TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN 3

Nghiên cứu về tính toán lượng tử và Áp dụng thuật toán Grover trong tìm kiếm

Đỗ Minh Đức
duc.dm200158@sis.hust.edu.vn

Ngành: Khoa học máy tính

Giảng viên hướng dẫn: ThS. Ngô Văn Linh _____

Chữ kí GVHD

Khoa: Khoa học máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 9/2023

LỜI CẢM ƠN

Đầu tiên và trên hết, em xin gửi lời cảm ơn chân thành tới giáo viên hướng dẫn, thầy Ngô Văn Linh, với sự kiên nhẫn và sự hướng dẫn tận tâm đã giúp em đi sâu vào chủ đề và phát triển khả năng nghiên cứu cũng như tư duy phân tích. Những lời khuyên và góp ý của thầy đã góp phần quan trọng để đưa đề tài này đến một tầm cao mới.

Em cũng xin bày tỏ lòng biết ơn đến tất cả những nguồn tài liệu và nguồn thông tin mà em đã sử dụng trong quá trình nghiên cứu. Sự đa dạng và phong phú của các nguồn tài liệu này đã giúp chúng tôi có cái nhìn toàn diện và chi tiết về đề tài.

Một lần nữa, em xin chân thành cảm ơn tất cả những người đã đồng hành cùng em trong hành trình này. Những lời cảm ơn này không thể nào bày tỏ hết lòng biết ơn chân thành của em. Xin chân thành cảm ơn và kính chúc mọi điều tốt lành đến tất cả mọi người.

Trân trọng,

Đức

Đỗ Minh Đức

TÓM TẮT NỘI DUNG ĐỒ ÁN

Đồ án này tập trung vào nghiên cứu và áp dụng tính toán lượng tử, đặc biệt là thuật toán Grover, trong bài toán tìm kiếm. Tính toán lượng tử là một lĩnh vực nổi bật trong khoa học máy tính, hứa hẹn mang lại khả năng tính toán vượt trội so với máy tính cổ điển trong nhiều ứng dụng. Thuật toán Grover đặc biệt phù hợp với bài toán tìm kiếm trong danh sách không có cấu trúc cụ thể.

Đồ án này bao gồm các bước chính như sau:

- Nghiên cứu cơ bản về tính toán lượng tử: Để hiểu cơ chế hoạt động của máy tính lượng tử, em đã tìm hiểu về nguyên lý lượng tử và sử dụng ngôn ngữ lập trình lượng tử như Qiskit để lập trình máy tính lượng tử.
- Triển khai thuật toán Grover: Xây dựng một phiên bản của thuật toán Grover sử dụng ngôn ngữ lập trình lượng tử. Đây là một bước quan trọng để áp dụng thuật toán vào việc tìm kiếm thực tế.
- Thực hiện thí nghiệm và đánh giá hiệu suất: Em đã thực hiện thí nghiệm bằng cách áp dụng thuật toán Grover vào bài toán tìm kiếm trong các tập dữ liệu mẫu. Kết quả từ các thí nghiệm đã được thu thập và phân tích để đánh giá hiệu suất của thuật toán Grover so với các phương pháp tìm kiếm cổ điển.
- So sánh và kết luận: Kết quả của đồ án cho thấy sự hiệu quả của thuật toán Grover trong việc tìm kiếm so với các phương pháp cổ điển. Em đã đưa ra những nhận xét và kết luận về tiềm năng của tính toán lượng tử trong lĩnh vực tìm kiếm và tối ưu hóa thông tin.

Cuối cùng, đồ án này giúp cung cấp một cái nhìn tổng quan về tính toán lượng tử và áp dụng của nó trong bài toán tìm kiếm. Nó cũng đặt ra câu hỏi về những tiềm năng và hạn chế của tính toán lượng tử trong các ứng dụng thực tế và khám phá các hướng phát triển tiềm năng cho lĩnh vực này.

Sinh viên thực hiện

(Ký và ghi rõ họ tên)

ABSTRACT

This project focuses on the research and application of quantum computing, particularly the Grover algorithm, in the context of search problems. Quantum computing is a prominent field in computer science, promising superior computational capabilities compared to classical computers in various applications. The Grover algorithm, in particular, is well-suited for unstructured search problems.

The project encompasses the following key steps:

- Fundamental Quantum Computing Research: To understand the workings of quantum computers, we delved into quantum principles and employed quantum programming languages like Qiskit for quantum computer programming.
- Grover Algorithm Implementation: We constructed a quantum version of the Grover algorithm using a quantum programming language. This implementation was a crucial step in applying the algorithm to real-world search problems.
- Experimentation and Performance Evaluation: Through experiments, we applied the Grover algorithm to search problems using sample datasets. Results from these experiments were collected and analyzed to assess the algorithm's performance compared to classical search methods.
- Comparison and Conclusion: The project's outcomes demonstrate the efficiency of the Grover algorithm in search problems relative to classical methods. We provide insights and conclusions regarding the potential of quantum computing in the field of search and information optimization.

In conclusion, this project offers an overview of quantum computing and its applications in search problems. It also raises questions about the potential and limitations of quantum computing in practical applications and explores potential directions for further development in this field.

