Procesamiento Cuántico de la Información - C. Cormick, FING - 1er sem. 2025

Práctico 4 - Algoritmo de Grover, transformada de Fourier y algoritmo de factorización de Shor

1. **Proyectores.** En un espacio vectorial complejo, un proyector es un operador P que satisface $P^2 = P = P^\dagger$. Estos operadores en general NO corresponden a compuertas, dado que no corresponden a matrices unitarias (no son inversibles ni preservan la norma, excepto en el caso trivial $P = I$).
   (a) Mostrar que los autovalores de un proyector solo pueden ser 0 o 1 (notar que si el único autovalor es 1, entonces $P = I$; si el único autovalor es 0, entonces $P = 0$).
   (b) Mostrar que si P es un proyector, entonces $I - P$ también lo es.
   (c) Mostrar que si P es un proyector, entonces $I - 2P$ es una operación que puede corresponder a una compuerta. Indicar cuáles son los posibles autovalores de $I - 2P$ y cuál es la degeneración de cada autovalor en relación con las propiedades de P.

2. **Proyectores de norma 1.**
   (a) Mostrar que dado el estado normalizado $|\psi\rangle$, el operador $P_\psi = |\psi\rangle\langle\psi|$ es un proyector.
   (b) Considerar a modo de ejemplo un espacio de dimensión 3 y escribir explícitamente la forma matricial del proyector que corresponde a cada elemento de la base.
   (c) Mostrar que el efecto de P_ψ es proyectar sobre el eje correspondiente al estado $|\psi\rangle$, es decir, dado un cierto estado $|\xi\rangle$, al aplicar P_ψ sobre él las componentes paralelas a $|\psi\rangle$ se mantienen inalteradas, mientras que las componentes ortogonales a $|\psi\rangle$ se anulan.

3. **Compuertas de fase de un qubit.** La compuerta Z es un caso particular de una familia de compuertas de fase de un qubit de la forma $U_\varphi = |0\rangle\langle 0| + e^{i\varphi}|1\rangle\langle 1|$.
   (a) Mostrar que U_φ es unitaria para un ángulo φ arbitrario.
   (b) Hallar los autovalores y autovectores de U_φ.
   (c) Considerar la compuerta $S = U_{\pi/2}$ y mostrar que al elevarla al cuadrado se obtiene Z.
   (d) Considerar la compuerta $T = U_{\pi/4}$ y mostrar que al elevarla al cuadrado se obtiene S, y a la cuarta se obtiene Z. Nota: Cualquier operación unitaria general se puede aproximar con precisión arbitraria usando solo H, $CNOT$, y T (aunque esta implementación no es eficiente).

   Ojo! A las compuertas S y T se las llama a veces"$\pi/4$" y "$\pi/8$" respectivamente por razones históricas poco afortunadas.

4. **Sumas geométricas de fases.**
   (a) Representar en el plano complejo todos los números de la forma $e^{2\pi ik/5}$ con $k = 0, 1, 2, 3, 4$. Ver geométricamente por qué la suma de esos cinco números debe dar cero.
   (b) Calcular la suma

