TẠP CHÍ KHOA HỌC, TRƯỜNG ĐẠI HỌC HỒNG ĐỨC - SỐ 18. 2014

Ở NGƯỠNG CỬA CỦA CÁCH MẠNG LƯỢNG TỬ TRONG TIN HỌC

Nguyễn Mạnh An[1], Nguyễn Văn Hóa[2], Cao Long Vân[3]

TÓM TẮT

Từ khóa:

Tin học và lý thuyết lượng tử chắc chắn là hai dòng thác trí thức lớn nhất của thế kỷ XX đã làm thay đổi hoàn toàn nền văn minh của nhân loại. Tin học, nói khác đi là khoa học về máy tinh, mặc dù phôi thai từ thời Charles Babbage vào đầu thế kỷ XIX, đã có được cơ sở toán học vững chắc nhờ các công trình của nhà toán học gốc Hung (mà người ta thường nói rằng, đó là một trong những người của „Sao Hỏa" đã hạ cánh xuống Hung-Ga-Ri vào đầu thế kỷ XX) John von Neumann trong những năm bốn mươi của thế kỷ trước. Một sự trùng lặp thú vị là Ông cũng đã xây dựng cơ sở toán học cho lý thuyết lượng tử, một trong hai trụ cột của vật lý hiện đại và là lĩnh vực của vật lý đã mang lại những hiệu quả thực tiễn lớn lao. Hai hiệu quả rực rỡ nhất là năng lượng hạt nhân và công nghệ bán dẫn, được khai trương bởi hai thí nghiệm nổi tiếng: bắn phá hạt nhân nguyên tử của Ernest Rutherford năm 1919 và tìm ra các bóng bán dẫn (transistor) năm 1948 bởi John Bardeen, Walter Brattain và William Shocley (Giải Nobel năm 1956). Có thể nói rằng việc phát hiện ra bóng bán dẫn đối với nhân loại là quan trọng hơn việc tìm ra năng lượng hạt nhân bởi lẽ năng lượng hạt nhân, mặc dù là một nguồn năng lượng mới quan trọng, đến nay vẫn chưa chiếm được ưu thế trong các nguồn năng lượng nói chung nhưng đã được tiềm vọng, thậm chí do vấn đề an ninh mà một số nước trên thế giới (như Đức) đã bỏ dần nguồn năng lượng này. Ngược lại việc phát hiện ra các bóng bán dẫn, và sau đó là các hệ liên kết (intergrated circuit) năm 1959 (Jack Kilby, Giải Nobel năm 2000) đã đưa đến việc vi hóa các máy tính ở mức không thể tưởng tượng được trước đó, thúc đẩy sự phát triển vĩ đại của loài người. Việc „cài đặt" bán dẫn các ý tưởng của Von Neuman đã dẫn đến việc sản xuất ra các máy tính càng ngày càng nhỏ, càng nhanh và càng rẻ.

[1,2] *TS. Khoa KHTN, Trường Đại học Hồng Đức*
[3] *GS. TS. Khoa Vật lý, Đại học Zielona Góra*