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

1.1 Đặt vấn đề

Trong thời đại hiện đại, khi dữ liệu và thông tin ngày càng trở nên khối lượng lớn và phức tạp, khả năng tìm kiếm hiệu quả đã trở thành một yếu tố quan trọng đối với sự thành công trong nhiều lĩnh vực khác nhau. Việc nhanh chóng và chính xác tìm kiếm thông tin trong cơ sở dữ liệu, bản đồ gen, tìm kiếm trên mạng, và nhiều bài toán khác đã trở thành một thách thức lớn.

Trong lĩnh vực khoa học máy tính, nghiên cứu và phát triển các thuật toán tìm kiếm là một phần quan trọng của công cuộc tối ưu hóa và hiệu suất tính toán. Máy tính cổ điển đã tiến hóa và cải thiện đáng kể trong việc xử lý dữ liệu, nhưng vẫn tồn tại một giới hạn về hiệu suất trong việc tìm kiếm thông tin trong các tập dữ liệu lớn và không cấu trúc.

Tính toán lượng tử, một lĩnh vực mới mẻ và hứa hẹn trong khoa học máy tính, đã đưa ra một câu hỏi đầy thách thức: Liệu chúng ta có thể sử dụng tính toán lượng tử để giải quyết các bài toán tìm kiếm một cách hiệu quả hơn? Thuật toán Grover, một trong những thuật toán quan trọng nhất trong tính toán lượng tử, đặc biệt được thiết kế để tối ưu hóa việc tìm kiếm trong danh sách không có cấu trúc cụ thể. Tuy nhiên, hiệu suất và tiềm năng thực sự của thuật toán Grover trong việc tìm kiếm còn đang cần được nghiên cứu và đánh giá một cách cụ thể.

Trong phần tiếp theo của đồ , chúng ta sẽ nghiên cứu tính toán lượng tử và áp dụng thuật toán Grover vào bài toán tìm kiếm. Em sẽ đánh giá hiệu suất của thuật toán này và so sánh với các phương pháp tìm kiếm truyền thống, nhằm khám phá tiềm năng của tính toán lượng tử trong tối ưu hóa việc tìm kiếm thông tin trong thế giới số ngày càng phát triển.

1.2 Các giải pháp hiện tại và hạn chế

Trước khi khám phá tiềm năng của tính toán lượng tử trong việc tìm kiếm, chúng ta cần xem xét các giải pháp hiện tại và những hạn chế mà chúng đang đối mặt. Dưới đây là một số giải pháp phổ biến và những hạn chế của chúng:

- Tìm kiếm tuyến tính: Phương pháp tìm kiếm này đơn giản và dễ hiểu, nhưng có độ phức tạp tăng theo tỷ lệ tuyến tính với kích thước của tập dữ liệu. Điều này làm cho nó không hiệu quả khi tìm kiếm trong các tập dữ liệu lớn.
- Tìm kiếm nhị phân: Phương pháp tìm kiếm nhị phân cải thiện đáng kể so với tìm kiếm tuyến tính, nhưng vẫn có độ phức tạp O(log n) trong trường hợp tìm kiếm trong danh sách đã sắp xếp. Đối với danh sách không có cấu trúc hoặc

đã sắp xếp theo thứ tự ngẫu nhiên, đây vẫn chỉ là một giải pháp trung bình.

- Tối ưu hóa phân tán: Trong các hệ thống phân tán, tìm kiếm thông tin có thể trở nên phức tạp hơn do cần tương tác với nhiều máy chủ. Giải pháp hiện tại thường liên quan đến sử dụng các giao thức phân tán và cơ sở dữ liệu phân tán, nhưng vẫn cần đối mặt với vấn đề hiệu suất.
- Hạn chế cơ học: Máy tính cổ điển dựa vào cơ học, và sự phát triển của chúng đã gặp hạn chế về việc tăng tốc tính toán và giảm kích thước. Điều này đặt ra hạn chế về khả năng tìm kiếm trong các tập dữ liệu lớn và phức tạp.

Tính toán lượng tử có tiềm năng giải quyết một số hạn chế của các giải pháp truyền thống. Thuật toán Grover, ví dụ, hứa hẹn có độ phức tạp O(n), đây là một tiến bộ lớn so với tìm kiếm tuyến tính và tìm kiếm nhị phân. Tuy nhiên, cũng cần xem xét những hạn chế của tính toán lượng tử, như sự phụ thuộc vào phân tích của thuật toán và sự yếu đuối của các hệ thống lượng tử hiện có.

Đồ án này sẽ đánh giá tiềm năng và hạn chế của tính toán lượng tử, đặc biệt là thuật toán Grover, để tìm hiểu xem liệu chúng có thể cải thiện hiệu suất tìm kiếm thông tin và tối ưu hóa quá trình tìm kiếm trong các tập dữ liệu lớn và phức tạp hơn.

