Universidad Nacional del Altiplano
Facultad de Ingeniería Estadística e Informática
Docente: Fred Torres Cruz
Estudiante: Ruth Karina Apaza Solis

Trabajo Encargado: Algoritmo de grove

Teoria y diagrama de flujo

¿Qué es el algoritmo de grove?

El algoritmo de Grover es un algoritmo de búsqueda cuántica muy rápido. El algoritmo proporciona una velocidad cuadrática para búsquedas no estructuradas, a diferencia de otros algoritmos clásicos. Se utiliza para buscar en una base de datos sin ordenar. Encuentra con alta probabilidad la única entrada a una función de caja negra que produce un valor de salida particular, utilizando sólo OraizN evaluaciones de la función, donde N es el tamaño del dominio de la función.

1. Explicación

Una de las muchas ventajas que tiene un ordenador cuántico sobre uno clásico es su velocidad superior a la hora de buscar en bases de datos. El algoritmo de Grover ejemplifica esta capacidad.

Lov Grover, informático estadounidense de origen indio, publicó en 1996 un artículo que le dio fama en el campo de la informática cuántica. En su investigación, había trabajado en la optimización de problemas de búsqueda no estructurados.

Grover sugiere aplicar un truco en cuántica conocido como Amplificación de Amplitud para reducir significativamente el tiempo que se tarda en encontrar el ganador w en una base de datos no estructurada. Grover tuvo varias inspiraciones al escribir su artículo. Según Grover, los sistemas cuánticos "se mueven"hacia puntos con bajo potencial. El sistema busca el punto con el potencial más bajo para que el estado acumule más amplitud de probabilidad.

En segundo lugar, había utilizado la ecuación de Schrodinger (que predice el comportamiento futuro de un sistema dinámico. La ecuación se basa en la función de onda y predice sucesos o resultados de forma analítica y precisa). Además, encuentra versiones unitarias de sus matrices de evolución discretizadas. La selección de una fase y la posterior difusión de un estado cuántico inicial o de prueba son los dos elementos esenciales del algoritmo de Grover. Grover utiliza la métrica basada en el estado marcado de naturaleza markoviana pero no unitaria (Una matriz de Markov, también conocida como matriz estocástica, se utiliza

para representar los pasos de una cadena de Markov. Cada entrada de la matriz de Markov representa la probabilidad de un resultado).

Según Grover, una operación de búsqueda puede presentarse utilizando una función f(x) que trabaja sobre el elemento x, si resuelve la búsqueda como exitosa entonces f(x)=1. Si el elemento x no se encuentra entonces f(x)=1. Si el elemento x no se encuentra entonces f(x)=0 . La computación cuántica se puede utilizar para resolver el problema de búsqueda no estructurada en ON que es muy eficiente en comparación con los algoritmos de búsqueda clásicos.

Otra ventaja del algoritmo de Grover es que funciona en sólo O(N log N) puertas. Grover utiliza el concepto de Oráculo, que es como una operación de caja negra que toma una entrada binaria de n bits y genera m bits. Asimismo sus operadores de difusión dan una inversión sobre la media de forma que los pequeños pasos a escala infinita se vuelven medibles.

2. Pasos del algoritmo de grove

El Algoritmo de Grover consta de dos pasos clave (el oráculo y la inversión sobre la media) que le permiten buscar en una base de datos una solución deseada:

El primer paso, el oráculo, es responsable de marcar los estados deseados en el espacio de búsqueda. Logra esto introduciendo un cambio de fase de -1 a la amplitud de los estados objetivo, mientras deja los otros estados sin cambios. El oráculo está diseñado en base al conocimiento del problema en cuestión y el espacio de búsqueda específico. El objetivo es construir un oráculo que pueda identificar de manera eficiente los estados objetivo y distinguirlos de los demás estados.

Para ilustrar el paso del oráculo, consideremos un ejemplo simple. Supongamos que tenemos una base de datos con N artículos y queremos encontrar un artículo específico. En el algoritmo de búsqueda cuántica, cada elemento de la base de datos está representado por un estado cuántico. El oráculo marcará el elemento deseado introduciendo un cambio de fase de -1 en su amplitud, mientras deja los demás elementos sin cambios. Este cambio de fase invierte efectivamente el signo de la amplitud del elemento deseado, lo que facilita su identificación durante los pasos posteriores del algoritmo.

