Nghệ thuật hỏi một lần

Tản mạn về tính toán lượng tử và cái nhìn toàn cục

$\langle Fan|Fan\rangle^*$

Tháng 4, 2026

1 Thế giới một phát súng

Thế giới cổ điển dung dưỡng một niềm tin ít khi bị nghi ngờ: niềm tin vào đặc quyền quan sát vô hạn. Trong đời sống thường ngày, ta có thể nghiền ngẫm một trang sách bao nhiêu lần tùy ý, hay ngắm đi ngắm lại một bức tranh để tìm ẩn ý của tác giả mà không làm mòn tác phẩm. Khoa học thực nghiệm cũng được xây dựng trên sự kiên nhẫn lặp lại thí nghiệm, còn thống kê thì đặt niềm tin mạnh mẽ vào luật số lớn. Thậm chí, ngay cả khi con người muốn giấu giếm thông tin, các hệ mật mã cổ điển không cấm đối thủ hỏi nhiều lần, mà sự an toàn được xây dựng trên sự khan hiếm thời gian: không ai có đủ thời gian để thử hết không gian đáp án trước khi dữ liệu hết giá trị. Tóm lại, dù là tìm kiếm chân lý hay che giấu thông tin, thế giới cổ điển đều đồng ý một luật chơi: sự lặp lại là hợp lệ.

Rồi cánh cửa lượng tử mở ra, với một luật chơi hoàn toàn mới. Vũ trụ vi mô tước đi quyền được hỏi nhiều lần. Trong thế giới này, sự đo lường là một hành vi không thể đảo ngược: trước khi đo, một trạng thái lượng tử tồn tại như một chồng chập của nhiều khả năng, như một bản nhạc mà mọi nốt đều có thể vang lên; nhưng ngay khoảnh khắc ta đo, hàm sóng sụp đổ, bản giao hưởng biến mất, chỉ để lại một nốt nhạc duy nhất còn rung động. Hơn nữa, ta không thể lách luật bằng cách sao chép một trạng thái ra nhiều bản để đo nhiều lần, vì Định lý cấm sao chép (No-cloning Theorem) của Wootters, Zurek và Dieks (1982) khẳng định rằng chúng ta không thể nhân bản hoàn hảo một trạng thái lượng tử bất kỳ. Mỗi trạng thái vi mô chưa biết là một độc bản; mỗi lần truy vấn đều làm thay đổi chính bản gốc.

Để nắm bắt luật chơi lượng tử, hãy hình dung có một chiếc hộp Magic, một công cụ "ảo thuật" có thể thao tác trên các khả thể chồng chập và giao thoa mà máy tính cổ điển không chạm tới được. Chừng nào ta chưa nhìn vào hộp, mọi phép màu lượng tử vẫn còn đó. Nhưng khoảnh khắc ta "mở hộp" thì phép màu tan biến: hộp trả lại đúng một kết quả duy nhất trước khi mất hết quyền năng. Muốn hỏi lại, ta phải chuẩn bị một hộp mới từ đầu.

Do đó, câu hỏi ở thế giới lượng tử mang một sức nặng hoàn toàn khác. Mỗi lần mở hộp là một phát súng duy nhất. Khi đó, một câu hỏi tự nhiên là: ta có thể làm được gì với chỉ một lần hỏi? Liệu hiểu biết thu được có đủ để giải quyết một vấn đề lớn, hay mãi mãi chỉ là một mẩu dữ liệu vô dụng? Và nghịch lý hơn: làm sao một công cụ chỉ được hỏi một lần lại có thể mạnh hơn máy tính cổ điển được hỏi nhiều lần?

Để trả lời câu hỏi này, chúng ta cần chuyển dịch từ trực giác cổ điển sang trực giác lượng tử: hỏi đúng quan trọng hơn hỏi nhiều. Vì chỉ được hỏi một lần, một câu hỏi tối ưu phải bỏ

*Phan Dương Hiệu & Phan Thành Nam

qua những "tiểu tiết" mà tập trung vào "đại cục". Về mặt triết học, mối quan hệ giữa "cục bộ" và "toàn cục" gợi nhớ đến Nguyên lý Bổ sung của Bohr: có những đối tượng mang trong mình nhiều mô tả đồng thời đúng, nhưng các mô tả này không thể được truy cập đầy đủ cùng lúc, vì hễ ta truy vấn tới cùng một mặt thì mặt kia sẽ ẩn đi. Đây là giới hạn của nhận thức ở thế giới vi mô: chân lý mang trong mình nhiều khuôn mặt, ta có thể biết tất cả chúng, nhưng không thể ép chúng cùng hiện diện trong cùng một cái chớp mắt.

Nghệ thuật hỏi một lần, vì thế, là nghệ thuật chọn đúng mặt để hỏi. Một ví dụ kinh điển cho tư duy này là thuật toán Shor (1994): bằng cách buông bỏ nhiều mô tả cục bộ để đổi lấy một thông tin toàn cục, một số hữu hạn các hộp Magic có thể phá sập thành trì RSA, hệ mật mã đang bảo vệ phần lớn các giao dịch ngân hàng trên thế giới.

2 Tính toán lượng tử qua hộp Magic

Nguyên lý nhìn một lần. Để hình dung chính xác luật chơi trong tính toán lượng tử, ta có thể đóng vai một người chơi cổ điển sống trong thế giới Hạt, nơi có thể làm các thao tác thông thường như quan sát và sao chép, với sự trợ giúp của một chiếc hộp ảo thuật, gọi là hộp sóng Magic, nơi có các khả thể chồng chập và giao thoa. Nói cách khác, thế giới bên ngoài hộp Magic là Hạt (cổ điển), thế giới bên trong là Sóng (lượng tử). Khi ta rải các hạt vào hộp, chúng lập tức mang tính chất sóng, có khả năng chồng chập và giao thoa. Đến khi ta yêu cầu lấy lại hạt nào thì hộp Magic đo hạt đó và trả về giá trị cho ta, đồng thời hạt này mất chức năng sóng và chính thức quay lại thế giới Hạt.

