SAPIENZA
UNIVERSITÀ DI ROMA

Completezza Funzionale di Porte Logiche nei Computer Quantistici

Scuola di Scienze Matematiche Fisiche e Naturali
Fisica

Daniele Lanciotti
Matricola 1849379

Relatore
Prof. Domenico Monaco

Anno Accademico 2024/2025

Completezza Funzionale di Porte Logiche nei Computer Quantistici
Sapienza Università di Roma

Questa tesi è stata composta con LaTeX e la classe Sapthesis.

Sito web: https://illancio.github.io

Email dell'autore: daniele9001@gmail.com

Last but not least.
P. C. V.

Introduzione

> «In principio era il Logos» — il verso che apre il Vangelo secondo Giovanni — è uno dei più celebri esempi di quanto la *ragione* sia centrale per la *conoscenza* e per la *scienza* che muovono l'uomo. La ragione non perderà mai il suo potere, perché essa è il mezzo per giungere al *significato* e, per coloro che vorranno ascoltare, all'affermazione della *Verità*.

La natura algoritmica dell'inferenza logica formale prende vita nelle computazioni della Macchina di Turing. È pertanto esplorando tali mezzi della deduzione che si può giungere a una risposta, o alla formulazione della giusta domanda.

I confini attuali della computazione sono illuminati dalla fisica contemporanea: la matematica che sottende la Meccanica Quantistica suggerisce un modello capace di estendere le potenzialità computazionali classiche — la Macchina di Turing Quantistica.

Per almeno alcune classi di problemi, la computazione quantistica si dimostra più efficiente rispetto a quella classica, offrendo vantaggi anche esponenziali nella complessità temporale delle soluzioni. Non si tratta soltanto di un'estensione teorica della Macchina di Turing, ma di un nuovo paradigma computazionale radicato nella struttura matematica della Meccanica Quantistica.

Nel contesto quantistico, i bit, ovvero le entità che codificano informazione, sono sostituiti dai *qubit*. Le *porte logiche quantistiche* agiscono su questi stati come trasformazioni unitarie, rappresentando le operazioni con cui il calcolo quantistico manipola l'informazione.

L'elaborato affronta la questione della *completezza funzionale quantistica*, intesa come possibilità di generare qualunque trasformazione unitaria ammissibile attraverso la composizione di un insieme finito di porte logiche. Si tratta di un'analogia diretta con la nozione classica di *completezza funzionale*, secondo cui un numero minimo di porte, come NAND o NOR, è sufficiente a costruire ogni circuito booleano.

A partire dai postulati della Meccanica Quantistica (Capitolo 2), l'elaborato introduce il formalismo del qubit (Capitolo 3) e definisce le trasformazioni ammissibili (Capitolo 4). Il percorso culmina nella dimostrazione dell'universalità di un insieme finito di porte logiche (Capitolo 5), che risulta completo per l'elaborazione quantistica dell'informazione.

L'elaborato prende ispirazione principalmente dagli argomenti trattati nei Capitoli 1 e 4 di [9], nei quali la dimostrazione della completezza funzionale si sviluppa sulla base dell'approccio introdotto in [2]. Il quadro teorico generale si colloca nella linea aperta da [4], in cui il concetto di calcolatore quantistico universale viene formulato come estensione fisica del modello di Turing.

Indice

Capitolo 1

Preliminari Matematici

La trattazione che segue è ispirata principalmente a [3, Capitolo II, Sezione F], con integrazioni e adattamenti ove necessario.

1.1 Prodotto tensoriale

Definizione 1.1 (Prodotto tensoriale)**.** Siano $\mathcal{H}_1$ e $\mathcal{H}_2$ due spazi di Hilbert[1]. Il prodotto tensoriale di $\mathcal{H}_1$ e $\mathcal{H}_2$, denotato con $\mathcal{H}_1 \otimes \mathcal{H}_2$, è uno spazio di Hilbert contenente tutte le coppie del tipo $|v_1\rangle \otimes |v_2\rangle$, dove $|v_1\rangle \in \mathcal{H}_1$ e $|v_2\rangle \in \mathcal{H}_2$ (detti *vettori decomponibili*)

$$\mathcal{H}_1 \otimes \mathcal{H}_2 := \operatorname{span}\{|v_1\rangle \otimes |v_2\rangle : |v_1\rangle \in \mathcal{H}_1 \wedge |v_2\rangle \in \mathcal{H}_2\}$$

che soddisfa le proprietà seguenti:

1. *linearità* della moltiplicazione per uno scalare:

   $$(\lambda |v_1\rangle) \otimes |v_2\rangle = |v_1\rangle \otimes (\lambda |v_2\rangle) = \lambda(|v_1\rangle \otimes |v_2\rangle)$$

   $\forall \lambda \in \mathbb{C}, \quad \forall |v_1\rangle \in \mathcal{H}_1, \quad \forall |v_2\rangle \in \mathcal{H}_2$

2. *distributività* dell'addizione tra vettori:

   $$|v_1\rangle \otimes (|v_2\rangle + |w_2\rangle) = |v_1\rangle \otimes |v_2\rangle + |v_1\rangle \otimes |w_2\rangle$$

   $$(|v_1\rangle + |w_1\rangle) \otimes |v_2\rangle = |v_1\rangle \otimes |v_2\rangle + |w_1\rangle \otimes |v_2\rangle$$

   $\forall |v_1\rangle, |w_1\rangle \in \mathcal{H}_1, \quad \forall |v_2\rangle, |w_2\rangle \in \mathcal{H}_2$

3. siano $\{|u_{1,i}\rangle\}$ e $\{|u_{2,i}\rangle\}$ due basi rispettivamente di $\mathcal{H}_1$ e $\mathcal{H}_2$. L'insieme $\{|u_{1,i}\rangle \otimes |u_{2,j}\rangle\}$ è una *base* di $\mathcal{H}_1 \otimes \mathcal{H}_2$.

4. il *prodotto scalare* di $\mathcal{H}_1 \otimes \mathcal{H}_2$ è definito a partire dai prodotti scalari di $\mathcal{H}_1$ e $\mathcal{H}_2$ come segue: sui vettori decomponibili si pone

   $$\langle v_1 v_2 | w_1 w_2 \rangle = \langle v_1 | w_1 \rangle \langle v_2 | w_2 \rangle$$

   dove $|v_1 v_2\rangle = |v_1\rangle \otimes |v_2\rangle$, $|w_1 w_2\rangle = |w_1\rangle \otimes |w_2\rangle$. La definizione è poi estesa per sesquilinearità.

[1] In tutta la trattazione, ogni spazio di Hilbert è inteso in campo complesso.

1.1.1 Prodotto tensoriale di operatori

Definizione 1.2 (Prodotto tensoriale di operatori)**.** Siano A_1 e A_2 operatori lineari agenti rispettivamente sugli spazi di Hilbert $\mathcal{H}_1$ e $\mathcal{H}_2$. Il prodotto tensoriale di A_1 e A_2, denotato con $A_1 \otimes A_2$, è un operatore lineare agente su $\mathcal{H}_1 \otimes \mathcal{H}_2$ nel modo seguente: sui vettori decomponibili si pone

$$(A_1 \otimes A_2)(|v_1\rangle \otimes |v_2\rangle) := A_1 |v_1\rangle \otimes A_2 |v_2\rangle$$

$\forall |v_1\rangle \in \mathcal{H}_1$, $\forall |v_2\rangle \in \mathcal{H}_2$. La definizione è poi estesa per linearità.

Proposizione 1.3 (Prodotto misto)**.** *Siano A_1, B_1 operatori lineari sullo spazio di Hilbert $\mathcal{H}_1$ e A_2, B_2 operatori lineari sullo spazio di Hilbert $\mathcal{H}_2$, tali per cui siano ben definiti i prodotti A_1B_1 e A_2B_2. Vale la seguente relazione:*

$$(A_1 \otimes A_2)(B_1 \otimes B_2) = (A_1B_1) \otimes (A_2B_2)$$

Proposizione 1.4. *Siano A_1 e A_2 operatori lineari agenti sugli spazi di Hilbert $\mathcal{H}_1$ e $\mathcal{H}_2$, rispettivamente. Allora:*

$$A_1, A_2 \textit{ autoaggiunti} \implies A_1 \otimes A_2 \textit{ autoaggiunto}$$
$$A_1, A_2 \textit{ unitari} \implies A_1 \otimes A_2 \textit{ unitario}$$

Per una trattazione più completa delle due proposizioni appena enunciate si veda [7], [6, Sezione 2.2] o [11, Sezione 8], tenendo a mente il risultato della proposizione 1.6 enunciata in seguito sul prodotto di Kronecker.

