Comparação entre estratégias de correção de erros para sistemas quânticos

Edmar José do Nascimento e Francisco Marcos de Assis

***Resumo*— Neste artigo, é analisado o problema da correção de erros para sistemas quânticos. Após uma introdução ao formalismo quântico para a correção de erros, são comparadas duas estratégias: a decodificação usual por tabela de síndrome e a decodificação usando a treliça quântica de Ollivier e Tillich. A principal contribuição desse artigo é servir como um tutorial que trata especificamente do problema da decodificação para CCEQs. Uma segunda contribuição consiste na modificação da construção usual da treliça quântica a fim de simplificar a sua construção quando ela é usada especificamente para a detecção de erros.**

***Palavras-Chave*— Códigos quânticos, síndrome, treliças quânticas.**

***Abstract*— In this article, we analise the problem of error correction for quantum systems. After a short introduction to quantum error correction formalism, two strategies are compared: the usual syndrome-table decoding and the quantum trellis decoding. The main contribution in this article is to provide a tutorial dealing specifically with decoding issues concerning quantum error correcting codes. The second contribution consists in a modification of the usual construction of quantum trellises in order to simplify it when applied specifically to quantum error detection.**

***Keywords*— Quantum codes, syndrome, quantum trellises.**

I. INTRODUÇÃO

A utilização de sistemas quânticos de modo eficiente na computação e no processamento de informação está condicionada à mitigação ou à eliminação dos efeitos de um fenômeno conhecido como descoerência. A descoerência pode ser vista como uma conseqüência do emaranhamento entre o sistema quântico e o ambiente, causando a perda da informação quântica para o ambiente [1], [2].

Uma das maneiras de minimizar o efeito da descoerência nas aplicações dos sistemas quânticos é através da utilização de Códigos Corretores de Erros Quânticos (CCEQs). Nos sistemas clássicos, os códigos corretores de erros são projetados para proteger a informação de determinados tipos de erros, os quais são representados por um modelo de canal. Analogamente, nos sistemas quânticos, os erros também são modelados por um canal, que pode representar tanto um meio de comunicação físico quanto a passagem do tempo para um conjunto de q-bits interagindo com o ambiente ou até o resultado de uma operação com uma porta quântica ruidosa em um computador quântico [3].

A construção de CCEQs é diferente da construção dos códigos clássicos, pois ela deve levar em conta as restrições impostas pela mecânica quântica. Essas restrições impedem que os resultados obtidos para os códigos clássicos sejam diretamente estendidos para os sistemas quânticos sem uma análise prévia a fim de verificar se as restrições quânticas não estão sendo violadas. Entretanto, apesar dessas particularidades, é possível construir códigos quânticos tomando como ponto de partida a ampla teoria desenvolvida para os códigos clássicos ao longo de décadas de pesquisa. Exemplos de construções que empregam conceitos usados nos códigos clássicos são encontrados nos códigos de Shor e CSS (Calderbank-Shor-Steane). O código de Shor utiliza os conceitos clássicos de repetição e concatenação e é capaz de corrigir um erro arbitrário em um q-bit. Os códigos CSS são construídos a partir de dois códigos clássicos quaisquer que satisfazem determinadas propriedades [2].

Além dos códigos de Shor e CSS, vários resultados importantes merecem destaque, pois constituem a base do que hoje é conhecido como a teoria quântica para a correção de erros [4]. Um dos resultados teóricos de grande importância se deve a Knill e Laflamme, que analisaram as condições necessárias e suficientes para que um determinado CCEQ seja capaz de corrigir um determinado conjunto de erros [5]. Além desse resultado, o formalismo de estabilizadores foi utilizado com bastante sucesso por Gottesman na definição de uma ampla classe de códigos quânticos, os códigos estabilizadores [3]. Recentemente, vários outros códigos clássicos ganharam equivalentes quânticos: códigos BCH [6], códigos convolucionais [7] e códigos LDPC [8].

A correção dos erros para os CCEQs envolve em geral três etapas: medição da síndrome, identificação do erro relacionado à síndrome obtida e correção do erro. Para realizar a medição da síndrome, pode-se construir um circuito quântico a partir do estabilizador do código usando operações quânticas unitárias elementares ou uma versão tolerante a falhas [3]. A identificação do erro ocorrido depende do modelo de canal considerado, pois, dependendo do canal, uma mesma síndrome pode corresponder a vários erros. Finalmente, a etapa de correção do erro consiste em aplicar a operação inversa ao erro identificado. Caso o erro identificado não seja igual ao ocorrido, a operação de correção não é bem sucedida.

Neste artigo, é abordado em detalhes o problema da correção de erros para sistemas quânticos. Após uma introdução ao formalismo quântico para correção de erros, é realizada uma comparação entre duas estratégias de correção. A primeira estratégia consiste na construção de uma tabela de síndromes. Essa estratégia é a maneira mais simples de identificar erros tanto para os códigos clássicos quanto para os códigos quânticos. A segunda consiste na utilização de uma treliça para códigos estabilizadores quânticos definida por

Edmar José do Nascimento, Doutorando em Engenharia Elétrica (Bolsista CNPq), Universidade Federal de Campina Grande, Campina Grande, Brasil, E-mail: ejnascimento@ee.ufcg.edu.br. Francisco Marcos de Assis, Departamento de Engenharia Elétrica, Universidade Federal de Campina Grande, Brasil, E-mail: fmarcos@dee.ufcg.edu.br.

