

CHỐNG SAI SỐ TRONG TRUYỀN TIN LƯỢNG TỬ DỰA TRÊN MÃ SỬA SAI CSS

ERROR CONTROL IN QUANTUM COMMUNICATION BASED ON CSS ERROR CORRECTION CODE

Hồ Ngọc Vinh

Trường Đại học Sư phạm Kỹ thuật Vinh

Received: 20/01/2026; Accepted: 26/01/2026; Published: 09/02/2026

Tóm tắt: Sự phát triển của tính toán lượng tử hứa hẹn khả năng xử lý thông tin vượt trội thông qua các thuật toán như Peter Shor hay Grover. Tuy nhiên, các hệ thống lượng tử thực tế đối mặt với thách thức lớn từ nhiễu môi trường (decoherence) và sai số thao tác cổng, dẫn đến sự tích lũy lỗi theo hàm lũy thừa. Mã sửa sai lượng tử (Quantum Error Correction - QEC) đóng vai trò then chốt trong việc xây dựng các máy tính lượng tử có khả năng chịu lỗi. Bài báo này tập trung nghiên cứu cơ sở lý thuyết về không gian Hilbert, mô hình lỗi Pauli và phân tích chi tiết cấu trúc mã Calderbank-Shor-Steane (CSS). Nghiên cứu cung cấp nền tảng quan trọng cho việc triển khai các giao thức truyền tin lượng tử bền vững.

Từ khóa: tính toán lượng tử, mã sửa sai lượng tử, CSS Code, mô hình lỗi Pauli, Qubit.

Abstract: The development of quantum computing promises superior information processing capabilities through algorithms such as Peter Shor or Grover. However, practical quantum systems face significant challenges from environmental noise (decoherence) and gate operation errors, leading to exponential error accumulation. Quantum Error Correction (QEC) plays a key role in building fault-tolerant quantum computers. This paper focuses on the theoretical basis of Hilbert space, the Pauli error model, and a detailed analysis of the structure of Calderbank-Shor-Steane (CSS) code. This research provides a crucial foundation for the implementation of robust quantum communication protocols.

Keywords: quantum computing, quantum error correction code, CSS Code, Pauli error model, Qubit.

1. Giới thiệu

Kể từ khi Richard Feynman đề xuất ý tưởng về máy tính lượng tử vào những năm 1980, lĩnh vực này đã chuyển mình mạnh mẽ từ các nghiên cứu thuần túy lý thuyết sang giai đoạn hiện thực hóa công nghệ. Sức mạnh vượt trội của máy tính lượng tử so với máy tính cổ điển đã được khẳng định thông qua các thuật toán mang tính đột phá: thuật toán Peter Shor có khả năng phá vỡ các hệ mật mã khóa công khai dựa trên việc phân tích số nguyên tố lớn trong thời gian đa thức, và thuật toán Grover giúp tối ưu hóa tốc độ tìm kiếm trong dữ liệu chưa cấu trúc. Những tiến bộ này dựa trên hai nguyên lý nền tảng của cơ học lượng tử là tính chồng chất (superposition) và sự rối lượng tử (entanglement), cho phép hệ thống xử lý song song một lượng thông tin khổng lồ mà không một siêu máy tính cổ điển nào có thể đạt tới.

Tuy nhiên, thực tế triển khai các hệ thống lượng tử đối mặt với một thách thức mang tính sống còn: sự mong manh của các trạng thái lượng tử. Do tính chất chồng chất nhạy cảm, các qubit (bit lượng tử) rất dễ bị tác động bởi các nhiễu động nhỏ nhất từ môi trường xung quanh, dẫn đến hiện tượng mất liên lạc lượng tử (decoherence). Thêm vào đó, các thao tác cổng logic (gate operations) và quá trình đo lường (measurement) trong thực tế luôn tồn tại sai số vật lý nhất định. Khác với thông tin cổ điển vốn có độ ổn định cao và dễ dàng sao chép để dự phòng, thông tin lượng tử không thể được sao chép theo “Định lý

không sao chép” (No-cloning Theorem), khiến việc áp dụng trực tiếp các kỹ thuật sửa sai cổ điển như mã lặp (repetition code) trở nên bất khả thi.

