Um Código Convolucional Quântico de Taxa 1/9

Antonio Carlos Aido de Almeida e Reginaldo Palazzo Jr.

***Resumo*— Neste artigo, propomos a construção de um código convolucional quântico (CCQ) concatenado de taxa 1/9 a partir de um código convolucional clássico (CCC) de taxa 1/3. Este CCQ pode corrigir até dois erros quânticos gerais.**

***Palavras-Chave*— Códigos Corretores de Erros Quânticos, Códigos Convolucionais, Códigos Estabilizadores, Códigos Concatenados.**

***Abstract*— In this paper, we propose a construction of a rate-1/9 concatenated quantum convolutional code (QCC) from a rate-1/3 classical convolutional code (CCC). This QCC can correct up to two general quantum errors.**

***Keywords*— Quantum Error-Correction Codes, Convolutional Codes, Stabilizer Codes, Concatenated Codes.**

I. INTRODUÇÃO

Códigos corretores de erros quânticos (CCEQs) têm sido desenvolvidos para proteger a informação quântica dos efeitos de erros de descoerência (veja [1] para uma revisão). O surgimento de CCEQs cada vez mais eficientes tem elevado a confiabilidade de armazenamento e transmissão de informação quântica e permitido a realização de computações quânticas com um número cada vez maior de qubits.

Em analogia com a teoria clássica, duas grandes classes de CCEQs têm sido desenvolvidas: a classe dos códigos de bloco quânticos (CBQs) e a classe dos códigos convolucionais quânticos (CCQs).

O primeiro CBQ a ser descoberto foi o código de Shor [2], cuja operação de codificação pode ser compactamente escrita como:

$$|u\rangle \mapsto \frac{1}{2\sqrt{2}} \sum_{p,\ q,\ r=(0,\ 0,\ 0)}^{(1,\ 1,\ 1)} (-1)^{(p+q+r)u} |p,\ p,\ p,\ q,\ q,\ q,\ r,\ r,\ r\rangle, \quad (1)$$

na qual $u = \{0, 1\}$ e $|u\rangle$ denota o vetor u. O código de Shor é construído a partir de um código de bloco clássico (CBC) de repetição de três bits. Mais precisamente, o CBC de repetição de três bits é concatenado ao seu CBC equivalente de taxa $3/9$, gerando um CBC de repetição de taxa $1/9$. Este CBC concatenado tem distância $d_c = 9$ e, portanto, pode corrigir até quatro erros clássicos. Estes quatro erros clássicos estão associados aos quatro erros quânticos da base de um erro quântico geral ($X,\ Z,\ Y = iXZ,\ I$). Portanto, o código de Shor é capaz de corrigir um erro quântico geral sobre a palavra-código gerada pela operação (1).

Em analogia com o código de Shor, recentemente apresentamos um CCQ concatenado de taxa 1/4 e três memórias, denotado por [(4, 1, 3)] [3]. Este CCQ é construído a partir de um código convolucional clássico (CCC) de taxa 1/2 e duas memórias, denotado por (2, 1, 2). Mais precisamente, o CCC (2, 1, 2) é concatenado ao seu CCC (4, 2, 1) equivalente, gerando um CCC (4, 1, 3). Este CCC concatenado tem $d_{free} = 9$ e, portanto, o correspondente CCQ [(4, 1, 3)] pode corrigir um erro quântico geral. A operação de codificação deste CCQ pode ser compactamente escrita como:

$$\bigotimes_{t=0}^{+\infty} |u_t\rangle \mapsto \bigotimes_{t=0}^{+\infty} \left\{ \sum_{(p_t,\ q_t)=(0,\ 0)}^{(1,\ 1)} \frac{1}{2}(-1)^{v_t^{(1)}p_t + v_t^{(2)}q_t} |p_t + p_{t-1}, p_t + p_{t-1} + q_{t-1}, q_t + q_{t-1}, q_t + q_{t-1} + p_t\rangle \right\}, \quad (2)$$

na qual $v_t^{(1)} = u_t + u_{t-2}$ e $v_t^{(2)} = u_t + u_{t-1} + u_{t-2}$, para todo $u_t \in \{0,\ 1\}$ e $\bigotimes$ denota o produto tensorial. Além disso, de£nimos $u_{-1} = u_{-2} = 0$ e $p_{-1} = q_{-1} = 0$.