Do đó, luật chơi rất khắc nghiệt: không được nhìn quá một lần, vì chỉ một ánh mắt tò mò của người chơi sẽ lập tức làm sụp đổ hàm sóng trong hộp và phép màu lượng tử biến mất. Do đó, người chơi trước hết phải đưa ra một chuỗi chỉ dẫn các thao tác "hợp lệ", còn gọi là các thao tác lượng tử, sao cho hộp Magic có thể làm mà không phá vỡ tính chất sóng, rồi cuối cùng mới đặt ánh nhìn vào hộp. Tại khoảnh khắc đó, Sóng lập tức đông cứng thành Hạt, và hộp Magic trả lại một giá trị quan sát tối hậu cho người chơi. Đó là nghệ thuật hỏi một lần.

Cụ thể hơn, hộp Magic có thể làm gì? Về mặt nguyên tắc, mỗi thao tác "hợp lệ" trên một hệ lượng tử kín sẽ tương ứng với một phép biến đổi tuyến tính unitary trên một không gian Hilbert phức (không gian các trạng thái lượng tử) phụ thuộc vào số qubit. Tính tuyến tính là giả thuyết tối giản cho phép các khả thể lượng tử tự do đan xen và chồng chập lên nhau như những gợn sóng mà không phá vỡ cấu trúc của nhau. Trong khi đó, tính unitary là một chiếc "vòng kim cô" của toán học, đảm bảo mọi sự biến đổi dù lắt léo đến đâu cũng phải bảo toàn tổng xác suất bằng 1. Sau một số thao tác "hợp lệ", người chơi có thể yêu cầu Magic đo một số qubit trong hộp. Hộp Magic sẽ trả về kết quả đo là các bít cổ điển, và các qubit bị đo coi như biến mất (nguyên lý nhìn một lần). Các qubit chưa bị đo vẫn tồn tại, và người chơi có thể tiếp tục yêu cầu hộp Magic làm các biến đổi "hợp lệ" trước khi quyết định đo chúng.

Mô hình toán học của luật chơi. Người chơi vốn có khả năng giới hạn như mô hình tính toán thông thường (tức là dùng một máy Turing cổ điển trong thời gian đa thức). Làm sao người chơi tăng cường sức mạnh cho mình với chiếc hộp Magic?

Về mặt toán học, một trạng thái của n qubit trong hộp Magic có thể được mô tả như một

vector đơn vị $(\alpha_x)_{x\in\{0,1\}^n}$ trong không gian Hilbert phức 2^n chiều:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle, \qquad \sum_x |\alpha_x|^2 = 1, \qquad \alpha_x \in \mathbb{C},$$

trong đó $|\alpha_x|^2$ chính là xác suất thu được một chuỗi n bít $x \in \{0,1\}^n$ khi đo toàn bộ n qubit.

Điểm quan trọng là người chơi cổ điển (với giới hạn sức mạnh đa thức) không thể lưu trữ một trạng thái tùy ý với 2^n hệ số phức. Thông thường, người chơi sẽ bắt đầu từ trạng thái tầm thường $|0^n\rangle$, tức là cả n qubit đều ở trạng thái tĩnh 0, tương ứng với vector hệ số $(\alpha_x)_{x\in\{0,1\}^n} = (1, 0, \ldots, 0)$. Sau đó, người chơi đưa nó vào hộp và yêu cầu Magic áp dụng một dãy đa thức các thao tác lượng tử, tức là các biến đổi tuyến tính unitary trên vector (α_x). Đây là chính là điểm tăng cường sức mạnh vì vector có độ dài 2^n vượt quá khả năng thao tác đa thức của người chơi cổ điển. Chừng nào còn các qubit chưa được nhìn/bị đo, thì người chơi vẫn có thể tiếp tục yêu cầu hộp Magic thực hiện các biến đổi unitary. Và cuối cùng khi người chơi yêu cầu hộp Magic thực hiện phép đo trên một số qubit (hoặc cả n qubit) thì sẽ nhận lại một chuỗi bit cổ điển với độ dài tối đa n, đồng thời các qubit tương ứng bị "bốc hơi".

Sức mạnh và hạn chế của chiếc hộp Magic. Qua một vài ví dụ, ta sẽ thấy sức mạnh của chiếc hộp Magic và cả những hạn chế của nó. Đầu tiên, chỉ từ hai qubit ban đầu $|00\rangle$, nếu Magic được yêu cầu áp dụng hai biến đổi unitary (tương ứng biến đổi Hadamard H lên qubit thứ nhất, rồi áp dụng CNOT[1]), ta sẽ thu được trạng thái Bell:

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Đây là ví dụ đơn giản nhất của vướng víu lượng tử: hai qubit được gắn với nhau thành một trạng thái chung không thể tách thành hai trạng thái riêng biệt. Cụ thể hơn, nếu ta đo qubit thứ nhất và nhận được 1, thì trạng thái còn lại sụp xuống $|11\rangle$, do đó qubit thứ hai chắc chắn cũng cho kết quả 1 (tương tự nếu đo được 0, thì qubit thứ hai chắc chắn cũng cho kết quả 0). Đây là một trong những trực giác nền tảng đằng sau trao đổi khoá lượng tử: hai bên có thể chia sẻ các hệ lượng tử có tương quan đặc biệt, rồi đo chúng để tạo ra các bít chung.

Người chơi cổ điển cũng có thể yêu cầu Magic đo một số qubit ở giữa quá trình tính toán. Chẳng hạn xét một hàm tính được $f : [Q] \to [Q]$ với $[Q] = \{0, 1, \ldots, Q-1\}$ và $Q = 2^m$. Ở đây, f là một hàm tính được có nghĩa là có một mạch tính toán cổ điển hiệu quả tính nó, và điều này cho phép xây dựng phép biến đổi tuyến tính unitary U_f:

$$U_f : |x\rangle \otimes |y\rangle \longmapsto |x\rangle \otimes |y \oplus f(x)\rangle.$$

Ta dùng hai thanh ghi m qubit để đưa vào hộp Magic, với trạng thái tầm thường ban đầu: $|0^m\rangle \otimes |0^m\rangle$. Sau đó, ta áp dụng Hadamard lên từng qubit của thanh ghi thứ nhất, rồi yêu cầu Magic áp dụng biến đổi U_f để thu được:

$$|0^m\rangle \otimes |0^m\rangle \longmapsto \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle \otimes |0^m\rangle \longmapsto \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle \otimes |f(x)\rangle.$$

[1]Hadamard tạo chồng chập trên một qubit: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. CNOT là cổng hai qubit: $|a\rangle|b\rangle \mapsto |a\rangle|b \oplus a\rangle$, tức là lật qubit thứ hai khi qubit thứ nhất bằng 1.

