Novos Códigos Convolucionais 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 são construídas a partir de códigos algébrico-geométricos (AG). Os códigos convolucionais construídos são novos no sentido que seus parâmetros são diferentes dos parâmetros dos códigos disponíveis na literatura. Em particular, uma família de códigos *almost near* MDS ou *near* MDS ou MDS é apresentada.**

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

I. Introdução

A classe de códigos convolucionais tem sido extensivamente investigada na literatura [6, 13, 14, 19, 21, 22]. Códigos de máxima distância de separação (MDS), bem como códigos convolucionais ótimos (no sentido que atingem o limitante de Singleton generalizado [21]) também têm sido explorado [6, 13, 14, 19, 21, 22]. Rosenthal *et al.* introduziram o limitante de Singleton generalizado [21] (veja também [22]) em 1999.

Além dos códigos convolucionais, a classe de códigos algébrico-geométricos (AG), que foi introduzida por Goppa [7] em 1981, possui uma grande diversidade de trabalhos em que os investigam [9–11, 16, 17]. Esses códigos possuem propriedades interessantes para diversas aplicações, além de serem assintoticamente bons [3, 5, 15]. Entretanto, apenas poucos deles [4, 18, 20] lidam com a construção de códigos convolucionais a partir da utilização de códigos AG como sua contrapartida fundamental.

Neste trabalho, são construídas diversas famílias de códigos convolucionais de memória unitária por meio da aplicação do método criado por Piret [19], generalizado por Aly *et al.*, em 2007 [1]. Mais especificadamente, este método utiliza códigos de bloco a fim de obter uma matriz reduzida e básica para o correspondente código convolucional. No caso deste trabalho, os códigos AG são utilizados como códigos de bloco para a construção dos códigos convolucionais de memória unitária. Uma vantagem da técnica utilizada aqui está no fato de que os novos códigos convolucionais são gerados algebricamente e não por procura computacional. Assim, novas famílias de códigos convolucionais são construídas, e não apenas códigos específicos, em contraste com muitos trabalhos em que apenas buscas computacionais são implementadas ou mesmo a construção de códigos específicos.

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.

O trabalho está organizado da seguinte forma. Na Seção II, são revisados os conceitos básicos sobre códigos convolucionais. 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 derivados de códigos AG. Em particular, uma família de códigos convolucionais *almost near* MDS ou *near* MDS ou MDS é exibida (que são códigos que tem a distância mínima distanciando-se do limitante de Singleton generalizado por valores de 2, 1 ou 0 unidades). 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

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, será apresentada uma breve revisão de códigos clássicos convolucionais. Para mais detalhes veja [1, 2, 8, 12, 13, 19].

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 [6, 8, 22]) se o *overall constraint length*, 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 *overall constraint length* γ é chamado de grau do correspondente código).

Definição 1: [2] 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 e básica

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

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 $\gamma_i := \max_{1\le j\le n} \{\deg g_{ij}\}$, $m := \max_{1\le i\le k}\{\gamma_i\}$

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.

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 e básica é 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 Derivados de Códigos de Bloco

Seja $[n, k, d]_q$ um código linear com matriz de paridade H. Agora subdivida H em $m+1$ submatrizes disjuntas H_i tais que

$$H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_m \end{bmatrix}, \tag{12}$$

em que cada H_i possui n colunas, obtendo a matriz polinomial

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \ldots + \tilde{H}_m D^m, \tag{13}$$

em que as matrizes $\tilde{H}_i$, para todo $1 \leq i \leq m$, são derivadas das respectivas matrizes H_i pela adição de linhas nulas na parte inferior, de forma que a matriz $\tilde{H}_i$ tenha κ linhas no total, em que κ é o número máximo de linhas entre todas as matrizes H_i. A matriz $G(D)$ gera um código convolucional com κ linhas (observe que m é a memória do código convolucional resultante de $G(D)$).

