Computación cuántica:

El procesamiento de información cuántica es el resultado de utilizar la realidad física que se menciona en la teoría cuántica con el fin de realizar tareas que antes se creían imposibles. Los dispositivos que realizan dicho procesamiento cuántico son las computadoras cuánticas. [An Introduction to Quantum Computing]

1. Circuitos:

   Los circuitos son redes compuestas por cables que transportan valores de bit a compuertas que realizan operaciones elementales en los bits. Todos los circuitos que consideramos serán acíclicos, lo que significa que los bits se mueven a través del circuito de forma lineal y los cables nunca retroalimentan a una ubicación anterior en el circuito. Un circuito es una matriz o red de puertas, que es la terminología que se usa a menudo en el entorno cuántico. Las puertas provienen de una familia finita, y toman información de los cables de entrada y entregan información a lo largo de algunos cables de salida. [An Introduction to Quantum Computing]

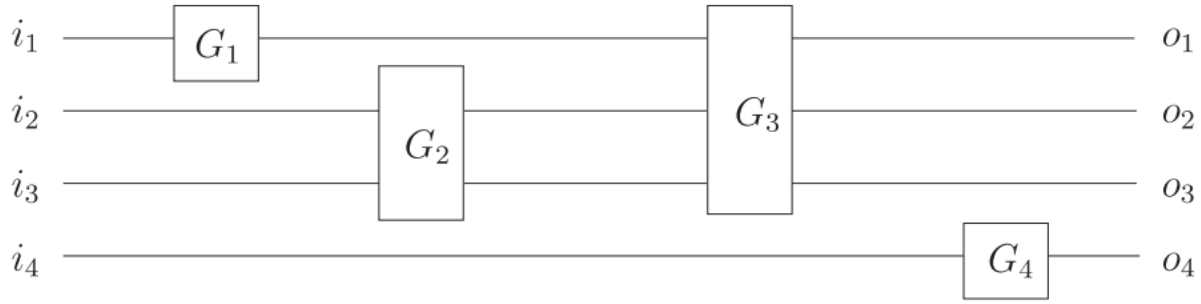
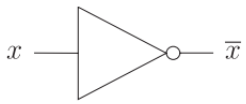


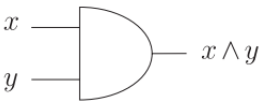
Fig. 1.1 A circuit diagram

Definicion: Un conjunto de compuertas es universal para el cálculo clásico si, para cualquier entero positivo n, m y función $f : {0, 1}^n → {0, 1}^m$, se puede construir un circuito para calcular f usando solo compuertas a partir de ese establecer. [An Introduction to Quantum Computing]

2. Computación reversible:

   La teoría de la computación cuántica está relacionada con una teoría de la computación reversible. Un cálculo es reversible si siempre es posible recuperar de forma única la entrada, dada la salida. Por ejemplo, la operación NOT es reversible, porque si el bit de salida es 0, sabe que el bit de entrada debe haber sido 1, y viceversa. Por otro lado, la operación AND no es reversible. [An Introduction to Quantum Computing]





x	$\overline{x}$
0	1
1	0

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

figura

Cada puerta en una familia finita de puertas se puede hacer reversible agregando algunos cables de entrada y salida adicionales si es necesario. [An Introduction to Quantum Computing]

3. Notación Dirac y espacios de Hilbert:

   La notación de Dirac fue inventada por Paul Dirac y se usa a menudo en mecánica cuántica. Dicha notación identifica un vector que se escribe dentro de un 'ket' y se parece a $|a\rangle$. [An Introduction to Quantum Computing]

   La base canónica de un espacio vectorial bidimensional tiene dos vectores, denotados por $\{|0\rangle, |1\rangle\}$ en la notación de Dirac, donde |0i y |1i tienen la siguiente representación: [Basic Quantum Algorithms]

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

   Estos vectores tienen dos entradas, longitud unitaria y son ortogonales. Entonces, esta base es ortonormal. Se llama base canónica en álgebra lineal y base computacional en computación cuántica. Tenga en cuenta que |0i no es el vector nulo, sino el primer vector de la base canónica. Todas las entradas del vector nulo son iguales a 0.[Basic Quantum Algorithms]

   Los espacios vectoriales están sobre números complejos y son de dimensión finita, lo que simplifica significativamente las matemáticas que se requiere, a su vez, los espacios vectoriales son miembros de una clase de espacios vectoriales llamados espacios de Hilbert y está dada por esta notación $\mathcal{H}$. [An Introduction to Quantum Computing]

