Determinação de Novos Códigos Convolucionais Quânticos com $d_{free} > 9$ através de Funções Armadilhas

Polyane Alves Santos e Reginaldo Palazzo Jr.

***Resumo*— Neste trabalho apresentamos alguns resultados novos decorrentes da aplicação de transformações armadilhas ao código convolucional quântico concatenado $[4, 1, 3]$ com o objetivo de utiliza-lo em sistemas criptográficos e com isso alcançar um alto grau de proteção e privacidade na informação a ser transmitida. Como conseqüência desse fato, novos códigos convolucionais quânticos com $d_{free} \geq 9$ foram determinados.**

***Palavras-Chave*— Criptografia, Códigos Convolucionais Quânticos, Transformações Armadilhas.**

***Abstract*— In this paper we present some new results as a consequence of applying trapdoor functions to the quantum concatenated convolutional code $[4, 1, 3]$ with the goal of using it in cryptographic systems such that good protection against attacks and a high degree of privacy in the information being transmitted. Therefore, new quantum convolutional codes with $d_{free} \geq 9$ are presented.**

***Keywords*— Cryptography, Quantum Convolutional Codes, Trapdoor functions.**

I. Introdução

A criptografia quântica é um afluente em desenvolvimento da criptografia que utiliza os princípipos da Mecânica Quântica para garantir uma comunicação segura, [1]. Com ela, tanto o transmissor quanto o receptor podem criar e partilhar uma chave secreta para cifrar e decifrar mensagens. Para isso, é necessário utilizar métodos clássicos para efetuar a troca da mensagem propriamente dita.

Embora o objetivo principal deste trabalho estivesse relacionado com a apresentação de uma proposta de um sistema de cifragem do tipo McEliece bem como de sua análise, para a nossa surpresa os resultados apresentados através das aplicações das transformações armadilhas aos códigos convolucionais clássicos concatenados (CCC) $(n, k, m) = (4, 1, 3)$, onde n denota o comprimento da palavra-código ramo, k denota o comprimento dos dígitos de informação, e m denota a quantidade de memória no codificador, conduziu a novos CCCs com capacidade de correção de erros maior que os anteriormente conhecidos, [3] e [5]. Os CCCs resultantes apresentam $d_{free} = 10$ ou $d_{free} = 11$ e, na maioria dos casos, o código com taxa $R = 2/4$ que o compõe é um código catastrófico, [2]. Todavia, o CCC resultante é um código não catastrófico.

Polyane Alves Santos e Reginaldo Palazzo Jr. Departamento de Telemática, Universidade Estadual de Campinas, Campinas, Brasil, E-mails: polyane@dt.fee.unicamp.br, palazzo@dt.fee.unicamp.br.
Este trabalho teve o suporte financeiro da CAPES.

II. Construção do CCQ [4,1,3]

Para a construção do código convolucional quântico concatenado (CCQ) $[4, 1, 3]$, [3] e [4], foram utilizados dois códigos convolucionais quânticos específicos $\mathcal{C}_1$ e $\mathcal{C}_2$. Cada um desses códigos é capaz de corrigir, respectivamente, um erro do tipo "phase-flip"Z e um erro do tipo "bit-flip"X, para um mesmo conjunto de registros quânticos. Em seguida é realizada a concatenação destes dois códigos da seguinte forma: primeiro $\mathcal{C}_1$ foi usado para codificar o estado quântico de informação e depois $\mathcal{C}_2$ foi utilizado para codificar o estado quântico resultante da codificação por $\mathcal{C}_1$. O código $\mathcal{C}$ resultante desta concatenação é capaz de corrigir um erro quântico geral com geradores Z e X, para o mesmo conjunto de registros quânticos protegidos por $\mathcal{C}_1$ e $\mathcal{C}_2$.

Apresentamos a seguir os passos para a construção do CCQ.

A. CCQ para o canal bit-flip

Para a obtenção de um CCQ para o canal bit-flip foi utilizado o CCC $(2, 1, 2)$ com a matriz geradora na forma polinomial dada por $\mathbf{G}(D) = [1 + D^2, 1 + D + D^2]$ na operação de codificação dos bits contidos em cada um dos kets da base de uma seqüência de registros quânticos que deve ser protegida da ação dos erros de um canal bit-flip. Desta operação de codificação clássica, podemos obter a correspondente operação de codificação quântica:

$$\bigotimes_{t=0}^{+\infty} \mid u_t \rangle \rightarrow \bigotimes_{t=0}^{+\infty} \mid u_t + u_{t-2}, u_t + u_{t-1} + u_{t-2} \rangle, \quad (1)$$

onde u_t denota o vetor de entrada 1-dimensional, o conteúdo do ket do lado direito, v_t denota a saída do codificador como sendo um vetor 2-dimensional, e $u_{-1} = u_{-2} = 0$.