Ollivier e Tillich [9]. Essa segunda abordagem permite utilizar o algoritmo de Viterbi para encontrar o caminho de menor peso (o erro mais provável). É também sugerida pelos autores desse artigo, uma modificação na construção usual da treliça quântica para os casos em que ela é usada especificamente para encontrar o erro mais provável. Essa modificação permite simplificar a construção da treliça, tornando-a mais eficiente a sua utilização para essa finalidade específica.

Este artigo está organizado da seguinte maneira. Na seção II é feita uma revisão sobre os modelos de erros para os sistemas quânticos. Na seção III, são apresentadas algumas definições acerca dos códigos quânticos, bem como alguns resultados úteis a respeito do formalismo dos estabilizadores. Na seção IV, é discutido como é feita a correção de erros por tabela de síndrome para um CCEQ. Finalmente, na seção V, discute-se sobre a construção da treliça quântica de Ollivier e Tillich e é apresentada a construção alternativa proposta pelos autores desse artigo.

II. Caracterização dos Erros

Os erros que atuam sobre os sistemas quânticos são geralmente representados como um conjunto de operadores, em uma representação conhecida como *representação de operador-soma*. Nessa representação, os efeitos da interação do sistema quântico com o ambiente são incorporados em um conjunto de operadores E_k. Se ρ representa o estado do sistema antes da interação, o estado após a interação, ρ_f é dado por:

$$\rho_f \quad = \quad \mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger. \tag{1}$$

Os operadores E_k são lineares no espaço de Hilbert do sistema quântico ρ e são conhecidos como *operadores de erro*.

A representação de operador-soma permite fazer uma analogia com os canais clássicos, resultando em um modelo para canais quânticos ruidosos. Para um conjunto de operadores de erro $\{E_k\}$, o estado do sistema é transformado de

$$\rho \quad \longrightarrow \quad \frac{E_k \rho E_k^\dagger}{tr(E_k \rho E_k^\dagger)} \tag{2}$$

com probabilidade $tr(E_k \rho E_k^\dagger)$.

Um operador de erro arbitrário com elementos complexos pode ser representado em uma base de erros em um procedimento conhecido como discretização do erro. A base escolhida para representar um erro arbitrário que atua sobre um único q-bit é em geral a base formada pelas matrizes de Pauli $(\sigma_0 = I_2, \sigma_x = X, \sigma_y = Y, \sigma_z = Z)$, que são definidas como:

$$\begin{aligned} \sigma_0 \quad &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x \quad = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_y \quad &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \; \sigma_z \quad = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned} \tag{3}$$

Pode-se verificar facilmente que: $\sigma_x = i\sigma_z\sigma_y = -i\sigma_y\sigma_z$, $\sigma_y = i\sigma_x\sigma_z = -i\sigma_z\sigma_x$ e $\sigma_z = -i\sigma_x\sigma_y = i\sigma_y\sigma_x$. Dessa forma, as matrizes de Pauli multiplicadas pelos fatores ± 1 e $\pm i$ formam um grupo sob multiplicação, o *grupo de Pauli* $\mathcal{G}_1$.

As matrizes de Pauli dadas pela equação (3) ou comutam ou anticomutam. Duas matrizes A e B comutam se $[A, B] \equiv AB - BA = 0$ e anticomutam se $\{A, B\} \equiv AB + BA = 0$. Para as matrizes de Pauli tem-se que:

1) $\{\sigma_i, \sigma_j\} = 0 \; (i,j) \in (x,y,z), i \neq j$;
2) $[\sigma_i, \sigma_i] = 0, \; i \in (x,y,z)$;
3) $[\sigma_0, \sigma_i] = 0 \quad , i \in (0,x,y,z)$

A importância das relações de comutação se deve ao fato que duas matrizes que comutam podem ser diagonalizadas simultaneamente.

Para operadores de erro que atuam sobre n q-bits, a base de erro passa a ser dada por todas as combinações de n produtos tensoriais das matrizes de Pauli. De modo similar, produtos tensoriais de matrizes de Pauli multiplicados pelos fatores ± 1 e $\pm i$ formam um grupo sob multiplicação, o grupo de Pauli $\mathcal{G}_n$. Elementos desse grupo também comutam ou anticomutam.

III. Códigos Quânticos

Um CCEQ que codifica k q-bits em n q-bits é definido através de um mapa de codificação ξ do espaço de Hilbert $H_2^{\otimes k}$ para um subespaço $\mathcal{C}_q$ de dimensão 2^k do espaço de Hilbert $H_2^{\otimes n}$ [4]. O subespaço $\mathcal{C}_q$ é chamado de *espaço do código* e os estados pertencentes a ele são chamados de *palavras-código*.

