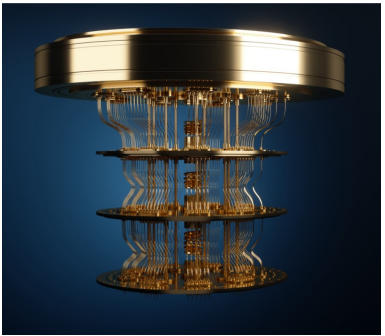
Algoritmo de Shor

Majo Gil

Teoría de Números

Computación Cuántica

¿Qué es la computación cuántica?
Es un campo que utiliza conocimientos
en ciencias de la computación, matemática y física
para aplicar mecánica cuántica en computadoras
y otros sistemas, de modo que estas sean capaces
de resolver problemas con complejidad alta
más rápido que las computadoras normales.Esto
al aprovechar efectos de la mecánica cuántica,
como interferencia cuántica y superposición



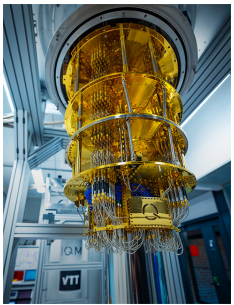
Computación Cuántica

¿Cuál es el estado actual?
Por el momento, no se han logrado crear computadoras que resuelvan de manera más eficiente que las computadoras normales. Sin embargo, desde el 2019 se han realizado grades avances, a partir de que se lograra que una computadora cuántica resolviera UN problema mucho más rápido que una sueprcomputadora. Se espera que en el futuro no muy distante, se logren estas computadoras.

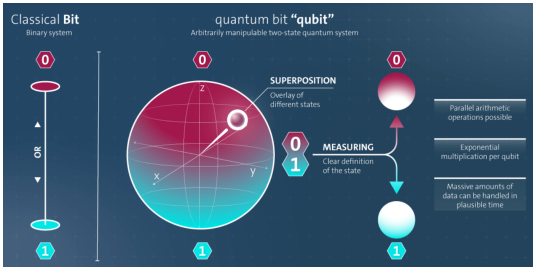
Problema 2019

Computación Cuántica

¿Cómo funciona una computadora cuántica? Las computadoras cuánticas comparte muchas cosas con las computadoras normales, sin embargo, su manera de operar es fundamentalmente diferente. Las dos tienen chips, circuitos, compuertas lógicas, usan código binario y algoritmos y otras cosas. La principal diferencia es cómo las computadoras codifican esos 1 y 0. Las computadoras cuánticas usan bits cuánticos, o qubits. Los qubits son creados manipulando átomos



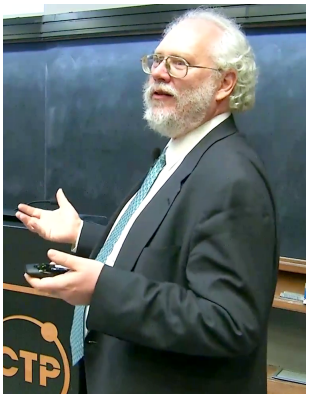
Computación Cuántica



Los qubits, a diferencia de los bits normales, pueden estar en una superosición de 1 y 0 a la vez hasta que un estado es medido. Además, los estados de múltiples qubits pueden estar entrelazados, estando cuántica mecánicamente relacionados el uno al otro. Esto es lo que les da la ventaja sobre las computadoras clásicas.

Peter Shor

Es un matemático estadounidense nacido en 1959. Es profesor de MIT de matemática aplicada e informática. En una estancia en New Jersey, desarrolló el algoritmo de Shor, inspirado en el *Problema de Simon*, donde primero, resolvió el problema del logaritmo discreto y luego resolvió el problema de factorización, diciendo que *existe una extraña relación entre el logaritmo discreto y factorización*. Gracias a este algoritmo le han dado premios como el premio Nevanlinna, el premio Gödel, el premio McArthur (genius Fellowship) y muchos otros más



Algoritmo de Shor

Algoritmo de Shor

Dado un entero impar N, encuentre sus factores enteros siguiendo los siguientes pasos:

