Quantum Computing

Alessandra Di Pierro

Appunti del corso - A.A. 2001-2002

Lezioni 9 e 10: Il modello dei circuiti per la computazione quantistica

1 Circuiti quantistici

Il modello di computazione basato sui circuiti quantistici é stato introdotto da Deutsch (1989) e sviluppato ulteriormente da Yao (1993) che ne dimostra anche l'equivalenza con un altro modello per la computazione quantistica: la Macchina di Turing quantistica. Quest'ultima é stata introdotta da Benioff (1980) e successivamente sviluppata da Deutsch (1985) e Yao (1993). L'articolo di Bernstein e Vazirani *Quantum Complexity Theory* (1997) contiene una descrizione completa e moderna della macchina di Turing quantistica. In questo articolo viene affrontato il tema della complessitá computazionale dimostrando per la computazione quantistica gli analoghi dei risultati della complessitá computazionale classica.

Questa lezione é dedicata al modello dei circuiti, mentre si consiglia fortemente la lettura dell'articolo di Bernstein e Vazirani per una descrizione del modello basato sulla Macchina di Turing quantistica.

1.1 Operazioni su un qubit

Le operazioni piú elementari sono quelle su un singolo qubit. Ricordiamo che un qubit é un vettore $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ nello spazio di Hilbert $\mathbb{C}^2$, tale che $|a|^2 + |b|^2 = 1$. Le operazioni su un qubit devono preservare questa norma e sono pertanto descritte da matrici unitarie 2×2. Tra queste abbiamo visto le matrici di Pauli:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ e } Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Un ruolo molto importante nella definizione del modello dei circuiti é svolto anche dalle seguenti operazioni:

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

Abbiamo giá visto la porta di Hadamard H. Il gate S é detto gate di fase, mentre il gate T é anche chiamato gate $\pi/8$ perché risulta

$$T = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}.$$

Si verifica facilmente che $H = (X + Z)/\sqrt{2}$, $S = T^2$ e $S = \sqrt{Z}$.

Ricordiamo inoltre che lo stato di un qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ puó essere visualizzato come un punto (θ, φ) sulla sfera unitaria in $\mathbb{R}^3$ (la sfera di Bloch) dato che esiste una corrispondenza biunivoca tra qubits e questi punti. Analogamente, le operazioni su un qubit (cioé le matrici unitarie 2×2) corrispondono alle *rotazioni* del punto che rappresenta il qubit sulla sfera di Bloch (cf. Sezione A.3 in Appendice). In generale il teorema di Bloch (cf. Teorema 1.3) assicura che qualsiasi matrice unitaria 2×2 si puó decomporre in un prodotto di rotazioni nel piano $(\vec{x}, \vec{y})$ e rotazioni intorno all'asse $\vec{z}$. Come spiegato in Appendice, le prime sono descritte da matrici della forma

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix},$$

mentre, come vedremo, le seconde corrispondono a operazioni unitarie della forma

$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}.$$

Per poter enunciare questo teorema abbiamo bisogno di introdurre la nozione di *esponenziale di una matrice* e la definizione di *operatore di rotazione* intorno agli assi $\vec{x}$, $\vec{y}$ e $\vec{z}$.

1.1.1 Esponenziale di una matrice

In generale, l'esponenziale e^A di una matrice complessa $n \times n$, A, é definita mediante la serie di potenze

$$e^A = \sum_{m=0}^{\infty} \frac{A^m}{m!}.$$

Si dimostra che questa serie converge e che e^A é una funzione continua di A. Si dimostrano inoltre le seguenti proprietá:

1. $e^0 = I$
2. e^A é invertibile e $(e^A)^{-1} = e^{-A}$
3. $e^{(a+b)A} = e^{aA}e^{bA}$, per ogni $a, b \in \mathbb{C}$
4. se $AB = BA$, allora $e^{A+B} = e^A e^B = e^B e^A$
5. se C é invertibile, allora $e^{CAC^{-1}} = Ce^A C^{-1}$
6. $\|e^A\| \leq e^{\|A\|}$.