Os sistemas quânticos baseados em q-bits são definidos em relação aos estados da base computacional, identificados pelos vetores $|\delta_j\rangle \; (\delta_j = 0, 1)$, em que $j = 1, \cdots, k$. Na maioria dos casos, a base computacional para um q-bit é escolhida a partir dos auto-estados da matriz Z de Pauli, ou seja:

$$Z_j \left|\delta_j\right\rangle \quad = \quad (-1)^{\delta_j} \left|\delta_j\right\rangle. \tag{4}$$

Para o espaço de Hilbert $H_2^{\otimes k}$, os estados base são obtidos através de todas as combinações possíveis de produtos tensoriais dos estados $|\delta_j\rangle$, ou seja:

$$|\delta\rangle \quad \equiv \quad |\delta_1 \cdots \delta_k\rangle = |\delta_1\rangle \otimes \cdots \otimes |\delta_k\rangle. \tag{5}$$

A operação de codificação $\xi : H_2^k \rightarrow \mathcal{C}_q$ é unitária, de modo que ela estabelece uma correspondência um a um entre a base do espaço H_2^k ($|\delta\rangle$) e a base do código ($\left|\overline{\delta}\right\rangle = \left|\overline{\delta_1 \cdots \delta_k}\right\rangle$). Sendo assim, tem-se:

$$\left|\overline{\delta_1 \cdots \delta_k}\right\rangle \quad = \quad \xi \left|\delta_1 \cdots \delta_k\right\rangle. \tag{6}$$

Os estados $\left|\overline{\delta_1 \cdots \delta_k}\right\rangle$ são chamados de *palavras-código base* ou *estados lógicos*. Qualquer combinação linear desses estados lógicos também é uma palavra-código. O mapa de codificação ξ também codifica operadores que atuam sobre os q-bits da mensagem, resultando em *operadores lógicos* que atuam sobre as palavras do código. Os operadores lógicos de inversão de bit $\overline{X}$ e de inversão de fase $\overline{Z}$ são dados por:

$$\xi: \quad Z_j \quad \rightarrow \quad \overline{Z_j} = \xi Z_j \xi^\dagger, \tag{7}$$

$$\xi: \quad X_j \quad \rightarrow \quad \overline{X_j} = \xi X_j \xi^\dagger. \tag{8}$$

Os efeitos dessas operações podem ser descritos como:

$$\overline{Z}(a\left|\overline{0}\right\rangle + b\left|\overline{1}\right\rangle) \quad \rightarrow \quad (a\left|\overline{0}\right\rangle - b\left|\overline{1}\right\rangle), \tag{9}$$

$$\overline{X}(a\left|\overline{0}\right\rangle + b\left|\overline{1}\right\rangle) \quad \rightarrow \quad (b\left|\overline{0}\right\rangle + a\left|\overline{1}\right\rangle). \tag{10}$$

Uma outra forma de descrever um CCEQ é através do formalismos dos estabilizadores. O *estabilizador* de um código $\mathcal{C}_q$ é um subgrupo abeliano $\mathcal{S}$ de $\mathcal{G}_n$ cujos elementos $S \in \mathcal{S}$ aplicados às palavras do código $|c\rangle \in \mathcal{C}_q$ verificam a relação:

$$S\,|c\rangle \;=\; |c\rangle\,. \tag{11}$$

O estabilizador $\mathcal{S}$ para um CCEQ $[[n,k,d]]$ é construído a partir de um conjunto de $n-k$ operadores $\{g_1,\cdots,g_{n-k}\}$, conhecidos como os geradores de $\mathcal{S}$. Cada elemento $S \in \mathcal{S}$ pode ser escrito como um produto único de potências dos geradores:

$$S \;=\; g_1^{p_1}\cdots g_{n-k}^{p_{n-k}}\,. \tag{12}$$

Devido ao fato de $\mathcal{S}$ ser abeliano, os geradores comutam entre si e além disso, são unitários, hermitianos e de segunda ordem ($g_i^2 = I$). Os elementos de $\mathcal{S}$ podem ser rotulados então por uma cadeia binária p de comprimento $n-k$: $p = p_1\cdots p_{n-k}$. Sendo assim, para cada elemento $S \in \mathcal{S}$ é associada uma cadeia binária $p \in F_2^{n-k}$ (F_2^{n-k} - espaço vetorial binário de dimensão $n-k$). Como existem 2^{n-k} cadeias binárias de comprimento $n-k$, a ordem de $\mathcal{S}$ é $|\mathcal{S}| = 2^{n-k}$.

A *síndrome do erro* para um código definido por um estabilizador $\mathcal{S}$ e um erro arbitrário pertencente ao grupo de Pauli $e \in \mathcal{G}_n$ pode ser definida como um vetor $s(e) = l_1\cdots l_{n-k}$ dado por

$$l_i \;=\; \begin{cases} 0, & [e,g_i]=0 \\ 1, & \{e,g_i\}=0. \end{cases} \tag{13}$$

Os erros podem ser representados por qualquer elemento de $\mathcal{G}_n$ ou de $\mathcal{G}_n/\mathcal{C}$, em que $\mathcal{C} = \{\pm I, \pm iI\}$ é o centro de $\mathcal{G}_n$. No segundo caso, os fatores de fase globais ± 1 e $\pm i$ não são levados em conta e a análise do erro é simplificada. O grupo $\mathcal{G}_n/\mathcal{C}$ possui ordem $|\mathcal{G}_n/\mathcal{C}| = 2^{2n}$, de modo que para um código de n q-bits são considerados 2^{2n} tipos de erro.