Ao final de cada seqüência de bits contidos dentro dos kets da base são acrescentados mais dois bits 0s para serem codificados, pois, na prática, o interesse é sempre codificar uma seqüência finita de qubits. Esta condição garante que tenhamos sempre palavras-código clássicas válidas dentro dos kets e, consequentemente, garante a obtenção de palavras-código quânticas válidas.

Este CCQ herda todas as propriedades do CCC associado. Isto é, se o CCC $(2,1,2)$ não é catstrófico, então o CCQ $[2,1,2]$ também não será catastrófico e manterá a mesma capacidade de correção de erros, ou seja, é capaz de corrigir até dois erros bit-flips em quaisquer dois qubits da palavra-código.

B. CCQ para o canal phase-flip

Uma maneira fácil de tratar o canal phase-flip como um canal bit-flip é fazer uso de uma base computacional apropriada. Para isso, suponha que ao invés de utilizarmos a base computacional $\{|0\rangle, |1\rangle\}$ para o qubit, utilizemos a base conjugada $\{|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}\}$. Com respeito a essa base, o operador Z leva o estado $|+\rangle$ ao estado $|-\rangle$ e vice-versa, isto é, este operador atua como se fosse um operador bit-flip em relação aos símbolos $+$ e $-$. Assim, todas as operações de codificação, detecção e correção de erros, podem ser executadas exatamente como no canal bit-flip, porém, em relação à base $\{|+\rangle, |-\rangle\}$, ao invés da base $\{|0\rangle, |1\rangle\}$. Usando este mesmo procedimento para os CCQs, a operação de codificação (1), descrita para um canal bit-flip pode ser escrita para um canal na base $\{|0\rangle, |1\rangle\}$ como:

$$0 \bigotimes_{t=0}^{+\infty} | \, u_t\rangle \rightarrow \bigotimes_{t=0}^{+\infty} | \, v_t\rangle \tag{2}$$

onde

$$v_t = \frac{1}{2}(|0\rangle + (-1)^{(u_t+u_{t-2})}|1\rangle)(|0\rangle + (-1)^{(u_t+u_{t-1}+u_{t-2})}|1\rangle).$$

Esta operação é denominada forma *compacta* (a palavra-código sempre pode ser escrita como um produto tensorial de blocos como este). Todavia, a operação mostrada a seguir, é denominada forma *explícita*, ou equivalentemente,

$$v_t = \frac{1}{2}\Sigma^{(1,1)}_{(p_t,q_t)=(0,0)}(-1)^{(u_t+u_{t-2})p_t+(u_t+u_{t-1}+u_{t-2})q_t}|p_t, q_t\rangle$$

onde $u_{-1} = u_{-2} = 0$. Ambas as formas são equivalentes, mas para um CCQ e um canal quântico com erro geral, a forma compacta é mais útil para o entendimento da operação de decodificação e a forma explícita, mais útil para o entendimento da operação de geração.

Evidentemente, este CCQ também está associado ao CCC com matriz geradora $\mathbf{G}(D) = [1 + D^2, 1 + D + D^2]$ e, consequentemente, é um código não catastrófico com capacidade de correção de até dois erros quaisquer do tipo Z. Através da tabela do arranjo padrão, pode-se mostrar que alguns padrões com mais de dois erros Z também poderão ser corrigidos.

A natureza convolucional esta explícita nos bits presentes dentro dos kets do código CCQ para o canal bit-flip. Todavia, para o canal phase-flip, a natureza convolucional aparece, de forma sutil, na distribuição dos *sinais* positivos/negativos em frente aos kets do código CCQ.

C. CCQ para o canal quântico com erro geral

Após a construção dos dois códigos quânticos, $\mathcal{C}_1$ e $\mathcal{C}_2$, capazes de corrigir erros de fase Z e de bit X, respectivamente, para um mesmo conjunto de registros quânticos, estamos praticamente prontos para concatena-los, obtendo o código concatenado $\mathcal{C}$.