Se A é diagonalizzabile possiamo calcolare esplicitamente e^A nel seguente modo[1]. Poiché A é diagonalizzabile esiste una matrice invertibile C tale che $A = CDC^{-1}$, dove

$$D = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}.$$

Osserviamo che e^A é la matrice diagonale con autovalori e^{λ_i}; quindi per la proprietá 5, otteniamo

$$e^A = C \begin{bmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{bmatrix} C^{-1}.$$

Esempio 1.1 *Consideriamo la matrice*

$$A = \begin{bmatrix} 0 & -a \\ a & 0 \end{bmatrix}.$$

A ha autovettori $\begin{bmatrix} 1 \\ i \end{bmatrix}$ e $\begin{bmatrix} i \\ 1 \end{bmatrix}$ con corrispondenti autovalori $-ia$ e ia. Si verifica facilmente che $D = CAC^{-1}$ dove $C = \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$ é una matrice diagonale e che $A = CDC^{-1}$. Pertanto

$$e^A = \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} e^{-ia} & 0 \\ 0 & e^{ia} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{-i}{2} \\ \frac{-i}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{bmatrix}.$$

[1]Nota che le nostre operazioni su qubits sono matrici unitarie e quindi in particolare operatori normali e ammettono pertanto una scomposizione spettrale, cioé sono diagonalizzabili.

1.1.2 Operatori di rotazione

Gli esponenziali delle matrici di Pauli danno luogo a tre utili classi di matrici unitarie: gli *operatori di rotazione* intorno agli assi $\vec{x}$, $\vec{y}$ e $\vec{z}$ definiti come:

$$R_x(\theta) \equiv e^{-i\theta\sigma_x/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_x = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \quad (1)$$

$$R_y(\theta) \equiv e^{-i\theta\sigma_y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_y = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \quad (2)$$

$$R_z(\theta) \equiv e^{-i\theta\sigma_z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \quad (3)$$

Possiamo usare il procedimento visto nell'Esempio 1.1 per calcolare esplicitamente l'esponenziale delle matrici di Pauli e verificare le espressioni (1), (2) e (3). Per esempio, per calcolare l'esponenziale $e^{-i\theta\sigma_z/2}$, ricordiamo che σ_z ha autovettori $|0\rangle$ e $|1\rangle$ con corrispondenti autovalori 1 e -1, quindi in questo caso $C = I$ e pertanto

$$e^{-i\theta\sigma_z/2} = I \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} I.$$

Analogamente, si calcolano gli esponenziali per σ_x e σ_y ricordando che gli autovettori sono:

$$|x_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ e } |x_2\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \text{ per } \sigma_x,$$

$$|y_1\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} \text{ e } |y_2\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \text{ per } \sigma_y,$$

corrispondenti rispettivamente agli autovalori 1 e -1. Si noti che la matrice C é in questo caso la matrice del cambio di base, cioé $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ per σ_x, e $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$ per σ_y.

Un modo alternativo per verificare le equazioni (1), (2) e (3) é usare la seguente proprietá che é una diretta conseguenza della definizione di esponenziale come serie di potenze data precedentemente .

Proposizione 1.2 *Dato $x \in \mathbb{R}$ e A una matrice tale che $A^2 = I$, allora*

$$e^{iAx} = \cos xI + i\sin xA.$$

Dimostrazione Per definizione

$$e^{iAx} = \sum_{m=0}^{\infty} \frac{(ix)^m}{m!} A^m.$$

Dall'ipotesi $A^2 = I$, si ha quindi, separando le somme sugli indici pari e dispari:

$$\begin{aligned} e^{iAx} &= \sum_{m=0}^{\infty} \frac{(ix)^{2m}}{(2m)!} I + \sum_{m=0}^{\infty} \frac{(ix)^{2m+1}}{(2m+1)!} A \\ &= \sum_{m=0}^{\infty} \frac{(-1)^m x^{2m}}{(2m)!} I + i \sum_{m=0}^{\infty} \frac{(-1)^m x^{2m+1}}{(2m+1)!} A \end{aligned}$$

Osserviamo ora che le due somme sono lo sviluppo in serie di potenze per $\cos x$ e $\sin x$ rispettivamente.

Se $\hat{n} = (n_x, n_y, n_z)$ é un vettore unitario nello spazio $\mathbb{R}^3$, allora possiamo generalizzare le definizioni di R_x, R_y e R_z per definire una rotazione di θ intorno all'asse $\hat{n}$:

$$R_{\hat{n}}(\theta) \equiv e^{-i\theta \hat{n}\cdot\vec{\sigma}/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z),$$

dove $\vec{\sigma} = \sigma_x + \sigma_y + \sigma_z$.

