Decodificação para Códigos Grafos Quânticos

Gilson O. dos Santos, Francisco M. de Assis, Aércio F. de Lima

***Resumo*— Em [Phys. Rev. A65, 012308(2001)] Schlingmann e Werner propõem uma técnica para construção de códigos estabilizadores com uso de grafos denominando-os códigos grafos quânticos. Neste trabalho apresenta-se uma operação de decodificação para esses códigos. Até onde foi possível verificar, trata-se da primeira operação proposta com esta finalidade.**

***Palavras-Chave*— Código corretor de erro quântico, Códigos grafos quânticos, Decodificação quântica, Transformada de Fourier quântica inversa.**

***Abstract*— In [Phys. Rev. A65, 012308 (2001)] Schlingmann and Werner introduced a technique for construction a class of stabilizers codes using graphs, coined quantum graph codes. In this work one introduces a decoding operation for that class of codes. Up to the authors knowledge, this is the first operation proposed with this purpose.**

***Keywords*— quantum error-correction code; quantum graph code; quantum decoding; inverse quantum Fourier transform.**

I. Introdução

A correção de erros quânticos é uma parte importante para vários esquemas de computação e comunicação quânticas. Devido a isso, códigos corretores de erros quânticos (CCEQ's) têm recebido muita atenção no decorrer dos últimos anos.

Um dos resultados teóricos importantes se deve a Knill e Laflamme [1] que analisaram as condições necessárias e suficientes para que um determinado CCEQ seja capaz de corrigir um determinado conjunto de erros.

Além desse resultado, o formalismo de estabilizadores foi utilizado com sucesso por Gottesman [2] na definição de uma ampla classe de códigos quânticos, os códigos estabilizadores.

Devido as construções existentes para códigos estabilizadores apresentarem grande dificuldade para realizar a verificação da capacidade de correção de erros (verificação das condições de Knill-Laflamme [1]), Schlingemann e Werner [3] fizeram uso da teoria dos grafos para apresentar uma nova maneira de construir códigos estabilizadores de tal forma que as condições necessárias e suficientes para a correção de erros sejam diretamente "visíveis" da estrutura do grafo. Com isso, eles adaptaram as condições de Knill e Laflamme [1] e estabeleceram as condições necessárias e suficientes para um grafo gerar um CCEQ.

Os códigos construídos dessa maneira são denominados *códigos grafos quânticos* (CGQ) [3], [4]. Usando esse método, novos códigos quânticos foram construídos [5], [6].

Para os códigos grafos quânticos, alguns aspectos relativos a decodificação têm sido abordados como, por exemplo, quais são as condições que um grafo deve satisfazer para a correção de e erros [7], [8]; e como identificar um erro considerando submatrizes que representam as configurações de erro [3], [6]. Foi mostrado também que a operação de decodificação para códigos grafos quânticos pode ser realizada em modelos de computador *one-way* [7].

Apesar das condições que um grafo deve satisfazer para que haja a decodificação terem sido apresentadas já há algum tempo, não foi encontrado na literatura nenhuma operação ou procedimento que efetivamente realize a decodificação para esses códigos quânticos.

Diante do que foi exposto, e considerando a importância dos códigos grafos quânticos no cenário dos CCEQ's, neste trabalho é mostrado uma operação de decodificação para esses códigos quânticos.

Gilson O. dos Santos (IF-AL, IQuanta, Prog. Pós-Grad. em Eng. Elétrica), Francisco M. de Assis (IQuanta, Depto. de Eng. Elétrica), Aércio F. de Lima (IQuanta, Depto. de Física), Universidade Federal de Campina Grande, Paraíba, Brasil. E-mails: gilson10@click21.com.br, fmarcos@dee.ufcg.edu.br, aerlima@df.ufcg.edu.br. Este trabalho foi parcialmente financiado pela CAPES/PIQDTec e CNPq (309431/2006.9).

II. Uma descrição geral dos códigos grafos quânticos

A descrição de um grafo (ou matriz) para códigos quânticos é dada a seguir.

Definição 2.1: [3] Todo código grafo construído é completamente determinado pelos seguintes elementos:

- Um grafo não dirigido G com duas classes de vértices: o conjunto X de vértices de entrada, com k elementos, e o conjunto Y de vértices de saída, com n elementos. As interligações dos grafos são dadas pela matriz de *adjacência* do grafo, a qual será denotada por Γ. Os elementos da matriz $\Gamma_{i,j}$ são iguais a 1 se, e somente se, os vértices $z_i, z_j \in (X \cup Y)$ estão interligados, considerando $i, j = 1, \ldots, k+n$ com $i < j$, e 0 caso contrário. De maneira geral, tem-se grafos ponderados, nos quais as matrizes de adjacência tem entradas inteiras arbitrárias, a partir das restrições $\Gamma_{i,j} = \Gamma_{j,i}$ e $\Gamma_{i,i} = 0$.
- Um grupo Abeliano $\mathcal{G}$ com um bicaracter simétrico não degenerado.

Considerando um grafo cuja descrição está de acordo com os elementos dados pela Definição 2.1 e também que os valores atribuídos aos vértices são elementos de um corpo finito $\mathbb{F}$ de ordem p, denotado por $\mathbb{F}_p$ (p é um número primo). Para identificar um vetor, faz-se também o uso da notação $d^V = (d^{v_j})_{v_j \in V} \in \mathbb{F}^{|V|}$, em que $|V|$ é o número de elementos de V e $j = 0, \ldots, |V|$. A operação de codificação é definida a seguir, a qual segue a formulação sugerida por Feng [6].

