Subgrupos Caraterísticos e Controlabilidade dos Códigos Convolucionais sobre Grupos

Jorge Pedraza Arpasi

Abstract— **Considerado os códigos sob o ponto de vista da teoria dos sistemas, este artigo propõe um critério de controlabilidade de códigos convolucionais sobre grupos usando subgrupos característicos de um grupo. Isto reduz a tarefa de procura por códigos ótimos, pois todo bom código necessariamente é controlável**

Keywords— **Códigos convolucionais, códigos controláveis, extensão de grupos, subgrupos característicos.**

I. introdução

A definição de códigos convolucionais sobre grupos é fornecido em [4] usando termos do enfoque da teoria dos sistemas dado por Willems em [10]. Desta forma um código convolucional é definido como um sistema que, entre outras coisas, tem que ser **invariante no tempo, controlável e observável**. Outros trabalhos anteriores a [4] também obtiveram resultados dos códigos convolucionais sob o ponto de vista da teoria dos sitemas. Naturalmente, todos os códigos convolucionais, sobre aneis, até então conhecidos são sistemas invariantes no tempo, controláveis e observáveis. Muitos destes códigos podem ser também considerados como códigos convolucionais sobre grupos abelianos.

Em [4] é dado um critério para construir códigos convolucionais usando um método chamado *shift register* a partir de uma estructura algébrica tal como grupo, anel ou corpo. No entanto, este critério é muito mais útil para mostrar que todos os códigos convolucionais podem ser gerados desta maneira do que para efetivamente gerar, de maneira prática, ese códigos.

Neste trabalho propomos um critério para a busca de grupos, especialmente não abelianos, que possam gerar sistemas controláveis e portanto sejam candidatos a códigos convolucionais. Para isto, particularizamos os sistemas bi-infinitos de [4], [10], [11] em sistemas indexados somente pelo conjunto dos números naturais $\mathbb{N}$. Estes códigos são mais "naturales"no sentido de que podem ser gerados por um codificador de estados a partir de um estado inicial dado. O aporte principal do presente trabalho é o uso dos **subgrupos característicos** de um grupo como ferramenta para decidir se um grupo pode gerar um sistema controlável que possa ser código convolucional sobre grupo.

Para isto, organizamos este artigo assim:

No Secão 2 damos uma introdução da extensão de grupos necessário para definir um codificador. Para maiores detalhes da teoria da extensão de grupos recomendamos [2] e [1]. Na Seção 3 definimos o codificador convolucional como uma máquina de entradas, estados e saídas cada uma destes possuindo uma estrutura de grupo. Este codificador esta associado de maneira biunívoca ao grupo extensão do grupo das entradas pelo grupo dos estados e pode gerar sistemas(códigos) não controláveis. Então, procurando por subgrupos característicos do grupo dos estados damos um critério para decidir se um codificador não poderá gerar um código controlavel.

Este trabalho foi financiado pela Fundação Universidade de Passo Fundo, Processo 40819-01. O autor é professor do Instituto de Cienias Exatas e Geociências - ICEG da Universidade de Passo Fundo - UPF. Email: arpasi@upf.tche.br

II. Preliminares algébricos

Se X e Q são grupos então uma **extensão** de X por Q é um grupo G que possui um subgrupo normal N isomorfo a X e o grupo quociente $\frac{G}{N}$ isomorfo a Q [2]. Simbólicamente, $N \cong X$ e $\frac{G}{N} \cong Q$.

Sejam $\psi : Q \to \frac{G}{N}$ e $\upsilon : N \to X$ isomorfismos tais que $Q \overset{\psi}{\cong} \frac{G}{N}$ e $N \overset{\upsilon}{\cong} X$. Seja $l : \frac{G}{N} \to G$ um levantamento tal que $l(N) = e_G$, o elemento identidade de G. Para cada $g \in G$ temos que $g \in Ng$, além disso existe um único $n \in N \triangleleft G$ tal que $g = n.l(Ng)$. Então, o mapeamento $\theta : G \to X \times Q$ definido por

$$\theta(g) = \theta(n.l(Ng)) = (\upsilon(n)\ ,\ \psi^{-1}(Ng)), \tag{1}$$

é bijetor.

