Quantum Computing e Data Analytics

Simone Benedetto
Università degli Studi di Salerno
b.simone@studenti.unisa.it

Sommario

Big Data è un termine che indica dati così grandi, complessi e difficili da elaborare con i metodi tradizionali. Analizzare i Big Data aiuta le aziende nel processo decisionale, permettendo loro di essere competitivi sul mercato. Per fare ciò è necessaria una straordinaria capacità di calcolo che la miniaturizzazione dei transistor non riesce più a garantire a causa di limiti fisici. Potenziale soluzione al problema è il Quantum Computing che, mediante l'applicazione di concetti di meccanica quantistica per l'elaborazione di informazioni, permette di risolvere problemi complessi in poco tempo.

1 Introduzione

Ogni giorno vengono generate grandi risorse di dati. Dietro questo aumento esponenziale c'è la crescita dell'economia ditigale dovuta al massivo utilizzo di Internet, attraverso i social network, nel settore sanitario, in quello bancario, e recentemente, nell' Internet of Things (IoT). Dati così grandi, veloci o complessi, difficili o impossibili da elaborare con i metodi tradizionali sono definiti *Big Data*.

Prima della rivoluzione dei Big Data le aziende erano impossibilitate nell'archiviare enormi quantità di dati per lunghi periodi a causa della mancanza di scalabilità, flessibilità e prestazioni necessarie nel contesto dei Big Data [1].

Gestire i Big Data richiede la pulizia, l'elaborazione, l'analisi, la protezione e l'accesso granulare a serie di dati in continua evoluzione ed ottenere informazioni da essi rappresenta una grande sfida che richiede risorse, metodologie e tecnologie potenti.

L'analisi dei Big Data è di fondamentale importanza per le aziende, perchè permette loro di essere competitivi sul mercato sviluppando prodotti e servizi intelligenti.

Per tale scopo, nonostante l'elevata disponibilità di strumenti, ci sono problemi ad alta complessità che non possono essere risolti in tempi ottimali dai computer classici più avanzati, ma richiedono sistemi con straordinarie capacità di elaborazione che dipendono dal numero di transistor.

L'azienda dei semiconduttori, seguendo costantemente le previsioni sulle prestazioni della legge di Moore, ha raddoppiato il numero di transistor nei circuiti informatici ogni due anni circa [2]. Ciò ha comportato la riduzione dei transistor ad una dimensione di circa 2 nanometri, paragonabili a pochi atomi disposti uno accanto all'altro [3]. Tuttavia la miniaturizzazione dei transistor è possibile solo in misura limitata a causa del calore che inevitabilmente si genera quando un numero crescente di circuiti di silicio vengono incastrati in uno spazio ridotto.

Una delle potenziali soluzioni al problema della capacità di elaborazione è il *Quantum Computing*, ovvero l'applicazione dei concetti di meccanica quantistica nel campo dell'elaborazione delle informazioni. Questa tecnologia permette di risolvere problemi complessi di ottimizzazione molto più velocemente e di affrontare problemi che con l'odierna tecnologia dei semiconduttori risultano impossibili da risolvere.

La potenza di elaborazione dei computer quantistici è superiore a quella dei computer convenzionali poiché funzionano nell'ordine di 2^n in termini di qubit. I computer quantistici, in una frazione di secondi, possono rispondere ad un problema a cui un computer tradizionale può rispondere in diverse ore. In questo caso si parla di Quantum Supremacy [4]. Nel 2019, Google ha confermato il raggiungimento della supremazia quantistica affermando che Sycamore, un processore quantistico a 53 qubit, ha risolto in tre minuti e 20 secondi un calcolo estremamente complesso [5].

2 Quantum Computing

Il Quantum Computing ottiene il suo grande potenziale da tre fenomeni della meccanica quantistica: sovrapposizione, interferenza ed entanglement [6].

Il principio di *sovrapposizione* quantistico è alla base del qubit, l'unità di informazione del Quantum Computing: al contrario del bit, che può assumere solo valore zero o valore uno, il qubit può assumere contemporaneamente valore zero, uno e tutte le somme pesate tra loro, garantendo un aumento esponenziale della potenza computazionale. Tali valori possono essere elaborati in parallelo (parallelismo quantistico) solo se nel qubit viene mantenuta la sovrapposizione. Il calcolo non è più possibile se avviene il collasso della particella in uno stato.