4. Qubit y superposición:

   La unidad de memoria básica de una computadora clásica es el bit, que asume 0 o 1. Por lo general, el bit se implementa usando dos voltajes distintos, siguiendo la convención de que el voltaje bajo o nulo representa el bit 0 y el voltaje alto representa el bit 1. La unidad de memoria básica de una computadora cuántica es el qubit, que también asume, al final del cálculo, 0 o 1. [Basic Quantum Algorithms]

La diferencia con el dispositivo clásico ocurre durante el cómputo ya que el qubit admite la coexistencia simultánea de 0 y 1, es decir, antes de la medición, el estado de un qubit está representado por un vector bidimensional norma-1 y los estados de un qubit correspondientes a 0 y 1 son |0i y |1i. La coexistencia cuántica se representa matemáticamente mediante una combinación lineal de vectores ortonormales de la siguiente manera: [Basic Quantum Algorithms]

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

where α and β are complex numbers that obey the constraint

$$|\alpha|^2 + |\beta|^2 = 1.$$

El estado del qubit es el vector |ψi de la norma 1 con las entradas α y β. Los números complejos α y β son las amplitudes del estado |ψi.

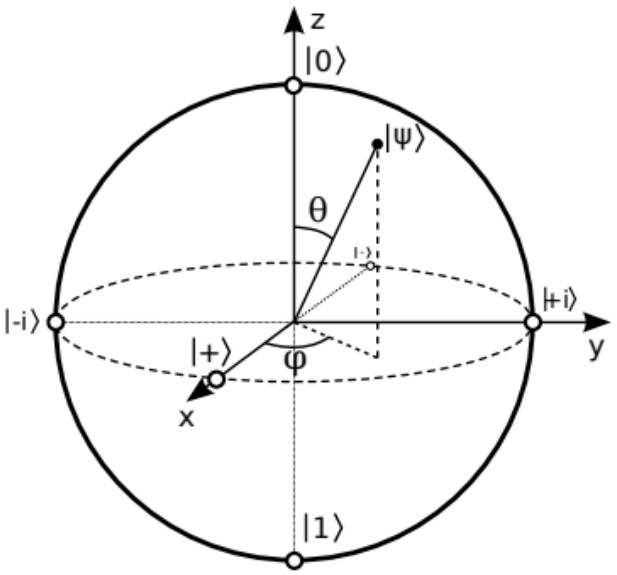


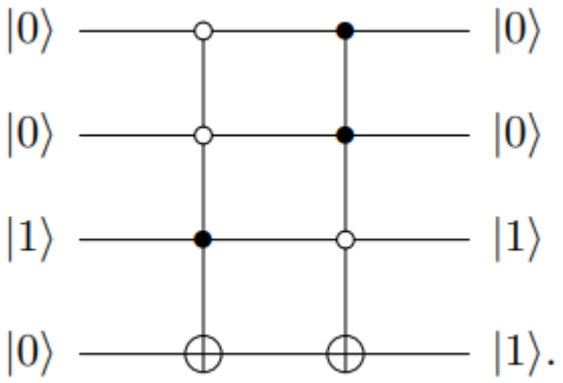
Figura 2.1: Esfera de Bloch y ubicación de los estados |0i, |1i, |±i y |±ii. Se muestra un estado arbitrario |ψi con ángulos esféricos θ y ϕ.

5. Circuito de una función Booleana:

Ahora se mostrarácómo obtener el circuito cuántico de una tabla de verdad; esto se logrará mediante puertas Toffoli multiqubit. Para mostrar que las puertas de Toffoli multiqubit puede implementar cualquier función booleana en una computadora cuántica, tomemos como ejemplo la función booleana de 3 bits f(a, b, c) definida por la siguiente tabla de verdad:[Basic Quantum Algorithms]

a	b	c	$f(a,b,c)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Como f tiene tres bits de entrada, usamos puertas Toffoli multiqubit con tres controles. El cuarto qubit es el objetivo. La salida de f es la salida de una medición del qubit objetivo. Como f tiene dos cláusulas en la forma normal disyuntiva, usamos dos compuertas Toffoli multiqubit. La primera compuerta debe ser activada por la entrada |001i y la segunda por |110i, que corresponden a las filas de la tabla de verdad cuya salida es:[Basic Quantum Algorithms]