O código de Shor e o CCQ [(4, 1, 3)] são exemplos de CCEQs concatenados. Neste artigo, construimos um CCQ [(9, 1, 4)] a partir de um CCC (3, 1, 3). Este CCQ é capaz de corrigir até dois erros quânticos gerais. Até onde temos conhecimento, é o único CCQ conhecido capaz de corrigir mais de um erro quântico geral.

II. CONCEITOS FUNDAMENTAIS

A. O Formalismo Estabilizador

A idéia básica do formalismo estabilizador é que muitos estados quânticos podem ser descritos mais facilmente pelos operadores que o estabilizam do que pelo próprio estado quântico. Muitos códigos quânticos, incluindo os deste artigo, podem ser descritos de forma muito mais compacta usando estabilizadores do que a descrição por vetores de estado. Isto é possível devido ao uso inteligente da teoria de grupos pelo formalismo estabilizador. Dois grupos de operadores são usados para descrever o subespaço do código quântico [4]:

1) **O Grupo Estabilizador:**
   - O grupo estabilizador S é um subgrupo abeliano do grupo multiplicativo de Pauli, $\mathcal{G}_n = \pm 1,\ \pm i\ \{I,\ X,\ Y,\ Z\}^{\otimes n}$.
   - O subespaço do código $\mathcal{C}$ é o maior subespaço de $\mathcal{H}^{\otimes n}$ (n produtos tensoriais de $\mathcal{H}$) estabilizado por S:
   $$|\psi\rangle \in \mathcal{C} \Longleftrightarrow S|\psi\rangle = |\psi\rangle. \quad (3)$$
   - Equivalentemente, se os M_i's são $n-k$ geradores independentes de S, então:
   $$|\psi\rangle \in \mathcal{C} \Longleftrightarrow \forall\ i,\ M_i|\psi\rangle = |\psi\rangle. \quad (4)$$

   Estas equações, chamadas de síndromes, de£nem o subespaço do código.

Antonio Carlos Aido de Almeida e Reginaldo Palazzo Jr., Departamento de Telemática, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, Brasil, E-mails: aido@dt.fee.unicamp.br, palazzo@dt.fee.unicamp.br. Este trabalho foi financiado pela FAPESP (02/07473-7 e 04/10979-5).

2) **O Grupo de Pauli Lógico:** Os operadores lógicos deixam o subespaço do código $\mathcal{C}$ globalmente invariante, mas possuem uma ação não trivial sobre este espaço. É possível exigir que tais operadores reproduzam exatamente as relações de comutação do grupo de Pauli para os qubits lógicos. Isto é matematicamente expresso por:

$$\overline{X}_i,\ \overline{Z}_i \ \in\ N(S)/S, \tag{5}$$

$$\{\overline{X}_i,\ \overline{Z}_i\} = 0, \tag{6}$$

$$\forall\ i \neq j,\ \ [\overline{X}_i,\ \overline{X}_j] = [\overline{Z}_i,\ \overline{Z}_j] = [\overline{X}_i,\ \overline{Z}_j] = 0. \tag{7}$$

Em (5), $N(S)$ é o normalizador de S, em (6) $\{.,.\}$ denota anticomutador e em (7) $[.,.]$ denota comutador.

B. Estrutura de um CCQ Concatenado

A construção de um CCQ concatenado dá-se através da concatenação de um CCQ phase flip com um CCQ bit flip. Estes CCQs podem ser gerados a partir de um único CCC ou a partir de dois CCCs distintos. O CCQ para um canal com erro quântico geral terá a taxa e a memória do CCC concatenado associado. Em notação algébrica, a concatenação de um CCC ($n_1,\ k_1,\ m_1$) com um CCC ($n_2,\ n_1,\ m_2$) dá origem a um CCC ($n_2,\ k_1,\ m_1+m_2$). Portanto, o CCQ gerado a partir do CCC concatenado será um CCQ [($n_2,\ k_1,\ m_1+m_2$)].

