

Hệ nhiều qubit

Nhập môn Tính toán Lượng tử
(Introduction to Quantum Computing)

Vũ Quốc Hoàng (vqhoang@fit.hcmus.edu.vn)

FIT - HCMUS

2025

Nội dung

1. Trạng thái
2. Vương lượng tử
3. Phép đo
4. Cổng lượng tử
5. Tập cổng lượng tử toàn năng

Nội dung

1. Trạng thái

2. Vương lượng tử

3. Phép đo

4. Cổng lượng tử

5. Tập cổng lượng tử toàn năng

Thanh ghi lượng tử

Một hệ thống lượng tử gồm n qubit thường được gọi là một **thanh ghi lượng tử** (quantum register) **cỡ** (size) n .

Cho hệ n qubit, để thuận tiện, ta đánh số các qubit lần lượt là $0, 1, \dots, n-1$. Vì mỗi qubit có 2 trạng thái cơ bản là 0, 1 nên hệ n qubit có 2^n trạng thái cơ bản. Trạng thái của hệ ứng với việc qubit i có trạng thái $b_i, i = 0, \dots, n-1$ được mô tả bằng chuỗi n bit (thứ tự này được gọi là **big-endian**, ngược với một lựa chọn khác là little-endian)

$$b_{n-1}b_{n-2}\dots b_1b_0 \in \{0, 1\}^n.$$

Vì mỗi chuỗi n bit $b = b_{n-1}b_{n-2}\dots b_1b_0$ là biểu diễn nhị phân của số nguyên không âm

$$[b] = \sum_{i=0}^{n-1} 2^{b_i} = 2^{b_{n-1}} + 2^{b_{n-2}} + \dots + 2^{b_1} + 2^{b_0}$$

nên ta có thể đánh số trạng thái cơ bản b bằng số nguyên $[b]$.

Trạng thái

Trạng thái của hệ n qubit là sự chồng chất của 2^n trạng thái cơ bản. Nếu đồng nhất trạng thái cơ bản $b = b_{n-1}...b_1b_0$ với ket thứ $[b]$ (tính từ 0) của cơ sở chuẩn tắc của \mathbb{C}^{2^n} thì trạng thái $|\psi\rangle$ của hệ n qubit được mô tả là một tổ hợp tuyến tính

$$|\psi\rangle = \sum_{b \in \{0,1\}^n} \alpha_b |b\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle \in \mathbb{C}^{2^n}.$$

Để thuận tiện tính toán, ta cũng yêu cầu $|\psi\rangle$ phải được chuẩn hóa ($|\psi\rangle$ là vector đơn vị)

$$||\psi\rangle|| = 1 \Leftrightarrow \sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1.$$

Cơ sở chuẩn tắc cũng được gọi là cơ sở tính toán.

Trạng thái (tt)

Nếu đồng nhất 2 trạng thái cơ bản 0, 1 của từng qubit với 2 ket

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbb{C}^2$$

thì với từng trạng thái cơ bản của hệ $b = b_{n-1} \dots b_1 b_0$, ta có (kiểm tra!)

$$|b_{n-1}\rangle \otimes \dots \otimes |b_1\rangle \otimes |b_0\rangle$$

chính là vector thứ $[b]$ (tính từ 0) của cơ sở chuẩn tắc của \mathbb{C}^{2^n} . Hơn nữa, theo cách viết gọn của kí pháp Dirac thì

$$|b_{n-1}\rangle \otimes \dots \otimes |b_1\rangle \otimes |b_0\rangle = |b_{n-1} \dots b_1 b_0\rangle = |b\rangle.$$

Như vậy, với $b = b_{n-1} \dots b_1 b_0$, $k = [b]$, ta có thể dùng lẫn lộn các kí hiệu

$$|k\rangle, \quad |b_{n-1} \dots b_1 b_0\rangle, \quad |b_{n-1}\rangle \otimes \dots \otimes |b_1\rangle \otimes |b_0\rangle.$$

Trạng thái (tt)

Cho hệ n qubit, nếu tất cả các qubit của hệ đều ở trạng thái $|\psi\rangle \in \mathbb{C}^2$ thì trạng thái của cả hệ được kí hiệu là

$$|\psi\rangle^{\otimes n} = \underbrace{|\psi\rangle \otimes |\psi\rangle \otimes \dots \otimes |\psi\rangle}_{n \text{ lần}} = \underbrace{|\psi\rangle |\psi\rangle \dots |\psi\rangle}_{n \text{ lần}} \in \mathbb{C}^{2^n}.$$

Chẳng hạn, trạng thái cơ bản ứng với vector đầu tiên của cơ sở chuẩn tắc là

$$|0\rangle^{\otimes n} = \underbrace{|0\rangle |0\rangle \dots |0\rangle}_{n \text{ lần}} = \underbrace{|00 \dots 0\rangle}_{n \text{ lần}} = |0\rangle_n.$$

Đặc biệt (kiểm tra!)