El segundo paso del algoritmo de Grover es la inversión sobre la media. Este paso es responsable de amplificar la amplitud de los estados marcados mientras suprime las amplitudes de los otros estados. Lo logra reflejando las amplitudes sobre la amplitud media de todo el espacio de búsqueda. La amplitud media se calcula tomando el promedio de todas las amplitudes en el espacio de búsqueda.

Para comprender mejor la inversión sobre el paso medio, continuemos con nuestro ejemplo anterior. Después de aplicar el oráculo, las amplitudes de los estados marcados se han modificado, pero aún son relativamente pequeñas en comparación con las amplitudes de los otros estados. La inversión sobre el paso medio amplificará las amplitudes de los estados marcados y suprimirá las amplitudes de los otros estados. Este proceso de amplificación y supresión se logra reflejando las amplitudes sobre la amplitud media. Al aplicar repetidamente la inversión sobre el paso medio, las amplitudes de los estados marcados continuarán

aumentando, mientras que las amplitudes de los otros estados disminuirán. Este proceso de amplificación y supresión eventualmente conduce a una alta probabilidad de medir los estados marcados en el paso final del algoritmo.

El algoritmo de Grover consta de dos pasos principales: el oráculo y la inversión sobre la media. El oráculo es responsable de marcar los estados deseados en el espacio de búsqueda, mientras que la inversión sobre la media amplifica las amplitudes de los estados marcados y suprime las amplitudes de los otros estados. Estos pasos trabajan juntos para buscar de manera eficiente en bases de datos no estructuradas y proporcionar una aceleración cuadrática sobre los algoritmos de búsqueda clásicos.

3. Aplicaciones del Algoritmo de Grover

3.1 Búsqueda en Bases de Datos: El Algoritmo de Grover se puede utilizar para buscar de manera eficiente en grandes bases de datos, incluso cuando los datos no están ordenados. Esto tiene implicaciones en campos como la minería de datos, el aprendizaje automático y la optimización.

3.2 Aprendizaje Automático: El Algoritmo de Grover se puede utilizar para acelerar ciertas tareas de aprendizaje automático, como encontrar soluciones óptimas o patrones en grandes conjuntos de datos.

3.3 Criptografía: Aunque el Algoritmo de Grover no es una amenaza por sí mismo, tiene implicaciones para la criptografía. Tiene el potencial de romper ciertos esquemas de cifrado que se basan en la dificultad de buscar en grandes espacios de claves. Como resultado, el desarrollo de métodos y protocolos de cifrado resistentes a cuántica es un área activa de investigación.

3.4 Simulación de sistemas físicos: Donde la búsqueda de estados específicos del sistema puede ser acelerada por este algoritmo.

Conclusión El algoritmo de Grover es un algoritmo cuántico que permite realizar búsquedas no estructuradas de manera más eficiente que los métodos clásicos. Su principal ventaja es que reduce el tiempo de búsqueda a O(RaizN), logrando una aceleración cuadrática.

Se basa en dos pasos clave: Oráculo: Marca el estado objetivo con un cambio de fase. Inversión sobre la media: Amplifica la probabilidad del estado marcado. Este algoritmo tiene aplicaciones en búsqueda de bases de datos, aprendizaje automático, criptografía y simulación de sistemas físicos.

Conclusión El algoritmo de Grover es un algoritmo cuántico que permite realizar búsquedas no estructuradas de manera más eficiente que los métodos clásicos. Su principal ventaja es que reduce el tiempo de búsqueda a O(RaizN), logrando una aceleración cuadrática.

Se basa en dos pasos clave:

Oráculo: Marca el estado objetivo con un cambio de fase. Inversión sobre la media: Amplifica la probabilidad del estado marcado. Este algoritmo tiene aplicaciones en búsqueda de bases de datos, aprendizaje automático, criptografía y simulación de sistemas físicos.