Para que $\mathcal{C}_2$ possa ser concatenado a $\mathcal{C}_1$, devemos antes construir um código equivalente a $\mathcal{C}_1$ com taxa $2/4$. A opção mais simples para esta tarefa é utilizar a matriz geradora

$$G_{\mathcal{C}_1} = \begin{bmatrix} 11 & 01 & 11 & & & \\ & 11 & 01 & 11 & & \\ & & 11 & 01 & 11 & \\ & & & \ddots & \ddots & \ddots \end{bmatrix},$$

que é a matriz discreta semi-infinita associada à matriz $\mathbf{G}(D) = [1 + D^2, 1 + D + D^2]$, usada na construção de $\mathcal{C}_1$. Agora, dois bits entrarão no codificador a cada instante de tempo e cada registro de deslocamento conterá apenas uma memória de modo que o número total de memórias permaneça o mesmo que de $\mathcal{C}_1$. Assim, o código equivalente a $\mathcal{C}_2$ com taxa $2/4$ será construído a partir da matriz geradora $G_{\mathcal{C}_1}$, escrita na forma:

$$G_{\mathcal{C}_2} = \begin{bmatrix} 1101 & 1100 & & & & \\ 0011 & 0111 & & & & \\ & 1101 & 1100 & & & \\ & 0011 & 0111 & & & \\ & & 1101 & 1100 & & \\ & & 0011 & 0111 & & \\ & & & \ddots & \ddots & \ddots \end{bmatrix}.$$

Com isso, a operação de codificação quântica para o código $\mathcal{C}_2$ $[4,2,1]$ será:

$$\bigotimes_{t=0}^{+\infty} | \, u_t\rangle \rightarrow \bigotimes_{t=0}^{+\infty} | \, v_t\rangle \tag{3}$$

onde

$$v_t = (u_t^1 + u_{t-1}^1, u_t^1 + u_{t-1}^1 + u_{t-1}^2, u_t^2 + u_{t-1}^2, u_t^2 + u_{t-1}^2 + u_t^1),$$

e u_t^1, $u_t^2 \in \{0,1\}$ e $u_{-1} = u_{-2} = 0$.

Esta codificação quântica é a equivalente trivial com taxa $2/4$ e memória unitária da operação (1). Devido a essa equivalência, a capacidade de correção do novo código é a mesma, ou seja, é possível garantir com $\mathcal{C}_2$ $[4,2,1]$ a correção de qualquer grupo com até dois erros X.

Concatenando-se os CCCs $(2,1,2)$ e $(4,2,1)$, respectivamente, associados aos CCQs $\mathcal{C}_1$ $[2,1,2]$ e $\mathcal{C}_2$ $[4,2,1]$, obtemos um novo CCC, com taxa $R = 1/4$ e matriz geradora dada por.

$$G_{\mathcal{C}} = \begin{bmatrix} 1110 & 1000 & 1001 & 1011 & & & \\ & 1110 & 1000 & 1001 & 1011 & & \\ & & 1110 & 1000 & 1001 & 1011 & \\ & & & 1110 & 1000 & 1001 & 1011 \\ & & & \ddots & \ddots & \ddots & \ddots \end{bmatrix}.$$

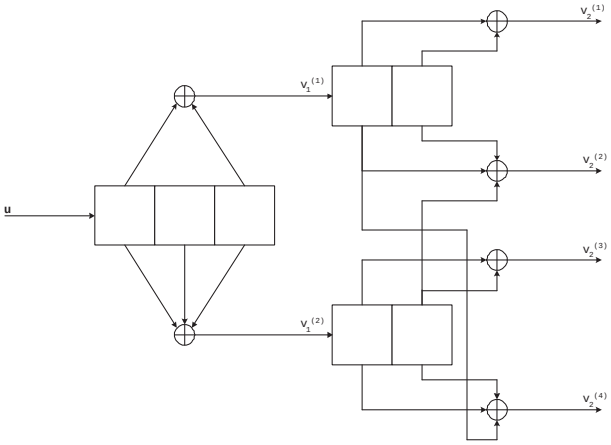

Fig. 1. Concatenação dos codificadores (2,1,2) e (4,2,1)

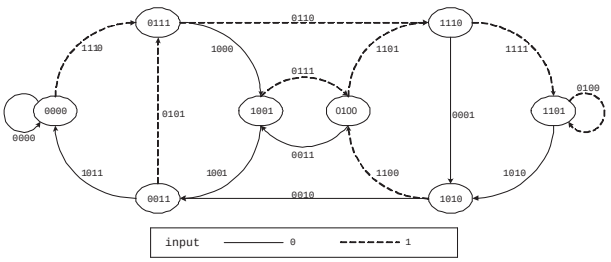

Fig. 2. Diagrama de estados para o CCC (4,1,3)

O codificador deste CCC concatenado pode ser visualizado na Figura 1, [3].