1.3 Mục tiêu và định hướng giải pháp

Mục tiêu chính của đồ án này là khám phá tiềm năng của tính toán lượng tử, đặc biệt là thuật toán Grover, trong việc tối ưu hóa quá trình tìm kiếm thông tin trong các tập dữ liệu lớn và không cấu trúc. Để đạt được mục tiêu này, chúng ta sẽ xác định các định hướng giải pháp cụ thể sau đây:

- Nghiên cứu về tính toán lượng tử: Chúng ta sẽ tiến hành nghiên cứu chi tiết về lý thuyết tính toán lượng tử và nguyên lý hoạt động của thuật toán Grover. Điều này bao gồm việc tìm hiểu về cách làm việc với trạng thái lượng tử, cách thực hiện các cổng lượng tử, và cách sử dụng ngôn ngữ lập trình lượng tử để triển khai thuật toán.
- Triển khai thuật toán Grover: Chúng ta sẽ xây dựng một phiên bản thực thi của thuật toán Grover sử dụng môi trường phát triển lượng tử, ví dụ như Qiskit cho Python. Việc triển khai này sẽ là cơ sở cho việc áp dụng thuật toán vào bài toán tìm kiếm cụ thể.
- Thực hiện thí nghiệm và đánh giá hiệu suất: Chúng ta sẽ thực hiện các thí nghiệm bằng cách áp dụng thuật toán Grover vào bài toán tìm kiếm trong các tập dữ liệu mẫu. Kết quả từ các thí nghiệm này sẽ được thu thập và phân tích để đánh giá hiệu suất của thuật toán Grover so với các phương pháp tìm kiếm

truyền thống.

- So sánh và kết luận: Chúng ta sẽ so sánh kết quả của thuật toán Grover với các phương pháp tìm kiếm cổ điển như tìm kiếm tuyến tính và tìm kiếm nhị phân. Dựa trên các kết quả và phân tích, chúng ta sẽ rút ra những kết luận về tiềm năng của tính toán lượng tử trong tối ưu hóa tìm kiếm thông tin.
- Đề xuất các ứng dụng tiềm năng: Cuối cùng, dự án này sẽ giúp chúng ta xác định các ứng dụng tiềm năng khác của tính toán lượng tử trong lĩnh vực tìm kiếm và tối ưu hóa thông tin, cũng như khám phá các hướng phát triển tiềm năng cho lĩnh vực này.

Mục tiêu chính là xem xét khả năng sử dụng tính toán lượng tử để cải thiện hiệu suất tìm kiếm thông tin và tối ưu hóa quá trình tìm kiếm, đặc biệt là trong ngữ cảnh của thuật toán Grover. Chúng ta hy vọng rằng dự án này sẽ cung cấp cái nhìn sâu hơn về tính toán lượng tử và tiềm năng của nó trong tối ưu hóa các nhiệm vụ tìm kiếm và xử lý thông tin..

1.4 Đóng góp của đồ án

Đồ án này có đóng góp quan trọng và đa chiều trong các khía cạnh sau:

- Nghiên cứu Tính toán Lượng tử: Dự án đã đóng góp vào sự hiểu biết về tính toán lượng tử, nguyên lý hoạt động của máy tính lượng tử, và thuật toán Grover. Điều này đã mở ra cơ hội để áp dụng kiến thức này vào việc tối ưu hóa quá trình tìm kiếm thông tin.
- Triển khai thuật toán Grover: Xây dựng một phiên bản thực thi của thuật toán Grover bằng cách sử dụng môi trường phát triển lượng tử, tạo điều kiện cho việc nghiên cứu và thử nghiệm thực tế.
- Thí nghiệm và Đánh giá hiệu suất: Tiến hành các thử nghiệm để đánh giá hiệu suất của thuật toán Grover trong việc tìm kiếm thông tin trong các tập dữ liệu mẫu. Kết quả thu thập từ các thí nghiệm này đã cung cấp thông tin cụ thể về hiệu suất của thuật toán Grover so với các phương pháp tìm kiếm truyền thống.
- So sánh và Kết luận: Thực hiện việc so sánh kết quả của thuật toán Grover với các phương pháp tìm kiếm cổ điển giúp rút ra các kết luận về tiềm năng của tính toán lượng tử trong việc tối ưu hóa tìm kiếm thông tin.
- Đề xuất ứng dụng tiềm năng: Đề xuất các ứng dụng tiềm năng của tính toán lượng tử trong lĩnh vực tìm kiếm và tối ưu hóa thông tin. Điều này có thể đóng góp vào việc phát triển ứng dụng và công nghệ mới trong tương lai.

Nhờ vào các đóng góp này, đồ án đã mang lại sự hiểu biết sâu sắc hơn về tính

toán lượng tử và tiềm năng của nó trong việc tối ưu hóa quá trình tìm kiếm thông tin, từ đó có thể đóng vai trò quan trọng trong phát triển các ứng dụng hiệu quả hơn trong nhiều lĩnh vực khác nhau.

1.5 Bố cục đồ án

Đồ án này được chia thành các chương sau đây để cung cấp một cái nhìn tổng quan và logic về nội dung:

1. **Chương 1: Giới thiệu**
    - Phần giới thiệu dự án và mục tiêu.
    - Đặt vấn đề và nêu rõ tầm quan trọng của bài toán tìm kiếm thông tin trong ngữ cảnh tính toán lượng tử.
    - Trình bày cấu trúc tổng quan của đồ án.
2. **Chương 2: Nền tảng Lý thuyết**
    - Trình bày kiến thức cơ bản về tính toán lượng tử, bao gồm nguyên tắc hoạt động của máy tính lượng tử, trạng thái lượng tử, cổng lượng tử, và ngôn ngữ lập trình lượng tử.
    - Đánh giá và giải thích thuật toán Grover, tập trung vào cách nó tối ưu hóa quá trình tìm kiếm thông tin.
3. **Chương 3: Đánh giá thực nghiệm**
    - Mô tả quá trình triển khai thuật toán Grover trong môi trường tính toán lượng tử.
    - Thực hiện thí nghiệm để đánh giá hiệu suất của Grover so với các phương pháp tìm kiếm truyền thống.
    - Trình bày và phân tích kết quả thực nghiệm.
4. **Chương 4: Kết luận**
    - Tóm tắt các kết quả quan trọng và những điểm nổi bật trong dự án.
    - Trình bày các hạn chế của dự án và các hướng phát triển trong tương lai.
    - Kết luận tổng quan về tầm quan trọng của tính toán lượng tử trong tối ưu hóa tìm kiếm thông tin