1. Una reducción clásica
2. Utilizar un algoritmo cuántico para resolver el order finding problem

Reducción clásica

Reducción clásica

Revisar que N no sea múltiplo de 2 o una potencia prima. Si es, la factorización es trivial hasta llegar a un impar no potencia prima (en caso de 2)
Dado entonces que N es un entero impar, no potencia prima
1. Elegir $a \in \mathbb{Z}$ cualquiera tal que $2 \leq a < N$.
2. Utilizando el algoritmo de Euclides, obtener el $gcd(a, N)$
3. Si el resultado no es trivial ($gcd(a, N) \neq 1$), se da por finalizado el algoritmo y el otro factor no trivial es $\frac{N}{gcd(a,N)}$
4. Si a y N son coprimos, utilizar una subrutina cuántica que dará como resultado un valor de $r \ni a^r \equiv 1 mod\ N$.
5. Si r es impar, regresar al paso 1
6. Calcular $g = gcd(N, a^{\frac{a}{2}} + 1$. Si g es trivial, regresar al paso 1

Algoritmo Cuántico

La meta de la subrutina cuántica del algoritmo de Shor es, dado un set de coprimos N y $1 < a < N$, encontrar el valor r más pequeño posible tal que se cumple que $a^r \equiv 1 mod\ N$

Notación importante

n es el entero más pequeño tal que $N \leq 2^n$
La notación bra-ket $\langle | \rangle$ se utilizará para denotar estados cuánticos
$\otimes$ denota el producto tensor

Algoritmo Cuántico

Order-finding subrutina cuántica, paso 1

Aplique la estimación de fase cuántica con U unitaria representendo la operación de multiplicar por $a(\textit{modulo } N)$ y estado inicial (input state) $|0\langle^{\otimes 2n+1} \otimes |1\rangle$, donde el segundo registro es $|1\rangle$ hecho con n qubits. Los eigenvalores de U codifican información sobre el periodo, y $|1\rangle$ son una suma escribible de eigenvectores. Esto devuelve un entero aleatorio de la forma $\frac{j}{r} 2^{2n+1}$ para $j = 0, 1, ..., r-1$ aleatorio.

Algoritmo Cuántico

Order-finding subrutina cuántica, paso 2

Utilizar el algoritmo de fracciones continuas para obtener el periodo de r del entero obtenido en la fase anterior

Cabe denotar que el paso 2 del algoritmo puede ser realizado con una computadora normal

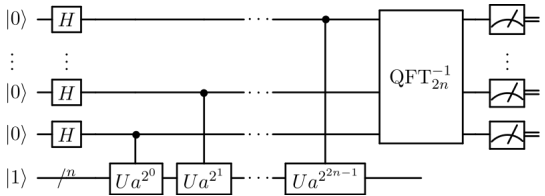


Figure: Quantum Phase estimation

Implementando el algoritmo

Por el momento, el algoritmo de Shor solo ha podido ser implementado pocas veces, en 2001, factorizando 15 y en 2012 factorizando 21, pero...

¿Qué pasaría si se pudiera implementar realmente?

Consecuencias

El algoritmo de Shor reduce la complejidad de la factorización de números a tiempo polinomial, precisamente a $O((\log N)^2(\log(\log N))$, $O(\log^3 N)$, y $O(\log N)$, dependiendo de la computadora, y se inutilizarían los siguientes sistemas de encriptación:

- RSA
- Diffie-Hellman de campo finito
- Diffie Hellman de curva elíptica

Por ello, actualmente se está trabajando apra desarrollar nuevos sistemas de encriptación que no dependan de complejidad de factorización.

Referencias

Xi Lin, F. (2013). Shor's Algorithm and the Quantum Fourier Transform. McGill University.

Wikipedia contributors. (2023, 13 noviembre). SHOR's algorithm. Wikipedia. https://en.wikipedia.org/wiki/Shor%27s_algorithm

SHOR's algorithm. (s.f.). https://www.qutube.nl/quantum-algorithms/shors-algorithm

Wikipedia contributors. (2023a, octubre 19). Peter Shor. Wikipedia. https://en.wikipedia.org/wiki/Peter_Shor

What is quantum computing? (s.f.). Caltech Science Exchange. https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-computing-computers