Tốc độ phát triển vi tính hóa được mô tả tốt nhất qua một quy luật kinh nghiệm (empirical) của Gordon Moore, một trong những người sáng lập ra công ty máy tính nổi tiếng Intel. Qua quan sát sự gia tăng số lượng bóng bán dẫn trong một hệ hợp nhất (intergrated system), ông đã rút ra được quy luật rằng, hàng năm số lượng này sẽ tăng gấp đôi (sau chu kỳ này được thay thành hai năm một). Theo quy luật này, càng ngày càng nhiều các bóng bán dẫn được đặt trong một hệ hợp nhất càng ngày càng nhỏ. Đến một lúc nào đó trong tương lai gần, ta sẽ tiến đến các giới hạn công nghệ và kinh tế được xác định bởi chính vật lý, điều có lẽ đã xảy ra hiện nay. Mọi quá trình quang ấn (photolitographic) hiện đại đều vô dụng. Không chỉ kích thước của các bóng bán dẫn bị nhỏ đi mà các các nối giữa chúng cũng bị thu nhỏ lại. Các mật độ dòng lớn sẽ phá hủy các mạch dẫn này. Một vấn đề khó khăn khác là giải nhiệt được sinh ra từ một mạch nhỏ như vậy. Ở đây nhiệt năng được sinh ra bởi hai nguyên nhân. Thứ nhất, các bóng bán dẫn tắt và bật trong hệ hợp nhất rất không có hiệu suất về năng lượng, một phần không nhỏ năng lượng bị mất mát qua giải nhiệt. Thứ hai, một định luật do Landauer tìm ra nói rằng, cứ xóa đi một bit thông tin, ta sẽ mất đi một năng lượng ở dạng tỏa nhiệt, cỡ bằng động năng của một phân tử khí ở nhiệt độ trong phòng. Các cổng logic cơ sở cổ điển như AND, OR hoạt động theo kiểu là ở đầu vào ta có hai bit, còn ở đầu ra chỉ còn một bit, do vậy một bit đã bị xóa, điều này gây ra sự tỏa nhiệt. Lúc đó ta nói rằng các cổng này là không thuận nghịch. Do nhiều tỷ tính toán kiểu này mà các hệ thống nhất được vi hóa bị ”tự nung nóng” và phá hủy trong một thời gian rất ngắn.

Ngoài ra có một lớp các vấn đề không thể giải được bằng những máy tính hiện đại. Mười mấy năm gần đây chúng đã bị gọi là các ”máy tính cổ điển”. Khái niệm cổ điển chỉ là tương đối, phụ thuộc nhiều vào tốc độ phát triển trong lĩnh vực liên quan, điều đã được Roy Glauber lưu ý đến trong bài giảng nhân dịp nhận giải Nobel năm 2005. Khi một lĩnh vực kiến thức hay nghệ thuật cho trước phát triển nhanh, khái niệm ”cổ điển” thường là rất mới, ví dụ nhạc cổ điển có trên hai trăm năm, vật lý cổ điển có cách đây hơn một trăm năm, còn máy tính cổ điển đến nay vẫn còn đang hoạt động. Trong nhiều trường hợp, ngay cả những vấn đề giải được cũng không thể được thực hiện do tính phức tạp lớn của các thuật toán mô tả chúng. Một ví dụ chuẩn thường được nói đến là vấn đề phân một số nguyên lớn ra các thừa số nguyên tố. Để phân một số có 400 chữ số ra các thừa số nguyên tố, công suất tính hiện thời cần phải có một thời gian tính toán cỡ bằng tuổi của Vũ trụ. Vấn đề toán học này là nhân tố căn bản trong mật mã nổi tiếng RSA (viết tắt theo tên của những người xây dựng ra mật mã này: R. L. Rivest, A. Shamir, L. Adelman). RSA đang được dùng rộng rãi trên internet và các ngân hàng. Như ta sẽ thấy, máy tính lượng tử giải được vấn đề này trong vòng vài phút, như vậy mật mã này hoàn toàn không phải là an toàn. Song lý thuyết lượng tử rất ”công bằng”, một tay lấy đi, một tay cho lại. Trong khuôn khổ lĩnh vực được gọi là mã hóa lượng tử, một số các hệ mã hóa an toàn được thiết lập. Chúng không thể bị giải hay nghe trộm được. Mã hóa lượng tử phát triển rất nhanh và nay đã chuyển sang giai đoạn

thương mại. Ở khía cạnh này nó đã vượt sự phát triển của các máy tính lượng tử, do để chuyển giao thông tin chúng chỉ cần một số lượng không lớn các qubit (được định nghĩa dưới đây).