Este codificador concatenado não catastrófico possui três memórias *efetivas*, duas do primeiro codificador e uma do segundo. Assim, apenas oito estados (e não dezesseis, como poderia sugerir o número total de memórias do codificador) são gerados por este codificador. Tal fato pode ser observado através do seu diagrama de estados, apresentado na Figura 2.

É fácil verificar neste diagrama de estados que são necessárias pelo menos quatro transições para sair do estado 0000 e retornar ao mesmo estado. Este também é o caminho que atinge o valor de $d_{free} = 9$.

O CCC $(4, 1, 3)$ pode ser usado na construção de um CCQ $[4, 1, 3]$ com capacidade de correção de um erro quântico geral em qualquer dos qubits da palavra-código quântica. Isto porque três condições são satisfeitas:

1) O CCC $(2, 1, 2)$ associado a $\mathcal{C}_1$ $[2, 1, 2]$, garante a correção de um erro quântico Z;
2) O CCC $(4, 2, 1)$, associado a $\mathcal{C}_2$ $[4, 2, 1]$, garante a correção de um erro quântico X;
3) O CCC $(4, 1, 3)$, associado à concatenação de $\mathcal{C}_2$ $[4, 2, 1]$ a $\mathcal{C}_1$ $[2, 1, 2]$, garante a correção de quatro erros. Estes erros clássicos estão associados aos erros quânticos $Z, X, Y(= XZ)$ e I, que constituem a base para um erro quântico geral.

Como os dígitos de entrada de $\mathcal{C}_2$ $[4, 2, 1]$ são provenientes da saída de $\mathcal{C}_1$ $[2, 1, 2]$, o código resultante desta concatenação, é o CCQ com taxa $R = 1/4$. Definindo o número de *memórias quânticas* como sendo $m = T - 1$, ver [3], onde T é o número de transições de unidades de tempo necessárias para a obtenção de uma palavra-código quântica válida, segue que a memória do CCQ concatenado é $m = 3$, equivalentemente, um CCQ $[4, 1, 3]$.

A operação de codificação do CCQ concatenado para um canal quântico com erro geral pode agora ser convenientemente escrita na base $\{|0\rangle, |1\rangle\}$ como:

$$\bigotimes_{t=0}^{+\infty} | u_t\rangle \rightarrow \bigotimes_{t=0}^{+\infty} | v_t\rangle \qquad (4)$$

onde

$$v_t = \frac{1}{2}\Sigma^{(1,1)}_{(p_t,q_t)=(0,0)}(-1)^{(u_t+u_{t-2})p_t+(u_t+u_{t-1}+u_{t-2})q_t} w_t,$$

com $w_t = |p_t + p_{t-1}, p_t + p_{t-1} + q_{t-1}, q_t + q_{t-1} + p_t\rangle$ e $u_{-1} = u_{-2} = 0$ e $p_{-1} = q_{-1} = 0$.

Foi necessário utilizar dois codificadores clássicos para este procedimento, pois o erro geral deste canal quântico possui dois geradores, Z e X.

Como o d_{free} do CCC associado é nove, o CCQ não corrige mais que um erro além do geral, o que nos leva a concluir que a distância quântica é três. Além disso, como os CCCs $(2, 1, 2)$, $(4, 2, 1)$ e $(4, 1, 3)$ são não-catastróficos, segue que o CCQ $[4, 1, 3]$ associado também é um código não-catastrófico.

Almeida, [3], ressalta que, para a construção de um CCQ que corrija apenas um erro X ou apenas um erro Z, é necessário um CCC mais simples, de memória unitária, como por exemplo, $\mathbf{G}(D) = [1 + D, D]$, com $d_{free} = 3$. Porém, este CCC quando concatenado a um equivalente com taxa $R = 2/4$ gera um CCC com $d_{free} < 9$ e, assim, o CCQ, associado à concatenação, não garantiria a correção de um erro quântico geral.

III. Aplicando Transformações no CCC (4,1,3)

Utilizaremos o código CCQ $[4, 1, 3]$ como referência no processo de aplicação das funções armadilhas.

Para aplicar as transformações armadilha no CCC (4,1,3) procedemos da seguinte maneira: primeiramente, aplicamos as transformações armadilhas A (pela esquerda) e B (pela direita) somente ao código $\mathcal{C}_2$, gerado pela matriz $G_{\mathcal{C}_2}$, isto é, $A.G_{\mathcal{C}_2}.B = G_{\mathcal{C}'_2}$ resultando no código $\mathcal{C}'_2$. Em seguida obtemos o valor da distância livre associada. A transformação armadilha A consiste da matriz identidade de ordem 2×2 e as transformações armadilhas B utilizadas são aquelas provenientes das representações matriciais dos elementos do grupo de permutações com 8 elementos.