Para $x \in X$ e $q \in Q$,considere $\psi(q) \in \frac{G}{N}$ e $\upsilon^{-1}(x) \in N$. Temos que $l(\psi(q)).\upsilon^{-1}(x).(l(\psi(r)))^{-1} \in N$. Então podemos construir um mapeamento $\phi : Q \to Aut(X)$ dado por,

$$\phi(q)(x) = \upsilon[l(\psi(q)).\upsilon^{-1}(x).(l(\psi(q)))^{-1}]. \tag{2}$$

Por outro lado, para $q, r \in Q$, $l(\psi(q)).l(\psi(r)) \in N\psi(qr) \in \frac{G}{N}$. Também $l(\psi(qr)) \in N\psi(qr)$. Daí $l(\psi(q)).l(\psi(r)).(l(\psi(qr)))^{-1} \in N$. Então, definimos $\varsigma : Q \times Q \to X$ como sendo

$$\varsigma(q, r) = \upsilon[l(\psi(q)).l(\psi(r)).(l(\psi(qr)))^{-1}]. \tag{3}$$

Os mapeamentos ϕ e ς satisfazem as seguintes condições

$$\phi(q)(\varsigma(r, s)).\varsigma(q, rs) = \varsigma(q, r).\varsigma(qr, s) \tag{4}$$

$$\phi(q)(\phi(r)(x)) = \varsigma(q, r).\phi(qr)(x).(\varsigma(q, r))^{-1} \tag{5}$$

Assim, se G possui um subgrupo normal $N \triangleleft G$, podemos decompor cada elemento $g \in G$, via o mapeamento θ de (1), como um par ordenado $(x,q) \in X \times Q$. A operação no grupo extensão $X \times Q$ é dada por

$$(x,q).(y,r) = (x.\phi(q)(y).\varsigma(q,r)\,,\ qr) \tag{6}$$

Usando esta operação (6), pode-se verificar que θ de (1) é um isomorfismo. Por outro lado, como o grupo extensão $X \times Q$ depende de ϕ e de ς denotaremos este grupo como $X_{\phi\varsigma}Q$, isto é, $G \overset{\theta}{\cong} X_{\phi\varsigma}$. Note que se o levantamento $l : \frac{G}{N} \to G$ é homomorfismo então, o mapeamento definido em (3) é dado por $\varsigma(q,r) = e_x$, para todo $x \in X$, entanto que (refeq:phi) é um homomorfismo de grupos. Logo, a operação definida por (6) converte-se em

$$(x,q).(y,r) = (x.\phi(q)(y)\,,\ qr), \tag{6'}$$

que é a operação do produto semidireto $X_{\phi\rtimes}Q$.

Exemplo 1: Considere o grupo $G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma, \delta, \alpha\delta, \beta\delta, \alpha\beta\delta, \gamma\delta, \alpha\gamma\delta, \beta\gamma\delta, \alpha\beta\gamma\delta\}$, gerado por quatro elementos que satifazem as seguintes relações

$$\begin{cases} \alpha^2 = e & & & \\ \beta^2 = e, & \beta\alpha = \alpha\beta, & & \\ \gamma^2 = e, & \gamma\alpha = \alpha\gamma, & \gamma\beta = \beta\gamma & \\ \delta^2 = e, & \delta\alpha = \alpha\delta\gamma, & \delta\beta = \beta\delta, & \delta\gamma = \delta\gamma \end{cases}$$

Temos que $N = \{e, \beta\gamma\}$ é um subgrupo normal de G. N é isomorfo ao grupo aditivo $\mathbb{Z}_2 = \{0,1\}$, as classes de congruência mod 4, via o isomorfismo $\upsilon(e) = 0$ e $\upsilon(\beta\gamma) = 1$. Por outro lado $\frac{G}{N} \cong D_8$, o grupo das simetrias do quadrado, via o isomorfismo $\psi : D_8 \to G/N$ definido por

$$\begin{array}{llll} R_0 \mapsto N & R_1 \mapsto N.\alpha\delta & R_2 \mapsto N.\beta & R_3 \mapsto N.\alpha\beta\delta \\ d_1 \mapsto N.\alpha & d_2 \mapsto N.\alpha\beta & H \mapsto N.\beta\delta & V \mapsto N.\delta \end{array}$$