Thật đáng ngạc nhiên là lý thuyết lượng tử được xây dựng trong những năm hai mươi của thế kỷ trước trên một khung toán học khá "cứng" tương ứng với "lý trí lành mạnh" của ta, lại đưa đến những hệ quả không ngờ, dường như trái ngược hoàn toàn với lý trí đó. Những hệ quả đó đem lại sự phát triển vượt bậc của nền văn minh, qua việc phát triển các ngành như điện tử học, đặc biệt trong lĩnh vực máy tính được nhắc đến ở trên. Chỉ cần nhớ rằng trên 80 phần trăm thu nhập của thế giới có sự tham gia của lý thuyết lượng tử. Thế giới lượng tử bí ẩn, kỳ lạ nhưng rõ ràng rất hữu hiệu luôn đem lại cho ta những kết quả bất ngờ, như sự phát triển của các công nghệ tin học lượng tử trong những năm chín mươi của thế kỷ trước. Chúng đã xuất hiện là kết quả nối vật lý lượng tử với công nghệ máy tính, dựa trên những thành quả mới nhất của vật lý chất rắn, vật lý nguyên tử và phân tử, của quang học và điện tử học lượng tử. Điều này dẫn đến sự xuất hiện một lĩnh vực khoa học mới là **tin học lượng tử**. Những thí nghiệm ban đầu thành công đã góp phần xây dựng những mẫu máy tính lượng tử đầu tiên, cho phép ta tin tưởng rằng, ta đang ở ngưỡng cửa của một cuộc cách mạng công nghệ mới, ít nhất có tầm cỡ như cuộc cách mạng đã xảy ra hơn sáu mươi năm trước, khi các bóng bán dẫn đã được phát kiến.

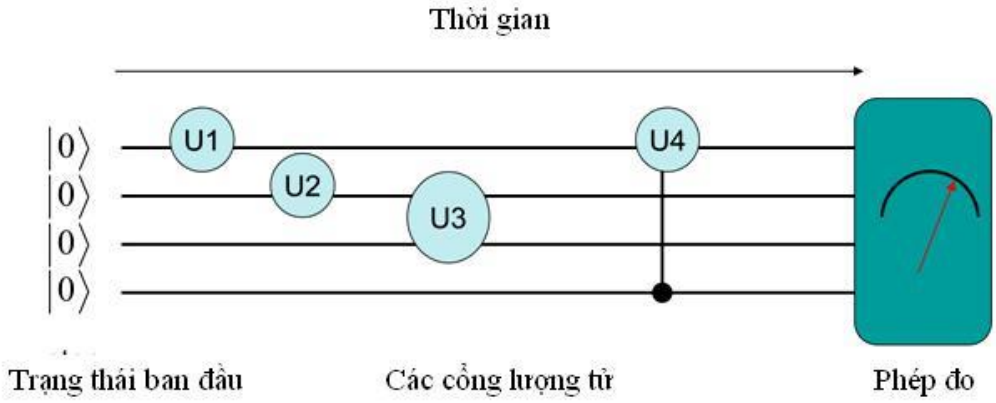
Ý tưởng tính toán lượng tử đã bắt nguồn từ "kho" các ý tưởng độc đáo của một trong những bộ óc vĩ đại nhất thế kỷ hai mươi, bộ óc của nhà vật lý Mỹ Richard Feynman (giải thưởng Nobel 1965). Từ năm 1982 ông đã thấy, khi giả lập động lực học của một hệ nhiều hạt bằng máy tính cổ điển, thời gian tính toán sẽ lớn theo hàm mũ khi số hạt tăng, đòi hỏi phải thiết kế một máy tính hoạt động theo những định luật lượng tử. Ba năm sau, nhà toán học Anh Dawid Deutsch đã xây dựng nên những cơ sở cho máy tính đó mà sau này được gọi là **máy tính lượng tử**.