Após a obtenção do código $\mathcal{C}'_2$, $G_{\mathcal{C}'_2}$, concatenamos tal código ao código $\mathcal{C}_1$, $G_{\mathcal{C}_1}$, dando origem ao código concatenado $\mathcal{C}'$, $G_{\mathcal{C}'} = G_{\mathcal{C}_1}.G_{\mathcal{C}'_2}$.

Os resultados das aplicações podem ser observados na Tabela I, onde são mostradas a permutação associada à transformação armadilha B, denotada como ρ, as submatrizes G'_0 e G'_1 do código ($\mathcal{C}'_2$ código este resultante da

aplicação das transformações armadilhas no código $\mathcal{C}_2$), d' distância livre do código resultante, e o símbolo $*$ denota que o código é catastrófico.

Além disso, $G_{C'}$ denota a matriz geradora do código clássico concatenado. Esta matriz é representada da seguinte forma:

$$G_{C'} = [G_0; G_1; G_2; G_3];$$

O ponto e vírgula separam as submatrizes geradoras. Como um exemplo, considere a matriz

$$G_{C'} = [1110 \quad 1000 \quad 1001 \quad 1011].$$

sua representação octal é dada por:

$$G_{C'} = [16; 10; 11; 13].$$

Há também na Tabela I, uma coluna com $d'(C')$, denotando a distância livre do código clássico concatenado resultante.

Observando a Tabela I, notamos que a maioria das transformações aplicadas ao código $\mathcal{C}_2$ manteve $d_{free} = 5$, porém em alguns casos houve decréscimo para 4 e 3 bem como conduzindo a códigos catastróficos.

Ao concatenarmos o código $\mathcal{C}_1$ com o código resultante $\mathcal{C}_2'$ obtemos o código clássico concatenado $\mathcal{C}'$ com taxa $R = 1/4$ e mesma quantidade de memórias $m = 3$ do código concatenado clássico original, $\mathcal{C}$.

Como conseqüência, obtivemos os seguintes resultados tabulados na Tabela I (última coluna): a maioria dos códigos resultantes mantiveram o valor da distância livre, igual a 9; em quatro casos houve o decréscimo na distância livre; e nos demais casos houve um aumento no valor da distância livre para os valores 10 e 11.

Concluímos que, através do processo de aplicação das transformações armadilhas ao código $\mathcal{C}_2$ e concatenando-o com o código $\mathcal{C}_1$, podemos encontrar códigos clássicos concatenados com maior capacidade de correção de erros quando comparado ao código clássico concatenado original.

Ao analisar os resultados encontrados na Tabela I, percebemos que não há uma relação direta entre o d_{free} do código $\mathcal{C}_2'$ e o d_{free} do código concatenado $\mathcal{C}'$ obtido, pois podemos encontrar situações em que $d' = 5$ resulta em um $d(\mathcal{C}') = 7$ ou 10 sendo que em sua maioria é igual a 9. Porém, observamos que em todos os casos em que o código $\mathcal{C}_2'$ é catastrófico (denotado na Tabela I por *), o $d'(C')$ aumenta.

Dos novos CCCs concatenados podemos obter os CCQs concatenados associados como descrito na Seção II-C.

TABELA I
TRANSFORMAÇÃO PERMUTAÇÃO APLICADA AO CCC CONCATENADO.

ρ	G_0'	G_1'	d'	$G_{C'}$	$d'(C')$
id	15:03	14:07	5	16;10;11;13	9
(5286374)	11:06	13:07	5	17;12;10;14	9
(21564)(38)	15:02	14:17	3	17;01;00;03	7
(425)	15:02	14:17	3	17;01;00;03	7
(31278465)	13:05	05:13	*	16;13;05;16	11
(61)(42)(7358)	17:14	04:13	3	03;03;17;10	8
(213874)(56)	05:12	16:13	3	17;17;04;05	10
(81674523)	11:16	13:06	5	07;03;01;15	9
(526874)	15:06	12:07	5	13;13;14;15	10
(61387)(52)	05:16	16:03	4	13;03;10;15	9
(3162574)	16:11	06:13	5	07;04;14;15	9
(51827364)	03:16	15:06	5	15;05;13;13	9
(2164)(73)(58)	15:12	05:16	5	07;01;06;06	9
(413865)(72)	01:16	02:17	3	17;10;06;06	9
(4257)(836)	17:02	02:17	*	15;17;02;15	10
(417328)(65)	03:14	15:13	5	17;12;04;06	9
(215678)(43)	16:03	11:16	4	15;04;03;07	9
(71583)(62)	15:07	06:11	5	12;10;03;17	9
(214738)(56)	14:13	15:06	5	07;00;01;13	7
(21743658)	06:13	07:12	*	15;06;07;15	11

IV. APLICANDO A TRANSFORMAÇÃO DE PERMUTAÇÃO AOS NOVOS CCCS (4,1,3)

Como visto na seção anterior, ao aplicarmos as transformações armadilha às submatrizes geradoras do código $\mathcal{C}_2$ com o objetivo de encontrar códigos concatenados com capacidade de correção menor que a do código original, geramos alguns códigos com maior poder de correção de erros.