O primeiro CCC da cadeia de concatenação é responsável pelo número de estados da superposição da palavra-código quântica e o segundo CCC da cadeia de concatenção é responsável pelo comprimento de cada um destes estados da superposição. Tanto o crescimento do número de estados quanto do comprimento de cada um destes estados é um crescimento exponencial com o número de qubits de informação.

Os geradores do grupo estabilizador e os operadores lógicos do CCQ concatenado podem ser obtidos, respectivamente, a partir das matrizes de verificação de paridade e de geração dos CCCs que fazem parte da cadeia de concatenação. A detecção de possíveis erros bit flip e phase flip pode ser feita através da adaptação de um algoritmo de decodificação de síndromes (ADS) clássico [5] ao contexto quântico de medida dos autovalores dos geradores do grupo estabilizador do CCQ[1].

Para que um CCQ concatenado possa corrigir até t erros quânticos gerais, é necessário que os CCCs da cadeia de concatenação assegurem a correção de pelo menos t erros cada um ($d_{free} \geq 2t+1$) e que o CCC concatenado assegure a correção de pelo menos $4t$ erros ($d_{free} \geq 8t+1$)[2]. Portanto, para que um CCQ concatenado corrija até $t = 1,\ 2,\ 3,\ 4, \ldots$ erros quânticos gerais, é necessário que os CCCs da cadeia de concatenação tenham $d_{free}(\mathit{min}) = 3,\ 5,\ 7,\ 9, \ldots$ e que o CCC concatenado tenha $d_{free}(\mathit{min}) = 9,\ 17,\ 25,\ 33, \ldots$

Determinada a distância do CCC concatenado, pode-se determinar facilmente a distância do correspondente CCQ concatenado. Sabemos que, para construir um CCC qualquer capaz de corrigir até t erros clássicos, é necessário que este CCC tenha uma distância d_c que satisfaça a relação $d_c \geq 2t{+}1$, e que, para construir um CCQ qualquer capaz de corrigir até t' erros quânticos gerais (portanto, associado a $4t$ erros clássicos), é necessário que este CCQ tenha uma distância d_q que satisfaça a relação $d_q \geq 2t'+1 = 8t+1$. Assim, as distâncias d_c e d_q estão relacionadas através da expressão:

$$d_q = \lfloor \frac{d_c+3}{4} \rfloor. \tag{8}$$

[1]Veja um exemplo de aplicação do ADS ao contexto quântico em [3].

[2]Se um código quântico é capaz de corrigir um conjunto discreto de erros do tipo bit flip, phase flip e bit-phase flip para um mesmo conjunto de registros quânticos, então este código quântico é capaz de corrigir automaticamente um erro quântico geral (ou *arbitrário*) com geradores Z e X para o mesmo conjunto de registros quânticos [6].

III. CONSTRUÇÃO DE UM CCQ [(9, 1, 4)]

Considere o codificador (3, 1, 3) ótimo com a seguinte matriz geradora:

$$\mathbf{G}(D) = [1+D^2+D^3,\ 1+D+D^3,\ 1+D+D^2+D^3]. \tag{9}$$

O CCC (3, 1, 3) gerado por este codificador tem $d_{free} = 10$ e, portanto, pode corrigir até quatro erros clássicos. Este CCC (3, 1, 3) pode ser usado na construção de um CCQ [(3, 1, 3)] para o canal bit flip com a seguinte operação de codificação:

$$\bigotimes_{t=0}^{+\infty} |u_t\rangle \mapsto \bigotimes_{t=0}^{+\infty} |v_t^{(1)},\ v_t^{(2)},\ v_t^{(3)}\rangle, \tag{10}$$

na qual

$$\begin{array}{rcl} v_t^{(1)} & = & u_t + u_{t-2} + u_{t-3}, \\ v_t^{(2)} & = & u_t + u_{t-1} + u_{t-3}, \\ v_t^{(3)} & = & u_t + u_{t-1} + u_{t-2} + u_{t-3}, \end{array} \tag{11}$$

para todo $u_t \in \{0,\ 1\}$. Definimos $u_{-1} = u_{-2} = u_{-3} = 0$.