Trong những năm bốn mươi của thế kỷ trước, cũng Feynman đã nhấn mạnh nguyên tắc cộng các biên độ xác suất chứ không phải cộng chính các xác suất, một khi tồn tại các khả năng thực hiện (các con đường) khác nhau của một quá trình cho trước. Các biên độ này là các số phức (người ta thường nói không gian các trạng thái của một hệ cho trước là một không gian Hilbert, mà trước hết nó là không gian vectơ trên trường số phức), tức là có thể biểu diễn các biên độ này bằng mô-đun và pha. Qua công thức Euler nổi tiếng ta có các sin và côsin. Từ trường trung học ta đều biết các hàm lượng giác này biểu diễn các sóng. Nếu chúng được chồng chất tương ứng, ta sẽ có các **giao thoa** xây (constructive) hay hủy (destructive). Cũng có thể từ định nghĩa số phức biểu diễn sự đóng góp của mỗi con đường bằng hai số thực, chúng được coi như hai thành phần của một vectơ có độ dài không đổi những có hướng tùy ý. Việc cộng những đóng góp từ các đường đi khác nhau tương đương với cộng các vectơ này. Trong trường hợp chung, những con đường này là vô số, đòi hỏi phải biết giải tích hàm được xây dựng bởi Stefan Banach và các nhà toán học khác. Lúc đó

ta có hình thức luận "tích phân đường" của Richard Feynman. Trong một số trường hợp, số lượng các đường chiếm ưu thế là hữa hạn. Lúc đó việc cộng một số lượng hữu hạn các vectơ không phải là vấn đề khó. Các thuật toán lượng tử về cơ bản là các thủ tục điều khiển các biên độ này. Cần phải nghĩ ra một thủ tục dẫn đến các giao thoa lượng tử xây, sao cho kết quả từ chúng là thu được những kết quả mong muốn, còn các kết quả không mong muốn sẽ bị loại trừ qua các giao thoa hủy.

Tất nhiên việc nghĩ ra các thuật toán như vậy là một việc làm rất khó, vì nhà nghiên cứu ngoài việc hiểu biết rất tốt tin học cổ điển còn phải biết sâu sắc lý thuyết lượng tử, một lý thuyết thường cho những kết quả ngược với "lý trí lành mạnh". Song thực tế đã chỉ ra rằng đây không phải là "mission impossible" (việc làm bất khả thi). Một số thuật toán lượng tử đã được tìm ra. Nổi tiếng nhất là thuật toán viễn tải đã được thực hiện trên một hệ vật lý cụ thể và thuật toán Shor phân tích một số tự nhiên lớn ra các thừa số nguyên tố, đã được thực hiện trên một bộ xử lý bảy **qubit** (bit lượng tử) để thực hiện thừa số hóa số 15 = 3.5. Trong thuật toán này, các giao thoa lượng tử xây dẫn đến các cặp số rất gần lời giải đúng với một xác suất lớn. Khả năng điều khiển ở mức các biên độ xác suất chứ không phải ở mức các xác suất là cơ sở của mọi công nghệ lượng tử, không chỉ cho việc xây dựng các máy tính lượng tử. Máy tinh cổ điển không có khả năng tiếp cận với các biên độ của vectơ trạng thái là tổ hợp tuyến tính của các vectơ của cái gọi là **cơ sở tính toán**, khái niệm sẽ được đề cập đến dưới đây.

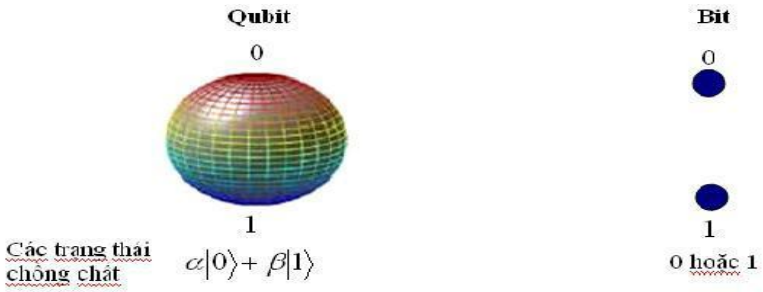
Một câu hỏi được đặt ra, các máy tính lượng tử có ưu thế gì đối với các máy tính cổ điển? Để thấy được điều này, ta hãy xem xét kỹ hơn sự hoạt động của một máy tính lượng tử. Sơ đồ các mày tính lượng tử được biểu diễn trên hình 1.