CHƯƠNG 2. NỀN TẢNG LÝ THUYẾT

2.1 Mô hình tính toán lượng tử

2.1.1 Giới thiệu về tính toán lượng tử

Máy tính lượng tử là máy tính mà ở đó thông tin không được lưu trữ dưới dạng bit mà ở dạng bit lượng tử, hay còn gọi là qubit. Nếu như trong máy tính cổ điển, một bit có thể mang giá trị 0 và 1, được biểu diễn tương ứng với mức điện áp thấp hay mức điện áp cao của một linh kiện điện tử, thì đối với máy tính lượng tử, 1 qubit có thể là một hạt lượng tử như photon, electron hoặc mạch siêu dẫn. Để làm việc với những đối tượng này, chúng ta cần sử dụng những nguyên lý của cơ học lượng tử để thực hiện những phép tính và xử lý thông tin. Do tính chất lượng tử đặc biệt, 1 qubit có thể tồn tại ở nhiều trạng thái đồng thời, giúp máy tính lượng tử thực hiện nhiều tính toán song song.

Hiện nay, phát triển máy tính lượng tử trên thế giới đang là một lĩnh vực được nghiên cứu và đầu tư sôi động. Nhiều công ty công nghệ lớn trên thế giới như IBM, Google, Microsoft, Intel, Amazon,... đã đầu tư mạnh vào việc phát triển máy tính lượng tử và đã cho ra mắt một số máy tính lượng tử:

- IBM Q System One: Được giới thiệu bởi IBM, đây là một máy tính lượng tử thương mại đầu tiên trên thế giới, ra mắt vào năm 2019. Máy tính này có 20 qubit và được thiết kế trong một khoang kín với điều kiện nhiệt độ rất thấp để duy trì tính ổn định của qubit.
- Google Quantum Computer (Sycamore): Máy tính lượng tử của Google, còn được gọi là Sycamore, là một máy tính lượng tử mạnh với 53 qubit. Năm 2019, Google tuyên bố rằng Sycamore đã thực hiện một tính toán trong khoảng thời gian 200 giây, mà máy tính cổ điển nếu tính toán sẽ mất khoảng 10.000 năm.
- IonQ Quantum Computer: IonQ là một công ty công nghệ lượng tử có trụ sở tại Mỹ, đã phát triển máy tính lượng tử sử dụng các qubit là các ion bị bẫy. Máy tính của IonQ có thể có tới hàng trăm qubit và được sử dụng cho nghiên cứu và thương mại.
- D-Wave Quantum Annealers: D-Wave là một công ty đầu tiên phát triển máy tính lượng tử thương mại, nhưng máy tính của họ được xem là máy tính lượng tử mạnh nhất, dựa trên kiến trúc của máy tính lượng tử ánh sáng có thể điều khiển (adiabatic quantum computing). D-Wave đã phát triển nhiều phiên bản máy tính với số lượng qubit từ vài chục đến hơn 500 qubit.

Ngoài ra, còn có nhiều dự án và máy tính lượng tử khác đang được phát triển và

nghiên cứu bởi các tổ chức, viện nghiên cứu và công ty trên khắp thế giới. Tuy vậy, việc phát triển máy tính lượng tử còn đối mặt với nhiều thách thức, như việc giải quyết vấn đề nhiễu trong hệ thống lượng tử, tăng cường tính ổn định và độ tin cậy của qubit, cũng như giảm thiểu chi phí và phức tạp trong việc xây dựng máy tính lượng tử.

2.1.2 Mô hình tính toán lượng tử

Tuy máy tính lượng tử sử dụng rất nhiều kiến thức phức tạp trong toán học và vật lý học, cơ sở để phát triển các thuật toán lượng tử đều dựa trên lý thuyết cơ bản của Đại số và Xác suất thống kê.

a, Bit lượng tử - Qubit

Bit là một khái niệm cơ bản trong tính toán và truyền thông cổ điển. Tính toán và thông tin lượng tử cũng được xây dựng dựa trên khái niệm tương tự, bit lượng tử (hay Qubit). Trong phần này chúng ta sẽ tìm hiểu các tính chất của hệ một bit lượng tử và hệ nhiều bit lượng tử, đồng thời so sánh các tính chất đó với các bit cổ điển.

Chúng ta sẽ mô tả qubits là các thực thể toán học (mathematical object) với các tính chất riêng biệt. Việc xử lý các qubit như các thực thể trừu tượng sẽ giúp chúng ta dễ dàng xây dựng cơ sở lý thuyết về tính toán và truyền thông tin lượng tử mà không phụ thuộc vào bản chất vật lý của các qubit.

