Định nghĩa sơ đồ về Tính toán Đa thức Lượng tử

Tomoyuki Yamakam ‡

Abstract

Trong bốn thập kỷ qua, khái niệm về tính toán đa thức lượng tử đã được mô hình hóa toán học bởi các máy Turing lượng tử cũng như các mạch lượng tử. Bài báo này tìm kiếm mô hình thứ ba, đó là một tương tự lượng tử của định nghĩa sơ đồ (quy nạp hoặc xây dựng) của các hàm (nguyên thủy) đệ quy. Đối với các hàm lượng tử ánh xạ không gian Hilbert hữu hạn chiều vào chính nó, chúng tôi trình bày một định nghĩa sơ đồ như vậy, bao gồm một tập hợp nhỏ các hàm lượng tử ban đầu và một số quy tắc xây dựng quy định cách xây dựng một hàm lượng tử mới từ các hàm hiện có. Chúng tôi chứng minh rằng định nghĩa sơ đồ của chúng tôi mô tả chính xác tất cả các hàm có thể tính toán được với xác suất thành công cao trên các máy Turing lượng tử được hình thành tốt trong thời gian đa thức, hoặc tương đương là các họ đồng nhất của các mạch lượng tử kích thước đa thức. Định nghĩa sơ đồ mới của chúng tôi khá đơn giản và trực quan và, quan trọng hơn, nó tránh được việc giới thiệu phức tạp về điều kiện hình thành tốt áp đặt lên mô hình máy Turing lượng tử cũng như điều kiện đồng nhất cần thiết cho mô hình mạch lượng tử. Cách tiếp cận mới của chúng tôi có thể mở ra cánh cửa cho sự phức tạp mô tả của các hàm lượng tử, lý thuyết về các hàm lượng tử loại cao hơn, phát triển các lý thuyết bậc một mới cho tính toán lượng tử và thiết kế các ngôn ngữ lập trình cho máy tính lượng tử thực tế.

Từ khóa: tính toán lượng tử, hàm lượng tử, máy Turing lượng tử, mạch lượng tử, định nghĩa sơ đồ, độ phức tạp mô tả, tính toán đa thức, định lý dạng chuẩn

1 Bối cảnh, Động lực và Kết quả Chính

Vào đầu những năm 1980, một ý tưởng đột phá đã xuất hiện về việc khai thác vật lý lượng tử để xây dựng các thiết bị tính toán cơ học, được gọi là máy tính lượng tử, đã hoàn toàn thay đổi cách chúng ta hình dung về "máy tính." Những khám phá tiếp theo về các tính toán lượng tử hiệu quả hơn để phân tích các số nguyên dương [30] và tìm kiếm cơ sở dữ liệu không có cấu trúc [14, 15] so với các tính toán cổ điển đã thúc đẩy chúng ta tìm kiếm thêm các vấn đề toán học và thực tiễn có thể được giải quyết hiệu quả trên các máy tính lượng tử. Tính hiệu quả trong tính toán lượng tử kể từ đó đã nhanh chóng trở thành một chủ đề nghiên cứu quan trọng của khoa học máy tính cũng như vật lý.

Như một mô hình toán học để hiện thực hóa tính toán lượng tử, Deutsch 11 đã giới thiệu khái niệm về máy Turing lượng tử (hoặc QTM, viết tắt) , sau này đã được Yao 40 thảo luận và tiếp tục được Bernstein và Vazirani [5] tinh chỉnh. Mô hình cơ học này mở rộng lớn mô hình Turing cổ điển (xác suất) bằng cách cho phép một hiện tượng vật lý, được gọi là giao thoa lượng tử, xảy ra trong quá trình tính toán của nó. Một hình thức Hamiltonian khác của các máy Turing cũng đã được Benioff [3] đề xuất. Một QTM có khả năng tính toán một hàm lượng tử ánh xạ một không gian Hilbert hữu hạn chiều vào chính nó bằng cách tiến hóa một cách đơn vị một sự superposition của các cấu hình (cổ điển) của máy, bắt đầu với một chuỗi đầu vào nhất định và một trạng thái bên trong ban đầu. Một cách sử dụng hạn chế hơn của thuật ngữ "hàm lượng tử" được tìm thấy trong, ví dụ, [38], trong đó các hàm lượng tử nhận các chuỗi đầu vào cổ điển và tạo ra hoặc là các chuỗi đầu ra cổ điển của các QTM hoặc là các xác suất chấp nhận của các QTM. Trong suốt bài báo này, tuy nhiên, các hàm lượng tử chỉ đề cập đến các hàm hoạt động trên các không gian Hilbert có kích thước tùy ý.

Để đảm bảo tính đơn vị của quá trình tính toán lượng tử, một QTM yêu cầu cơ chế của nó phải đáp ứng các điều kiện được gọi là điều kiện hình thành tốt trên một mô hình QTM băng đơn 5 và một mô hình đa băng 36, 38 cũng như [27]. Tham khảo phần 2.2 để biết định nghĩa chính xác của chúng.

Bernstein và Vazirani đã hình thành một lớp độ phức tạp mới, được ký hiệu là BQP, như là tập hợp của tất cả các ngôn ngữ được công nhận bởi các QTM được hình thành tốt chạy trong thời gian đa thức với xác suất lỗi bị giới hạn từ trên xuống dưới bởi 1/3. Hơn nữa, các QTM được trang bị băng xuất có thể tính toán các hàm có giá trị chuỗi thay vì các ngôn ngữ, và các hàm đó tạo thành một lớp hàm, được gọi là FBQP .

Từ một góc độ khác, Yao 40 đã mở rộng khái niệm mạng lượng tử của Deutsch 11 và hình thành một khái niệm về mạch lượng tử, đó là một tương tự lượng tử của mạch Boolean cổ điển. Khác với mô hình mạch Boolean cổ điển, một mạch lượng tử được cấu thành từ các cổng lượng tử, mỗi cổng đại diện cho một phép biến đổi đơn vị tác động lên một không gian Hilbert có kích thước nhỏ, cố định. Để hoạt động như một "bộ lập trình" phép toán đơn vị, một họ các mạch lượng tử yêu cầu điều kiện đồng nhất, đảm bảo rằng bản thiết kế của mỗi mạch lượng tử có thể được thực hiện dễ dàng. Yao đã chỉ ra rằng một họ đồng nhất của các mạch lượng tử đủ mạnh để mô phỏng một máy Turing lượng tử được hình thành tốt. Như Nishimura và Ozawa 26 đã chỉ ra, điều kiện đồng nhất của một họ mạch lượng tử là cần thiết để nắm bắt chính xác tính toán đa thức lượng tử. Với điều kiện đồng nhất này, BQP và FBQP được đặc trưng

*Công việc này được thực hiện trong khi tác giả còn ở Đại học Ottawa giữa năm 1999 và 2003, và nó được hỗ trợ tài chính bởi Hội đồng Khoa học Tự nhiên và Kỹ thuật Canada.

† Một tóm tắt mở rộng đã xuất hiện dưới tiêu đề "Một định nghĩa đệ quy về tính toán đa thức lượng tử (tóm tắt mở rộng)" trong Kỷ yếu của Hội thảo lần thứ 9 về Các Mô hình Tự động và Ứng dụng Không Cổ điển (NCMA 2017), Prague, Cộng hòa Séc, 17-18 tháng 8 năm 2017, Österreichische Computer Gesellschaft 2017, Hội máy tính Áo, trang 243-258, 2017. Bài báo hiện tại nhằm mục đích sửa chữa các mô tả sai trong tóm tắt mở rộng và cung cấp các giải thích chi tiết hơn cho tất cả các chứng minh bị bỏ qua do giới hạn trang.