Verrà utilizzata la notazione $A^{\otimes n}$ per indicare il prodotto tensoriale di un operatore, uno spazio di Hilbert o un vettore A per se stesso n volte.

1.1.2 Prodotto di Kronecker

Definizione 1.5 (Prodotto di Kronecker)**.** Siano A una matrice $m \times n$ e B una matrice $p \times q$. Il *prodotto di Kronecker* di A e B è una matrice $mp \times nq$ definita a blocchi come segue:

$$A \otimes_K B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$$

Il prodotto di Kronecker è la rappresentazione matriciale del prodotto tensoriale di operatori lineari quando si scelgono basi fissate negli spazi di Hilbert coinvolti.

Proposizione 1.6. *Siano $\mathcal{H}_1$ e $\mathcal{H}_2$ due spazi di Hilbert finito-dimensionali, di dimensione m e n, $\{|u_{1,i}\rangle\}_{i=1}^m$ una base di $\mathcal{H}_1$, $\{|u_{2,j}\rangle\}_{j=1}^n$ una base di $\mathcal{H}_2$. Allora ogni operatore lineare A_1 su $\mathcal{H}_1$ è rappresentato, rispetto alla base $\{|u_{1,i}\rangle\}$, da una matrice $m \times m$, e ogni operatore A_2 su $\mathcal{H}_2$, rispetto alla base $\{|u_{2,j}\rangle\}$, da una matrice $n \times n$. Il prodotto tensoriale $A_1 \otimes A_2$, è rappresentato, rispetto alla base tensoriale $\{|u_{1,i}\rangle \otimes |u_{2,j}\rangle\}$, dalla matrice di Kronecker $A_1 \otimes_K A_2$.*

Per un esempio dimostrativo dell'enunciato, si rimanda a [5, Capitolo 11, Proposizione 17].

Da questo punto in poi sarà utilizzato il simbolo $\otimes$ per indicare il prodotto di Kronecker o il prodotto tensoriale tra spazi di Hilbert; sarà invece omesso nella rappresentazione dei vettori del prodotto tensoriale per i quali si adotta la seguente notazione:

$$|v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle = |v_1\rangle\,|v_2\rangle \cdots |v_n\rangle = |v_1 v_2 \cdots v_n\rangle$$

Capitolo 2

Postulati della Meccanica Quantistica

Ogni teoria fisica si basa su un insieme minimale di definizioni prime irriducibili, che facciano da ponte tra la loro natura sperimentale (il significato) e le definizioni matematiche (il significante) che ne permettono di enunciare relazioni sotto forma di postulati. Se nel caso della Meccanica Newtoniana queste definizioni prime includono lo *spazio* o il *tempo*, nella Meccanica Quantistica sono protagonisti i concetti di *osservabile* e *misura*.

- **Sistema fisico**: Un sistema quantistico è la coppia $(\mathcal{H}, \hat{H})$ dove $\mathcal{H}$ è uno spazio di Hilbert complesso separabile e $\hat{H}$ un operatore autoaggiunto su $\mathcal{H}$, detto *Hamiltoniana*, corrispondente alla quantità fisica *energia del sistema*.
- **Sistema composto**: Sia $\mathcal{H}$ lo spazio di Hilbert di un sistema fisico composto da n sottosistemi, i cui spazi sono $\mathcal{H}_1, \cdots, \mathcal{H}_n$. Allora:
$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$$
- **Stato del sistema**: Si definisce una relazione di equivalenza $\sim$ su $\mathcal{H} \setminus \{0\}$ ponendo $|\Psi\rangle \sim |\Phi\rangle \Leftrightarrow \exists\, \alpha \in \mathbb{C} \setminus \{0\}$ tale che $|\Psi\rangle = \alpha\, |\Phi\rangle$. Lo *stato fisico* di un sistema quantistico è allora un elemento dello spazio quoziente $\mathcal{H}/\sim$, ovvero un raggio dello spazio di Hilbert $\mathcal{H}$.
- **Osservabile**: Ogni quantità sperimentalmente misurabile (osservabile) è associata ad un operatore autoaggiunto che agisce sullo spazio di Hilbert del sistema quantistico.
- **Misura dell'osservabile**: Una misura dell'osservabile $\hat{A}$ produce come risultato uno degli autovalori λ_i dello spettro di $\hat{A}$.
- **Ipotesi del collasso** (interpretazione di Copenaghen): Dopo aver misurato il valore λ_i per un'osservabile, lo stato del sistema diventa il suo autovettore (anche detto *autostato*) corrispondente $|\lambda_i\rangle$.
- **Probabilità di transizione** (regola di Born): La probabilità di misurare il valore λ_i nello stato $|\Psi\rangle$ è data dalla relazione
$$P = \frac{|\,\langle \lambda_i | \Psi \rangle\,|^2}{\langle \lambda_i | \lambda_i \rangle \, \langle \Psi | \Psi \rangle}$$

- **Evoluzione temporale**: Uno stato $|\Psi\rangle$ dopo un intervallo di tempo t diventa lo stato

$$e^{-i\frac{\hat{H}}{\hbar}t}\,|\Psi\rangle$$

dove $\hbar$ è la *costante di Planck*.

Capitolo 3

Sistema Fisico di un Calcolatore Quantistico

Definizione 3.1 (Qubit)**.** Un *qubit* è un sistema fisico il cui spazio di Hilbert è di dimensione due[1].

Un esempio di qubit è quello di un qualsiasi fermione di *spin* 1/2.

Definizione 3.2 (Computer quantistico)**.** Un *Computer Quantistico* è un sistema fisico di n *qubit* unito ad una sequenza di *porte logiche* (cf. Definizione 4.1) agenti sul suo stato.

Definizione 3.3 (Base computazionale)**.** Sia $\hat{S}$ un'osservabile di singolo qubit e $\{|0\rangle, |1\rangle\}$ una base ortonormale di autovettori di $\hat{S}$. Si dice *base computazionale* di un sistema di n qubit la base, di cardinalità 2^n, dello spazio di Hilbert, isomorfo a $(\mathbb{C}^2)^{\otimes n}$, del sistema:

$$\{|0\cdots00\rangle, |0\cdots01\rangle, |0\cdots10\rangle, \cdots, |1\cdots11\rangle\}$$

In tutta la trattazione si considererà fissata l'osservabile $\hat{S}$ di singolo qubit a cui farà riferimento ogni misura. Ogni stato $|0\rangle$ o $|1\rangle$ sarà relativo alla base computazionale da essa definita, così come ogni rappresentazione matriciale degli operatori lineari. Inoltre con l'espressione "*misurare 0 o 1*" verrà inteso "*misurare l'autovalore corrispondente a* $|0\rangle$ *o a* $|1\rangle$". L'espressione "*misurare l'i-esimo qubit*" starà quindi ad indicare l'operazione di misura, sull'intero sistema, dell'osservabile:

$$I^{\otimes(i-1)} \otimes \hat{S} \otimes I^{\otimes(n-i)}$$

Lo stato $|\Psi\rangle$ di un sistema di n qubit è pertanto definito da una combinazione lineare dei vettori di base:

$$|\Psi\rangle = \alpha_0 |0\cdots00\rangle + \alpha_1 |0\cdots01\rangle + \alpha_2 |0\cdots10\rangle + \cdots + \alpha_{2^n-1} |1\cdots11\rangle$$

dove $\alpha_i \in \mathbb{C}$, $\forall i \in [0, 2^n - 1] \cap \mathbb{N}$.

Esempio 3.4 (Singolo qubit)**.** Lo stato di un singolo qubit è quindi definito da una combinazione lineare dei vettori della base $\{|0\rangle, |1\rangle\}$:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

[1]Lo spazio di Hilbert di un qubit può essere un prodotto tensoriale di spazi in cui almeno uno di essi abbia dimensione 2.

dove $\alpha, \beta \in \mathbb{C}$.

In caso di vettore normalizzato, è semplice verificare che le probabilità che la misura sia 0 piuttosto che 1, quindi le probabilità che lo stato collassi nell'autostato $|0\rangle$ piuttosto che $|1\rangle$, sono date dal modulo quadro dei coefficienti della combinazione lineare $|\alpha|^2$, $|\beta|^2$.

Esempio 3.5 (Due qubit)**.** Lo stato di un sistema di due qubit è invece definito dalla base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$|\Psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

dove $\alpha, \beta, \gamma, \delta \in \mathbb{C}$.