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

mô tả trạng thái “tổ hợp đều” các trạng thái cơ bản.

Trạng thái (tt)

Ví dụ 1

Xét hệ $n = 2$ qubit được đánh số là qubit 0, qubit 1. Hệ này có $2^n = 4$ trạng thái cơ bản ứng với các cặp trạng thái cơ bản của qubit 1, qubit 0 là $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ mà được kí hiệu bằng các chuỗi $n = 2$ bit là 00, 01, 10, 11. Các chuỗi này cũng được đánh số bằng số nguyên mà chúng biểu diễn là 0, 1, 2, 3.

Các trạng thái cơ bản 00, 01, 10, 11 được đồng nhất với lần lượt các

vector của cơ sở chuẩn tắc của $\mathbb{C}^{2^n} = \mathbb{C}^4$ là $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

mà lần lượt các vector này cũng là các tích tensor

$|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$. Dùng số thứ tự, các vector này lần lượt được kí hiệu là $|0\rangle_2$, $|1\rangle_2$, $|2\rangle_2$, $|3\rangle_2$.

Trạng thái (tt)

Ví dụ 1 (tt)

Trạng thái của hệ 2 qubit được mô tả là

$$\begin{aligned} |\psi\rangle &= \sum_{b \in \{0,1\}^2} \alpha_b |b\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \\ &= \sum_{k=0}^3 \alpha_k |k\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle \\ &= \alpha_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \alpha_3 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} \in \mathbb{C}^4. \end{aligned}$$

Hơn nữa $|\psi\rangle$ là vector đơn vị $\sum_{k=0}^3 |\alpha_k|^2 = 1$.

Trạng thái (tt)

Ví dụ 1 (tt)

Xét trạng thái sau của hệ 2 qubit

$$|\psi\rangle = \sum_{k=0}^3 \frac{1}{2} |k\rangle = \frac{1}{2} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Nhận xét, $|\psi\rangle = |+\rangle|+\rangle$ (kiểm tra!). Ket $|\psi\rangle$ mô tả trạng thái “tổ hợp đều” 4 trạng thái cơ bản. Ngược lại, ket

$$|\phi\rangle = \frac{\sqrt{3}}{2} |01\rangle + \frac{1}{2} |10\rangle = \begin{bmatrix} 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 \end{bmatrix}^T$$

mô tả trạng thái “thiên về” 01.

Trạng thái (tt)

Với hệ 2 qubit, ngoài các trạng thái cơ bản ứng với cơ sở chuẩn tắc là $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ thì các trạng thái sau cũng hay được dùng, gọi là các **trạng thái Bell** (Bell state)

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}, |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}, \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}, |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}. \end{aligned}$$

Các trạng thái này tạo thành một cơ sở trực chuẩn của \mathbb{C}^4 (kiểm tra!) được gọi là **cơ sở Bell** (Bell basis).

Nội dung

1. Trạng thái

2. Vương lượng tử

3. Phép đo

4. Cổng lượng tử

5. Tập cổng lượng tử toàn năng

Vướng lượng tử

Nếu trạng thái $|\psi\rangle \in \mathbb{C}^{2^n}$ của hệ n qubit có thể được viết thành tích tensor của các trạng thái $|\psi_i\rangle \in \mathbb{C}^2$ của qubit i ($i = 0, \dots, n - 1$)

$$|\psi\rangle = |\psi_{n-1}\rangle|\psi_{n-2}\rangle\cdots|\psi_0\rangle$$

thì $|\psi\rangle$ được gọi là **trạng thái tích** (product state) hay **trạng thái tách được** (seperable state). Ngược lại, $|\psi\rangle$ được gọi là **trạng thái vướng (lượng tử)** (entangled state).

Khi hệ ở trạng thái vướng, các qubit “vướng víu nhau” một cách “thật sự rối rắm” nên không thể phân tách ra thành các trạng thái riêng lẻ của từng qubit.

Các trạng thái Bell $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ là các trạng thái vướng điển hình của hệ 2 qubit. (kiểm tra!)

Vướng lượng tử (tt)

Ví dụ 2 (tiếp Ví dụ 1)

Rõ ràng các trạng thái cơ bản $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ là các trạng thái tách được của hệ 2 qubit. Hơn nữa, trạng thái “tổ hợp đều”

$$|\psi\rangle = \sum_{k=0}^3 \frac{1}{2} |k\rangle = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

cũng tách được vì $|\psi\rangle = |+\rangle|+\rangle$.