Definição 2.2 (Codificação CGQ): Seja G um grafo satisfazendo a Definição 2.1. A codificação para CGQ é dada pelo operador

$$f(|v\rangle) = \frac{1}{\sqrt{p^{|Y|}}} \sum_{d^Y \in \mathbb{F}_p^{|Y|}} \lambda(d^Y)|d^Y\rangle \ \in (\mathbb{C}^p)^{\otimes n}, \tag{1}$$

em que

$$|v\rangle = \sum_{d^X \in \mathbb{F}_p^{|X|}} c(d^X)|d^X\rangle \in (\mathbb{C}^p)^{\otimes k} \tag{2}$$

é um vetor não nulo com $c(d^X) \in \mathbb{C}$, sendo

$$\lambda(d^Y) = \sum_{d^X \in \mathbb{F}_p^{|X|}} e^{(\frac{2\pi i}{p})\left\{\frac{1}{2}\left[(d^X)^T,(d^Y)^T\right].\Gamma.\left[\begin{array}{c} d^X \\ d^Y \end{array}\right]\right\}} c(d^X) \quad (3)$$

com $i = \sqrt{-1}$ e $\sum_k [c(d^X)]^2 = 1$.

Os expoentes $\Gamma_{i,j}$ são dados pela matriz de adjacência Γ de um grafo ponderado não dirigido com pesos $\Gamma_{i,j} \in \mathbb{Z}$. Como (1) é independente dos elementos da diagonal $\Gamma_{i,i}$, pode-se assumir, sem perda de generalidade, que o grafo é simples.

Aqui os vértices representam os qbits (ou partículas) e as arestas representam as interações entre os qbits.

Além disso, considera-se nessa construção que as interações (arestas) entre os qbits (vértices) são realizadas como no modelo de Ising, isto é, somente são consideradas interações (arestas) entre os qbits (vértices) mais próximos. Um número diferente de zero (peso) associado a aresta pode ser visto como a força ou poder da interação. Isso pode ser pensado, por exemplo, como uma estrutura de um reticulado óptico bidimensional, em que cada qbit ocupa um ponto dentro de um reticulado cúbico bidimensional com interações entre os vizinhos mais próximos [3].

Após a realização da codificação fazendo uso da expressão (1), obtém-se o estado

$$|\psi\rangle = \frac{1}{\sqrt{p^{|Y|}}}\Big[\lambda(d^{Y(1)}) \cdot |d^{Y(1)}\rangle + \ldots + \lambda(d^{Y(p^{|Y|})}) \cdot |d^{Y(p^{|Y|})}\rangle\Big]. \quad (4)$$

III. Representação de erros em palavras-código de grafos quânticos

A modelagem dos erros computacionais para CGQ segue a notação e as recomendações propostas por Feng [6].

Um erro computacional quântico $\sigma_b\tau_s$ $(b, s \in \mathbb{F}_p)$ em um qbit é um operador linear unitário em $\mathbb{C}^p$, o qual age na base

$$\{|0\rangle, |1\rangle, \ldots, |p-1\rangle\} = \{|a\rangle : a \in \mathbb{F}_p\} \quad (5)$$

em $\mathbb{C}^p$ como

$$\sigma_b\tau_s|a\rangle = e^{\frac{2\pi i}{p}(sa)}|a+b\rangle \quad (a \in \mathbb{F}_p). \quad (6)$$

O conjunto

$$\mathcal{E}_1 = \{e^{(\frac{2\pi i}{p})m}\sigma_b\tau_s | m, b, s \in \mathbb{F}_p\} \quad (7)$$

forma um grupo de erro (não abeliano) [6]. Um erro computacional em n qbits é um operador linear unitário em $(\mathbb{C}^p)^{\otimes n}$

$$\xi = e^{(\frac{2\pi i}{p})m}\omega_1 \otimes \ldots \otimes \omega_n \quad (\omega_j = \sigma_{b_j}\tau_{s_j}; m, b_j, s_j \in \mathbb{F}_p), \quad (8)$$

o qual age na base

$$\{|a_1 \ldots a_n\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \ldots \otimes |a_n\rangle : (a_1, \ldots, a_n) \in \mathbb{F}_p^n\} \quad (9)$$

de $(\mathbb{C}^p)^{\otimes n}$ como

$$\begin{aligned} \xi|a_1 \ldots a_n\rangle &= e^{(\frac{2\pi i}{p})m}.(\omega_1|a_1\rangle) \otimes \ldots \otimes (\omega_n|a_n\rangle) \\ &= e^{(\frac{2\pi i}{p})m}.e^{(\frac{2\pi i}{p})[(s)^T.(a)]}|a+b\rangle. \end{aligned} \quad (10)$$

em que $s = (s_1, \ldots, s_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_p^n$.

O conjunto de todos os erros ξ de (8) forma um grupo de erro $\mathcal{E}_n$.