Esses novos códigos com capacidade de correção maior que o original serão agora utilizados no processo de codificação e então, novas transformações serão aplicadas a $\mathcal{C}_2$ para que possamos obter d_{free} menores no CCC obtido após a concatenação, e a partir disso utilizar o CCC concatenado resultante no sistema criptográfico.

Nas Tabelas II, III e IV, o símbolo $*$ denota código catastrófico. Em todos os casos, a transformação armadilha A utilizada, foi a matriz identidade.

A. Código CCC_1

Considere o CCC_1 $(4, 1, 3)$ com matriz geradora semi-infinita dada por

$$GC_1 = \begin{bmatrix} 1101 & 0110 & 0111 & 1101 & & \\ & 1101 & 0110 & 0111 & 1101 & \\ & & 1101 & 0110 & 0111 & 1101 \\ & & \ddots & \ddots & \ddots & \ddots \end{bmatrix},$$

resultante da concatenação dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$. Este CCC concatenado tem $d_{free} = 11$ e, portanto, tem capacidade para corrigir até cinco erros clássicos.

As matrizes geradoras semi-infinitas dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ são dadas, respectivamente, por:

$$G_{\mathcal{C}_1} = \begin{bmatrix} 11 & 01 & 11 & & & \\ & 11 & 01 & 11 & & \\ & & 11 & 01 & 11 & \\ & & & \ddots & \ddots & \ddots \end{bmatrix}$$

e

$$G_{\mathcal{C}_2} = \begin{bmatrix} 0110 & 0111 & & & \\ 1011 & 1010 & & & \\ & 0110 & 0111 & & \\ & 1011 & 1010 & & \\ & & 0110 & 0111 & \\ & & 1011 & 1010 & \\ & & & \ddots & \ddots \end{bmatrix},$$

onde $\mathcal{C}_1$ tem $d_{free} = 5$ e $\mathcal{C}_2$ é um código catastrófico. Aplicando as transformações armadilha ao novo código $\mathcal{C}_2$ obtemos os resultados apresentados na Tabela II.

A Tabela II apresenta a permutação associada a transformação armadilha B, denotada como ρ, as submatrizes G'_0 e G'_1 do código $\mathcal{C}'_2$ código resultante da aplicação das transformações armadilhas ao código $\mathcal{C}_2$, a distância livre do código resultante, denotado por d', G_C, matriz geradora do CCC concatenado e $d'(C)$, a distância livre do CCC concatenado resultante.

Como pode ser observado na Tabela II, após aplicarmos as transformações de permutação ao código $\mathcal{C}_2$, obtemos os seguintes resultados: manutenção do $d' = 11$, e a diminuição do d' para 10 e 9 nos demais casos.

TABELA II
TRANSFORMAÇÃO PERMUTAÇÃO APLICADA AO NOVO CCC_1 CONCATENADO.

ρ	G'_0	G'_1	d'	G_C	$d'(C)$
id	06:13	07:12	$*$	15;06;07;15	11
(2143)(657)	03:15	13:14	5	16;12;02;07	9
(8142367)	07:14	06:15	$*$	13;07;06;13	11
(4123)(76)	14:07	07:14	$*$	13;14;07;13	11
(815)(62)(37)	06:13	16:03	$*$	15;06;16;15	11
(82576)	02:17	17:10	2	15;10;05;07	9
(6185)(42)(37)	13:06	12:07	$*$	15;13;12;15	11
(21375)(68)	12:17	15:02	3	05;00;07;17	9
(218)(756)	12:07	15:06	5	15;14;13;13	10
(5138)(247)	13:15	06:11	4	06;02;17;17	10

A obtenção dos CCQs equivalentes aos CCCs segue os mesmos procedimentos realizados na Seção II.