Khó thấy hơn, trạng thái sau cũng tách được

$$|\phi\rangle = \frac{1}{2\sqrt{2}} \left(\sqrt{3}|00\rangle - \sqrt{3}|01\rangle + |10\rangle - |11\rangle \right).$$

Vướng lượng tử (tt)

Ví dụ 2 (tt)

Thật vậy

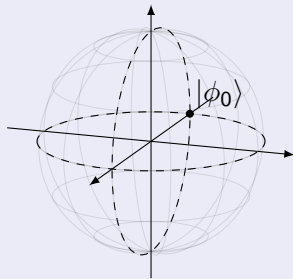
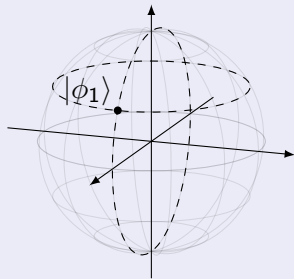
$$\begin{aligned} |\phi\rangle &= \frac{1}{2\sqrt{2}} \left(\sqrt{3}|00\rangle - \sqrt{3}|01\rangle + |10\rangle - |11\rangle \right) \\ &= \frac{1}{2\sqrt{2}} \left(\sqrt{3}|0\rangle|0\rangle - \sqrt{3}|0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle \right) \\ &= \frac{1}{2\sqrt{2}} \left(\sqrt{3}|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle) \right) \\ &= \frac{1}{2\sqrt{2}} \left(\sqrt{3}|0\rangle + |1\rangle \right) (|0\rangle - |1\rangle) \\ &= \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle \right) \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right) = |\phi_1\rangle|\phi_0\rangle. \end{aligned}$$

Vướng lượng tử (tt)

Ví dụ 2 (tt)

Như vậy $|\phi\rangle$ có thể được tách thành các trạng thái riêng lẻ của qubit 0 là $|\phi_0\rangle$ và qubit 1 là $|\phi_1\rangle$. Hơn nữa, có thể biểu diễn $|\phi_0\rangle, |\phi_1\rangle$ trên mặt cầu Bloch (kiểm tra!)

$$|\phi_0\rangle = \cos \frac{\pi}{4} |0\rangle + e^{-i\pi} \sin \frac{\pi}{4} |1\rangle, |\phi_1\rangle = \cos \frac{\pi}{6} |0\rangle + e^{0i} \sin \frac{\pi}{6} |1\rangle.$$



Vướng lượng tử (tt)

Ví dụ 2 (tt)

Với hệ 3 qubit các trạng thái sau hay được dùng.

Trạng thái GHZ (Greenberger–Horne–Zeilinger state)

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle.$$

Trạng thái W (Wolfgang Dür state)

$$|W\rangle = \frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle.$$

Các trạng thái này đều là các trạng thái vướng. (kiểm tra!)

Nội dung

1. Trạng thái

2. Vương lượng tử

3. Phép đo

4. Cổng lượng tử

5. Tập cổng lượng tử toàn năng

Phép đo

Một hệ n qubit ở trạng thái $|\psi\rangle = \sum_{b \in \{0,1\}^n} \alpha_b |b\rangle$ khi được thực hiện phép đo theo cơ sở tính toán sẽ được một chuỗi n bit b với xác suất $|\alpha_b|^2$ và ngay sau khi đo thì qubit chuyển sang trạng thái $|b\rangle$. Việc chuyển trạng thái khi đo còn được gọi là sự sụp đổ.

Kết quả đo $b = b_{n-1} \dots b_1 b_0$ nghĩa là qubit 0 được bit b_0 , qubit 1 được bit b_1 , ... và trạng thái của hệ sụp đổ thành $|b\rangle = |b_{n-1}\rangle \dots |b_1\rangle |b_0\rangle$ nghĩa là qubit 0 sụp đổ thành $|b_0\rangle$, qubit 1 sụp đổ thành $|b_1\rangle$, ... Như vậy, phép đo này đo đồng thời tất cả các qubit.

Để phân biệt, trong trạng thái lượng tử $|\psi\rangle = \sum_{b \in \{0,1\}^n} \alpha_b |b\rangle$, các hệ số α_b được gọi là các amplitude, còn $|\alpha_b|^2$ là các xác suất. Nhận xét, $\sum_{b \in \{0,1\}^n} |\alpha_b|^2 = 1$ như yêu cầu của xác suất vì việc đo chỉ cho ra một chuỗi n bit.