Através de uma transformada de Hadamard, é possível obter também a operação de codificação do CCQ [(3, 1, 3)] para o canal phase flip, a saber:

$$\bigotimes_{t=0}^{+\infty} |u_t\rangle \mapsto \bigotimes_{t=0}^{+\infty} \left\{ \frac{1}{2\sqrt{2}} (|0\rangle + (-1)^{v_t^{(1)}} |1\rangle) \right. \\ \left. (|0\rangle + (-1)^{v_t^{(2)}} |1\rangle)(|0\rangle + (-1)^{v_t^{(3)}} |1\rangle) \right\}, \tag{12}$$

Ou, mais compactamente,

$$\bigotimes_{t=0}^{+\infty} |u_t\rangle \mapsto \bigotimes_{t=0}^{+\infty} \left\{ \frac{1}{2\sqrt{2}} \sum_{(p_t,\ q_t,\ r_t)=(0,\ 0,\ 0)}^{(1,\ 1,\ 1)} \right. \\ \left. (-1)^{v_t^{(1)} p_t + v_t^{(2)} q_t + v_t^{(3)} r_t} |p_t,\ q_t,\ r_t\rangle \right\}. \tag{13}$$

Os CCQs [(3, 1, 3)] gerados pelas operações (10) e (12) são capazes de corrigir, respectivamente, até quatro erros X e quatro erros Z. Para determinarmos os geradores do grupo estabilizador destes CCQs, devemos encontrar uma matriz verificação de paridade para a matriz geradora (9). Com o auxílio do teorema do fator invariante [7], temos:

$$\mathbf{H}(D) = \begin{bmatrix} 1+D+D^3 & 1+D^2+D^3 & 0 \\ 1+D+D^2 & D^2 & 1 \end{bmatrix}. \tag{14}$$

As linhas da matriz (14) na forma semi-infinita são usadas para escrever os geradores do grupo estabilizador. No caso do CCQ [(3, 1, 3)] para o canal bit flip, os 0s e 1s devem ser substituídos, respectivamente, por operadores Is e Zs, e no caso do CCQ [(3, 1, 3)] para o canal phase flip, os 0s e 1s devem ser substituídos, respectivamente, por operadores Is e Xs.

Analogamente, as linhas da matriz (9) na forma semi-infinita são usadas para escrever os operadores lógicos sobre os qubits de informação. No caso do CCQ [(3, 1, 3)] para o canal bit flip, os 0s e 1s devem ser substituídos, respectivamente, por operadores Is e Xs, e no caso do CCQ [(3, 1, 3)] para o canal phase flip, os 0s e 1s devem ser substituídos, respectivamente, por operadores Is e Zs.

A detecção de possíveis erros X e Z sobre as palavras-código geradas pelas operações (10) e (12) é feita através das medidas dos geradores do grupo estabilizador. É fácil de verificar que existe um mapeamento entre as síndromes clássicas $s_t = \{0, 1\}$ e os autovalores $\alpha_t = \{+1, -1\}$ destes geradores observáveis. Este mapeamento é estabelecido pela relação $s_t = (1 - \alpha_t)/2$ (mod 2)(para $t = 0,\ 1,\ 2, \ldots$). Portanto, podemos usar esta relação para adaptar o ADS ao contexto quântico. Esta técnica permite-nos identificar sem ambigüidades o vetor "erro de bit" sobre os qubits da palavra-código gerada pela operação (10) e o vetor "erro de fase" sobre os *blocos* da palavra-código gerada pela operação (12).

Para que possamos usar o ADS no processo de detecção de possíveis erros X e Z sobre as palavras-código geradas pelas operações (10) e (12), temos que obter as soluções gerais da equação de síndromes $\mathbf{s}(D) = \mathbf{e}(D)\mathbf{H}^T(D)$ para o codificador (3, 1, 3) com matriz geradora (9). De acordo com [5], estas soluções são:

$$\begin{aligned}
\mathbf{e}^{(1)}(D) &= D\mathbf{s}^{(1)}(D) + \mathbf{t}(D) + D^2\mathbf{t}(D) + D^3\mathbf{t}(D), \\
\mathbf{e}^{(2)}(D) &= \mathbf{s}^{(1)}(D) + D\mathbf{s}^{(1)}(D) + \mathbf{t}(D) + D\mathbf{t}(D) \\
&\quad + D^3\mathbf{t}(D), \\
\mathbf{e}^{(3)}(D) &= D\mathbf{s}^{(1)}(D) + \mathbf{s}^{(2)}(D) + \mathbf{t}(D) + D\mathbf{t}(D) \\
&\quad + D^2\mathbf{t}(D) + D^3\mathbf{t}(D),
\end{aligned} \tag{15}$$

nas quais $\mathbf{t}(D)$ é um polinômio arbitrário do anel $F[D]$.