Possiamo ora enunciare il teorema di Bloch:

Teorema 1.3 *Per ogni matrice unitaria 2×2, U esistono numeri reali α, β, γ e δ tali che*

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

Il seguente corollario sará utile nel seguito per dimostrare il risultato di universalitá in 1.3.

Corollario 1.4 *Supponiamo che U sia un'operazione unitaria su un singolo qubit. Allora esistono operatori unitari su un singolo qubit A, B e C tali che $ABC = I$ e $U = e^{i\alpha} AXBXC$, per qualche $\alpha \in \mathbb{R}$.*

Inoltre le seguenti identitá sono utili e facili da verificare:

$$HXH = Z;\ HYH = -Y;\ HZH = X.$$

La terza identitá ci permette di dimostrare la seguente proposizione

Proposizione 1.5 *$HTH = R_x(\pi/4)$ a meno di un fattore di fase globale.*

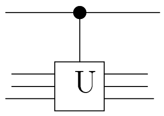

Figure 1: Operazione controllata su singolo qubit

Dimostrazione
Per definizione di operatore di rotazione e dalla identitá $HZH = X$, si ha che $R_x(\pi/4) = e^{-i\frac{\pi}{8}\sigma_x} = e^{-i\frac{\pi}{8}H\sigma_z H}$. Poiché H é invertibile, per la proprietá (5) dell'esponeziale di una matrice (cf. 1.1.1) otteniamo

$$e^{-i\frac{\pi}{8}H\sigma_z H} = H \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix} H \approx He^{i\frac{\pi}{8}} \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix} H = HTH.$$

Esercizio 1.6 *Dimostrare che un arbitrario operatore unitario su singolo qubit puó essere scritto nella forma*

$$U = e^{i\gamma} R_{\hat{n}} \alpha,$$

dove $\gamma, \alpha \in \mathbb{R}$ *e* $\hat{n}$ *é un vettore unitario in* $\mathbb{R}^3$.

1.2 Operazioni "controllate"

Il prototipo di queste operazioni é il `CNOT` (controlled-`NOT`), introdotto nella Lezione 3. Ricordiamo che `CNOT` agisce su due qubits chiamati rispettivamente *controllo* e *target* e che il suo effetto nella base computazionale é dato da $|c\rangle |t\rangle \to |c\rangle |t \oplus c\rangle$.

In generale, si puó definire un'operazione controllata a partire da una qualsiasi operazione unitaria U mediante il circuito in Figura 1. Se U agisce su un singolo qubit, il circuito trasforma i qubits in input $|c\rangle |t\rangle$ in $|c\rangle U^c |t\rangle$, cioé U é applicata al qubit target soltanto se il qubit di controllo é 1.

Il circuito in Figura 2 rappresenta l'operazione controllata piú generale $C^n(U)$, dove n é il numero dei qubits di controllo e U é una operazione unitaria su k qubits per qualche intero k.

Le operazioni controllate possono essere implementate usando solo `CNOT` e operazioni unitarie su un singolo qubit che, come vedremo in 1.3, costituisce un insieme *universale* per la computazione quantistica. Un aspetto fondamentale della computazione quantistica é l'implementazione fault-tolerant (cioé resistente agli errori) delle varie operazioni. Esiste un insieme discreto di operazioni elementari che é universale e puó essere implementato in modo robusto usando dei codici di correzione degli errori. Come vedremo in

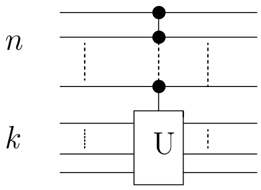

Figure 2: Controlled-U generale con n qubit di controllo e operazione U su k qubit

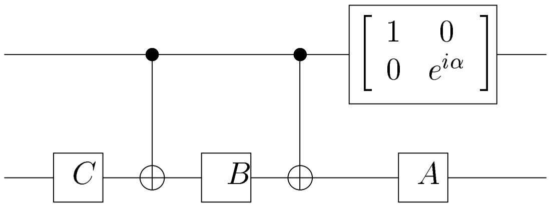

Figure 3: Circuito che implementa controlled-U per operazioni U su singolo qubit.