Đến đây, chúng ta có thể thấy sự liên hệ mật thiết giữa hai thanh ghi: nếu thanh ghi thứ nhất là x thì bắt buộc thanh ghi thứ hai là $f(x)$. Từ đó, nếu người chơi yêu cầu hộp Magic đo thanh ghi thứ hai và thu được giá trị y, thì thanh ghi thứ nhất sụp xuống chồng chập đều trên các giá trị x thỏa mãn $f(x) = y$:

$$\frac{1}{\sqrt{N_y}} \sum_{\substack{0 \le x < Q \\ f(x)=y}} |x\rangle, \quad N_y = \#\{x : 0 \le x < Q,\ f(x) = y\}.$$

Đây là một mẫu rất phổ biến trong các thuật toán lượng tử: dùng một biến đổi unitary để tạo tương quan giữa hai thanh ghi, rồi đo một thanh ghi và để lại trên thanh ghi kia một chồng chập có cấu trúc. Đây là cách để nghiên cứu các tính chất ẩn của một hàm f.

Đặc biệt trong trường hợp rất phổ dụng là f có tính chất đồng cấu nhóm thì thanh ghi thứ nhất bên trên cho ta trạng thái chồng chập trên một coset của nhân (Kernel) của f. Đó là thông tin rất quan trọng đứng sau nhiều bài toán. Sau khi đưa về chồng chập của các trạng thái có tính chất "tuần hoàn", với Kernel của f đóng vai trò như "'chu kỳ", ta có thể áp dụng biến đổi Fourier (cũng là một phép biến đổi unitary) trước khi quan sát. Vì đây là biến đổi Fourier rời rạc áp dụng lên vector biên độ phức $(\alpha_x)_{x\in\{0,1\}^n} \in \mathbb{C}^{2^n}$ của trạng thái lượng tử, nên thường được gọi là biến đổi Fourier lượng tử (QFT). Với hộp Magic lượng tử chúng ta có thể thực hiện phép biến đổi này thông qua một mạch lượng tử trên n qubit, trong khi để mô phỏng nó trên máy thông thường thì cần phép biến đổi trong không gian hàm mũ với 2^n số phức. Sức mạnh lượng tử nằm ở khả năng điều khiển các biên độ bằng các phép biến đổi unitary, làm cho các biên độ giao thoa với nhau: các khả năng "sai" có thể bị triệt tiêu, còn các khả năng "đúng" có thể được khuếch đại. Ta sẽ minh họa ý tưởng này trong trường hợp RSA và một số bài toán khác.

Tuy chiếc hộp Magic cho ta sức mạnh thao tác trong không gian Hilbert với số chiều hàm mũ, tính toán lượng tử không phải là công cụ vạn năng cho ta tăng tốc độ hàm mũ cho mọi bài toán. Mặt hạn chế là Magic chỉ tuân theo yêu cầu thực hiện các phép biến đổi tuyến tính unitary và chỉ cho ta nhìn kết quả một lần qua các phép đo lượng tử mang tính xác suất. Do đó, chúng ta phải đánh đổi giữa thông tin cục bộ và toàn cục, đúng như Nguyên lý Bổ sung của Bohr. Có những mục tiêu tưởng như đơn giản, chẳng hạn sao chép một trạng thái lượng tử tùy ý, mà nó cũng không thể làm được (Định lý cấm sao chép). Hay với các bài toán trong lớp NP-đầy đủ, hiện nay chưa có thuật toán lượng tử có sức mạnh vượt trội đáng kể (tăng tốc siêu đa thức) so với máy cổ điển; lợi thế đã biết chủ yếu là tăng tốc bậc hai với thuật toán Grover, nên nhìn chung chưa có bước đột phá tương tự Shor.

3 Từ cấm sao chép tới Thuật toán Shor

Quay lại Định lý cấm sao chép lượng tử, về mặt toán học, để sao chép trạng thái $|\psi\rangle$, ta cần ghép nó với một "tờ giấy trắng" $|0\rangle$ độc lập để "hứng lấy" bản copy thông qua tích tensor $|\psi\rangle \otimes |0\rangle$. Sự sao chép xảy ra nếu ta tìm được một toán tử tuyến tính unitary biến $|\psi\rangle \otimes |0\rangle$ thành $|\psi\rangle \otimes |\psi\rangle$ Trong điều kiện lý tưởng, toán tử này không phụ thuộc vào trạng thái $|\psi\rangle$, tức là nó cũng biến $|\phi\rangle \otimes |0\rangle$ thành $|\phi\rangle \otimes |\phi\rangle$ với mọi $|\phi\rangle$. Lấy tích vô hướng hai biến đổi kiểu này, ta thu được $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$, tức là $\langle\psi|\phi\rangle \in \{0, 1\}$. Điều này chỉ xảy ra khi hai trạng thái hoặc trùng nhau hoàn toàn, hoặc trực giao. Do đó, một cách tổng quát chúng ta không thể nào nhân bản một trạng thái lượng tử bất kỳ.

Nhìn từ góc độ đại số, định lý cấm sao chép là hệ quả của một sự bất đối xứng: phép sao chép về bản chất là một phép biến đổi phi tuyến bậc hai, vì nó nhân $|\psi\rangle$ với chính nó, nhưng một phép toán bậc hai không thể thực hiện được bằng một biến đổi tuyến tính. Nói cách khác, việc cấm nhân bản có thể hiểu như là hệ quả trực tiếp của tính tuyến tính của cơ học lượng tử.