Para ξ da forma (8), pode-se encontrar $\mathcal{E} \subset Y$, $\mathcal{I} = Y \setminus \mathcal{E}$, tal que

$$\begin{aligned} \xi|d^Y\rangle &= \xi|d^{\mathcal{E}}, d^{\mathcal{I}}\rangle = e^{(\frac{2\pi i}{p})m}.e^{(\frac{2\pi i}{p})[(s^{\mathcal{E}})^T.(d^{\mathcal{E}})]}|d^{\mathcal{E}} + b^{\mathcal{E}}, d^{\mathcal{I}}\rangle \\ &\quad (m, s^{\mathcal{E}}, b^{\mathcal{E}} \in \mathbb{F}_p^{\mathcal{E}}). \end{aligned} \quad (11)$$

Quando o estado $|\psi\rangle$ da Eq. (4) sofrer um erro especificado por (8), este estado passa a ser descrito da seguinte maneira:

$$\begin{aligned} |\varphi\rangle = \xi|\psi\rangle &= \sum_{d^Y \in \mathbb{F}_p^{|Y|}} \lambda(d^Y)\xi|d^Y\rangle \\ &= \sum_{d^Y \in \mathbb{F}_p^{|Y|}} \lambda(d^{\mathcal{E}}, d^{\mathcal{I}}).\xi.|d^{\mathcal{E}}, d^{\mathcal{I}}\rangle \\ &= \sum_{d^Y \in \mathbb{F}_p^{|Y|}} \lambda(d^{\mathcal{E}}, d^{\mathcal{I}}).e^{(\frac{2\pi i}{p})m}.e^{(\frac{2\pi i}{p})[(s^{\mathcal{E}})^T.(d^{\mathcal{E}})]} \\ &\quad .|d^{\mathcal{E}} + b^{\mathcal{E}}, d^{\mathcal{I}}\rangle \\ &= \sum_{d^Y \in \mathbb{F}_p^{|Y|}} \lambda(d^{\mathcal{E}} - b^{\mathcal{E}}, d^{\mathcal{I}}).e^{(\frac{2\pi i}{p})m} \\ &\quad .e^{(\frac{2\pi i}{p})[(s^{\mathcal{E}})^T.(d^{\mathcal{E}} - b^{\mathcal{E}})]}.|d^{\mathcal{E}}, d^{\mathcal{I}}\rangle \end{aligned} \quad (12)$$

em que

$$\lambda(d^{\mathcal{E}} - b^{\mathcal{E}}, d^{\mathcal{I}}) = \sum_{d^X \in \mathbb{F}_p^{|X|}} e^{(\frac{2\pi i}{p})[\eta]}.c(d^X) \quad (13)$$

e

$$\eta = \frac{1}{2}\Big[(d^X)^T, (d^{\mathcal{E}} - b^{\mathcal{E}})^T, (d^{\mathcal{I}})^T\Big].\Gamma.\left[\begin{array}{c} d^X \\ d^{\mathcal{E}} - b^{\mathcal{E}} \\ d^{\mathcal{I}} \end{array}\right]. \quad (14)$$

A matriz Γ em (14) tem a seguinte forma:

$$\Gamma = \left[\begin{array}{ccc} \Gamma_{X,X} & \Gamma_{X,\mathcal{E}} & \Gamma_{X,\mathcal{I}} \\ \Gamma_{\mathcal{E},X} & \Gamma_{\mathcal{E},\mathcal{E}} & \Gamma_{\mathcal{E},\mathcal{I}} \\ \Gamma_{\mathcal{I},X} & \Gamma_{\mathcal{I},\mathcal{E}} & \Gamma_{\mathcal{I},\mathcal{I}} \end{array}\right]. \quad (15)$$

Ao substituir a matriz (15) em (14) e realizando algumas manipulações algébricas, tomando que as submatrizes $\Gamma_{X,X} = 0$, $\Gamma_{X\mathcal{E}} = (\Gamma_{\mathcal{E},X})^T$, $\Gamma_{X,\mathcal{I}} = (\Gamma_{\mathcal{I},X})^T$ e $\Gamma_{\mathcal{E},\mathcal{I}} = (\Gamma_{\mathcal{I},\mathcal{E}})^T$ (Definição 2.1), obtém-se que

$$\begin{aligned} \eta(j) &= (d^X)^T\Gamma_{X,\mathcal{E}}(d^{\mathcal{E}}) - (d^X)^T\Gamma_{X,\mathcal{E}}(b^{\mathcal{E}}) \\ &\quad +(d^X)^T\Gamma_{X,\mathcal{I}}(d^{\mathcal{I}}) + (d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}}) \\ &\quad -(b^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}}) + \frac{1}{2}(d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}) \\ &\quad -\frac{1}{2}(d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}}) - \frac{1}{2}(b^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}) \\ &\quad +\frac{1}{2}(b^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}}) + \frac{1}{2}(d^{\mathcal{I}})^T\Gamma_{\mathcal{I},\mathcal{I}}(d^{\mathcal{I}}). \end{aligned} \quad (16)$$

É importante notar que em (12) o elemento responsável pelo erro de troca de bit $b^{\mathcal{E}}$ é agora representado na forma exponencial em $\lambda(d^{\mathcal{E}} - b^{\mathcal{E}}, d^{\mathcal{I}})$ - veja (13) e (14). Portanto, os elementos que representam os erros de troca de bit e troca de fase estão todos na forma exponencial.

IV. Operação de Decodificação

Com base no operador de codificação (1) e nas condições que um grafo deve satisfazer para corrigir e erros [7] foi desenvolvido uma operação de decodificação que faz uso de uma transformada de Fourier quântica inversa (TFQI) que foi adaptada aqui para os CGQ.