In questo caso, se il vettore è normalizzato, misurare uno dei due qubit, ad esempio il primo, equivale a misurare l'osservabile $\hat{S} \otimes I$, i cui autostati sono:

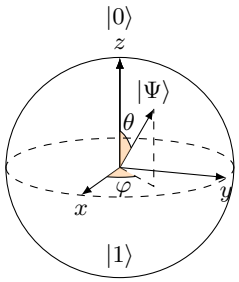
$$|\lambda_0\rangle = \alpha\,|00\rangle + \beta\,|01\rangle, \quad |\lambda_1\rangle = \gamma\,|10\rangle + \delta\,|11\rangle$$

Quindi le probabilità di misurare 0 piuttosto che 1, o le probabilità che lo stato collassi in $|\lambda_0\rangle$ piuttosto che in $|\lambda_1\rangle$, sono:

$$P(0) = |\alpha|^2 + |\beta|^2, \quad P(1) = |\gamma|^2 + |\delta|^2$$

Definizione 3.6 (Sfera di Bloch)**.** Viene detta *sfera di Bloch* la superficie sferica di raggio 1 in coordinate sferiche:

$$\begin{cases} x = \sin\theta\cos\varphi \\ y = \sin\theta\sin\varphi \\ z = \cos\theta \end{cases} \qquad \begin{matrix} 0 \le \theta \le \pi \\ 0 \le \varphi \le 2\pi \end{matrix}$$



della quale ogni punto, quindi ogni coppia di coordinate sferiche (θ, φ), indica univocamente uno stato normalizzato di singolo qubit:

$$|\Psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle$$

Tale cambiamento di variabili in coordinate sferiche è attuabile poiché, come osservato nell'esempio 3.4, lo stato di un singolo qubit è:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \alpha, \beta \in \mathbb{C}$$

Lo stato, se normalizzato, essendo $|\alpha|^2 + |\beta|^2 = 1$, può essere espresso come:

$$|\Psi\rangle = e^{i\gamma}\cos\frac{\theta}{2}\,|0\rangle + e^{i(\gamma+\varphi)}\sin\frac{\theta}{2}\,|1\rangle$$

Dove il fattore $e^{i\gamma}$, non essendo influente sullo stato del sistema, può essere ignorato.

3.1 Entanglement

Definizione 3.7 (Stato entangled)**.** Sia $|\Psi\rangle$ lo stato di un sistema composto da n sottosistemi i cui spazi di Hilbert sono $\mathcal{H}_1, \cdots, \mathcal{H}_n$. Lo stato $|\Psi\rangle$ è detto *entangled* se non è decomponibile, cioè se non può essere espresso come prodotto tensoriale degli stati dei singoli sottosistemi ma solo come combinazione lineare non banale dei vettori di base dello spazio $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ al quale appartiene:

$$|\Psi\rangle \neq |v_1 \cdots v_n\rangle\,, \quad \forall\, |v_i\rangle \in \mathcal{H}_i$$

L'effetto che la misura ha sugli stati entangled è un'ovvia conseguenza dell'ipotesi del collasso e delle proprietà del prodotto tensoriale.

Esempio 3.8 (Due qubit entangled)**.** Sia il sistema di due qubit nello stato entangled:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

Misurando il primo qubit, lo stato collassa in uno dei due autostati equiprobabili $|00\rangle$, $|11\rangle$, quindi la misura del primo qubit determina il risultato di una successiva misura del secondo.

Capitolo 4

Porte Logiche

Definizione 4.1 (Porta logica quantistica)**.** Una *porta logica* a n qubit è un operatore unitario U che opera sullo spazio di Hilbert di un sistema di n qubit.

Risulta ragionevole definire l'applicazione di una o più porte logiche su un sistema con un numero di qubit maggiore di quello in cui operano singolarmente.

Definizione 4.2 (Applicazione simultanea di porte logiche)**.** Siano $U_1, \cdots, U_k$ porte logiche rispettivamente a $n_1, \cdots, n_k$ qubit. La loro *applicazione simultanea* su sottoinsiemi distinti e ordinati di qubit di un sistema di $n \geq n_{\text{tot}} = \sum_{i=1}^{k} n_i$ qubit, è definita dalla seguente porta logica a n qubit:

$$P^{-1} \left[U_1 \otimes \cdots \otimes U_k \otimes I^{\otimes(n-n_{\text{tot}})} \right] P \tag{4.1}$$

dove P è un operatore di permutazione che porta gli n_{tot} qubit target nelle prime n_{tot} posizioni del tensore, lasciando gli altri inalterati.

L'evoluzione temporale, essendo un operatore unitario, è a tutti gli effetti una porta logica, pertanto perturbare il sistema in modo tale da modificare a piacimento la sua Hamiltoniana equivale a scegliere la porta logica che vi agisce.

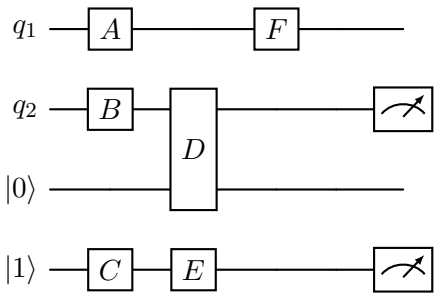
4.1 Circuiti

Un circuito quantistico è una schematizzazione del computer quantistico, quindi dell'applicazione delle porte logiche allo stato dei suoi qubit.

Ogni linea orizzontale rappresenta un qubit, ogni simbolo che vi giace indica la porta logica agente su di essi, fatta eccezione per l'unico simbolo rappresentante la misurazione (figura 4.1). Le porte allineate verticalmente si applicano simultaneamente, pertanto combinandosi come nell'espressione (4.1). Le porte risultanti vanno moltiplicate tra loro da destra a sinistra. A sinistra del circuito possono essere presenti eventuali nomi assegnati ai qubit e vettori che ne rappresentano lo stato iniziale. In particolare, se accanto alla linea corrispondente al qubit in posizione n è indicato un vettore $|\psi\rangle$, lo stato iniziale del sistema è una combinazione lineare dei vettori della base computazionale, in cui il termine associato alla posizione n nel prodotto tensoriale è sostituito da $|\psi\rangle$ anziché dal consueto $|0\rangle$ o $|1\rangle$.

Figura 4.1. Simbolo rappresentante la misurazione di singolo qubit.

Esempio 4.3. Circuito di un computer quantistico con 4 qubit (2 generici e 2 inizializzati) e 6 porte logiche:



La porta logica che agisce sul sistema totale dei qubit risulta quindi essere la seguente:

$$U_{\text{tot}} = (F \otimes I^{\otimes 3})(I \otimes D \otimes E)(A \otimes B \otimes I \otimes C)$$

Utilizzando la proprietà del prodotto tensoriale tra operatori, enunciata nella proposizione 1.3, è possibile riesprimere la porta logica risultante come segue:

$$U_{\text{tot}} = (FA) \otimes (D(B \otimes I)) \otimes (EC)$$

Lo stato iniziale del sistema, in questo caso, corrisponde a ciò che si ottiene misurando gli ultimi due qubit di diversi sistemi generici e selezionando quello in cui le rispettive misure diano risultati 0 e 1. Tale stato è il seguente:

$$\alpha\,|0001\rangle + \beta\,|0101\rangle + \gamma\,|1001\rangle + \delta\,|1101\rangle$$

dove $\alpha, \beta, \gamma, \delta \in \mathbb{C}$.

Ciò significa che la matrice rappresentante la porta logica risultante U_{tot} agisce sul seguente vettore di coordinate:

$$(0, \alpha, 0, 0, 0, \beta, 0, 0, 0, \gamma, 0, 0, 0, \delta, 0, 0)$$

4.2 Porte logiche notevoli

Ogni porta logica quantistica può essere definita con la relativa rappresentazione matriciale o, equivalentemente, specificando l'azione sui vettori della base computazionale, ottenendo quindi una rappresentazione funzionale analoga alla *tavola di verità* dei connettivi logici classici.

Di seguito si riportano le definizioni delle principali porte logiche a singolo qubit.