L'*interferenza* quantistica è la probabilità del qubit di collassare in un modo o nell'altro. Essa influisce sullo stato di un qubit per influenzare la probabilità di

un determinato risultato durante la misura e questo stato probabilistico è il punto di eccellenza della potenza del calcolo quantistico. Ad esempio, per due bit in un computer classico, ogni bit può archiviare un valore di 1 o 0 e vengono così archiviati insieme quattro valori possibili: 00, 01, 10 e 11, ma solo uno di questi alla volta. Con due qubit in sovrapposizione, tuttavia, ogni qubit può essere 1 o 0 o entrambi, quindi è possibile rappresentare contemporaneamente gli stessi quattro valori.

L'*entanglement* è la correlazione tra due particelle che formano un sistema globale, in modo che lo stato quantistico dei singoli sottosistemi non possa essere descritto in modo indipendente. Quindi, agendo su una particella, si cambierà lo stato (il comportamento) anche dell'altra, con un'accelerazione importante del processo computazionale.

2.1 Qubit

I computer classici utilizzano come unità di informazione di base il cosiddetto bit. Da un punto di vista prettamente fisico il bit è un sistema a due stati: può infatti essere indotto in uno dei due stati distinti rappresentanti due valori logici, 0 e 1.

I computer quantistici invece, utilizzano il *qubit* (quantum bit). Come il bit classico può esistere in due stati distinti, indicati con $|0\rangle$ e $|1\rangle$. Inoltre però, può trovarsi in una sovrapposizione di stati (o combinazione lineare) di due stati fondamentali (o stati della base computazionale). Nello stato di sovrapposizione, il qubit può assumere contemporaneamente valore zero, uno e tutte le somme pesate tra loro. Un generico qubit è dato da una combinazione lineare

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

dove α e β sono numeri complessi tali che $|\alpha|^2 + |\beta|^2 = 1$.

Quando misuriamo lo stato di un qubit possiamo ottenere lo stato $|0\rangle$ con una probabilità pari a $|\alpha|^2$ oppure lo stato $|1\rangle$ con una probabilità pari a $|\beta|^2$. Per questo motivo i valori α e β sono chiamati *ampiezze di probabilità* e la somma $|\alpha|^2 + |\beta|^2$ deve essere uguale a 1. La misura dello stato di un qubit darà sempre come risultato lo stato $|0\rangle$ o lo stato $|1\rangle$.

Per visualizzare un qubit si può utilizzare una sfera di raggio unitario, che rappresenta sulla sua superficie gli stati di un qubit. Il polo nord della sfera corrisponde a 0, mentre il polo sud corrisponde a 1. Tutte le altre posizioni sulla sfera sono gli stati di sovrapposizione. Tale sfera prende il nome di *sfera di Bloch* (Figura 1).

Esistono molte rappresentazioni fisiche di qubit che possono essere manipolate per calcoli controllati, come le codifiche di stato in un atomo, lo spin di un elettrone, la polarizzazione o sistemi più complessi.

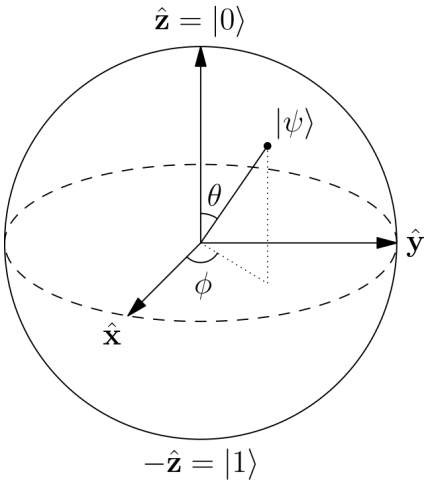

Figura 1: Stato $|\psi\rangle$ generico di un qubit sulla sfera di Bloch.

