Computación Cuantica
Modelos de Computacion

Luis José Quintana Bolaño

Enero, 2014

Resumen

Este documento comprende un relativamente breve análisis del paradigma de la computación cuantica. Incluyendo como mínimo definición, ejemplos de cálculo, definición de función computable, relaciones con otros modelos de computación conocidos.

1. Definición y orígenes

La computación cuantica es un paradigma de computación basado en "qubits", en lugar de los clásicos bits. Esta diferencia fundamental da lugar nuevas puertas lógicas, que permite la creación de nuevos algoritmos. Tareas iguales pueden tener diferentes niveles de complejidad en computación clásica y computación cuantica, siendo esta una de las principales fuentes de interés por este paradigma, ya que problemas tradicionalmente intratables pasan a ser tratables bajo este modelo.

Mientras que en computación digital se mantiene una memoria compuesta de bits, cada bit representando solo uno de dos valores (0 o 1), un computador cuántico mantiene una secuencia de qubits, cada cual puede representar 1, 0 o una superposición coherente de ambos estados (dos estados ortogonales de una partícula subatómica). Esto permite que en computación cuantica puedan realizarse varias operaciones a la vez, dependiendo del número de qubits.
El número de qubits indica la cantidad de bits que pueden estar en superposición. Mientras que un registro de 3 bits ofrece un total de 8 posiciones conel mismo tomando solo una de ellas, un vector de 3 qbits ofrece la posibilidad de que la partícula tome ocho valores distintos a la vez mediante superposición cuántica. El número de operaciones es exponencial respecto al número de qubits.

Un ordenador cuántico de 30 qubits equivaldría a un procesador convencional de 10 teraflops (10 billones de operaciones en coma flotante por segundo), cuando actualmente las computadors trabajan en orden de gigaflops (millardos de operaciones por segundo).

En general n qubits pueden estar en cualquier suporposición arbitraria de hasta 2^n estados diferentes simultaneamente.

1.1. Origenes e historia

La idea de computación cuántica surge en 1981, cuando Paul Benioff expuso su teoría para aprovechar las leyes cuánticas en el entorno de la computación. The field of quantum computing was first introduced by Yuri Manin in 1980[2] and Richard Feynman in 1982

2. Modelos de computación

Con los suficientes recursos computacionales, una computadora clásica puede simular cualquier algorítmo cuántico; la computación cuántica no viola la tésis de Church-Turing. Sin embargo, las bases computacionales de 500 qubits, por ejemplo, serían demasiado grandes para representarlas en computación clásica, requiriendo 2^{501} bits de almacenamiento. (En comparación, un terabyte de información solo equivale a 2^{43} bits.)

2.1. Maquina de Turing cuantica

Un modelo teórico del modelo cuantico es la máquina de Turing cuantica, también conocida como computadora cuantica universal.
Es un modelo sencillo que camputa todo el poder de la computación cuántica.
Fuerin originalmente propuestas en 1985 por David Deutsh.

2.2. Circuitos cuánticos

Con más frecuentemente usados que las máquinas de Turing cuanticas y computacionalmente equivalentes. Los ordenadores cuanticos comparten similaridades teóricas con las computadoras no deterministas y probabilisticas.

3. Computación Quantica

Los cambios que ocurren a un estado cuantico se pueden describir mediante el uso del lenguaje de la computación quantica. Analogo al modo en que los computadores clásicos se construyen de circuitos electricos que contienen cables y puertas lógicas, las computadoras cuanticas contienen cables y puertas cuanticas elementales que transportan y manipulan la información cuantica. En esta sección se describen algunas puestas cuanticas simples y se presentan varios ejemplos de circuito que ilustran su aplicación, incluyendo un circuito que teleporta qubits!

3.1. Puertas de un solo qubit

Las computadoras clásicas consistian en cables y puertas logicas. Los cables se usan para transportar la información por el circuito, mientras que las puertas lógicas realizan manipulaciones de la información, convirtiendola de una orma en otra. Considere, por ejemplo, las puertas lógicas clásicas de un solo bit. El único miembro no trivial de esta clase en la puerta NOT, cuya operación se define por su tabla de la verdad, en la que $0 \to 1$ y $1 \to 0$, es decor, que los estados 0 y 1 se intercambian.

Puede una puerta cuantica NOT analoga para qubits ser definida? Imagina que tenemos un proceso que lleve del estado $|0\rangle$ al $|1\rangle$ y viceversa. Semejante proceso obviamente sería un buen candidato a analogo cuantico de la puerta NOT. Sin embargo, especificar la acción de la puerta en los estados $0 \to 1$ y $1 \to 0$ no nos dice que pasa para la superposición de ambos sin más conocimiento de las propiedades de las puertas cuanticas. De hecho, la puerta cuantica NOT actua de forma linear, es decir, toma el estado $\alpha|0\rangle + \beta|1\rangle$ al estado correspondiente en el que el rol de $|0\rangle$ y $|1\rangle$ han sido intercambiados, $\alpha|1\rangle + \beta|0\rangle$

A. Bibliografía