‡ Đơn vị hiện tại: Khoa Kỹ thuật, Đại học Fukui, 3-9-1 Bunkyo, Fukui, 910-8507 Nhật Bản

chính xác bởi các họ mạch lượng tử đồng nhất được tạo thành từ nhiều cổng lượng tử có kích thước đa thức.

Bài báo hiện tại táo bạo tiếp cận theo cách thứ ba để đặc trưng hóa tính toán đa thức lượng tử. Khác với các mô hình thiết bị cơ học đã đề cập, cách tiếp cận của chúng tôi là mở rộng định nghĩa sơ đồ (quy nạp hoặc xây dựng) của các hàm (nguyên thủy) đệ quy trên các số tự nhiên. Định nghĩa sơ đồ như vậy đã được Peano nghĩ ra vào thế kỷ 19 [28], trái ngược với định nghĩa được đưa ra bởi mô hình máy Turing của Turing 32. Sơ đồ cổ điển này bao gồm một tập hợp nhỏ các hàm ban đầu và một tập hợp nhỏ các quy tắc, quy định cách xây dựng một hàm mới từ các hàm hiện có. Ví dụ, mỗi hàm đệ quy nguyên thủy được xây dựng từ các hàm hằng số, kế tiếp, và chiếu bởi việc áp dụng hữu hạn các quy tắc hợp thành và quy tắc đệ quy nguyên thủy. Đặc biệt, quy tắc đệ quy nguyên thủy giới thiệu một hàm mới có giá trị được xác định bởi quy tắc suy diễn. Các hàm đệ quy (dưới dạng các hàm đệ quy μ [19, 20]) yêu cầu thêm một sơ đồ, được gọi là phép toán tối thiểu (hoặc số nhỏ nhất). Các hàm này trùng với hình thức chính quy của các hàm đệ quy tổng quát của Gödel-Herbrand (xem [10]). Để có cái nhìn lịch sử về những khái niệm này, xem, ví dụ, 29. Những cách tiếp cận sơ đồ tương tự để nắm bắt tính toán đa thức cổ điển đã được tìm kiếm trong tài liệu [7, 8, 9, 24, 35. Những cách tiếp cận đó đã dẫn đến những chủ đề nghiên cứu khá khác biệt so với những gì mô hình máy Turing cung cấp.

Mục đích của chúng tôi trong bài báo này là đưa ra một định nghĩa sơ đồ của các hàm lượng tử để nắm bắt khái niệm về tính toán đa thức lượng tử và, quan trọng hơn, để làm cho một định nghĩa như vậy đơn giản hơn và trực quan hơn cho lợi ích thực tiễn của chính chúng tôi. Định nghĩa sơ đồ của chúng tôi (Định nghĩa 3.1) bao gồm một tập hợp các hàm lượng tử ban đầu, I (đơn vị), NOT (phủ định của một qubit), $PHASE_\theta$ (dịch pha bởi $e^{i\theta}$), ROT_θ (xoay quanh trục xy bởi góc θ), $SWAP$ (hoán đổi giữa hai qubit), và MEAS (đo lường dự đoán từng phần), cũng như các quy tắc xây dựng, bao gồm hợp thành (Compo $[\cdot,\cdot]$), phân nhánh (Branch $[\cdot,\cdot]$), và đệ quy lượng tử nhiều qubit ($kQRec[\cdot,\cdot \mid \cdot]$). Lựa chọn của chúng tôi về các hàm lượng tử ban đầu và các quy tắc xây dựng này chủ yếu xuất phát từ một tập hợp các cổng lượng tử phổ quát đã được sử dụng trong tài liệu trước đây. Ngược lại, đệ quy lượng tử của chúng tôi thì hoàn toàn khác về bản chất so với quy tắc đệ quy được sử dụng để xây dựng các hàm đệ quy nguyên thủy. Thay vì sử dụng hàm kế tiếp để đếm ngược số lần lặp quy nạp trong quy tắc đệ quy nguyên thủy, đệ quy lượng tử sử dụng một chiến lược chia để trị để giảm số lượng qubit có thể truy cập cần thiết cho việc thực hiện một hàm lượng tử xác định. Trong khuôn khổ mới của chúng tôi, chúng tôi có thể thực hiện các phép toán đơn vị điển hình, chẳng hạn như biến đổi Walsh-Hadamard (WH), biến đổi có điều kiện-NOT (CNOT), và dịch pha toàn cục (GPS).

Một lợi ích ngay lập tức của định nghĩa sơ đồ của chúng tôi là chúng tôi có thể tránh được việc giới thiệu phức tạp về điều kiện hình thành tốt áp đặt lên mô hình QTM và điều kiện đồng nhất trên mô hình mạch lượng tử. Một lợi thế khác của các sơ đồ của chúng tôi là mỗi sơ đồ có một phép đảo ngược riêng; nghĩa là, đối với bất kỳ hàm lượng tử nào g được định nghĩa bởi một

trong các sơ đồ, phép đảo ngược của nó g^{-1} cũng được định nghĩa bởi cùng một loại sơ đồ. Ví dụ, các phép đảo ngược của các hàm lượng tử ROT_θ và $kQRec_t\left[g, h, p \mid \{f_s\}_{s\in\{0,1\}^k}\right]$ được giới thiệu trong Định nghĩa 3.1 chính xác là $ROT_{-\theta}$ và $kQRec_t\left[g^{-1}, p^{-1}, h^{-1} \mid \left\{f_s^{-1}\right\}_{s\in\{0,1\}^k}\right]$, tương ứng (Định lý 3.5).

Để giải thích thêm về những đóng góp chính của chúng tôi, đã đến lúc giới thiệu một ký hiệu ngắn gọn của $\square_1^{\mathrm{QP}}$ (nơi $\square$ được phát âm là "hình vuông") để chỉ tập hợp tất cả các hàm lượng tử được xây dựng từ các hàm lượng tử ban đầu và bằng một chuỗi hữu hạn các ứng dụng tuần tự của các quy tắc xây dựng. Vì phép đo từng phần (MEAS) không phải là một phép toán đơn vị, chúng tôi ký hiệu lớp thu được từ $\square_1^{\mathrm{QP}}$ mà không sử dụng MEAS là $\widehat{\square_1^{\mathrm{QP}}}$. Ngắn gọn, hãy để chúng tôi thảo luận về những khác biệt rõ ràng giữa định nghĩa sơ đồ của chúng tôi và hai hình thức đã đề cập của các hàm có thể tính toán đa thức lượng tử về mặt các QTMs và các mạch lượng tử. Hai sự khác biệt chính được liệt kê dưới đây.

1. Trong khi một mạch lượng tử đơn lẻ nhận một số qubit đầu vào cố định, hàm lượng tử của chúng tôi nhận một số "tùy ý" qubit làm đầu vào. Tình huống này tương tự như các QTMs vì một QTM có một băng vô hạn và sử dụng một số ô băng tùy ý trong quá trình tính toán của nó như là không gian lưu trữ bổ sung. Ngược lại với các QTMs, một hàm $\widehat{\square_1^{\mathrm{QP}}}$-function được xây dựng bằng cách sử dụng cùng một số qubit như đầu vào ban đầu của nó
   theo cách mà một mạch lượng tử có cùng số qubit đầu vào và qubit đầu ra.

