

Código Concatenado para a Correção de Erro e Apagamento Quântico

Gilson Oliveira dos Santos, Francisco Marcos de Assis, Aécio Ferreira de Lima

Resumo— Este trabalho apresenta um código concatenado que possibilita tanto proteção contra erro arbitrário quanto proteção contra a ocorrência de apagamento quântico. Para isso, utiliza-se como código externo um código grafo quântico de cinco qbits, o qual irá realizar proteção contra a ocorrência de um erro arbitrário. Como código interno, utiliza-se uma codificação via estado GHZ de cinco qbits, na proteção contra um apagamento quântico.

Palavras-Chave— Código concatenado, código corretor de erro quântico, apagamento quântico, código grafo quântico, estado GHZ.

Abstract— This paper presents a concatenated code that allows both the protection against arbitrary error and the quantum erasure occurrence. For this, is used as external code a quantum graph code of five-qbit, which will achieve the protection against the occurrence of an arbitrary error. As internal code, is used an encoding of five-qbit GHZ state for protection against a quantum erasure.

Keywords— Concatenated code, quantum error-correcting code, quantum erasure, quantum graph code, GHZ state.

I. INTRODUÇÃO

Sistemas quânticos estão sujeitos à descoerência, que é uma séria limitação para o processamento quântico de informação [1], [2]. Códigos corretores de erros quânticos (CCEQ) permitem neutralizar os efeitos da descoerência.

Knill e Laflamme [5] estabeleceram as condições necessárias e suficientes a serem obedecidas por um CCEQ.

Gottesman [6] estabeleceu o formalismo de estabilizadores que foi utilizado com bastante sucesso na definição de uma ampla classe de códigos quânticos, os códigos estabilizadores.

Grassl e outros [7] consideraram uma situação em que a posição dos qbits errôneos é conhecida, denominando-a modelo de canal de apagamento quântico (QEC - *quantum erasure channel*, em inglês).

Recentemente, Schlingemann e Werner [8] apresentaram uma técnica para construir códigos estabilizadores quânticos por meio de grafos com propriedades específicas, denominados códigos grafos quânticos. Eles também estabeleceram as condições necessárias e suficientes para um grafo gerar um código de correção de erro quântico, adaptadas de Knill e Laflamme [5].

Este trabalho apresenta um código concatenado que possibilita tanto proteção contra um erro arbitrário quanto proteção contra a ocorrência de um apagamento. Para isso,

utiliza-se como código externo um código grafo quântico de cinco qbits, o qual irá realizar proteção contra a ocorrência de um erro arbitrário. Como código interno, utiliza-se uma codificação via estado GHZ de cinco qbits, na proteção contra um apagamento.

O trabalho é organizado como segue. Na seção II serão brevemente apresentadas as ideias de apagamento quântico e estado GHZ. Na seção III mostra-se a construção do código concatenado fazendo uso de um código grafo quântico e de um esquema via estado GHZ. Finalmente, na seção IV faz-se as conclusões a respeito deste trabalho.

II. PRELIMINARES

Usualmente admite-se que o espaço do sistema \mathcal{H}_{sys} seja um produto tensorial de espaços bidimensionais \mathcal{H}_2 (qbits), isto é,

$$\mathcal{H}_{sys} = \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_2. \quad (1)$$

Entretanto, isso é uma aproximação. Por exemplo, átomos usualmente tem muitos níveis que podem ser ocupados, isso é atribuído a uma evolução dinâmica não desejada do sistema [7]. Portanto, o espaço de Hilbert do sistema \mathcal{H}_{sys} é um produto tensorial de espaços multidimensionais com subespaços bidimensionais usados para computação:

$$\mathcal{H}_{sys} = \mathcal{H}_k \otimes \dots \otimes \mathcal{H}_k,$$

$$\mathcal{H}_{comp} = \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_2,$$

em que \mathcal{H}_{comp} é o subespaço de estados computacionais "permitidos". Cada espaço bidimensional \mathcal{H}_2 é um subespaço de \mathcal{H}_k , mas não necessariamente um fator tensorial de \mathcal{H}_k (para simplificar foi assumido que a dimensão de todos os fatores tensoriais são iguais). Consequentemente, o espaço do sistema \mathcal{H}_{sys} somente pode ser decomposto como uma soma direta de subespaços

$$\mathcal{H}_{sys} = \mathcal{H}_{comp} \oplus \mathcal{H}_{comp}^\perp$$

e geralmente não como um produto tensorial. Durante as computações livres de erro o sistema permanece em \mathcal{H}_{comp} . Qualquer população encontrada em \mathcal{H}_{comp}^\perp é uma indicação de erro [7].

O modelo QEC é ilustrado na situação a seguir [9]. Considere um sistema físico constituído por um átomo no qual a informação é corretamente codificada em dois níveis energéticos. Estes níveis constituem o espaço computacional \mathcal{H}_{comp} . Uma transição que leva um estado do sistema para fora

do espaço computacional \mathcal{H}_{comp}^\perp é então chamada transição não-ressonante. A manipulação do sistema se faz através de técnicas, utilizando um laser sintonizado na diferença de energia entre esses dois estados (transição ressonante), que permitem identificar a população dos níveis de trabalho. Se uma transição é sinalizada através da emissão de um fóton, por exemplo, e a medição da população do nível previsto não indica variação, conclui-se que houve uma transição não-ressonante. O estado assim foi levado para fora do espaço computacional. Este fato caracteriza o canal de apagamento quântico.

Para explicitar o que foi exposto acima, considere uma situação de transição de níveis via emissão espontânea, um fenômeno que naturalmente é produzido em sistemas quânticos, que é uma fonte de erro (transição não-ressonante) cuja importância não deve ser desprezada. Pode-se medir a população nesses níveis, por exemplo, pela aplicação de técnicas de salto quântico (*quantum-jump*, em inglês). Além disso, tem-se que, apesar das transições estimuladas serem mais frequentes que as espontâneas na faixa de microondas (frequência $\nu \sim 2 \times 10^{10} Hz$), as transições espontâneas são bem mais frequentes que as estimuladas no domínio óptico (frequência $\nu \sim 6 \times 10^{14} Hz$) [10]. Deve-se observar que a óptica é atualmente o domínio para comunicação quântica, o que torna a ocorrência de apagamento bastante relevante para esse tipo de comunicação.

Se há a possibilidade de detecção de apagamento, então não é necessário fazer uso de um código que proteja contra erros arbitrários para realizar a correção de erros ocorridos no canal de apagamento. Para tal, pode-se usar um código que realize a proteção somente contra apagamento [1], [7]. Levando em conta isso e o que foi exposto acima, considera-se aqui um código concatenado em que a codificação e a decodificação internas sejam para proteção contra apagamento.

Em geral, corrupção de informação não é *a priori* óbvia para o observador, que deve codificar a informação de modo especial para detectar tal corrupção. Uma forma que pode ser explorada para realizar essa codificação é o uso de estado Greenberger-Horne-Zeilinger (GHZ) [11], [12], [13]. O estado GHZ é um estado maximamente emaranhado de três qbits [11]. Mas, apesar do estado GHZ ter sido idealizado para três qbits, ele pode ser estendido para N-qbits, conforme [13], [15], [16]. Devido a isso, o estado GHZ tem sido útil para muitas aplicações, entre elas a construção de códigos corretores de erros quânticos para sistemas multidimensionais [13].