A operação de decodificação de um CGQ é baseada em uma extensão apropriada do grafo de codificação pela adição de vértices síndromes L e arestas conectando esses vértices com os vértices de saída Y de um modo apropriado [7]. Os vértices síndromes L são vértices de medidas usados para estabelecer a síndrome. O conjunto de grafos corretores de e erros com vértices de entrada X, vértices de saída Y e vértices de síndrome L devem satisfazer as condições de admissibilidade estabelecidas por Schlingemann [7], dadas a seguir.

Definição 4.1: [7] O conjunto de grafos corretores de e erros $\mathcal{G}_e(X, Y, L)$ é definido como sendo composto por todos os grafos na união dos vértices de entrada X, de saída Y e de síndrome L para os quais a matriz de adjacência $\hat{\Gamma} = \hat{\Gamma}_{i,j}$, em que $i, j \in X \cup Y \cup L$, satisfazem as seguintes condições:

- (c1) A matriz bloco $\hat{\Gamma}_{Y,X\cup L}$ é inversível com inversa $\check{\Gamma}_{X\cup L,Y}$;
- (c2) Não existem arestas que conectem vértices de entrada com vértices síndrome, isto é, $\Gamma_{X,L} = 0$ e $\Gamma_{L,X} = 0$;
- (c3) Para todos os conjuntos $\mathcal{E} \subset Y$ que contém no máximo $2e$ elementos, a condição

$$\Gamma_{Y\setminus\mathcal{E},X\cup\mathcal{E}} d^{X\cup\mathcal{E}} = 0 \text{ implica } d^X = 0 \text{ e } \Gamma_{X,\mathcal{E}} d^{\mathcal{E}} = 0 \quad (17)$$

é satisfeita.

Os vértices síndromes L são vistos como qbits que são medidos para fixar a síndrome de erro. A síndrome de erro é o resultado da medição que permite saber qual(ais) erro(s) ocorreu(am) e que correção tem-se que realizar.

Considere que $|\varphi\rangle$ seja o estado obtido após $|\psi\rangle$ ter sofrido a ocorrência de erros computacionais, i.e., $|\varphi\rangle = \xi\,|\psi\rangle$. Levando em conta um grafo que satisfaça a Definição 4.1, foi desenvolvida uma operação de decodificação para CGQ fazendo uso da TFQI adaptada para CGQ, a qual é dada pelo teorema a seguir.

Teorema 1: Seja $|\varphi\rangle$ o estado obtido ao passar pelo canal quântico, o qual foi originalmente codificado de acordo com a Definição 2.2. Sendo $\mathcal{G}_e(\mathcal{X}, \mathcal{Y}, L)$ um grafo que satisfaça a Definição 4.1 e cuja matriz de adjacência é $\hat{\Gamma}$, então a decodificação para CGQ é obtida pelo operador

$$\mathcal{T}(|\varphi\rangle) = \frac{1}{\sqrt{p^{|Y|}}} \sum_{d^L \in \mathbb{F}_p^{|L|}} \sum_{d^{\hat{X}} \in \mathbb{F}_p^{|X|}} e^{-(\frac{2\pi i}{p})[\mu]} |d^L d^{\hat{X}}\rangle, \quad (18)$$

que é a TFQI adaptada para CGQ, sendo

$$\mu = \frac{1}{2}\left[(d^{\hat{X}})^T, (d^{\mathcal{E}})^T, (d^{\mathcal{I}})^T, (d^L)^T\right] \cdot \hat{\Gamma} \cdot \begin{bmatrix} d^{\hat{X}} \\ d^{\mathcal{E}} \\ d^{\mathcal{I}} \\ d^L \end{bmatrix}. \quad (19)$$

Demonstração: Será mostrado que a TFQI adaptada para códigos grafos quânticos, dada pelo operador $\mathcal{T}$, permite identificar no estado $|\varphi\rangle$ a ocorrência de erros computacionais descritos em (8). Para simplificar a notação, serão omitidos os fatores de normalização.

Considere que o estado $|\psi\rangle$, codificado pela expressão (1), tenha sofrido a ocorrência de erros computacionais, ou seja,

$$\begin{aligned} |\varphi\rangle = \xi\,|\psi\rangle \quad = \quad & \sum_{d^Y \in \mathbb{F}_p^{|Y|}} e^{(\frac{2\pi i}{p})\left[m + (s^{\mathcal{E}})^T \cdot (d^{\mathcal{E}} - b^{\mathcal{E}})\right]} \\ & \cdot \lambda(d^{\mathcal{E}} - b^{\mathcal{E}}, d^{\mathcal{I}}) \cdot |d^{\mathcal{E}}, d^{\mathcal{I}}\rangle. \end{aligned} \quad (20)$$

em que $|Y| = |\mathcal{E}| + |\mathcal{I}|$.