Tenga en cuenta que si la entrada es |a, b, ci|0i, entonces la salida es |a, b, ci|f(a, b, c)i. Esto muestra que la computadora cuántica puede calcular cualquier función booleana de n bits utilizando una puerta Toffoli multiqubit con (n + 1) qubits para cada salida 1 de la tabla de verdad. Desafortunadamente, esta técnica de construcción de circuitos cuánticos para calcular tablas de verdad no es eficiente, ya que el número de puertas de Toffoli multiqubit aumenta exponencialmente en función del número de qubits en el peor de los casos. [Basic Quantum Algorithms]

ANÁLISIS DE FORTALEZAS Y DEBILIDADES:

Si bien la computación cuántica ha avanzado dramáticamente durante la última década, sus aplicaciones potenciales aún no se han demostrado a gran escala. Es probable que tales demostraciones requieran avances en física, informática e ingeniería, ya que, las computadoras cuánticas son propensas a errores debido a la coherencia cuántica y las condiciones ambientales.[Grover's Algorithm]

Por otro lado, se dice que en el futuro, una computadora cuántica (QC) puede resolver algunos problemas mucho más rápido que una computadora clásica (CC), lo que se denomina ventaja cuántica, esto se debe a que la potencia de cómputo de QC está creciendo más rápido que la de CC. Una de las medidas del rendimiento de la Computadora

Cuántica introducida por IBM es el Volumen Cuántico. Para lograr una ventaja cuántica en la próxima década, IBM declaró que “necesitan al menos duplicar el volumen cuántico de nuestros sistemas de computación cuántica cada año.” En enero de 2020, Chow y Gambetta confirmaron que IBM está en camino de alcanzar este objetivo con una nueva computadora cuántica de 28 qubits que demuestra el volumen cuántico de 32 [Quantum Advantage and Y2K].

Asimétrico:

Todos los algoritmos asimétricos actuales (RSA, ECC, DH, DSA) se pueden descifrar mediante computadoras cuánticas. Se basan en el problema de factorización prima o el problema del logaritmo discreto, que son fáciles de resolver en computadoras cuánticas utilizando el algoritmo de Shor.Matemáticos y criptógrafos utilizaron estos problemas de teoría de números para fundamentar la seguridad de los algoritmos asimétricos. Ahora tienen que buscar nuevos problemas matemáticos que las computadoras cuánticas no puedan resolver fácilmente. [Post Quantum Cryptography Techniques]

Simétrico:

Los algoritmos simétricos y las funciones hash son relativamente seguros en un mundo poscuántico. El algoritmo de Grover puede acelerar los ataques por complejidad de raíz cuadrada, sin embargo, la mayoría de los algoritmos se pueden volver a asegurar duplicando el tamaño de la clave. [Post Quantum Cryptography Techniques]

Todos los algoritmos asimétricos actuales se basan en problemas matemáticos para los que la gente ha buscado soluciones durante siglos. Sin embargo, la debilidad que tienen es que las computadoras cuánticas son buenas en tareas paralelas que requieren un resultado al final. Dado que los algoritmos requieren solo un resultado al final, se puede usar una superposición de qubits para paralelizar todos los cálculos y luego se puede medir el resultado. Para evitar aprovechar el paralelismo de las computadoras cuánticas se pueden utilizar algoritmos que requieren varios resultados. De esta manera, el paralelismo de las computadoras cuánticas no se puede utilizar en toda su extensión.[Post Quantum Cryptography Techniques]

CITAS:

[Grover's Algorithm]

@unknown{Grover's AlgorithmSinghal,
author = {Singhal, Akanksha and Chatterjee, Arko},
year = {2018},
month = {07},
pages = {},
title = {Grover's Algorithm},
doi = {10.13140/RG.2.2.30860.95366}
}

[Post Quantum Cryptography Techniques]

@article{Post Quantum Cryptography Techniques,
  author   = {Ritik Bavdekar and
               Eashan Jayant Chopde and
               Ashutosh Bhatia and
               Kamlesh Tiwari and
               Sandeep Joshua Daniel and
               Atul},
  title   = {Post Quantum Cryptography: Techniques, Challenges, Standardization,
               and Directions for Future Research},
  journal   = {CoRR},
  volume   = {abs/2202.02826},
  year   = {2022},
  eprinttype = {arXiv},
  eprint   = {2202.02826},
  timestamp = {Wed, 09 Feb 2022 15:43:35 +0100}
}

[Quantum Advantage and Y2K].

@unknown{QuantumAdvantageandY2K,
author = {Zhang, Lei and Miranskyy, Andriy and Rjaibi, Walid},
year = {2019},
month = {07},
pages = {},
title = {Quantum Advantage and Y2K Bug: Comparison}
}