Phép đo (tt)

Tổng quát, cho $B = \{|a_k\rangle, k = 0, \dots, 2^n - 1\}$ là một cơ sở trực chuẩn của \mathbb{C}^{2^n} , trạng thái $|\psi\rangle$ của hệ n qubit có thể được viết theo cơ sở B là

$$|\psi\rangle = \sum_{k=0}^{2^n-1} \langle a_k|\psi\rangle |a_k\rangle.$$

Khi đó, phép đo (đồng thời) theo cơ sở B sẽ cho kết quả $|a_k\rangle$ (có thể gọi là kết quả k) với xác suất $|\langle a_k|\psi\rangle|^2$ và trạng thái của hệ sụp đổ thành $|a_k\rangle$. Lưu ý, $(\langle a_k|\psi\rangle, k = 0, \dots, 2^n - 1)$ là tọa độ của $|\psi\rangle$ theo cơ sở B .

(Kiểm tra $\sum_{k=0}^{2^n-1} |\langle a_k|\psi\rangle|^2 = 1$!)

(Kiểm tra phép đo theo cơ sở tính toán chỉ là một trường hợp của định nghĩa này!)

Phép đo (tt)

Ví dụ 3 (tiếp Ví dụ 2)

Xét hệ 2 qubit với trạng thái

$$|\psi\rangle = \sum_{k=0}^3 \frac{1}{2} |k\rangle = \frac{1}{2} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle.$$

Khi đo $|\psi\rangle$ theo cơ sở tính toán ta được 00, 01, 10, 11 với xác suất đều là $|\frac{1}{2}|^2 = 25\%$ nên $|\psi\rangle$ được gọi là “tổ hợp đều”. Nếu dùng số thứ tự ta cũng có thể nói là được 0, 1, 2, 3 với xác suất đều là 50%.

Ngược lại, theo cơ sở Bell, $|\psi\rangle$ được viết là

$$\begin{aligned} |\psi\rangle &= \langle\Phi^+|\psi\rangle|\Phi^+\rangle + \langle\Phi^-|\psi\rangle|\Phi^-\rangle + \langle\Psi^+|\psi\rangle|\Psi^+\rangle + \langle\Psi^-|\psi\rangle|\Psi^-\rangle \\ &= \frac{1}{\sqrt{2}}|\Phi^+\rangle + \frac{1}{\sqrt{2}}|\Psi^+\rangle \end{aligned}$$

Phép đo (tt)

Ví dụ 3 (tt)

nên khi đo theo cơ sở Bell ta được chỉ 1 trong 2 kết quả $|\Phi^+\rangle, |\Psi^+\rangle$ với xác suất đều là 50%. Nếu dùng số thứ tự ($|\Phi^+\rangle$ là 0, $|\Phi^-\rangle$ là 1, $|\Psi^+\rangle$ là 2, $|\Psi^-\rangle$ là 3) ta cũng có thể nói là được 0, 2 với xác suất đều là 50% (không thể được 1, 3).

Khi đo trạng thái $|\phi\rangle = \frac{1}{2\sqrt{2}} (\sqrt{3}|00\rangle - \sqrt{3}|01\rangle + |10\rangle - |11\rangle)$ theo cơ sở tính toán ta được: 00, 01 với cùng xác suất $\left|\frac{\sqrt{3}}{2\sqrt{2}}\right|^2 = \frac{3}{8}$ và 10, 11 với cùng xác suất $\left|\frac{1}{2\sqrt{2}}\right|^2 = \frac{1}{8}$.

Xét riêng qubit 0, ta được 0 với xác suất $\frac{3}{8} + \frac{1}{8} = 50\%$ (được 1 với xác suất 50%). Xét riêng qubit 1, ta được 0 với xác suất $\frac{3}{8} + \frac{3}{8} = 75\%$ (được 1 với xác suất 25%).

Phép đo riêng

Cho hệ n qubit ở trạng thái $|\psi\rangle \in \mathbb{C}^{2^n}$, ta có thể tiến hành phép đo riêng lẻ trên các qubit, gọi là **phép đo riêng** (partial measurement). Chẳng hạn, để đo qubit 0 theo cơ sở tính toán, ta viết lại $|\psi\rangle$ theo dạng (có duy nhất một cách viết, kiểm tra!)

$$|\psi\rangle = |\psi_0\rangle|0\rangle + |\psi_1\rangle|1\rangle, |\psi_0\rangle, |\psi_1\rangle \in \mathbb{C}^{2^{(n-1)}}.$$