Hadamard	H	$\begin{array}{c\|c} \lvert\Psi\rangle & H\lvert\Psi\rangle \\ \hline \lvert 0\rangle & \frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle) \\ \lvert 1\rangle & \frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle) \end{array}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli $\boldsymbol{\sigma_1}$	X	$\begin{array}{c\|c} \lvert\Psi\rangle & \sigma_1\lvert\Psi\rangle \\ \hline \lvert 0\rangle & \lvert 1\rangle \\ \lvert 1\rangle & \lvert 0\rangle \end{array}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli $\boldsymbol{\sigma_2}$	Y	$\begin{array}{c\|c} \lvert\Psi\rangle & \sigma_2\lvert\Psi\rangle \\ \hline \lvert 0\rangle & i\lvert 1\rangle \\ \lvert 1\rangle & -i\lvert 0\rangle \end{array}$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli $\boldsymbol{\sigma_3}$	Z	$\begin{array}{c\|c} \lvert\Psi\rangle & \sigma_3\lvert\Psi\rangle \\ \hline \lvert 0\rangle & \lvert 0\rangle \\ \lvert 1\rangle & -\lvert 1\rangle \end{array}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase	S	$\begin{array}{c\|c} \lvert\Psi\rangle & S\lvert\Psi\rangle \\ \hline \lvert 0\rangle & \lvert 0\rangle \\ \lvert 1\rangle & i\lvert 1\rangle \end{array}$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\boldsymbol{\pi/8}$	T	$\begin{array}{c\|c} \lvert\Psi\rangle & T\lvert\Psi\rangle \\ \hline \lvert 0\rangle & \lvert 0\rangle \\ \lvert 1\rangle & e^{i\pi/4}\lvert 1\rangle \end{array}$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Tabella 4.1. Nomi, simboli, tavole di verità e matrici unitarie per porte logiche a singolo qubit.

Definizione 4.4 (Porta logica di rotazione indotta dalle matrici di Pauli)**.** Sia $\hat{n}$ un versore in $\mathbb{R}^3$. La *rotazione* di un angolo θ attorno all'asse di $\hat{n}$ è definita come la porta logica a singolo qubit seguente:

$$R_{\hat{n}}(\theta) := \exp\left(-\frac{i\theta}{2}\hat{n}\cdot\vec{\sigma}\right) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(\hat{n}\cdot\vec{\sigma})$$

dove $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$.

Come mostrato nella tavola di verità in tabella 4.2, la porta σ_1 presenta un comportamento del tutto analogo a quello della porta logica classica NOT, motivo per cui viene comunemente denominata *porta NOT quantistica*. Nel circuito quantistico, essa può essere rappresentata indifferentemente con una delle due notazioni illustrate in figura 4.2.

A	$\neg A$
0	1
1	0

$\|\Psi\rangle$	$\sigma_1 \|\Psi\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

Tabella 4.2. Confronto tra tavole di verità $\neg$ e σ_1.

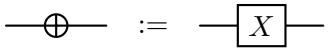
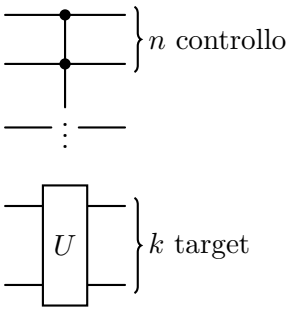


Figura 4.2. Rappresentazione circuitale alternativa di σ_1.

Definizione 4.5 (Operazione controllata)**.** Sia U una porta logica a k qubit. L'*operazione controllata* (o *porta logica controllata*) $C^n(U)$ è una porta logica a $n+k$ qubit definita a blocchi come segue:

$$C^n(U) := \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

dove I è la matrice identità di dimensione $2^{n+k} - 2^k$.



Dei qubit su cui agisce tale porta, i primi n sono detti qubit di *controllo*, i restanti k sono chiamati qubit *target*.

Nella categoria di porte controllate $C^n(U)$ rientrano anche porte i cui qubit di controllo sono preceduti e succeduti da porte σ_1, i quali sono rappresentati graficamente mediante un cerchio vuoto, come in figura 4.3. Tale rappresentazione grafica è ragionevole poiché i qubit di controllo a cerchio pieno definiscono una porta che agisce non banalmente solo sui vettori della base computazionale con $|1\rangle$ nella posizione di quei qubit, mentre quelli a cerchio vuoto definiscono una porta che agisce solo quando i corrispondenti qubit sono inizializzati a $|0\rangle$. Questa inversione della condizione è ottenuta grazie all'inserimento delle porte NOT, che invertono temporaneamente lo stato del qubit durante il controllo (come visto in tabella 4.2).

Quando più porte controllate condividono lo stesso qubit di controllo, è utile adottare una notazione compatta come quella illustrata in figura 4.4.

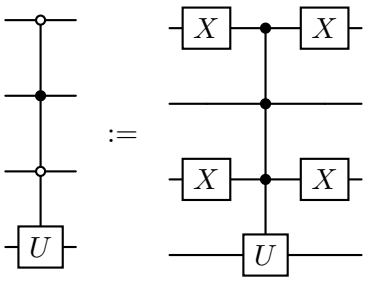


Figura 4.3. Qubit di controllo a cerchio vuoto.

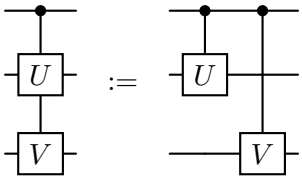
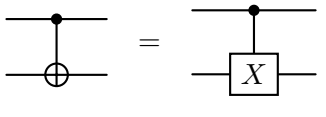


Figura 4.4. Porte logiche controllate con qubit di controllo condiviso.

Tra le porte logiche a più qubit, rivestono particolare importanza le porte *NOT controllate*, tra cui le due fondamentali — la porta *CNOT* e la porta *Toffoli* — sono definite di seguito.

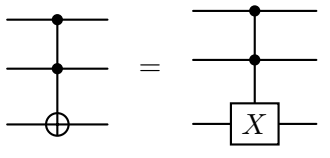
Definizione 4.6 (NOT controllato)**.** La porta *NOT controllato*, anche detta *CNOT*, è la porta logica $C(\sigma_1)$:



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

$\lvert\Psi\rangle$	CNOT$\lvert\Psi\rangle$
$\lvert 00\rangle$	$\lvert 00\rangle$
$\lvert 01\rangle$	$\lvert 01\rangle$
$\lvert 10\rangle$	$\lvert 11\rangle$
$\lvert 11\rangle$	$\lvert 10\rangle$

Definizione 4.7 (Toffoli)**.** La porta *Toffoli*, anche detta *CCNOT* o *TOFF*, è la porta logica $C^2(\sigma_1)$:



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

$\lvert\Psi\rangle$	TOFF$\lvert\Psi\rangle$
$\lvert 000\rangle$	$\lvert 000\rangle$
$\lvert 001\rangle$	$\lvert 001\rangle$
$\lvert 010\rangle$	$\lvert 010\rangle$
$\lvert 011\rangle$	$\lvert 011\rangle$
$\lvert 100\rangle$	$\lvert 100\rangle$
$\lvert 101\rangle$	$\lvert 101\rangle$
$\lvert 110\rangle$	$\lvert 111\rangle$
$\lvert 111\rangle$	$\lvert 110\rangle$

Analogamente al caso della porta NOT, anche la porta Toffoli può essere considerata l'analogo quantistico della porta logica classica *NAND*. Infatti, se il qubit target viene inizializzato nello stato $|1\rangle$ — come nel circuito mostrato in figura 4.5 — e si interpretano i due qubit di controllo come input e il qubit target come output, la tavola di verità risultante (tabella 4.3) coincide con quella della porta NAND classica.

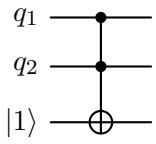


Figura 4.5. Circuito NAND con porta Toffoli a qubit target $|1\rangle$.

$\lvert\Psi\rangle\lvert 1\rangle$	TOFF$\lvert\Psi\rangle\lvert 1\rangle$
$\lvert 001\rangle$	$\lvert 001\rangle$
$\lvert 011\rangle$	$\lvert 011\rangle$
$\lvert 101\rangle$	$\lvert 101\rangle$
$\lvert 111\rangle$	$\lvert 110\rangle$

A	B	A NAND B
0	0	1
0	1	1
1	0	1
1	1	0

Tabella 4.3. Confronto tra tavole di verità Toffoli e NAND.

La porta NAND classica è *funzionalmente completa* (o *universale*), ovvero consente di costruire qualsiasi altra funzione logica booleana (come AND, OR, NOT) utilizzando esclusivamente combinazioni di porte NAND. Una dimostrazione di questo risultato si trova in [10, Sezione 8.1] ed in [8, Sezione 1.3].