2.2 Porte quantistiche

Sia un computer classico che uno quantistico è formato da circuiti costituiti da porte logiche. Per un singolo bit, nel caso classico, esiste solo una porta (non banale) a un bit, la porta NOT, che implementa l'operazione logica di negazione definita mediante una tabella di verità. Per definire la stessa operazione su un qubit dovremmo considerare, oltre all'azione sugli stati base $|0\rangle$ e $|1\rangle$, anche l'azione su una sovrapposizione di stati $|0\rangle$ e $|1\rangle$.

Dato lo stato iniziale $\alpha|0\rangle + \beta|1\rangle$, lo stato ottenuto dalla porta NOT sarà $\beta|0\rangle + \alpha|1\rangle$. La matrice corrispondente al NOT quantistico è chiamata X ed è definita da:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Se pensiamo alle porte quantistiche su un singolo qubit come a matrici 2x2, ciò vuol dire che qualsiasi matrice 2x2 può essere una porta quantistica. Non è proprio cosi, perchè la condizione di normalizzazione richiede che $|\alpha|^2 + |\beta|^2 = 1$ in qualsiasi stato quantistico. Ciò significa che tale condizione deve valere anche per gli stati ottenuti dopo una operazione. Dato questo vincolo, solo le matrici unitarie, che trasformano un vettore unitario in un vettore ancora unitario, possono essere porte quantistiche. Una matrice è unitaria se $U^+U = I$, dove U^+ è l'aggiunto di U (ottenuto trasponendo ed effettuando il complesso coniugato di U) e I è una matrice identità $2x2$.

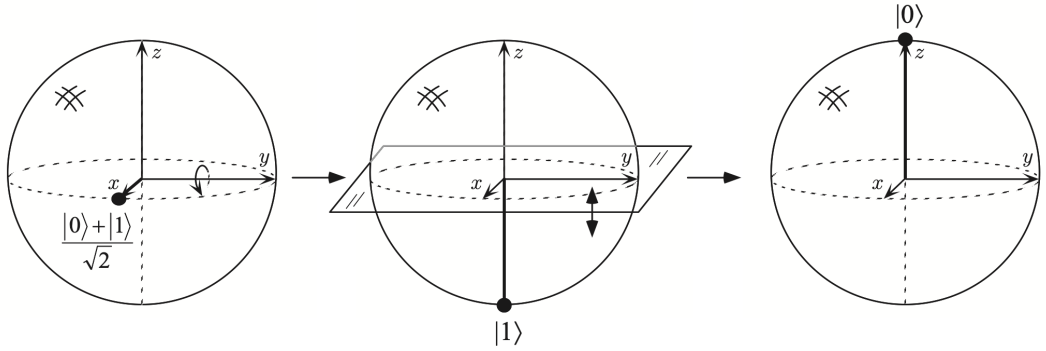

Figura 2: Visualizzazione della porta di Hadamard sulla sfera di Bloch, agendo sullo stato di ingresso $(|0\rangle + |1\rangle)/\sqrt{2}$.

Nel caso quantistico esistono molte operazioni non banali su un singolo qubit. Di notevole importanza sono la porta di Hadamard e le tre matrici di Pauli. La porta di Hadamard, definita come

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

trasforma $|0\rangle$ in $(|0\rangle + |1\rangle)/\sqrt{2}$, e trasforma $|1\rangle$ in $(|0\rangle - |1\rangle)/\sqrt{2}$. Siccome le porte a singolo qubit corrispondono a rotazioni e riflessioni della sfera, la porta di Hadamard definisce un operazione di rotazione di 90° della sfera intorno all'asse y, seguita da una riflessione attraverso il piano (x,y) (Figura 2) .

Le tre matrici di Pauli invece, sono definite come

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

La matrice X è la porta NOT che trasforma $|0\rangle$ in $|1\rangle$ e viceversa. La matrice Z lascia invariato lo stato $|0\rangle$ e inverte il segno dello stato $|1\rangle$. Le matrici X e Z sono note anche come matrice *bit flip* e matrice *phase flip*. La matrice Y è la combinazione delle matrici X e Z, ed effettua sia il bit flip che il phase flip.

Le operazioni su registri quantistici di due o più qubit sono necessarie per descrivere le trasformazioni di stati composti e in particolare dei cosiddetti stati entangled. Nel caso classico, le porte AND, OR, XOR, NAND e NOR implementano operazioni su due bit.