2. Hai mô hình máy tính này yêu cầu một mô tả thuật toán để chỉ định hành vi của mỗi máy; cụ thể hơn, một QTM sử dụng một hàm chuyển tiếp, mô tả thuật toán cách mỗi bước của máy tác động lên một số qubit nhất định, và một họ các mạch lượng tử sử dụng điều kiện đồng nhất của nó để thể hiện thiết kế của các cổng lượng tử trong mỗi mạch lượng tử. Không giống như hai mô hình này, không có hàm $\square_1^{\mathrm{QP}}$-function nào có bất kỳ cơ chế nào để lưu trữ thông tin về chính mô tả của hàm đó mà quá trình xây dựng tự nó chỉ định hành vi của hàm.

Như một hệ quả, những khác biệt đã đề cập ở trên giúp các hàm $\square_1^{\mathrm{QP}}$-functions có một vị trí đặc biệt trong số tất cả các mô hình tính toán có thể đặc trưng cho tính toán đa thức lượng tử, và do đó chúng tôi mong đợi chúng sẽ đóng một vai trò quan trọng trong việc phân tích các đặc điểm của tính toán đa thức lượng tử từ một góc độ hoàn toàn khác.

Trong Phần 3.1, chúng tôi sẽ trình bày chính thức định nghĩa sơ đồ của chúng tôi về các hàm $\square_1^{\mathrm{QP}}$ (cũng như các hàm $\widehat{\square_1^{\mathrm{QP}}}$) và chỉ ra trong Phần 4.1 rằng $\square_1^{\mathrm{QP}}$ (cũng như $\widehat{\square_1^{\mathrm{QP}}}$) có thể đặc trưng cho tất cả các hàm trong FBQP. Chính xác hơn, chúng tôi khẳng định trong định lý chính (Định lý 4.1) rằng bất kỳ hàm nào từ $\{0,1\}^*$ đến $\{0,1\}^*$ trong FBQP đều có thể được đặc trưng bởi

một đa thức nhất định p và một hàm lượng tử nhất định $g \in \square_1^{\mathrm{QP}}$ theo cách mà, bằng cách sử dụng một sơ đồ mã hóa thích hợp, trong trạng thái lượng tử cuối cùng của g trên các thể hiện x và giới hạn thời gian $p(|x|)$, chúng tôi quan sát được một giá trị đầu ra $f(x)$ với xác suất cao. Định lý này sẽ được chia thành hai định lý phụ, các Định lý 4.2 và 4.3 Định lý phụ trước sẽ được chứng minh trong Phần 4.1 tuy nhiên, chứng minh của định lý phụ sau thì dài đến mức sẽ được hoãn lại cho đến Phần 5. Trong chứng minh này, chúng tôi sẽ xây dựng một hàm $\square_1^{\mathrm{QP}}$-function có thể mô phỏng hành vi của một QTM nhất định.

Lưu ý rằng, vì BQP là một trường hợp đặc biệt của FBQP, BQP cũng được đặc trưng bởi mô hình của chúng tôi. Trong chứng minh của chúng tôi về định lý đặc trưng (Định lý 4.1), chúng tôi sẽ sử dụng một kết quả chính của Bernstein và Vazirani [5] và của Yao 40 một cách rộng rãi. Trong Phần 4.2, chúng tôi sẽ áp dụng sự đặc trưng của chúng tôi, với sự trợ giúp của một QTM phổ quát [5, 26], để thu được một phiên bản lượng tử của định lý dạng chuẩn của Kleene [19, 20, trong đó có một cặp hàm và đại số đệ quy nguyên thủy phổ quát có thể mô tả hành vi của mọi hàm đệ quy.

Khác với tính toán cổ điển trên các số tự nhiên (tương đương, các chuỗi trên các bảng chữ cái hữu hạn bằng các sơ đồ mã hóa thích hợp), tính toán lượng tử là một chuỗi nhất định của các phép biến đổi của một vectơ trong một không gian Hilbert hữu hạn chiều và chúng tôi chỉ cần độ chính xác cao để xấp xỉ mỗi hàm trong FBQP bằng một vectơ như vậy. Thực tế này cho phép chúng tôi chọn một tập hợp các sơ đồ (các hàm lượng tử ban đầu và các quy tắc xây dựng) khác nhau để nắm bắt bản chất của tính toán lượng tử. Trong Phần 6.1, chúng tôi sẽ thảo luận về vấn đề này bằng một ví dụ về dạng tổng quát của biến đổi Fourier lượng tử (QFT). Biến đổi này có thể không được "tính toán chính xác" trong khuôn khổ hiện tại của chúng tôi về $\square_1^{\mathrm{QP}}$ nhưng chúng tôi có thể dễ dàng mở rộng $\square_1^{\mathrm{QP}}$ để tính toán chính xác QFT tổng quát nếu chúng tôi bao gồm một hàm lượng tử ban đầu bổ sung, chẳng hạn như CROT (xoay có điều kiện).

Liên quan đến nghiên cứu trong tương lai về chủ đề hiện tại, chúng tôi sẽ thảo luận trong Phần 6 bốn hướng nghiên cứu mới của chủ đề này. Định nghĩa sơ đồ của chúng tôi không chỉ cung cấp một cách khác để mô tả các ngôn ngữ và hàm có thể tính toán lượng tử trong thời gian đa thức mà còn một cách đơn giản để đo lường độ phức tạp "mô tả" của một ngôn ngữ và một hàm bị giới hạn cho các thể hiện có độ dài xác định. Đo lường độ phức tạp mới này sẽ hữu ích để chứng minh các tính chất cơ bản của các hàm $\widehat{\square_1^{\mathrm{QP}}}$-functions trong Phần 3. Ứng dụng trong tương lai của nó sẽ được thảo luận ngắn gọn trong Phần 6.2

Kleene 21, 22 đã định nghĩa các hàm đệ quy của các loại cao hơn bằng cách mở rộng các hàm đệ quy nguyên thủy đã đề cập ở trên. Một nghiên cứu tổng quát hơn về các hàm loại cao hơn đã được tiến hành trong lý thuyết độ phức tạp tính toán trong nhiều thập kỷ [8, 9, 24, 31, 35]. Theo một tinh thần tương tự, định nghĩa sơ đồ của chúng tôi cho phép chúng tôi nghiên cứu các hàm lượng tử loại cao hơn. Trong Phần 6.3, bằng cách sử dụng các hàm oracle (các oracle hàm hoặc oracle), chúng tôi sẽ định nghĩa các hàm lượng tử loại 2, có thể dẫn dắt chúng tôi đến một lĩnh vực nghiên cứu phong phú trong tương lai.

Một định nghĩa sơ đồ về cách xây dựng một hàm mục tiêu $\square_1^{\mathrm{QP}}$-function có thể được coi là một "chương trình" mô tả một chuỗi các hướng dẫn về các sơ đồ nào sẽ sử dụng. Do đó, việc hình thành sơ đồ của chúng tôi mở ra một cánh cửa cho một ứng dụng thực tiễn mới trong việc thiết kế các ngôn ngữ lập trình ngắn gọn để điều khiển các hoạt động của các máy tính lượng tử thực tế trong tương lai. Trong Phần 6.4, chúng tôi sẽ tranh luận ngắn gọn về một ứng dụng của định nghĩa sơ đồ đối với sự phát triển trong tương lai của "các ngôn ngữ lập trình lượng tử." Như một ứng dụng tiếp theo của định nghĩa sơ đồ của chúng tôi, chúng tôi cũng có thể xem xét một khía cạnh mới của các lý thuyết bậc nhất và các tiểu lý thuyết của chúng. Trước đây, một tương tự lượng tử của NP (lớp thời gian đa thức không xác định) và hơn thế nữa đã được tìm kiếm trong [37] với việc sử dụng các định lượng bị giới hạn trên các trạng thái lượng tử trong các không gian Hilbert hữu hạn chiều. Theo một cách tương tự, chúng tôi mong đợi rằng $\square_1^{\mathrm{QP}}$ sẽ phục vụ như một nền tảng cho việc giới thiệu các lý thuyết bậc nhất và các tiểu lý thuyết của chúng trên các trạng thái lượng tử trong các không gian Hilbert.