Sự tích lũy sai số trong quá trình tính toán lượng tử diễn ra theo hàm lũy thừa, chỉ cần một lỗi nhỏ ở mức độ qubit vật lý cũng có thể làm hỏng toàn bộ kết quả của thuật toán. Do đó, việc xây dựng các mã sửa sai lượng tử (Quantum Error Correction - QEC) đóng vai trò là “chìa khóa” then chốt để lấp đầy khoảng cách giữa lý thuyết lý tưởng và các thiết bị lượng tử có nhiều ở quy mô trung bình (NISQ). Trong số các phương pháp tiếp cận, họ mã Calderbank-Shor-Steane (CSS) nổi lên như một giải pháp xuất sắc nhờ khả năng tận dụng sự tinh túy của lý thuyết mã hóa cổ điển để bảo vệ thông tin trước cả lỗi nhảy bit và lỗi đảo pha. Kết quả nghiên cứu không chỉ góp phần làm rõ giới hạn hoạt động của mã CSS mà còn cung cấp nền tảng quan trọng cho việc triển khai các giao thức truyền tin lượng tử bền vững trong tương lai.

2. Cơ sở lý thuyết về tính toán và sai số lượng tử

2.1. Đơn vị thông tin lượng tử

Khác với đơn vị thông tin cổ điển (bit) chỉ nhận một trong hai giá trị rời rạc, đơn vị thông tin lượng tử (qubit) được định nghĩa là một vectơ trạng thái trong không gian Hilbert phức hai chiều $\mathcal{H} \cong \mathbb{C}^2$. Một qubit có thể tồn tại trong sự chồng chất tuyến tính của các trạng thái cơ sở $|0\rangle$ và $|1\rangle$, được biểu diễn dưới dạng: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Trong đó, α và β là các số phức đóng vai trò là biên độ xác suất (probability amplitudes). Theo tiên đề của cơ học lượng tử, tổng xác suất tìm thấy hệ ở các trạng thái cơ sở phải bằng 1, do đó các biên độ phải thỏa mãn điều kiện chuẩn hóa: $|\alpha|^2 + |\beta|^2 = 1$. Ở đây, $|\alpha|^2$ đại diện cho xác suất hệ suy sụp về trạng thái $|0\rangle$ và $|\beta|^2$ là xác suất hệ suy sụp về trạng thái $|1\rangle$ khi thực hiện phép đo chuẩn trực giao.

Để hình dung trực quan, một qubit đơn lẻ thường được biểu diễn thông qua mặt cầu Bloch (Bloch Sphere). Bằng cách sử dụng các tọa độ góc (θ, ϕ) , trạng thái $|\psi\rangle$ có thể được viết lại như sau:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \text{ với } 0 \leq \theta \leq \pi \text{ và } 0 \leq \phi < 2\pi.$$

Trong biểu diễn này, các trạng thái cổ điển $|0\rangle$ và $|1\rangle$ nằm tại hai cực Bắc và Nam của mặt cầu, trong khi các trạng thái chồng chất vô hạn nằm trên bề mặt mặt cầu. Biến số ϕ đại diện cho pha tương đối (relative phase) – một thành phần đặc trưng quyết định tính giao thoa lượng tử nhưng không có tương đương trong thông tin cổ điển.

Khi xét hệ thống gồm n qubit, không gian trạng thái sẽ mở rộng theo tích tensor $\mathcal{H}^{\otimes n}$, tạo ra một không gian Hilbert 2^n chiều. Sự gia tăng số chiều theo hàm lũy thừa này chính là nguồn gốc tạo nên sức mạnh tính toán vượt trội của máy tính lượng tử, cho phép xử lý đồng thời lượng thông tin khổng lồ. Tuy nhiên, chính sự nhạy cảm của các tham số θ và ϕ trước các tác động từ môi trường bên ngoài dẫn đến hiện tượng mất liên lạc lượng tử (decoherence), làm sai lệch thông tin và đòi hỏi các cơ chế sửa sai nghiêm ngặt sẽ được trình bày trong các phần tiếp theo.