III. CÓDIGO CONCATENADO PARA A CORREÇÃO DE UM ERRO E UM APAGAMENTO QUÂNTICO

Nesta seção apresenta-se a principal contribuição deste artigo que é a construção de um código quântico concatenado para proteção contra a ocorrência de um erro arbitrário e um apagamento.

Para mostrar como esse esquema de proteção da informação pode ser realizado por concatenação, será considerado como código externo o código quântico [[5,1,3]] obtido via um grafo 3-regular, o qual irá proteger a informação contra um erro arbitrário. Como código interno, para a proteção contra

um apagamento, faz-se uso de um esquema via estado GHZ obtido em [19], devidamente adaptado e estendido para a situação de cinco qbits, já que o mesmo foi apresentado para três qbits.

O código [[5,1,3]], o menor código de Hamming, foi independentemente descoberto por Laflamme e outros [20] e por Bennet e outros [21]. Uma nova prova da existência desse código quântico foi dada por Schlingemann e Werner [8] via códigos grafos, fazendo uso do grafo roda W_6 . Já neste trabalho, será apresentado a obtenção do código quântico [[5,1,3]] via um grafo 3-regular, o qual satisfaz as condições estabelecidas em [8] para um código grafo corretor de erro quântico, conforme mostrado em [22].

Schlingemann [17] estabelece uma relação direta entre códigos grafos e os chamados "estados agrupados" (*cluster states*, em inglês). Esses estados foram introduzidos por Briegel e Raussendorf para desenvolver algoritmos quânticos por meio das medidas locais de von Neumann [23], [24]. Dessa forma, considera-se que um estado agrupado corresponde a um sistema de múltiplos qbits para os quais as posições são rotuladas por vértices do grafo. Cada aresta do grafo pode ser vista como uma interação entre os qbits (vértices) conectados por ela. Um número não nulo (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.

Este trabalho segue a notação dada por Feng [25] para códigos grafos quânticos. \mathbb{F}_p representa um corpo finito com p (primo) elementos.

Definição 1: Considere um mapeamento \mathbb{C} -linear

$$f : (\mathbb{C}^p)^{\otimes k} \rightarrow (\mathbb{C}^p)^{\otimes n}$$

$$|v\rangle \mapsto f(|v\rangle)$$

Um qbit $|v\rangle$ é um vetor não nulo em \mathbb{C}^p , neste caso $k=1$, em que

$$|v\rangle = c_0|0\rangle + c_1|1\rangle + \dots + c_{p-1}|p-1\rangle \quad (c_i \in \mathbb{C}).$$

Um n-qbit é um vetor não nulo em $(\mathbb{C}^p)^{\otimes n} = \mathbb{C}^{p^n}$. Pode-se escolher uma base de \mathbb{C}^{p^n} por

$$\{|a_1 \dots a_n\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \dots \otimes |a_n\rangle : (a_1, \dots, a_n) \in \mathbb{F}_p^n\}. \quad (2)$$

Dessa forma, um k-qbit pode ser expresso como um vetor não nulo

$$|v\rangle = \sum_{a=(a_1, \dots, a_k) \in \mathbb{F}_p^k} c_a |a\rangle = \sum_{(a_1, \dots, a_k) \in \mathbb{F}_p^k} c_{a_1, \dots, a_k} |a_1, \dots, a_k\rangle$$

$$= \sum_{d^X \in \mathbb{F}_p^X} c(d^X) |d^X\rangle \in (\mathbb{C}^p)^{\otimes k}, \text{ sendo } (c_{a_i}, c(d^X)) \in \mathbb{C} \quad (3)$$

e $f(|v\rangle)$ (estado codificado) definido por

$$f(|v\rangle) = \sum_{d^Y \in \mathbb{F}_p^Y} f(d^Y) |d^Y\rangle \in (\mathbb{C}^p)^{\otimes n} \quad (4)$$

em que

$$f(d^Y) \triangleq \sum_{d^X \in \mathbb{F}_2^X} e^{\frac{2\pi i}{p} \left(\frac{1}{2} ((d^X)^t, (d^Y)^t) \cdot A \cdot \begin{pmatrix} d^X \\ d^Y \end{pmatrix} \right)} c(d^X). \quad (5)$$

O conjunto $Q = \{f(|v\rangle) : |v\rangle \in (\mathbb{C}^p)^{\otimes k}\}$ é um código quântico $[[n, k, d]]_p$.

Sejam X e Y dois conjuntos disjuntos representando os qbits de entrada e saída, respectivamente, e $|X| = k$ e $|Y| = n$. Para o código $[[5, 1, 3]]$, tem-se $n = 5$, $k = 1$ e $d = 3$. Assim, $|X| = 1$ e $|Y| = 5$. O grafo 3-regular considerado possui seis vértices, como pode ser visto na Figura 1.

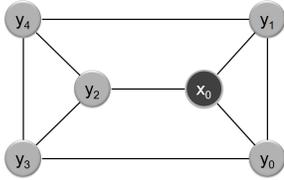


Fig. 1. Uma representação geométrica de um grafo 3-regular para o código $[[5, 1, 3]]$.

Considerando o corpo \mathbb{Z}_2 , este grafo tem matriz

$$A = \left(\begin{array}{c|ccccc} & x_0 & y_0 & y_1 & y_2 & y_3 & y_4 \\ \hline x_0 & 0 & 1 & 1 & 1 & 0 & 0 \\ y_0 & 1 & 0 & 1 & 0 & 1 & 0 \\ y_1 & 1 & 1 & 0 & 0 & 0 & 1 \\ y_2 & 1 & 0 & 0 & 0 & 1 & 1 \\ y_3 & 0 & 1 & 0 & 1 & 0 & 1 \\ y_4 & 0 & 0 & 1 & 1 & 1 & 0 \end{array} \right).$$

Considere o vértice $x_0 \in X$ como vértice de entrada e os cinco vértices restantes como sendo de saída, ou seja, $y_0, y_1, y_2, y_3, y_4 \in Y$ (ver Figura 1). Assim, tem-se que

$$d^X = (x_0); \quad d^Y = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}.$$

Portanto, de acordo com a Definição 1, o código quântico para esse grafo é:

$$|v\rangle = \sum_{x_0 \in \mathbb{F}_2^X} c(x_0) |x_0\rangle, \text{ em que } c(x_0) \in \mathbb{C} \quad (6)$$

é o estado inicial a ser codificado, e

$$f(|v\rangle) = \sum_{(y_0, y_1, y_2, y_3, y_4) \in \mathbb{F}_2^Y} f(d^Y) |y_0 y_1 y_2 y_3 y_4\rangle \quad (7)$$

em que

$$f(d^Y) = \sum_{x_0 \in \mathbb{F}_2^X} e^{\pi i (w)} c(x_0)$$

sendo $w = x_0 y_0 + x_0 y_1 + x_0 y_2 + y_0 y_1 + y_0 y_3 + y_1 y_4 + y_2 y_3 + y_2 y_4 + y_3 y_4$, fornece o estado codificado por meio do grafo utilizado (3-regular).