Tương tự, trong bài toán phân tích thừa số nguyên tố, nền tảng cốt lõi của thuật toán RSA, khi ta viết $N = p \times q$ như là tích của hai số nguyên tố rất lớn, thì đẳng thức này đã giấu một sự bất đối xứng rất sâu về độ phức tạp trong tính toán: đi từ thông tin cục bộ (p, q) tới thông tin toàn cục N là một thao tác thuận chiều, dễ làm, nhưng từ N muốn tách ngược về (p, q) là cực khó. Giống như trong truyện cổ tích Tấm Cám, trộn thóc và gạo thì mất 1 giây, nhưng nhặt thóc ra thóc, gạo ra gạo, thì mất cả ngày. Đây cũng là ý tưởng trong xây dựng các hàm một chiều (one-way function) ở đó tính xuôi dễ còn tính ngược khó. Các hàm một chiều là nền tảng cơ bản trong lý thuyết mật mã.

Về mặt triết học, Định lý cấm sao chép là một rào cản kỹ thuật cần thiết để bảo vệ Nguyên lý bổ sung Bohr ở cấp độ vi mô. Nếu phép sao chép được phép, ta có thể tạo ra nhiều phiên bản của một trạng thái lượng tử và truy vấn từng mô tả khác nhau trên từng bản riêng biệt, qua đó phá vỡ tinh thần đối ngẫu-bổ sung mà Bohr đã xác lập. Trong mối quan hệ giữa thông tin cục bộ và toàn cục, sự "bất khả sao chép" này buộc chúng ta phải chọn: nếu muốn nhìn rõ từng nốt nhạc cục bộ, thì bản giao hưởng toàn cục sẽ không bao giờ xuất hiện; và ngược lại, khi kiên nhẫn ngồi đợi một sự thật toàn cục hiển lộ, ta phải nhắm mắt làm ngơ trước mọi tiểu tiết địa phương. Và đây cũng chính là ý tưởng mấu chốt để bẻ gãy RSA bằng thuật toán lượng tử.

Máy tính lượng tử không bẻ gãy RSA bằng cách tính nhanh hơn theo nghĩa cổ điển, mà cú đột phá của Shor (1994) nằm ở chỗ ông đổi hẳn cách hỏi. Khi đứng trước số N, thay vì cứ mãi ám ảnh về câu hỏi trực diện "p và q là gì?", Shor tìm cách nhúng mô tả cục bộ của bài toán trong một cấu trúc toàn cục. Lấy một số a nguyên tố cùng nhau với N, thì hàm $f(x) = a^x \pmod N$ chắc chắn là một hàm tuần hoàn do Định lý Euler. Tuy nhiên câu hỏi mấu chốt của Shor là hàm số này có chu kỳ bao nhiêu, tức là làm sao tìm ra số nguyên dương nhỏ nhất r sao cho $a^r \equiv 1 \pmod N$. Biết được chu kỳ r, ta có thể quay ngược trở lại để tìm các ước của N bằng vài bước tính toán cổ điển tương đối đơn giản. Chẳng hạn, nếu $r = 2s$ là số chẵn và $a^s \not\equiv -1 \pmod N$, thì $a^r - 1 = (a^s - 1)(a^s + 1)$ sẽ chứa các nhân tử của N, và các ước nguyên tố p, q có thể tính được dễ dàng từ thuật toán Euclid cho ước chung lớn nhất. (Trong thực tế, nếu ta chọn a ngẫu nhiên thì xác suất tìm ra r chẵn và $a^s \not\equiv -1 \pmod N$ ít nhất là 50%.Nhìn dưới quan hệ đối ngẫu giữa cục bộ và toàn cục, chu kỳ của $a^x \pmod N$ không phải một con số từ trên trời rơi xuống, mà nó được tạo nên từ các chu kỳ cục bộ của a^x khi nhìn modulo p và modulo q, rồi được khâu lại thành một nhịp toàn cục ở mức modulo N.

Máy tính cổ điển bị giam trong mô tả cục bộ: nó có thể đọc rất rõ giá trị của N, nhưng không có cách nào "nghe" được nhịp tuần hoàn toàn cục ẩn bên trong ngoài việc mò mẫm thử sai trong một không gian nghiệm khổng lồ. Chính khoảng cách giữa cái thấy được ở bề mặt và cái ẩn đi trong cấu trúc là nơi RSA dựng nên thành trì kiên cố của mình. Câu hỏi mấu chốt bây giờ là: liệu có thể dùng đúng một phát súng lượng tử để chạm thẳng vào phần cấu trúc toàn cục ấy hay không?

Để tận dụng sức mạnh của tính toán lượng tử, ý tưởng của Shor như sau: Ta dùng hai thanh ghi lượng tử có dung lượng trạng thái $Q = 2^L$, trong đó L là số qubit. Thanh ghi thứ nhất chạy qua mọi giá trị x từ 0 đến $Q - 1$, còn thanh ghi thứ hai lưu giá trị tương ứng $f(x) = a^x$

(mod N). Sau khi đưa toàn hệ vào trạng thái chồng chập

$$Q^{-1/2} \sum_{x=0}^{Q-1} |x\rangle \otimes |f(x)\rangle$$

rồi đo thanh ghi thứ hai, ta sẽ khiến thanh ghi thứ nhất sụp đổ về các giá trị x cho cùng một giá trị $f(x)$. Vì f là hàm tuần hoàn chu kỳ r, nên $|x\rangle$ sẽ là một trạng thái chồng chập của các giá trị $|z\rangle, |z+r\rangle, |z+2r\rangle, ...$ với một độ dịch chuyển ngẫu nhiên z.

Đến đây, ta đứng trước một thời khắc rất mong manh. Chu kỳ r đã thực sự có mặt trong cấu trúc của trạng thái $|x\rangle$, nhưng nó còn bị phủ bởi điểm mù z. Nếu ta bóp cò phép đo ngay lúc này, viên đạn duy nhất của ta sẽ chỉ có thể găm vào một giá trị cục bộ có dạng $z + jr$, và ta vĩnh viễn không tìm ra chu kỳ r ẩn bên trong cấu trúc vì điểm mù z đã che khuất nó.