Teorema 1: [1, Teorema 3] Seja $C \subseteq \mathbb{F}_q^n$ um código linear com parâmetros $[n, k, d]_q$ e suponha também que $H \in \mathbb{F}_q^{(n-k)\times n}$ é uma matriz de verificação de paridade para C particionada nas submatrizes $H_0, H_1, \ldots, H_m$ como na Eq. (1) de tal forma que $\kappa = \text{rk}H_0$ e $\text{rk}H_i \leq \kappa$, para $1 \leq i \leq m$, em que rk é o posto da matriz, e considere que a matriz polinomial $G(D)$ é dada como em Eq. (13). Então a matriz $G(D)$ é uma matriz geradora reduzida e básica. Adicionalmente, se d_f denota a distância livre do código convolucional V gerado por $G(D)$ e $d^{\perp}$ é a distância mínima de $C^{\perp}$, então tem-se que $d_f \geq d^{\perp}$.

Por fim, Rosenthal *et al.* [22] apresentaram o limitante de Singleton generalizado, em que o mesmo é dado por, para um código convolucional $(n, k, \gamma; m, d_f)_q$,

$$d_f \leq (n-k)[\lfloor \gamma/k \rfloor + 1] + \gamma + 1. \tag{14}$$

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 [24, 25].

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

$$\mathbb{P}_F := \{P | P \textit{ é um lugar de } F/\mathbb{F}_q\}. \tag{15}$$

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

$$D := \sum_{P \in \mathbb{P}_F} n_P P, \textit{ com } n_P \in \mathbb{Z}, \textit{ para quase todo } n_P = 0. \tag{16}$$

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

$$\mathcal{L}(G) := \{x \in F/K\{0\} | (x) \geq -G\}. \tag{17}$$

Seja $\Omega_F := \{\omega | \omega \textit{ é um diferencial de Weil } F/K\}$ 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 A, define-se

$$\Omega_F(G) := \{\omega \in \Omega_F | \omega = 0 \textit{ or } (\omega) \geq G\}, \tag{18}$$

e sua dimensão por $i(G)$.

Teorema 2: (Teorema de Riemann-Roch)[24, 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

$$\ell(G) = degG + 1 - g + \ell(W - G), \tag{19}$$

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: [24, 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: [24, 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

$$k = \ell(G) - \ell(G - D) \text{ e } d \geq n - degG. \tag{20}$$

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

$$G_{\mathcal{L}} = \begin{bmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{bmatrix}. \tag{21}$$

Definição 3: [24, 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

$$C_\Omega(D, G) := \{(resp_{P_1}(\omega), \ldots, resp_{P_n}(\omega) | \omega \in \Omega_F(G - D)\}, \tag{22}$$

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

Proposição 2: [24, 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

$$k' = n + g - 1 - \deg(G) \tag{23}$$

e

$$d' \geq degG - (2g - 2). \tag{24}$$

A conexão entre os códigos $C_{\mathcal{L}}(D, G)$ e $C_\Omega(D, G)$ é fornecido na proposição dada a seguir.

Proposição 3: [24, 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

$$C_{\mathcal{L}}(D, G)^{\perp} = C_\Omega(D, G) = C_{\mathcal{L}}(D, D - G + (\eta)), \tag{25}$$

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

IV. Novos Códigos AG Convolucionais

Nesta seção é apresentado um método geral para construção de códigos convolucionais a partir de códigos AG. Mais precisamente, são construídos códigos convolucionais nos quais a matriz geradora é derivada de um código AG dado por $C_\Omega(D, G)$. O primeiro resultado é dado 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 $C_\Omega(D, G)$.

Demonstração: Considere o código AG dado por $C_\Omega(D, G)$ e definido sobre $F/\mathbb{F}_q$ com matriz de verificação de paridade

$$H_\Omega = \begin{bmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{bmatrix}, \tag{26}$$

em que $x_1, \ldots, x_k$ é uma base de $\mathcal{L}(G)$. Seja $C_{\mathcal{L}}(D, G)$ o dual (euclideano) do código $C_\Omega(D, G)$. Neste caso H_Ω é uma matriz geradora de $C_{\mathcal{L}}(D, G)$ e $C_{\mathcal{L}}(D, G)$ é um código AG com parâmetros $[n, k = \deg G + 1 - g,\ d \geq n - \deg G]_q$, em que $n = \deg D$. Será construído um código convolucional derivado de $C_\Omega(D, G)$ da seguinte forma. Defina um código convolucional com matriz geradora