1.4, questo insieme universale discreto é formato da Hadmard, `CNOT`, S e T. Poiché l'insieme delle operazioni unitarie é continuo, l'universalitá di questo insieme discreto deve essere intesa nel senso che le quattro operazioni che lo compongono possono essere usate per *approssimare* una qualsiasi operazione unitaria, piuttosto che per implementarla esattamente. Il significato di tale approssimazione verrá chiarito in 1.4.

1.2.1 Implementazione di $C^n(U)$ mediante `CNOT` e operazioni su singolo qubit

Consideriamo pima il caso piú semplice dove $n = 1$ e U é un'operazione unitaria su un singolo qubit, cioé circuiti come quello in Figura 1 dove U ha un solo qubit di input. Per il Corollario 1.4, esistono matrici unitarie su un singolo qubit A, B, C tali che $U = e^{i\alpha}AXBXC$. Allora possiamo costruire un circuito equivalente usando solo `CNOT`, le operazioni A, B, C e l'operazione che realizza la moltiplicazione controllata del qubit target per $e^{i\alpha}$ come mostrato in Figura 3.

L'operazione

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$$

applicata al primo qubit effettivamente realizza la moltiplicazione del sec-

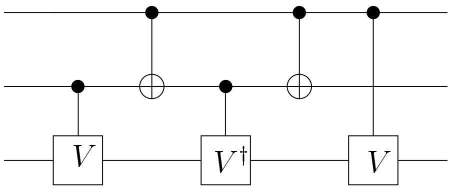

Figure 4: Circuito che realizza $C^2(U)$ per $U = V^2$

ondo qubit per $e^{i\alpha}$ se il qubit di controllo é 1, come si puó verificare valutandone l'effetto sulla base computazionale:

$$|00\rangle \to |00\rangle\,, |01\rangle \to |01\rangle\,, |10\rangle \to e^{i\alpha}\,|10\rangle\,, |11\rangle \to e^{i\alpha}\,|11\rangle\,.$$

Consideriamo ora il caso in cui $n = 2$ e U é ancora un operatore unitario su un singolo qubit. Allora il circuito in Figura 4 implementa $C^2(U)$ nell'ipotesi che esista un operatore unitario V tale che $V^2 = U$.

Per $U = X$ si ottiene l'operazione di Toffoli che, vista come operazione classica, é universale per le computazioni classiche reversibili. Ricordiamo che questo risultato di universalitá non si poteva ottenere con un numero di input inferiore a tre. Al contrario, l'operazione di Toffoli si puó implementare come operazione quantistica usando solo operazioni su uno o due qubit. Tale implementazione si ottiene mediante il circuito in Figura 4 con $V = (1 - i)(I + iX)/2$.

Possiamo ora considerare il caso di n qubits di controllo e ancora un solo qubit target, cioé l'operazione $C^n(U)$ definita dall'equazione

$$C^n(U)\,|c_1c_2\dots c_n\rangle\,|\psi\rangle = |c_1c_2\dots c_n\rangle\,U^{c_1c_2\dots c_n}\,|\psi\rangle\,.$$

L'operatore U é applicato al qubit target $|\psi\rangle$ se i primi n qubits sono tutti 1 (l'esponente di U nell'equazione rappresenta un `AND` dei bit c_i). Un circuito che implementa $C^n(U)$ si puó ottenere usando l'operazione di Toffoli per realizzare l'`AND` reversibile dei bit di controllo come mostrato in Figura 5.

1.3 Universalitá di `CNOT` e operazioni su singolo qubit

Qualsiasi operatore unitario si puó esprimere in maniera *esatta* mediante `CNOT` e operazioni su singolo qubit. Per dimostrarlo dobbiamo completare i risultati visti precedentemente per le operazioni controllate, considerando operazioni unitarie U su un numero arbitrario $k \geq 2$ di qubits. L'idea fondamentale é quella di scomporre una U arbitraria nel prodotto di matrici unitarie che operano in maniera non banale su al piú due componenti del

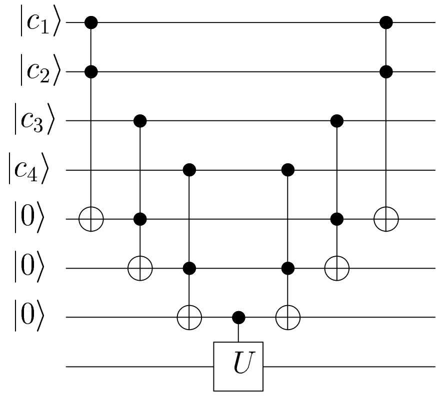

Figure 5: Circuito che realizza $C^n(U)$ per $n = 4$ e $k = 1$

vettore a cui sono applicate. Poiché tali matrici, dette *matrici unitarie a due livelli*, si possono implementare mediante circuiti costruiti usando `CNOT` e operazioni su singolo qubit, potremo quindi concludere il risultato di universalitá sopra citato.