Poiché un computer quantistico è in grado di replicare il comportamento della porta NAND tramite la porta Toffoli, esso può simulare qualsiasi circuito logico classico e quindi emulare una macchina di Turing. Per una trattazione completa del modello di macchina di Turing si rimanda a [12]. Ne consegue che il modello computazionale quantistico è *Turing completo*.

Capitolo 5

Porte Logiche Universali

Per gli argomenti trattati in questo capitolo, si segue la presentazione fornita in [9, Capitolo 4].

Analogamente al caso classico, anche nell'ambito della computazione quantistica ci si interroga sull'esistenza di un insieme finito di porte logiche quantistiche che possieda la proprietà di completezza funzionale, ovvero tale che ogni operatore unitario (e quindi ogni porta logica quantistica) possa essere realizzato come combinazione circuitale delle porte contenute nell'insieme. Tuttavia, ciò non è possibile in senso stretto: gli operatori che agiscono su uno spazio di Hilbert a dimensione finita ma su campo complesso formano un insieme non numerabile, mentre le combinazioni finite di elementi di un insieme finito sono numerabili. Ne consegue che non esiste un insieme finito di porte logiche quantistiche in grado di generare esattamente tutti gli operatori unitari possibili.

La questione viene quindi riformulata in termini più pratici e teoricamente rilevanti: ci si chiede se esista un insieme finito di porte logiche quantistiche tale che ogni operatore unitario possa essere approssimato con accuratezza arbitraria come combinazione circuitale delle porte che esso contiene. Tale nozione prende il nome di **completezza funzionale** (o **universalità**) **quantistica**.

In questo capitolo si dimostra che l'insieme {Hadamard, $\pi/8$, NOT controllato} è funzionalmente completo.

Per chiarezza espositiva, può essere utile fare riferimento allo schema concettuale riportato in figura 5.1, che illustra in maniera sintetica i principali passaggi costruttivi attraverso cui è possibile ottenere qualsiasi operatore unitario U, a partire dal set universale appena citato.

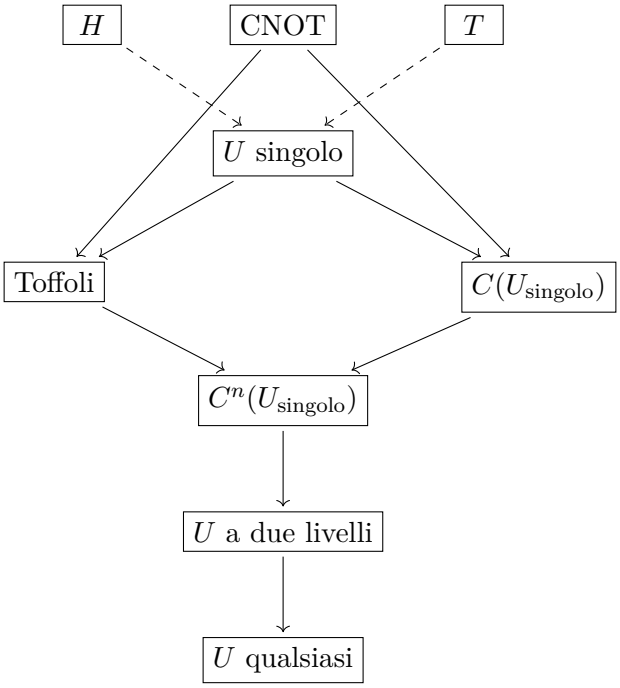


Figura 5.1. Schema concettuale di costruzione di qualsiasi porta logica U utilizzando porte Hadamard, $\pi/8$ e NOT controllato. Ogni riquadro rappresenta una porta logica. Le freccie tratteggiate indicano una costruzione approssimata a differenza delle altre.

I seguenti risultati sulle porte logiche di rotazione saranno utili in seguito. Per le dimostrazioni, si rimanda a [9, Teorema 4.1].

Lemma 5.1 (di decomposizione per porte logiche a singolo qubit)**.** *Per ogni U porta logica a singolo qubit, esistono $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ tali che:*

$$U = e^{i\alpha} R_{\hat{z}}(\beta) R_{\hat{y}}(\gamma) R_{\hat{z}}(\delta)$$

Corollario 5.2. *Siano $\hat{n}$ e $\hat{m}$ versori in $\mathbb{R}^3$ non paralleli. Per ogni U porta logica a singolo qubit, esistono $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ tali che:*

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta)$$

Corollario 5.3. *Per ogni U porta logica a singolo qubit, esistono A, B, C porte logiche a singolo qubit tali che:*

$$ABC = I \quad \wedge \quad U = e^{i\alpha} A\sigma_1 B\sigma_1 C$$

dove $\alpha \in \mathbb{R}$.

5.1 Approssimazione di porte logiche

Definizione 5.4 (Approssimazione di porte logiche)**.** Un insieme A di porte logiche si dice *approssimabile* da un insieme B di porte logiche se $\forall \varepsilon \in \mathbb{R}_{>0}$ e $\forall U \in A$ a n qubit $\exists V$ circuito quantistico di sole porte logiche di B tale che:

$$E(U, V) := \sup_{|\lambda\rangle} \sup_{|\Psi\rangle} |P_U(\lambda, \Psi) - P_V(\lambda, \Psi)| < \varepsilon$$

dove $|\Psi\rangle$ è uno stato di un sistema di n qubit[1] e $|\lambda\rangle$ un autostato appartenente alla base computazionale, il cui autovalore corrispondente λ, negli stati $U|\Psi\rangle$ e $V|\Psi\rangle$, ha probabilità di essere misurato[2] rispettivamente $P_U(\lambda, \Psi)$ e $P_V(\lambda, \Psi)$.

Definizione 5.5 (Completezza funzionale quantistica)**.** Un insieme C di porte logiche quantistiche si dice *funzionalmente completo* se l'insieme di tutte le porte logiche è approssimabile da C.

Definizione 5.6 (Norma operatoriale)**.** Sia A un'operatore lineare che opera sullo spazio di Hilbert $\mathcal{H}$. La *norma* di A è:

$$\|A\|_{\text{op}} := \sup_{|\Psi\rangle} \|A|\Psi\rangle\|$$

dove $|\Psi\rangle \in \mathcal{H}$ è normalizzato.

Definizione 5.7 (Distanza tra operatori)**.** Siano A e B operatori lineari su uno spazio di Hilbert $\mathcal{H}$. La *distanza* tra A e B è la distanza indotta dalla norma operatoriale:

$$d(A, B) := \|A - B\|_{\text{op}}$$

Lemma 5.8. *Siano U e V porte logiche a n qubit. Allora:*

$$E(U, V) \leq 2d(U, V) \tag{5.1}$$

e inoltre, se $U = U_m U_{m-1} \cdots U_1$ e $V = V_m V_{m-1} \cdots V_1$ sono sequenze di m porte logiche a n qubit:

$$d(U, V) \leq \sum_{i=1}^{m} d(U_i, V_i) \tag{5.2}$$

Dimostrazione. Siano P_U e P_V le probabilità introdotte nella definizione 5.4 e $|\lambda\rangle$ e $|\Psi\rangle$ gli stati normalizzati tali che $E(U, V) = |P_U(\lambda, \Psi) - P_V(\lambda, \Psi)|$. Secondo il postulato della regola di Born, tali probabilità sono esprimibili come:

$$\begin{aligned} P_U - P_V &= |\langle\lambda|U|\Psi\rangle|^2 - |\langle\lambda|V|\Psi\rangle|^2 \\ &= \langle\Psi|U^\dagger|\lambda\rangle\langle\lambda|U|\Psi\rangle - \langle\Psi|V^\dagger|\lambda\rangle\langle\lambda|V|\Psi\rangle \end{aligned}$$

Aggiungendo e sottraendo lo stesso termine $\langle\Psi|U^\dagger|\lambda\rangle\langle\lambda|V|\Psi\rangle$ e fattorizzando, si ottiene:

$$\begin{aligned} P_U - P_V &= \langle\Psi|U^\dagger|\lambda\rangle(\langle\lambda|U|\Psi\rangle - \langle\lambda|V|\Psi\rangle) + (\langle\Psi|U^\dagger|\lambda\rangle - \langle\Psi|V^\dagger|\lambda\rangle)\langle\lambda|V|\Psi\rangle \\ &= \langle\Psi|U^\dagger|\lambda\rangle\langle\lambda|U - V|\Psi\rangle + \langle\Psi|(U - V)^\dagger|\lambda\rangle\langle\lambda|V|\Psi\rangle \end{aligned}$$

Applicando prima la disuguaglianza triangolare e dopo la disuguaglianza di Cauchy-Schwarz e poiché i fattori $|\langle\Psi|U^\dagger|\lambda\rangle|$ e $|\langle\lambda|V|\Psi\rangle|$ sono entrambi minori o uguali ad 1, si ha:

$$\begin{aligned} |P_U - P_V| &\leq |\langle\Psi|U^\dagger|\lambda\rangle\langle\lambda|U - V|\Psi\rangle| + |\langle\Psi|(U - V)^\dagger|\lambda\rangle\langle\lambda|V|\Psi\rangle| \\ &\leq \|(U - V)|\Psi\rangle\| + \|(U - V)|\Psi\rangle\| \\ &\leq 2d(U, V) \end{aligned}$$

[1] Nel caso in cui il circuito V sia ad un numero di qubit $m > n$, la sua applicazione allo stato $|\Psi\rangle$ è intesa come l'applicazione di V su uno stato esteso ad uno sistema di m qubit, e che il confronto tra P_U e P_V avviene considerando le probabilità di misura sui soli n qubit logici, trascurando quelli ausiliari.