2 Các Khái niệm và Ký hiệu Cơ bản

Chúng tôi bắt đầu bằng cách giải thích các khái niệm và ký hiệu cơ bản cần thiết để đọc các phần tiếp theo. Giả sử độc giả đã quen thuộc với các máy Turing cổ điển (xem, ví dụ, [16]). Đối với nền tảng của thông tin và tính toán lượng tử, ngược lại, độc giả tham khảo các sách giáo khoa cơ bản, ví dụ, [18, 25].

2.1 Số, Ngôn ngữ và Qustrings

Ký hiệu $\mathbb{Z}$ chỉ tập hợp tất cả các số nguyên và $\mathbb{N}$ biểu thị tập hợp tất cả các số tự nhiên (tức là, các số nguyên không âm). Để tiện lợi, chúng tôi đặt $\mathbb{N}^+ = \mathbb{N} - \{0\}$. Hơn nữa, $\mathbb{Q}$ biểu thị tập hợp tất cả các số hữu tỷ và $\mathbb{R}$ chỉ ra tập hợp tất cả các số thực. Đối với hai số $m, n \in \mathbb{Z}$ với $m \leq n$, ký hiệu $[m, n]_{\mathbb{Z}}$ biểu thị một khoảng số nguyên $\{m, m+1, m+2, \ldots, n\}$, so với một khoảng thực $[\alpha, \beta]$ cho $\alpha, \beta \in \mathbb{R}$ với $\alpha \leq \beta$. Đặc biệt, $[n]$ là viết tắt cho $[1, n]_{\mathbb{Z}}$ cho bất kỳ $n \in \mathbb{N}^+$. Bằng $\mathbb{C}$, chúng tôi biểu thị tập hợp tất cả các số phức. Cho $\alpha \in \mathbb{C}, \alpha^*$ biểu thị liên hợp phức của α. Các đa thức được giả định có các hệ số là số tự nhiên và do đó chúng tạo ra các giá trị không âm từ các đầu vào không âm. Một số thực α được gọi là có thể xấp xỉ trong thời gian đa thức $^{\mathrm{g}}$ nếu tồn tại một máy Turing xác định đa băng trong thời gian đa thức M (được trang bị một băng xuất chỉ ghi) mà, trên mỗi đầu vào có dạng 1^n cho một số tự nhiên n, sản xuất một phân số nhị phân hữu hạn, $M(1^n)$, trên băng xuất được chỉ định của nó với $|M(1^n) - \alpha| \leq 2^{-n}$. Gọi $\widetilde{\mathbb{C}}$ là tập hợp các số phức mà phần thực và phần ảo của chúng đều có thể xấp xỉ trong thời gian đa thức. Đối với một bit $a \in \{0, 1\}, \bar{a}$ chỉ ra $1 - a$. Cho một ma trận A, A^T biểu thị chuyển vị của nó và $A^\dagger$ biểu thị chuyển vị liên hợp của A.

Một bảng chữ cái là một tập hợp hữu hạn không rỗng các "ký hiệu" hoặc

"chữ cái." Cho một bảng chữ cái như vậy Σ, một chuỗi trên Σ là một chuỗi hữu hạn các ký hiệu lấy từ Σ. Phép nối của hai chuỗi u và w được biểu thị là $u \cdot w$ hoặc đơn giản hơn là uw. Độ dài của một chuỗi x, được ký hiệu là $|x|$, là số lần xuất hiện của các ký hiệu trong x. Đặc biệt, chuỗi rỗng có độ dài 0 và được ký hiệu là λ. Chúng tôi viết Σ^n cho tập hợp con của Σ^* chỉ bao gồm tất cả các chuỗi có độ dài n và chúng tôi đặt $\Sigma^* = \bigcup_{n\in\mathbb{N}} \Sigma^n$ (tập hợp tất cả các chuỗi trên Σ). Một ngôn ngữ trên Σ là một tập con của Σ^*. Cho một ngôn ngữ S, hàm đặc trưng của nó cũng được biểu thị bởi S; tức là, $S(x) = 1$ cho tất cả $x \in S$ và $S(x) = 0$ cho tất cả $x \notin S$. Một hàm trên Σ^* (tức là, từ Σ^* đến Σ^*) được giới hạn bởi đa thức nếu tồn tại một đa thức p thỏa mãn $|f(x)| \leq p(|x|)$ cho tất cả các chuỗi $x \in \Sigma^*$.

Đối với mỗi số tự nhiên $k \geq 1, \mathcal{H}_k$ biểu thị một không gian Hilbert có kích thước k và mỗi phần tử của $\mathcal{H}_k$ được biểu thị dưới dạng $|\phi\rangle$ bằng cách sử dụng ký hiệu "ket" của Dirac. Trong bài báo này, chúng tôi chỉ quan tâm đến trường hợp mà k là một lũy thừa của 2 và chúng tôi ngầm giả định rằng k có dạng 2^n cho một số nhất định $n \in \mathbb{N}$. Bất kỳ phần tử nào của $\mathcal{H}_2$ có chuẩn đơn vị được gọi là một bit lượng tử hoặc một qubit. Bằng cách chọn một cơ sở tính toán chuẩn $B_1 = \{|0\rangle, |1\rangle\}$, mỗi qubit $|\phi\rangle$ có thể được biểu thị dưới dạng $\alpha_0|0\rangle + \alpha_1|1\rangle$ cho một sự lựa chọn thích hợp của hai giá trị $\alpha_0, \alpha_1 \in \mathbb{C}$ (được gọi là biên độ) thỏa mãn $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Chúng tôi cũng biểu thị $|\phi\rangle$ dưới dạng một vectơ cột có dạng $\binom{\alpha_0}{\alpha_1}$; đặc biệt, $|0\rangle = \binom{1}{0}$ và $|1\rangle = \binom{0}{1}$. Trong trường hợp tổng quát hơn của $n \geq 1$, chúng tôi sử dụng $B_n = \{|s\rangle \mid s \in \{0,1\}^n\}$ làm cơ sở tính toán của $\mathcal{H}_{2^n}$ với $|B_n| = 2^n$. Cho bất kỳ số nào $n \in \mathbb{N}^+$, một qustring có độ dài n là một vectơ $|\phi\rangle$ của $\mathcal{H}_{2^n}$ có chuẩn đơn vị; nghĩa là, nó có dạng $\sum_{s\in\{0,1\}^n} \alpha_s|s\rangle$, trong đó mỗi biên độ α_s nằm trong $\mathbb{C}$ với $\sum_{s\in\{0,1\}^n} |\alpha_s|^2 = 1$. Lưu ý rằng một qubit là một qustring có độ dài 1 . Ngoại lệ là vectơ null, được ký hiệu đơn giản là $\mathbf{0}$, có chuẩn 0 . Mặc dù vectơ null có thể là một qustring của độ dài "tùy ý" n, chúng tôi thay vào đó gọi nó là qustring có độ dài 0 để tiện lợi. Chúng tôi sử dụng ký hiệu Φ_n cho mỗi $n \in \mathbb{N}$ để chỉ tập hợp tất cả các qustring có độ dài n. Cuối cùng, chúng tôi đặt $\Phi_\infty = \bigcup_{n\in\mathbb{N}} \Phi_n$ (tập hợp tất cả các qustring).