2.2. Mô hình lỗi lượng tử

Trong môi trường tính toán cổ điển, sai số chủ yếu tồn tại dưới dạng lỗi nhảy bit (bit-flip), tức là sự biến đổi trạng thái từ 0 sang 1 hoặc ngược lại. Tuy nhiên, trong hệ thống lượng tử, sai số phức tạp hơn rất nhiều do tính chất liên tục của các biên độ xác suất và sự tồn tại của pha lượng tử. Bất kỳ tương tác không mong muốn nào giữa qubit và môi trường (hiện tượng decoherence) đều có thể gây ra những biến đổi đơn nhất (unitary) hoặc không đơn nhất làm sai lệch trạng thái gốc.

Mặc dù không gian lỗi là liên tục, một đặc điểm quan trọng của lý thuyết sửa sai lượng tử là mọi lỗi bất kỳ E tác động lên một qubit đều có thể được biểu diễn dưới dạng tổ hợp tuyến tính của các ma trận Pauli cơ sở $\{\sigma_I, \sigma_x, \sigma_y, \sigma_z\}$. Điều này cho phép ta “rời rạc hóa” các lỗi lượng tử thành các loại hình cụ thể:

+ **Lỗi nhảy bit (Bit-flip error -)**: Tương ứng với ma trận Pauli $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Tác động của lỗi này làm

hoán đổi biên độ xác suất của các trạng thái cơ sở:

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

+ **Lỗi đảo pha (Phase-flip error -)**: Tương ứng với ma trận Pauli $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Đây là loại lỗi đặc thù lượng tử, không có tương đương trong hệ cổ điển. Nó làm thay đổi dấu giữa các thành phần chồng chất mà không làm thay đổi xác suất đo đạt: $Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$.

+ **Lỗi hỗn hợp pha-bit (Bit-phase-flip error -)**: Tương ứng với ma trận Pauli $\sigma_y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Lỗi này xảy ra khi một qubit vừa bị nhảy bit vừa bị đảo pha đồng thời.

Mô hình lỗi phổ biến nhất được sử dụng trong nghiên cứu này là Kênh khử cực (Depolarizing Channel). Trong mô hình này, mỗi qubit có xác suất $1 - p$ là không bị lỗi, và xác suất p bị lỗi, trong đó các lỗi X, Y, Z xảy ra với xác suất bằng nhau là $p/3$. Khi xét hệ thống n -qubit, toán tử lỗi tổng quát $\mathcal{E}$ sẽ là tích tensor của các toán tử Pauli trên từng qubit riêng lẻ: $\mathcal{E} = E_1 \otimes E_2 \otimes \dots \otimes E_n$.

Việc hiểu rõ cấu trúc của các toán tử này là điều kiện tiên quyết để xây dựng các phép đo Syndrome (syndrome measurements). Trong mục tiếp theo, chúng ta sẽ thấy cách mã CSS sử dụng các tính chất giao hoán và phản giao hoán của nhóm Pauli để phát hiện lỗi mà không làm sụp đổ trạng thái chồng chất của dữ liệu, qua đó bảo toàn tính toàn vẹn của thông tin lượng tử.

3. Mã sửa sai calderbank-shor-steane

3.1. Cấu trúc mã hóa

Mã Calderbank-Shor-Steane (CSS) là một lớp quan trọng của mã ổn định (stabilizer codes), được xây dựng dựa trên sự kết hợp khéo léo giữa hai mã sửa sai cổ điển tuyến tính. Điểm đặc biệt của mã CSS là khả năng chuyển hóa bài toán sửa lỗi lượng tử phức tạp thành bài toán sửa lỗi trên các bit cổ điển đơn thuần.