Để xoá nhiễu do điểm mù z gây ra, ta bắt buộc phải buông bỏ việc truy vấn thông tin địa phương để hướng về một mô tả toàn cục về cấu trúc tuần hoàn của f. Chính ở đây, biến đổi Fourier bước vào như cây cầu toán học nối liền hai bờ của nguyên lý bổ sung. Trong truyền thống Heisenberg–Bohr, biến đổi Fourier từ lâu đã là ngôn ngữ tự nhiên để chuyển hoá quan hệ đối ngẫu giữa vị trí và động lượng: một bên là mô tả cục bộ của hàm sóng trong không gian vị trí, bên kia là mô tả cục bộ trong không gian tần số nhưng đồng thời là mô tả toàn cục trong không gian vị trí. Nói một cách hình tượng, nếu hình dung giá trị $f(x)$ tại mỗi điểm x là một nốt nhạc riêng lẻ, thì biến đổi Fourier cho phép ta nghe cả bản nhạc cùng một lúc dưới dạng phổ tần số, trong đó trọng số tại mỗi tần số y tương ứng với một sóng phẳng (plane wave) có dạng $e^{2\pi ixy/Q}$.

Về mặt giải tích, một tính chất then chốt của biến đổi Fourier là nó biến phép tịnh tiến trong không gian vị trí thành một hệ số pha trong không gian tần số: biến đổi Fourier của $f(x-z)$ chính là $e^{-2\pi izy/Q}\hat{f}(y)$. Đây cũng là lý do biến đổi Fourier cho phép chéo hóa toán tử đạo hàm trên x thành toán tử nhân trên y, qua đó biến các bài toán vi phân thành phương trình đại số, và chứng minh Nguyên lý bất định Heisenberg từ đẳng thức giao hoán tử $[\partial_x, x] = 1$.

Thuật toán Shor vận dụng đúng tinh thần ấy: thay vì tiếp tục đứng trong không gian vị trí, nơi mọi giá trị $\{z + jr\}$ đều có thể hiện ra nhưng không có ý nghĩa thông tin vì bị nhiễu hoá, ta chuyển toàn bộ trạng thái sang không gian tần số để buộc cấu trúc tuần hoàn phải tự khai báo danh tính. Cụ thể hơn, bằng cách áp dụng biến đổi Fourier lượng tử lên thanh ghi thứ nhất, ta có thể biểu diễn được từng trạng thái $|x\rangle$ như là chồng chập của các trạng thái $e^{2\pi ixy/Q}|y\rangle$ với $y = 0, 1, ..., Q-1$. Khi áp dụng lên trạng thái chồng chập của $|z\rangle, |z+r\rangle, |z+2r\rangle, ...$, độ dịch z sẽ sinh ra một nhân tử pha có dạng $e^{2\pi izy/Q}$. Như vậy, điểm mù z chưa biến mất hoàn toàn, nhưng nó chỉ còn sống sót dưới dạng một nhân tử pha có module bằng 1. Khi lấy bình phương module, toàn bộ dấu vết của z bị bốc hơi, và ta thu được xác suất để tần số y xuất hiện đúng bằng

$$P(y) = (mQ)^{-1} \left| \sum_{j=0}^{m-1} e^{2\pi ijry/Q} \right|^2 ,$$

trong đó m chính là số lần chu kỳ r lặp lại trọn vẹn bên trong thanh ghi lượng tử thứ nhất.

Bây giờ là khoảnh khắc quyết định. Trong công thức $P(y)$, những giá trị y không ăn khớp với chu kỳ r sẽ sinh ra các vector pha quay lệch nhau dẫn tới giao thoa triệt tiêu, còn những giá trị y làm cho ry/Q xấp xỉ một số nguyên k sẽ cộng hưởng thành những đỉnh xác suất rất cao. Như vậy, biến đổi Fourier không trực tiếp trả lời câu hỏi "r là bao nhiêu", mà nó dọn sạch nhiễu

cục bộ để cấu trúc toàn cục của hàm số f tự hiện ra trong xác suất đo. Trước Fourier, phép đo chỉ có thể găm vào một điểm cục bộ vô nghĩa, nhưng sau Fourier, cùng một phép đo ấy lại có thể chạm đúng vào nhịp tuần hoàn của toàn bộ cấu trúc. Nói cách khác, nó tạo ra cơ chế để các sai lầm tự triệt tiêu lẫn nhau, còn chân lý thì nắm tay nhau lớn lên. Đó chính là nghệ thuật của Shor: không hỏi trực diện vào thứ mình cần, mà đặt lại câu hỏi trong hệ quy chiếu mới để bài toán tự khai ra câu trả lời.

Cuối cùng, phát súng lượng tử quyết định sẽ được bắn ra sau khi phép biến đổi Fourier đã hoàn tất. Phép đo duy nhất trả về cho ta một giá trị y. Đến đây, thuật toán lượng tử hoàn tất nhiệm vụ. Phần còn lại được xử lý bởi thuật toán liên phân số cổ điển: Định lý Legendre khẳng định rằng nếu phép xấp xỉ $y/Q \approx k/r$ có sai số nhỏ hơn $1/(2r^2)$, thì k/r là phân số duy nhất có mẫu số nhỏ hơn N thoả mãn điều kiện đó. Đây là ranh giới cứng giữa sự nhiễu loạn và độ chính xác, cho phép chúng ta khoá mục tiêu chu kỳ r. Trong thực tế, giá trị đo được của y hiếm khi rơi chính xác vào một đỉnh cộng hưởng kQ/r, mà ta chỉ có thể hi vọng y là số nguyên gần nhất, tức $|y - kQ/r| \leq 1/2$. Do đó, thuật toán lượng tử đảm bảo phép xấp xỉ $y/Q \approx k/r$ có sai số không quá $1/(2Q)$. Đây là giới hạn độ phân giải của thanh ghi lượng tử. Để thuật toán Shor thành công, ta phải đảm bảo sai số lượng tử nằm trong phạm vi an toàn của Định lý Legendre, tức là $Q > r^2$. Nếu ta chỉ biết $r \leq N$ và không có thông tin gì khác, thì yêu cầu $Q > N^2$ là cần và đủ để đảm bảo thuật toán Shor vận hành. Nói cách khác, số qubit tối thiểu cho mỗi thanh ghi là $L = \log_2 Q > 2 \log_2 N$.