Para que um código estabilizador corrija um conjunto de erros $\{E_i\}$, é necessário que $E_a^\dagger E_b$ anticomute com algum elemento de $\mathcal{S}$ para quaisquer a e b. O grupo de Pauli $\mathcal{G}_n/\mathcal{C}$ pode ainda ser particionado em 2^{n-k} classes laterais, de modo que cada elemento pertence a uma das 2^{n-k} classes laterais definidas por $e_i\mathcal{C}(\mathcal{S}) = \{e_i c : c \in \mathcal{C}(\mathcal{S})\}$. $\mathcal{C}(\mathcal{S})$ é o *centralizador* de $\mathcal{S}$, que é formado pelo conjunto de erros $e \in \mathcal{G}_n$ que comuta com todos os geradores do estabilizador. A ordem de $\mathcal{C}(\mathcal{S})/\mathcal{C}$ é $|\mathcal{C}(\mathcal{S})/\mathcal{C}| = 2^{n+k}$, de modo que cada uma das 2^{n-k} possíveis síndromes do erro corresponde a uma classe lateral com 2^{n+k} operadores de erro.

Os elementos do centralizador $c \in \mathcal{C}(\mathcal{S})/\mathcal{C}$ são obtidos através do produto dos operadores lógicos $\overline{X}$ e $\overline{Z}$ pelos elementos do estabilizador, ou seja:

$$c_{a,b,j} \;=\; \overline{X}^a\overline{Z}^b S_j. \tag{14}$$

Sendo que $a,b \in \{0,1\}$ e S_j é dado pela equação (12).

IV. Decodificação por Síndrome

O primeiro passo da decodificação consiste em medir a síndrome do erro. A síndrome pode ser extraída através de um circuito quântico que possui como entrada $n-k$ q-bits auxiliares (*ancillas*) e os n q-bits de informação codificados afetados pelo erro. Na saída do circuito, medindo-se os $n-k$ ancillas na base computacional, obtém-se a síndrome do erro, mantendo-se inalterados os q-bits de informação. Um exemplo de circuito usado na medição da síndrome é mostrado na Figura 1. Uma vez obtida a síndrome, a decodificação pode ser feita consultando uma tabela de síndromes com 2^{n-k} entradas compostas pela síndrome e o erro mais provável de ter ocorrido.

A construção da tabela de síndromes e o procedimento de correção de erros é ilustrado no exemplo mostrado a seguir para o código $[[5,1,3]]$ [10]. Esse código é o menor código quântico capaz de corrigir um erro arbitrário em um q-bit. Essa afirmação pode ser verificada pelo fato de que qualquer produto $E_a E_b^\dagger$, E_a e E_b dados por (21), anticomuta com pelo menos um elemento do estabilizador do código (16). Essas condições são equivalentes às condições de Knill e Laflame [5] para que um CCEQ corrija um conjunto arbitrário de erros.

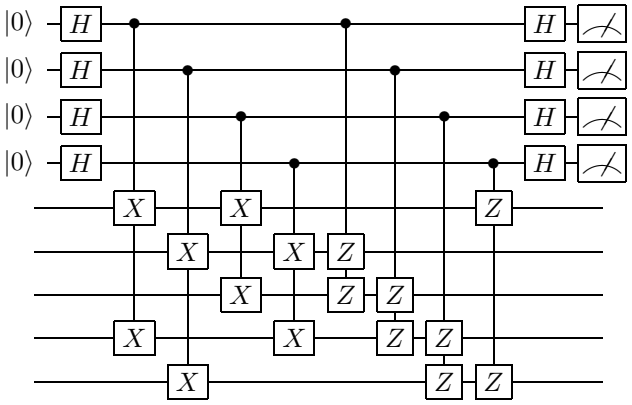

Fig. 1. Circuito quântico para medir a síndrome para o código definido pelo gerador da equação (15)

O código quântico $[[5,1,3]]$ é descrito pelos geradores

$$\begin{aligned} g_1 &= XZZXI \\ g_2 &= IXZZX \\ g_3 &= XIXZZ \\ g_4 &= ZXIXZ \end{aligned} \tag{15}$$

Um elemento do estabilizador $S \in \mathcal{S}$ pode ser obtido através da equação (12) com $n-k=4$, resultando no estabilizador:

$$\begin{aligned} S_1 &= IIIII & S_9 &= XZZXI \\ S_2 &= ZXIXZ & S_{10} &= YYZIZ \\ S_3 &= XIXZZ & S_{11} &= IZYYZ \\ S_4 &= YXXYI & S_{12} &= ZYYZI \\ S_5 &= IXZZX & S_{13} &= XYIYX \\ S_6 &= ZIZYY & S_{14} &= YZIZY \\ S_7 &= XXYIY & S_{15} &= IYXXY \\ S_8 &= YIYXX & S_{16} &= ZZXIX \end{aligned} \tag{16}$$

Um conjunto de operadores lógicos para esse código pode ser dado por:

$$\overline{X} \;=\; XXXXX \tag{17}$$

$$\overline{Z} \;=\; ZZZZZ \tag{18}$$

Esse código possui duas palavras-código base $|\overline{0}\rangle$ e $|\overline{1}\rangle$, sendo que a primeira é dada por:

$$\begin{aligned} |\overline{0}\rangle &= \sum_{S\in\mathcal{S}} S\,|00000\rangle \qquad (19)\\ &= |00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle + \\ &\quad |01001\rangle - |00011\rangle - |11101\rangle - |10111\rangle + \\ &\quad |10010\rangle - |11000\rangle - |00110\rangle - |01100\rangle - \\ &\quad |11011\rangle - |10001\rangle - |01111\rangle + |00101\rangle \end{aligned}$$