Dato un operatore U su uno spazio d-dimensionale, é sempre possibile mediante una procedura puramente algebrica costruire matrici unitarie a due livelli $V_1, V_2 \dots V_{d'}$ tali che $U = V_1 V_2 \dots V_{d'}$ e $d' \leq d(d-1)/2$. Quindi non ci rimane altro che far vedere come costruire un circuito che implementa una matrice unitaria a due livelli ed é formato solo da `CNOT` e operazioni su singolo qubit.

Supponiamo che U sia una matrice unitaria a due livelli che opera su n qubits e supponiamo che gli stati su cui agisce effettivamente siano tutti quelli generati dai due stati $|s\rangle$ e $|t\rangle$ della base computazionale, dove s e t sono le rappresentazioni binarie dei numeri $s, t \in [0, n-1]$. Allora la sottomatrice non banale $\tilde{U}$ di U é una matrice unitaria 2×2 e si puó vedere come un operatore unitario su un singolo qubit. Per costruire il nostro circuito consideriamo la sequenza $g_1, g_2, \dots, g_m$ di numeri binari tali che $g_1 = s$, $g_m = t$ e per ogni $1 \leq i < m$, g_i e g_{i+1} differiscono per esattamente un bit. Usando operazioni controllate si realizza il passaggio da g_i a g_{i+1} per $1 \leq i < m-1$. A questo punto si esegue un controlled-$\tilde{U}$ con qubit target corrispondente al singolo bit su cui g_{m-1} e g_m differiscono e con i qubits di controllo corrispondenti ai valori dei bits che sono identici in g_{m-1} e g_m. Le operazioni di passaggio da g_i a g_{i+1} devono essere realizzate in modo reversibile e quindi in generale saranno necessarie $2(n-1)$ operazioni controllate per implementarle.

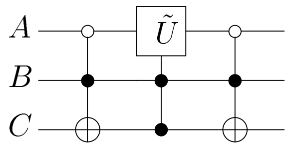

Figure 6: Circuito che implementa la matrice a due livelli U dell'esempio 1.7

Esempio 1.7 *Considera la matrice su tre qubits definita da*

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix},$$

dove $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ *é una arbitraria matrice unitaria* 2×2. *Notiamo che* U *agisce effettivamente solo sugli stati (generati da)* $|s\rangle = |010\rangle$ *e* $|t\rangle = |111\rangle$. *Il circuito che implementa* U *é dato in Figura 6. Gli input* A, B, C *sono inizialmente nella configurazione corrispondente a* s*, cioé* 010. *Lo stato successivo della sequenza* $\{g_i\}$ *é* 011 *e il passaggio é effettuato da un* `NOT` *su* C *condizionato dai valori dei bit* $A = 0$ *e* $B = 1$ *(ricordiamo che il pallino bianco indica che il target viene modificato se il controllo é* 0*, in maniera duale al pallino nero). Lo stato successivo é lo stato finale* $|t\rangle = |111\rangle$. *Quindi applichiamo* $\tilde{U}$ *ad* A *a condizione che* $B = 1$ *e* $C = 1$. *La parte destra del circuito riproduce simmetricamente la parte sinistra per ottenere la reversibilitá.*

1.4 Universalitá di Hadamard, `CNOT` e T

Le operazioni Hadamard, `CNOT` e T formano un insieme universale per la computazione quantistica nel senso che dato un circuito contenente `CNOT` e operazioni unitarie arbitrarie su singolo qubit, é possibile simularlo con una buona *approssimazione* usando solo questo insieme discreto di operazioni. Un operatore unitario V approssima un operatore unitario U se la quantitá

$$E(U, V) \equiv max_{|\psi\rangle} \| (U - V) |\psi\rangle \|,$$

dove il massimo é su tutti i vettori normalizzati nello spazio degli stati, é strettamente positiva. La quantitá $E(U,V)$ definisce l'errore di approssimazione. Se questo errore é piccolo, allora misurazioni eseguite sugli stati $V|\psi\rangle$ e $U|\psi\rangle$ daranno approssimativamente le stesse statistiche per ogni stato iniziale $|\psi\rangle$. Quindi le probabilitá dei risultati di una misurazione saranno simili sia che venga eseguito U sia che venga eseguito V.