Mở rộng thuật toán Shor cho HSP. Các hệ mật mã khoá công khai đang được sử dụng trong thực tế hiện nay hầu hết dựa trên độ khó của hai bài toán nền tảng: bài toán phân tích thừa số nguyên tố (cơ sở của hệ mã RSA), và bài toán tính logarit rời rạc (cơ sở của hệ mã ElGamal và nhiều hệ thống chữ ký số). Điểm thú vị là, dù khác biệt về bản chất, cả hai bài toán này đều che giấu một cấu trúc mang tính lặp (tương tự chu kỳ r nói trên), và ý tưởng của Shor có thể được mở rộng để áp dụng cho lớp các bài toán như thế. Ta sẽ giải thích ngắn gọn cấu trúc của lớp bài toán này và cấu trúc "chu kỳ" của nó.

Giả sử $G = \langle g \rangle$ là một nhóm cyclic bậc q sinh bởi g, và ta được cho một phần tử $h \in G$. Khi đó h có thể được biểu diễn dưới dạng $h = g^x$, trong đó x là số bí mật cần tìm. Bài toán logarit rời rạc chính là khôi phục x từ g và h.

Thoạt nhìn, bài toán này không có dạng tìm chu kỳ của một hàm một biến như $f(r) = a^r \bmod N$ trong bài toán phân tích số. Tuy nhiên, ta có thể biến nó thành một bài toán tìm cấu trúc ẩn trong một hàm hai biến. Xét ánh xạ $f : \mathbb{Z}_q^2 \to G$ cho bởi $f(a, b) = g^a h^b$. Vì $h = g^x$, ta có $f(a, b) = g^a (g^x)^b = g^{a+bx}$. Khi đó

$$\ker f = \{(a, b) \in \mathbb{Z}_q^2 : \ a + bx \equiv 0 \pmod{q}\} = \langle (x, -1) \rangle.$$

Nói cách khác, hàm f không phân biệt được các điểm nằm trên cùng một lớp song song với véc-tơ $(x, -1)$: $f((a, b) + k(x, -1)) = f(a, b)$. Vì vậy, vector $(x, -1)$ đóng vai trò giống như một "chu kỳ" của hàm f, giống như chu kỳ r trong bài toán phân tích số. Thuật toán lượng tử khai thác cấu trúc này theo cùng tinh thần như trong bài toán phân tích thừa số.

Nhìn rộng hơn nữa, $H = \langle (x, -1) \rangle$ là một nhóm con ẩn của $\mathbb{Z}_q^2$, và hàm f là bất biến trên các coset của H. Do đó nhiệm vụ tìm x của ta chính là tìm cấu trúc của H. Từ đó bài toán tìm chu kỳ được tổng quát hoá thành bài toán tìm cấu trúc nhóm con ẩn của một nhóm giao hoán, gọi là *Hidden Subgroup Problem* (HSP). Các bạn quan tâm có thể tìm đọc thêm các nghiên cứu

mở rộng theo hướng rất thú vị này.

4 Khoảng cách giữa lý thuyết và thực tế

Trong điều kiện lý tưởng, để phá một khoá của hệ mã RSA, chúng ta cần hàng ngàn qubit logic, tức phải là qubit "sạch" chứ không phải chỉ là qubit vật lý "đầy nhiễu".

Cụ thể hơn, trái tim của thuật toán Shor chính là các hệ số pha giữa các thành phần chồng chập, là thứ sinh ra lực cộng hưởng toàn cục mà phép biến đổi Fourier lượng tử khai thác. Để việc tính toán có ý nghĩa, ta cần giữ hệ lượng tử ổn định trong một thời gian đủ lâu. Tuy nhiên, trong thực tế, không có hệ lượng tử nào bị cô lập hoàn toàn, và chỉ một tác động cực nhỏ của môi trường xung quanh cũng có thể làm hỏng điều kiện thuần khiết mà thuật toán Shor dựa vào. Về mặt toán học, hiện tượng bất ổn định do môi trường bên ngoài này gọi là mất kết hợp (decoherence). Khi hệ lượng tử tương tác với môi trường, thông tin về pha bị mã hóa ra các bậc tự do của môi trường mà ta không thể theo dõi. Do đó, khi truy xuất thông tin, ta buộc phải lấy vết riêng phần qua môi trường (partial trace, giống như khái niệm marginal trong lý thuyết xác suất thống kê). Vấn đề là phép lấy vết này tự động xóa đi thông tin pha, là thứ làm nên tính lượng tử, và do đó sau một thời gian rất ngắn, hệ lượng tử trở thành một hệ cổ điển tầm thường.

Đây là thách thức kỹ thuật cực lớn mà mọi cấu trúc máy tính lượng tử đều phải đối mặt. Toán học đã chỉ ra viên đạn hoàn hảo, nhưng vật lý phải rèn một nòng súng đủ mạnh để giữ cho viên đạn còn nguyên vẹn trước khi được bắn ra. Nói cách khác, không có gì là hoàn hảo, kể cả chiếc hộp Magic. Hộp Magic tuân theo lệnh của ta để làm các phép biến đổi unitary, nhưng nó thỉnh thoảng cũng có quyền gặp lỗi. Mà vì tất cả các thao tác nằm trong chiếc hộp Magic đều rất "bí ẩn" (ta không biết gì trước khi nhìn mỗi qubit một lần duy nhất), nên ta phải nghĩ ra cách thức để hộp Magic tự có khả năng sửa lỗi nội tại của mình! Liệu có thể dùng độ dư thừa thông tin (như sửa lỗi cổ điển) để làm chiếc hộp Magic vận hành trơn tru, và cái giá phải trả là bao nhiêu?

Một lần nữa, Shor đã đưa ra một bước tiến lớn. Để bảo vệ tính chính xác của hộp Magic, thuật toán Sửa lỗi lượng tử (Quantum Error Correction – QEC) hiện nay dựa trên ý tưởng "tàng hình thông tin" như sau: thay vì lưu một qubit logic vào một hạt lượng tử, ta phân mảnh nó vào các mối tương quan vướng víu giữa n hạt. Lúc này dữ liệu không nằm ở từng hạt riêng lẻ, mà nằm ở cấu trúc tương quan tập thể, và ở đó các nhiễu cục bộ không còn đủ sức chạm tới được.