[2] La misura coinvolge tutti i qubit, in quanto si considera l'osservabile globale $\hat{S}^{\otimes n}$, il cui insieme di autostati ortonormali corrisponde alla base computazionale.

L'espressione (5.1) è così dimostrata.

Siano ora $U = U_2U_1$ e $V = V_2V_1$ sequenze di 2 porte logiche a n qubit. Per almeno uno stato $|\Psi\rangle$ si ha:

$$d(U_2U_1, V_2V_1) = \|(U_2U_1 - V_2V_1)\,|\Psi\rangle\,\|$$

Aggiungendo e sottraendo lo stesso termine $V_2U_1\,|\Psi\rangle$ e fattorizzando si ottiene:

$$d(U_2U_1, V_2V_1) = \|(U_2U_1 - V_2U_1)\,|\Psi\rangle + (V_2U_1 - V_2V_1)\,|\Psi\rangle\,\|$$

Applicando la disuguaglianza triangolare e la definizione di distanza tra porte logiche, poiché le norme sono invarianti sotto operatori unitari, si ha:

$$\begin{aligned} d(U_2U_1, V_2V_1) &\leq \|(U_2 - V_2)U_1\,|\Psi\rangle\,\| + \|V_2(U_1 - V_1)\,|\Psi\rangle\,\| \\ &\leq d(U_2, V_2) + d(U_1, V_1) \end{aligned}$$

La dimostrazione dell'espressione (5.2), per sequenze di un generico numero m di porte logiche a n qubit, segue per induzione. □

Teorema 5.9. *Tutte le porte logiche a singolo qubit sono approssimabili dalle porte Hadamard e $\pi/8$.*

Dimostrazione. Si consideri che:

$$T \cdot HTH = R_{\hat{z}}(\pi/4) \cdot R_{\hat{x}}(\pi/4)$$

Ciò è evidente essendo $T = R_{\hat{z}}(\pi/4)$ e, poiché $H\sigma_3H = \sigma_1$:

$$HTH = HR_{\hat{z}}(\pi/4)H = He^{-\frac{i\pi}{8}\sigma_3}H = e^{-\frac{i\pi}{8}H\sigma_3H} = R_{\hat{x}}(\pi/4)$$

Poiché $\sigma_3\sigma_1 = i\sigma_2$, segue che:

$$\begin{aligned} T \cdot HTH &= \cos^2\left(\frac{\pi}{8}\right) I - i\sin\left(\frac{\pi}{8}\right)\left[\cos\left(\frac{\pi}{8}\right)\sigma_1 + \sin\left(\frac{\pi}{8}\right)\sigma_2 + \cos\left(\frac{\pi}{8}\right)\sigma_3\right] \\ &= \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(\hat{n}\cdot\vec{\sigma}) = R_{\hat{n}}(\theta) \end{aligned}$$

dove il versore $\hat{n}$ e l'angolo θ sono definiti come segue:

$$\vec{n} := \left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right) \implies \hat{n} = \frac{\vec{n}}{\|\vec{n}\|} = \frac{\vec{n}}{\sqrt{1 + \cos^2\left(\frac{\pi}{8}\right)}}$$

$$\begin{aligned} \cos\left(\frac{\theta}{2}\right) := \cos^2\left(\frac{\pi}{8}\right) \implies \sin\left(\frac{\theta}{2}\right) &= \sqrt{1 - \cos^2\left(\frac{\theta}{2}\right)} = \sqrt{1 - \cos^4\left(\frac{\pi}{8}\right)} \\ &= \sin\left(\frac{\pi}{8}\right)\sqrt{1 + \cos^2\left(\frac{\pi}{8}\right)} \end{aligned}$$

L'angolo θ così definito è un multiplo irrazionale di 2π, ovvero tale che:

$$\frac{\theta}{2\pi} \in \mathbb{R}/\mathbb{Q}$$

Per la dimostrazione, si rimanda a [2].

Da ciò e dal *teorema del ritorno di Poincaré*, per il quale si rimanda a [1, Capitolo 3], consegue che l'immagine $\{a_n\}_{n\in\mathbb{N}}$ della successione $a_n = (n\theta) \bmod 2\pi$ è un insieme *denso* in $\mathbb{R}$, ovvero:

$$\forall \alpha \in \mathbb{R}\, \forall \delta \in \mathbb{R}_{>0}\, \exists n \in \mathbb{N} : \quad |n\theta - \alpha| \bmod 2\pi < \delta$$

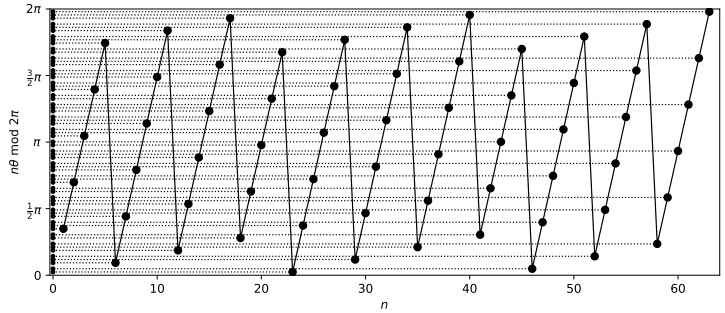


Figura 5.2. Successione $a_n = (n\theta) \bmod 2\pi$ con θ tale che $\cos(\theta/2) = \cos^2(\pi/8)$.

Fissato ora un versore $\hat{m} \in \mathbb{R}^3$, si ha per ogni $\alpha, \beta \in \mathbb{R}$ quanto segue:

$$R_{\hat{m}}(\alpha) - R_{\hat{m}}(\alpha+\beta) = e^{-\frac{i}{2}\alpha\hat{m}\cdot\vec{\sigma}} - e^{-\frac{i}{2}(\alpha+\beta)\hat{m}\cdot\vec{\sigma}} = R_{\hat{m}}(\alpha)\left[I - R_{\hat{m}}(\beta)\right]$$

Essendo le rotazioni operatori unitari, $R_{\hat{m}}(\alpha)$ conserva la norma, pertanto:

$$\| \left[R_{\hat{m}}(\alpha) - R_{\hat{m}}(\alpha+\beta)\right] |\Psi\rangle \| = \left\| \left(I - e^{-\frac{i}{2}\beta\hat{m}\cdot\vec{\sigma}}\right) |\Psi\rangle \right\|$$

Poiché $(\hat{m}\cdot\vec{\sigma})^2 = I$, gli autovalori di $\hat{m}\cdot\vec{\sigma}$ sono ± 1, dunque lo spettro di $I - e^{-\frac{i}{2}\beta\hat{m}\cdot\vec{\sigma}}$ è $\{1 - e^{\pm\frac{i}{2}\beta}\}$. Ne consegue che

$$\begin{aligned} d(R_{\hat{m}}(\alpha), R_{\hat{m}}(\alpha+\beta)) &= \sup_{\|\Psi\|=1} \|(R_{\hat{m}}(\alpha) - R_{\hat{m}}(\alpha+\beta))\,|\Psi\rangle\| \\ &= \max(|1 - e^{-\frac{i}{2}\beta}|, |1 - e^{\frac{i}{2}\beta}|) = |1 - e^{\frac{i}{2}\beta}| \end{aligned}$$