$$G(D) = H_0 + \widetilde{H}_1 D, \tag{27}$$

em que H_0 é a submatriz de H_Ω consistindo das primeiras $k - l$ linhas e $\widetilde{H}_1$ é a matriz consistindo das últimas l linhas de H_Ω adicionando-se, abaixo, linhas nulas, de forma que a matriz $\widetilde{H}_1$ tenha $k - l$ linhas no total. Por hipótese, segue que

$$\operatorname{rk} H_0 \geq \operatorname{rk} \widetilde{H}_1. \tag{28}$$

Pelo Teorema 1, a matriz $G(D)$ é uma matriz reduzida e básica. O código convolucional gerado por $G(D)$ é um código de memória unitária com dimensão $k - l$, grau l e distância livre d_f. Utilizando novamente o Teorema 1, segue-se que $d_f \geq d$. Assim, existe um código convolucional com parâmetros $(n, k - l, l; 1, d_f)_q$, em que $d_f \geq d$, como requerido. ■

Observação 1: É interessante notar que o Teorema 3 pode ser facilmente generalizado para códigos convolucionais com multi-memória. Entretanto, como códigos de memória unitária atingem distâncias livres máximas possíveis dentre os códigos de mesma taxa, nos restringiremos apenas a esse caso (veja [14]).

Corolário 1: Com as hipóteses do Teorema 3, tem-se que existe um código convolucional com parâmetros $(n, k - 1, 1; 1, d_f \geq d)_q$.

Demonstração: É suficiente considerar $l = 1$ no Teorema 3. ■

Observação 2: Note que, aplicando-se o Corolário 1 e o limitante de Singleton generalizado, segue-se que a distância livre do código convolucional aqui construído é limitada por $d_f \leq n-k+3$ (em que n e k são os parâmetros de $C_{\mathcal{L}}(D, G)$).

Além disso, $d_f \geq n-deg(G) = n-(k+g-1) = n-k+1-g$, donde a distância livre d_f é limitada por $n-k+1-g \leq d_f \leq n-k+3$. Em particular, para o corpo de funções $F/\mathbb{F}_q$ em que $g=0$ os novos códigos convolucionais têm distância livre limitada por $n-k+1 \leq d_f \leq n-k+3$. Nesse caso, observe que esses códigos são *almost near MDS* ou *near MDS* ou *MDS*. Em outras palavras, a distância livre dista de, no máximo, duas unidades do máximo valor possível. Assim, as famílias de códigos derivados desses corpos de funções possuem bons parâmetros.

Corolário 2: Seja $F = \mathbb{F}_q(z)$ um corpo de funções racionais. Para $\beta \in \mathbb{F}_q$, seja P_β o zero de $z-\beta$ e denote por P_∞ o pólo de z em $\mathbb{F}_q(x)$. Então existem códigos convolucionais com parâmetros $(q, r, 1; 1, d_f \geq q-r)_q$, com $1 < r \leq q-1$.

Demonstração: Considere o código $C_{\mathcal{L}}(D,G)$ com $D = \sum_{\beta \in \mathbb{F}_q} P_\beta$ e $G = rP_\infty$, em que $1 < r \leq q-1$. O código $C_{\mathcal{L}}(D,G)$ tem parâmetros $n=q$, $k=r+1$ e $d \geq n-r$. Aplicando o Corolário 1 para $C_{\mathcal{L}}(D,G)^\perp$ obtêm-se códigos convolucionais com os parâmetros mencionados. ■

Teorema 4: Seja $q = 2^t$, em que $t \geq 1$ é um inteiro. Então existe um $(2q^2, m-q/2, 1; 1, d_f \geq 2q^2-m)_q$ código convolucional, em que $q-2 < m < 2q^2$.