Os valores de $\mathbf{t}(D)$, $D\mathbf{t}(D)$, $D^2\mathbf{t}(D)$ e $D^3\mathbf{t}(D)$ ao longo da treliça do ADS podem ser obtidos através da Tabela I. Definimos o estado inicial da treliça como $(D\mathbf{t}(D),\ D^2\mathbf{t}(D),\ D^3\mathbf{t}(D)) = (0,\ 0,\ 0)$. Além disso, definimos $\mathbf{s}^{(1)}(D) = \mathbf{s}^{(2)}(D) = 0$ antes do estágio 0. O ADS então seleciona o caminho na treliça com o menor peso de Hamming [5].

Com o codificador (9, 3, 1) equivalente trivial do codificador (3, 1, 3)[3] é possível construir um CCQ [(9, 3, 1)] capaz de corrigir até quatro erros X. A operação de codificação deste CCQ é escrita de forma análoga a operação (10). A concatenação do codificador (3, 1, 3) com o seu equivalente trivial (9, 3, 1) dá origem a um codificador (9, 1, 4) com a seguinte matriz geradora na forma semi-infinita:

[3] O codificador (9, 3, 1) equivalente trivial do codificador (3, 1, 3) é o codificador (9, 3, 1) com a *mesma* matriz geradora do codificador (3, 1, 3).

TABELA I

TABELA DE ESTADOS DO REGISTRO DE DESLOCAMENTO PARA $\mathbf{t}(D)$.

$D\mathbf{t}(D)$, $D^2\mathbf{t}(D)$, $D^3\mathbf{t}(D)$	$\mathbf{t}(D)$=0	$\mathbf{t}(D)$=1
$a = 000$	$a = 000$	$c = 100$
$b = 001$	$a = 000$	$c = 100$
$c = 010$	$b = 001$	$d = 101$
$d = 011$	$b = 001$	$d = 101$
$a = 100$	$a = 010$	$c = 110$
$b = 101$	$a = 010$	$c = 110$
$c = 110$	$b = 011$	$d = 111$
$d = 111$	$b = 011$	$d = 111$

$$\mathbf{G}_C = \begin{bmatrix} \mathbf{G}_{C,0} & \mathbf{G}_{C,1} & \mathbf{G}_{C,2} & \mathbf{G}_{C,3} & \mathbf{G}_{C,4} & & \\ & \mathbf{G}_{C,0} & \mathbf{G}_{C,1} & \mathbf{G}_{C,2} & \mathbf{G}_{C,3} & \mathbf{G}_{C,4} & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \end{bmatrix}, \tag{16}$$

na qual

$$\begin{aligned}
\mathbf{G}_{C,0} &= [111100001], \\
\mathbf{G}_{C,1} &= [001101011], \\
\mathbf{G}_{C,2} &= [001001101], \\
\mathbf{G}_{C,3} &= [011001110], \\
\mathbf{G}_{C,4} &= [001010111].
\end{aligned} \tag{17}$$

O CCC (9, 1, 4) gerado por este codificador tem $d_{free} = 24$. Veja o diagrama de estados na Figura 1. Portanto, o CCQ [(9, 1, 4)] associado tem $d_q = \lfloor (24+3)/4 \rfloor = 6$, ou seja, é capaz de corrigir até dois erros quânticos gerais. A operação de codificação para este CCQ pode ser escrita como:

$$\bigotimes_{t=0}^{+\infty} |u_t\rangle \mapsto \bigotimes_{t=0}^{+\infty} \left\{ \sum_{(p_t,q_t,r_t)=(0,\,0,\,0)}^{(1,\,1,\,1)} \frac{1}{2\sqrt{2}} (-1)^{v_t^{(1)} p_t + v_t^{(2)} q_t + v_t^{(3)} r_t} \right.$$
$$\left. |w_t^{(1)}, w_t^{(2)}, w_t^{(3)}, w_t^{(4)}, w_t^{(5)}, w_t^{(6)}, w_t^{(7)}, w_t^{(8)}, w_t^{(9)}\rangle \right\}, \tag{18}$$