Giả sử ta có hai mã tuyến tính cổ điển C_1 và C_2 lần lượt có các thông số $[n, k_1]$ và $[n, k_2]$, thỏa mãn điều kiện $C_2 \subset C_1$. Điều này có nghĩa là mọi từ mã trong C_2 cũng đồng thời là từ mã trong C_1 . Không gian vector con C_2 chia mã C_1 thành các lớp kề (cosets) dạng $x + C_2$ với $x \in C_1$. Mã lượng tử CSS tương ứng, ký hiệu là $CSS(C_1, C_2)$, sẽ có số chiều là $k = k_1 - k_2$, nghĩa là nó mã hóa được k qubit logic vào n qubit vật lý. Với mỗi từ mã $x \in C_1$, ta định nghĩa một trạng thái lượng tử logic $|\xi_x\rangle$ là sự chồng chất chuẩn hóa của tất cả các vector trong lớp kề tương ứng:

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x \oplus y\rangle$$

Trong đó biểu thức $x \oplus y$ thực hiện phép cộng modulo 2 trên từng bit. Cần lưu ý rằng nếu $x - x' \in C_2$ thì $|x + C_2\rangle$ và $|x' + C_2\rangle$ biểu diễn cùng một trạng thái lượng tử. Do đó, các trạng thái cơ sở của mã

lượng từ này được xác định bởi tập hợp các lớp kề của C_2 trong C_1 .

Cấu trúc này mang lại một ưu thế toán học cực kỳ quan trọng: tính trực giao. Vì các lớp kề khác nhau là rời nhau, các trạng thái lượng tử tương ứng sẽ đôi một trực giao, đảm bảo không gian mã hóa là một không gian con hợp lệ trong không gian Hilbert n -qubit. Hơn nữa, điều kiện để mã CSS có thể sửa đồng thời lỗi bit và lỗi pha liên quan trực tiếp đến khoảng cách Hamming tối thiểu của C_1 và mã đối ngẫu $C_2^\perp$. Cụ thể, nếu C_1 sửa được t lỗi bit và $C_2^\perp$ sửa được t lỗi pha, thì mã lượng tử CSS tổng hợp có khả năng hiệu chỉnh bất kỳ lỗi lượng tử nào có trọng số không vượt quá t . Sự lồng ghép này biến mã CSS trở thành “cầu nối” hoàn hảo, cho phép áp dụng toàn bộ kho tàng lý thuyết mã hóa cổ điển (như mã Hamming, mã BCH hay mã Reed-Muller) vào lĩnh vực truyền tin lượng tử đầy thách thức.

3.2. Cơ chế phát hiện và hiệu chỉnh sai số của mã CSS

Cơ chế sửa lỗi của mã CSS dựa trên một nguyên lý cốt lõi: sự độc lập tương đối giữa lỗi nhảy bit (X) và lỗi đảo pha (Z) trong cấu trúc đại số của mã. Quy trình này được thực hiện thông qua hai giai đoạn chính, sử dụng các phép đo không phá hủy để trích xuất thông tin về lỗi (error syndrome) mà không làm sụp đổ trạng thái lượng tử của qubit dữ liệu.

a. Phép đo Syndrome và Hiệu chỉnh lỗi Bit-flip

Giả sử trạng thái mã hóa ban đầu là $|\psi\rangle$. Khi xảy ra lỗi bit-flip E_x (tương ứng với các toán tử Pauli X), trạng thái trở thành $E_x|\psi\rangle$. Để phát hiện lỗi này, mã CSS sử dụng ma trận kiểm tra parity H_1 của mã cổ điển C_1 .

Trong mạch lượng tử, điều này được thực hiện bằng cách sử dụng các qubit phụ trợ (ancilla qubits). Các ancilla được chuẩn bị ở trạng thái $|0\rangle$, sau đó tương tác với các qubit dữ liệu thông qua các cổng CNOT, trong đó qubit dữ liệu đóng vai trò điều khiển và ancilla đóng vai trò đích. Phép đo trên các ancilla này sẽ trả về trị riêng (eigenvalue) của toán tử kiểm tra, tương ứng với hội chứng lỗi (syndrome) $s_x = H_1 \cdot e_x$ (với e_x là vector lỗi cổ điển).

Vì s_x là một giá trị cổ điển, ta có thể sử dụng các thuật toán giải mã cổ điển (như hội chứng giải mã - syndrome decoding) để xác định vị trí lỗi và áp dụng toán tử X tương ứng để đảo ngược sai số, đưa hệ thống về trạng thái ban đầu đối với kênh lỗi bit.

b. Chuyển đổi và Hiệu chỉnh lỗi Phase-flip

Thách thức lớn nhất của mã lượng tử so với mã cổ điển là lỗi đảo pha (Z). Mã CSS giải quyết vấn đề này bằng một kỹ thuật tinh vi: chuyển đổi lỗi pha thành lỗi bit thông qua phép biến đổi Hadamard (H).

Toán tử Hadamard có tính chất biến đổi cơ sở: $HXH = Z$ và $HZH = X$. Do đó, bằng cách áp dụng cổng H lên toàn bộ n qubit của mã CSS, lỗi pha E_z ban đầu sẽ biến thành lỗi bit E'_x tác động lên trạng thái trong không gian liên hợp.

Lúc này, mã CSS tận dụng mã cổ điển thứ hai C_2 . Quy trình đo syndrome diễn ra tương tự như phần 3.2.1 nhưng sử dụng ma trận kiểm tra H_2 của mã đối ngẫu $C_2^\perp$. Sau khi thu được syndrome pha s_z , một thuật toán giải mã cổ điển lại được thực thi để xác định các vị trí bị đảo pha. Cuối cùng, một phép biến đổi Hadamard ngược lại được áp dụng để đưa các qubit về cơ sở chuẩn sau khi đã hiệu chỉnh.

c. Tính chất không phá hủy và bảo toàn chồng chất

Một đặc điểm quan trọng bậc nhất trong cơ chế sửa lỗi CSS là phép đo syndrome chỉ trích xuất thông tin về vị trí và loại lỗi, chứ không trích xuất thông tin về trạng thái dữ liệu (α và β).

Xét về mặt toán học, các toán tử đo (stabilizers) của mã CSS được thiết kế để giao hoán với nhau. Phép đo syndrome thực chất là phép chiếu trạng thái lỗi vào các không gian con trực giao của các toán tử này. Vì trạng thái mã hóa nằm trong không gian riêng có trị riêng bằng +1 của tất cả các stabilizer, nên phép đo sẽ không làm thay đổi biên độ xác suất của dữ liệu nếu không có lỗi, hoặc sẽ chỉ “chỉ điểm” lỗi nếu có.

d. Quy trình tổng quát (R)

Quy trình hiệu chỉnh tổng quát đối với một mã CSS có thể tóm tắt qua các bước:

1. **Trích xuất Syndrome Bit:** Sử dụng các qubit phụ trợ tương tác với khối mã để thu được s_x .
2. **Xử lý cổ điển:** Giải mã s_x để tìm vector lỗi e_x .
3. **Phục hồi Bit:** Áp dụng X^{e_x} lên các qubit tương ứng.
4. **Chuyển cơ sở:** Áp dụng cổng H trên toàn khối mã.
5. **Trích xuất Syndrome Pha:** Thu được s_z thông qua các qubit phụ trợ.
6. **Xử lý cổ điển:** Giải mã s_z để tìm vector lỗi e_z .
7. **Phục hồi Pha:** Áp dụng X^{e_z} (hiệu chỉnh bit trong cơ sở Hadamard, tương đương hiệu chỉnh pha trong cơ sở chuẩn).
8. **Hoàn tất:** Áp dụng cổng H để trở lại cơ sở ban đầu.

Nhờ khả năng tách biệt hoàn toàn việc xử lý hai loại lỗi này, mã CSS cho phép tận dụng tối đa các bộ giải mã cổ điển hiệu năng cao (như giải mã dựa trên đồ thị hoặc xác suất), tạo tiền đề cho việc xây dựng các kiến trúc tính toán lượng tử chịu lỗi (Fault-tolerant quantum computing).

(Xem tiếp trang 206)