однокубітні унітарні матриці.
Результатом дії такой операції на стан-добуток $|v_1\rangle|v_2\rangle...|v_n\rangle$ буде стан-добуток $U_1|v_1\rangle \otimes U_2|v_2\rangle \otimes ... \otimes U_n|v_n\rangle$.
Звідси випливає, що дія такої операції на заплутаному стані завжди буде заплутаний стан (оскільки обернене перетворення до унітарного є унітарним).
Оскільки

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

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

Унітарні перетворення. Перестановки базису.

Будь-якій перестановці 2^n елементів стандартного базису відповідає перестановочна матриця. Такі матриці є унітарними. Для одного кубіту існує єдина нетотожня 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):

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

яка діє за правилом $\mathrm{CNOT}|00\rangle = |00\rangle$, $\mathrm{CNOT}|01\rangle = |01\rangle$, $\mathrm{CNOT}|10\rangle = |11\rangle$, $\mathrm{CNOT}|11\rangle = |10\rangle$.
Також її можна записати як

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

Унітарні перетворення. Перестановки базису.

Матрицю CNOT неможливо представити як тензорний добуток двох унітарних, тобто

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

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

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

тобто стан Белла, який є заплутаним.
Також окремо виділяють SWAP матрицю

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

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

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

Вона змінює значення третього біту лише коли перші два одиничи, тобто
$\mathrm{CCNOT}|110\rangle = |111\rangle$, $\mathrm{CCNOT}|111\rangle = |110\rangle$.

Унітарні перетворення. Перестановки кубітів.

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

$$\mathrm{SWAP}_\pi \left|b_1 b_2 \ldots b_n\right\rangle = \left|b_{\pi(1)} b_{\pi(2)} \ldots b_{\pi(n)}\right\rangle$$

по всіх наборах значень бітів b_i.

Для неї також виконується

$$\mathrm{SWAP}_\pi \left|v_1\right\rangle \left|v_2\right\rangle \ldots \left|v_n\right\rangle = \left|v_{\pi(1)}\right\rangle \left|v_{\pi(2)}\right\rangle \ldots \left|v_{\pi(n)}\right\rangle$$

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

Унітарні перетворення. Діагональні матриці.

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

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

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.

Універсальний набір

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

$$U = U_1 U_2 \dots U_k$$

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

Основна модель і мета квантових обчислень

1. Маємо доступ до n кубітів у стані $|\text{init}\rangle = |00\ldots0\rangle$
2. Можемо подіяти унітарним перетворенням U
3. Після чого виміряти стан $|\text{final}\rangle = U|\text{init}\rangle$ у стандартному базисі

Як це використати?

Змішані стани та матриця (оператор) густини

Змішаним станом на системі H називається ймовірністний 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, $p_i \geqslant 0$, $\sum_i p_i = 1$.

Результат вимірювання змішаного стану задовільняє правилу 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*:

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

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

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

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

Частковий слід

Для тензорного добутку двох гільбертових просторів $H_1 \otimes H_2$ існує поняття часткового сліду.
Частковий слід по другій системі це лінійний оператор $\mathrm{Tr}_2 : L(H_1 \otimes H_2) \to L(H_1)$, який на матрицях виду $A \otimes B$ діє як

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

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

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

де $\{|i\rangle\}$ це базис H_2.

Частковий слід

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

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

Завдання

1. Чи буде стан $\mathrm{CNOT}\,|+\rangle|-\rangle$ заплутаним?

2. Нехай є змішаний стан з розподілом $\{\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{3}\right), \left(|++\rangle, \frac{2}{3}\right)\}$. Яка ймовірність отримати 0 при вимірюванні другого кубіту в базисі $\{|0\rangle, |1\rangle\}$?

3. Нехай $|v\rangle = \frac{1}{\sqrt{3}}(|00\rangle + i\,|01\rangle - |10\rangle)$. Знайти матрицю густини на першому кубіті.