La computación cuántica es un área de la informática que utiliza las leyes de la mecánica cuántica, en particular la superposición de estados y el entrelazamiento cuántico, para abordar problemas que resultan difíciles o muy costosos para las computadoras clásicas. En esta guía haremos una breve introducción a este campo.

Computación clásica

1 Compuertas básicas

Las compuertas lógicas clásicas son los bloques fundamentales de la computación digital. Un conjunto funcionalmente completo de compuertas, es decir, un conjunto de compuertas lógicas con el que se puede construir cualquier función lógica booleana, está dado por las compuertas AND, OR y NOT. Claude Shannon probó que estas compuertas pueden implementarse a través de circuitos electrónicos[1].

(a) Usando el conjunto funcionalmente completo de compuertas dado, diseñar un circuito lógico que implemente la función $f(a, b, c) = (a \wedge \neg b) \vee (b \wedge c)$.

(b) Expresar esta función utilizando únicamente compuertas NAND.

2 Máquina de Turing

Una máquina de Turing es un modelo teórico fundamental de la computación. Está compuesta por una cinta infinita dividida en celdas, un cabezal de lectura/escritura que se desplaza sobre ella, y un conjunto finito de estados. Su principal importancia radica en que permite definir formalmente el concepto de computabilidad, ya que puede simular cualquier proceso que sea computacionalmente realizable.

(a) Escribir el programa de una máquina de Turing que dado un número binario x calcule la función constante $f(x) = 1$.

(b) Escribir el programa de una máquina de Turing que determine si una cadena binaria contiene un número par de unos.

3 Complejidad computacional

La teoría de la complejidad computacional clasifica los problemas según la cantidad de recursos necesarios para resolverlos (tiempo, espacio, etc.). Las clases P, NP y NP-completo son fundamentales para entender qué se puede resolver eficientemente.

Les proponer leer sobre la definición de estas clases de complejidad y clasificar los siguientes problemas en las clases P, NP o NP-completo:

(a) Factorización de un número entero.

(b) Problema del viajante.

(c) Búsqueda binaria en un arreglo ordenado.

[1] Claude E. Shannon. *A symbolic analysis of relay and switching circuits.* Transactions of the American Institute of Electrical Engineers, vol. **57** (1938), pp. 713–723.

Computación cuántica

4 **Algoritmo de Deutsch**

El algoritmo de Deutsch (ver figura) fue el primero en mostrar una ventaja cuántica sobre algoritmos clásicos. Determina si una función binaria $f : \{0,1\} \to \{0,1\}$ es constante o balanceada con una sola evaluación.

Simular el algoritmo para una función génerica y verificar que cuando se empieza con el estado $|0\rangle$ el resultado al final permite distinguir si la función es constante o balanceada. De forma grandilocuente, podemos decir que este algoritmo nos permite obtener el periodo de la función. Hallar periodos es importante dado que el problema de factorización de un número tiene su mayor complejidad en la búsqueda del periodo de una función, algo para lo que las computadoras cuánticas son más eficientes que las clásicas.

5 **Algoritmo de Shor**

El algoritmo de Shor (1994) es un algoritmo cuántico que factoriza números enteros en tiempo polinomial, resolviendo eficientemente un problema que es exponencialmente difícil para computadoras clásicas.

Para simplificar la presentación, consideremos un número N que es producto de dos números primos. Para hallar dichos factores primos, se deben realizar los siguientes pasos:

1. Elige un natural aleatorio $a < N$.
2. Calcula el periodo r de la función $f(x) = a^x \bmod N$.
3. Si r es par y $a^{r/2} + 1 \neq 0 \bmod N$, entonces los factores de N son GCD $\left(a^{r/2} \pm 1, N\right)$.
4. Si el procedimiento anterior falla, repetir con otro valor de a.

Les proponemos utilizar este algoritmo para hallar a mano los factores primos de $N = 35$.

Como mencionamos en el ejercicio anterior, las computadoras cuánticas son buenas calculando periodos, por lo que el paso 2 del algoritmo de Shor (el que más tiempo consume) se puede acelerar enormemente con el uso de una computadora cuántica.

6 **Teleportación cuántica**

La teleportación cuántica es un protocolo que permite transferir un estado cuántico entre dos sistemas separados, utilizando entrelazamiento y comunicación clásica. Este protocolo suele estar contado en los libros de mecánica cuántica o lo pueden ver también en este video: https://www.youtube.com/watch?v=TY2odT9oHDE

¿Qué sucede con el estado inicial del sistema luego de la aplicación del protocolo?

7 **Codificación superdensa**

Como vimos en clases, la codificación superdensa permite enviar dos bits clásicos usando un solo qubit, si se comparte previamente un par entrelazado. Escribir un observable que puede medir Bob para acceder a los dos bits de información que le envía Alice.