Scuola di
Scienze Matematiche
Fisiche e Naturali
Corso di Laurea Triennale Fisica e Astrofisica

Relatore:
Prof.ssa Paola Verrucchi
verrucchi@fi.infn.it

Candidato:
Laura Gentini

Trasformare secondo Fourier in Computazione Quantistica

Nel 1847 George Boole pubblica *The Mathematical Analysis of Logic*, formalizzando l'algebra di Boole, in cui le variabili possono assumere solo i valori "vero" e "falso". Quasi un secolo dopo, con la nascita dell'elettronica digitale, l'algebra di Boole diviene fondamento della computazione classica. La storia della computazione classica affonda quindi le radici nella matematica e nella logica, e si è sviluppata poi, con l'avanzamento tecnologico scaturito dall'invenzione dei transistor (1925), nella realizzazione di dispositivi fisici capaci di portare a termine i più vari algoritmi. La storia della computazione quantistica non differisce da questa solo perchè più recente, ma anche per il diverso ordine cronologico con cui fisica, logica e computazione sono emerse. Agli inizi del 1900, attorno ai molti problemi concettuali emergenti dall'analisi di nuovi fenomeni fisici, è nata la logica quantistica, come strumento a supporto della nuova teoria della Meccanica Quantistica (MQ). Si dovrà poi aspettare mezzo secolo affinchè la logica quantistica sia utilizzata come fondamento di una nuova computazione, che solo in tempi recenti sta trovando le sue prime realizzazioni fisiche in veri e propri dispositivi di calcolo.

Essendo nata in diretta relazione con la descrizione della realtà fisica, la computazione quantistica non può prescindere da essa nelle sue definizioni fondamentali: per questo motivo nel primo capitolo di questa tesi, verranno presentati gli elementi principali della computazione quantistica, sottolineando come la loro definizione discenda dai postulati della MQ, e dalle proprietà dei sistemi quantistici, in particolare l'entanglement. Quest'ultimo è una caratteristica peculiare dei sistemi quantistici, di importanza comparabile con altre quantità fisiche, come l'energia, le funzioni di correlazione o l'entropia, ed ha un ruolo chiave in molte applicazioni in computazione e teoria dell'informazione quantistica. Nel secondo capitol tratteremo un importante risultato ottenuto in computazione quantistica: l'algoritmo quantistico per la trasformata di Fourier. Al di là dell'importanza teorica di poter dimostrare l'esistenza di algoritmi quantistici, la trasformata di Fourier è uno degli strumenti formali più utilizzati per la risoluzione dei problemi fisici, e il circuito quantistico che la realizza ha alcune proprietà rilevanti, una fra tutte quella di realizzare il cosiddetto parallelismo quantistico, diretta conseguenza dell'entanglement. Il parallelismo è la caratteristica responsabile dell'efficienza di un dispositivo quantistico nell'eseguire la trasformata di Fourier, efficienza che è molto superiore rispetto a qualsiasi dispositivo classico. La correlazione fra sfruttamento del parallelismo in un algoritmo e maggior efficienza dello stesso non è però una peculiarità della trasformata di Fourier quantistica. Si può mostrare infatti che qualunque algoritmo quantistico che contiene porte entangling e sfrutta il parallelismo, porta a termine il suo compito in un tempo che scala in modo polinomiale col numero di qubit in ingresso, anche quando il corrispondente algoritmo classico scala esponenzialmente con il numero di bit in ingresso.

Proprio grazie alla sua efficienza, la trasformata di Fourier è impiegata come componente in molti algoritmi quantistici più complessi, uno dei quali, il Phase Estimation, viene presentato qui nel terzo capitolo. L'algoritmo del Phase Estimation è importante in computazione quantistica non solo per la sua efficienza, dovuta all'uso della trasformata di Fourier quantistica, ma anche per la sua versatilità. Viene applicato recentemente in molti algoritmi, incluso l'algoritmo di Shor per la fattorizzazione in numeri primi, che è stato implementato in un computer quantistico costruito da IBM, che nel 2014 riusciva a fattorizzare il numero 56153, il numero ad oggi più grande fattorizzato da un computer quantistico (Dattani, N. S. and Bryans, N. *Quantum factorization of 56153 with only 4 qubits*, https://arxiv.org/abs/1411.6758, Dicembre 2014).