Tendo os elementos $x_0, y_0, y_1, y_2, y_3, y_4 \in \mathbb{Z}_2 = \{0, 1\}$,

assim o qbit será dado pelo vetor

$$|v\rangle = c(0)|0\rangle + c(1)|1\rangle, \text{ em que } c(0), c(1) \in \mathbb{C}. \quad (8)$$

Substituindo o vetor acima na equação (7), e realizando os cálculos, obtém-se que o estado codificado $f(|v\rangle) = |\psi\rangle_{12345}$ é

$$\begin{aligned} |\psi\rangle_{12345} = & \alpha_0 |00000\rangle + \alpha_1 |00001\rangle + \alpha_2 |00010\rangle + \alpha_3 |00011\rangle \quad (9) \\ & + \alpha_4 |00100\rangle + \alpha_5 |00101\rangle + \alpha_6 |00110\rangle + \alpha_7 |00111\rangle \\ & + \alpha_8 |01000\rangle + \alpha_9 |01001\rangle + \alpha_{10} |01010\rangle + \alpha_{11} |01011\rangle \\ & + \alpha_{12} |01100\rangle + \alpha_{13} |01101\rangle + \alpha_{14} |01110\rangle + \alpha_{15} |01111\rangle \\ & + \alpha_{16} |10000\rangle + \alpha_{17} |10001\rangle + \alpha_{18} |10010\rangle + \alpha_{19} |10011\rangle \\ & + \alpha_{20} |10100\rangle + \alpha_{21} |10101\rangle + \alpha_{22} |10110\rangle + \alpha_{23} |10111\rangle \\ & + \alpha_{24} |11000\rangle + \alpha_{25} |11001\rangle + \alpha_{26} |11010\rangle + \alpha_{27} |11011\rangle \\ & + \alpha_{28} |11100\rangle + \alpha_{29} |11101\rangle + \alpha_{30} |11110\rangle + \alpha_{31} |11111\rangle \end{aligned}$$

em que

$$\begin{aligned} \alpha_0 &= c(0) + c(1); & \alpha_1 &= c(0) + c(1); & \alpha_2 &= c(0) + c(1); \\ \alpha_3 &= -c(0) - c(1); & \alpha_4 &= c(0) - c(1); & \alpha_5 &= -c(0) + c(1); \\ \alpha_6 &= -c(0) + c(1); & \alpha_7 &= -c(0) + c(1); & \alpha_8 &= c(0) - c(1); \\ \alpha_9 &= -c(0) + c(1); & \alpha_{10} &= c(0) - c(1); & \alpha_{11} &= c(0) - c(1); \\ \alpha_{12} &= c(0) + c(1); & \alpha_{13} &= c(0) + c(1); & \alpha_{14} &= -c(0) - c(1); \\ \alpha_{15} &= c(0) + c(1); & \alpha_{16} &= c(0) - c(1); & \alpha_{17} &= c(0) - c(1); \\ \alpha_{18} &= -c(0) + c(1); & \alpha_{19} &= c(0) - c(1); & \alpha_{20} &= c(0) + c(1); \\ \alpha_{21} &= -c(0) - c(1); & \alpha_{22} &= c(0) + c(1); & \alpha_{23} &= c(0) + c(1); \\ \alpha_{24} &= -c(0) - c(1); & \alpha_{25} &= c(0) + c(1); & \alpha_{26} &= c(0) + c(1); \\ \alpha_{27} &= c(0) + c(1); & \alpha_{28} &= -c(0) + c(1); & \alpha_{29} &= -c(0) + c(1); \\ \alpha_{30} &= -c(0) + c(1); & \alpha_{31} &= c(0) - c(1). \end{aligned}$$

Os estados gerados pela codificação acima são ortogonais entre si. Por exemplo, se for considerado $c(0) = 1$ e $c(1) = 0$, obtém-se

$$|v\rangle = |0\rangle$$

e consequentemente $f(|0\rangle) = |0\rangle_{12345}$.

Agora, considerado $c(0) = 0$ e $c(1) = 1$, obtém-se

$$|v\rangle = |1\rangle$$

e consequentemente tem-se que $f(|1\rangle) = |1\rangle_{12345}$.

Depois de realizar os produtos tensoriais e as somas e/ou subtrações para os estados $|0\rangle_{12345}$ e $|1\rangle_{12345}$, verifica-se que

$$\langle 0|1\rangle_{12345} = 0.$$

Deve-se ter em mente que erros arbitrários $\varepsilon = \{\sigma_X, \sigma_Z, \sigma_Y, I\}$ podem ser introduzidos nessa codificação. Assim, para a ocorrência de erros no estado codificado, tem-se

$$\varepsilon |\psi\rangle_{12345} = |\psi'\rangle_{12345}$$

gerando modificações.

Tendo em vista que essa codificação obedece as condições estabelecidas por [8], isso implica que os estados após sofrerem a ocorrência de um erro ε continuam ortogonais.

Para ilustrar, considere a ocorrência de um erro de inversão

de bit no primeiro bit, destacado em **negrito e sublinhado**:

$$\begin{aligned}
 |\psi'\rangle_{12345} = & \alpha_0|\underline{10000}\rangle + \alpha_1|\underline{10001}\rangle + \alpha_2|\underline{10010}\rangle + \alpha_3|\underline{10011}\rangle \quad (10) \\
 & + \alpha_4|\underline{10100}\rangle + \alpha_5|\underline{10101}\rangle + \alpha_6|\underline{10110}\rangle + \alpha_7|\underline{10111}\rangle \\
 & + \alpha_8|\underline{11000}\rangle + \alpha_9|\underline{11001}\rangle + \alpha_{10}|\underline{11010}\rangle + \alpha_{11}|\underline{11011}\rangle \\
 & + \alpha_{12}|\underline{11100}\rangle + \alpha_{13}|\underline{11101}\rangle + \alpha_{14}|\underline{11110}\rangle + \alpha_{15}|\underline{11111}\rangle \\
 & + \alpha_{16}|\underline{00000}\rangle + \alpha_{17}|\underline{00001}\rangle + \alpha_{18}|\underline{00010}\rangle + \alpha_{19}|\underline{00011}\rangle \\
 & + \alpha_{20}|\underline{00100}\rangle + \alpha_{21}|\underline{00101}\rangle + \alpha_{22}|\underline{00110}\rangle + \alpha_{23}|\underline{00111}\rangle \\
 & + \alpha_{24}|\underline{01000}\rangle + \alpha_{25}|\underline{01001}\rangle + \alpha_{26}|\underline{01010}\rangle + \alpha_{27}|\underline{01011}\rangle \\
 & + \alpha_{28}|\underline{01100}\rangle + \alpha_{29}|\underline{01101}\rangle + \alpha_{30}|\underline{01110}\rangle + \alpha_{31}|\underline{01111}\rangle.
 \end{aligned}$$

Note que na ocorrência desse erro as amplitudes $\alpha_i (i = 0, \dots, 31)$ não são alteradas.

Agora, considerando que essa informação codificada (incluindo os erros inseridos) venha a passar por um canal com apagamento, apresenta-se a seguir como protegê-la.

Assim, no esquema a ser utilizado a partir de agora, cada estado lógico é um produto de duas partes gêmeas do estado GHZ (*twin GHZ state*, em inglês) de cinco qbits, sendo uma extensão do esquema relatado em [19]. O código produzido requer cinco qbits auxiliares (formando um total de dez qbits) para a proteção de cinco qbits de informação quântica contra a ocorrência de um apagamento.

Usando cinco qbits auxiliares ($1'2'3'4'5'$), pode-se codificar o estado $|\psi'\rangle_{12345}$, fazendo uso de

$$\mathcal{U}_e(|\psi'\rangle_{12345}|00000\rangle_{1'2'3'4'5'}) = |\psi'\rangle_L \quad (11)$$

em que a operação de codificação é realizada por

$$\begin{aligned}
 \mathcal{U}_e = & C_{5'4'}C_{5'3'}C_{5'2'}C_{5'1'}C_{54}C_{53}C_{52}C_{51} \quad (12) \\
 & H_{5'}H_5C_{55'}C_{44'}C_{33'}C_{22'}C_{11'}
 \end{aligned}$$

Note que os cinco qbits auxiliares $1', 2', 3', 4', 5'$ estão inicialmente no estado $|00000\rangle$. Neste trabalho, toda operação conjunta, como a exposta acima, irá seguir a sequência da direita para a esquerda.

A codificação (12) é realizada por operações CNOT (NOT-Controlada) quântica, em que o primeiro índice de C_{ij} refere-se ao bit de controle e o segundo ao bit alvo, e por transformadas de Hadarmard H_i no qbit i , a qual leva $|0\rangle \rightarrow (|0\rangle + |1\rangle)$ e $|1\rangle \rightarrow (|0\rangle - |1\rangle)$. Assim, depois desta codificação, obtém-se

$$\begin{aligned}
 |\psi'\rangle_L = & \alpha_0|0\rangle_L + \alpha_1|1\rangle_L + \alpha_2|2\rangle_L + \alpha_3|3\rangle_L + \alpha_4|4\rangle_L + \alpha_5|5\rangle_L \quad (13) \\
 & + \alpha_6|6\rangle_L + \alpha_7|7\rangle_L + \alpha_8|8\rangle_L + \alpha_9|9\rangle_L + \alpha_{10}|10\rangle_L + \alpha_{11}|11\rangle_L \\
 & + \alpha_{12}|12\rangle_L + \alpha_{13}|13\rangle_L + \alpha_{14}|14\rangle_L + \alpha_{15}|15\rangle_L + \alpha_{16}|16\rangle_L \\
 & + \alpha_{17}|17\rangle_L + \alpha_{18}|18\rangle_L + \alpha_{19}|19\rangle_L + \alpha_{20}|20\rangle_L + \alpha_{21}|21\rangle_L \\
 & + \alpha_{22}|22\rangle_L + \alpha_{23}|23\rangle_L + \alpha_{24}|24\rangle_L + \alpha_{25}|25\rangle_L + \alpha_{26}|26\rangle_L \\
 & + \alpha_{27}|27\rangle_L + \alpha_{28}|28\rangle_L + \alpha_{29}|29\rangle_L + \alpha_{30}|30\rangle_L + \alpha_{31}|31\rangle_L
 \end{aligned}$$

em que os trinta e dois estados lógicos são

$$\begin{aligned}
 |0\rangle_L &= (|10000\rangle + |\underline{01111}\rangle) \otimes (|10000\rangle + |\underline{01111}\rangle), \\
 |1\rangle_L &= (|10000\rangle - |\underline{01111}\rangle) \otimes (|10000\rangle - |\underline{01111}\rangle), \\
 |2\rangle_L &= (|10010\rangle + |\underline{01101}\rangle) \otimes (|10010\rangle + |\underline{01101}\rangle), \\
 |3\rangle_L &= (|10010\rangle - |\underline{01101}\rangle) \otimes (|10010\rangle - |\underline{01101}\rangle), \\
 |4\rangle_L &= (|10100\rangle + |\underline{01011}\rangle) \otimes (|10100\rangle + |\underline{01011}\rangle), \\
 |5\rangle_L &= (|10100\rangle - |\underline{01011}\rangle) \otimes (|10100\rangle - |\underline{01011}\rangle), \\
 |6\rangle_L &= (|10110\rangle + |\underline{01001}\rangle) \otimes (|10110\rangle + |\underline{01001}\rangle), \\
 |7\rangle_L &= (|10110\rangle - |\underline{01001}\rangle) \otimes (|10110\rangle - |\underline{01001}\rangle), \\
 |8\rangle_L &= (|11000\rangle + |\underline{00111}\rangle) \otimes (|11000\rangle + |\underline{00111}\rangle), \\
 |9\rangle_L &= (|11000\rangle - |\underline{00111}\rangle) \otimes (|11000\rangle - |\underline{00111}\rangle), \\
 |10\rangle_L &= (|11010\rangle + |\underline{00101}\rangle) \otimes (|11010\rangle + |\underline{00101}\rangle), \\
 |11\rangle_L &= (|11010\rangle - |\underline{00101}\rangle) \otimes (|11010\rangle - |\underline{00101}\rangle), \\
 |12\rangle_L &= (|11100\rangle + |\underline{00011}\rangle) \otimes (|11100\rangle + |\underline{00011}\rangle), \\
 |13\rangle_L &= (|11100\rangle - |\underline{00011}\rangle) \otimes (|11100\rangle - |\underline{00011}\rangle),
 \end{aligned}$$

$$\begin{aligned}
 |14\rangle_L &= (|11110\rangle + |\underline{00001}\rangle) \otimes (|11110\rangle + |\underline{00001}\rangle), \\
 |15\rangle_L &= (|11110\rangle - |\underline{00001}\rangle) \otimes (|11110\rangle - |\underline{00001}\rangle), \\
 |16\rangle_L &= (|11111\rangle + |\underline{00000}\rangle) \otimes (|11111\rangle + |\underline{00000}\rangle), \\
 |17\rangle_L &= (|11111\rangle - |\underline{00000}\rangle) \otimes (|11111\rangle - |\underline{00000}\rangle), \\
 |18\rangle_L &= (|11010\rangle + |\underline{00010}\rangle) \otimes (|11010\rangle + |\underline{00010}\rangle), \\
 |19\rangle_L &= (|11010\rangle - |\underline{00010}\rangle) \otimes (|11010\rangle - |\underline{00010}\rangle), \\
 |20\rangle_L &= (|11011\rangle + |\underline{00001}\rangle) \otimes (|11011\rangle + |\underline{00001}\rangle), \\
 |21\rangle_L &= (|11011\rangle - |\underline{00001}\rangle) \otimes (|11011\rangle - |\underline{00001}\rangle), \\
 |22\rangle_L &= (|11001\rangle + |\underline{00010}\rangle) \otimes (|11001\rangle + |\underline{00010}\rangle), \\
 |23\rangle_L &= (|11001\rangle - |\underline{00010}\rangle) \otimes (|11001\rangle - |\underline{00010}\rangle), \\
 |24\rangle_L &= (|11000\rangle + |\underline{00011}\rangle) \otimes (|11000\rangle + |\underline{00011}\rangle), \\
 |25\rangle_L &= (|11000\rangle - |\underline{00011}\rangle) \otimes (|11000\rangle - |\underline{00011}\rangle), \\
 |26\rangle_L &= (|10101\rangle + |\underline{01010}\rangle) \otimes (|10101\rangle + |\underline{01010}\rangle), \\
 |27\rangle_L &= (|10101\rangle - |\underline{01010}\rangle) \otimes (|10101\rangle - |\underline{01010}\rangle), \\
 |28\rangle_L &= (|10110\rangle + |\underline{01001}\rangle) \otimes (|10110\rangle + |\underline{01001}\rangle), \\
 |29\rangle_L &= (|10110\rangle - |\underline{01001}\rangle) \otimes (|10110\rangle - |\underline{01001}\rangle), \\
 |30\rangle_L &= (|10111\rangle + |\underline{01000}\rangle) \otimes (|10111\rangle + |\underline{01000}\rangle), \\
 |31\rangle_L &= (|10111\rangle - |\underline{01000}\rangle) \otimes (|10111\rangle - |\underline{01000}\rangle).
 \end{aligned}$$

Note que, para todos os estados lógicos, a parte esquerda do produto corresponde aos cinco qbits da mensagem, enquanto que a parte direita do produto corresponde aos cinco qbits auxiliares e a sequência do arranjo dos dez qbits é $1, 2, 3, 4, 5, 1', 2', 3', 4', 5'$ da esquerda para a direita. Para simplificar a notação, fatores de normalização serão omitidos aqui e no resto deste trabalho.