A segunda palavra-código base $|\overline{1}\rangle$ é dada por:

$$\begin{aligned} |\overline{1}\rangle &= \overline{X}\,|\overline{0}\rangle = XXXXX\,|\overline{0}\rangle \qquad (20)\\ &= |11111\rangle + |10101\rangle + |01011\rangle - |00001\rangle + \\ &\quad |10110\rangle - |11100\rangle - |00010\rangle - |01000\rangle + \\ &\quad |01101\rangle - |00111\rangle - |11001\rangle - |10011\rangle - \\ &\quad |00100\rangle - |01110\rangle - |10000\rangle + |11010\rangle \end{aligned}$$

Esse código pode corrigir qualquer tipo de erro em apenas um q-bit, os quais são indicados a seguir:

$$\begin{aligned} E_1 &= IIIII \quad E_9 = IIYII \qquad (21)\\ E_2 &= XIIII \quad E_{10} = IIIYI\\ E_3 &= IXIII \quad E_{11} = IIIIY\\ E_4 &= IIXII \quad E_{12} = ZIIII\\ E_5 &= IIIXI \quad E_{13} = IZIII\\ E_6 &= IIIIX \quad E_{14} = IIZII\\ E_7 &= YIIII \quad E_{15} = IIIZI\\ E_8 &= IYIII \quad E_{16} = IIIIZ \end{aligned}$$

Para os 16 erros que o código $[[5,1,3]]$ pode corrigir, as síndromes calculadas pela equação (13) são usadas para construir a Tabela I.

TABELA I

ERROS E SÍNDROMES PARA O CÓDIGO $[[5,1,3]]$.

Erro	Síndrome
$E_1 = IIIII$	$s_1 = [0\ 0\ 0\ 0]$
$E_2 = XIIII$	$s_2 = [0\ 0\ 0\ 1]$
$E_3 = IIZII$	$s_3 = [0\ 0\ 1\ 0]$
$E_4 = IIIIX$	$s_4 = [0\ 0\ 1\ 1]$
$E_5 = IIIIZ$	$s_5 = [0\ 1\ 0\ 0]$
$E_6 = IZIII$	$s_6 = [0\ 1\ 0\ 1]$
$E_7 = IIIXI$	$s_7 = [0\ 1\ 1\ 0]$
$E_8 = IIIIY$	$s_8 = [0\ 1\ 1\ 1]$
$E_9 = IXIII$	$s_9 = [1\ 0\ 0\ 0]$
$E_{10} = IIIZI$	$s_{10} = [1\ 0\ 0\ 1]$
$E_{11} = ZIIII$	$s_{11} = [1\ 0\ 1\ 0]$
$E_{12} = YIIII$	$s_{12} = [1\ 0\ 1\ 1]$
$E_{13} = IIXII$	$s_{13} = [1\ 1\ 0\ 0]$
$E_{14} = IYIII$	$s_{14} = [1\ 1\ 0\ 1]$
$E_{15} = IIYII$	$s_{15} = [1\ 1\ 1\ 0]$
$E_{16} = IIIYI$	$s_{16} = [1\ 1\ 1\ 1]$

Considerando um modelo de erros independentes para cada q-bit e um modelo de canal quântico pode-se associar probabilidades aos possíveis operadores de erro. O canal de despolarização é um exemplo de canal quântico de grande importância que pode ser representado por:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z). \qquad (22)$$

A interpretação para esse canal é que o estado permanece inalterado (erro I) com probabilidade $1-p$ e sofre inversão de bit (erro X), de fase (erro Z) e de bit e fase (erro Y) com probabilidade $p/3$.

Fazendo-se $p = 1/2$, o q-bit: permanece inalterado (erro I) com probabilidade $1/2$, sofre inversão de bit (erro X) com probabilidade $1/6$, sofre inversão de fase (erro Z) com probabilidade $1/6$ e sofre inversão de bit e fase (erro Y) com probabilidade $1/6$. Para essa distribuição, os erros com menor peso (menor número de elementos diferentes de I) possuem maior probabilidade que elementos de maior peso. Sendo assim, para as classes laterais do código $E_k\mathcal{C}(\mathcal{S})$, os elementos com maior probabilidade são aqueles passíveis de correção para esse código (equação (21)) e dessa forma, a Tabela I pode ser usada na decodificação do código $[[5,1,3]]$ considerando o modelo de canal adotado.

Cada um dos $2^{5+1} = 64$ erros definidos pela classe lateral $E_k\mathcal{C}(\mathcal{S})$ possui a mesma síndrome do erro, pois $c_{a,b,j}$ comuta com os elementos do estabilizador. Esse fato é ilustrado na Tabela II para o operador E_5, multiplicando E_5 pelo centralizador indicado na equação (14).