Tendo em vista que o operador $\mathcal{T}$ em (18) é uma TFQI, então pela propriedade de linearidade a operação de decodificação para o estado $|\varphi\rangle$ é dada por

$$\begin{aligned} \mathcal{T}(|\varphi\rangle) \quad = \quad & \sum_{d^Y \in \mathbb{F}_p^{|Y|}} e^{(\frac{2\pi i}{p})\left[m + (s^{\mathcal{E}})^T \cdot (d^{\mathcal{E}} - b^{\mathcal{E}})\right]} \\ & \cdot \lambda(d^{\mathcal{E}} - b^{\mathcal{E}}, d^{\mathcal{I}}) \cdot \mathcal{T}(|d^{\mathcal{E}}, d^{\mathcal{I}}\rangle). \end{aligned} \quad (21)$$

Substituindo em (21) a expressão para $\lambda(d^{\mathcal{E}} - b^{\mathcal{E}}, d^{\mathcal{I}})$ dada em (13), já considerando (16), obtém-se

$$\begin{aligned} \mathcal{T}(|\varphi\rangle) \quad = \quad & \sum_{d^X \in \mathbb{F}_p^{|X|}} \Bigg\{ \sum_{d^Y \in \mathbb{F}_p^{|Y|}} e^{(\frac{2\pi i}{p})\left[m + (s^{\mathcal{E}})^T \cdot (d^{\mathcal{E}} - b^{\mathcal{E}})\right]} \\ & \cdot e^{(\frac{2\pi i}{p})\left[(d^X)^T \Gamma_{X,\mathcal{E}}(d^{\mathcal{E}}) - (d^X)^T \Gamma_{X,\mathcal{E}}(b^{\mathcal{E}})\right.} \\ & + (d^X)^T \Gamma_{X,\mathcal{I}}(d^{\mathcal{I}}) + (d^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}}) \\ & - (b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}}) + \tfrac{1}{2}(d^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}) \\ & - \tfrac{1}{2}(d^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}}) - \tfrac{1}{2}(b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}) \\ & \left. + \tfrac{1}{2}(b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}}) + \tfrac{1}{2}(d^{\mathcal{I}})^T \Gamma_{\mathcal{I},\mathcal{I}}(d^{\mathcal{I}})\right] \\ & \cdot \mathcal{T}(|d^{\mathcal{E}}, d^{\mathcal{I}}\rangle)\Bigg\} \cdot c(d^X). \end{aligned} \quad (22)$$

A matriz $\widehat{\Gamma}$ em (19) tem a forma

$$\widehat{\Gamma} = \begin{bmatrix} \Gamma_{X,X} & \Gamma_{X,\mathcal{E}} & \Gamma_{X,\mathcal{I}} & \Gamma_{X,L} \\ \Gamma_{\mathcal{E},X} & \Gamma_{\mathcal{E},\mathcal{E}} & \Gamma_{\mathcal{E},\mathcal{I}} & \Gamma_{\mathcal{E},L} \\ \Gamma_{\mathcal{I},X} & \Gamma_{\mathcal{I},\mathcal{E}} & \Gamma_{\mathcal{I},\mathcal{I}} & \Gamma_{\mathcal{I},L} \\ \Gamma_{L,X} & \Gamma_{L,\mathcal{E}} & \Gamma_{L,\mathcal{I}} & \Gamma_{L,L} \end{bmatrix}. \quad (23)$$

Substituindo (18) em (22) e considerando que as submatrizes $\Gamma_{\mathcal{X},\mathcal{X}} = 0$ e $\Gamma_{L,L} = 0$ (Definição 2.2), $\Gamma_{X,L} = 0$ e $\Gamma_{L,X} = 0$ (condição c2, Definição 4.1), $\Gamma_{X,\mathcal{E}} = (\Gamma_{\mathcal{E},X})^T$, $\Gamma_{X,\mathcal{I}} = (\Gamma_{\mathcal{I},X})^T$, $\Gamma_{\mathcal{E},\mathcal{I}} = (\Gamma_{\mathcal{I},\mathcal{E}})^T$, $\Gamma_{\mathcal{E},L} = (\Gamma_{L,\mathcal{E}})^T$ e $\Gamma_{\mathcal{I},L} = (\Gamma_{L,\mathcal{I}})^T$, após realizar algumas manipulações é obtido

$$\begin{aligned} \mathcal{T}(|\varphi\rangle) \quad = \quad & \sum_{d^X \in \mathbb{F}_p^{|X|}} \Bigg\{ \sum_{d^Y \in \mathbb{F}_p^{|Y|}} e^{(\frac{2\pi i}{p})\left[m + (s^{\mathcal{E}})^T \cdot (d^{\mathcal{E}} - b^{\mathcal{E}})\right]} \\ & \cdot e^{(\frac{2\pi i}{p})\left[(d^X)^T \Gamma_{X,\mathcal{E}}(d^{\mathcal{E}}) - (d^X)^T \Gamma_{X,\mathcal{E}}(b^{\mathcal{E}})\right.} \\ & + (d^X)^T \Gamma_{X,\mathcal{I}}(d^{\mathcal{I}}) - (b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}}) \\ & - \tfrac{1}{2}(d^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}}) - \tfrac{1}{2}(b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}) \\ & \left. + \tfrac{1}{2}(b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}})\right] \\ & \cdot \Bigg(\sum_{d^L \in \mathbb{F}_p^{|L|}} \sum_{d^{\hat{X}} \in \mathbb{F}_p^{|X|}} e^{-(\frac{2\pi i}{p})\left[+(d^{\hat{X}})^T \Gamma_{X\mathcal{E}}(d^{\mathcal{E}})\right.} \\ & + (d^{\hat{X}})^T \Gamma_{X,\mathcal{I}}(d^{\mathcal{I}}) + (d^{\mathcal{E}})^T \Gamma_{\mathcal{E},L}(d^L) \\ & \left. + (b^{\mathcal{I}})^T \Gamma_{\mathcal{I},L}(d^L)\right] |d^L d^{\hat{X}}\rangle \Bigg)\Bigg\} \cdot c(d^X). \end{aligned} \quad (24)$$

Nota-se que na expressão (24) as duas primeiras exponenciais representam os erros de troca de fase e de troca de bit, respectivamente, enquanto que a expressão entre colchetes é a TFQI.