Le porte NOT e AND formano un insieme universale, cioè qualsiasi funzione booleana si può realizzare mediante una combinazione di queste due operazioni. Al contrario, lo XOR preso singolarmente o anche insieme al NOT non è universale. Qualsiasi circuito che coinvolga solo le porte NOT e XOR, se due ingressi x e y

hanno la stessa parità, darà uscite con la stessa parità, limitando la classe di funzioni che possono essere calcolate e quindi precludendo l'universalità.

L'analogo quantistico di XOR è la porta CNOT (controlled-NOT) che opera su due qubit: il primo è chiamato qubit di *controllo* e il secondo è il qubit *target*. Se il controllo è zero allora il target resta inalterato; se il controllo è uno, allora il target viene negato, cioè:

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle.$$

La rappresentazione della porta CNOT è

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

dove la prima colonna descrive la trasformazione del vettore della base computazionale $|00\rangle$, la seconda quella del vettore $|01\rangle$, la terza di $|10\rangle$ e la quarta di $|11\rangle$. Essendo una trasformazione unitaria, il CNOT è invertitile. La porta CNOT e le porte a un qubit sono alla base di tutte le porte logiche quantistiche, infatti sono operazioni universali.

2.3 Accelerazione dei processi di calcolo quantistico

Uno degli obiettivi della ricerca nel campo quantistico è quello di studiare quali problemi possono essere risolti più velocemente da un computer quantistico rispetto a un computer classico mediante l'utilizzo di algoritmi quantistici.

Un noto esempio è *l'algoritmo di Grover*, che accelera la soluzione alle ricerche di dati non strutturate, eseguendo la ricerca in meno passaggi rispetto a qualsiasi algoritmo classico [7]. Dati N record in un database non ordinato, il problema risiede nell'identificare quell'unico record che soddisfa una particolare proprietà. Qualsiasi algoritmo classico, deterministico o probabilistico, richiede $O(N)$ passi, poiché in media dovrà esaminare una grande frazione degli N record. L'algoritmo di Grover invece, garantisce una complessità pari a $O(\sqrt{N})$ dato che i sistemi quantistici possono eseguire più operazioni simultaneamente. Questo metodo è ottimale per problemi di ricerca completamente non strutturati e le sue applicazioni più importanti e utili si riscontrano nella risoluzione di problemi NP-completi.

Tale algoritmo di ricerca può essere in realtà utilizzato per qualsiasi problema che consenta di verificare se un dato valore x è una soluzione valida. Di seguito vengono riportati alcuni esempi [6]:

- **Problema di soddisfacibilità booleana**: il set di valori booleani x è un'interpretazione (un'assegnazione di valori a variabili) che soddisfa la formula booleana data?

- **Problema del commesso viaggiatore**: x descrive il tragitto più breve possibile che connette tutte le città?

- **Problema di fattorizzazione di un intero**: il numero fisso N è divisibile per il numero x?

2.4 Apprendimento automatico quantistico

L'apprendimento automatico nei computer classici sta rivoluzionando il mondo della scienza e dell'impresa. Essendo una branca dell'intelligenza artificiale, ottiene il suo potere imparando dalle esperienze precedenti al fine di prevedere il futuro, fornendo un notevole supporto al processo decisionale in tutti i campi. L'attuale mondo dei Big Data crea una sfida per l'apprendimento automatico, a causa del costo di calcolo elevato per l'addestramento dei modelli. In questo caso, il calcolo quantistico può aiutare con la formazione continua di grandi quantità di dati fornendo algoritmi più veloci di quelli tradizionali. Classicamente ci sono tre tipi di apprendimento automatico [8]:

- **Supervised learning**: vengono utilizzati insiemi di dati etichettati. Questi insiemi sono progettati per addestrare o "supervisionare" gli algoritmi nella classificazione di dati o nella predizione di risultati. Grazie alle etichette, il modello può misurare le proprie performance e imparare nel tempo.

- **Unsupervised learning**: vengono utilizzati insiemi di dati non etichettati. Gli algoritmi scoprono modelli nascosti nei dati senza la necessità di un intervento umano.