Khi đó, phép đo qubit 0 theo cơ sở tính toán sẽ cho 1 trong 2 kết quả

- qubit 0 được 0 với xác suất $|||\psi_0\rangle||^2$ và hệ sụp đổ thành

$$\frac{1}{|||\psi_0\rangle||} |\psi_0\rangle|0\rangle,$$

- qubit 0 được 1 với xác suất $|||\psi_1\rangle||^2$ và hệ sụp đổ thành

$$\frac{1}{|||\psi_1\rangle||} |\psi_1\rangle|1\rangle.$$

(kiểm tra $|||\psi_0\rangle||^2 + |||\psi_1\rangle||^2 = 1!$)

Phép đo riêng (tt)

Ví dụ 4 (tiếp Ví dụ 3)

Xét hệ 2 qubit với trạng thái

$$|\phi\rangle = \frac{1}{2\sqrt{2}} \left(\sqrt{3}|00\rangle - \sqrt{3}|01\rangle + |10\rangle - |11\rangle \right).$$

Để khảo sát phép đo riêng qubit 0 theo cơ sở tính toán, ta viết lại

$$|\phi\rangle = \frac{1}{2\sqrt{2}} (\sqrt{3}|0\rangle + |1\rangle)|0\rangle + \frac{1}{2\sqrt{2}} (-\sqrt{3}|0\rangle - |1\rangle)|1\rangle.$$

Do đó ta có qubit 0 được 0 với xác suất $\left| \frac{1}{2\sqrt{2}} (\sqrt{3}|0\rangle + |1\rangle) \right|^2 = 50\%$ và sụp đổ thành $\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle \right) |0\rangle$; được 1 với xác suất 50% và sụp đổ thành $\left(-\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \right) |1\rangle \equiv \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle \right) |1\rangle$.

Phép đo riêng (tt)

Ví dụ 4 (tt)

Xác suất được 0 (hay 1) của qubit 0 khi đo riêng qubit 0 khớp với kết quả đo đồng thời cả 2 qubit ở Ví dụ 3.

Thật ra, ví dụ này khá đặc biệt, vì ở Ví dụ 2 ta đã thấy

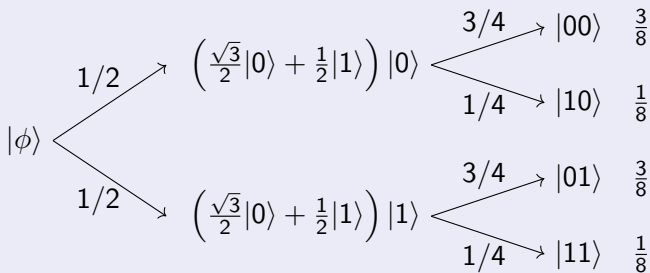
$$|\phi\rangle = \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle \right) \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right) = |\phi_1\rangle|\phi_0\rangle$$

nên trạng thái $|\phi\rangle$ của hệ có thể được phân tách riêng biệt thành trạng thái của qubit 0 là $|\psi_0\rangle$ và trạng thái của qubit 1 là $|\psi_1\rangle$. Khi đó, phép đo riêng lẻ trên từng qubit “không ảnh hưởng” đến qubit còn lại. Do đó, dù đo riêng qubit 0 ra kết quả gì (0 hay 1) thì qubit 1 vẫn giữ trạng thái $|\phi_1\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$. (Kiểm tra, nếu đo riêng qubit 1, dù ra kết quả gì thì qubit 0 vẫn giữ trạng thái $|\phi_0\rangle$.)

Phép đo riêng (tt)

Ví dụ 4 (tt)

Sơ đồ sau khảo sát phép đo $|\phi\rangle$ riêng theo qubit 0 rồi đến qubit 1
đo riêng theo qubit 0 đo riêng theo qubit 1



Ta thấy kết quả chung cuộc giống với kết quả đo đồng thời cả 2 qubit. (Kiểm tra, nếu đo riêng theo qubit 1 rồi đến qubit 0 cũng cho cùng kết quả.)

Nội dung

1. Trạng thái
2. Vương lượng tử
3. Phép đo
- 4. Cổng lượng tử**
5. Tập cổng lượng tử toàn năng

Cổng lượng tử

Cổng lượng tử trên hệ n qubit là toán tử tuyến tính bảo toàn chuẩn trên \mathbb{C}^{2^n} . Cổng lượng tử được đồng nhất với ma trận biểu diễn nó là ma trận unita kích thước $2^n \times 2^n$.