Il risultato di universalitá sopra citato é conseguenza del fatto che le due operazioni H e HTH possono essere usate per approssimare una qualsiasi operazione unitaria su singolo qubit con un errore arbitrariamente piccolo. Ricordiamo che, a meno di un fattore di fase globale, T corrisponde a una rotazione di $\pi/4$ intorno all'asse $\hat{z}$ e HTH a una rotazione di $\pi/4$ intorno all'asse $\hat{x}$ (cf. Proposizione 1.5). Componendo queste due operazioni si ottiene:

$$\begin{aligned}
e^{-i\frac{\pi}{8}\sigma_x}e^{-i\frac{\pi}{8}\sigma_z} &= (\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}\sigma_x)(\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}\sigma_z) \\
&= \cos^2\frac{\pi}{8}I - i(\cos\frac{\pi}{8}(\sigma_x+\sigma_z) + i\sigma_x\sigma_z\sin\frac{\pi}{8})\sin\frac{\pi}{8} \\
&= \cos^2\frac{\pi}{8}I - i(\cos\frac{\pi}{8}(\sigma_x+\sigma_z) + \sin\frac{\pi}{8}\sigma_z)\sin\frac{\pi}{8}
\end{aligned}$$

Ricordando che $R_{\hat{n}}(\theta) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)$, l'espressione ottenuta é quindi una rotazione intorno all'asse $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$, con corrispondente vettore unitario $\hat{n}$, di un angolo θ definito da $\cos\theta/2 = \cos^2\frac{\pi}{8}$. Iterando l'applicazione di $R_{\hat{n}}(\theta)$ per un numero sufficiente di volte si puó approssimare una qualsiasi rotazione $R_{\hat{n}}(\alpha)$ in modo da ottenere un arbitrario livello di precisione ϵ.

Quindi, ricordando il risultato dimostrato nell'esercizio 1.6, dato un operatore unitario U su singolo qubit e un $\epsilon > 0$, é possibile approssimare U con precisione ϵ usando un circuito composto soltanto da operazioni T e H.

A Richiami di teoria dei gruppi

A.1 Definizioni e proprietá

Un gruppo é un insieme G con una operazione $* : G \times G \to G$ che gode delle seguenti proprietá:

1. Per ogni $g_1, g_2 \in G$, $g_1 * g_2 \in G$ (chiusura di G rispetto a $*$).
2. Per ogni $g_1, g_2, g_3 \in G$ $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ (associativitá di $*$).

3. Esiste un elemento $e \in G$ tale che per ogni $g \in G$, $g * e = e * g = g$ (esistenza dell'elemento neutro).

4. per ogni $g \in G$, esiste $h \in G$ tale che $g * h = h * g = e$ (esistenza dell'inverso).

Se $g_1 * g_2 = g_2 * g_1$ per ogni $g_1, g_2 \in G$ allora il gruppo si dice abeliano (o commutativo). L'elemento e é unico ed é detto l'identitá del gruppo, cosí come é unico l'inverso $h = g^{-1}$ di un elemento g.

Un sottogruppo H di un gruppo G é un sottoinsieme di G tale che:

1. L'identitá é un elemento di H,

2. Se $h \in H$ allora $h^{-1} \in H$,

3. Se $h_1, h_2 \in H$ allora $h_1 * h_2 \in H$.

Dati due gruppi G e H, una funzione $\phi : G \to H$ é detta un omomorfismo se $\phi(g_2 * g_1) = \phi(g_1) * \phi(g_2)$, per ogni $g_1, g_2 \in G$. Se ϕ é biunivoca allora é detta isomorfismo.

A.1.1 Esempi di gruppi

L'insieme degli interi $\mathbb{Z}$ e l'insieme dei reali $\mathbb{R}$ formano un gruppo abeliano rispetto all'operazione di addizione. Lo spazio n-dimensionale $\mathbb{R}^n$ forma un gruppo abeliano rispetto all'operazione di somma vettoriale. L'insieme dei numeri reali non nulli $\mathbb{R} \setminus \{0\}$ e l'insieme dei numeri complessi non nulli $\mathbb{C} \setminus \{0\}$ formano un gruppo abeliano rispetto all'operazione di moltiplicazione. Per ogni intero positivo n, l'insieme di tutte le matrici complesse $n \times n$ invertibili forma un gruppo rispetto all'operazione di prodotto tra matrici, detto gruppo generale lineare su $\mathbb{C}$ e denotato da $\mathtt{GL}(n;\mathbb{C})$. Per $n \geq 2$ il gruppo non é commutativo.