na qual

$$\begin{aligned}
v_t^{(1)} &= u_t + u_{t-2} + u_{t-3}, \\
v_t^{(2)} &= u_t + u_{t-1} + u_{t-3}, \\
v_t^{(3)} &= u_t + u_{t-1} + u_{t-2} + u_{t-3},
\end{aligned} \tag{19}$$

para todo $u_t \in \{0,\ 1\}$, com $u_{-1} = u_{-2} = u_{-3} = 0$, e

$$\begin{aligned}
w_t^{(1)} &= p_t + p_{t-1} + r_{t-1}, \\
w_t^{(2)} &= p_t + p_{t-1} + r_{t-1}, \\
w_t^{(3)} &= p_t + p_{t-1} + q_{t-1} + r_{t-1}, \\
w_t^{(4)} &= q_t + q_{t-1} + r_{t-1}, \\
w_t^{(5)} &= p_t + q_t + q_{t-1}, \\
w_t^{(6)} &= p_t + q_t + q_{t-1} + r_{t-1}, \\
w_t^{(7)} &= p_t + r_t + r_{t-1}, \\
w_t^{(8)} &= r_t + q_t + q_{t-1}, \\
w_t^{(9)} &= p_t + r_t + q_t + q_{t-1},
\end{aligned} \tag{20}$$

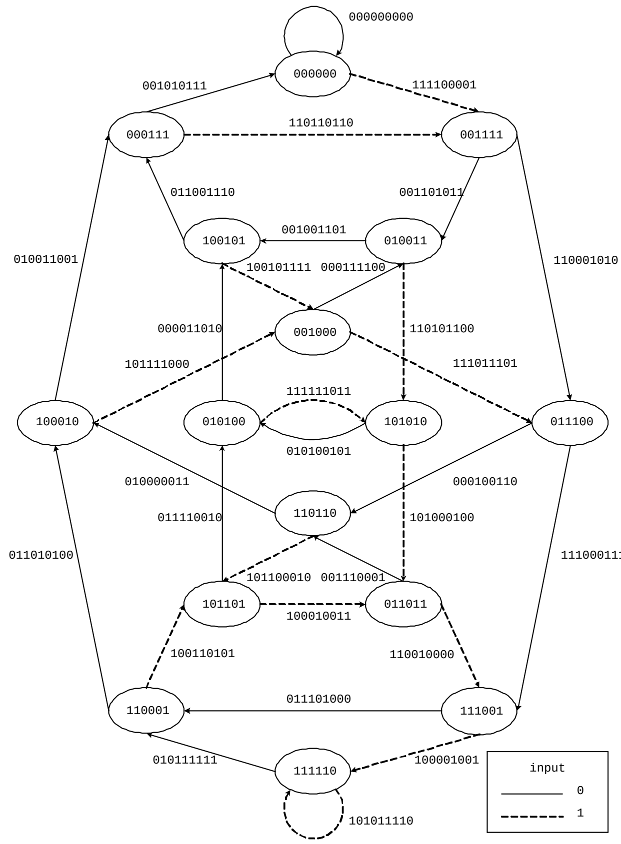

Fig. 1. Diagrama de estados do codificador (9, 1, 4) com matriz geradora (16).

com $p_{-1} = q_{-1} = r_{-1} = 0$.

Para um melhor entendimento da dinâmica de geração deste código, deixe-nos considerar o exemplo simples de uma sequência de informação com dois qubits. Cada um dos quatro estados da base é codificado em uma superposição de 2^3 estados de comprimento 9 no estágio 0, uma superposição de 2^6 estados de comprimento 18 no estágio 1, uma superposição de 2^9 estados de comprimento 27 no estágio 2, uma superposição de 2^{12} estados de comprimento 36 no estágio 3, uma superposição de 2^{15} estados de comprimento 45 no estágio 4 e uma superposição de 2^{15} estados de comprimento 54 no estágio 5. Neste estágio, temos uma palavra-código válida para dois qubits de informação. Repare que o comprimento deste código cresce durante uma unidade de tempo além do número de estados. Isto ocorre porque o código bit flip é o segundo da cadeia de concatenação e possui memória unitária. Generalizando, cada um dos 2^N estados da base de uma sequência de informação com N qubits é codificado em uma superposição de $2^{3(N+3)}$ estados, cada um dos quais com $3(3(N+3)+3) = 9N+36$ qubits.