- **Reinforcement learning**: tecnica in cui un agente impara a svolgere un'attività tramite ripetute interazioni di tipo "trial-and-error" con un ambiente dinamico. Questo approccio consente all'agente di adottare una serie di decisioni in grado di massimizzare una metrica di ricompensa per l'attività, senza essere esplicitamente programmato per tale operazione e senza l'intervento dell'uomo.

2.4.1 *k*-Nearest Neighbors

Metodo molto diffuso per la classificazione di dati è l'algoritmo *k-Nearest Neighbors*. Dato un set di addestramento T di vettori di caratteristiche con le rispettive classificazioni e un vettore di input non classificato $\vec{x}$, l'idea è quella di assegnare al vettore di input la classe più comune che appare tra i suoi k vicini (Figura 3). Tale approccio è basato sulla vicinanza tra i vettori per considerarli istanze simili. Le misure di distanza più comuni per la manipolazione di vettori sono la distanza Euclidea e la distanza Manhattan [9]. La distanza Euclidea, definita come

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2}$$

misura una linea retta tra il punto di query e il punto che si sta misurando, ed è utilizzabile solo con vettori aventi valori reali. La distanza Manhattan, definita come

$$d(x,y) = (\sum_{i=1}^{m}|x_i - y_i|)$$

misura il valore assoluto tra due punti.

Sfida di tale algoritmo è la scelta del parametro k, la cui scelta errata può influenzare negativamente il risultato. Scegliendo un k molto grande, si perdono informazioni sulla località e la classificazione sarà una banale votazione per maggioranza sull'intero set di addestramento. Un k molto piccolo invece, porta a risultati affetti da rumore. Essendo la distanza il fattore base di funzionamento dell'algoritmo, per creare una versione quantistica bisogna focalizzarsi sulla valutazione efficiente di una distanza classica attraverso un algoritmo quantistico.

Ad esempio, si potrebbe utilizzare come "misura di somiglianza" la sovrapposizione o la *fedeltà* $\langle a|b\rangle$ di due stati quantistici $|a\rangle$ e $|b\rangle$ [10]. Il Control-Swap test (Figura 4) rende possibile calcolare la somiglianza tra due stati $|a\rangle$ e $|b\rangle$, misurata come loro fedeltà.

Siccome viene utilizzato un qubit ausiliario impostato su $|0\rangle$, l'input per il circuito sarà $|0\rangle|a\rangle|b\rangle$. Dopo aver applicato la prima porta H, lo stato evolve verso la sovrapposizione

$$\frac{1}{\sqrt{2}}|0\rangle|a\rangle|b\rangle + \frac{1}{\sqrt{2}}|1\rangle|a\rangle|b\rangle.$$

Applicando la porta C-Swap, che scambia $|a\rangle$ e $|b\rangle$ se lo stato del qubit di controllo è 1, lo stato evolve in

$$\frac{1}{\sqrt{2}}|0\rangle|a\rangle|b\rangle + \frac{1}{\sqrt{2}}|1\rangle|b\rangle|a\rangle.$$

Dopo aver applicato la seconda porta H, lo stato diventa

$$\frac{1}{2}|0\rangle(|a\rangle|b\rangle + |b\rangle|a\rangle) + \frac{1}{2}|1\rangle(|a\rangle|b\rangle - |b\rangle|a\rangle).$$

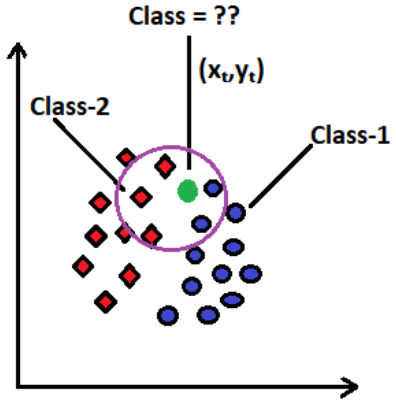

Figura 3: K-Nearest Neighbour.

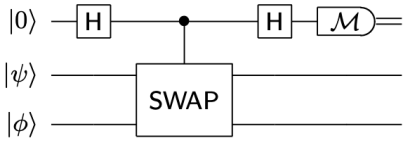

Figura 4: Circuito del Control-SWAP test.