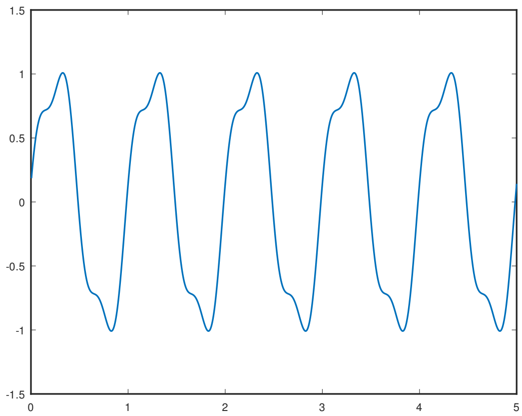
   $$\sum_{j=0}^{N-1} e^{2\pi ijk/N}$$

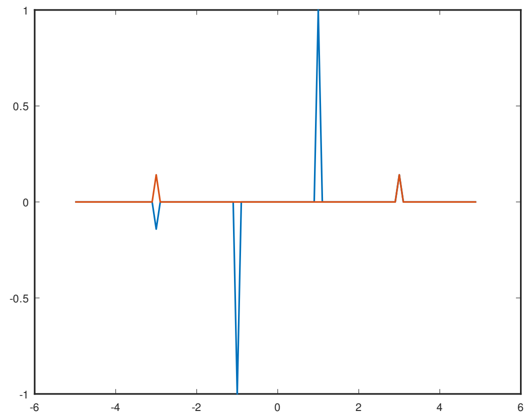
   donde k y N son dos números naturales arbitrarios. Ayuda: si $x \neq 1$, vale usar la expresión

   $$\sum_{j=0}^{N-1} x^j = \frac{1 - x^N}{1 - x}$$

5. **Transformada de Fourier y análisis de señales**.

El siguiente es un ejemplo de una función oscilatoria junto a su transformada de Fourier:





A través de la transformada podemos averiguar que la función es de la forma $f(x) = \sin(2\pi x) + 0.2\sin(6\pi x + \pi/2)$ (nos muestra cuáles son las frecuencias que aparecen en la señal, sus respectivas amplitudes y sus fases).

La transformada usa que al multiplicar funciones tipo seno y coseno, o tipo $e^{i\alpha x}$, la integral promedia a cero cuando las frecuencias son diferentes pero no cuando son iguales (¡esto no pretende ser una explicación rigurosa! quien quiera saber más, pregunte por material extra).

Entrar a: https://www.projectrhea.org/rhea/index.php/Fourier_analysis_in_Music y comparar la descomposición de Fourier correspondiente al sonido de distintos instrumentos musicales. ¿Qué instrumento produce el "la" más "limpio"? (notar que la amplitud de la nota base está representada sobre el eje vertical). ¿En qué instrumento se sienten más fuerte los armónicos?

6. **Transformada de Fourier discreta.** Dado un arreglo de N números complejos $x_0, x_1, \ldots, x_{N-1}$, se define su transformada de Fourier como la operación que retorna un arreglo de N números complejos $y_0, y_1, \ldots y_{N-1}$ dados por:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$$

   (a) Considerar el caso $N = 20$, y dos secuencias dada por $x_j = e^{-2\pi i m j/N}$, con $j = 0, 1, \ldots, N-1$, y tomando los casos $m = 1$ y $m = 5$. Graficar las secuencias, ya sea descomponiendo x_j en sus partes reales e imaginarias o marcando los sucesivos puntos sobre el plano complejo. Calcular las transformadas de Fourier de cada secuencia e interpretar el resultado.

   (b) Verificar (para el caso general) que la inversa de la transformada de Fourier se obtiene cambiando i por $-i$ en la transformación, es decir que vale:

$$x_l = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k e^{-2\pi i l k/N}$$

7. **Transformada de Fourier cuántica.** Es una transformación unitaria que actúa sobre los elementos de la "base computacional" en la forma:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

donde $j, k \in \{0, 1, \ldots, N-1\}$.

   (a) Mostrar que cuando aplico esta transformación sobre un estado general de la forma:

$$|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$$

obtengo un estado de la forma

$$|\tilde{\psi}\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$$

donde los elementos y_k corresponden a la transformada de Fourier discreta de los x_j.

(b) Considerar el caso de tres qubits, y escribir explícitamente la forma del circuito completo que realiza la transformada de Fourier cuántica. Aplicar este circuito sobre un sistema inicialmente preparado en el estado computacional $|j = 5\rangle$, y verificar que el resultado sea el correcto. Implementar en el simulador IBM y corroborar que ande todo bien.

8. **Factorización y período de la exponenciación modular.** Hallar los factores del número $N = 91$ usando el período de la función $F_x(j) = x^j \bmod N$ para distintos valores de $x \in \{2, 3, \ldots, N-1\}$.