Demonstração: Este resultado segue do Teorema 3 e de [9, 23]. ■

V. Exemplos de Códigos

Nesta seção, são apresentados os parâmetros dos novos códigos convolucionais 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. Na Tabela I, é mostrado uma família de códigos aproximadamente *almost near* MDS (ou *near* MDS ou MDS) construídos com o Corolário 2.

TABELA I
Novos Códigos *Almost Near* MDS ou *Near* MDS ou MDS

Novos códigos obtidos do Corolário 2
$(n, k, \gamma; m, d_f)$
$(8, 2, 1; 1, d_f \geq 6)_8$
$(8, 5, 1; 1, d_f \geq 3)_8$
$(37, 17, 1; 1, d_f \geq 20)_{37}$
$(37, 33, 1; 1, d_f \geq 4)_{37}$
$(71, 35, 1; 1, d_f \geq 36)_{71}$
$(71, 68, 1; 1, d_f \geq 3)_{71}$
$(128, 64, 1; 1, d_f \geq 64)_{128}$
$(128, 125, 1; 1, d_f \geq 3)_{128}$
$(256, 128, 1; 1, d_f \geq 128)_{256}$
$(256, 253, 1; 1, d_f \geq 3)_{256}$

Os códigos apresentados na Tabela II são obtidos pela aplicação do Teorema 4. 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.

TABELA II
Novos Códigos Convolucionais

Novos Códigos
$(32, 15, 1; 1, d_f \geq 15)_4$
$(32, 1, 1; 1, d_f \geq 30)_4$
$(128, 64, 1; 1, d_f \geq 60)_8$
$(128, 3, 1; 1, d_f \geq 122)_8$
$(512, 128, 1; 1, d_f \geq 376)_{16}$
$(512, 256, 1; 1, d_f \geq 248)_{16}$
$(2048, 1024, 1; 1, d_f \geq 1008)_{32}$
$(2048, 15, 1; 1, d_f \geq 2017)_{32}$

VI. Conclusão

Neste trabalho foram construídos novos códigos convolucionais derivados de códigos algébrico-geométricos. Estes novos códigos têm bons parâmetros. Mais precisamente, uma família de códigos *almost near* MDS ou *near* MDS ou MDS. Além disso, foi apresentada outra família 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] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli, "Quantum convolutional bch codes," 2007.

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

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

[4] J. I. I. Curto, J. M. M. noz Porras, F. J. P. Martín, and G. S. Sotelo, "Convolutional goppa codes defined on fibrations," *AAECC*, vol. 23, pp. 165–178, 2012.

[5] 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.

[6] 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.

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

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

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

[10] 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.

[11] 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.

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

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

[14] L. N. Lee, "Short unit-memory byte-oriented binary convolutional codes having maximum free distance," *IEEE Trans. Inform. Theory*, vol. 22, pp. 349–352, May 1976.

[15] C. Munuera, A. SepÃºlveda, and F. Torres, "Generalized hermitian codes," *Designs, Codes and Cryptography*, vol. 69, pp. 123–130, 2013.

[16] 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.

[17] F. Ozbudak and H. Stichtenoth, "Constructing codes from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2502–2505, August 2002.
[18] J. A. D. Pérez, J. M. noz Porras, and G. S. Sotelo, "Convolutional codes of goppa type," *AAECC*, vol. 51, pp. 51–61, 2004.
[19] P. Piret, *Convolutional Codes: An Algebraic Approach*. Cambridge, Massachusetts: The MIT Press, 1988.
[20] F. J. Plaza-MartÃn, J. I. Iglesias-Curto, and G. Serrano-Sotelo, "Constructing codes from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 59, no. 7, pp. 4615–4625, July 2013.
[21] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Applicable Algebra in Eng. Comm. Comput.*, vol. 10, pp. 15–32, 1999.
[22] 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.
[23] H. Stichtenoth, "Self-dual goppa codes," *Journal of Pure and Applied Algebra*, vol. 55, no. 1, pp. 199–211, 1988.
[24] ——, *Algebraic Function Fields and Codes*. Springer, 2009.
[25] M. Tsfasman, S. Vladut, and D. Nogin, *Algebraic Geometric Codes: Basic Notions*. American Mathematical Society, 2007.