Códigos Convolucionais Quânticos Derivados de Códigos Algébrico-Geométricos

Francisco Revson F. Pereira, Giuliano G. La Guardia, Francisco M. de Assis

***Resumo*— Neste artigo, novas famílias de códigos convolucionais quânticos são construídas a partir de códigos algébrico-geométricos (AG). Os códigos convolucionais quânticos apresentados são novos no sentido que seus parâmetros são diferentes dos parâmetros dos códigos disponíveis na literatura. Em particular, uma família de códigos com máxima distância de separação é apresentada.**

***Palavras-Chave*— Códigos Convolucionais Quânticos, Códigos Algébrico-Geométricos, Construção Algébrica de Códigos.**

I. Introdução

A Teoria de Códigos Convolucionais Quânticos (QCC, do inglês *Quantum Convolutional Codes*) foi introduzida recentemente na literatura pelos trabalhos de Ollivier e Tillich [1, 2]. Da mesma forma que para códigos de bloco quânticos, a descrição de tais códigos foi feita por meio de estabilizadores do código. Construções de códigos convolucionais quânticos tem sido feitas em alguns trabalhos da literatura [1–11].

Entretanto, é difícil construir novos QCC's que tenham máxima distância de separação (MDS), visto as necessidades que o código clássico deve possuir. De fato, há poucos trabalhos existentes na literatura que trabalham com a construção de tais códigos ótimos. Nas Refs. [11–13], o autor constrói códigos convolucionais quânticos MDS de comprimento $n = q + 1$ ou $n = \frac{(q+1)}{2}$ (no último caso, $q \equiv 3 \bmod 4$) sobre $\mathbb{F}_q$. Outro exemplo é dado na Ref. [7], na qual QCC's MDS, sobre $\mathbb{F}_q$, tem comprimento $n|(q^2-1)$ e $q+1 < n \leq q^2-1$.

Existe outra família de códigos de bastante interesse devido suas descrições e características matemáticas, essa é a classe de códigos algébrico-geométricos (AG). Foi introduzida por Goppa [14] em 1981 e teve seu principal foco de interesse quando Tsfasman, Vladut e Zink mostraram que existia uma família de códigos AG com taxas não-triviais que ultrapassavam o limitante de Gilbert-Varshamov [15]. Por isso, o interesse em códigos AG levou ao desenvolvimento de diversos trabalhos [16–21]. Entretanto, para o conhecimento dos autores deste artigo, nenhum trabalho na literatura aborda a utilização de códigos AG para a construção de códigos convolucionais quânticos.

Neste trabalho, são construídas três famílias de códigos convolucionais quânticos de memória unitária por meio da utilização dos códigos convolucionais clássicos derivados de códigos AG apresentado no trabalho de Pereira *et al.* [22] no método de criação de códigos QCC de Aly *et al.* [6]. Mais especificadamente, este método usa o método de criação de códigos convolucionais a partir de códigos AG apresentado em [22] e, posteriormente, utiliza-os no método de Aly *et al.* [6] para construir QCC's. Uma vantagem da técnica utilizada aqui está no fato de que os dois métodos utilizados geram códigos de forma algébrica e não por procura computacional. Assim, novas famílias de códigos convolucionais quânticos são construídas, e não apenas códigos específicos. Assim, neste contexto, este trabalho apresenta contribuições relevantes, visto que, como será mostrado posteriormente, uma família de códigos QCC aqui apresentada é MDS.

O trabalho está organizado da seguinte forma. Na Seção II, são revisados os conceitos básicos sobre códigos convolucionais clássicos e quânticos. Na Seção III, uma recapitulação dos conceitos relativos aos códigos algébrico-geométricos é feita. Na Seção IV, é proposto um método de construção de novos códigos convolucionais quânticos derivados de códigos AG. Em particular, é mostrado que pelo menos uma das famílias aqui construídas de códigos convolucionais quânticos é MDS (no sentido do limitante de Singleton quântico generalizado). Na Seção V, alguns parâmetros numéricos das famílias de códigos que foram construídos são expostos. Finalmente, na Seção VI, as considerações finais do trabalho são dadas.

II. Revisão de Códigos Convolucionais Clássicos e Quânticos

Ao longo deste trabalho, p denota um número primo, q uma potência de primo, $\mathbb{F}_q$ um corpo finito com q elementos e $F/\mathbb{F}_q$ denota o corpo de funções algébricas sobre $\mathbb{F}_q$ de gênero g.

Nesta seção é apresentada uma breve revisão de códigos clássicos convolucionais. Para mais detalhes veja [6, 7, 23–26].

Uma matriz polinomial de codificação

$$G(D) \in \mathbb{F}_q[D]^{k\times n} \tag{1}$$

é denominada *básica* se $G(D)$ tem uma inversa polinomial à esquerda. Uma matriz geradora básica é dita ser reduzida (ou minimal [26–28]) se o comprimento de restrição, dado por

$$\gamma := \sum_{i=1}^{k} \gamma_i, \tag{2}$$

possui o menor valor possível entre todas as matrizes geradoras básicas (neste contexto, o comprimento de restrição γ é chamado de grau do correspondente código).

Francisco Revson F. Pereira é doutorando no Programa de Pós-Graduação em Engenharia Elétrica, PPgEE/UFCG, E-mail: francisco.pereira@ee.ufcg.edu.br.

Giuliano G. La Guardia é professor do Departamento de Matemática e Estatística na Universidade Estadual de Ponta Grossa, E-mail: gguardia@uepg.br

Francisco M. de Assis é professor do Departamento de Engenharia Elétrica na Universidade Federal de Campina Grande, E-mail: fmarcos@dee.ufcg.edu.br.

Definição 1: [7] Um código convolucional C com parâmetros $(n, k, \gamma;\ m, d_f)_q$ é um submódulo de $\mathbb{F}_q[D]^n$ gerado pela matriz reduzida

$$G(D) := (g_{ij}) \in \mathbb{F}_q[D]^{k\times n}, \tag{3}$$

isto é,

$$C := \{\mathbf{u}(D)G(D) | \mathbf{u}(D) \in \mathbb{F}_q[D]^k\}, \tag{4}$$

em que n é o comprimento, k é a dimensão, $\gamma = \sum_{i=1}^{k} \gamma_i$ é o grau, com $\gamma_i := \max_{1\leq j\leq n} \{\deg g_{ij}\}$, $m := \max_{1\leq i\leq k}\{\gamma_i\}$ é a memória e $d_f := wt(C) = \min\{wt(\mathbf{v}(D)) \mid \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}$ é a distância livre do código. Lembrando que o peso de um elemento $\mathbf{v}(D) \in \mathbb{F}_q[D]^n$ é definido como

$$wt(\mathbf{v}(D)) := \sum_{i=1}^{n} wt(v_i(D)), \tag{5}$$

em que $wt(v_i(D))$ é o número dos coeficientes não-nulos de $v_i(D)$.

Seja $\mathbb{F}_q((D))$ o corpo de séries de Laurent, sobre $\mathbb{F}_q$, no qual os elementos são dados por

$$\mathbf{u}(D) = \sum\nolimits_i u_i D^i, \tag{6}$$

em que $u_i \in \mathbb{F}_q$ e $u_i = 0$ para $i \leq r$, para algum $r \in \mathbb{Z}$. O peso de $\mathbf{u}(D)$ é definido como

$$wt(\mathbf{u}(D)) = \sum\nolimits_{\mathbb{Z}} wt(u_i). \tag{7}$$

Uma matriz geradora $G(D)$ é chamada de catastrófica se existe algum $\mathbf{u}(D)^k \in \mathbb{F}_q((D))^k$ de peso de Hamming infinito tal que $\mathbf{u}(D)^k G(D)$ tem peso de Hamming finito. Desde que uma matriz geradora básica seja não-catastrófica, o código convolucional construído neste trabalho terá matriz geradora não-catastrófica.

O produto interno euclidiano de duas n-uplas

$$\mathbf{u}(D) = \sum\nolimits_i \mathbf{u}_i D^i \tag{8}$$

e

$$\mathbf{v}(D) = \sum\nolimits_j \mathbf{u}_j D^j \tag{9}$$

em $\mathbb{F}_q[D]^n$ é definido por

$$\langle \mathbf{u}(D) \mid \mathbf{v}(D)\rangle = \sum\nolimits_i \mathbf{u}_i \cdot \mathbf{v}_i. \tag{10}$$

Se C é um código convolucional, então o código

$$C^{\perp} := \{\mathbf{u}(D) \in \mathbb{F}_q[D]^n \mid \langle \mathbf{u}(D) \mid \mathbf{v}(D)\rangle = 0, \forall \mathbf{v}(D) \in C\} \tag{11}$$

denota seu dual euclidiano.

A. Códigos Convolucionais Quânticos Derivados de Códigos de Convolucionais Clássicos

No início desta seção é descrito brevemente o conceito de códigos convolucionais quânticos. Para mais detalhes, o leitor deve consultar [2].

Um QCC é definido por meio de seu estabilizador, o qual é um subgrupo da versão infinita do grupo de Pauli, que consiste do produto tensorial de matrizes de Pauli generalizadas atuando sobre uma sequência semi-infinita de dígitos quânticos (qudits). O estabilizador pode ser definido por uma matriz estabilizadora da forma

$$S(D) = (X(D) \mid Z(D)) \in F_q[D]^{(n-k)\times 2n}$$

satisfazendo $X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$ (ortogonalidade simplética). Mais precisamente, considere um QCC C definido pela matriz estabilizadora de posto completo $S(D)$ dada anteriormente. Então C é um código com taxa k/n e parâmetros $[(n, k, m; \gamma, d_f)]_q$, com n sendo o tamanho da sequência de saída, k o número de qudits lógicos por sequência de saída, $m = \max_{1\leq i\leq n-k, 1\leq j\leq n}\{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$ é a memória, d_f é a distância livre e γ é o grau do código. Os índices de Forney são definidos como sendo $\gamma_i = \max_{1\leq j\leq n}\{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$ e o grau por $\gamma = \sum_{i=1}^{n-k} \gamma_i$.

Um código convolucional quântico pode também ser descrito em termos da matriz estabilizadora semi-infinita S com entradas em $\mathbb{F}_q \times \mathbb{F}_q$. De fato, se $S(D) = \sum_{i=0}^{m} G_i D^i$, com cada matriz G_i, para todo $i = 0, \ldots, m$, é uma matriz de tamanho $(n - k) \times n$, então a matriz semi-infinita é definida como

$$S = \begin{bmatrix} G_0 & G_1 & \ldots & G_m & 0 & \ldots & \ldots & \ldots \\ 0 & G_0 & G_1 & \ldots & G_m & 0 & \ldots & \ldots \\ 0 & 0 & G_0 & G_1 & \ldots & G_m & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

O modelo dos erros é caracterizado da seguinte forma. Considere o espaço de Hilbert $\mathcal{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$ e $|x\rangle$ sendo um vetor de uma base ortonormal de $\mathbb{C}^q$, o qual os índices $x \in \mathbb{F}_q$. Considere que $a, b \in \mathbb{F}_q$ e adote que $X(a)$ e $Z(b)$ são operadores unitários em $\mathbb{C}^q$ definidos por $X(a)|x\rangle = |x + a\rangle$ e $Z(b)|x\rangle = w^{tr(bx)}|x\rangle$, respectivamente, com $w = \exp(2\pi i/p)$ sendo a p-ésima raíz primitiva da unidade (p é a característica de $\mathbb{F}_q$) e tr é a aplicação traço de $\mathbb{F}_q$ em $\mathbb{F}_p$.

Considerando a *base de erro* $\mathbb{E} = \{X(a), Z(b) | a, b \in \mathbb{F}_q\}$, define-se o conjunto P_∞ (de acordo com [7]) como sendo o conjunto do produto tensorial infinito de todas as matrizes $N \in \langle M \mid M \in \mathbb{E}\rangle$, nas quais tem, a menos de um número finito, todas as componentes iguais a I, com I sendo a matriz identidade $q \times q$. O peso $\mathrm{wt}(A)$, $A \in P_\infty$, é definido como sendo o número de componentes diferentes da identidade. Neste contexto, diz-se que um QCC tem distância livre d_f se, e somente se, pode detectar todos os erros de peso menor que d_f, mas não consegue detectar algum erro de peso d_f.

No Lema 1 é apresentado um método de construção de QCC's a partir de códigos convolucionais clássicos.

Lema 1: [6, Proposição 1 and 2] Seja C um código convolucional com parâmetros $(n,(n-k)/2,\gamma;m)_{q^2}$ tal que $C \subseteq C^{\perp_h}$ (respectivamente $C \subseteq C^{\perp}$ com parâmetros $(n,(n-k)/2,\gamma;m)_q$). Então existe um código convolucional quântico com parâmetros $[(n,k,m;\gamma,d_f)]_q$, com d_f =wt$(C^{\perp_h}\backslash C)$ (respectivamente d_f =wt$(C^{\perp}\setminus C)$).

Em [7] é mostrado o limitante de *Singleton* quântico generalizado para QCC's, o qual é apresento no Teorema 1.

Teorema 1: (Limitante de Singleton Quântico Generalizado) Seja C um QCC com parâmetros $[(n,k,m;\gamma,d_f)]_q$. Relembre que C é um código puro se não existe erros de peso menor que d_f no estabilizador de C. A distância livre de um código convolucional quântico puro com parâmetros $[(n,k,m;\gamma,d_f)]_q$ F_{q^2} é limitada por

$$d_f \leq \frac{n-k}{2}\left(\left\lfloor \frac{2\gamma}{n+k}\right\rfloor + 1\right) + \gamma + 1.$$

Se os parâmetros do QCC satisfazem o limitante anterior com igualdade, então o código é chamado código de máxima distância de separação (MDS, do inglês maximum distance separable).

Observação 1: É interessante ressaltar que este limitante é um dos raros que existem na literatura para códigos convolucionais quânticos.

III. Códigos Algébrico-Geométricos

Nesta seção, serão introduzidos algumas notações básicas e resultados de códigos algébricos geométricos. Para mais detalhes, é possível examinar as referências [15, 29].

Seja $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g. Um lugar P de $F/\mathbb{F}_q$ é o ideal maximal de algum anel de valorização $\mathcal{O}$ de $F/\mathbb{F}_q$. Também é definido

$$\mathbb{P}_F := \{P | P \textit{ é um lugar de } F/\mathbb{F}_q\}. \tag{12}$$

Um divisor de $F/\mathbb{F}_q$ é uma soma formal de lugares dado por

$$D := \sum_{P\in\mathbb{P}_F} n_P P, \textit{ com } n_P \in \mathbb{Z}, \textit{ para quase todo } n_P = 0. \tag{13}$$

O suporte de D é definido como $suppD := \{P \in \mathbb{P}_F | n_p \neq 0\}$. A valorização discreta correspondente ao lugar P é escrita como ν_P. Para todo elemento x de $F/\mathbb{F}_q$, pode-se definir um divisor principal de x por $(x) := \sum_P \nu_P(x)P$. Para algum divisor G, denota-se o espaço de Riemann-Roch associado a G por

$$\mathcal{L}(G) := \{x \in F/\mathbb{F}_q | (x) \geq -G\} \cup \{0\}. \tag{14}$$

Seja $\Omega_F := \{\omega | \omega \textit{ é um diferencial de Weil } F/\mathbb{F}_q\}$ o espaço das diferenciais de $F/\mathbb{F}_q$. Dado um diferencial não-nulo w, denota-se por $(\omega) := \sum_P \nu_P(w)P$ o seu divisor canônico. Todos os divisores canônicos são equivalentes e tem grau igual a $2g-2$. Além disso, para um divisor G, define-se

$$\Omega_F(G) := \{\omega \in \Omega_F | \omega = 0 \textit{ or } (\omega) \geq G\}, \tag{15}$$

e sua dimensão por $i(G)$, que é denominado índice de especialidade.

Teorema 2: (Teorema de Riemann-Roch)[29, Teorema 1.5.15, pg 30] Seja W um divisor canônico de F/K. Então para cada divisor G, a dimensão de $\mathcal{L}(G)$ é dada por

$$\ell(G) = degG + 1 - g + \ell(W - G), \tag{16}$$

em que W é um divisor canônico.

Seja $P_1, \ldots, P_n$ lugares distintos dois-a-dois de $F/\mathbb{F}_q$ de grau 1 e $D = P_1 + \ldots + P_n$. Escolha um divisor G de $F/\mathbb{F}_q$ tal que $suppG \cap suppD = \varnothing$.

Definição 2: [29, Definição 2.2.1, pg 48] O código algébrico-geométrico (ou código AG) $C_{\mathcal{L}}(D,G)$ associado com os divisores D e G é definido como $C_{\mathcal{L}}(D,G) := \{(x(P_1),\ldots,x(P_n)) | x \in \mathcal{L}(G)\}$.

Proposição 1: [29, Corolário 2.2.3, pg 49] Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g. Então o código AG $C_{\mathcal{L}}(D,G)$ é um código linear $[n,k,d]$ sobre $\mathbb{F}_q$ com parâmetros

$$k = \ell(G) - \ell(G-D) \textit{ e } d \geq n - degG. \tag{17}$$

Se $2g-2 < \deg(G) < n$, então $k = \deg(G) - g + 1$.

Se $x_1, \ldots, x_k$ é uma base de $\mathcal{L}(G)$, então uma matriz geradora de $C_{\mathcal{L}}(D,G)$ é dada por

$$G_{\mathcal{L}} = \begin{bmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{bmatrix}. \tag{18}$$

Antes de ser apresentado a outra classe de códigos AG, será definido o semigrupo de Weierstrass de um divisor Q. Essa quantidade será utilizada posteriormente para extrair os parâmetros de códigos convolucionais quânticos derivados de códigos AG.

Definição 3: [21, Subseção 3.2] Seja Q um lugar de $F/\mathbb{F}_q$ de grau 1. Seja $\mathcal{L}(\infty Q) = \cup_{r\geq 0}\mathcal{L}(rQ)$ o espaço de funções racionais tendo pólos apenas em Q. O semigrupo de Weierstrass de Q é definido como

$$S = S(Q) = \{-\nu_Q(f) | f \in \mathcal{L}(\infty Q)\} = \{0 = \rho_1 < \rho_2 < \cdots\}, \tag{19}$$

com ν_Q sendo a valorização em Q.

Definição 4: [29, Definição 2.2.6, pg 51] Sejam G e $D = P_1 + \ldots + P_n$ divisores como na Definição 2. Então define-se o código $C_\Omega(D,G)$ por

$$C_\Omega(D,G) := \{(resp_{P_1}(\omega),\ldots,resp_{P_n}(\omega)) | \omega \in \Omega_F(G-D)\}, \tag{20}$$

em que $resp_{P_i}(\omega)$ denota o resíduo de ω em P_i.

Proposição 2: [29, Teorema 2.2.7, pg 51] Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g. Seja G e $D = P_1 + \ldots + P_n$ divisores como na Definição 2. Se $2g-2 < \deg(G) < n$, então $C_\Omega(D,G)$ é um código linear $[n,k',d']$ sobre $\mathbb{F}_q$, em que

$$k' = n + g - 1 - \deg(G) \tag{21}$$

e

$$d' \geq degG - (2g-2). \quad (22)$$

A conexão entre os códigos $C_{\mathcal{L}}(D,G)$ e $C_{\Omega}(D,G)$ é fornecido na Proposição 3.

Proposição 3: [29, Proposição 2.2.10 e 2.2.11, pg 54] Seja η um diferencial de Weil tal que $\nu_{P_i}(\eta) = -1$ e $\eta_{P_i} = 1$ para todo $i = 1, \ldots, n$. Então

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\Omega}(D,G) = C_{\mathcal{L}}(D, D - G + (\eta)), \quad (23)$$

em que $C_{\mathcal{L}}(D,G)^{\perp}$ é o dual euclidiano de $C_{\mathcal{L}}(D,G)$.

IV. Construção de Novos Códigos Convolucionais Quânticos

Nesta seção é apresentado um método geral para construção de códigos convolucionais quânticos a partir de códigos AG. Mais precisamente, são construídos códigos convolucionais quânticos aplicando-se o Teorema 1 nos códigos AG convolucionais de [22]. Assim, é necessário mostrar o resultado de [22] em que este trabalho se baseia, o que é feito a seguir:

Teorema 3: Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g. Considere o código AG $C_{\Omega}(D,G)$ com $2g-2 < \deg(G) < n$, em que $\deg(G)$ é o grau do divisor G. Então existe um código convolucional de memória unitária com parâmetros $(n, k-l, l; 1, d_f \geq d)_q$, em que $l \leq k/2$, derivado de $C_{\Omega}(D,G)$.

Como será demonstrado no teorema seguinte, com a aplicação do Teorema 1 no Teorema 3 e utilizando a ideia de semigrupo de Weierstrass, é possível construir códigos AG convolucionais quânticos e extrair seus parâmetros. Este é o principal resultado deste trabalho.

Teorema 4: Seja $C_{\mathcal{L}}(D,G)$ um código auto-ortogonal de um ponto (como na Definição 2) com parâmetros $[n,k,d]_q$ e matriz geradora M. Se d_1 é a distância mínima do código com matriz verificadora de paridade $\tilde{M}_1$ e $C_{\mathcal{L}}(D,G')$ é um código AG gerado pelo divisor G', com $\dim(\mathcal{L}(G')) = k-l$, então existe um código convolucional quântico derivado de $C_{\mathcal{L}}(D,G)$ com parâmetros $[(n, n-2(k-l), 1; l, d_f)]$, sendo $d_f \geq \min\{d(C_{\mathcal{L}}(D,G')) + d_1, d(C_{\Omega}(D,G))\}$. Em particular, se $2g-2 \leq \deg(G) \leq n/2+g$ então $d_f \geq \deg(G) - (2g-2)$.

Demonstração: Seja $S(Q) = \{0 = \rho_1 < \rho_2 < \ldots\}$ o semigrupo de Weierstrass de Q. Constrói-se a *base de Weierstrass* do espaço de Riemann-Roch $\mathcal{L}(rQ)$, $r \geq 0$, com dimensão $\ell(rQ) = k$ da seguinte forma. O primeiro da base de $\mathcal{L}(rQ)$ é um vetor $x_1 \in F/\mathbb{F}_q$ tal que $\nu_Q(x_1) = \rho_1 = 0$. A escolha do segundo vetor segue a mesma ideia, ou seja, pega-se um $x_2 \in F/\mathbb{F}_q$ com $\nu_Q(x_2) = \rho_2$, e assim por diante. Por construção, segue que cada um destes vetores tem valorização diferente no lugar Q, de tal forma que o conjunto $\{x_1, x_2, \ldots, x_k\}$ contêm k vetores linearmente independentes. Além disso, estes vetores pertencem ao espaço $\mathcal{L}(rQ)$. Em outras palavras, $\{x_1, x_2, \ldots, x_k\}$ é uma base de $\mathcal{L}(rQ)$ e será chamada de base de Weierstrass de $\mathcal{L}(rQ)$. Assim, o conjunto $\{x_1, x_2, \ldots, x_{k-1}\}$ também é uma base do espaço de Riemann-Roch $\mathcal{L}(r'Q)$, com $\mathcal{L}(r'Q) \subset \mathcal{L}(rQ)$ e $\ell(r'Q) = k-1$.

Agora é possível construir os códigos convolucionais quânticos desejados e calcular seus parâmetros.

Seja $C_{\mathcal{L}}(D,G)$ um código auto-ortogonal de um ponto (como dado na Definição 2) com parâmetros $[n,k,d]_q$, tendo matriz geradora M com linhas $\{m_1, \ldots, m_k\}$. Seja $\{x_1, \ldots, x_k\}$ a base de Weierstrass de $\mathcal{L}(G)$ apresentada anteriormente. Aplicando o Teorema 3, o correspondente código convolucional também será auto-ortogonale terá parâmetros $(n, k-l, l; 1, d_f \geq d(C_{\mathcal{L}}(D,G)))_q$. Aplicando o Teorema 1 para tal código, e como os vetores $\{x_1, \ldots, x_{k-l}\}$ geram outro espaço de Riemann-Roch associado com o divisor $G' = \rho_{k-l}Q$, com ρ_{k-l} sendo o $(k-l)$-ésimo elemento de $S(Q)$, então é possível construir um código convolucional quântico com parâmetros $[(n, n-2(k-l), 1; l, d_f)]$, sendo $d_f \geq \min\{d(C_{\mathcal{L}}(D,G')) + d_1, d(C_{\Omega}(D,G))\}$. ■

Observação 2: Note que, no Teorema 4, pela aplicação do limitante quântico de Singleton generalizado, segue que a distância livre do código convolucional quântico construído aqui é limitado por $d_f \leq \deg(G) - g + 2$ (com $2g-2 \leq deg(G) \leq n/2+g$). Além disso, $d_f \geq \deg(G) - 2g + 2$; então, a distância livre d_f está limitada por $\deg(G) - 2g + 2 \leq df \leq \deg(G) - g + 2$. Em particular, para corpo de funções $F/\mathbb{F}_q$ com $g = 0$, os novos códigos convolucionais quânticos criados a partir do Teorema 4 serão MDS. Em outras palavras, o *generalized quantum Singleton defect* dos novos QCC's é no máximo igual ao gênero da curva utilizada para construir o código AG (clássico).

Teorema 5: Assuma que todas as hipóteses do Teorema 4 se mantenham e que $F = \mathbb{F}_q(z)$ seja o corpo de função racional. Então existe um código convolucional quântico MDS com parâmetros $[(q, q-2m, 1; 1, d_f)]_q$, sendo $1 \leq m \leq (q-2)/2$ e $d_f \geq m+2$.

Demonstração: Procedendo de forma similar ao Teorema 3, um corpo de função racional é utilizado para construir um código convolucional. Como para $m \leq (q-2)/2$ (veja [29]), tem-se que o código AG será auto-ortogonal; assim, o código convolucional derivado deste código é também auto-ortogonal. Aplicando o Teorema 4, obtêm-se o código desejado. ■

Teorema 6: Seja $q = t^2$ com t sendo uma potência de um número primo. Se $t(t-1) < m \leq (t^3 + t^2 - t - 2)/2$, então tem-se que existe um código convolucional quântico com parâmetros $[(t^3, t^3 + t - 2m - 3, 1; 1, d_f)]_q$, sendo $d_f \geq m - t^2 + t + 2$.

Demonstração: Seja $F/\mathbb{F}_q$ o corpo de função definido pela curva $y^t + y = x^{t+1}$, ou seja, a curva de Hermite. Como é mostrado na Ref. [30], para $t(t-1) < m \leq (t^3 + t^2 - t - 2)/2$, é possível construir um código AG auto-ortogonal com parâmetros $(t^3, m+1-t(t-1)/2, d_f \geq t^3 - m)$. Assim, construindo o código convolucional a partir deste código de bloco pela utilização do Teorema 3 e utilizando-o no Teorema 4, o código convolucional quântico desejado é obtido. ■

Teorema 7: Seja $q = 2^t$ com $t \geq 3$. Se $q-2 \leq m \leq q^2 + q/2 - 1$, então existe uma nova família de QCC's com parâmetros $[(2q^2, 2q^2 + q - 2m, 1; 1, d_f)]_{q^2}$, sendo $d_f \geq m - q + 2$.

Demonstração: Seja $F/\mathbb{F}_q$ o corpo de função utilizado no Teorema 4 da Ref. [22]. Para $q-2 \leq m \leq q^2+q/2-1$, o código AG utilizado para construir o código convolucional clássico sobre $F/\mathbb{F}_q$ na referência supracitada é auto-ortogonal euclidiano (veja [20]). Assim, aplicando os Teoremas 3 e 4 obtêm-se o QCC desejado, o qual tem parâmetros $[(2q^2, 2q^2+q-2m, 1; 1, d_f)]_{q^2}$. ■

V. Exemplos de Códigos Convolucionais Quânticos

Nesta seção, são apresentados os parâmetros dos novos códigos convolucionais quânticos que são obtidos a partir dos resultados apresentados. Os valores que serão mostrados consistem de apenas uma substituição numérica nos parâmetros dos códigos que foram obtidos, ou seja, não foi necessário a utilização de *softwares* de computação algébrica para tal cálculo. Nas Tabelas I e II são mostrados exemplos das duas famílias de QCC's referentes aos Teoremas 6 e 7, respectivamente.

TABELA I

Novos QCC's – Teorema 6

$[(t^3, t^3+t-2m-3, 1; 1, d_f \geq m-t^2+t+2)]_{t^2}$
$t(t-1) < m \leq (t^3+t^2-t-2)/2$ e t potência de primo
$[(8, 1, 1; 1, d_f \geq 3)]_4$
$[(64, 15, 1; 1, d_f \geq 15)]_{16}$
$[(125, 27, 1; 1, d_f \geq 32)]_{25}$
$[(512, 317, 1; 1, d_f \geq 46)]_{64}$

TABELA II

Novos QCC's – Teorema 7

$[(2q^2, 2q^2+q-2m, 1; 1, d_f \geq m-q+2)]_{q^2}$
$q-2 \leq m \leq q^2+q/2-1$ e $q=2^t$ com $t \geq 3$
$[(512, 328, 1; 1, d_f \geq 86)]_{16}$
$[(2048, 1880, 1; 1, d_f \geq 70)]_{1024}$
$[(8192, 8056, 1; 1, d_f \geq 38)]_{4096}$
$[(32768, 12896, 1; 1, d_f \geq 9874)]_{16384}$

Note que esses códigos têm parâmetros diferentes dos que existem na literatura. Na realidade, os novos códigos aqui apresentados não tem análogos na literatura. Devido a isso, não é possível compará-los com os códigos existentes.

VI. Conclusão

Neste trabalho foram apresentados três novas famílias de códigos convolucionais quânticos derivados de códigos algébrico-geométricos. Estes novos códigos têm bons parâmetros, no sentido que ou são novos ou são superiores aos da literatura. Mais precisamente, uma família de códigos é MDS. Além disso, foi apresentada outras duas famílias de novos códigos convolucionais que não possuem parâmetros similares aos códigos disponíveis na literatura.

Agradecimentos

Os autores agradecem as agências de fomento CAPES e CNPq pelo suporte financeiro a este trabalho.

Referências

[1] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Physical Review Letters*, vol. 91, no. 17, pp. 177 902–4, October 2003.

[2] ——, "Quantum convolutional codes: fundamentals," 2004, preprint quant-ph/0401134.

[3] A. A. D. Almeida and R. Palazzo, "A concatenated $[(4, 1, 3)]$ quantum convolutional code," *Proc. IEEE Information Theory Workshop (ITW)*, pp. 28–33, 2004.

[4] M. Grassl and M. Rötteler, "Quantum block and convolutional codes from self-orthogonal product codes," *Proc. International Symposium on Information Theory (ISIT)*, pp. 1018–1022, 2005.

[5] ——, "Constructions of quantum convolutional codes," *Proc. International Symposium on Information Theory (ISIT)*, pp. 816–820, 2007.

[6] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli, "Quantum convolutional bch codes," 2007.

[7] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "Quantum convolutional codes derived from reed-solomon and reed-muller codes," 2007.

[8] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 865–880, March 2007.

[9] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Physical Review A*, vol. 81, no. 4, p. 042333, April 2010.

[10] P. Tan and J. Li, "Efficient quantum stabilizer codes: Ldpc and ldpc-convolutional constructions," *IEEE Transactions Information Theory*, vol. 56, no. 1, pp. 476–491, 2010.

[11] G. G. L. Guardia, "On classical and quantum mds-convolutional bch codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 1, pp. 304–312, 2014.

[12] ——, "On negacyclic mds-convolutional codes," *Linear Algebra and its Applications*, vol. 448, pp. 85–96, 2014.

[13] G. G. Guardia, "On optimal constacyclic codes," *Linear Algebra and its Applications*, vol. 496, pp. 594–610, 2016.

[14] V. D. Goppa, "Codes on algebraic curves," *Soviet Math. Dokl*, vol. 22, no. 1, pp. 170–172, 1981.

[15] M. Tsfasman, S. Vladut, and D. Nogin, *Algebraic Geometric Codes: Basic Notions*. American Mathematical Society, 2007.

[16] A. Garcia and H. Stichtenoth, "A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound," *Inventiones mathematicae*, vol. 121, pp. 211–222, 1995.

[17] L. F. Jin, S. Ling, J. Q. Luo, and C. P. Xing, "Application of classical hermitian self-othogonal mds codes to quantum mds codes," *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4735–4740, September 2010.

[18] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth, "Towers of function fields over non-prime finite fields," 2012.

[19] L. F. Jin and C. P. Xing, "Euclidean and hermitian self-orthogonal algebraic geometry codes and their application to quantum codes," *IEEE Trans. Inform. Theory*, vol. 58, no. 8, pp. 5484–5489, August 2012.

[20] L. Jin, "Quantum stabilizer codes from maximal curves," *IEEE Trans. Inform. Theory*, vol. 60, no. 1, pp. 313–316, January 2014.

[21] C. Munuera, W. Tenório, and F. Torres, "Quantum error-correcting codes from algebraic geometry codes of castle type," *Quantum Information Processing*, vol. 16, no. 10, pp. 4071–4088, October 2016.

[22] F. R. F. Pereira, G. G. L. Guardia, and F. M. Assis, "Novos códigos convolucionais derivados de códigos algébrico-geométricos," in *Anais do XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, 2017.

[23] G. D. F. Jr, "Convolutional codes i: algebraic structure," *IEEE Trans. Inform. Theory*, vol. 16, no. 6, pp. 720–738, November 1970.

[24] P. Piret, *Convolutional Codes: An Algebraic Approach*. Cambridge, Massachusetts: The MIT Press, 1988.

[25] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Digital and Mobile Communication, Wiley-IEEE Press, 1999.

[26] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.

[27] R. Smarandache, H. G.-Luerssen, and J. Rosenthal, "Constructions of mds-convolutional codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 2045–2049, July 2001.

[28] H. Gluesing-Luerssen and F.-L. Tsang, "A matrix ring description for cyclic convolutional codes," *Advances in Math. Communications*, vol. 2, no. 1, pp. 55–81, 2008.

[29] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer, 2009.

[30] ——, "Self-dual goppa codes," *Journal of Pure and Applied Algebra*, vol. 55, no. 1, pp. 199–211, 1988.