Considerando che $R^n_{\hat{m}}(\theta) = R_{\hat{m}}(n\theta)\ \forall n \in \mathbb{N}$, dalla continuità della funzione $\beta \mapsto |1 - e^{\frac{i}{2}\beta}|$ segue per definizione che:

$$\forall \alpha \in \mathbb{R}\, \forall \varepsilon \in \mathbb{R}_{>0}\, \exists \delta \in \mathbb{R}_{>0} :$$

$$|n\theta - \alpha| \bmod 2\pi < \delta \implies d(R_{\hat{m}}(\alpha), R^n_{\hat{m}}(\theta)) < \varepsilon$$

Unendo questo risultato a quello di densità si ottiene:

$$\forall \alpha \in \mathbb{R}\, \forall \varepsilon \in \mathbb{R}_{>0}\, \exists n \in \mathbb{N} : \quad d(R_{\hat{m}}(\alpha), R^n_{\hat{m}}(\theta)) < \varepsilon$$

Ricordando le relazioni $H\sigma_1 H = \sigma_3$, $H\sigma_2 H = -\sigma_2$, $H\sigma_3 H = \sigma_1$, è semplice dedurre che:

$$H R_{\hat{n}}(\alpha) H = R_{\hat{m}}(\alpha)$$

dove, se $\hat{n} = (n_x, n_y, n_z)$, allora $\hat{m} = (n_x, -n_y, n_z)$. In particolare $\hat{n}$ e $\hat{m}$ non sono paralleli perché $n_y = \frac{\sin(\pi/8)}{\sqrt{1+\cos^2(\pi/8)}} \neq 0$.

Siano U una qualsiasi porta logica a singolo qubit, esprimibile come segue secondo il corollario 5.2, e V la seguente porta logica composta da sole porte Hadamard e $\pi/8$:

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta), \quad V = R_{\hat{n}}^{n_1}(\theta) H R_{\hat{n}}^{n_2}(\theta) H R_{\hat{n}}^{n_3}(\theta)$$
$$= (THTH)^{n_1} H (THTH)^{n_2} H (THTH)^{n_3}$$

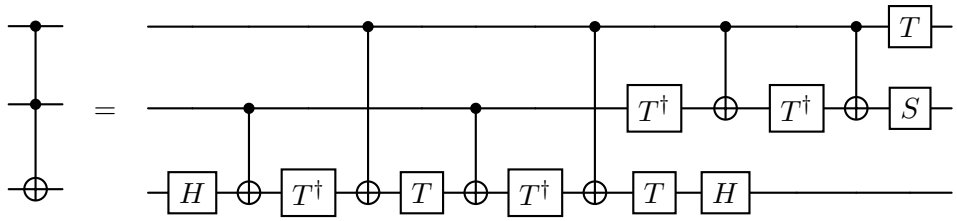
Utilizzando la disequazione (5.2) del teorema 5.8 e considerando che, stando alla definizione 5.4, $E(U,V) = E(U/e^{i\alpha}, V)$, segue l'approssimabilità da dimostrare.

$$\forall U_{\text{singolo}}\, \forall \varepsilon \in \mathbb{R}_{>0}\, \exists n_1, n_2, n_3 \in \mathbb{N} : \quad E(U,V) \leq 2d(U/e^{i\alpha}, V) < \varepsilon$$

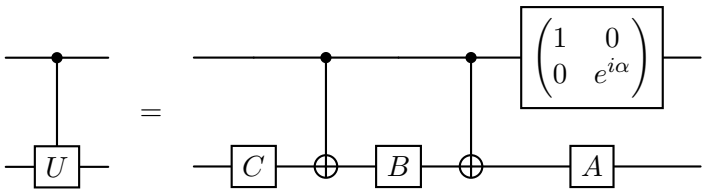
□

5.2 Costruzione di porte controllate

La porta Toffoli è realizzabile con una composizione di sole porte a singolo qubit e porte CNOT. La dimostrazione per costruzione è data dal seguente circuito.



Sia U una porta a singolo qubit. L'operazione controllata $C(U)$ è realizzabile con una composizione di sole porte a singolo qubit e porte CNOT. Infatti, come assicura il corollario 5.3, esistono $\alpha \in \mathbb{R}$ e A, B, C porte logiche a singolo qubit tali che $U = e^{i\alpha} A\sigma_1 B\sigma_1 C$, che permettono la costruzione del seguente circuito equivalente alla porta controllata $C(U)$.

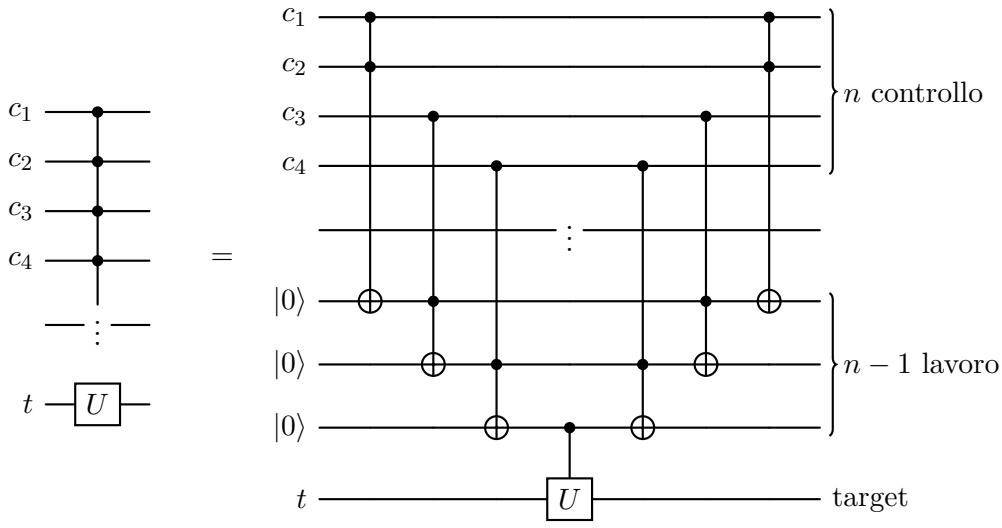


L'uguaglianza è evidente calcolando esplicitamente l'operatore matriciale rappresenta-

to dal circuito:

$$\left[\begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix}\otimes A\right]\cdot \mathrm{CNOT}\cdot(I\otimes B)\cdot\mathrm{CNOT}\cdot(I\otimes C)$$
$$=\begin{pmatrix}A & 0\\ 0 & e^{i\alpha}A\end{pmatrix}\begin{pmatrix}B & 0\\ 0 & \sigma_1 B\end{pmatrix}\begin{pmatrix}C & 0\\ 0 & \sigma_1 C\end{pmatrix}$$
$$=\begin{pmatrix}ABC & 0\\ 0 & e^{i\alpha}A\sigma_1 B\sigma_1 C\end{pmatrix}=\begin{pmatrix}I & 0\\ 0 & U\end{pmatrix}=C(U)$$

Sia U una porta a singolo qubit. L'operazione controllata $C^n(U)$ è realizzabile, come mostrato dal circuito seguente, con una composizione di sole porte Toffoli e della porta $C(U)$, sfruttando $n-1$ qubit ausiliari inizializzati a $|0\rangle$, detti *qubit di lavoro* o (*qubit ancilla*). L'equivalenza è evidente se si considerano le tavole di verità di queste porte e quindi di come ogni porta che compone il circuito trasformi sequenzialmente gli stati della base computazionale.



5.3 Porte logiche a due livelli

Definizione 5.10 (Operatore a due livelli)**.** Sia A un operatore agente sullo spazio di Hilbert a dimensione finita $\mathcal{H}$. L'operatore A si dice *a due livelli* se esiste un sottospazio $\mathcal{V}\subseteq\mathcal{H}$ al più a 2 dimensioni tale che:

$$\forall\,|\Psi\rangle\in\mathcal{V}^{\perp},\quad A\,|\Psi\rangle=|\Psi\rangle$$

dove $\mathcal{V}^{\perp}$ è il sottospazio di $\mathcal{H}$ ortogonale a $\mathcal{V}$.

Teorema 5.11. *Per ogni U porta logica a n qubit a due livelli, esiste un circuito equivalente ad U composto da sole porte $C^{n-1}(\sigma_1)$ e una porta $C^{n-1}(\tilde{U})$, dove $\tilde{U}$ è la porta logica a singolo qubit che definisce l'azione di U nel sottospazio bidimensionale su cui U agisce non banalmente.*

Dimostrazione. Sia $|\Psi\rangle$ un generico stato di n qubit.

$$|\Psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle = \alpha_0 |0\cdots00\rangle + \alpha_1 |0\cdots01\rangle + \cdots + \alpha_{2^n-1} |1\cdots11\rangle$$

dove $\alpha_k \in \mathbb{C}$ e $|k\rangle$ sono gli elementi della base computazionale, quindi k indica il codice binario associato secondo la nomenclatura utilizzata.