TABELA II

ERROS, SÍNDROMES E PROBABILIDADES PARA E_{16}

Erro	Síndrome	Probabilidade
$E_{5,1} = IIIIZ$	$s_{5,1} = [0\ 1\ 0\ 0]$	$0,0104$
$E_{5,2} = YIIYI$	$s_{5,2} = [0\ 1\ 0\ 0]$	$0,0035$
$E_{5,3} = IXXII$	$s_{5,3} = [0\ 1\ 0\ 0]$	$0,0035$
$E_{5,4} = IIZXI$	$s_{5,4} = [0\ 1\ 0\ 0]$	$0,0035$
$\vdots$	$\vdots$	$\vdots$
$E_{5,64} = ZXXZX$	$s_{5,64} = [0\ 1\ 0\ 0]$	$0,00012$

Uma vez obtida a síndrome através de um circuito quântico como o da Figura 1, a decodificação pode ser feita consultando a Tabela I. Por exemplo, se a síndrome obtida foi $[0\ 1\ 0\ 0]$, o erro mais provável de ter ocorrido foi a inversão de fase no quinto q-bit. Sendo assim, aplica-se a operação de reconstrução $E_5^\dagger = IIIIZ$ no estado recebido. O estado corrigido é igual ao obtido se o erro ocorrido foi realmente o mais provável, caso contrário a palavra corrigida ainda pertence ao código, mas não é igual àquela transmitida. Considerando o estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Após a codificação, tem-se $|\overline{\psi}\rangle = a\,|\overline{0}\rangle + b\,|\overline{1}\rangle$. A atuação do erro $E_{5,2} = YIIYI$ seguido da correção por $E_{5,1}^\dagger = IIIIZ$ resulta em $|\overline{\psi}\rangle_R = -a\,|\overline{0}\rangle + b\,|\overline{1}\rangle$. Apesar de $|\overline{\psi}\rangle_R$ pertencer ao código, ele difere de $|\overline{\psi}\rangle$ por um fator de fase.

A construção da tabela de síndromes para o código $[[5,1,3]]$ usando o modelo de canal proposto foi bastante simples. Entretanto, para outros tipos de códigos e outros modelos de canais, a obtenção da tabela pode ser uma tarefa mais trabalhosa. Para o código CSS $[[7,1,3]]$, pode-se mostrar que ele corrige um erro arbitrário em um único q-bit através da verificação das condições de Knill e Laflame para um conjunto de 22 erros (3 erros em cada um dos 7 q-bits mais

a identidade). Contudo, a tabela de síndromes deve conter $2^{7-1} = 64$ entradas. Essas entradas adicionais correspondem a erros com peso maior que um. Além disso, alguns desses erros podem ser passíveis de correção e outros não. Dessa forma, para exemplos mais gerais, pode ser necessário fazer uma busca em cada classe lateral a fim de construir a tabela de síndromes para um dado código.

V. Decodificação por Treliça

A construção de uma treliça quântica é feita para uma classe lateral do grupo de Pauli formada pelos elementos $E_k\mathcal{C}(\mathcal{S}) = \{E_k c : c \in \mathcal{C}(\mathcal{S})\}$. Uma vez obtida a síndrome do erro para uma palavra de informação recebida, a treliça para essa síndrome é construída da seguinte maneira:

1) Os vértices são agrupados em $n+1$ conjuntos V_i com $|V_0| = |V_n| = 1$.
2) As arestas são dirigidas e podem ser agrupadas em n conjuntos A_i. Uma aresta de A_i parte de um vértice pertencente a V_{i-1} para um vértice pertencente a V_i.
3) Uma aresta $a \in A_i$ é rotulada por $l(a)$, em que $l(a) \in \{I, X, Y, Z\}$.
4) Cada elemento $E = E^1 \otimes \cdots \otimes E^n \in \mathcal{G}_n$ com síndrome $s(E)$ está associado a um único caminho $(a^1, \cdots, a^n)$ tal que $l(a^i) = E^i$.
5) O vértice inicial é rotulado por um vetor nulo com $n-k$ coordenadas.
6) O vértice final é a síndrome do erro.

Os vértices V_i correspondem às síndromes parciais para cada elemento $P = P^1 \otimes \cdots \otimes P^n \in E_k\mathcal{C}(\mathcal{S})$. Para cada i, $V_i \in s(\pi_i(P))$, em que $\pi_i(P)$ é um produto tensorial de n matrizes de Pauli definido por $\pi_i(P) = P^1 \otimes \cdots \otimes P^i \otimes I \otimes \cdots \otimes I$, com a convenção de que $\pi_0(P) = I \otimes \cdots \otimes I$. Um vértice $v \in V_i$ é conectado ao vértice $w \in V_{i+1}$ se existe um P tal que $v = s(\pi_i(P))$ e $w = s(\pi_{i+1}(P))$. Nesse caso, o rótulo da aresta que liga v e w é dado por P^{i+1}.

A construção da treliça para o código $[[5, 1, 3]]$ e para a síndrome $[0\ 1\ 0\ 0]$ usando o gerador da equação (15) é ilustrada na Figura 2. Observa-se nessa construção que os elementos da classe lateral para a síndrome $[0\ 1\ 0\ 0]$ indicados na Tabela II representam percursos da treliça. O elemento $YIIYI$ por exemplo, corresponde ao percurso $(0000) - (1011) - (1011) - (1011) - (0100) - (0100)$.