Tương tự như các bit cổ điển chỉ có 2 trạng thái là 0, hoặc 1, các qubit cũng có các trạng thái của nó. 2 Trạng thái có thể có của qubit (nhưng không phải tất cả) là $|0\rangle$ và $|1\rangle$, chúng ta sẽ nghĩ hai trạng thái này tương ứng với 0 và 1 như các bit cổ điển. Kí hiệu ' $|\rangle$' được gọi là kí pháp Dirac và sẽ được sử dụng nhiều do đây là kí hiệu chuẩn để kí hiệu trạng thái của các qubit trong tính toán lượng tử. Sự khác biệt giữa các bit cổ điển với qubit là ngoài hai trạng thái $|0\rangle$ và $|1\rangle$, các qubit còn có thể tồn tại ở các trạng thái là tổ hợp tuyến tính của các trạng thái, thường được gọi là superpositon:

$$|\psi\rangle=\alpha\ |0\rangle+\beta\ |1\rangle$$

Trong đó α và β là các số phức. Như vậy, ta có thể thấy trạng thái của các qubit là một vector trong không gian vector phức 2 chiều. Các trạng thái đặc biệt $|0\rangle$ và $|1\rangle$ được gọi là các trạng thái cơ sở, 2 trạng thái này lập thành một hệ cơ sở trực giao cho không gian vector này.

Trong máy tính cổ điển, chúng ta hoàn toàn có thể kiểm tra trạng thái một bit, để thu được kết quả 0 hoặc 1. Tuy nhiên, đối với các bit lượng tử, chúng ta không thể kiểm tra trạng thái lượng tử của nó (chúng ta không thể kiểm tra để biết chính

xác giá trị của α và β). Thay vào đó, việc đo các bit lượng tử sẽ cho chúng ta ít thông tin hơn về các qubit. Cụ thể, khi chúng ta đo qubit ở trên, chúng ta sẽ nhận được kết quả là 0 , với xác suất $|\alpha^2|$, hoặc kết quả là 1, với xác suất $|\beta^2|$. Như vậy, $|\alpha^2|$ + $|\beta^2|$ = 1 , do tổng xác suất phải bằng 1.

Như vậy, bao nhiêu thông tin có thể được biểu hiện bởi 1 qubit. Nghịch lý là, có vô hạn các giá trị α và β thỏa mãn điều kiện tổng xác suất là 1, như vậy về mặt lý thuyết 1 qubit có thể lưu trữ vô hạn thông tin. Tuy nhiên, điều này dễ gây nhầm lẫn, do khi chúng ta đo một qubit, chúng ta chỉ có thể nhận được kết quả là 0 hoặc 1. Thêm vào đó, việc đo các qubit sẽ làm các qubit bị sụp đổ, đưa trạng thái các qubit từ superpositon sang các trạng thái đặc biệt. Ví dụ, với qubit ở trên, giả sử sau khi đo, chúng ta nhận được giá trị 0, trạng thái của qubit sẽ chuyển từ trạng thái superposition sang trạng thái $|0\rangle$.

b, Hệ nhiều bit lượng tử

Đối với hệ thống gồm 2 bit cổ điển, trạng thái của 2 bit có thể là 00, 01, 10, và 11. Tương ứng như vậy trong hệ thống gồm 2 qubit, hệ thống cũng có 4 trạng thái cơ sở, được kí hiệu là $|00\rangle$, $|01\rangle$, $|10\rangle$ và $|11\rangle$. 2 qubit cũng có thể tồn tại dưới dạng superposition, là tổ hợp tuyến tính của các trạng thái :

$$|\psi\rangle = \alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$$

Tương tự như trường hợp 1 qubit, kết quả khi ta đo hệ 2 qubit sẽ là x(= 00, 01, 10 hoặc 11) với các xác suất tương ứng là $|\alpha_x^2|$. Đồng thời, trạng thái của 2 qubit sau khi đo sẽ là $|x\rangle$. Đối với hệ nhiều qubit, chúng ta có thể chỉ đo một phần của hệ, việc đo 1 phần của hệ sẽ dẫn tới sự thay đổi của hệ. Ví dụ, đối với hệ 2 qubit, chúng ta có thể tiến hành đo qubit đầu tiên, giả sử chún ta nhận được 0 với xác suất $|\alpha_{00}^2|$ + $|\beta_{01}^2|$, như vậy trạng thái của hệ sau khi đo sẽ là:

$$|\psi\rangle = \frac{\alpha_{00}|00\rangle+\alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}}$$

Một trong các trạng thái quan trọng của 2 qubit là trạng thái Bell hay trạng thái EPR:

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

Đây là một trạng thái quan trọng, là cơ sở của nhiều ứng dụng của tính toán và thông tin lượng tử như quantum teleportation, superdense coding,... Trạng thái Bell có đặc điểm, sau khi chúng ta tiến hành đo qubit đầu tiên, chúng ta sẽ nhận được 1 trong 2 kết quả: 0 với xác suất 1/2, trạng thái sau khi đo là $||00\rangle|$ hoặc 1, với xác suất 1/2, trạng thái sau khi đo là $|11\rangle$. Như vậy, việc đo qubit thứ 2 sẽ cho ta kết quả giống như việc đo qubit thứ nhất. Ta nói hai qubit này tương quan với nhau. Khi ta tiến hành một vài biến đổi với qubit thứ nhất, sự tương quan vẫn được giữ nguyên

đối với qubit thứ hai.