Khi $s = s_1 s_2 \cdots s_n$ với $s_i \in \{0,1\}$ cho bất kỳ chỉ số nào $i \in [n]$, qustring $|s\rangle$ trùng với $|s_1\rangle \otimes |s_2\rangle \otimes \cdots \otimes |s_n\rangle$, trong đó $\otimes$ biểu thị tích tensor và được biểu thị như, ví dụ, $|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$, $|01\rangle = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}^T$, và $|11\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^T$. Liên hợp transposed của $|s\rangle$ được ký hiệu là $\langle s|$ (với ký hiệu "bra"). Ví dụ, nếu $|\phi\rangle = \alpha|01\rangle + \beta|10\rangle$, thì $\langle\phi| = \alpha^*\langle 01| + \beta^*\langle 10|$. Tích vô hướng của $|\phi\rangle$ và $|\psi\rangle$ được biểu thị là $\langle\phi \mid \psi\rangle$ và chuẩn của $|\phi\rangle$ do đó là $\sqrt{\langle\phi \mid \psi\rangle}$. Khi chúng tôi quan sát hoặc đo lường $|\phi\rangle$ trong cơ sở tính toán B_n, chúng tôi thu được mỗi chuỗi $s \in \{0,1\}^n$ với xác suất $|\langle s \mid \phi\rangle|^2$.

Gọi $\mathcal{H}_\infty = \bigcup_{n\in\mathbb{N}^+} \mathcal{H}_{2^n}$. Chúng tôi mở rộng khái niệm "độ dài" cho các trạng thái lượng tử tùy ý trong $\mathcal{H}_\infty$. Đối với mỗi vectơ không null $|\phi\rangle$ trong $\mathcal{H}_\infty$, độ dài của $|\phi\rangle$, được ký hiệu là $\ell(|\phi\rangle)$, là số nguyên tối thiểu $n \in \mathbb{N}$ thỏa mãn $|\phi\rangle \in \mathcal{H}_{2^n}$; nói cách khác, $\ell(|\phi\rangle)$ là logarit của kích thước của vectơ $|\phi\rangle$. Theo quy ước, chúng tôi cũng đặt $\ell(\mathbf{0}) = \ell(\alpha) = 0$ cho vectơ null $\mathbf{0}$ và bất kỳ số vô hướng nào $\alpha \in \mathbb{C}$. Với quy ước này, nếu $\ell(|\phi\rangle) = 0$ cho một trạng thái lượng tử $|\phi\rangle$, thì $|\phi\rangle$ nhất định phải là qustring có độ dài 0 . Một qustring $|\phi\rangle$ có độ

dài n được gọi là cơ bản nếu $|\phi\rangle = |s\rangle$ cho một chuỗi nhị phân nhất định s và chúng tôi thường xác định một qustring cơ bản như vậy $|s\rangle$ với chuỗi nhị phân cổ điển tương ứng s vì sự tiện lợi. Vì tất cả các qustring cơ bản trong Φ_n tạo thành $B_n, \mathcal{H}_{2^n}$ được tạo thành bởi tất cả các phần tử trong Φ_n.

Phép dấu chấm phẩy trên một hệ thống B của một hệ thống tổ hợp AB, được ký hiệu là tr_B, là một toán tử lượng tử mà $\mathrm{tr}_B(|\phi\rangle\langle\phi|)$ là một vectơ thu được bằng cách loại bỏ B từ sản phẩm ngoài $|\phi\rangle\langle\phi|$ của một trạng thái lượng tử $|\phi\rangle$. Liên quan đến một trạng thái lượng tử $|\phi\rangle$ của n qubit, chúng tôi sử dụng ký hiệu tiện lợi $\mathrm{tr}_k(|\phi\rangle\langle\phi|)$ để chỉ trạng thái lượng tử thu được từ $|\phi\rangle$ bằng cách loại bỏ tất cả các qubit ngoại trừ k qubit đầu tiên. Ví dụ, nó theo cho $\sigma_1, \sigma_2, \tau_1, \tau_2 \in \{0,1\}$ rằng $\mathrm{tr}_1\left(|\sigma_1\rangle\langle\sigma_2| \otimes |\tau_1\rangle\langle\tau_2|\right) = |\sigma_1\rangle\langle\sigma_2| \cdot \mathrm{tr}\left(|\tau_1\rangle\langle\tau_2|\right)$, trong đó $\mathrm{tr}(B)$ biểu thị dấu chấm của một ma trận B. Chuẩn dấu chấm $\|A\|_{\mathrm{tr}}$ của một ma trận vuông A được định nghĩa bởi $\|A\|_{\mathrm{tr}} = \mathrm{tr}\left(\sqrt{AA^\dagger}\right)$. Khoảng cách biến thiên tổng thể giữa hai tập hợp $p = \{p_i\}_{i\in A}$ và $q = \{q_i\}_{i\in A}$ của các số thực trên một tập hợp chỉ số hữu hạn A là $\frac{1}{2}\|p-q\|_1 = \frac{1}{2}\sum_{i\in A}||p_i|-|q_i||$.

Trong suốt bài báo này, chúng tôi có những quy ước đặc biệt liên quan đến ba ký hiệu, $|\cdot\rangle, \otimes$, và $\|\cdot\|$, lần lượt biểu thị các trạng thái lượng tử, tích tensor, và chuẩn ℓ_2-norm. Những quy ước này hơi khác so với các quy ước tiêu chuẩn được sử dụng trong, ví dụ, 25, nhưng chúng làm cho các mô tả toán học của chúng tôi trong các phần sau đơn giản và ngắn gọn hơn.