A.2 Gruppi di matrici di Lie

Un gruppo di matrici di Lie é un sottogruppo chiuso di $\mathtt{GL}(n;\mathbb{C})$, cioé un qualsiasi sottogruppo H che soddisfa la seguente proprietá: se A_n é una sequenza di matrici in H e A_n converge ad A, allora o $A \in H$ oppure A non é invertibile. Una sequenza di matrici complesse A_n converge ad una matrice A se e solo se $(A_n)_{ij}$ converge ad A_{ij} per ogni $1 \leq i, j \leq n$. Un omomorfismo di gruppo di Lie é un omomorfismo di gruppo che é continuo.

Due importanti esempi di gruppi di matrici di Lie sono il gruppo delle matrici ortogonali speciali $\mathtt{SO}(n)$, e il gruppo delle matrici unitarie speciali

$\mathtt{SU}(n)$. Una matrice $n \times n$ reale é ortogonale se e solo se $A^t = A^{-1}$, dove A^t é la trasposta di A. Equivalentemente, si puó definire A ortogonale se e solo se preserva i prodotti interni, cioé per ogni $x, y \in \mathbb{R}^n$, $(Ax, Ay) = (x, y)$. Le matrici speciali ortogonali sono le matrici ortogonali con determinante 1. Analogamente si definiscono le matrici speciali unitarie come le matrici $n \times n$ complesse unitarie con determinante 1. Geometricamente gli elementi di $\mathtt{SO}(n)$ rappresentano rotazioni nello spazio reale n-dimensionale. In particolare, si puó dimostrare che ogni elemento di $\mathtt{SO}(2)$ é della forma

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

che rappresenta una rotazione di un angolo θ nel piano reale.

A.3 I gruppi $\mathtt{SU}(2)$ e $\mathtt{SO}(3)$

I gruppi di matrici di Lie $\mathtt{SU}(2)$ e $\mathtt{SO}(3)$ sono correlati da una importante corrispondenza che é alla base della nostra interpretazione delle operazioni unitarie su un qubit come rotazioni nella sfera unitaria in $\mathbb{R}^3$ (la sfera di Bloch). Questa corrispondenza é formalizzata da un omomorfismo di gruppo di Lie $\phi : \mathtt{SU}(2) \to \mathtt{SO}(3)$, definito come segue.

Consideriamo lo spazio V di tutte le matrici complesse 2×2 che sono Hermitiane e hanno traccia nulla. Questo é uno spazio vettoriale *reale* a tre dimensioni con base:

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; A_2 = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \text{ e } A_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Se definiamo il prodotto scalare su V come

$$(A, B) = \frac{1}{2} tr(AB),$$

allora $\{A_1, A_2, A_3\}$ forma una base ortonormale per V e possiamo identificare V con $\mathbb{R}^3$. Si verifica facilmente che se $U \in \mathtt{SU}(2)$ e $A \in V$, allora $UAU^{-1} \in \mathtt{SU}(2)$. Quindi la funzione definita da

$$\phi_U(A) = UAU^{-1},$$

é un operatore lineare su V. Poiché, dati $A, B \in V$,

$$(\phi_U(A), \phi_U(B)) = \frac{1}{2} tr(UAU^{-1}UBU^{-1}) = \frac{1}{2} tr(AB) = (A, B),$$

ϕ_U é ortogonale. Si dimostra inoltre che ha determinante 1 e quindi che $\phi_U \in \mathtt{SO}(3)$. Possiamo ora definire la funzione $\phi : \mathtt{SU}(2) \to \mathtt{SO}(3)$ come $\phi(U) = \phi_U$ e verificare che questa definisce un omomorfismo di gruppo di Lie da $\mathtt{SU}(2)$ e $\mathtt{SO}(3)$.

Nota che per ogni $U \in \mathtt{SU}(2)$, $\phi_U = \phi_{-U}$. Pertanto ϕ non é un isomorfismo.