Trường hợp đơn giản, cổng lượng tử trên hệ n qubit là tích tensor các cổng lượng tử 1 qubit. Chẳng hạn, xét hệ 2 qubit đang có trạng thái $|\psi\rangle$, nếu ta tác động cổng U_0 lên qubit 0 và cổng U_1 lên qubit 1 thì hệ sẽ chuyển sang trạng thái (lưu ý qui ước big-endian)

$$|\phi\rangle = (U_1 \otimes U_0)|\psi\rangle.$$

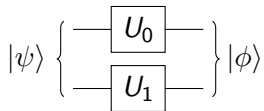
Đơn giản hơn nữa, nếu $|\psi\rangle$ tách được $|\psi\rangle = |\psi_1\rangle|\psi_0\rangle$ thì

$$|\phi\rangle = (U_1 \otimes U_0)(|\psi_1\rangle \otimes |\psi_0\rangle) = U_1|\psi_1\rangle \otimes U_0|\psi_0\rangle = U_1|\psi_1\rangle U_0|\psi_0\rangle.$$

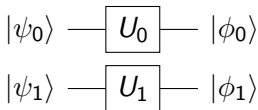
Khi đó $|\phi\rangle$ cũng tách được.

Cổng lượng tử (tt)

Biến đổi $|\phi\rangle = (U_1 \otimes U_0)|\psi\rangle$ được mô tả bằng sơ đồ mạch



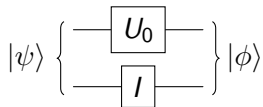
Ta qui ước các đường ứng với các qubit được vẽ từ trên xuống (đường trên cùng ứng với qubit 0, ..., đường dưới cùng ứng với qubit $n - 1$ của hệ). Cặp ngoặc nhọn nối các đường để chỉ các qubit có thể ở trạng thái vướng. Trường hợp đầu vào $|\psi\rangle$ tách được, $|\psi\rangle = |\psi_1\rangle|\psi_0\rangle$, sơ đồ mạch sau mô tả rõ ràng hơn



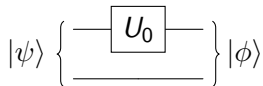
Đầu ra $|\phi\rangle = |\phi_1\rangle|\phi_0\rangle$.

Cổng lượng tử (tt)

Nếu một qubit nào đó trong hệ không bị tác động, ta có thể xem như nó bị tác động bởi cổng đơn vị I (cổng NOOP). Chẳng hạn, mạch sau



mô tả tác động U_0 lên qubit 0 mà không làm gì với qubit 1. Dĩ nhiên, mạch trên có thể được mô tả đơn giản hơn là



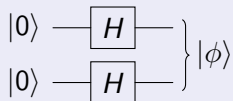
Trường hợp ta tác động cổng 1 qubit U lên tất cả n qubit của hệ thì tác động lên hệ là

$$U^{\otimes n} = \underbrace{U \otimes U \otimes \dots \otimes U}_{n \text{ lần}} \in \mathbb{C}^{2^n \times 2^n}.$$

Cổng lượng tử (tt)

Ví dụ 5

Mạch 2 qubit



cho đầu ra là trạng thái (tách được)

$$|\phi\rangle = H|0\rangle H|0\rangle = |+\rangle|+\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle.$$

Tổng quát, với hệ n qubit, đầu ra là trạng thái “tổ hợp đều”

$$H^{\otimes n}|0\rangle^{\otimes n} = (H|0\rangle)^{\otimes n} = |+\rangle^{\otimes n} = \sum_{k=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|k\rangle.$$

Cổng lượng tử (tt)

Ví dụ 6

Xét mạch 2 qubit

$$|\Phi^+\rangle \left\{ \begin{array}{c} \text{---} \boxed{X} \text{---} \\ \text{---} \end{array} \right\} |\chi\rangle$$

Mạch này mô tả hệ 2 qubit ở trạng thái vướng $|\Phi^+\rangle$, nhận tác động cổng X lên qubit 0 (không tác động gì đến qubit 1), chuyển sang

$$\begin{aligned} |\chi\rangle &= (I \otimes X)|\Phi^+\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} [1 \ 0 \ 0 \ 1]^T \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = |\Psi^+\rangle. \end{aligned}$$

Cổng CNOT

Cổng CNOT (CNOT gate, controlled-NOT, CX, controlled-X) là cổng 2 qubit được xác định bởi

$$\begin{aligned}\text{CNOT}|00\rangle &= |00\rangle, & \text{CNOT}|01\rangle &= |01\rangle, \\ \text{CNOT}|10\rangle &= |11\rangle, & \text{CNOT}|11\rangle &= |10\rangle,\end{aligned}$$

mà có thể được mô tả gọn hơn là

$$\text{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle, a, b \in \{0, 1\}.$$

CNOT là phiên bản lượng tử của cổng XOR cổ điển!