Các Quy ước Ký hiệu: Chúng tôi viết tắt $|\phi\rangle \otimes |\psi\rangle$ là $|\phi\rangle|\psi\rangle$ cho bất kỳ hai vectơ $|\phi\rangle$ và $|\psi\rangle$. Đối với hai chuỗi nhị phân s và $t, |st\rangle$ có nghĩa là $|s\rangle \otimes |t\rangle$ hoặc $|s\rangle|t\rangle$. Giả sử k và n là hai số nguyên với $0 < k < n$. Bất kỳ qustring nào $|\phi\rangle$ có độ dài n được biểu thị chung là $|\phi\rangle = \sum_{s:|s|=k}|s\rangle|\phi_s\rangle$, trong đó mỗi $|\phi_s\rangle$ là một qustring có độ dài $n-k$. Qustring $|\phi_s\rangle$ này có thể được coi là kết quả của việc áp dụng một phép đo dự đoán từng phần lên k qubit đầu tiên của $|\phi\rangle$, và do đó có thể biểu thị ngắn gọn là $\langle s \mid \phi\rangle$. Với ký hiệu mới, thuận tiện này, $|\phi\rangle$ trùng với $\sum_{s:|s|=k}|s\rangle \otimes \langle s \mid \phi\rangle$, được đơn giản hóa thành $\sum_{s:|s|=k}|s\rangle\langle s \mid \phi\rangle$. Lưu ý rằng, khi $k = n, \langle s \mid \phi\rangle$ là một số vô hướng, giả sử, α trong $\mathbb{C}$. Do đó, $|s\rangle \otimes \langle s \mid \phi\rangle$ là $|s\rangle \otimes \alpha$ và nó được coi là một vectơ cột $\alpha|s\rangle$; tương tự, chúng tôi xác định $\alpha \otimes |s\rangle$ với $\alpha|s\rangle$. Trong những trường hợp này, $\otimes$ chỉ được coi là phép nhân vô hướng. Do đó, sự bình đẳng $|\phi\rangle = \sum_{s:|s|=k}|s\rangle\langle s \mid \phi\rangle$ vẫn đúng ngay cả khi $k = n$. Liên quan đến vectơ null $\mathbf{0}$, chúng tôi cũng có quy định đặc biệt sau đây: đối với bất kỳ vectơ nào $|\phi\rangle \in \mathcal{H}_\infty$, (i) $0 \otimes |\phi\rangle = |\phi\rangle \otimes 0 = \mathbf{0}$, (ii) $|\phi\rangle \otimes \mathbf{0} = \mathbf{0} \otimes |\phi\rangle = \mathbf{0}$, và (iii) khi $|\psi\rangle$ là vectơ null, $\langle\phi \mid \psi\rangle = \langle\psi \mid \phi\rangle = 0$. Liên quan đến những quy ước về phép đo dự đoán từng phần $\langle\phi \mid \psi\rangle$, chúng tôi cũng mở rộng việc sử dụng quy ước về chuẩn $\|\cdot\|$ cho các số vô hướng. Khi $\ell(|\phi\rangle) = \ell(|\psi\rangle), \|\langle\phi \mid \psi\rangle\|$ biểu thị giá trị tuyệt đối $|\langle\phi \mid \psi\rangle|$; nói chung hơn, đối với bất kỳ số nào $\alpha \in \mathbb{C}, \|\alpha\|$ có nghĩa là $|\alpha|$. Với những quy ước bổ sung này, khi $|\phi\rangle$ có dạng $\sum_{s:|s|=k}|s\rangle\langle s \mid \phi\rangle$, phương trình $\|\||\phi\rangle\Big\|^2 = \sum_{s:|s|=k}\Big\|\langle s \mid \phi\rangle\|^2$ luôn đúng cho bất kỳ chỉ số $k \in [n]$.

[g] Ko và Friedman 23 đã lần đầu tiên giới thiệu khái niệm này dưới cái tên "có thể tính toán trong thời gian đa thức." Để tránh sự nhầm lẫn của độc giả trong bài báo này, chúng tôi thích sử dụng thuật ngữ "xấp xỉ trong thời gian đa thức."

2.2 Máy Turing Lượng Tử

Chúng tôi giả định rằng độc giả đã có kiến thức cơ bản về khái niệm máy Turing lượng tử (hoặc QTM) được định nghĩa trong 5. Như đã làm trong 36, chúng tôi cho phép một QTM được trang bị nhiều băng và di chuyển các đầu băng của nó không đồng thời sang bên phải hoặc bên trái, hoặc làm cho các đầu băng đứng yên. Một QTM như vậy cũng đã được thảo luận ở nơi khác (ví dụ, 27) và được biết là tương đương với mô hình được đề xuất trong [5].

Để tính toán các hàm từ Σ^* đến Σ^* trên một bảng chữ cái cho trước Σ, chúng tôi thường giới thiệu các QTM như là những máy được trang bị các băng xuất trên đó các chuỗi xuất được ghi theo một cách nhất định bởi thời gian mà các máy dừng lại. Bằng cách xác định các ngôn ngữ với các hàm đặc trưng của chúng, các QTM như vậy có thể được coi là các bộ chấp nhận ngôn ngữ.

Một cách chính thức, một máy Turing lượng tử k băng (được gọi là QTM k băng), với $k \in \mathbb{N}^+$, là một bộ sáu $(Q, \Sigma, \Gamma_1 \times \cdots \times \Gamma_k, \delta, q_0, Q_f)$, trong đó Q là một tập hợp hữu hạn các trạng thái bên trong bao gồm trạng thái ban đầu q_0 và một tập hợp các trạng thái cuối Q_f với $Q_f \subseteq Q$, mỗi Γ_i là một bảng chữ cái được sử dụng cho băng i với một ký hiệu trống được phân biệt # thỏa mãn $\Sigma \subseteq \Gamma_1$, và δ là một hàm chuyển tiếp lượng tử từ $Q \times \tilde{\Gamma}^{(k)} \times Q \times \tilde{\Gamma}^{(k)} \times \{L, N, R\}^k$ đến $\mathbb{C}$, trong đó $\tilde{\Gamma}^{(k)}$ đại diện cho $\Gamma_1 \times \cdots \times \Gamma_k$. Để tiện lợi, chúng tôi xác định L, N, và R với $-1, 0$, và $+1$, tương ứng, và chúng tôi đặt $D = \{0, \pm 1\}$. Để biết thêm thông tin, tham khảo [36].

Tất cả các ô băng của mỗi băng được đánh số tuần tự bởi các số nguyên. Ô được đánh số 0 trên mỗi băng được gọi là ô bắt đầu. Vào đầu quá trình tính toán, M ở trong trạng thái bên trong q_0, tất cả các băng ngoại trừ băng đầu vào đều trống, và tất cả các đầu băng đang quét các ô bắt đầu. Một chuỗi đầu vào nhất định $x_1 x_2 \cdots x_n$ ban đầu được ghi trên băng đầu vào theo cách mà, đối với mỗi chỉ số $i \in [n], x_i$ nằm trong ô i (không phải ô $i - 1$). Khi M vào một trạng thái cuối, đầu ra của M là nội dung của chuỗi được ghi trên một băng xuất (nếu M chỉ có một băng, thì băng xuất là cùng một băng được sử dụng để giữ các đầu vào) từ ô bắt đầu, kéo dài sang bên phải cho đến ký hiệu trống đầu tiên. Một cấu hình của M được biểu thị dưới dạng một bộ ba $\left(p, (h_i)_{i\in[k]}, (z_i)_{i\in[k]}\right)$, chỉ ra rằng M hiện đang ở trong trạng thái bên trong p với k đầu băng tại các ô được đánh số bởi $h_1, \ldots, h_k$ với nội dung băng $z_1, \ldots, z_k$, tương ứng. Khái niệm cấu hình sẽ được sửa đổi một chút trong các Phần 45 để đơn giản hóa chứng minh cho định lý chính của chúng tôi. Một cấu hình ban đầu có dạng ($q_0, 0, x$) và một cấu hình cuối là một cấu hình có trạng thái cuối. Không gian cấu hình được tạo thành bởi các vectơ cơ sở trong $\left\{|q, h, z\rangle \mid q \in Q, h \in \mathbb{Z}^k, z \in \Gamma_1^* \times \cdots \Gamma_k^*\right\}$. Đối với một chuỗi không rỗng z_i và một chỉ số $h \in [|z_i|], z_i[h]$ biểu thị ký hiệu h trong z_i. Ví dụ, nếu $z_i = 01101$, thì $z_i[1] = 0, z_i[2] = 1$, và $z_i[5] = 1$. Toán tử tiến hóa theo thời gian U_δ của M tác động lên không gian cấu hình được sinh ra từ δ như sau

$$U_\delta |p, h, z\rangle = \sum_{q,w,d} \delta\left(p, z_h, q, z'_h, d\right) |q, h_d, z'\rangle ,$$

trong đó $p \in Q$, $h = (h_i)_{i\in[k]} \in \mathbb{Z}^k, z = (z_i)_{i\in[k]} \in \Gamma_1^* \times \cdots \Gamma_k^*, z_h = (z_i [h_i])_{i\in[k]}, h_d = (h_i + d_i)_{i\in[k]}$, và $z' = (z'_i)_{i\in[k]}$, trong đó mỗi z'_i giống như z ngoại trừ ký hiệu ở vị trí h_i. Hơn nữa, trong tổng, các biến $q, z'_h = (z'_i [h_i])_{i\in[k]}$, và $d = (d_i)_{i\in[k]}$ lần lượt thay đổi trên $Q, \tilde{\Gamma}^{(k)}$, và D^k. Bất kỳ mục nào của U_δ được gọi là một biên độ. Cơ học lượng tử yêu cầu toán tử tiến hóa theo thời gian U_δ của QTM phải là đơn vị.

