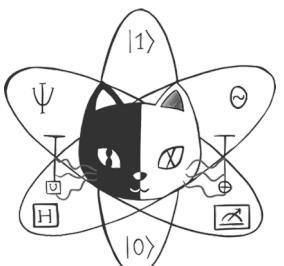
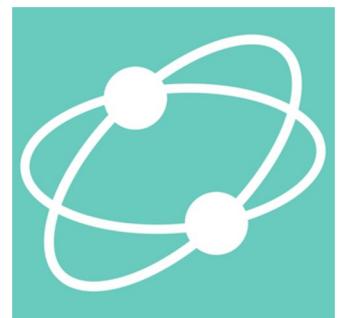
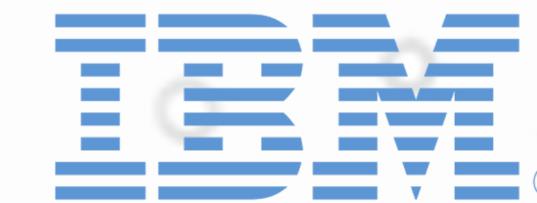


ESCUELA EN ESPAÑOL

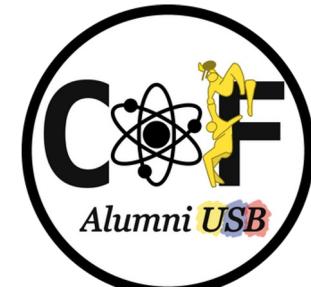
QISKIT FALL FEST



UNIVERSIDAD SIMÓN BOLÍVAR

Algoritmo de Grover: Aplicaciones

Dani Guijo



ESCUELA EN ESPAÑOL

QISKIT FALL FEST

Contenido

- Criptografía
 - Problema de Colisión
 - Algoritmo BHT
- Machine Learning
 - Clústering
 - Clústering Divisivo Cuántico
- Logística
 - Problema de Coloración de Grafos
 - Problema de Ordenamiento de Trabajos



Criptografía

Problema de Colisión

Dada una función $f : \{0, N\} \rightarrow \{0, N\}$ a la que se accede a través de un oráculo, y sabiendo que la función es 2-a-1, encontrar dos elementos x e y tal que $x \neq y$ cuya imagen coincide, $f(x) = f(y)$.

- Utilizando fuerza bruta, se requieren $O(N)$ intentos.
- Con ayuda de la paradoja del cumpleaños, se puede encontrar una colisión cuadráticamente más rápido.
- Combinando esto con el algoritmo de Grover, se puede encontrar en tan solo $O(N^{1/3})$ intentos.

Algoritmo de Brassard-Hoyer-Tapp (BHT)

1. Escoger un subconjunto K del dominio de tamaño $N^{1/3}$, y se construye una tabla L de pares $(x, f(x))$ con x en K .
1. Ordenar L de acuerdo a la segunda entrada de sus elementos.
1. Comprobar si existe una colisión en L . Si es así, finalizar el algoritmo.
1. Utilizar el algoritmo de Grover sobre $H : \{0, N\} \rightarrow \{0, 1\}$, que cumple $H(x) = 1$ si y sólo si existe x_0 en K tal que $(x_0, f(x))$ pertenece a L , y obtener la solución x_1 .
1. Encontrar el par $(x_0, f(x_1))$ en L .
1. La colisión es $\{x_0, x_1\}$.

Machine Learning

Clustering

Dado un dataset $D = \{x_1, \dots, x_n\}$, se debe encontrar una partición del mismo en **clústers**, que minimice la distancia entre elementos de un mismo clúster y maximice la de aquellos que pertenecen a clústers distintos.

- Se tiene acceso a un oráculo que devuelve la **distancia entre dos puntos**.
- Existe un criterio que determina si un clúster es válido.
- Clásicamente, se requiere comprobar todas las distancias por pares, resultando en **$O(n^2)$ llamadas al oráculo**.
- Utilizando Grover, se puede hacer en **solamente $O(n \log(n))$** .

Clustering Divisivo Cuántico

1. Encontrar los dos puntos a distancia máxima en D , $\{x_a, x_b\}$:
 - a. Partiendo de $d_{max} = 0$, utilizar Grover para encontrar dos puntos cuya distancia sea mayor que d_{max} y actualizar su valor.
 - b. Repetir hasta que no se puedan encontrar dichos puntos.
1. Asociar a cada punto del dataset el punto más cercano de $\{x_a, x_b\}$.
1. Definir los clústers D_a y D_b como los puntos asociados a x_a y x_b respectivamente.
1. Repetir el proceso con D_a y D_b .
1. Repetir hasta que los clústers resultantes sean válidos según el criterio elegido.

Logística

Problema de Coloración de Grafos

Dado un grafo G , se deben asignar colores a sus nodos de forma que dos nodos conectados por un arista no tengan el mismo color.

- Este problema se puede representar como un conjunto de **variables que deben obedecer unas cláusulas**.
- Estas variables se pueden **transformar en variables binarias** con sus correspondientes cláusulas.
- Encontrar el valor de estas variables binarias que cumplan las correspondientes cláusulas se conoce como **problema de satisfacibilidad booleano (SAT)**.
- Estas cláusulas definen una **función que actúa como oráculo**.

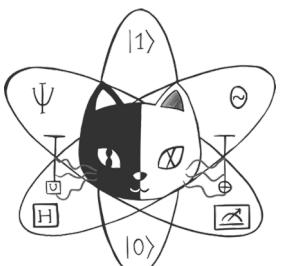
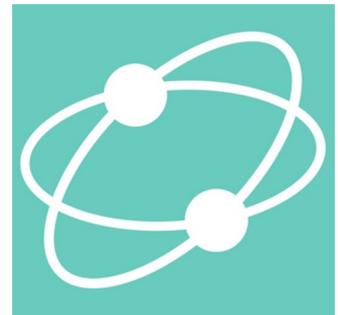
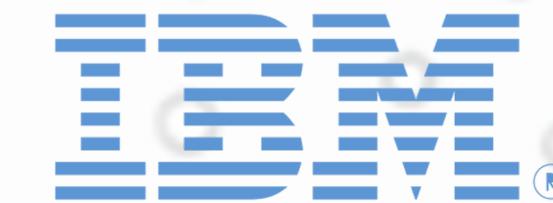
Problema de Ordenamiento de Trabajos

Dado un conjunto de trabajos a realizar $\{v_1, \dots, v_n\}$, unos recursos (humanos, equipamiento...) y unas restricciones sobre su uso, encontrar el orden en que deben realizarse dichos trabajos.

1. Se transforman las variables en variables binarias.
1. Se formulan las correspondientes restricciones, que conforman el oráculo.
1. Se utiliza Grover para encontrar el valor de las variables binarias.
1. Se vuelven a transformar las variables binarias para obtener el orden.

ESCUELA EN ESPAÑOL

QISKIT FALL FEST



QWORLD



UNIVERSIDAD SIMÓN BOLÍVAR

¡Gracias por asistir!



EECC-D4-3968

