Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Sobre códigos estabilizadores

Luciano Alves Vieira[1]
FEEC/UNICAMP, Campinas, SP
Clarice Dias de Albuquerque[2]
CCT/UFCA, Juazeiro do Norte, CE
Reginaldo Palazzo Junior[3]
FEEC/UNICAMP, Campinas, SP

1 Introdução

Uma das maiores dificuldades para a construção de um computador quântico é a perda de informação devido a interação do sistema quântico com o meio em que ele está inserido, um fenômeno conhecido como *decoerência*. Dessa forma, a proteção da informação quântica pelo uso de *Códigos Quânticos Corretores de Erros* é uma das ferramentas fundamentais para permitir o desenvolvimento dessa nova tecnologia. Gottesman propôs em 1996 [1] a classe de códigos quânticos denominada *Códigos Estabilizadores*, que inclui, por exemplo, o código de Shor e os códigos de Calderbank-Shor-Steane (CSS). Os códigos estabilizadores têm sua base fundamentada na Teoria de Grupos, de fato, um código dessa classe é o espaço simultaneamente fixado por todos os elementos de um subgrupo abeliano do grupo de Pauli.

O presente trabalho tem como objetivo apresentar de forma direta e simplificada os códigos quânticos estabilizadores, indicando nesse processo as principais estruturas matemáticas presentes em sua teoria.

2 O formalismo estabilizador

O grupo de Pauli de ordem n, denotado por $\mathcal{G}_n$, é de fundamental importância no estudo dos Códigos Quânticos Corretores de Erros. Esse grupo é formado pelo conjunto dos produtos tensoriais de ordem n das matrizes de Pauli (I, σ_x, σ_y e σ_z), conjuntamente com os fatores multiplicativos ± 1 e $\pm i$, sob operação de multiplicação matricial.

Se um código consegue corrigir os erros E e F, então ele corrige erros da forma $aE + bF$. Logo, só é necessário verificar se ele consegue corrigir uma base de erros. Uma base conveniente é a formada pelos tensoriais de I, σ_x, σ_y e σ_z [2]. De fato, os tensoriais de σ_x e σ_z (e I) geram os outros elementos do grupo, e, portanto, são suficientes para gerar os erros.

O grupo de Pauli $\mathcal{G}_n$ possui ainda as seguintes características:(i) Todo elemento é unitário, ou seja, $\forall M \in \mathcal{G}_n, M^{-1} = M^\dagger$; (ii) Se $M^2 = I$, então M é Hermitiano ($M = M^\dagger$); se $M^2 = -I$, então M é anti-Hermitiano ($M = -M^\dagger$); (iii) Dados M e $N \in \mathcal{G}_n$, M e N comutam ($MN = NM$) ou anticomutam ($MN = -NM$).

[1]luciano.alves.vieira@gmail.com
[2]clarice.albuquerque@ufca.edu.br
[3]palazzo@dt.fee.unicamp.br

De forma geral, define-se o estabilizador S como um subgrupo abeliano de $\mathcal{G}_n$ que não contém $-I$. O código estabilizador $\mathcal{C}_S$ associado ao estabilizador S é o autoespaço simultâneo com autovalor 1 de todos os elementos de S, ou seja: $\mathcal{C}_S = \{|\psi\rangle ; M|\psi\rangle = |\psi\rangle , \forall M \in S\}$.

A denominação de S por estabilizador deve-se ao fato de que cada operador aplicado a cada palavra-código resulta na própria palavra-código. Diz-se que um conjunto de elementos independentes de S, $\{M_1, M_2, \dots M_l\}$, gera S se todo elemento de S pode ser escrito como um produto de $M_1, M_2, \dots M_l$. Em muitas situações é mais interessante, e mais compacto, trabalhar apenas com um conjunto gerador do estabilizador S, por exemplo: a fim de identificar se um estado $|\psi\rangle$ é uma palavra-código de um determinado código estabilizador $\mathcal{C}_S$ podemos apenas verificar se esse estado é fixado por todos os geradores, em vez de verificar para todo os elementos do estabilizador. Assim, os códigos estabilizadores possuem semelhança com os códigos corretores de erros clássicos, no sentido que os geradores funcionam como *operadores verificação de paridade* do código estabilizador, sendo as medidas desses operadores utilizadas para a identificação da existência de erros.

Seja $\varepsilon = \{E_a\} \subset \mathcal{G}_n$ um conjunto de erros. Um operador erro $E_a \in \varepsilon$ satisfaz uma das seguintes situações: (i)E_a anticomuta com pelo menos um gerador M do estabilizador S; (ii)E_a comuta com todos os geradores M mas $E_a \notin S$; (iii) E_a comuta com todos os geradores M e $E_a \in S$; Analisemos as três situações. Se o erro E_a anticomutar com algum gerador M do estabilizador, então, para um estado $|\psi\rangle \in \mathcal{C}_S$: $ME_a|\psi\rangle = -E_aM|\psi\rangle = -E_a|\psi\rangle$, e portanto conseguimos identificar o erro E_a por meio de uma medida de M. No caso de E_a comutar com todos os geradores de S temos que: $ME_a|\psi\rangle = E_aM|\psi\rangle = E_a|\psi\rangle$. Em outras palavras, $E_a|\psi\rangle$ pertence ao espaço do código. Caso $E_a \in S$, então a ação do erro sobre a palavra-código é trivial ($E_a|\psi\rangle = |\psi\rangle$), e portanto não há perda de informação. Porém, se E_a comuta com todos os elementos de S, mas $E_a \notin S$, então alguma palavra-código não é fixada por E_a. Dessa forma o efeito de E_a sobre o código $\mathcal{C}_S$ é um rearranjo dos elementos, causando perda de informação quântica.

Definimos então o peso de um elemento de $\mathcal{G}_n$, como o número de fatores no tensor que diferem de I. Dessa forma, a distância de um código estabilizador $\mathcal{C}_S$ será d se todo $E \in \mathcal{G}_n$ com peso menor que d pertencer ao estabilizador ou anticomutar com algum elemento dele.

Os códigos estabilizadores formam uma das classes de códigos quânticos corretores de erros mais importantes. Descrever um código por meio do seu estabilizador e de seus geradores, permite, além de uma abordagem compacta, maior facilidade na identificação do conjunto de erros corrigível pelo código. Para mais informações sobre o tema dos códigos estabilizadores sugerimos ao leitor interessado as referências [2,3].

Agradecimentos

Agradecemos ao CNPq pela concessão das bolsas de Produtividade em Pesquisa, por meio do projeto 305656/2015-5, e de Mestrado que possibilitaram a realização deste trabalho.

Referências

[1] Gottesman, D. Class of quantum error-correcting codes saturating the quantum Hamming bound, *Physical Review A*, 54:1862-1868, 1996. DOI:10.1103/physreva.54.1862.

[2] Gottesman, D. Stabilizer Codes and Quantum Error Correction, Tese de Doutorado, California Institute of Technology, 2008.

[3] Preskill, J. Lecture notes for physics 219: quantum computation. California Institute of Technology, 2004.