Uma vez medida a síndrome através do circuito da Figura 1, a treliça é construída seguindo o procedimento indicado anteriormente. Para encontrar o erro mais provável é necessário utilizar um modelo de canal, assim como foi feito na seção IV. A partir do canal, cada aresta é então associada a um peso definido por $peso(a^i) = -\log(Prob(E^i))$, em que $E^i \in \{I, X, Y, Z\}$. O erro mais provável é aquele no qual o percurso na treliça possui o menor peso. No algoritmo da mini-soma proposto em [9], parte-se de um vértice V_{i-1} e seleciona-se o vértice V_i cujo caminho possui o menor peso, os demais caminhos de maior peso são descartados.

Para o canal de despolarização indicado na equação (22), com a distribuição de probabilidade usada no exemplo da seção IV, o algoritmo da mini-soma resulta no erro mais provável $IIIIZ$ para a síndrome $[0\ 1\ 0\ 0]$. O peso total para esse caminho, usando o logaritmo na base 2, é $6,585$.

Várias treliças podem ser construídas para um mesmo código, já que a ordem dos geradores é arbitrária e novos geradores podem ser escolhidos dentre os elementos do grupo estabilizador. Para garantir que os conjuntos de vértices V_i tenham cardinalidade mínima é necessário que o gerador do estabilizador esteja em uma forma específica, a forma *orientada à treliça*. Um estabilizador está na forma orientada à treliça se para $1 \leq j \leq n-k$ tem-se que:

1) $c(j)$ é uma função não decrescente, sendo que $c(j)$ representa a posição da primeira componente de g_j diferente de I.
2) $g_{j'}^{c(j)} = I$ para $j' > j+1$ e $g_{j+1}^{c(j)} \neq g_j^{c(j)}$.
3) Existe no máximo um $j' \neq j$ tal que $d(j) = d(j')$ e para esse caso $g_j^{d(j)} \neq g_{j'}^{d(j')}$, sendo que $d(j)$ representa a posição da última componente de g_j diferente de I.

Pode-se observar claramente que o gerador da equação (15) não está na forma orientada à treliça de modo que a treliça mostrada na Figura 2 não é mínima. Foram realizadas várias tentativas de modificar o conjunto de geradores do código a fim de obter a treliça mínima, mas não se teve sucesso para esse código.

A. Construção Alternativa

Para construir uma treliça quântica é necessário calcular as síndromes parciais para 2^{n+k} elementos de uma classe lateral de $\mathcal{G}_n/\mathcal{C}$. Se o objetivo da treliça é ser usada na identificação do erro mais provável, a tarefa de construção pode ser simplificada integrando-se o algoritmo da mini-soma à construção da treliça, de modo que os caminhos de maior peso já podem ser descartados durante a construção.

Os erros que compõem a treliça podem ser representados por um vetor binário $f = (a, b, p_1, \cdots, p_{n-k})$, já que para um erro com E com síndrome $s(E)$, a classe lateral de erros equivalentes é dada por:

$$E_f = (E).(\overline{X}^a).(\overline{Z}^b).(g_1^{p_1}) \cdots (g_{n-k}^{p_{n-k}}). \qquad (23)$$

Como $(A \otimes B).(C \otimes D) = (AC) \otimes (BD)$, os elementos E_f^i de E_f podem ser calculados individualmente para um determinado vetor f. Por exemplo, para $f = (1, 0, 1, 0, 0, 0, 0)$, $E = IIIIZ$, tem-se que $E_f = (XXXXX).I^{\otimes 5}.(XZZXI).I^{\otimes 5}.I^{\otimes 5}.I^{\otimes 5} = IYYIX$ e $E_f^1 = X.I.X.I.I.I = I$.

Para construir a treliça simplificada deve-se:

1) Gerar os 2^{n+k} vetores binários f.
2) Calcular E_f^1 para os vetores f.
3) Calcular V_1 usando E_f^1, já que $\pi_1(E_f) = E_f^1 \otimes I^{\otimes(n-1)}$.
4) Calcular o peso dos elementos E_f^1.
5) Descartar os vetores f para os quais os elementos E_f^1 possuem pesos diferentes do mínimo.
6) Repetir os passos 2-5 para $E_f^2, \cdots, E_f^n$.

Na Figura 3, é mostrado a construção da treliça simplificada usando o método proposto.

VI. Conclusões

Neste artigo foi analisado o problema da correção de erros para sistemas quânticos em detalhes. A construção da tabela