2.2 Tính toán lượng tử

Sự thay đổi diễn ra với các trạng thái lượng tử có thể được miêu tả bằng thuật ngữ tính toán lượng tử. Tương tự như cách mà máy tính cổ điển được xây dựng từ các mạch điện bao gồm dây và các cổng logic, máy tính lượng tử được xây dựng từ các mạch lượng tử bảo gồm dây điện và các cổng lượng tử, có nhiệm vụ vận chuyển và thay đổi trạng thái các qubit. Trong phần này, chúng ta sẽ đề cập đến một vài cổng lượng tử đơn giản.

2.2.1 Cổng 1 qubit

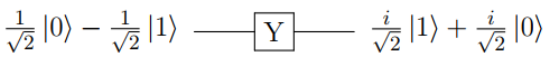
Cổng NOT

Như tên gọi, cổng NOT sẽ làm qubit có trạng thái $|0\rangle$ chuyển sang trạng thái $|1\rangle$ và ngược lại.

Hình 2.1: Cổng NOT

Cổng Y

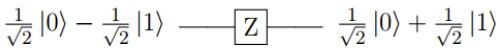
Cổng Y sẽ làm qubit từ trạng thái $|0\rangle$ chuyển sang trạng thái $i|1\rangle$ và từ trạng thái. $|1\rangle$ chuyển sang trạng thái $i|0\rangle$



Hình 2.2: Cổng Y

Cổng Z

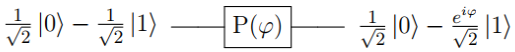
Cổng Z sẽ làm qubit từ trạng thái $|1\rangle$ chuyển sang trạng thái $-|1\rangle$ và giữ nguyên trạng thái $|0\rangle$.



Hình 2.3: Cổng Z

Cổng dịch pha

Cổng dịch pha, kí hiệu là P(ϕ) giữ nguyên trạng thái $|0\rangle$, biến đổi trạng thái $|1\rangle$ thành $e^{i\phi}|1\rangle$

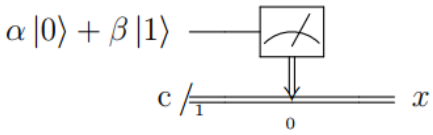


Hình 2.4: Cổng dịch pha

Phép đo

Phép đo không phải là một cổng lượng tử do đây là 1 biến đổi 1 chiều. Phép đo sẽ nhận vào 1 qubit rồi chiếu trạng thái của nó lên các vector cơ sở. Ta sẽ thu được giá trị cổ điển của qubit khi thực hiện phép đo.

Giá trị của x sau khi thực hiện phép đo sẽ bằng 0 với xác suất $|\alpha|^2$, bằng 1 với xác suất $|\beta|^2$, với điều kiện $|\alpha|^2 + |\beta|^2 = 1$.

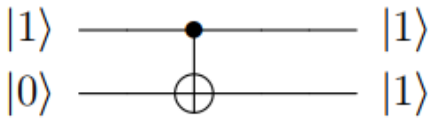


Hình 2.5: Phép đo

2.2.2 Cổng nhiều qubit

Cổng CNOT

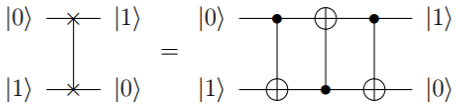
Cổng CNOT (controlled NOT gate) nhận đầu vào là 2 qubit, thực hiện biến đổi NOT lên qubit thứ 2 nếu qubit đầu tiên có trạng thái là $|1\rangle$, ngược lại sẽ giữ nguyên. Cổng CNOT là phiên bản lượng tử của cổng XOR.



Hình 2.6: Cổng CNOT

Cổng hoán vị

Cổng hoán vị dùng để hoán đổi trạng thái của 2 qubit, có thể thực hiện bằng cách dùng cổng CNOT.



Hình 2.7: Cổng hoán vị

2.3 Bài toán tìm kiếm trong lượng tử

Bài toán tìm kiếm trong lượng tử được phát biểu như sau:

Dữ liệu đầu vào: Một danh sách các phần tử, trong đó một phần tử cụ thể được gắn với một chỉ số duy nhất.

Mục tiêu: Tìm ra chỉ số của phần tử cụ thể trong danh sách hoặc xác định rằng phần tử đó không tồn tại trong danh sách.

Phương pháp giải quyết: Sử dụng tính toán lượng tử để tối ưu hóa quá trình tìm kiếm thông tin. Trong trường hợp này, thuật toán Grover là một trong những phương pháp phổ biến nhất được sử dụng để giải quyết bài toán tìm kiếm trong lượng tử. Thuật toán này tối ưu hóa số bước cần thiết để tìm kiếm phần tử so với các phương pháp tìm kiếm cổ điển.

2.4 Thuật toán Grover

Thuật toán Grover được tìm ra bởi Lov Grover vào năm 1996. Về cơ bản, thuật toán Grover là một thuật toán tìm kiếm, cho phép thời gian đi tìm x khi biết f(x) giảm từ O(N) xuống O($\sqrt{N}$). Điều này có nghĩa là, nếu thuật toán hiện tại mất 10,000 ngày thì thuật toán của Grover chỉ mất 100 ngày. Người ta khuyến cáo rằng các hàm mật mã hiện nay cần tăng kích thước của khoá lên gấp đôi, ví dụ từ 128 bit lên 256 bit để tránh bị tấn công bởi Grover's algorithm.