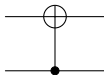
Ta cũng thấy

- nếu qubit 1 là $|0\rangle$ thì $\text{CNOT}|0\rangle|b\rangle = |0\rangle|b\rangle$,
- nếu qubit 1 là $|1\rangle$ thì $\text{CNOT}|1\rangle|b\rangle = |1\rangle|1 \oplus b\rangle = |1\rangle|\text{NOT } b\rangle$.

Như vậy, qubit 1 điều khiển thao tác NOT trên qubit 0!

Cổng CNOT (tt)

Cổng CNOT thường được vẽ trên mạch là



Dấu chấm cho biết **qubit điều khiển** (control qubit), ở đây là qubit 1; dấu cộng trong vòng tròn cho biết **qubit mục tiêu** (target qubit), ở đây là qubit 0.

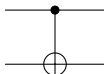
CNOT có ma trận biểu diễn và tác động lên $|\psi\rangle = \sum_{k=0}^3 \alpha_k |k\rangle$ là

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{CNOT} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_3 \\ \alpha_2 \end{bmatrix}.$$

Cổng CNOT (tt)

Tổng quát, ta kí hiệu CNOT_{ij} là cổng CNOT với qubit điều khiển i và qubit mục tiêu j . Như vậy, CNOT chính là CNOT_{10} .

Cổng CNOT_{01}



có ma trận biểu diễn và tác động lên $|\psi\rangle = \sum_{k=0}^3 \alpha_k |k\rangle$ là

$$\text{CNOT}_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad \text{CNOT}_{01} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_3 \\ \alpha_2 \\ \alpha_1 \end{bmatrix}.$$

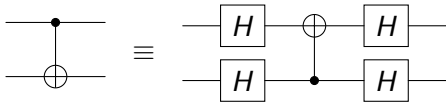
(kiểm tra!)

Cổng CNOT (tt)

Nhận xét (kiểm tra!)

$$\text{CNOT}_{01} = (H \otimes H)\text{CNOT}(H \otimes H).$$

Do đó



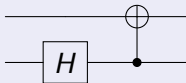
tức là, ta có thể “cài đặt” hay “thi công” hay “hiện thực” CNOT_{01} bằng các cổng H và CNOT!

(Lưu ý, nếu chỉ được phép dùng các cổng H và CNOT thì mạch trên có thể được coi là một “thuật toán lượng tử” giúp thực hiện tính toán ta cần là CNOT_{01} bằng các tính toán ta có là H và CNOT! Hơn nữa, ý tưởng của thuật toán này là “ CNOT_{01} trong cơ sở tính toán (cơ sở Z) chính là CNOT_{10} trong cơ sở X!”)

Cổng CNOT (tt)

Ví dụ 7

Mạch sau có vai trò rất quan trọng trong tính toán lượng tử



Nếu đầu vào là $|00\rangle$ thì đầu ra là

$$\begin{aligned}\text{CNOT}(H|0\rangle \otimes I|0\rangle) &= \text{CNOT}(|+\rangle|0\rangle) = \text{CNOT} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \\ &= \frac{1}{\sqrt{2}}\text{CNOT}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle.\end{aligned}$$

Mạch này chuyển cơ sở tính toán gồm các trạng thái tách được sang cơ sở Bell gồm các trạng thái vướng. (kiểm tra!)

Cổng điều khiển

Mở rộng cổng CNOT, với U là cổng 1 qubit bất kỳ, **cổng kiểm soát- U** (controlled- U gate) là cổng 2 qubit được xác định bởi

$$CU|00\rangle = |00\rangle, \quad CU|01\rangle = |01\rangle,$$

$$CU|10\rangle = |1\rangle U|0\rangle, \quad CU|11\rangle = |1\rangle U|1\rangle.$$

CU tác động U lên qubit 0 nếu qubit 1 là 1 (không làm gì nếu qubit 1 là 0). Nhận xét, CNOT chính là CX .

Nếu U có ma trận biểu diễn là

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{C}^{2 \times 2}$$

thì

$$U|0\rangle = a|0\rangle + c|1\rangle, \quad U|1\rangle = b|0\rangle + d|1\rangle.$$

Cổng điều khiển (tt)

Khi đó

$$CU|00\rangle = |00\rangle, \quad CU|01\rangle = |01\rangle,$$

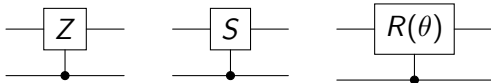
$$CU|10\rangle = |1\rangle U|0\rangle = |1\rangle(a|0\rangle + c|1\rangle) = a|10\rangle + c|11\rangle.$$

$$CU|11\rangle = |1\rangle U|1\rangle = |1\rangle(b|0\rangle + d|1\rangle) = b|10\rangle + d|11\rangle.$$