As linhas da matriz (14) na forma semi-infinita podem ser usadas para escrever os geradores do grupo estabilizador do CCQ [(9, 1, 4)]. Para isto, considere que a matriz verificação de paridade do codificador (9, 3, 1) seja chamada de $\mathbf{H}_X$, e que a matriz verificação de paridade do codificador (3, 1, 3), expandida para o codificador (9, 1, 4) (para isto, basta tomar cada uma das linhas da matriz verificação de paridade do codificador (3, 1, 3) como sequências de informação para o codificador (9, 3, 1)), seja chamada de $\mathbf{H}_Z$. Com as matrizes $\mathbf{H}_X$ e $\mathbf{H}_Z$ podemos construir a matriz verificação de paridade $\mathbf{H}_C$ da matriz geradora (16):

$$\mathbf{H}_C = \begin{bmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{bmatrix} =$$

$$\begin{bmatrix}
\mathbf{H}_{X,0} & & & & & & \\
\mathbf{H}_{X,1} & \mathbf{H}_{X,0} & & & & & \\
 & \mathbf{H}_{X,1} & \mathbf{H}_{X,0} & & & & \\
 & & \mathbf{H}_{X,1} & \mathbf{H}_{X,0} & & & \\
 & & & \mathbf{H}_{X,1} & \mathbf{H}_{X,0} & & \\
 & & & & \mathbf{H}_{X,1} & \mathbf{H}_{X,0} & \\
 & & & & & \ddots & \ddots \\
\mathbf{H}_{Z,-0} & \mathbf{H}_{Z,0} & & & & & \\
\mathbf{H}_{Z,-1} & \mathbf{H}_{Z,1} & \mathbf{H}_{Z,0} & & & & \\
\mathbf{H}_{Z,-2} & \mathbf{H}_{Z,2} & \mathbf{H}_{Z,1} & \mathbf{H}_{Z,0} & & & \\
\mathbf{H}_{Z,-3} & \mathbf{H}_{Z,3} & \mathbf{H}_{Z,2} & \mathbf{H}_{Z,1} & \mathbf{H}_{Z,0} & & \\
 & \mathbf{H}_{Z,-3} & \mathbf{H}_{Z,3} & \mathbf{H}_{Z,2} & \mathbf{H}_{Z,1} & \mathbf{H}_{Z,0} & \\
 & & \ddots & \ddots & \ddots & \ddots & \ddots
\end{bmatrix}, \quad (21)$$

na qual

$$\mathbf{H}_{X,0} = \begin{bmatrix} 110000000 \\ 101000000 \\ 100110000 \\ 100101000 \\ 010100110 \\ 110100101 \end{bmatrix}, \quad \mathbf{H}_{X,1} = \begin{bmatrix} 110010100 \\ 000110100 \\ 000110010 \\ 000000110 \\ 000000110 \\ 000000000 \end{bmatrix},$$

$$\mathbf{H}_{Z,0} = \begin{bmatrix} 010111000 \\ 100101111 \end{bmatrix}, \quad \mathbf{H}_{Z,-0} = \begin{bmatrix} 111100110 \\ 111011010 \end{bmatrix},$$

$$\mathbf{H}_{Z,1} = \begin{bmatrix} 000100110 \\ 000011010 \end{bmatrix}, \quad \mathbf{H}_{Z,-1} = \begin{bmatrix} 111011101 \\ 111011101 \end{bmatrix},$$

$$\mathbf{H}_{Z,2} = \begin{bmatrix} 010100101 \\ 101100101 \end{bmatrix}, \quad \mathbf{H}_{Z,-2} = \begin{bmatrix} 000111011 \\ 111100110 \end{bmatrix},$$

$$\mathbf{H}_{Z,3} = \begin{bmatrix} 010000011 \\ 111100110 \end{bmatrix}, \quad \mathbf{H}_{Z,-3} = \begin{bmatrix} 111100110 \\ 000000000 \end{bmatrix} \quad (22)$$