2.4.1 Thuật toán Grover

Các bước của thuật toán được thực hiện như sau. Cho $|s\rangle$ là chồng chập của các trạng thái:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

Toán tử

$$U_s = 2 |s\rangle \langle s| - I$$

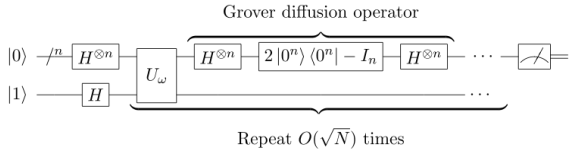
là toán tử truyền thông tin (diffusion operator).

Thuật toán gồm các bước:

1. Khởi tạo hệ thống ở trạng thái:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

2. Thực hiện "Vòng lặp Grover" $r(N)$ lần. Hàm $r(N)$, có độ phức tạp $O(N^{1/2})$, được miêu tả như sau.
   (a) Thực hiện toán tử U_ω.
   (b) Thực hiện toán tử U_s.
3. Thực hiện phép đo . Kết quả của phép đo sẽ là λ_ω với xác suất tiến tới 1 khi $N \gg 1$. Từ λ_ω, ta có thể tìm thấy ω.



Hình 2.8: Mạch lượng tử thể hiện thuật toán Grover

2.4.2 Chứng minh thuật toán Grover

Vòng lặp đầu tiên

Từ định nghĩa, ta có bước khởi tạo:

$$U_s = 2\left|s\right\rangle\left\langle s\right| - I,$$

U_ω có thể được biểu diễn theo cách:

$$U_\omega = I - 2\left|\omega\right\rangle\left\langle\omega\right|.$$

Các bước sau cho thấy những gì xảy ra trong vòng lặp đầu tiên:

$$\langle\omega|s\rangle = \langle s|\omega\rangle = \frac{1}{\sqrt{N}}.$$

$$\langle s|s\rangle = N\frac{1}{\sqrt{N}}\cdot\frac{1}{\sqrt{N}} = 1.$$

$$U_\omega|s\rangle = (I - 2|\omega\rangle\langle\omega|)|s\rangle = |s\rangle - 2|\omega\rangle\langle\omega|s\rangle = |s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle.$$

$$U_s(|s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle) = (2|s\rangle\langle s| - I)(|s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle) = 2|s\rangle\langle s|s\rangle - |s\rangle - \frac{4}{\sqrt{N}}|s\rangle\langle s|\omega\rangle + \frac{2}{\sqrt{N}}|\omega\rangle =$$

$$= 2|s\rangle - |s\rangle - \frac{4}{\sqrt{N}}\cdot\frac{1}{\sqrt{N}}|s\rangle + \frac{2}{\sqrt{N}}|\omega\rangle = |s\rangle - \frac{4}{N}|s\rangle + \frac{2}{\sqrt{N}}|\omega\rangle = \frac{N-4}{N}|s\rangle + \frac{2}{\sqrt{N}}|\omega\rangle.$$

Sau khi 2 toán tử (U_ω và U_s) được sử dụng, giá trị cần tìm đã tăng từ $|\langle\omega|s\rangle|^2 = 1/N$ lên đến $|\langle\omega|U_sU_\omega s\rangle|^2 \approx 9/N$.

CHƯƠNG 3. ĐÁNH GIÁ THỰC NGHIỆM

3.1 Phần mềm mã nguồn mở Qiskit

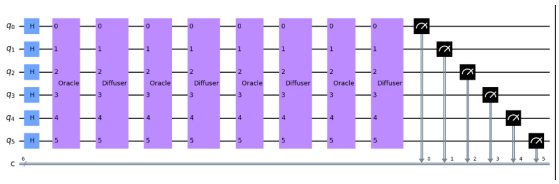
Trong thời đại hiện đại của tính toán lượng tử, việc phát triển và sử dụng các phần mềm mã nguồn mở là rất quan trọng để đảm bảo sự tiến bộ trong lĩnh vực này. Một trong những nền tảng tính toán lượng tử mã nguồn mở hàng đầu hiện nay là Qiskit.

Qiskit là một framework mã nguồn mở phát triển bởi IBM Quantum, được thiết kế để hỗ trợ việc nghiên cứu và phát triển ứng dụng tính toán lượng tử. Được ra mắt vào năm 2017, Qiskit đã nhanh chóng trở thành một trong những công cụ phổ biến nhất trong cộng đồng tính toán lượng tử và đã đóng góp quan trọng vào việc đưa tính toán lượng tử vào ứng dụng thực tế.

Đồ án sử dụng Qiskit để xây dựng chương trình chạy thử nghiệm thuật toán Shor trong môi trường máy tính lượng tử của IBM.

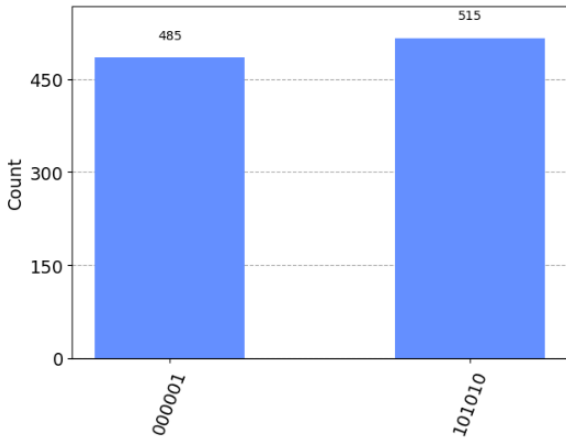
3.2 Chương trình thử nghiệm thuật toán Grover

Trong đồ án này, em sẽ thử nghiệm triển khai mạch lượng tử đánh dấu 2 phần tử '000001' và '101010'. Đầu ra của thuật toán là 1 trong 2 phần tử trên.