Mỗi bước của M bao gồm hai giai đoạn: đầu tiên áp dụng δ và sau đó thực hiện một phép đo dự đoán từng phần, trong đó chúng tôi kiểm tra xem M có đang ở trong trạng thái cuối hay không (tức là, một trạng thái bên trong thuộc Q_f). Một cách hình thức, một quá trình tính toán của M trên đầu vào x là một chuỗi các superposition của các cấu hình được tạo ra bởi các ứng dụng tuần tự của U_δ, bắt đầu từ một cấu hình ban đầu của M trên x. Nếu M vào một trạng thái cuối dọc theo một đường dẫn tính toán, đường dẫn tính toán này sẽ kết thúc; nếu không, quá trình tính toán của nó phải tiếp tục.

Một QTM k băng $M = \left(Q, \Sigma, \tilde{\Gamma}^{(k)}, \delta, q_0, Q_f\right)$ được hình thành tốt nếu δ thỏa mãn ba điều kiện cục bộ: độ dài đơn vị, tách biệt, và trực giao. Để giải thích các điều kiện này, như đã trình bày trong [36, Lemma 1], trước tiên chúng tôi giới thiệu các ký hiệu sau. Để tiện lợi, chúng tôi đặt $E = \{0, \pm 1, \pm 2\}$ và $H = \{0, \pm 1, \natural\}$. Cho các phần tử $(p, \sigma, \tau) \in Q \times \left(\tilde{\Gamma}^{(k)}\right)^2, \epsilon = (\varepsilon_i)_{i\in[k]} \in E^k$, và $d = (d_i)_{i\in[k]} \in D^k$, chúng tôi định nghĩa $D_\epsilon = \left\{d \in D^k \mid \forall i \in [k] \left(|2d_i - \varepsilon_i| \leq 1\right)\right\}$ và $E_d = \left\{\varepsilon \in E^k \mid d \in D_\epsilon\right\}$. Hơn nữa, đặt $h_{d,\epsilon} = (h_{d_i,\varepsilon_i})_{i\in[k]}$, trong đó $h_{d_i,\varepsilon_i} = 2d_i - \varepsilon_i$ nếu $\varepsilon_i \neq 0$ và $h_{d_i,\varepsilon_i} = \natural$ trong trường hợp ngược lại. Cuối cùng, chúng tôi định nghĩa $\delta(p, \sigma) = \sum_{q,\tau,d} \delta(p, \sigma, q, \tau, d)|q, \tau, d\rangle$ và $\delta[p, \sigma, \tau \mid \epsilon] = \sum_{q\in Q} \sum_{d\in D_\epsilon} \delta(p, \sigma, q, \tau, d) \left|E_d\right|^{-1/2} |q\rangle \left|h_{d,\epsilon}\right\rangle$, trong đó $\sigma, \tau \in \tilde{\Gamma}^{(k)}$ và $d \in D^k$.

1. (độ dài đơn vị) $\|\delta(p, \sigma)\| = 1$ cho tất cả $(p, \sigma) \in Q \times \tilde{\Gamma}^{(k)}$.

2. (trực giao) $\delta(p_1, \sigma_1) \cdot \delta(p_2, \sigma_2) = 0$ cho bất kỳ cặp khác biệt nào $(p_1, \sigma_1), (p_2, \sigma_2) \in Q \times \tilde{\Gamma}^{(k)}$.

3. (tách biệt) $\delta[p_1, \sigma_1, \tau_1 \mid \epsilon] \cdot \delta[p_2, \sigma_2, \tau_2 \mid \epsilon'] = 0$ cho bất kỳ cặp khác biệt nào $\epsilon, \epsilon' \in E^k$ và cho bất kỳ cặp $(p_1, \sigma_1, \tau_1), (p_2, \sigma_2, \tau_2) \in Q \times \left(\tilde{\Gamma}^{(k)}\right)^2$.
   Điều kiện hình thành tốt của một QTM nắm bắt tính đơn vị của toán tử tiến hóa theo thời gian của nó.
   Định lý 2.1 (Định lý Hình thành tốt của [36]) Một QTM k băng với một hàm chuyển tiếp δ được hình thành tốt nếu và chỉ nếu toán tử tiến hóa theo thời gian của M bảo toàn chuẩn ℓ_2.

Cho một tập hợp không rỗng K của $\mathbb{C}$, chúng tôi nói rằng một QTM có biên độ trong K nếu tất cả các giá trị của hàm chuyển tiếp lượng tử của nó thuộc về K. Việc giới hạn lựa chọn biên độ trong một tập hợp hợp lý K là rất quan trọng. Với việc sử dụng một tập hợp như vậy K, chúng tôi giới thiệu hai lớp độ phức tạp quan trọng BQP_K và FBQP_K.

Định nghĩa 2.2 Giả sử K là bất kỳ tập hợp không rỗng nào của $\mathbb{C}$ và Σ là bất kỳ bảng chữ cái nào.

1. Một tập hợp con S của Σ^* thuộc về BQP_K nếu tồn tại một QTM đa băng, thời gian đa thức, được hình thành tốt M với biên độ trong K sao cho, đối với mọi chuỗi x, M xuất ra $S(x)$ với xác suất ít nhất 2/3[5].

2. Một hàm đơn giá trị f từ Σ^* đến Σ^* được gọi là có thể tính toán trong thời gian đa thức với lỗi giới hạn nếu tồn tại một QTM đa băng, thời gian đa thức, được hình thành tốt M với biên độ trong K sao cho, trên mọi đầu vào x, M xuất ra $f(x)$ với xác suất ít nhất 2/3. Gọi FBQP_K là tập hợp tất cả các hàm như vậy 38.

Việc sử dụng các biên độ phức tạp tùy ý hóa ra làm cho BQP_K trở nên mạnh mẽ. Như Adleman, DeMarrais, và Huang 1 đã chứng minh, $\mathrm{BQP}_{\mathbb{C}}$ chứa tất cả các ngôn ngữ có thể có, và do đó $\mathrm{BQP}_{\mathbb{C}}$ không còn là đệ quy nữa. Do đó, chúng tôi thường chỉ chú ý đến các biên độ có thể xấp xỉ trong thời gian đa thức và, vì lý do này, khi $K = \tilde{\mathbb{C}}$, chúng tôi luôn bỏ qua chỉ số K và viết tắt BQP và FBQP thay cho BQP_K và FBQP_K, tương ứng. Cũng có thể giới hạn tập hợp biên độ K hơn nữa thành $\left\{0, \pm 1, \pm\frac{3}{5}, \pm\frac{4}{5}\right\}$ vì $\mathrm{BQP} = \mathrm{BQP}_{\left\{0, \pm 1, \pm\frac{3}{5}, \pm\frac{4}{5}\right\}}$ đúng 1 .

