Factorización cuántica de números:

Algoritmo de Shor

Complejidad de los problemas

- P / NP
- Problema de factorización de números enteros ¿Qué clase? ¿P? ¿NP? -> BQP
- Computación cuántica como acelerador de algunos problemas explotando su estructura.

Bits Cuánticos

- Estados
- Combinación lineal de estados: superposiciones.

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

- Consulta del valor del bit probabilística.
- Electrón como ejemplo real de estos bits.

Computación cuántica

- Transformaciones unitarias en los vectores de estados
- Puertas cuánticas
- Quantum gate array
- Transformada cuántica de Fourier: cambio de dominio (tiempo/espacio -> frecuencia)

Algoritmo de Shor: Parte clásica

1. Escoge un número pseudoaleatorio a < N
2. Obtiene el mcd(a,N)
3. Si mcd(a,N) != 1 termina. Si NO realiza llamada a la parte cuántica del algoritmo para hallar el periodo r de la función f(x)=a^x mod N
4. Si r impar vuelve a paso 1
5. Si a^(r/2) = -1 vuelve a paso 1
6. Obtiene los factores de N como mcd(a^(r/2)+-1,N) y termina

Algoritmo de Shor: Parte cuántica (I)

1. Inicializa dos qubits de entrada y salida a: $N^{\frac{-1}{2}} \sum_{x=0}^{N-1} |x\rangle |0\rangle$

2. Construye f(x) como función cuántica y aplica al estado anterior: $N^{\frac{-1}{2}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$

3. Aplica la QTF al registro de entrada alcanzando el estado: $N^{-1} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle |f(x)\rangle$

Algoritmo de Shor: Parte cuántica (II)

4. Realiza una medición obteniendo y en el registro de entrada f(x0) en el de salida
5. Convierte y/N en una fracción irreductible y extrae el denominador r' candidato a r
6. Comprueba si f(x) = f(x+r'), en caso afirmativo termina
7. Obtiene más candidatos a r usando valores cercanos a y o múltiplos de r'. Si alguno cumple termina.
8. Vuelve al paso 1 de la parte cuántica.

Conclusiones

- Buenos resultados
- No generalizable a los NP-completos
- Falta hardware
- Avance rápido por parte de IBM