B. Código CCC_2

Considere agora CCC_2 $(4, 1, 3)$. Este código possui matriz geradora semi-infinita dada por

$$GC_2 = \begin{bmatrix} 1101 & 1111 & 0010 & 1101 & & \\ & 1101 & 1111 & 0010 & 1101 & \\ & & 1101 & 1111 & 0010 & 1101 \\ & & & \ddots & \ddots & \ddots \end{bmatrix}.$$

O CCC concatenado foi obtido a partir da concatenação dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ e tem $d_{free} = 10$.

As matrizes geradoras semi-infinitas dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ são dadas, respectivamente, por:

$$G_{\mathcal{C}_1} = \begin{bmatrix} 11 & 01 & 11 & & \\ & 11 & 01 & 11 & \\ & & 11 & 01 & 11 \\ & & \ddots & \ddots & \ddots \end{bmatrix}$$

e

$$G_{\mathcal{C}_2} = \begin{bmatrix} 0110 & 0111 & & & \\ 1011 & 1010 & & & \\ & 0110 & 0111 & & \\ & 1011 & 1010 & & \\ & & 0110 & 0111 & \\ & & 1011 & 1010 & \\ & & & \ddots & \ddots \end{bmatrix},$$

onde $\mathcal{C}_1$ tem $d_{free} = 5$ e $\mathcal{C}_2$ é um código catastrófico. Aplicamos as transformações armadilha de permutação no novo código $\mathcal{C}_2$ obtendo os resultados apresentados na Tabela III.

Na Tabela III apresentamos a permutação associada a transformação armadilha B, denotada ρ, as submatrizes G'_0 e G'_1 do código $\mathcal{C}'_2$ (que é o código resultante da aplicação das transformações armadilhas no código $\mathcal{C}_2$) e a distância livre do código resultante, d'. G_C, é a matriz geradora do CCC concatenado e $d'(C)$ é a distância livre do CCC concatenado resultante.

Após efetuar a aplicação das transformações armadilha ao CCC_2 os seguintes resultados foram obtidos:

1) O d'_{free} do código resultante permaneceu igual ao d_{free} do código original, ou seja, o novo código é capaz de corrigir até quatro erros clássicos;
2) Houve uma diminuição no valor do d'_{free}, de 10 para 9. Mesmo assim, continuou com a mesma capacidade de correção, isto é, pode corrigir até quatro erros clássicos;
3) O valor do d'_{free} do código obtido é 8, havendo uma redução na capacidade de correção de erros do código.
4) Como aconteceu com o CCC concatenado $(4, 1, 3)$, apresentado na Seção III, houve um aumento no valor do d'_{free} do novo código, passando de 10 para 11. Com isso, o novo CCC concatenado tem a capacidade de corrigir até 5 erros clássicos.

TABELA III
TRANSFORMAÇÃO PERMUTAÇÃO APLICADA AO NOVO CCC_2 CONCATENADO.

ρ	G'_0	G'_1	d'	G_C	$d'(C)$
id	17:02	02:17	$*$	15;17;02;15	10
(2143)(657)	17:01	10:17	2	16;06;01;07	9
(8142367)	15:06	05:16	$*$	13;15;05;13	11
(4123)(76)	17:04	02:17	$*$	13;17;04;13	10
(815)(62)(37)	03:16	07:12	$*$	13;03;07;15	11
(82576)	13:06	11:16	5	15;01;03;07	9
(21375)(68)	17:12	10:07	3	05;05;03;17	8
(5138)(247)	15:13	12:05	5	06;04;03;17	9

A obtenção dos CCQs equivalentes aos CCCs segue os mesmos procedimentos realizados na Seção II.

C. Código CCC_3

Considere o código CCC_3 $(4, 1, 3)$ com matriz geradora semi-infinita dada por

$$GC_3 = \begin{bmatrix} 1110 & 1011 & 0101 & 1110 & & \\ & 1110 & 1011 & 0101 & 1110 & \\ & & 1110 & 1011 & 0101 & 1110 \\ & & & \ddots & \ddots & \ddots \end{bmatrix}.$$

Este CCC_3 concatenado foi obtido a partir da concatenação dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ e apresenta $d_{free} = 11$.

As matrizes geradoras semi-infinitas dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ são dadas, respectivamente, por:

$$G_{\mathcal{C}_1} = \begin{bmatrix} 11 & 01 & 11 & & \\ & 11 & 01 & 11 & \\ & & 11 & 01 & 11 \\ & & \ddots & \ddots & \ddots \end{bmatrix}$$

e

$$G_{\mathcal{C}_2} = \begin{bmatrix} 1011 & 0101 & & & \\ 0101 & 1011 & & & \\ & 1011 & 0101 & & \\ & 0101 & 1011 & & \\ & & 1011 & 0101 & \\ & & 0101 & 1011 & \\ & & & \ddots & \ddots \end{bmatrix},$$

sendo que $\mathcal{C}_1$ possui $d_{free} = 5$ e $\mathcal{C}_2$ é um código catastrófico. Aplicando as transformações armadilha de permutação ao novo código $\mathcal{C}_2$ obtemos os resultados mostrados na Tabela IV.

Na Tabela IV, apresentamos a permutação associada à transformação armadilha B, denotada como ρ, as submatrizes G'_0 e G'_1 do código $\mathcal{C}'_2$ código resultante da aplicação das transformações armadilhas no código $\mathcal{C}_2$, a distância livre do código resultante, representada por d'. G_C, a matriz geradora do CCC concatenado e a distância livre do CCC concatenado resultante, denotada $d'(C)$.

Após aplicar as transformações armadilha ao CCC_3, obtivemos os seguintes resultados:

1) O d' do código resultante permaneceu igual ao d_{free} do código original, sendo capaz de corrigir até cinco erros clássicos;
2) Houve uma diminuição no valor do d', de 11 para 10, e de 11 para 9 em outros casos;
3) O valor do d' do novo código passou a ser igual a 9, o que o torna capaz de corrigir até quatro erros clássicos;
4) O valor do d'_{free} do código obtido foi igual a 7, havendo uma redução na capacidade de correção de erros do código, ou seja, o novo código é capaz de corrigir até três erros clássicos.

A obtenção dos CCQs equivalentes aos CCCs segue os mesmos procedimentos realizados na Seção II.

V. Conclusões

Neste artigo apresentamos o CCQ $[4, 3, 1]$ associado ao CCC $(4, 3, 1)$ com $d_{free} = 9$. Este CCQ é obtido a partir do código CCC resultante da concatenação do código $\mathcal{C}_1$ $(2, 1, 2)$ com o código $\mathcal{C}_2$ $(4, 2, 1)$. As transformações armadilhas (permutações) foram aplicadas ao código $\mathcal{C}_2$ $(4, 2, 1)$, obtendo novos CCCs $\mathcal{C}'_2$. Em seguida, concatenamos os CCCs $\mathcal{C}'_2$ com o CCC $\mathcal{C}_1$ $(2, 1, 2)$. Novos CCCs $(4, 3, 1)$ concatenados foram obtidos. Como consequência alguns desses códigos mantiveram o valor da distância livre, outros diminuiram e outros surpreendentemente aumentaram o valor do d_{free} do código concatenado original. Em geral, esse resultado foi obtido com a utilização na concatenação de um dos códigos sendo catastrófico.

Acreditamos que o objetivo proposto pela aplicação das transformações armadilha foi alcançado. Além disso, obtivemos bons códigos concatenados com capacidade de correção maior que o do código CCC $(4, 3, 1)$. Consequentemente, os novos CCCs $(4, 3, 1)$ estão associados aos novos CCQs $[4, 3, 1]$.

TABELA IV

Transformação permutação aplicada ao novo CCC_3 concatenado.

ρ	G'_0	G'_1	d'	G_C	$d'(C)$
id	13:05	05:13	$*$	16;13;05;16	11
(2143)(657)	15:12	03:15	4	07;04;12;16	9
(8142367)	16:11	03:16	4	07;04;11;15	9
(4123)(76)	17:12	03:15	5	15;04;00;16	7
(815)(62)(37)	05:13	13:14	4	16;14;02;07	9
(82576)	13:05	06:15	5	16;16;03;13	10
(6185)(42)(37)	14:17	16:01	3	03;00;02;17	7
(21375)(68)	15:03	05:16	5	16;10;00;13	7
(218)(756)	17:11	10:07	3	06;06;01;17	9
(5138)(247)	16:07	14:03	5	11;10;12;17	9

Referências

[1] N. Gisin et al, *Rev. Mod. Phys.*, vol. 74, 145, (2002).

[2] J. L. Massey. Catastrophic error-propagation in convolutional codes. Proc. of the 11th Midwest Symp. Cir. Th., pages 583 – 587, Notre Dame, IN, 1968.

[3] A. C. A. de Almeida, *Códigos Convolucionais Quânticos Concatenados*, Tese de Doutorado, Universidade Estadual de Campinas (UNICAMP), Brasil, Outubro de 2004.

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

[5] P. A. Santos, *Uma Proposta de um Sistema Criptográfico Utilizando Códigos Convolucionais Clássicos e Quânticos.*, Dissertação de mestrado, Universidade Estadual de Campinas (UNICAMP), Brasil, Julho de 2008.