Do đó, CU có ma trận biểu diễn là

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}.$$

Ngoài CX thì các cổng điều khiển khác cũng hay được dùng



Cổng SWAP

Cổng SWAP (SWAP gate) là cổng 2 qubit được xác định bởi

$$\begin{aligned}\text{SWAP}|00\rangle &= |00\rangle, & \text{SWAP}|01\rangle &= |10\rangle, \\ \text{SWAP}|10\rangle &= |01\rangle, & \text{SWAP}|11\rangle &= |11\rangle,\end{aligned}$$

mà có thể được mô tả gọn hơn là

$$\text{SWAP}|a\rangle|b\rangle = |b\rangle|a\rangle, a, b \in \{0, 1\}.$$

SWAP hoán đổi trạng thái 2 qubit vì với

$$|\psi\rangle = a|0\rangle + b|1\rangle, |\phi\rangle = c|0\rangle + d|1\rangle \in \mathbb{C}^2,$$

$$\begin{aligned}\text{SWAP}|\psi\rangle|\phi\rangle &= \text{SWAP}(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \\ &= \text{SWAP}(ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle) \\ &= (ac|00\rangle + ad|10\rangle + bc|01\rangle + bd|11\rangle) \\ &= (c|0\rangle + d|1\rangle)(a|0\rangle + b|1\rangle) = |\phi\rangle|\psi\rangle.\end{aligned}$$

Cổng SWAP (tt)

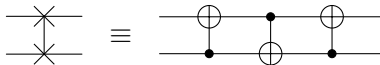
Cổng SWAP thường được vẽ trên mạch là



SWAP có ma trận biểu diễn và tác động lên $|\psi\rangle = \sum_{k=0}^3 \alpha_k |k\rangle$ là

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{SWAP} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_2 \\ \alpha_1 \\ \alpha_3 \end{bmatrix}.$$

SWAP có thể được “thi công” bằng 3 cổng CNOT qua đẳng thức mạch sau (kiểm tra!)



Cổng Toffoli

Cổng Toffoli (Toffoli gate) là cổng 3 qubit được xác định bởi

$$\text{Toffoli}|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|ab \oplus c\rangle, a, b, c \in \{0, 1\}.$$

Toffoli là phiên bản lượng tử của cổng AND hoặc NAND cổ điển vì

$$\text{Toffoli}|a\rangle|b\rangle|0\rangle = |a\rangle|b\rangle|ab\rangle, a, b \in \{0, 1\},$$

$$\text{Toffoli}|a\rangle|b\rangle|1\rangle = |a\rangle|b\rangle|\text{NOT}ab\rangle, a, b \in \{0, 1\}.$$

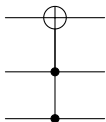
Toffoli còn được gọi là cổng CCNOT hoặc CCX vì

- $\text{Toffoli}|1\rangle|1\rangle|c\rangle = |1\rangle|1\rangle|\text{NOT}c\rangle,$
- $\text{Toffoli}|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|c\rangle, a, b, c \in \{0, 1\}, ab \neq 1.$

Lưu ý, qubit 0 là qubit mục tiêu còn qubit 1, 2 là qubit điều khiển.

Cổng Toffoli (tt)

Cổng Toffoli thường được vẽ trên mạch là



Toffoli có ma trận biểu diễn và tác động lên $|\psi\rangle = \sum_{k=0}^7 \alpha_k |k\rangle$ là

$$\text{Toffoli} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{Toffoli} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_7 \\ \alpha_6 \end{bmatrix}.$$

Nội dung

1. Trạng thái
2. Vương lượng tử
3. Phép đo
4. Cổng lượng tử
- 5. Tập cổng lượng tử toàn năng**

Tập cổng lượng tử toàn năng

Một tập (“nhỏ”) các cổng lượng tử cho phép “xấp xỉ” mọi toán tử lượng tử với độ chính xác tùy ý được gọi là **tập cổng lượng tử toàn năng** (universal quantum gate set).

Các tập cổng lượng tử toàn năng điển hình

- {CNOT và tất cả các cổng một qubit},
- {CNOT, H , T },
- {CNOT, $R_{\frac{\pi}{8}}$, S },
- {Toffoli, H , S },
- {Toffoli, H },
- { CH }.

Tài liệu tham khảo

Chapter 4. Thomas G. Wong. *Introduction to Classical and Quantum Computing*. Rooted Grove, 2022.

Chapter 4, 5. Noson S. Yanafsky, Mirco A. Mannucci. *Quantum Computing for Computer Scientists*. Cambridge University Press, 2008.