Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

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

Códigos Quânticos Topológicos

Fernanda Taranto Castanheira Caseca[1]
Cátia Regina de Oliveira Quilles Queiroz[2]
UNIFAL-MG, Alfenas, MG

Uma enorme quantidade de dados é transmitida a todo momento nos dias de hoje. Os dois principais problemas nessa transmissão são: garantir que, se a mensagem for interceptada por um indivíduo diferente do destinatário, essa esteja codificada e o referido indivíduo não consiga compreendê-la, mas o destinatário consiga decodificá-la sem maiores problemas; garantir que a mensagem chegue sem erros (ou ruídos) ao destinatário.

Um código corretor de erros é, essencialmente, uma forma de acrescentar ambiguidades a cada informação que se queira transmitir ou armazenar, de forma a permitir detectar e corrigir erros ao recuperar a informação. Um dos objetivos de um código é que o mesmo possua uma quantidade grande de palavras para poder transmitir muita informação, mas que consiga detectar e corrigir muitos erros. Além disso, espera-se que possua algoritmos de codificação e decodificação simples e rápidos. Esses objetivos conflitam entre si, em que a questão de se encontrar valores satisfatórios para tais variáveis talvez seja uma das questões principais na Teoria de Códigos [2].

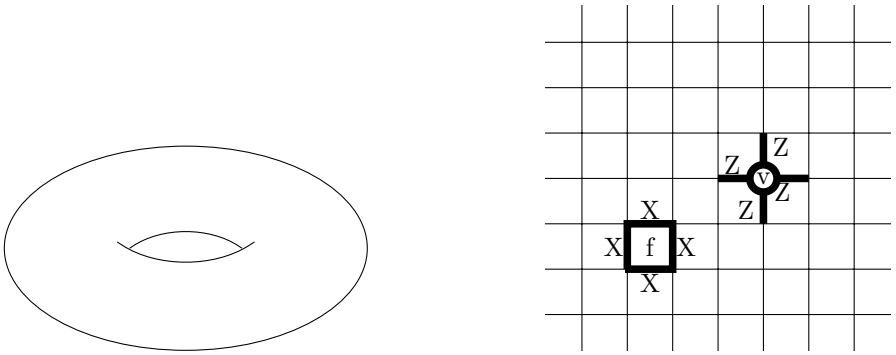
A Teoria dos Códigos Corretores de Erros teve início na década de quarenta. Richard W. Hamming desenvolveu um código capaz de detectar até dois erros e corrigir um erro, se ele for o único, mas ele publicou diversos memorandos questionando sobre a possibilidade de se construir códigos mais eficientes que aquele proposto inicialmente. A questão foi respondida indiretamente em outubro de 1948, por C. E. Shannon no artigo intitulado "A Mathematical Theory of Communication", também publicado no "The Bell System Technical Journal". O artigo de C. E. Shannon deu início a dois novos campos de pesquisa em matemática: a Teoria de Códigos (em conjunto com o trabalho de Hamming) e a Teoria da Informação. A partir desse artigo, pode-se dizer que houve um desenvolvimento contínuo e significativo da Teoria dos Códigos Corretores de Erros até o presente momento [3].

O estudo dos códigos corretores de erros quânticos, assim como os clássicos, tem o objetivo de transmitir e armazenar dados de maneira confiável, de modo que ao recuperar essa informação, seja possível detectar e corrigir tais erros, utilizando ferramentas matemáticas como teoria de grupos e combinatória. A Teoria dos Códigos Quânticos de Correção de Erros estende as noções básicas dos códigos clássicos, uma diferença marcante reside no fato de que os erros quânticos estão muito mais presentes do que no caso clássico. Não é possível implementar um hardware quântico sem lidar com correções de erros, pois os estados quânticos facilmente entram em decoerência, sendo esta as interações do sistema com o ambiente a sua volta, podendo destruir os estados quânticos (superposições dos estados $|0\rangle$ e $|1\rangle$, ou produtos tensoriais dos mesmos) provocando a perda de informação, devido à influências do sistema macroscópico sobre o sistema quântico. A correção de erros é possível quando armazenamos a informação quântica de forma redundante. Os códigos eficientes maximizam a chance de sucesso sem usar um excesso de redundância. No caso quântico, vai usar bits quânticos (qubits) para escrever a mensagem. Um código quântico mais simples é o código de 3 qubits para corrigir inversão de 1 qubit (do inglês, quantum bit) [4].

[1] fernanda.caseca@sou.unifal-mg.edu.br.
[2] catia.quilles@unifal-mg.edu.br.

Os códigos quânticos topológicos (CQTs), são uma generalização dos códigos tóricos descritos inicialmente por Kitaev, os quais associam qubits às arestas de um reticulado quadrado de um toro. Os códigos CQTs [1] consideram outras superfícies orientáveis bidimensionais diferentes do toro, e formam uma subclasse dos códigos estabilizadores [4].

Um reticulado no $\mathbb{R}^n$ é definido como um subconjunto discreto infinito de $\mathbb{R}^n$ que é um grupo aditivo sob adição usual de vetores, e pode ser visto como um conjunto infinito de pontos dispostos de forma regular. O reticulado quadrado é gerado pelos vetores $u = (1, 0)$ e $v = (0, 1)$. Um toro é uma superfície orientável com gênero um, ou seja, é equivalente a uma esfera com um "buraco". Um toro planar pode ser descrito como um quadrado cujos lados opostos são identificados, e dessa forma um reticulado quadrado $\mathbb{Z}^2$ no toro pode ser visto como um ladrilhamento por quadrados unitários no toro planar, como mostrado na Figura 1.



(a) Toro superfície.

(b) Reticulado quadrado do toro planar e operadores.

Figura 1: Representações do Toro no espaço e no plano.

Considerando um reticulado quadrado $l \times l$ no toro, temos que V é o conjunto de vértices, E o de arestas e F o de faces do reticulado. Os qubits estão em correspondência um-a-um com as arestas do reticulado. Como cada aresta pertence simultaneamente a duas faces do reticulado, temos que $|E| = 2l^2$, ou seja, o comprimento do código é $n = |E| = 2l^2$ qubits.

De uma maneira geral, pode-se estender a construção de Kitaev em outras superfícies bidimensionais para obtenção de códigos quânticos topológicos corretores de erros, e esse será o foco do nosso trabalho.

Referências

[1] Albuquerque, C. D. Análise e construção de códigos quânticos topológicos sobre variedades bidimensionais, Tese de Doutorado, Unicamp, 2009.

[2] Figueiredo, L. A., Oliveira, G. S. e Ribas, S. Códigos corretores de erros. *Seminário de Iniciação Científica do Instituto Federal de Minas Gerais - Ouro Preto*, 2018.

[3] Milies, C. P. Breve introdução à teoria dos códigos corretores de erros. *Colóquio de Matemática da Região Centro-Oeste*, SBM, 2009.

[4] Portugal, R. Códigos quânticos. *1º Encontro de Teoria dos Códigos e Criptografia da UFABC*, 2010.