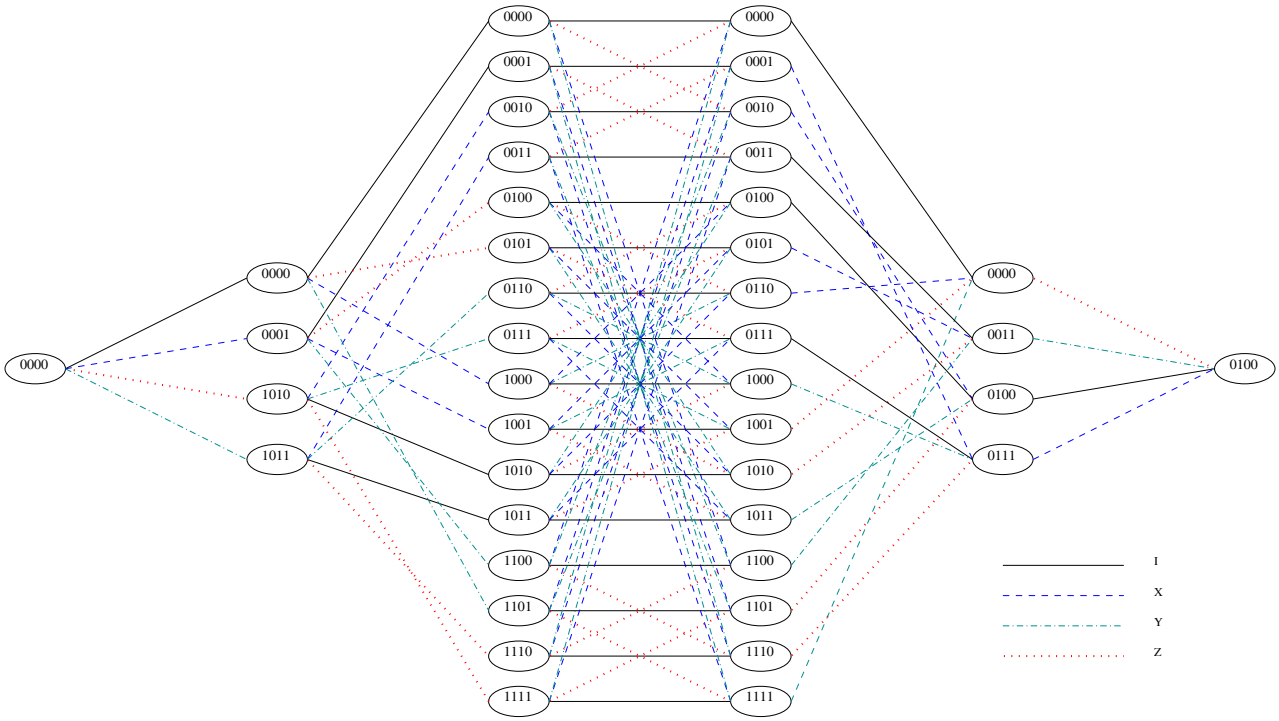

Fig. 2. Treliça para a síndrome $[0\ 1\ 0\ 0]$ do código $[[5, 1, 3]]$ usando o gerador da equação (15).

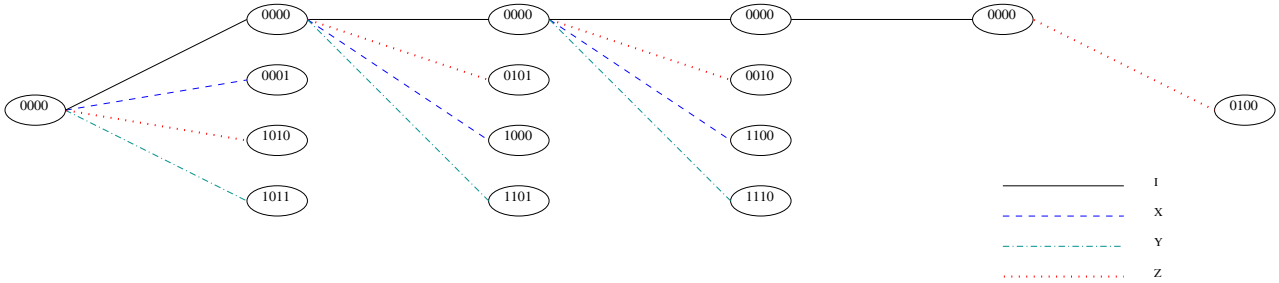

Fig. 3. Treliça para a síndrome $[0\ 1\ 0\ 0]$ do código $[[5, 1, 3]]$ usando a construção simplificada.

de síndromes é interessante para códigos pequenos como o mostrado no exemplo, na qual a busca pelo elemento de maior probabilidade em cada classe lateral não é necessária em virtude do conhecimento sobre a estrutura do código. Para construir a treliça é necessário obter a classe lateral para um determinado erro. Entretanto, colocando o estabilizador na forma orientada à treliça e utilizando a construção simplificada, pode-se reduzir bastante o esforço computacional necessário para a decodificação.

REFERÊNCIAS

[1] D. Bouwmeester, A. Ekert e A. Zeilinger, *The Physics of Quantum Information*. Springer, 2000.

[2] Michael A. Nielsen e Isaac L. Chuang, *Computação Quântica e Informação Quântica*. Bookman, 2005.

[3] Daniel Gottesman, *Stabilizer Codes and Quantum Error Correction*. California Institute of Technology, 1997.

[4] Frank Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing*. CRC Press, 2008.

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

[6] S. A. Aly, A. Klappenecker e P. K. Sarvepalli, "On Quantum and Classical BCH Codes," *IEEE Transactions on Information Theory*, v. 53, pp. 1183–1188, Março, 2007.

[7] Antonio Carlos Aido de Almeida, *Códigos Convolucionais Quânticos Concatenados*. FEEC/UNICAMP, 2004.

[8] Manabu Hagiwara e Hideki Imai, *Quantum Quasi-Cyclic LDPC Codes*. http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0701020, 2007.

[9] Harold Ollivier e Jean-Pierre Tillich, "Trellises for stabilizer codes: Definition and uses," *Physical Review A*, v. 74, 032304, 2006.

[10] R. Laflamme, C. Miquel, J. P. Paz e V. W. Zurek, "Perfect Quantum Error Correcting Code," *Phys. Rev. Lett.*, v. 77, pp. 198–201, 1996.