Usamos as linhas da matriz $\mathbf{H}_X$ para obter os geradores Z e as linhas da matriz $\mathbf{H}_Z$ para obter os geradores X. Os 0s e 1s da matriz $\mathbf{H}_X$ devem ser substituídos, respectivamente, por operadores Is e Zs, e os 0s e 1s da matriz $\mathbf{H}_Z$ devem ser substituídos, respectivamente, por operadores Is e Xs. Para uma sequência de informação finita com N qubits, precisamos considerar somente a medida de $(9-3)((N+4)+1) = 6N+30$ geradores Z e de $(3-1)((N+3)+3) = 2N+12$ geradores X para descrever o subespaço do CCQ [(9, 1, 4)] truncado. Usamos as síndromes das medidas dos geradores Z e X nas soluções (15) para detectar, através de duas treliças do ADS, o "vetor erro de bit" sobre os qubits da palavra-código (18) e o "vetor erro de fase" sobre os *blocos* do CCQ phase flip [(3, 1, 3)] associado[4].

Os operadores lógicos $\overline{X}$ e $\overline{Z}$ atuando sobre os qubits de informação são obtidos através das linhas da matriz (16). Para obter $\overline{X}$, os 0s e 1s da matriz (16) devem ser substituídos,

[4]Identificado o "vetor erro de fase" sobre os blocos do CCQ phase flip [(3, 1, 3)] associado, pode-se então determinar para qual (ou quais) qubit(s) da palavra-código (18) o(s) erro(s) de fase se propagou (ou se propagaram).

respectivamente, por operadores Is e Zs, e para obter $\overline{Z}$, os 0s e 1s da matriz (16) devem ser substituídos, respectivamente, por operadores Is e Xs.

IV. CONCLUSÕES

Neste artigo construimos um CCQ de taxa 1/9 capaz de corrigir até dois erros quânticos gerais. Até onde temos conhecimento, este é o primeiro CCQ a ser proposto que é capaz de corrigir mais de um erro quântico geral. Além disso, a capacidade de correção deste código quântico supera a de seu homólogo da classe dos CBQs, o código de Shor. Em comum, ambos são códigos quânticos construídos a partir da concatenação de um código phase flip com um código bit flip, gerados a partir de um único código clássico de taxa 1/3.

A simplicidade do processo de codificação e decodificação dos CCQs concatenados faz com que o estudo de uma subclasse de CCQs concatenados se torne particularmente interessante, sobretudo se o objetivo for a construção de CCQs capazes de corrigir mais do que um erro quântico geral [8].

REFERÊNCIAS

[1] J. Preskill, *A Course on Quantum Computation and Quantum Information - Lecture Notes*, California Institute of Technology, 1998; disponível em www.theory.caltech.edu/people/preskill/ph229.

[2] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, 52, pp. 2493-2496, 1995.

[3] A. C. A. de Almeida and R. Palazzo Jr., "A Concatenated [(4, 1, 3)] Quantum Convolutional Code", *2004 IEEE Information Theory Workshop*, San Antonio, Texas, 2004.

[4] D. Gottesman, *Stabilizer codes and quantum error correction*, PhD Thesis, California Institute of Technology, USA, 1997; disponível em arXiv e-print quant-ph/9705052.

[5] I. S. Reed and T. K. Truong, "New syndrome decoding techiniques for the (n, k) convolutional codes", *IEE Proceedings*, 131-F(4), pp. 412-416, 1984.

[6] E. Knill and R. La¤amme, "A theory of quantum error-correcting codes", *Phys. Rev. A*, 55, pp. 900-911, 1997.

[7] G. D. Forney, "Convolutional codes I: algebraic structure", *IEEE Trans. Inf. Th.*, IT-16(6), pp. 720-738, 1970.

[8] A. C. A. Almeida, *Concatenated Quantum Convolutional Codes*, PhD Thesis, Universidade Estadual de Campinas (UNICAMP), Brazil, Oct. 2004.