Considere o caso no qual o qbit 1 sofreu descoerência. Devido a $|0\rangle$ e $|1\rangle$ formarem uma base para o qbit 1, é preciso somente saber o que aconteceu naqueles dois estados. Em geral, o processo de descoerência deve ser

$$|e_0\rangle|0\rangle \rightarrow |e_0\rangle|0\rangle + |\epsilon_1\rangle|1\rangle, \quad (14)$$

$$|e_0\rangle|1\rangle \rightarrow |\epsilon'_0\rangle|0\rangle + |\epsilon'_1\rangle|1\rangle,$$

em que $|e_0\rangle, |\epsilon_1\rangle, |\epsilon'_0\rangle$ e $|\epsilon'_1\rangle$ são estados apropriados do ambiente, não necessariamente ortogonais ou normalizados e $|e_0\rangle$ é o estado inicial do ambiente. Será mostrado a seguir, que durante a operação de restauração não existe a necessidade de realizar quaisquer operações no qbit 1. Para simplificar, a equação (14) será reescrita como

$$|e_0\rangle|0\rangle \rightarrow |\tilde{0}\rangle, \quad (15)$$

$$|e_0\rangle|1\rangle \rightarrow |\tilde{1}\rangle,$$

em que os estados do ambiente acima $|\epsilon_0\rangle, |\epsilon_1\rangle, |\epsilon'_0\rangle$ e $|\epsilon'_1\rangle$ estão incluídos em $|\tilde{0}\rangle$ e $|\tilde{1}\rangle$. Será visto agora o que ocorrerá ao estado codificado $|\psi'\rangle_L$. Depois da descoerência, ele ficará da seguinte forma

$$\begin{aligned}
 |\psi'\rangle_L \otimes |e_0\rangle = & \alpha_0|\tilde{0}\rangle_L + \alpha_1|\tilde{1}\rangle_L + \alpha_2|\tilde{2}\rangle_L + \alpha_3|\tilde{3}\rangle_L + \alpha_4|\tilde{4}\rangle_L \quad (16) \\
 & + \alpha_5|\tilde{5}\rangle_L + \alpha_6|\tilde{6}\rangle_L + \alpha_7|\tilde{7}\rangle_L + \alpha_8|\tilde{8}\rangle_L + \alpha_9|\tilde{9}\rangle_L \\
 & + \alpha_{10}|\tilde{10}\rangle_L + \alpha_{11}|\tilde{11}\rangle_L + \alpha_{12}|\tilde{12}\rangle_L + \alpha_{13}|\tilde{13}\rangle_L \\
 & + \alpha_{14}|\tilde{14}\rangle_L + \alpha_{15}|\tilde{15}\rangle_L + \alpha_{16}|\tilde{16}\rangle_L + \alpha_{17}|\tilde{17}\rangle_L \\
 & + \alpha_{18}|\tilde{18}\rangle_L + \alpha_{19}|\tilde{19}\rangle_L + \alpha_{20}|\tilde{20}\rangle_L + \alpha_{21}|\tilde{21}\rangle_L \\
 & + \alpha_{22}|\tilde{22}\rangle_L + \alpha_{23}|\tilde{23}\rangle_L + \alpha_{24}|\tilde{24}\rangle_L + \alpha_{25}|\tilde{25}\rangle_L \\
 & + \alpha_{26}|\tilde{26}\rangle_L + \alpha_{27}|\tilde{27}\rangle_L + \alpha_{28}|\tilde{28}\rangle_L + \alpha_{29}|\tilde{29}\rangle_L \\
 & + \alpha_{30}|\tilde{30}\rangle_L + \alpha_{31}|\tilde{31}\rangle_L
 \end{aligned}$$

em que

$$\begin{aligned}
 |\tilde{0}\rangle_L &= (|\tilde{10000}\rangle + |\tilde{01111}\rangle) \otimes (|10000\rangle + |\underline{01111}\rangle), \\
 |\tilde{1}\rangle_L &= (|\tilde{10000}\rangle - |\tilde{01111}\rangle) \otimes (|10000\rangle - |\underline{01111}\rangle), \\
 |\tilde{2}\rangle_L &= (|\tilde{10010}\rangle + |\tilde{01101}\rangle) \otimes (|10010\rangle + |\underline{01101}\rangle), \\
 |\tilde{3}\rangle_L &= (|\tilde{10010}\rangle - |\tilde{01101}\rangle) \otimes (|10010\rangle - |\underline{01101}\rangle), \\
 |\tilde{4}\rangle_L &= (|\tilde{10100}\rangle + |\tilde{01011}\rangle) \otimes (|10100\rangle + |\underline{01011}\rangle), \\
 |\tilde{5}\rangle_L &= (|\tilde{10100}\rangle - |\tilde{01011}\rangle) \otimes (|10100\rangle - |\underline{01011}\rangle), \\
 |\tilde{6}\rangle_L &= (|\tilde{10110}\rangle + |\tilde{01001}\rangle) \otimes (|10110\rangle + |\underline{01001}\rangle), \\
 |\tilde{7}\rangle_L &= (|\tilde{10110}\rangle - |\tilde{01001}\rangle) \otimes (|10110\rangle - |\underline{01001}\rangle),
 \end{aligned}$$