Diagrama de flujo

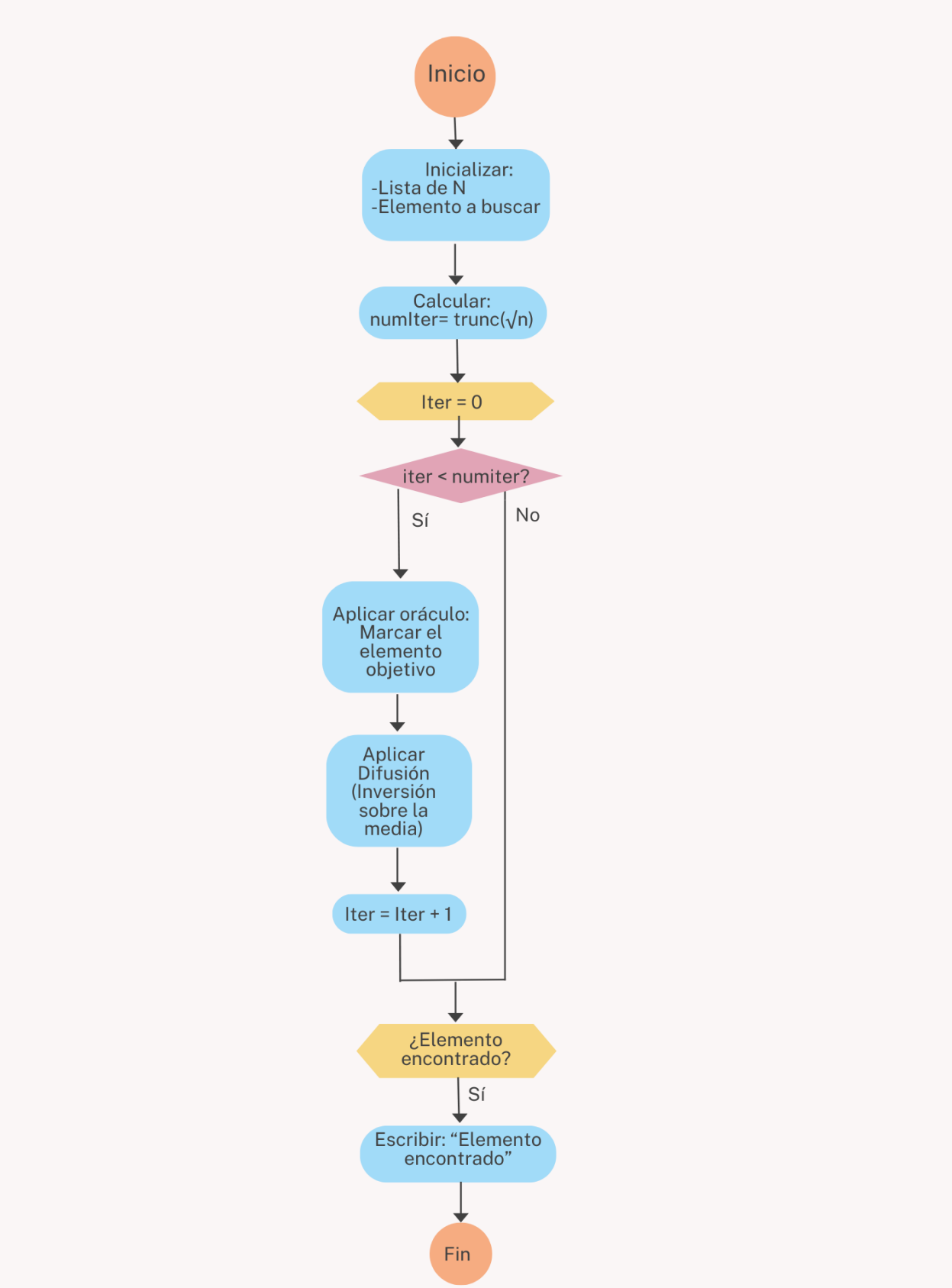

Figura 1: Diagrama de flujo

Referencias

[1] Grover, L. K. (1996b, mayo 29). A fast quantum mechanical algorithm for database search. arXiv.org. https://arxiv.org/abs/quant-ph/9605043

[2] Search — arXiv e-print repository. (s. f.). https://arxiv.org/search/?searchtype=all&query=Grover%27s+algorithm&abstracts=show&size=50&order=announced_date_first