Universidad Simón Bolívar
CI-5651 - Diseño de Algoritmos I
Prof. Ricardo Monascal

Resuelto por:
Christopher Gómez

Tarea 10: Algoritmos Cuánticos

1. Se desea que ejecute una simulación del algoritmo de Shor para $N = 21$. Para calcular las amplitudes que obtendría la QFT, puede usar la DFT (Transformada Discreta de Fourier clásica).

   Siga iterando hasta que se cumpla alguna de estas condiciones:

   (a) Se encontró algún factor no trivial para N.

   (b) Se han probado ya 10 valores de x, sin éxito.

   Nota 1: En todo momento, simule las operaciones sobre registros cuánticos de manera clásica (tratando tales superposiciones como una lista de valores y usando algún generador de números aleatorios cuando requiera colapsar alguna de estas).

   Nota 2: Puede usar un generador de números aleatorios online o alguno que venga con un lenguaje de su elección.

   - Escogemos un valor aleatorio para x entre 1 y $N - 1$.

     $$x = 8$$

   - Definimos n una potencia de 2 mayor o igual a 21:

     $$n = 32$$

   - Los registros simulados son:
     - `r1 = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19]`.
     - `r2 = [1, 8, 1, 8, 1, 8, 1, 8, 1, 8, 1, 8, 1, 8, 1, 8, 1, 8, 1, 8]` $(x^{r1} \bmod n)$.

   - Repetimos $s = 2\lg(32) = 10$ veces:
     - FFT(`r1`) = `[90, 0, 0, 0, 0, 0, 0, 0, 0, 0, 70, 0, 0, 0, 0, 0, 0, 0, 0, 0]`, el muestreo cuántico colapsa a **0**.
     - FFT(`r1`) = `[160, 20, 160, 2000000000000014, 160, 20, 160, 2000000000000014, 160, 20, 160, 20, 160, 2000000000000014, 160, 20, 160, 2000000000000014, 160, 20]` el muestreo cuántico colapsa a **16**.
     - FFT(`r1`) = `[1800, 2.71e-15, 21.49, 3.74e-15, 4.82e-14, 0, 4.82e-14, 3.74e-15, 21.49, 2.71e-15, 1400, 2.71e-15, 21.49, 3.74e-15, 4.82e-14, 0, 4.82e-14, 3.74e-15, 21.49, 2.71e-15]` el muestreo cuántico colapsa a **0**.
     - FFT(`r1`) = `[3200, 400, 3200, 400, 3200, 400, 3200, 400, 3200, 400, 3200, 400, 3200, 400, 3200, 400, 3200, 400, 3200, 400]` el muestreo cuántico colapsa a **6**.
     - FFT(`r1`) = `[36000, 0, 46, 2.88e-13, 0, 0, 0, 2.49e-13, 3.31e-13, 0, 28000, 0, 3.31e-13, 2.49e-13, 0, 0, 0, 2.88e-13, 46, 0]` el muestreo cuántico colapsa a **0**.
     - FFT(`r1`) = `[64000, 7999.99, 64000, 8000, 64000, 8000, 64000, 8000, 64000, 7999.99, 64000, 7999.99, 64000, 8000, 64000, 8000, 64000, 8000, 64000, 7999.99]` el muestreo cuántico colapsa a **12**.
     - FFT(`r1`) = `[720000, 2.41e-12, 1.19e-11, 8.67e-13, 5.76e-12, 0, 5.76e-12, 8.67e-13, 1.19e-11, 2.41e-12, 560000, 2.41e-12, 1.19e-11, 8.67e-13, 5.76e-12, 0, 5.76e-12, 8.67e-13, 1.19e-11, 2.41e-12]` el muestreo cuántico colapsa a **10**.

- $\mathrm{FFT}(\mathtt{r1}) =$ `[1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000, 1280000, 160000]` el muestreo cuántico colapsa a **6**.
- $\mathrm{FFT}(\mathtt{r1}) =$ `[14400000, 0, 0, 0, 0, 0, 0, 0, 0, 0, 11200000, 0, 0, 0, 0, 0, 0, 0, 0, 0]` el muestreo cuántico colapsa a **0**.
- $\mathrm{FFT}(\mathtt{r1}) =$ `[25600000, 3200000, 25600000, 320000000000002, 25600000, 3200000, 25600000, 320000000000002, 25600000, 3200000, 25600000, 3200000, 25600000, 320000000000002, 25600000, 3200000, 25600000, 320000000000002, 25600000, 3200000]` el muestreo cuántico colapsa a **6**.

- Así, $g = \mathrm{mcd}(0, 16, 0, 6, 0, 12, 10, 6, 0, 6) = 2$.
- $\frac{21}{2} = 10$ es **par**, devolvemos entonces $\mathrm{mcd}\left(8^5 + 1, 21\right) = \mathrm{mcd}(32769, 21) = \mathbf{7}$.
- Se halló en 1 intento un factor no trivial de 21: **7**, y podemos hallar el otro haciendo $\frac{21}{7} = 3$.

Hemos hallado así los factores primos de 21: **3** y **7**.

2. Cree algún buen meme que tenga que ver con alguna parte del curso.

   Puede ser, por ejemplo, sobre alguno de los temas que vimos o sobre la experiencia en general de la materia. Lo que sea que los inspire y les parezca cómico.

   Nota: Diga si puedo compartirlo anónimamente en el grupo de Telegram y/o redes sociales.

Sí se puede compartir.