$$\begin{aligned}
 |8\rangle_L &= (|\bar{1}1000\rangle + |\bar{0}0111\rangle) \otimes (|11000\rangle + |00111\rangle), \\
 |9\rangle_L &= (|\bar{1}1000\rangle - |\bar{0}0111\rangle) \otimes (|11000\rangle - |00111\rangle), \\
 |10\rangle_L &= (|\bar{1}1010\rangle + |\bar{0}0101\rangle) \otimes (|11010\rangle + |00101\rangle), \\
 |11\rangle_L &= (|\bar{1}1010\rangle - |\bar{0}0101\rangle) \otimes (|11010\rangle - |00101\rangle), \\
 |12\rangle_L &= (|\bar{1}1100\rangle + |\bar{0}0011\rangle) \otimes (|11100\rangle + |00011\rangle), \\
 |13\rangle_L &= (|\bar{1}1100\rangle - |\bar{0}0011\rangle) \otimes (|11100\rangle - |00011\rangle), \\
 |14\rangle_L &= (|\bar{1}1110\rangle + |\bar{0}0001\rangle) \otimes (|11110\rangle + |00001\rangle), \\
 |15\rangle_L &= (|\bar{1}1110\rangle - |\bar{0}0001\rangle) \otimes (|11110\rangle - |00001\rangle), \\
 |16\rangle_L &= (|\bar{0}0000\rangle + |\bar{1}1111\rangle) \otimes (|\bar{0}0000\rangle + |\bar{1}1111\rangle), \\
 |17\rangle_L &= (|\bar{0}0000\rangle - |\bar{1}1111\rangle) \otimes (|\bar{0}0000\rangle - |\bar{1}1111\rangle), \\
 |18\rangle_L &= (|\bar{0}0010\rangle + |\bar{1}1101\rangle) \otimes (|\bar{0}0010\rangle + |\bar{1}1101\rangle), \\
 |19\rangle_L &= (|\bar{0}0010\rangle - |\bar{1}1101\rangle) \otimes (|\bar{0}0010\rangle - |\bar{1}1101\rangle), \\
 |20\rangle_L &= (|\bar{0}0100\rangle + |\bar{1}1011\rangle) \otimes (|\bar{0}0100\rangle + |\bar{1}1011\rangle), \\
 |21\rangle_L &= (|\bar{0}0100\rangle - |\bar{1}1011\rangle) \otimes (|\bar{0}0100\rangle - |\bar{1}1011\rangle), \\
 |22\rangle_L &= (|\bar{0}0110\rangle + |\bar{1}1001\rangle) \otimes (|\bar{0}0110\rangle + |\bar{1}1001\rangle), \\
 |23\rangle_L &= (|\bar{0}0110\rangle - |\bar{1}1001\rangle) \otimes (|\bar{0}0110\rangle - |\bar{1}1001\rangle), \\
 |24\rangle_L &= (|\bar{0}1000\rangle + |\bar{1}0111\rangle) \otimes (|\bar{0}1000\rangle + |\bar{1}0111\rangle), \\
 |25\rangle_L &= (|\bar{0}1000\rangle - |\bar{1}0111\rangle) \otimes (|\bar{0}1000\rangle - |\bar{1}0111\rangle), \\
 |26\rangle_L &= (|\bar{0}1010\rangle + |\bar{1}0101\rangle) \otimes (|\bar{0}1010\rangle + |\bar{1}0101\rangle), \\
 |27\rangle_L &= (|\bar{0}1010\rangle - |\bar{1}0101\rangle) \otimes (|\bar{0}1010\rangle - |\bar{1}0101\rangle), \\
 |28\rangle_L &= (|\bar{0}1100\rangle + |\bar{1}0011\rangle) \otimes (|\bar{0}1100\rangle + |\bar{1}0011\rangle), \\
 |29\rangle_L &= (|\bar{0}1100\rangle - |\bar{1}0011\rangle) \otimes (|\bar{0}1100\rangle - |\bar{1}0011\rangle), \\
 |30\rangle_L &= (|\bar{0}1110\rangle + |\bar{1}0001\rangle) \otimes (|\bar{0}1110\rangle + |\bar{1}0001\rangle), \\
 |31\rangle_L &= (|\bar{0}1110\rangle - |\bar{1}0001\rangle) \otimes (|\bar{0}1110\rangle - |\bar{1}0001\rangle).
 \end{aligned}$$

Comparando os estados lógicos de (16) com os de (13), pode-se notar que para cada estado lógico "ruim" (com apagamento) de (16), a parte direita do produto, que corresponde a codificação dos cinco qbits auxiliares, está intacta.

Depois disso, realiza-se uma transformação unitária nos cinco qbits auxiliares que será considerada como a operação de decodificação parcial (desde que os qbits 1,2,3,4 e 5 não estão envolvidos na operação de decodificação). A operação de decodificação é como segue

$$U_d = H_5 C_{5'4'} C_{5'3'} C_{5'2'} C_{5'1'}. \quad (17)$$

Depois da decodificação, obtém-se

$$\begin{aligned}
 |\bar{0}\rangle_L &= (|\bar{1}0000\rangle + |\bar{0}1111\rangle) \otimes |\bar{1}0000\rangle, \\
 |\bar{1}\rangle_L &= (|\bar{1}0000\rangle - |\bar{0}1111\rangle) \otimes |\bar{1}0001\rangle, \\
 |\bar{2}\rangle_L &= (|\bar{1}0010\rangle + |\bar{0}1101\rangle) \otimes |\bar{1}0010\rangle, \\
 |\bar{3}\rangle_L &= (|\bar{1}0010\rangle - |\bar{0}1101\rangle) \otimes |\bar{1}0011\rangle, \\
 |\bar{4}\rangle_L &= (|\bar{1}0100\rangle + |\bar{0}1011\rangle) \otimes |\bar{1}0100\rangle, \\
 |\bar{5}\rangle_L &= (|\bar{1}0100\rangle - |\bar{0}1011\rangle) \otimes |\bar{1}0101\rangle, \\
 |\bar{6}\rangle_L &= (|\bar{0}0110\rangle + |\bar{1}1001\rangle) \otimes |\bar{0}0110\rangle, \\
 |\bar{7}\rangle_L &= (|\bar{0}0111\rangle + |\bar{1}1000\rangle) \otimes |\bar{0}0111\rangle, \\
 |\bar{8}\rangle_L &= (|\bar{1}1000\rangle + |\bar{0}0111\rangle) \otimes |\bar{1}1000\rangle, \\
 |\bar{9}\rangle_L &= (|\bar{1}1000\rangle - |\bar{0}0111\rangle) \otimes |\bar{1}1001\rangle, \\
 |\bar{10}\rangle_L &= (|\bar{1}1010\rangle + |\bar{0}0101\rangle) \otimes |\bar{1}1010\rangle, \\
 |\bar{11}\rangle_L &= (|\bar{1}1010\rangle - |\bar{0}0101\rangle) \otimes |\bar{1}1011\rangle, \\
 |\bar{12}\rangle_L &= (|\bar{1}1100\rangle + |\bar{0}0011\rangle) \otimes |\bar{1}1100\rangle, \\
 |\bar{13}\rangle_L &= (|\bar{1}1100\rangle - |\bar{0}0011\rangle) \otimes |\bar{1}1101\rangle, \\
 |\bar{14}\rangle_L &= (|\bar{1}1110\rangle + |\bar{0}0001\rangle) \otimes |\bar{1}1110\rangle, \\
 |\bar{15}\rangle_L &= (|\bar{1}1110\rangle - |\bar{0}0001\rangle) \otimes |\bar{1}1111\rangle, \\
 |\bar{16}\rangle_L &= (|\bar{0}0000\rangle + |\bar{1}1111\rangle) \otimes |\bar{0}0000\rangle, \\
 |\bar{17}\rangle_L &= (|\bar{0}0000\rangle - |\bar{1}1111\rangle) \otimes |\bar{0}0001\rangle, \\
 |\bar{18}\rangle_L &= (|\bar{0}0010\rangle + |\bar{1}1101\rangle) \otimes |\bar{0}0010\rangle, \\
 |\bar{19}\rangle_L &= (|\bar{0}0010\rangle - |\bar{1}1101\rangle) \otimes |\bar{0}0011\rangle, \\
 |\bar{20}\rangle_L &= (|\bar{0}0100\rangle + |\bar{1}1011\rangle) \otimes |\bar{0}0100\rangle, \\
 |\bar{21}\rangle_L &= (|\bar{0}0100\rangle - |\bar{1}1011\rangle) \otimes |\bar{0}0101\rangle, \\
 |\bar{22}\rangle_L &= (|\bar{0}0110\rangle + |\bar{1}1001\rangle) \otimes |\bar{0}0110\rangle, \\
 |\bar{23}\rangle_L &= (|\bar{0}0110\rangle - |\bar{1}1001\rangle) \otimes |\bar{0}0111\rangle, \\
 |\bar{24}\rangle_L &= (|\bar{0}1000\rangle + |\bar{1}0111\rangle) \otimes |\bar{0}1000\rangle, \\
 |\bar{25}\rangle_L &= (|\bar{0}1000\rangle - |\bar{1}0111\rangle) \otimes |\bar{0}1001\rangle, \\
 |\bar{26}\rangle_L &= (|\bar{0}1010\rangle + |\bar{1}0101\rangle) \otimes |\bar{0}1010\rangle, \\
 |\bar{27}\rangle_L &= (|\bar{0}1010\rangle - |\bar{1}0101\rangle) \otimes |\bar{0}1011\rangle, \\
 |\bar{28}\rangle_L &= (|\bar{0}1100\rangle + |\bar{1}0011\rangle) \otimes |\bar{0}1100\rangle, \\
 |\bar{29}\rangle_L &= (|\bar{0}1100\rangle - |\bar{1}0011\rangle) \otimes |\bar{0}1101\rangle, \\
 |\bar{30}\rangle_L &= (|\bar{0}1110\rangle + |\bar{1}0001\rangle) \otimes |\bar{0}1110\rangle, \\
 |\bar{31}\rangle_L &= (|\bar{0}1110\rangle - |\bar{1}0001\rangle) \otimes |\bar{0}1111\rangle.
 \end{aligned}$$