Đây chính là mặt đối ngẫu của thuật toán Shor. Trong khi Shor dùng toàn cục để ép chân lý hiện ra, thì QEC dùng toàn cục để giấu đi chân lý. Cả hai đều có thể đọc dưới lăng kính bổ sung của Bohr, cùng một sự dịch chuyển từ cục bộ sang toàn cục, nhưng theo hai chiều ngược nhau: một chiều là phát hiện, chiều kia là bảo vệ. Nhưng dưới chiều nào thì bài học vẫn như nhau: tri thức quan trọng rất khó sống sót ở cấp cục bộ.

Về mặt toán học, kỹ thuật "tàng hình thông tin" trong QEC chính là nghệ thuật nhúng không gian lượng tử của một dữ liệu nhỏ vào một không gian Hilbert có số chiều lớn hơn theo cấp số nhân (2^n chiều). Nhờ khoảng không gian thừa thãi này, thông tin cốt lõi được giấu an toàn vào một không gian con (subspace) cực nhỏ. Để minh hoạ cho kỹ thuật này, chúng ta hãy xét một ví dụ kinh điển được chính Shor phát minh (1995). Để bảo vệ một trạng thái chồng chập của một hạt $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ với điều kiện chuẩn hoá $|\alpha|^2 + |\beta|^2 = 1$, ông nhúng nó vào

một trạng thái chồng chập của 9 hạt $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$, trong đó hai trạng thái cơ sở

$$|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3}, \quad |1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}$$

đã được thiết kế tinh vi để hệ thống có tính vướng víu tối đa. Cụ thể hơn, nếu môi trường tò mò muốn "nhìn trộm" một cách cục bộ bằng cách tập trung tương tác với hạt số 1, thì về mặt toán học, điều này tương đương với việc lấy vết riêng phần (partial trace) qua 8 hạt còn lại. Kết quả trả về cho ma trận mật độ của riêng hạt số 1 luôn luôn là:

$$\rho_1 = \mathrm{Tr}_{2\ldots9}(|\psi_L\rangle\langle\psi_L|) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Đây chính xác là một trạng thái nhiễu trắng, với mọi thông tin về α, β đã bị triệt tiêu hoàn toàn. Vì môi trường không thu được bất kỳ thông tin gì về dữ liệu gốc, sự tương tác cục bộ này không đủ sức làm sụp đổ hàm sóng toàn cục, và α, β có thể an tâm "ngủ yên" trong không gian vướng víu toàn cục mà không hề bị đánh thức.

Tuy nhiên, để bảo vệ dữ liệu, thuật toán lượng tử còn phải đối mặt với một nghịch lý: ta bắt buộc phải "tàng hình dữ liệu" để môi trường không làm sụp đổ hàm sóng, nhưng đồng thời ta lại bắt buộc phải có khả năng "tự sửa lỗi" liên tục để cấu trúc không bị phân rã theo thời gian. Chúng là hai mảnh bổ sung của một vòng lặp ổn định. Câu hỏi là khi máy tính lượng tử không được phép đo α, β, làm sao nó biết khi nào có nhiễu xảy ra để tự sửa lỗi?

Câu trả lời cũng nằm ngay trong thiết kế mã Shor 9-qubit phía trên, khi ngoài cơ chế phòng thủ bị động là "tàng hình dữ liệu", nó còn có cơ chế phòng thủ chủ động "Tự sửa lỗi". Về mặt cấu trúc, mã Shor 9-qubit sở hữu một lớp khiên kép lồng ghép tinh vi: lớp khiên bên trong bảo vệ sự đồng bộ của từng cụm hạt khỏi lỗi lật Bit (từ $0 \to 1$), và lớp khiên bên ngoài bảo vệ sự đồng bộ về dấu giữa các cụm khỏi lỗi lật Pha (từ $+$ sang $-$). Chẳng hạn, nếu hạt số 1 bị tiếng ồn làm lật bit, khiến cụm đầu tiên từ $(|000\rangle \pm |111\rangle)$ biến thành $(|100\rangle \pm |011\rangle)$, thì thay vì đo từng hạt xem nó mang giá trị 0 hay 1, hệ thống chỉ đo tính chẵn lẻ cục bộ của các cặp hạt lân cận bằng các toán tử ổn định. Nó so sánh hạt 1 với hạt 2 (thấy khác nhau), rồi so sánh hạt 2 với hạt 3 (thấy giống nhau)[2] Kết quả trả về một thông điệp báo động: *"Hạt số 1 đang bị ngược bit"*, và ngay lập tức một thao tác can thiệp địa phương được thực hiện để lật hạt số 1 lại. Tương tự với lỗi lật Pha, nếu dấu $+$ bị biến thành dấu $-$, ta có thể dùng một phép đo chẵn lẻ toàn cục để bắt lỗi này. Một lần nữa, sự kết hợp hai phép đo địa phương và toàn cục là mấu chốt, cho phép chúng ta hoàn tất bộ khiên kép của thuật toán "Tự sửa lỗi".

Dù lý thuyết QEC đẹp đẽ như thế, nhưng cái giá phải trả cũng rất đắt. Mã 9-qubit của Shor thực chất chỉ là một chiếc áo giáp mỏng manh: nó bảo vệ hệ thống xuất sắc nếu chỉ có một phát đạn từ môi trường, nhưng sẽ sụp đổ nếu môi trường vô tình bắn trúng 2 hạt cùng lúc. Để gia tăng sự lì lợm của hệ thống khi nhiều lỗi xảy ra đồng thời, ta buộc phải mở rộng cấu trúc sang các không gian 2^n chiều lớn hơn rất nhiều. Trong các cỗ máy hiện nay, tỷ lệ lỗi vật lý rơi vào khoảng 10^{-3} (1000 phép tính sai 1 lần). Tuy nhiên, để thuật toán Shor chạy trơn tru hàng tỷ phép toán nhằm bẻ khóa RSA, tỷ lệ lỗi logic phải bị ép xuống mức 10^{-15}, và điều này yêu cầu ta phải huy động hàng ngàn qubit vật lý làm "lá chắn" chỉ để bảo vệ một qubit logic duy nhất. Trong những ước tính gần đây của Gidney và Ekerå (2021) và Gidney (2025), để bảo vệ 6000

[2]Để so sánh hai hạt, ta có thể dùng thêm một qubit phụ trợ, khởi tạo ở trạng thái $|0\rangle$, rồi thực hiện phép biến đổi unitary $|x_1x_2\rangle|0\rangle_a \mapsto |x_1x_2\rangle|x_1 \oplus x_2\rangle_a$, sau đó đo qubit phụ trợ này.

qubit sạch, tức là để bẻ gãy RSA thật sự, chúng ta cần hàng triệu qubit vật lý, vượt xa giới hạn công nghệ hiện tại.