Para cada estado da base de $|\varphi\rangle$ a TFQI resultará em $p^{|Y|}$ estados $|d^L d^{\hat{X}}\rangle$ ($|Y| = |L|+|X|$). Combinando o resultado da TFQI com o resultado das duas primeiras exponenciais para os $p^{|Y|}$ estados da base de $|\varphi\rangle$, resultará na permanência de apenas um estado $|d^L d^{\hat{X}}\rangle$ que para cada $c(d^X)$. Tendo que d^L é o conjunto dos qbits de medição e que eles serão os mesmos para todos os $c(d^X)$, então realizando a medição deles na base computacional se pode verificar na tabela síndromes qual operação de correção deve ser executada a fim de restaurar o estado originalmente codificado. ■

V. EXEMPLO

Para ilustrar como é a realização da operação de decodificação, nesta seção será considerado um exemplo simples em que o código [[5,1,3]] é codificado via um grafo 3-regular para proteger a informação contra um erro computacional.

Para o código $[[5, 1, 3]]$ tem-se que $n = 5$, $k = 1$ e $d = 3$. Pela Definição 2.1, tem-se as cardinalidade $|X| = 1$ e $|Y| = 5$, respectivamente. Um dos grafos que representam esse código é o grafo 3-regular mostrado na Figura 1 [3].

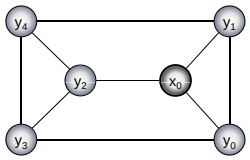

Fig. 1. Representação geométrica de um grafo para o código [[5, 1, 3]].

A matriz de adjacência correspondente ao grafo da Figura 1 é

$$\Gamma = \left(\begin{array}{c|c} \Gamma_{X,X} & \Gamma_{X,Y} \\ \hline \Gamma_{Y,X} & \Gamma_{Y,Y} \end{array}\right) = \begin{array}{c} \\ x_0 \\ y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccccc} x_0 & y_0 & y_1 & y_2 & y_3 & y_4 \end{array} \\ \left(\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \end{array}. \tag{25}$$

Será considerado aqui o corpo $\mathbb{F}_2 = \{0, 1\}$ e que x_0 rotula o vértice de entrada e os vértices restantes rotulam os vértices de saída, isto é, y_0, y_1, y_2, y_3 e y_4 (veja Figura 1). Dessa maneira, $d^X = (d^{x_0}) \in \mathbb{F}_2$ e $d^Y = (d^{y_0}, d^{y_1}, d^{y_2}, d^{y_3}, d^{y_4}) \in \mathbb{F}_2^5$.

Assim, de acordo com a Definição 2.2, a operação de codificação para este grafo é dada como segue (para simplificar a notação, os fatores de normalização serão omitidos).

$$\begin{aligned} f(|v\rangle) \quad = \quad & \sum_{d^{x_0}=0}^{1} \Bigg(\sum_{d^{y_0}=0}^{1} \sum_{d^{y_1}=0}^{1} \sum_{d^{y_2}=0}^{1} \sum_{d^{y_3}=0}^{1} \sum_{d^{y_4}=0}^{1} \\ & e^{(\pi i)\left\{ \frac{1}{2}\left[(d^{x_0})^T, (d^{y_0}, d^{y_1}, d^{y_2}, d^{y_3}, d^{y_4})^T\right] \cdot \Gamma \cdot \left[\begin{array}{c} d^{x_0} \\ d^{y_1} \\ d^{y_2} \\ d^{y_3} \\ d^{y_4} \end{array}\right] \right\}} \\ & |d^{y_0} d^{y_1} d^{y_2} d^{y_3} d^{y_4}\rangle \Bigg) c(d^{x_0}). \end{aligned} \tag{26}$$

em que $|v\rangle = \sum_{d^{x_0}=0}^{1} c(d^{x_0})|d^{x_0}\rangle = c(0)|0\rangle + c(1)|1\rangle$.

Dessa forma, após a codificação, tem-se

$$\begin{aligned} |\psi\rangle \quad = \quad & \Big(|00000\rangle + |00001\rangle + |00010\rangle - |00011\rangle + |00100\rangle \\ & -|00101\rangle - |00110\rangle - |00111\rangle + |01000\rangle - |01001\rangle \\ & +|01010\rangle + |01011\rangle + |01100\rangle + |01101\rangle - |01110\rangle \\ & +|01111\rangle + |10000\rangle + |10001\rangle - |10010\rangle + |10011\rangle \\ & +|10100\rangle - |10101\rangle + |10110\rangle + |10111\rangle - |11000\rangle \\ & +|11001\rangle + |11010\rangle + |11011\rangle - |11100\rangle - |11101\rangle \\ & -|11110\rangle + |11111\rangle\Big) c(0) + \Big(|00000\rangle + |00001\rangle \\ & +|00010\rangle - |00011\rangle - |00100\rangle + |00101\rangle + |00110\rangle \\ & +|00111\rangle - |01000\rangle + |01001\rangle - |01010\rangle - |01011\rangle \\ & +|01100\rangle + |01101\rangle - |01110\rangle + |01111\rangle - |10000\rangle \\ & -|10001\rangle + |10010\rangle - |10011\rangle + |10100\rangle - |10101\rangle \\ & +|10110\rangle + |10111\rangle - |11000\rangle + |11001\rangle + |11010\rangle \\ & +|11011\rangle + |11100\rangle + |11101\rangle + |11110\rangle - |11111\rangle\Big) c(1). \end{aligned} \tag{27}$$

Depois desta etapa de codificação, a informação codificada é submetida ao canal quântico.