Infine, il processo di misura è definito come

$$P(|0\rangle) = \frac{1}{2} + \frac{1}{2}|\langle a|b\rangle|^2,$$

$$P(|1\rangle) = \frac{1}{2} - \frac{1}{2}|\langle a|b\rangle|^2.$$

Se a e b sono ortogonali ($|\langle a|b\rangle|^2 = 0$), la probabilità che venga misurato 0 oppure 1 è $1/2$. Se gli stati sono uguali ($|\langle a|b\rangle|^2 = 1$) , la probabilità che venga misurato 0 è 1, mentre la probabilità che venga misurato 1 è 0.

Combinando il C-Swap test con un algoritmo di minimizzazione quantistica, ad esempio l'algoritmo di Grover, si può ridurre il tempo di ricerca dei vicini dal classico $O(n)$ a $O(\sqrt{n})$ [11].

3 Conclusioni

La raccolta di dati da più applicazioni cresce ogni giorno molto rapidamente, ed è evidente che questi dati sono utili solo se analizzati in modo intelligente. Siccome la gestione dei Big Data pone problemi ad altà complessità difficili da risolvere in tempi ottimali dai computer classici, una delle soluzioni è il Quantum Computing. Ottenendo il suo grande potenziale da fenomeni di meccanica quantistica, quali sovrapposizione, interferenza ed entanglement, permette di risolvere problemi complessi di ottimizzazione più velocemente rispetto ai computer classici. In questo articolo, sono state dapprima analizzate le differenze tra computer classici e computer quantistici considerando l'unità di informazione utilizzata e le porte logiche. Successivamente è stato analizzato come il Quantum Computing aiuta nell'accelerazione

dei processi di calcolo, ad esempio, mediante l'utilizzo dell'algoritmo di Grover che garantisce una complessità pari a $O(\sqrt{N})$ rispetto a qualsiasi algoritmo di ricerca classico avente complessità $O(N)$. Infine, si è analizzata una tecnica molto importante per l'analisi dei dati, l'apprendimento automatico. Dovendo trattare una quantità eccessiva di dati per l'addestramento dei modelli, il Quantum Computing può fornire algoritmi più veloci di quelli tradizionali. È stata analizzata la versione quantistica dell'algoritmo K-Nearest Neighbors che utilizza come metrica di somiglianza la fedeltà di due stati quantistici e grazie all'utilizzo dell'algoritmo di Grover garantisce la ricerca di un vicino in tempo $O(\sqrt{n})$ rispetto al classico $O(n)$.

Riferimenti bibliografici

[1] Oussous, Ahmed, et al. "Big Data technologies: A survey." Journal of King Saud *University-Computer and Information Sciences 30.4 (2018): 431-448.*

[2] Waldrop, M. Mitchell. "More than moore." *Nature 530.7589 (2016): 144-148.*

[3] B.H. McCarthy, S. Ponedal, "IBM Unveils World's First 2 Nanometer Chip Technology, Opening a New Frontier for Semiconductors", 2021. [Online]. *Available: https://newsroom.ibm.com/2021-05-06-IBM-Unveils-Worlds-First-2-Nanometer-Chip-Technology,-Opening-a- New-Frontier-for-Semiconductors.*

[4] Markov, Igor L., et al. "Quantum supremacy is both closer and farther than it appears." *arXiv preprint arXiv:1807.10749 (2018)*

[5] F. Arute et al., "Quantum supremacy using a programmable superconducting processor", *Nature, 574(7779):505–510, 2019.*

[6] [Online]https://docs.microsoft.com/it-it/azure/quantum/overview-understanding-quantum-computing

[7] Grover, Lov K. "A fast quantum mechanical algorithm for database search." *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.*

[8] Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. "An introduction to quantum machine learning." *Contemporary Physics 56.2 (2015): 172-185.*

[9] [Online]https://www.ibm.com/it-it/topics/knn

[10] Aïmeur, Esma, Gilles Brassard, and Sébastien Gambs. "Machine learning in a quantum world." *Conference of the Canadian Society for Computational Studies of Intelligence. Springer, Berlin, Heidelberg, 2006.*

[11] [Online] https://medium.com/@gordenstein30/quantum-knn-5deda06c5578