2.3 Mạch Lượng Tử

Một cổng lượng tử k-qubit, với $k \in \mathbb{N}^+$, là một phép toán đơn vị tác động lên một không gian Hilbert có kích thước 2^k. Vì bất kỳ trạng thái lượng tử nào cũng là một vectơ trong một không gian Hilbert nhất định, nên mỗi mục của trạng thái lượng tử như vậy thường được gọi là một biên độ. Các phép toán đơn vị, chẳng hạn như biến đổi Walsh-Hadamard (WH) và biến đổi có điều kiện-NOT (CNOT) được định nghĩa như sau

$$WH = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ và } CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

là các cổng lượng tử điển hình tác động lên 1 qubit và 2 qubit, tương ứng. Nếu một cổng lượng tử U tác động lên k qubit được áp dụng cho một trạng thái lượng tử k-qubit $|\phi\rangle$, thì chúng tôi thu được một trạng thái lượng tử mới $U|\phi\rangle$. Lưu ý rằng mỗi cổng lượng tử đều bảo toàn chuẩn của bất kỳ trạng thái lượng tử nào được cung cấp dưới dạng đầu vào. Một mạch lượng tử là một tích của một số hữu hạn các lớp, trong đó mỗi lớp là một tích Kronecker của các cổng lượng tử được phép. Chúng tôi thường tập trung vào một tập hợp cụ thể các cổng lượng tử để xây dựng các mạch lượng tử. Hãy xem xét các cổng lượng tử cụ thể: cổng CNOT và ba cổng một qubit có dạng

$$Z_{1,\theta} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix}, \quad Z_{2,\theta} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \quad \text{và } R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

trong đó θ là một số thực với $0 \leq \theta \leq 2\pi$. Lưu ý rằng WH bằng $R_{\frac{\pi}{4}}$. Những cổng này tạo thành một tập hợp cổng lượng tử phổ quát [2] vì WH và $Z_{2,\frac{\pi}{4}}$ (được gọi là cổng $\pi/8$) có thể xấp xỉ bất kỳ phép toán đơn vị một qubit nào với độ chính xác tùy ý. Vì sự tiện lợi, chúng tôi gọi chúng là các cổng cơ bản. Tập hợp các cổng CNOT, WH, và $Z_{2,\frac{\pi}{4}}$ cũng được biết là phổ quát 6.

Cho một tập hợp biên độ K, một mạch lượng tử C được cho là có biên độ trong K nếu tất cả các mục của mỗi cổng lượng tử được sử dụng bên trong C đều được lấy từ K. Đối với bất kỳ cổng lượng tử k-qubit và bất kỳ số nguyên nào $n > k, G^{(n)}$ biểu thị $G \otimes I^{\otimes n-k}$, sự mở rộng n-qubit của G. Một mạch lượng tử n-qubit được định nghĩa một cách chính thức là một chuỗi hữu hạn $(G_m, \pi_m), (G_{m-1}, \pi_{m-1}), \cdots, (G_1, \pi_1)$ sao cho mỗi G_i là một cổng lượng tử n_i-qubit với $n_i \leq n$ và π_i là một hoán vị trên $\{1, 2, \ldots, n\}$. Mạch lượng tử này đại diện cho phép toán đơn vị $U = U_m U_{m-1} \cdots U_1$, trong đó U_i có dạng $V_{\pi_i}^\dagger G_i^{(n)} V_{\pi_i}$ và $V_{\pi_i}(|x_1 \cdots x_n\rangle) = \left|x_{\pi_i(1)} \cdots x_{\pi_i(n)}\right\rangle$ cho mỗi $i \in [m]$. Kích thước của một mạch lượng tử là tổng số cổng lượng tử trong đó. Yao 40 và sau này Nishimura và Ozawa 26 đã chỉ ra rằng, đối với bất kỳ QTM k băng và một đa thức p, tồn tại một họ các mạch lượng tử có kích thước $O\left(p(n)^{k+1}\right)$ chính xác mô phỏng M.

Một họ $\{C_n\}_{n\in\mathbb{N}}$ của một mạch lượng tử được gọi là đồng nhất P nếu tồn tại một máy Turing (cổ điển) xác định mà, trên đầu vào 1^n, tạo ra một mã của C_n trong thời gian đa thức kích thước của C_n, với điều kiện chúng tôi sử dụng một sơ đồ mã hóa cố định, hiệu quả để mô tả mỗi mạch lượng tử.

Định lý 2.3 [40 (xem thêm [26]) Đối với bất kỳ ngôn ngữ nào L trên một bảng chữ cái $\{0,1\}, L$ thuộc về BQP nếu và chỉ nếu tồn tại một đa thức p và một họ đồng nhất P $\{C_n\}_{n\in\mathbb{N}}$ của các mạch lượng tử có biên độ $\tilde{\mathbb{C}}$-amplitudes sao cho $\left\|\langle L(x)|C_{|x|}\left|x10^{p(|x|)}\right\rangle\right\|^2 \geq \frac{2}{3}$ đúng cho tất cả $x \in \{0,1\}^*$, trong đó L được coi là hàm đặc trưng của L.

Chứng minh đầy cảm hứng của Yao 40 về Định lý 2.3 cung cấp nền tảng cho chứng minh của chúng tôi về Định lý 4.3 , điều này cung cấp trong Phần 3.1 một sự mô phỏng của một QTM được hình thành tốt bởi một hàm $\square_1^{\mathrm{QP}}$ -function được chọn một cách thích hợp.

3 A New, Simple Schematic Definition

Như đã lưu ý trong Phần 1 , định nghĩa "sơ đồ" của hàm đệ quy có nghĩa là một cách quy nạp (hoặc xây dựng) để định nghĩa tập hợp các hàm có thể tính toán và nó liên quan đến một tập hợp nhỏ các hàm được gọi là các hàm ban đầu cũng như một tập hợp nhỏ các quy tắc xây dựng, được áp dụng tuần tự hữu hạn nhiều lần để xây dựng các hàm phức tạp hơn từ một số hàm đã được xây dựng trước đó. Một sự đặc trưng sơ đồ tương tự đã được biết đến đối với các hàm có thể tính toán trong thời gian đa thức (cũng như các ngôn ngữ) [7, 8, 9, 24, 35. Theo hướng đi này, chúng tôi mong muốn trình bày một định nghĩa sơ đồ mới, đơn giản được cấu thành từ một tập hợp nhỏ các hàm lượng tử ban đầu và một tập hợp nhỏ các quy tắc xây dựng, nhằm mục đích làm cho định

nghĩa sơ đồ này nắm bắt một cách thích hợp các hàm lượng tử có thể tính toán trong thời gian đa thức, nơi mà một hàm lượng tử là một hàm ánh xạ $\mathcal{H}_\infty$ đến $\mathcal{H}_\infty$. Như đã được đề cập ngắn gọn trong Phần 1, điều quan trọng cần lưu ý là thuật ngữ "hàm lượng tử" của chúng tôi hoàn toàn khác với thuật ngữ được sử dụng trong, ví dụ, [38], trong đó "hàm lượng tử" đề cập đến các hàm nhận các chuỗi đầu vào cổ điển và tạo ra hoặc là các chuỗi đầu ra cổ điển hoặc là các xác suất chấp nhận của các QTM đa băng có thời gian đa thức được hình thành tốt và do đó nó ánh xạ Σ^* đến hoặc là Σ^* hoặc là khoảng thực $[0, 1]$, nơi mà Σ là một bảng chữ cái thích hợp.