Hình 1

Ở đầu vào là trạng thái ban đầu của hệ vật lý thực hiện các tính toán lượng tử theo các định luật của vật lý lượng tử. Hệ đơn giản nhất là một **qubit**, đơn vị nhỏ nhất của tin học lượng tử, là khái niệm tương ứng của bit cổ điển với các trạng thái chỉ có thể là 0 hoặc 1. Bit là một phần tử cơ bản của một máy tính cổ điển bất kỳ, có thể được cài đặt bằng một

hệ vật lý bất kỳ chỉ có hai trạng thái. Trong các máy tính hiện thời, hệ này là một bóng bán dẫn đã được nói đến ở trên. Khác với bit, trạng thái của một qubit nằm trên một continum của mặt cầu hai chiều với bán kính bằng 1, được gọi là mặt cầu Bloch (Hình 2)., vì qubit không chỉ nằm trong hai trạng thái đặc biệt mà còn nằm trong một trạng thái bất kỳ là tổ hợp tuyến tính (phức) của chúng, điều là hệ quả của việc không gian Hilbert các trạng thái của qubit trước hết là một không gian vectơ, trong đó một vectơ bất kỳ có thể được biểu diễn ở dạng chồng chất của các vectơ thuộc **cơ sở tính toán**. Nó có thể được cài đặt bằng một hệ lượng tử bất kỳ hai trạng thái, ví dụ bằng một hạt có spin ½ như điện tử, hay một phôtôn ở các trạng thái phân cực khác nhau.



Hình 2

Vậy một qubit có thể nằm trong các trạng thái 0 hay 1, hoặc trong một tổ hợp bất kỳ của chúng, có nghĩa là có thể đồng thời biểu diễn cho không hay một. Như ta đã nhấn mạnh trên đây, đây là hệ quả của tiên đề về các trạng thái, một trong những tiên đề cơ bản của hình thức luận lượng tử. Cho đến nay không có bất cứ một dữ liệu thực nghiệm nào mâu thuẫn với tiên đề này. Thế nào là đồng thời "tàng trữ" không và một? Theo minh họa của trường phái Copenhagen hiện đang được chấp nhận bởi cộng đồng các nhà vật lý, nếu ta thực hiện một phép đo trên qubit như vậy, trạng thái tổ hợp sẽ bị phá hủy (collapse) đến một trong hai trạng thái 0 hay 1 (tức là qubit sẽ rơi hoặc vào trạng thái 0, hoặc trạng thái 1) với xác suất tương ứng bằng $|\alpha|^2$ hay $|\beta|^2$ (tất nhiên $|\alpha|^2 + |\beta|^2 = 1$). Từ đó ta thấy rằng hệ lượng tử rất "hà tiện". Từ sợi giàu có lớn lao (continuum) của nguồn tài nguyên thông tin của mình, hệ chỉ cho ta biết một số lượng hữu hạn các thông tin, hơn nữa chỉ ở dạng ngẫu nhiên! Song như ta thấy dưới đây, "kẻ hà tiện" lượng tử đó cho phép ta ghi một số lượng thông tin khổng lồ so với bộ nhớ cổ điển. Ngoài ra nó còn cho phép ta được **tính toán trước khi đo**, nghĩa là tính toán trên các tổ hợp: khi có một qubit có thể thực hiện tính toán đồng thời hai tính toán song song. Như vậy qubit đảm nhận đồng thời vai trò là bộ nhớ hoạt lẫn là một đơn vị tính toán.

