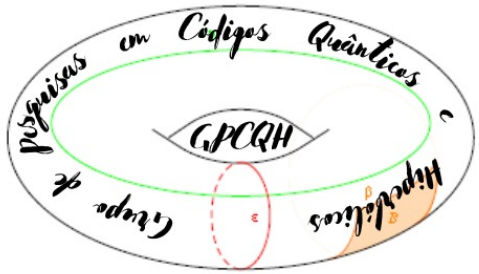
Códigos Quânticos: do código de Shor aos códigos topológicos

Leandro Bezerra de Lima (UFMS)
Giuliano G. La Guardia (UEPG)
Clarice Dias de Albuquerque (UFCA)



15 de agosto de 2022

Sumário

Lei de Moore: miniaturização dos componentes, escala onde as leis quânticas devem ser respeitadas.

Complexidade Computacional: acredita-se que o computador quântico use menos passos computacionais para realizar tarefas devido às propriedades quânticas, como emaranhamento e superposição de estados.
Exemplos: Algoritmo de Shor, Algoritmo de Grover, outros.

Criptografia Quântica: Protocolos de Criptografia mais seguros.

Simulação de Sistemas Quânticos: acredita-se que propriedades quânticas que não possuem análogo clássico não devam ser simuláveis por computadores clássicos.

Algumas apostas e pesquisas de grandes empresas:

- **IBM:** processador de 50 qubits. Disponibilização online de um processador de 20 qubit. Permite que clientes usem a plataforma para efetuar cálculos e simulações.
- **Intel:** Tangle Lake, processador de 49 qubits.
- **Google:** Processador quântico Bristlecon com 72 qubits. Destinado a experimentos científicos e pesquisas.
- **D-Wave 2000Q:** Estão sendo testados pela NASA e Loockheed Martin, foram projetados para resolver Problemas (específicos) de Otimização - ganho de 100 milhões de vezes.
- **Station Q:** Laboratório localizado no campus da Universidade da Califórnia, em Santa Barbara, focado nos estudos de computação quântica topológica. O grupo foi fundado por Dr. Michael Freedman.

Deutsch: o aparato computacional de um computador quântico deve se basear nos princípios da mecânica quântica.

A realização de um computador quântico depende especialmente de: PERMITIR ACESSO AO SISTEMA E IMPEDIR A DECOERÊNCIA DA INFORMAÇÃO ATÉ QUE SE COMPLETE UM CÁCULO COMPUTACIONAL.

Vantagens:

- Superposição - Uma partícula está em uma superposição de estados quando se considera todas as amplitudes.
- Emaranhamento - recurso físico fundamental na computação e informação quântica, sendo responsável pela aceleração da computação quântica em relação à computação clássica.

Postulados da Mecânica Quântica

[M. Nielsen and I. Chuang] Mecânica quântica é a parte da física responsável pelo estudo do comportamento de átomos, elétrons, moléculas, entre outras, cujos postulados foram desenvolvidos através de um longo processo. Em essência, iremos considerar a mecânica quântica como sendo uma estrutura matemática que permite descrever sistemas quânticos.

Postulado 1: Existe um espaço vetorial complexo, com produto interno, associado a qualquer sistema físico *fechado* (sistema que não interage com outros sistemas). Um estado desse sistema é completamente descrito por um vetor unitário, chamado **vetor de estado**.

A unidade de informação quântica ou sistema quântico que nos interessa é o **bit quântico** ou *q-bit*, cujo espaço vetorial associado é o $\mathbb{C}^2$, com o produto interno usual. Uma base ortonormal para esse espaço pode ser dada pelos vetores $|0\rangle$ e $|1\rangle$, que serão representados usando a **notação de Dirac**:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

e

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Existem várias maneiras para a representação física de um q-bit. Entretanto, direcionaremos nosso estudo apenas sobre a sua representação matemática.

Ou seja, um q-bit é um vetor unitário de $\mathbb{C}^2$. Um estado arbitrário $|\psi\rangle$ nesse sistema pode ser descrito por

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

onde $\alpha, \beta \in \mathbb{C}$ e a restrição $|\alpha|^2 + |\beta|^2 = 1$ deve ser satisfeita. A base $\{|0\rangle, |1\rangle\}$ é chamada **base computacional** e o vetor $|\psi\rangle$ denota a **superposição** dos vetores $|0\rangle$ e $|1\rangle$, com **amplitudes** α e β (usaremos os termos vetor e estado indistintamente).

O nome q-bit vem do fato de que o bit quântico pode ser visto como uma generalização do bit clássico, que assume apenas 2 estados: 0 ou 1. A diferença entre eles é que um q-bit pode, além dos estados $|0\rangle$ e $|1\rangle$, assumir uma quantidade infinita de estados!
Base conjugada: $\{|+\rangle, |-\rangle\}$, onde

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad e \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Postulado 2: A evolução de um sistema quântico fechado é descrita por um operador linear que preserva o produto interno (operador **unitário)**. O estado $|\psi_1\rangle$ do sistema, no tempo t_1, está relacionado ao estado $|\psi_2\rangle$, no tempo t_2, através de um operador unitário U que depende apenas de t_1 e t_2. Ou seja,

$$|\psi_2\rangle = U|\psi_1\rangle.$$

Existe um operador unitário que transforma o estado $|0\rangle$ em $|1\rangle$ e o estado $|1\rangle$ em $|0\rangle$. Esse operador é denotado por X e sua representação matricial, na base computacional, é dada por

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{1}$$

Outro exemplo de um operador unitário sobre um q-bit é o operador Z, cuja representação matricial, também na base computacional, é dada por:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2}$$

Os operadores X e Z, quando aplicados sobre o estado $|0\rangle$, ainda retornam estados da base computacional $\{|0\rangle, |1\rangle\}$. Ou seja,

$$X|0\rangle = |1\rangle$$

e

$$Z|0\rangle = |0\rangle.$$

Entretanto, o operador unitário *Hadamard* H, cuja representação matricial, na base computacional, é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

produz uma superposição de estados, quando aplicado sobre um estado da base computacional.

Ou seja,

$$H|0\rangle = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$$

e

$$H|1\rangle = \frac{\sqrt{2}}{2}|0\rangle - \frac{\sqrt{2}}{2}|1\rangle.$$

Matrizes de Pauli:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

As matrizes de Pauli formam uma base para o espaço vetorial das operações sobre um qubit. Ou seja, todo operador unitário (ou transformação unitária) sobre um qubit pode ser expresso como uma combinação linear das matrizes de Pauli.

Para prosseguirmos, precisamos definir três conceitos: *dual, produto interno* e *produto externo*. O dual de um vetor $|\varphi\rangle \in \mathbb{C}^n$, denotado por $\langle\varphi|$, é o vetor transposto de $|\varphi\rangle$ com os elementos substituídos pelos seus conjugados. Ou seja,

$$\langle\varphi| = (|\varphi\rangle)^\dagger.$$

Matricialmente, no caso de um q-bit, dado por

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

temos que

$$\langle\varphi| = \left(\begin{bmatrix} \alpha \\ \beta \end{bmatrix}\right)^\dagger = [\alpha^* \ \beta^*].$$

Dados dois vetores $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^n$, o produto interno $\langle\varphi|\psi\rangle$ e o produto externo $|\varphi\rangle\langle\psi|$ são definidos, respectivamente, por

$$\langle\varphi|\psi\rangle = (|\varphi\rangle)^\dagger |\psi\rangle$$

e

$$|\varphi\rangle\langle\psi| = |\varphi\rangle(|\psi\rangle)^\dagger.$$

Note que $|\varphi\rangle, |\psi\rangle$ são vetores "coluna" e $\langle\varphi|, \langle\psi|$ são vetores "linha".

Sejam $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ e $|\psi\rangle = \gamma|0\rangle + \xi|1\rangle$, dois vetores pertencentes a $\mathbb{C}^2$, temos para o produto interno e para o produto externo, respectivamente:

$$\langle\varphi|\psi\rangle = (|\varphi\rangle)^\dagger|\psi\rangle = [\alpha^* \ \beta^*]\begin{bmatrix} \gamma \\ \xi \end{bmatrix} = \alpha^*\gamma + \beta^*\xi.$$

e

$$|\varphi\rangle\langle\psi| = |\varphi\rangle(|\psi\rangle)^\dagger = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}[\gamma^* \ \xi^*] = \begin{bmatrix} \alpha\gamma^* & \alpha\xi^* \\ \beta\gamma^* & \beta\xi^* \end{bmatrix}.$$

Outro exemplo pode ser dado por:

$$\langle 0|1\rangle = [1\ 0]\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1.0 + 0.1 = 0$$

e

$$|0\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}[0\ 1] = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

A interpretação física do q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, para α e β não nulos, é que ele está simultaneamente nos estados $|0\rangle$ e $|1\rangle$! Pelo postulado 2, já sabemos que, aplicando um operador unitário sobre o estado $|\psi\rangle$, o novo estado ainda será uma superposição dos estados $|0\rangle$ e $|1\rangle$. Isso faz com que a quantidade de informação armazenada no estado $|\psi\rangle$ possa ser infinita. Entretanto, essa quantidade infinita de informação está no nível quântico. Para torná-la acessível no nível clássico, precisamos fazer uma medida. Para considerar esse fato, existe um terceiro postulado.

Postulado 3: As medidas sobre sistemas quânticos são descritas por operadores **hermitianos** M ($M^\dagger = M$), chamados **observáveis**.
Pelo fato de M ser hermitiano, podemos escrever

$$M = \sum_{i=1}^{n} \lambda_i |i\rangle\langle i|,$$

onde $\{|i\rangle\}$, $i = 1, ..., n$, é uma base ortonormal de autovetores de M com os respectivos autovalores λ_i. Os possíveis resultados da medida correspondem aos autovalores λ_i de M. Supondo que o resultado da medida seja "λ_i", o estado $|\psi_{\lambda_i}\rangle$, após a medida, é dado por

$$|\psi_{\lambda_i}\rangle = \frac{(|i\rangle\langle i|)|\psi\rangle}{\sqrt{p_{\lambda_i}}}, \tag{3}$$

onde $|\psi\rangle$ é o estado anterior à medida e p_{λ_i} é a probabilidade de se obter "λ_i", dada por

$$p_{\lambda_i} = \langle\psi|(|i\rangle\langle i|)|\psi\rangle. \tag{4}$$

Na realidade, a medida descrita no Postulado 3, chamada *medida projetiva*, é um caso particular de uma medida mais geral.

Vejamos um exemplo. Façamos uma medida de um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, usando o observável Z, dado em (2), que pode ser escrito como

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Usando (3) e (4), temos:

$$p_1 = \left(\alpha^\dagger\langle 0|0\rangle + \beta^\dagger\langle 1|0\rangle\right)\left(\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle\right) = |\alpha|^2$$

e

$$|\psi_1\rangle = \frac{\alpha\langle 0|0\rangle|0\rangle + \beta\langle 0|1\rangle|0\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle.$$

De forma similar, podemos obter

$$p_{-1} = |\beta|^2$$

e

$$|\psi_{-1}\rangle = \frac{\beta}{|\beta|}|1\rangle.$$

Resumindo: usando o observável Z para fazer uma medida de um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, podemos obter o estado $\frac{\alpha}{|\alpha|}|0\rangle$, com probabilidade $|\alpha|^2$, ou o estado $\frac{\beta}{|\beta|}|1\rangle$, com probabilidade $|\beta|^2$ (em termos de observação, os estados $\frac{\alpha}{|\alpha|}|0\rangle$ e $|0\rangle$ são idênticos, assim como os estados $\frac{\beta}{|\beta|}|1\rangle$ e $|1\rangle$.

Para descrever estados com mais de um q-bit, temos o postulado 4.

Postulado 4: O estado composto por n estados, $|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_n\rangle$, é o produto tensorial $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.
Para os nossos propósitos, definimos o produto tensorial $A \otimes B$, entre as matrizes
$A \in \mathbb{C}^{m\times n}$ e $B \in \mathbb{C}^{p\times q}$, como sendo a matriz

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix},$$

onde A_{ij} é o elemento da linha i e da coluna j de A. Note que a dimensão da matriz $A \otimes B$ é $mp \times nq$ e que o produto tensorial não é comutativo.

Por exemplo,

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

e

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Usaremos também a notação $|v\rangle|w\rangle$ ou $|vw\rangle$ para o produto tensorial $|v\rangle \otimes |w\rangle$.

Para prosseguirmos, necessitamos de algunas definições da álgebra linear:

Definição

O traço de uma matriz A é a soma dos elementos da sua diagonal principal,

$$tr(A) \equiv \sum_i A_{ii}.$$

Definição

Um operador positivo A é aquele para o qual $\langle\psi|A|\psi\rangle \geq 0$ para todo $|\psi\rangle$.

Uma alternativa para a formulação dos postulados da mecânica quântica é em termos do *operador densidade*. Essa formulação é útil para descrever sistemas quânticos cujos estados não são completamente conhecidos. Suponha que um sistema quântico esteja em um do estados $|\psi_1\rangle, ..., |\psi_n\rangle$, com as respectivas probabilidades $p_1, ..., p_n$.

Chamaremos o conjunto $\{p_i, |\psi_i\rangle\}$, um "ensemble "de estados puros. O operador densidade do sistema é dado por

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i|.$$

Por exemplo, a representação de um q-bit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, na forma de operador densidade, ficaria no seguinte formato:

$$\rho = |\alpha|^2|0\rangle\langle 0| + \alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|.$$

Os operadores que podem representar operador densidade são caracterizados pelo seguinte teorema.

Teorema

Um operador ρ é operador densidade do "ensemble "$\{p_i, |\psi_i\rangle\}$ se, e somente se, satisfizer as seguintes condições:
1-(Condição sobre o traço) O traço de ρ deve ser igual a 1.
2-(Condição de positividade) ρ deve ser positivo.

Dizemos ainda que ρ está num *estado puro* se $\rho = |\psi\rangle\langle\psi|$ e, neste caso, vale a propriedade $tr(\rho^2) = 1$. Quando o estado não é puro, ele é chamado *estado misturado ou misto* e, neste caso, temos $tr(\rho^2) < 1$. Baseado nessa nova formulação, iremos reescrever os postulados da mecânica quântica.

Postulado 1: Associado a qualquer sistema físico existe um espaço vetorial complexo (ou seja, um espaço de Hilbert) conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu operador densidade, que é um operador positivo com traço 1 atuando no espaço de estados. Se o sistema está no estado ρ_i, com probabilidade p_i, o seu operador densidade será $\sum_i p_i \rho_i$.

Postulado 2: A evolução de um sistema quântico fechado é descrita por transformações unitárias. Isto é, o estado ρ do sistema em um instante t_1 está relacionado ao estado $\rho^{'}$ em um instante t_2 por um operador unitário U que depende somente de t_1 e t_2,

$$\rho^{'} = U\rho U^{\dagger}.$$

Postulado 3: Medidas quânticas são descritas por uma coleção de operadores de medidas $\{M_n\}$. Esses operadores atuam sobre o espaço de estados do sistema sendo medido. O índice n refere-se a um resultado possível da medida. Se o estado do sistema imediatamente antes da medida for ρ, a probabilidade de o resultado n ocorrer será

$$p(n) = tr(M_n^\dagger M_n \rho)$$

e o estado do sistema após a medida será

$$\frac{M_n \rho M_n^\dagger}{tr(M_n^\dagger M_n \rho)}.$$

Os operadores de medida satisfazem a equação de completitude

$$\sum_n M_n^\dagger M_n = I.$$

Postulado 4: O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados das suas componentes. Além disso, se tivermos sistemas numerados de 1 até n, e o i-ésimo sistema for preparado em ρ_i, o estado do sistema composto será $\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$.

Um código (n, k) de comprimento n com q^k palavras-código é um **código linear** se suas q^k palavras-código formam um subespaço de dimensão k sobre $\mathbb{F}_q$.

A **distância mínima** de um código $\mathcal{C}$ é dada por

$$d = min\{d(\mathbf{v}, \mathbf{w}); \mathbf{v}, \mathbf{w} \in \mathcal{C}, \mathbf{v} \neq \mathbf{w}\}.$$

Procedimento de codificação: $v = u.G$, onde G é a matriz geradora do código.

Teorema: Seja $\mathcal{C}$ um código com distância mínima d. Então, $\mathcal{C}$ pode detectar até $d - 1$ erros e corrigir até t erros, onde $t = \lfloor \frac{d-1}{2} \rfloor$.

A **taxa de codificação** do código (n, k, d) é dada por $\frac{k}{n}$.

Um código linear (n, k, d) deve satisfazer:

- **Limitante de Singleton:**

$$d \leq n - k + 1$$

Um código que satisfaz com igualdade o limitante de Singleton é chamado MDS (Maximum Distance Separable).

- **Limitante de Hamming:**

$$M\left[1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{t}(q-1)^t\right] \leq q^n$$

Um código que satisfaz com igualdade o limitante de Hamming é um *código perfeito* (corrige todos os erros de peso menor ou igual a t e nenhum de peso maior que t).

No sentido de superar o obstáculo da decoerência muitas pesquisas são desenvolvidas em códigos quânticos corretores de erros, computação tolerante à falhas e em modelos diversos de computador quântico.

Código Quântico Corretor de Erros $[[n, k, d]]$**:** k qubits são codificados em n qubits. Um código com distância mínima d pode detectar até $d-1$ erros e corrigir até $\lfloor \frac{d-1}{2} \rfloor$ erros.

Código de Shor $[[9, 1, 3]]$**:** pode corrigir um erro arbitrário ocorrido em um qubit.

Bibliografia


M. Nielsen and I. Chuang, **Quantum Computation and Quantum Information**, Cambridge University Press, 2000.


R.W. Hamming **Error Detecting and Error Correcting Codes**, The Bell System Technical Journal, vol. 27, 1948.


F. MacWillians and N. Sloane, **The Theory of Error-Correcting Codes**, The Mathematical Association of America, vol. 21, 1983.


C.E. Shannon, **A Mathematical Theory of Comunication**, The Bell System Technical Journal, vol. 28, 1948.

Obrigado pela Atenção!