Hình 3.1: Mạch lượng tử thử nghiệm

3.3 Kết quả thử nghiệm



Hình 3.2: Kết quả chạy thử nghiệm

Qua hình trên ta có thể thấy, thuật toán Grover với mạch lượng tử trên cho đầu ra là 1 trong hai phần tử được đánh dấu với độ chính xác lên tới 99%.

CHƯƠNG 4. KẾT LUẬN

4.1 Kết luận

Trong đồ án này, em đã nghiên cứu và áp dụng tính toán lượng tử, đặc biệt là thuật toán Grover, vào bài toán tìm kiếm thông tin trong các tập dữ liệu lớn và không có cấu trúc cụ thể. Dưới đây là những điểm quan trọng trong kết luận của đồ án này:

- Tính toán Lượng tử và Thuật toán Grover: Nghiên cứu nguyên lý hoạt động của tính toán lượng tử và triển khai thuật toán Grover. Thuật toán Grover đặc biệt được thiết kế để cải thiện hiệu suất tìm kiếm thông tin trong danh sách không có cấu trúc cụ thể.
- Thử nghiệm và Đánh giá Hiệu suất: Thực hiện các thử nghiệm bằng cách áp dụng thuật toán Grover vào bài toán tìm kiếm trong các tập dữ liệu mẫu. Kết quả cho thấy rằng Grover có độ phức tạp thấp hơn so với tìm kiếm tuyến tính, đặc biệt là trong các tập dữ liệu lớn.
- Ứng Dụng Tiềm Năng: Đề xuất các ứng dụng tiềm năng của tính toán lượng tử trong lĩnh vực tìm kiếm và tối ưu hóa thông tin. Tính toán lượng tử có tiềm năng cải thiện hiệu suất tìm kiếm trong nhiều lĩnh vực ứng dụng, từ tìm kiếm trên web đến xử lý dữ liệu khoa học.

Tuy nhiên, cần lưu ý rằng tính toán lượng tử vẫn còn trong giai đoạn phát triển và đối mặt với một số hạn chế, như sự phụ thuộc vào phân tích của thuật toán và yếu đuối của các hệ thống lượng tử hiện có. Tương lai của tính toán lượng tử trong lĩnh vực tìm kiếm và tối ưu hóa thông tin sẽ đòi hỏi sự nghiên cứu và phát triển tiếp tục để khai thác hết tiềm năng của nó.

4.2 Hướng phát triển trong tương lai

Đồ án này đã mở ra nhiều cơ hội và tiềm năng cho sự phát triển trong lĩnh vực tính toán lượng tử và ứng dụng của nó trong tìm kiếm và tối ưu hóa thông tin. Dưới đây là một số hướng phát triển trong tương lai mà có thể được khám phá:

- Tối ưu hóa Thuật toán Grover: Cần tiếp tục nghiên cứu và phát triển thuật toán Grover để tối ưu hóa hiệu suất của nó. Điều này có thể bao gồm việc xem xét cách cải thiện chi tiết triển khai thuật toán hoặc tìm ra cách sử dụng nó trong các tình huống cụ thể.
- Ứng dụng Thực Tế: Tiếp tục nghiên cứu và phát triển các ứng dụng thực tế của tính toán lượng tử trong việc tìm kiếm và tối ưu hóa thông tin. Các lĩnh

vực như tìm kiếm trên web, tối ưu hóa dữ liệu khoa học, và xử lý hình ảnh có tiềm năng để sử dụng tính toán lượng tử.

- Phát triển Hệ thống Lượng tử: Cần tiến hành nghiên cứu và phát triển các hệ thống lượng tử mạnh mẽ hơn để triển khai thuật toán lượng tử. Điều này bao gồm việc phát triển cả phần cứng lẫn phần mềm để hỗ trợ tính toán lượng tử hiệu quả.
- Học máy và Tối ưu hóa: Kết hợp tính toán lượng tử với các lĩnh vực như học máy và tối ưu hóa để tạo ra các giải pháp mạnh mẽ hơn cho các vấn đề tìm kiếm và tối ưu hóa thông tin.
- Giáo dục và Nhận thức: Xây dựng chương trình giáo dục và tạo ra nhận thức về tính toán lượng tử trong cộng đồng khoa học máy tính và lĩnh vực liên quan. Điều này sẽ giúp thu hút và đào tạo những nhà nghiên cứu và chuyên gia trong lĩnh vực này.
- Tích hợp tính toán lượng tử vào ứng dụng thực tế: Tìm cách tích hợp tính toán lượng tử vào các ứng dụng thực tế, từ tìm kiếm thông tin trên web đến tối ưu hóa quá trình sản xuất và dịch vụ khách hàng.

Trong tương lai, tính toán lượng tử có tiềm năng biến đổi cách chúng ta xử lý và tìm kiếm thông tin. Việc tiếp tục nghiên cứu và phát triển trong lĩnh vực này sẽ đóng một vai trò quan trọng trong việc khai thác tiềm năng của tính toán lượng tử để giải quyết các vấn đề tìm kiếm và tối ưu hóa thông tin trong tương lai.