Tập một số hữu hạn các qubit được gọi là một **bộ ghi (register)**. Một tiên đề tiếp của cơ học lượng tử nói rằng, trạng thái của register là tích tenxơ của tất cả các không gian qubit hai chiều có trong thành phần của register cho trước. Những tính toán đại số đơn giản chỉ ra rằng, một register hai qubit biểu diễn một tổ hợp bất kỳ của bốn trạng thái (00, 01, 10,

11), còn một register ba qubit – một tổ hợp bất kỳ của tám trạng thái (000, 001, 010, 011, 100, 101, 110, 111) v.v. Ví dụ nếu ta chuẩn bị trạng thái ban đầu của một qubit là $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, lúc đó register hai qubit tàng trữ đồng thời bốn số 0, 1, 2, 3 (có dạng nhị phân 00, 01, 10, 11) , còn register ba qubit – tám số 0, 1, 2, 3, 4, 5, 6, 7. Nói chung, một register N qubit tàng trữ 2^N số. Ngoài ra, việc tính toán trước khi đo trên các trạng thái tổ hợp cho ta khả năng tính toán song song: một bước tính lượng tử tác động lên cả register, ngay cả khi chỉ tác động lên một hay vài qubit của register (kiểu U1, U2, U3, U4 trên hình 1) gây ra sự thay đổi tất cả các số được ghi trên register cho trước.

Theo một tiên đề khác của cơ học lượng tử, các phép tính là các toán tử (ma trận) unita, quan trọng hơn nữa là các phép tính (các cổng) lượng tử là thuận nghịch, dẫn đến không có sự tỏa nhiệt do xóa đi các thông tin (các bit) như định lý Landauer đã đề cập đến. Một bộ xử lý N qubit tương đương với 2^N bộ xử lý cổ điên song song, tức là giải được một vấn đề cho trước trong thời gian gần bằng thời gian tính toán của một số lượng như vậy các bộ xử lý cổ điển song song.

Hệ tổng hợp của hai hay nhiều các hệ con còn có một tính chất quan trọng: các hệ con của nó có các tương quan lượng tử mà tồn tại ngay cả khi các hệ con này ở rất xa nhau, nghĩa là khi không hề có bất cứ một sự liên quan nào theo nghĩa cổ điển. Sự „tác động ma quái trên khoảng cách" này, như Albert Einstein đã gọi, là hệ quả của tính phi địa phương của cơ học lượng tử. Cùng với các cộng sự trẻ hơn của mình là Borys Podolski i Natan Rosen, ông đã dùng điều này trong một công trình được công bố năm 1935 để phê phán minh họa của trường phái Copenhagen với người đứng đầu là Niels Bohr. Để ví dụ ta xem xét một thí nghiệm tưởng tượng, trong đó có chú mèo nổi tiếng của Erwin Schrödinger. Theo nguyên tắc chồng chất, hệ phức hợp (nguyên tử + chú mèo) có thể nằm trong trạng thái

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\text{, mèosèng }\rangle + |\text{, mèochÕt }\rangle\right).$$

Bây giờ ta sẽ tưởng tượng rằng, hai nhân vật, ví dụ như Alice và Bob, có hệ được chuẩn bị trong một trạng thái như vậy. Một ngày nào đó Bob du hành rất xa, ví dụ đến một hệ thiên hà láng giềng sông Ngân Hà của chúng ta. Anh mang theo chú mèo và để lại cho Alice trên Trái đất nguyên tử. Cũng một ngày nào đó Alice thực hiện việc quan sát nguyên tử trong phòng thí nghiệm của mình. Chị sẽ thu được hai kết quả có thể có với xác suất như nhau: nguyên tử bị phân rã hay không bị phân rã. Khi kết quả chị thu được là sự phân rã của nguyên tử, chị biết là ngay lúc đó chú mèo mà Bob mang theo bị chết, còn khi nguyên tử chưa phân rã, chú mèo sống. Trong thư của mình viết cho Einstein, ông đã gọi „sự tác động ma quái trên khoảng cách", này (cũng giống như sự tương quan giữa hai hạt trong thí nghiệm tưởng tượng của EPR) bằng tiếng Đức là **verschränkung** (tiếng Anh:

entanglement – sự đan rối). Sự nhất trí của hai nhà bác học này trong phê phán cơ học lượng tử đã bị Niels Bohr bình luận sau đó (trong tháng ba năm 1936) là một việc làm „đáng chê trách", có thể coi đó như là „một vụ đảo chính"! Những thí nghiệm được thực hiện trong năm 1982 bởi Alain Aspect và các cộng sự đã chỉ ra rằng lý thuyết lượng tử theo minh họa Copenhagen là đúng, còn sự phê phán của Einstein và những người khác là sai. Nói một cách toán học, trong không gian Hilbert các trạng thái của hệ phức hợp là tích tenxơ của các không gian trạng thái thành phần, tồn tại các vectơ trạng thái mà không thể biểu diễn chúng được là các tích ten xơ của các vec tơ trạng thái thành phần. Trong ví dụ trên ta có:

$$\left| \ \right\rangle \neq \Psi_{\text{Nguyên tử}} \otimes \Psi_{\text{Mèo}} .$$

Tính đan rối không địa phương là một trong những nguồn tài nguyên chính của tin học lượng tử, ví dụ nó được dùng trong **viễn tải các trạng thái lượng tử.** các cặp hạt đan rối như các nguyên tử hay các phôtôn (được gọi là các cặp EPR) trở thành các thành phần quan trọng của các thuật toán (các biên bản-protocol) lượng tử khác nhau. Tưởng như rằng nhờ đan rối có thể xây dựng được các hệ chuyển thông tin ngay tức thì. Song như ta thấy từ ví dụ ở trên, Bob chỉ có thể khẳng định chắc chắn là chú mèo của mình sống hay chết khi Alice thông báo cho Bob những thông tin về kết quả quan sát của mình qua các kênh truyền thống như điện thoại hay internet. Vậy tiên đề nói vận tốc ánh sáng là vận tốc giới hạn vẫn được bảo toàn. Tương tự trong trường hợp viễn tải, khi không có những thông tin từ Alice qua các kênh truyền thông truyền thống, Bob không thể „chế biến" thích hợp trạng thái của hạt thuộc cặp EPR mà anh mang theo để thu được trạng thái qubit được viễn tải. Hai trụ cột của vật lý hiện đại, lý thuyết lượng tử và lý thuyết tương đối một lần nữa lại „chung sống hòa bình", cũng như chúng đã làm trong khuôn khổ lý thuyết trường lượng tử, một lý thuyết kết hợp hai trụ cột đó để mô tả mọi hiện tượng trong thiên nhiên.

Theo quan điểm toán học, tính toán lượng tử về cơ bản là rất đơn giản. Nó được thực hiện trong các không gian Hilbert hữu hạn chiều, trong đó các vectơ (rejestr) và các toán tử tuyến tính (các cổng) được biểu diễn bằng các cột và các ma trận. Mọi khó khăn liên quan đến tính vô hạn không còn nữa.

Dường như yếu điểm của các máy tính lượng tử có thể là việc đọc một cách ngẫu nhiên các kết quả của phép đo trên trạng thái cuối như trên hình 1.

Thật may là số lượng các kết quả có thể có là hữu hạn. Có thể thẩm tra chúng bằng các thuật toán nhanh để khẳng định kết quả nào từ chúng là đúng. Như trong trường hợp thuật toán Shor được đề cập đến trên đây, nhân hai số nguyên tố thu được là một việc làm hết sức dễ, dễ hơn nhiều việc làm ngược lại là phân tích một số cho trước ra hai thừa số nguyên tố.

Khó khăn chính trong việc xây dựng máy tinh lượng tử là ở chỗ khác, đó là sự mâu thuẫn giữa các yêu cầu được đặt ra đối với máy tính lượng tử. Một mặt các máy tính này