O próximo passo é aplicar uma operação de recuperação de erro para extrair o estado (9). Ela pode ser realizada por uma transformação unitária nos qbits 2,3,4,5,1',2',3',4' e 5', a qual é descrita por

$$U_r = T_{1'5'4} Z_{5'4} T_{1'5'4} C_{2'2} C_{3'3'} C_{4'4'} C_{1'2} C_{1'3} C_{1'4} C_{1'5} \quad (18)$$

em que $T_{1'5'4}$ é uma operação de porta Toffoli [1], e $Z_{5'4}$ é uma operação σ_Z de Pauli controlada. Uma operação de porta Toffoli T_{ijk} tem dois bits de controle correspondendo ao primeiro e segundo índice (i, j), e o bit alvo k . Quando os dois bits de controle estão no estado $|11\rangle$, o estado do bit alvo irá mudar, seguindo $|0\rangle \rightarrow |1\rangle$ e $|1\rangle \rightarrow |0\rangle$; enquanto que quando os dois bits de controle estão no estado $|00\rangle$, $|01\rangle$ ou $|10\rangle$, o estado do bit alvo será invariante. A operação σ_Z de Pauli controlada Z_{ij} tem o bit de controle i e bit alvo j , o qual envia o estado do bit alvo $|0\rangle \rightarrow |0\rangle$ e $|1\rangle \rightarrow -|1\rangle$ quando o bit de controle está no estado $|1\rangle$; caso contrário, quando o bit de controle está no estado $|0\rangle$, o estado do bit alvo não muda. Realizando os cálculos, pode-se facilmente verificar que depois da operação U_r , o sistema composto dos dez qbits e o ambiente estarão no estado

$$(|\bar{0}0000\rangle + |\bar{1}1111\rangle) \otimes |\psi'\rangle_{1'2'3'4'5'}, \quad (19)$$

em que

$$\begin{aligned}
 |\psi'\rangle_{1'2'3'4'5'} &= \alpha_0 |\bar{1}0000\rangle + \alpha_1 |\bar{1}0001\rangle + \alpha_2 |\bar{1}0010\rangle + \alpha_3 |\bar{1}0011\rangle \\
 &+ \alpha_4 |\bar{1}0100\rangle + \alpha_5 |\bar{1}0101\rangle + \alpha_6 |\bar{1}0110\rangle + \alpha_7 |\bar{1}0111\rangle \\
 &+ \alpha_8 |\bar{1}1000\rangle + \alpha_9 |\bar{1}1001\rangle + \alpha_{10} |\bar{1}1010\rangle + \alpha_{11} |\bar{1}1011\rangle \\
 &+ \alpha_{12} |\bar{1}1100\rangle + \alpha_{13} |\bar{1}1101\rangle + \alpha_{14} |\bar{1}1110\rangle \\
 &+ \alpha_{15} |\bar{1}1111\rangle + \alpha_{16} |\bar{1}0000\rangle + \alpha_{17} |\bar{1}0001\rangle \\
 &+ \alpha_{18} |\bar{0}0010\rangle + \alpha_{19} |\bar{0}0011\rangle + \alpha_{20} |\bar{0}0100\rangle \\
 &+ \alpha_{21} |\bar{0}0101\rangle + \alpha_{22} |\bar{0}0110\rangle + \alpha_{23} |\bar{0}0111\rangle \\
 &+ \alpha_{24} |\bar{0}1000\rangle + \alpha_{25} |\bar{0}1001\rangle + \alpha_{26} |\bar{0}1010\rangle \\
 &+ \alpha_{27} |\bar{0}1011\rangle + \alpha_{28} |\bar{0}1100\rangle + \alpha_{29} |\bar{0}1101\rangle \\
 &+ \alpha_{30} |\bar{0}1110\rangle + \alpha_{31} |\bar{0}1111\rangle.
 \end{aligned} \quad (20)$$

Das equações (19) e (20), pode-se notar que a operação de restauração anterior é uma operação de desemaranhamento, que faz os cinco qbits 1',2',3',4' e 5' não mais emaranhados com o sistema restante, isto é, os cinco qbits 1,2,3,4,5 e o ambiente. Ainda que os cinco qbits 1,2,3,4, e 5 estejam emaranhados com o ambiente, a informação originalmente carregada pelos qbits 1,2,3,4 e 5, tem sido completamente transferida dentro dos cinco qbits 1',2',3',4' e 5', e o estado (9) é exatamente reconstruído diretamente dos cinco qbits 1',2',3',4' e 5'.

Diretamente se extrai o estado que serviu de entrada na operação de codificação quando o erro ocorre no qbit 2, 3, 4 ou 5. As operações de decodificação e recuperação para o caso do qbit 1' ou 2' ou 3' ou 4' ou 5' sofrer apagamento são similares a essas - veja quadro no Apêndice I.

O exemplo acima demonstra que os erros que são protegidos pelo código externo não são alterados por esse esquema de codificação-decodificação-recuperação (código interno), utilizado para proteger contra a ocorrência de um apagamento.

Assim, uma vez recuperada a informação que passou pelo canal de apagamento, deve-se aplicar o decodificador para o código externo, código grafo quântico, a fim de corrigir a ocorrência de um erro arbitrário e recuperar a informação original.

A operação de decodificação de um código grafo quântico é baseada em uma extensão apropriada do grafo de codificação pela adição de vértices síndromes L e arestas que conectam estes vértices com os vértices de saída Y de uma maneira apropriada [26]. Os vértices síndromes L são vértices de medida usados para estabelecer a síndrome.

A implementação da decodificação para esse código grafo quântico pode ser descrita como um procedimento de quatro operações elementares [26]:

- 1) Os qbits de entrada X , bem como os qbits síndromes L , são individualmente preparados no "estado padrão"(3);
- 2) Um passo elementar inverso da dinâmica discreta (4), o qual corresponde ao grafo de codificação estendido, é realizado;
- 3) Os qbits de saída Y são medidos independentemente na autobase σ_X e os qbits síndromes L são medidos independentemente na autobase σ_Z , que produzem uma medida resultante que é a síndrome de erro;
- 4) Dependendo da síndrome de erro, uma operação unitária local é efetuada, que é a operação de correção final.

Dessa forma, a informação original é recuperada por este código concatenado na ocorrência de um erro arbitrário e um apagamento.

IV. CONCLUSÕES

Neste trabalho foi proposto um código concatenado que protege a informação da ocorrência um erro arbitrário e um apagamento, em que se utilizou como código externo um código grafo quântico de cinco qbits e, como código interno, um esquema de codificação via estados GHZ. Com isso, mostrou-se como codificar um qbit via um grafo 3-regular, gerando o código grafo quântico $[[5,1,3]]$, para proteger contra a ocorrência de um erro arbitrário. Depois, esse código passou por uma codificação via estados GHZ, usando cinco qbits auxiliares, para proteger contra a ocorrência de um apagamento quântico. Ao final, ilustrou-se o esquema de proteção contra apagamento, recuperando o estado codificado - com a permanência do erro ocorrido antes dessa codificação interna, o qual será corrigido pelo código externo.

Além disso, contribuiu-se aqui com a extensão para estados GHZ de cinco qbits do esquema apresentado em [19], incluindo todos os operadores de decodificação e recuperação - ver Apêndice I.

Este trabalho também representa uma contribuição para os códigos grafos quânticos, tendo em vista que o mesmo mostra uma maneira de inserir a proteção contra a ocorrência de um apagamento para esses códigos por meio da concatenação apresentada.

REFERÊNCIAS

[1] M. A. Nielsen. e I. R. Chuang, *Quantum Computation and Quantum Information*. Nova York: Cambridge University Press, 2000.
 [2] D. Bouwmeester; A. K. Ekert; A. Zeilinger, *The Physics of Quantum Information*. Springer, 2000.

[3] W. K Wootters e W. H. Zurek "A single quantum cannot be cloned", *Nature*, vol. 299, pp. 802-803, 1982.
 [4] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, v. 52, pp. 2493-2496. 1995.
 [5] E. K. Knill. e R. Laflamme, "Theory of quantum error-correcting codes", *Phys. Rev. A*, v. 55, pp. 900-911, Fev. 1997.
 [6] D. Gottesman, *Stabilizer codes and quantum error correction*, PhD thesis, California Institute of Technology, 1997, disponível em: quant-ph/9705052.
 [7] M. Grassl; Th. Beth ; T. Pellizzari, "Codes for the quantum erasure channel", *Phys. Rev. A*, vol. 56, no. 1, 1997.
 [8] D. M. Schlingemann e R. F. Werner, "Quantum error-correcting codes associated with graphs", *Phys. Rev. A*, vol. 65, p. 012308, 2001.
 [9] H. Mabuchi e P. Zoller, "Perfect quantum error correction code", *Phys. Rev. Lett.*, vol. 76, 3108. 1996.
 [10] F. Caruso e V. Oguri, *Física Moderna: Origens Clássicas e Fundamentos Quânticos*. Rio de Janeiro: Elsevier, 2006.
 [11] D. M. Greenberger; M. A. Horne; A. Zeilinger, "Bell's Theorem, Quantum Theory, and Conceptions of the Universe", ed. M. Kafatos (*Kluwer, Dordrecht*), 1989.
 [12] J. Pan; D. Bouwmeester; M. Daniell; H. Weinfurter; A. Zeilinger, "Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement", *NATURE*, v. 403, Feb. 2000.
 [13] N. Cerf; S. Massar; S. Pironio, "Greenberger-Horne-Zeilinger paradoxes for many qudits", *Phys. Rev. Lett.*, v. 89, no. 8, Aug. 2002.
 [14] Ming-jun Shi; Chang-liang Ren; Bo Chong; Jiang-feng Du, "GHZ argument for four-qubit entangled states in the presence of white and colored noise", *Phys. Lett. A*, v. 372, pp. 2980-2983, 2008.
 [15] V. Scarani; A. Acin; E. Schenck; M. Aspelmeyer, "Nonlocality of cluster states of qubits", *Phys. Rev. A*, v. 71, 2005.
 [16] J. Lee; S. Lee; M. S. Ki "Greenberger-Horne-Zeilinger nonlocality in arbitrary even dimensions", *Phys. Rev. A*, v. 73, 032316, 2006.
 [17] D. M. Schlingemann, "Logical network implementation for cluster states and graph codes", *Quant. Inf. Comp.*, vol 3, No. 5, pp. 431-449, 2003.
 [18] M. Hein; J. Eisert; H.J. Briegel, "Multiparty entanglement in graph states", *Phys. Rev. A*, vol. 69, 2004.
 [19] C. Yang; S. Chu; S. Han, "A small error-correction code for protecting three-qubit quantum information", *JETP Letters*, v. 79, No. 5, pp. 236-240, 2004.
 [20] R. Laflamme; C. Miquel; J. P. Paz; W. H. Zurek, "Perfect quantum error correction code", *Phys. Rev. Lett.*, vol. 77, pp. 198-201. 1996.
 [21] C. H. Bennet; D. DiVicenzo; J. A. Smolin; W. K. Wootters, "Mixed state entanglement and quantum error correction", *Phys. Rev. A*, v. 54, pp. 3824-3851, 1996.
 [22] G. O. dos Santos, *Uso de Grafos para Construção de Códigos Corretores de Erros Quânticos*. Relatório Técnico de Pesquisa, Programa de Pós-Graduação em Engenharia Elétrica, Univ. Fed. de Campina Grande, Julho 2008.
 [23] H. J. Briegel e R. Raussendorf, "Quantum computing via measurements only", eprint arXiv:quant-ph/0010033, 2000.
 [24] H. J. Briegel e R. Raussendorf, "A one-way quantum computer", *Phys. Rev. Lett.*, vol. 86, no. 22, pp. 5188-5191, 2001.
 [25] K. Feng, "Quantum Codes $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p$ ($p \geq 3$) Exist", *IEEE Trans. on Information Theory*, v. 48, no. 8, Aug. 2002.
 [26] D. Schlingemann, "Error syndrome calculation for graph codes on a one-way quantum computer: Towards a quantum memory", *Journal of Math. Phys.*, vol 45, no. 11, pp. 4322-4333, 2004.

APÊNDICE I

Posição qbit	Operador Decodificação
1, 2, 3, 4, 5	$U_d = H_5' C_5' C_4' C_3' C_2' C_1'$
1', 2', 3', 4', 5'	$U_d = H_5 C_5 C_4 C_3 C_2 C_1$

Posição qbit	Operador Recuperação
1	$U_r = T_{1'5'4} Z_{5'4} T_{1'5'4} C_{2'2} C_{3'3} C_{4'4} C_{1'2} C_{1'3} C_{1'4} C_{1'5}$
2	$U_r = T_{2'5'3} Z_{5'3} T_{2'5'3} C_{1'1} C_{3'3} C_{4'4} C_{2'1} C_{2'3} C_{2'4} C_{2'5}$
3	$U_r = T_{3'5'2} Z_{5'2} T_{3'5'2} C_{1'1} C_{2'2} C_{4'4} C_{3'1} C_{3'2} C_{3'4} C_{3'5}$
4	$U_r = T_{4'5'1} Z_{5'1} T_{4'5'1} C_{1'1} C_{2'2} C_{3'3} C_{4'1} C_{4'2} C_{4'3} C_{4'5}$
5	$U_r = Z_{5'4} C_{1'1} C_{2'2} C_{3'3} C_{4'4}$
1'	$U_r = T_{154'} Z_{54'} T_{154'} C_{22'} C_{33'} C_{44'} C_{12'} C_{13'} C_{14'} C_{15'}$
2'	$U_r = T_{253'} Z_{53'} T_{253'} C_{11'} C_{33'} C_{44'} C_{21'} C_{23'} C_{24'} C_{25'}$
3'	$U_r = T_{352'} Z_{52'} T_{352'} C_{11'} C_{22'} C_{44'} C_{31'} C_{32'} C_{34'} C_{35'}$
4'	$U_r = T_{451'} Z_{51'} T_{451'} C_{11'} C_{22'} C_{33'} C_{41'} C_{42'} C_{43'} C_{45'}$
5'	$U_r = Z_{54'} C_{11'} C_{22'} C_{33'} C_{44'}$