La porta logica a due livelli U opera non banalmente sui soli vettori di un sottospazio $\mathcal{V}$ generato da al massimo due vettori di base $|i\rangle$ e $|j\rangle$.

$$\mathcal{V} = \text{span}\{|i\rangle, |j\rangle\}, \quad U|\Psi\rangle = \beta_i |i\rangle + \beta_j |j\rangle + \sum_{k\neq i,j} \alpha_k |k\rangle$$

dove $\beta_i, \beta_j \in \mathbb{C}$ e definiscono la porta a singolo qubit $\tilde{U}$ come:

$$\tilde{U} \begin{pmatrix} \alpha_i \\ \alpha_j \end{pmatrix} = \begin{pmatrix} \beta_i \\ \beta_j \end{pmatrix}$$

Definizione 5.12 (Codice Gray)**.** Siano i e j due codici binari diversi ed entrambi ad n cifre. Un *codice Gray* da i a j è una sequenza finita di codici binari ad n cifre dove il primo è i, l'ultimo è j e i codici adiacenti differiscono per esattamente una cifra.

L'implementazione di U avviene tramite l'utilizzo dei *codici Gray* appena definiti ed è suddivisa nei tre seguenti punti:

1. Applicazione sequenziale di m porte controllate $C_1 = C_1^n(\sigma_1), \cdots, C_m = C_m^n(\sigma_1)$, in modo da implementare un circuito che trasformi soltanto il vettore di base $|i\rangle$ in $|g_m\rangle$, dove g_m è il penultimo elemento del codice Gray da i a j:

   $$i, g_1, g_2, \cdots, g_m, j \qquad C_m \cdots C_1 |i\rangle = C_m \cdots C_2 |g_1\rangle = \cdots = |g_m\rangle$$

   con $m \in [0, n-1] \cap \mathbb{N}$.

2. Applicazione di una porta controllata $C^{n-1}(\tilde{U})$, con qubit target nella posizione dell'unica cifra diversa tra gli ultimi due elementi del codice Gray, e con qubit di controllo che limitino la trasformazione ai soli vettori di base rappresentati dal codice le cui restanti cifre siano del valore di quelle dell'ultimo codice j.

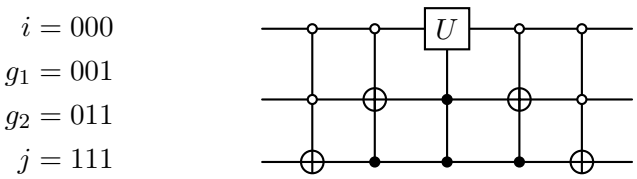
3. Applicazione in ordine inverso delle porte $C_1, \cdots, C_m$ utilizzate al primo punto.

□

Esempio 5.13. Sia U la seguente porta logica a due livelli e $\tilde{U}$ la relativa porta logica a singolo qubit che definisce l'azione di U nel sottospazio bidimensionale su cui U agisce non banalmente.

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \qquad \tilde{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

In questo caso i vettori di base su cui U agisce non banalmente sono $|i\rangle = |000\rangle$ e $|j\rangle = |111\rangle$, di cui un codice Gray e, di conseguenza, un circuito che implementa U sono:



Teorema 5.14. *Per ogni U operatore unitario che opera su uno spazio di Hilbert $\mathcal{H}$ di dimensione n, esistono n operatori su $\mathcal{H}$ unitari a due livelli $U_1, \cdots, U_n$ tali che:*

$$U = U_1 \cdots U_n$$

Dimostrazione. La seguente è una dimostrazione per costruzione del caso di operatori rappresentati da matrici in $\mathbb{C}^{3\times 3}$, generalizzabile al caso di operatori agenti su spazi di Hilbert n-dimensionali. Abbia quindi U la seguente rappresentazione matriciale:

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

Siano definite di conseguenza le matrici U_1, U_2, U_3 come segue[3]:

$$U_1 = \begin{cases} I & \text{se } b = 0 \\ \begin{pmatrix} a^* & b^* & g \\ b & -a & h \\ c & f & \lambda \end{pmatrix} \cdot \dfrac{1}{\lambda} & \text{se } b \neq 0 \end{cases} \quad \Longrightarrow \quad U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix}$$

$$U_2 = \begin{cases} \begin{pmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \text{se } c' = 0 \\ \begin{pmatrix} a'^* & 0 & c'^* \\ 0 & \lambda' & 0 \\ c' & 0 & -a' \end{pmatrix} \cdot \dfrac{1}{\lambda'} & \text{se } c' \neq 0 \end{cases} \quad \Longrightarrow \quad U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}$$

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix}$$

dove gli apici definiscono le componenti delle matrici risultanti e

$$\lambda = \sqrt{|a|^2 + |b|^2}, \quad \lambda' = \sqrt{|a'|^2 + |b'|^2}$$

Moltiplicando tra loro le matrici così definite ed essendo la trasposta coniugata di una matrice unitaria a due livelli ancora una matrice unitaria a due livelli, per definizione di operatore unitario, si ottiene la tesi.

$$U_3 U_2 U_1 U = I \implies U = U_1^{-1} U_2^{-1} U_3^{-1} = U_1^\dagger U_2^\dagger U_3^\dagger$$

□

[3]Si denota con a^* il complesso coniugato di $a \in \mathbb{C}$.

Bibliografia

[1] V.I. Arnold. *Mathematical methods of classical mechanics*, volume 60. Springer, 1989.

[2] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999.

[3] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum Mechanics, Volume 1: Basic Concepts, Tools, and Applications*. Wiley, 2019.

[4] David Deutsch and Roger Penrose. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[5] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3 edition, 2004.

[6] Amy N. Langville and William J. Stewart. The Kronecker product and stochastic automata networks. *Journal of Computational and Applied Mathematics*, 167(2):429–447, 2004.

[7] Shuangzhe Liu, Götz Trenkler, Tõnu Kollo, Dietrich von Rosen, and Oskar Maria Baksalary. Professor Heinz Neudecker and matrix differential calculus. *Statistical Papers*, 65(4):2605–2639, 2024.

[8] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman and Hall/CRC, 6th edition, 2015.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Cambridge, 2010.

[10] A. Nigro. *Segnali e Sistemi: Elettronica per Studenti Di Fisica*. Independently Published, 2018.

[11] D.S.G. Pollock. On kronecker products, tensor products and matrix differential calculus. *International Journal of Computer Mathematics*, 90(11):2462–2476, 2013.

[12] Michael Sipser. *Introduction to the Theory of Computation*. Course Technology, Boston, MA, third edition, 2013.

Ringraziamenti

Desidero ringraziare il professor Domenico Monaco, per la disponibilità, l'attenzione e la guida durante la stesura di questa tesi.

Il mio grazie più grande va a Mamma, Babbo e mia Sorella per essere stati pazienti e amorevoli.

Grazie alla mia stupenda ragazza Mihaela per essermi rimasta vicina in ogni momento (ancora mi chiedo come abbia fatto).

Un pensiero speciale va anche a mia nonna, zio Luigi, zia Gabriella e al resto della mia famiglia, per l'affetto silenzioso e costante che non mi è mai mancato.

Sono convinto del fatto che lo scopo primario dell'università non sia la mera acquisizione di conoscenze ma la possibilità di condividerle con le persone giuste, alimentando un ambiente prospero e vitale, che ho sempre sognato e che sono felice di aver vissuto. La prova sperimentale di ciò è l'effetto della chiusura del balcone di Fisica sul mio rendimento universitario. Pertanto ringrazio tutti i miei amici e colleghi universitari: Youyou Lin (spero non stia dormendo), Paolo Mangini (a cui devo una laurea), Lorenzo Gregoris (anche per la futura ospitalità in Olanda), Jacopo Masia, Giulio Ricci e Enrico Massara (ovunque sei spero ti ripigli). Spero continueremo a condividere momenti pieni, com'erano pieni davanti ai caffé rubati dai dipartimenti altrui.

Last but not least, sono profondamente grato ad Andrea Di Salvatore e Marco Maloni per essere miei grandi amici e compagni di vita.

Grazie a tutti, anche ai diversi fuoriclasse che non ho citato.