Considere que um dos qbits sofra alterações causadas pelo ambiente. Pelo fato de $|0\rangle$ e $|1\rangle$ formarem uma base para o qbit, necessita-se somente saber o que aconteceu naqueles dois estados. De maneira geral, o processo de mudanças trazidas pelo ambiente pode ser descrita como

$$\begin{aligned} |e_0\rangle|0\rangle \quad &\rightarrow \quad |\epsilon_0\rangle|0\rangle + |\epsilon_1\rangle|1\rangle, \\ |e_0\rangle|1\rangle \quad &\rightarrow \quad |\epsilon_0'\rangle|0\rangle + |\epsilon_1'\rangle|1\rangle, \end{aligned} \tag{28}$$

em que $|\epsilon_0\rangle, |\epsilon_1\rangle, |\epsilon_0'\rangle$ e $|\epsilon_1'\rangle$ são estados apropriados do ambiente, não necessariamente ortogonal ou normalizado e $|e_0\rangle$ é o estado inicial do ambiente.

Explicitamente, considere a situação em que o estado codificado $|\psi\rangle$ sofra ação do ambiente e cause, por exemplo, troca de bit (*bit-flip*) no qbit 1. Portanto, depois dessas alterações o estado codificado ficará como segue:

$$\begin{aligned} |\varphi\rangle = \xi\,|\psi\rangle \quad = \quad & \Big(|\underline{1}0000\rangle + |\underline{1}0001\rangle + |\underline{1}0010\rangle - |\underline{1}0011\rangle \\ & +|\underline{1}0100\rangle - \ldots - |\underline{0}1110\rangle + |\underline{0}1111\rangle\Big) c(0) \\ & +\Big(|\underline{1}0000\rangle + |\underline{1}0001\rangle + |\underline{1}0010\rangle - |\underline{1}0011\rangle \\ & -|\underline{1}0100\rangle + \ldots + |\underline{0}1110\rangle - |\underline{0}1111\rangle\Big) c(1). \end{aligned} \tag{29}$$

A representação do grafo de decodificação para o estado (29), satisfazendo a Definição 4.1, é como mostrado na Figura 2.

Assim, considerando o grafo da Figura 2, o operador de decodificação para CGQ, neste caso, fica da seguinte maneira (os fatores de normalização são omitidos):

$$\mathcal{T}(|\varphi\rangle) \quad = \quad \sum_{d^{l_0}=0}^{1} \sum_{d^{l_1}=0}^{1} \sum_{d^{l_3}=0}^{1} \sum_{d^{l_4}=0}^{1} \sum_{d^{\hat{x}_0}=0}^{1} e^{-(\pi i)(\theta)} |d^{l_0} d^{l_1} d^{l_3} d^{l_4} d^{\hat{x}_0}\rangle, \tag{30}$$

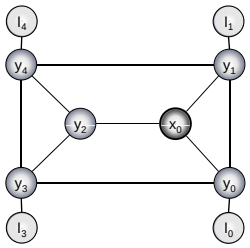

Fig. 2. Grafo 3-regular para o código [[5,1,3]] com os vértices síndrome.

em que $\theta = d^{\hat{x}_0}d^{y_0} + d^{\hat{x}_0}d^{y_1} + d^{\hat{x}_0}d^{y_2} + d^{y_0}d^{y_1} + d^{y_0}d^{y_3} + d^{y_1}d^{y_4} + d^{y_2}d^{y_3} + d^{y_2}d^{y_4} + d^{y_3}d^{y_4} + d^{y_0}d^{l_0} + d^{y_1}d^{l_1} + d^{y_3}d^{l_3} + d^{y_4}d^{l_4}$.

Como o operador $\mathcal{T}$, que é uma TFQI, é uma transformação linear, então ele pode ser aplicado a cada um dos estados da base de $|\varphi\rangle$. Dessa forma, a operação de decodificação fica como segue:

$$\begin{aligned}\mathcal{T}(|\varphi\rangle) \quad = \quad & \Big(\mathcal{T}(|\underline{1}0000\rangle) + \mathcal{T}(|\underline{1}0001\rangle) + \mathcal{T}(|\underline{1}0010\rangle) - \mathcal{T}(|\underline{1}0011\rangle) \\ & + \mathcal{T}(|\underline{1}0100\rangle) - \ldots - \mathcal{T}(|\underline{0}1110\rangle) + \mathcal{T}(|\underline{0}1111\rangle)\Big)c(0) \\ & + \Big(\mathcal{T}(|\underline{1}0000\rangle) + \mathcal{T}(|\underline{1}0001\rangle) + \mathcal{T}(|\underline{1}0010\rangle) - \mathcal{T}(|\underline{1}0011\rangle) \\ & - \mathcal{T}(|\underline{1}0100\rangle) + \ldots + \mathcal{T}(|\underline{0}1110\rangle) - \mathcal{T}(|\underline{0}1111\rangle)\Big)c(1). \end{aligned} \tag{31}$$