phải được cách ly khỏi môi trường xung quanh để bảo toàn được các tính chất kết hợp cần thiết, tức là bảo toàn được các tổ hợp của các trạng thái. Chúng rất mong manh, dễ bị phá vỡ. Môi trường xung quanh không ngừng đo và phá hủy chúng. Sự mất mát thông tin ra ngoài hệ lượng tử được gọi là sự **hủy kết hợp**. Đây cũng là nguyên nhân chính tại sao ta không quan sát được các biểu hiện lượng tử kỳ quặc trong cuộc sống hàng ngày. Mặt khác các qubit đồng thời phải sẵn sàng là đối tượng cho những điều khiển (sự tiến hóa) và đọc (các phép đo). Nhiệm vụ của các nhà thiết kế máy tính lượng tử là phải tìm ra được sự "dung hòa vàng", cho phép sự hủy kết hợp tác động một cách hữu ích, nghĩa là cho phép nó phá hủy (kolaps) tổ hợp lớn các trạng thái của máy tính lượng tử cùng với các tính chất giao thoa tế nhị của chúng đến một trạng thái đơn độc biểu diễn kết quả mong muốn. Để tiến đến mục đích này, gần đây nhiều kết quả căn bản đã đạt được trong điều khiển các trạng thái lượng tử đơn độc, đã vài lần được giải thưởng Nobel như: Claude Cohen Tannoudji, Steven Chu, Williams Phillips (1997), Eric Cornell, Wolfgang Keterle, Carl Wieman (2001), Roy Glauber (2005), và gần đây nhất là Serge Haroche, David Wineland đã nhận giải thưởng này vào năm ngoái. Cũng trong năm này, viễn tải cũng là một trong những đối thủ "nghiêng ngửa". Có thể dự đoán rằng, không sớm thì muộn thành tựu này sẽ được đăng quang.

Tình trạng hiện nay trong tin học lượng tử có thể so sánh với tình trạng của năng lượng nguyên tử trong những năm ba mươi của thế kỷ trước. Ta tin tưởng rằng, cũng như trong năng lượng hạt nhân, sau mươi năm nữa ta sẽ có thể có những máy tính lượng tử đầu tiên làm thay đổi hoàn toàn bộ mặt của nền văn minh nhân loại.

Trong các số tới của tập san *Journal of Science*, chúng tôi sẽ lần lượt đang một loạt bài tổng quan, vừa nhằm mục đích giới thiệu lĩnh vực mới này của vật lý với các ý nghĩa hiểu biết và thực tiễn lớn lao, vừa cung cấp những thông tin căn bản để các sinh viên vật lý và toán học có thể tiệm cận và tham gia nghiên cứu những vấn đề liên quan đến thông tin lượng tử. Bạn đọc cũng có thể làm quen với chúng trước trong các công trình tổng quan [1,2,3]. Song các bài viết sắp tới sẽ ở dạng mở rộng hơn, dễ hiểu hơn, dựa trên các bài giảng trong học kỳ hai niên học 2012/2013 tại Trung tâm Nghiên Cứu Khoa Học Cao của ĐHBK Vác-xa-va (Ba Lan).

Đồng thời một số công trinh liên quan đầu tiên cũng sẽ được công bố với sự tham gia của các nhà vật lý trong và ngoài nước.

TÀI LIỆU THAM KHẢO

[1] Cao Long Vân, Tạ Phương Hạnh, Tin học lượng tử và máy tính lượng tử (I), Tạp Chí Ứng Dụng Toán Học, Tập III, Số 1, 2005, 83-102.

[2] Cao Long Vân, Tin học lượng tử và máy tính lượng tử (II), Tạp Chí Ứng Dụng Toán Học, Tập III, Số 2, 2005, 77-100.

[3] Cao Long Vân, Tin học lượng tử và máy tính lượng tử (III): Các thuật toán lượng tử, Tạp Chí Ứng Dụng Toán Học, Tập IV, Số 1, 2006, 73-90.

Nguyen Van Hoa, Nguyen Manh An, Cao Long Van

ABSTRACT

This paper is an introduction to the new domain of physics, namely Quantum Information and Quantum Computer. We introduce some fundamental concepts in three related sciences: computer science, mathematics and physics. The reader could treat this paper as a prelude to our series of papers printed in this Journal, presenting the fundamental tools of quantum information. The paper in an extended form of a lecture given by the third author in the Center of Advanced Studies, Warsaw Technical University in 10 January 2013.

Keywords: