MOOC: Computación y Criptografía Cuánticas

Lección 3: Algoritmos Cuánticos

Soluciones razonadas a los test de evaluación

1. Dada $f : \{0,1\}^2 \to \{0,1\}^2$ tal que $f(a,b) = (0,b)$, la transformación unitaria U_f verifica:

a) $U_f(W_n(|00\rangle) \otimes |00\rangle)) = \frac{1}{2}(|0000\rangle + |0101\rangle + |1000\rangle + |1101\rangle)$.

Nótese que $W_n(|00\rangle)) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ y que $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$.

Por tanto $U_f(W_n(|00\rangle) \otimes |00\rangle)) = \frac{1}{2}(|00\rangle \otimes |00\rangle + |01\rangle \otimes |01\rangle + |10\rangle \otimes |00\rangle + |11\rangle \otimes |01\rangle)$

$U_f(W_n(|00\rangle) \otimes |00\rangle)) = \frac{1}{2}(|0000\rangle + |0101\rangle + |1000\rangle + |1101\rangle)$.

---

2. Dada $f : Z_2^3 \to Z_2^3$, periódica y 2 a 1, se aplica el algoritmo cuántico para resolver el problema de Simon dos veces y como resultado de las mediciones se obtienen los valores $k = 001$ y $k = 011$. Se puede asegurar que el periodo de f es

b) T=100.

El periodo T debe verificar $k \cdot T = 0$ para los dos valores de k. Es un sistema de rango dos, con solución única 100.

---

3. La transformada cuántica de Fourier sobre estados de n-qubits F_n verifica:

c) Para $n = 1$, la transformación unitaria F_1 coincide con $W_1 = H$.

Es inmediato que:

$$F_1(|0\rangle) = \frac{1}{\sqrt{2}}(e^0|0\rangle + e^0|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = H(|0\rangle),$$

$$F_1(|1\rangle) = \frac{1}{\sqrt{2}}(e^0|0\rangle + e^{\pi i}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H(|1\rangle)$$

Si dos aplicaciones lineales coinciden sobre los elementos de una base, se puede afirmar que son coincidentes, luego $F_1 = H$.

Para un n cualquiera, se verifica que $F_n(|0\rangle) = W_n(|0\rangle)$, pero las transformaciones no son coincidentes.

---

4. Se pretende factorizar N=221 con el algoritmo de Shor y se elige aleatoriamente $a = 11$. Entonces

a) El periodo de $f(k) = 11^k$ mod 221 es 48 y por lo tanto $mcd(11^{24}+1, 221)$ es un factor de 221.

El periodo de $f(k) = 11^k$ mod 221 es 48, ya que $k = 48$ es el menor entero positivo tal que $11^k \text{mod } 221 = 1$.

Con el algoritmo de Euclides se puede calcular $mcd(11^{24} + 1, 221) = 17$, que evidentemente es un factor propio de 221.

---

5. El algoritmo de Shor propone la utilización de computación cuántica para:

b) Calcular el periodo de una función del tipo $f(k) = a^k \text{mod } N$.

La idea es elegir a alatoriamente entre 1 y $N - 1$ y usar la QFT para calcular el periodo de $f(k) = a^k \text{mod } N$.