Substituindo os resultados obtidos pela aplicação do operador $\mathcal{T}$ a cada um dos estados da base de $|\varphi\rangle$ em (31) (para auxiliar nesse processamento foi usado o software de computação algébrica Maple^{TM}), obtém-se

$$\begin{aligned}\mathcal{T}(|\varphi\rangle) \quad &= \quad |01100\rangle c(0) - |01101\rangle c(1) \\ &= \quad |0\rangle|1\rangle|1\rangle|0\rangle(c(0)|0\rangle - c(1)|1\rangle). \end{aligned} \tag{32}$$

Observe que, de acordo com a expressão (30), os quatro primeiros qbits são de síndromes (medidas). Assim, realizando uma medição nestes qbits síndromes na base computacional se pode verificar na Tabela de Síndromes (Tabela I) qual tipo de ocorrência eles correspondem e, com isso, decidir que ação deve ser realizada no quinto qbit para obter o estado originalmente codificado.

Portanto, consultando a Tabela I, verifica-se que o erro causado é o de troca de bit no qbit 1 e a operação a ser realizada é a troca de sinal (ou troca de fase) no quinto qbit (destacado em negrido).

Do mesmo modo que para a situação apresentada acima, caso o estado $|\psi\rangle$ tivesse sofrido a ação de qualquer outro erro computacional, como apresentados na coluna "Erro" da Tabela I, o operador dado em (30) estaria apto a realizar a decodificação.

VI. Considerações Finais

Neste trabalho foi mostrado como é o operador de decodificação para os códigos grafos quânticos.

Para ilustrar a aplicação deste operador, foi efetuada a decodificação da informação proveniente do código [[5,1,3]] codificada via um grafo 3-regular. Além disso, foi caracterizada a tabela de síndromes gerada para este exemplo.

TABELA I
TABELA DE SÍNDROMES: CÓDIGO DE 5 QBITS VIA GRAFO 3-REGULAR

Qbits síndromes $q_1q_2q_3q_4$	Erro (*)	Estado do qbit q_5	Operação de correção (*)
0000	Nenhum	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0001	S_5	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0010	S_4	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0011	B_3	$c(0)\|0\rangle - c(1)\|1\rangle$	S_5
0100	S_2	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0101	B_4	$c(0)\|1\rangle + c(1)\|0\rangle$	B_5
0110	$\mathbf{B_1}$	$\mathbf{c(0)\|0\rangle - c(1)\|1\rangle}$	$\mathbf{S_5}$
0111	BS_4	$-c(0)\|1\rangle - c(1)\|0\rangle$	SBS_5
1000	S_1	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
1001	B_2	$c(0)\|0\rangle - c(1)\|1\rangle$	S_5
1010	B_5	$c(0)\|1\rangle + c(1)\|0\rangle$	B_5
1011	BS_5	$-c(0)\|1\rangle - c(1)\|0\rangle$	SBS_5
1100	S_3	$c(0)\|1\rangle + c(1)\|0\rangle$	B_5
1101	BS_2	$-c(0)\|0\rangle + c(1)\|1\rangle$	BSB_5
1110	BS_1	$-c(0)\|0\rangle + c(1)\|1\rangle$	BSB_5
1111	BS_3	$-c(0)\|1\rangle + c(1)\|0\rangle$	BS_5

(*) B_n denota troca de bit no n-ésimo qbit;
S_n denota troca de sinal ou troca de fase no n-ésimo qbit;
BS_n denota troca de sinal e bit no n-ésimo qbit;
BSB_5 denota troca de bit, troca de sinal e troca de bit no n-ésimo qbit, respectivamente;
SBS_5 denota troca de sinal, troca de bit e troca de sinal no n-ésimo qbit, respectivamente.

Uma das vantagens do operador de decodificação apresentado é que ele faz uso da TFQI. Tal característica viabiliza a sua implementação em um computador quântico, conforme referências [9], [10].

Referências

[1] E. K. Knill e R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, v. 55, pp. 900–911, 1997.

[2] D. Gottesman, *Stabilizer codes and quantum error correction*, Tese de Doutorado, California Institute of Technology, 1997. Disponível em: quant-ph/9705052.

[3] D. M. Schlingemann e R. F. Werner, "Quantum error-correcting codes associated with graphs," *Phys. Rev. A*, v. 65, p. 012308, 2001.

[4] D. M. Schlingemann, "Stabilizer codes can be realized as graph codes," *Quant. Inf. Comp.*, v. 2 (4), pp. 307–323, 2002. Disponível em: quant-ph/0111080v1.

[5] L. E. Danielsen, "On Self-Dual Quantum Codes, Graphs, and Boolean Functions," *MS. thesis of Informatics*, University of Bergen, Norway, 2005. Disponível em: quant-ph/0503236.

[6] K. Feng, "Quantum Codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ ($p \geq 3$) Exist," *IEEE Trans. on Information Theory*, v. 48, p. 2384–2391, 2002.

[7] D. M. Schlingemann, "Error syndrome calculation for graph codes on a one-way quantum computer: Towards a quantum memory," *J. of Math. Phys.*, v. 45, pp. 4322–4333, 2004.

[8] D. M. Schlingemann, "Cluster states, algorithms and graphs," *Quant. Inf. Comp.*, v. 4, pp. 287–324, 2004. Disponível em: quant-ph/0305170.

[9] M. A. Nielsen e I. R. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[10] L. Hales e S. Hallgren, "An improved quantum Fourier transform algorithm and applications," in *41st Annual Symposium on Foundations of Computer Science*, 2000.