Tuy vậy, bóng ma lượng tử vẫn phủ lên thế giới thông tin với chiến lược đe doạ "Thu thập hôm nay, giải mã ngày mai": những thông tin tối mật quan trọng có thể được lưu trữ để 10, 20 hay 30 năm sau có thể bị phá mã trên máy tính lượng tử. Do đó, một mặt, chúng tôi cho rằng chúng ta không nên đổ nguồn kinh phí khổng lồ vào cuộc chạy đua để phát triển các máy tính lượng tử, vừa cực kỳ tốn kém (cả xây dựng và duy trì trong những điều kiện phải cực kỳ lý tưởng)[3]. vừa hầu như chỉ giải quyết được một lớp bài toán có dạng "tìm chu kỳ" như đã mô tả. Nhưng mặt khác, nghiên cứu và nắm bắt nền tảng lý thuyết cơ bản để từ đó thiết lập các phương pháp bảo vệ an toàn các hệ thống trước những tấn công lượng tử lại là điều cần thiết và khả thi ngay: dựa trên các bài toán ngoài lớp có thể giải tốt bởi máy lượng tử để xây dựng các hệ thống an toàn. Đó chính là hướng phát triển mật mã "Hậu lượng tử", có thể chạy rất nhanh trên các máy tính thông thường hiện nay, nhưng đồng thời vẫn có thể đứng vững trước các đòn tấn công từ máy tính lượng tử.

5 Cục bộ và toàn cục

Tối ưu hóa sự biết trong một lần hỏi là nghệ thuật chọn đúng cặp đối ngẫu-bổ sung. Nghệ thuật của Shor là không hỏi trực diện vào thứ mình cần, mà đặt lại câu hỏi trong một hệ quy chiếu mới để bài toán tự khai ra cấu trúc ẩn của nó. Trong khi máy tính cổ điển đứng quá gần bài toán và chỉ có thể mò mẫm cục bộ trong một không gian nghiệm bao la, thì tính toán lượng tử đổi sang cách nhìn toàn cục để chạm đúng vào nhịp tuần hoàn ẩn bên dưới. Trong cuộc đời cũng vậy, nếu ta không có quyền thử sai vô hạn hay quay ngược thời gian để vá víu những gì đã sụp đổ, thì đôi khi ta cần dũng cảm thực hiện một phép biến đổi Fourier trong tâm thức: buông bỏ những tiểu tiết để lùi ra đúng khoảng cách, nơi những nhiễu động cục bộ tự triệt tiêu và hình thế lớn hơn của sự thật dần lộ diện. Để tìm thấy chân lý, vấn đề không nằm ở việc ta thu thập được bao nhiêu mảnh dữ liệu rời rạc, mà ở việc ta có dám từ bỏ hệ quy chiếu địa phương để lắng nghe bản giao hưởng vĩ mô của tương quan hay không.

Trong toán học cũng như trong cuộc đời, đôi khi ta phải sống rất sâu trong một vấn đề để thấu hiểu bản chất từng khó khăn, để biết tường tận nguồn cội từng chi tiết, nhưng đồng thời cũng phải biết bước ra ngoài nó, biết lùi lại đủ xa để có cái nhìn toàn cục, như câu thơ của Phan Đình Diệu:

> Ta hiểu tình ta từ nửa vòng trái đất
> Hiểu cái lắng sâu của cuộc sống bình thường
> Bởi tự rất xa nhìn cái gần mới thật
> Mới rõ tình người từ muôn dặm trùng dương

Cái hiểu về tình ta thường bắt đầu từ bên trong, từ những gì rất gần gũi và tưởng như bình thường. Nhưng khi lắng đủ sâu, ta mới nhận ra ở đó cái riêng chưa bao giờ tách khỏi cái chung. Khi từ xa quan sát, ta mới thấy cái thật nhất của cái gần, và khi đó cái điều riêng trong mỗi người không còn khép kín nơi mình, mà mở sang tình người chung và bóng hình đất nước.

Trực giác ấy cũng giống như tâm sự của Tô Đông Pha từ ngàn năm trước khi ngắm vẻ hùng vĩ của núi Lư Sơn:

[3]Bài này chỉ giới hạn bàn về máy tính lượng tử (Quantum Computer) chứ không bàn tới các công nghệ lượng tử khác như Quantum Simulation (QSim), Quantum Communication (QComm), và Quantum Sensing (QS).

Hoành khan thành lĩnh trắc thành phong
Viễn cận cao đê các bất đồng
Bất thức Lư Sơn chân diện mục
Chỉ duyên thân tại thử sơn trung

Phóng dịch:

Nhìn ngang như lụa, chếch như mâu
Xa gần cao thấp thảy khác nhau
Mặt thật Lư Sơn nào thấy hết
Khi thân còn đứng giữa non sâu

Câu thơ đầu của Tô Đông Pha, cùng một ngọn núi nhưng nhìn ngang thành dãy, nhìn nghiêng thành đỉnh, gợi đúng tinh thần của biến đổi Fourier: cùng một thực tại, nếu đứng trong không gian vị trí thì ta chỉ thấy những giá trị cục bộ, còn khi đổi sang không gian tần số thì cấu trúc tuần hoàn ẩn sâu bên dưới mới hiện ra. Đứng trước bí ẩn của vũ trụ, điều giới hạn ta nhiều khi không phải bóng tối, mà chính là khoảng cách quá gần với nguồn sáng mà mình đang bám giữ. Giá trị của một lần được gõ cửa không nằm ở việc ta gõ mạnh hay nhẹ, mà ở việc ta đã biết cách lùi lại nửa bước để nhìn ra đâu mới là cánh cửa dẫn tới "Lư Sơn chân diện" hay chưa.