Considere o levantamento $l : G/N \to G$ definido por $l(N) = e$, $l(N.\alpha\delta) = \alpha\delta$, $l(N.\beta) = \beta$, $l(N.\alpha\beta\delta) = \alpha\beta\delta$, $l(N.\alpha) = \alpha$, $l(N.\alpha\beta) = \alpha\beta$, $l(N.\beta\delta) = \beta\delta$ e $l(N.\delta) = \delta$.

Assim, os mapeamentos, ς e ϕ de (3) e (2) respectivamente, estão definidos e por tanto o grupo extensão extensão $\mathbb{Z}_{2\phi\varsigma}D_8$ é isomorfo a G vía o isomorfismo θ.

$$\begin{array}{ll} e \mapsto (0,R_0) & \alpha \mapsto (0,d_1) \\ \beta \mapsto (0,R_2) & \gamma \mapsto (1,R_2) \\ \delta \mapsto (0,V) & \alpha\beta \mapsto (0,d_2) \\ \alpha\gamma \mapsto (1,d_2) & \alpha\delta \mapsto (0,R_1) \\ \beta\gamma \mapsto (1,R_0) & \beta\delta \mapsto (0,H) \\ \gamma\delta \mapsto (1,H) & \alpha\beta\gamma \mapsto (1,d_1) \\ \alpha\beta\delta \mapsto (0,R_3) & \alpha\gamma\delta \mapsto (1,R_3) \\ \beta\gamma\delta \mapsto (1,V) & \alpha\beta\gamma\delta \mapsto (1,R_1) \end{array}$$

III. Códigos controláveis

Definição 1: Dados os grupos finitos X, Q, Y, considere a extensão X por Q. Um codificador convolucional sobre grupos é uma máquina $M = (X, Y, Q, \nu, \omega)$, onde $\nu : X \times Q \to Y$ e $\omega : X \times Q \to Q$ são homomorfismos de grupos com ω sobrejetora.

Dado um codificador $M = (X, Y, Q, \nu, \omega)$, seja e_Q o elemento identidade do grupo de estados Q. Considere a sequência $\{Q_i\}$ definida assim

$$\begin{array}{ll} Q_0 & = \{e_Q\} \\ Q_1 & = \{\omega(x,q)\ ;\ x \in X, q \in Q_0\} \\ Q_2 & = \{\omega(x,q)\ ;\ x \in X, q \in Q_1\} \\ \vdots & \vdots \\ Q_i & = \{\omega(x,q)\ ;\ x \in X, q \in Q_{i-1}\} \\ \vdots & = \vdots \end{array} \tag{7}$$

Lema 1: Propriedades da familia $\{Q_i\}$;

1. $Q_{i-1} \subset Q_i$, para todo $i = 1, 2, \ldots$
2. $Q_{i-1} \triangleleft Q_i$, para todo $i = 1, 2, \ldots$.
3. $Q_{i-1} = Q_i$ implica que $Q_i = Q_{i+1}$
4. Se $Q_i = Q$, para algum i então, existe $j \leq |Q|$, onde $|Q|$ é a cardinalidade de Q tal que $Q_j = Q$.

Prova.-

1. Claramente $Q_0 \subset Q_1$. Suponha que para $i > 1$, $Q_{j-1} \subset Q_j$, para todo $j \leq i$. Dado $q \in Q_i$ existem $p \in Q_{i-1}$ e $x \in X$ tais que $\omega(x,p) = q$. Por outro lado, $p \in Q_{i-1} \subset Q_i$ implica que $\omega(x,p) = q \in Q_{i+1}$.
2. Claramente $Q_0 \triangleleft Q_1$. Suponha que para $i > 1$, $Q_{j-1} \subset Q_j$, para todo $j \leq i$. Dados $q \in Q_{i+1}$ e $p \in Q_i$, considere $q.p.q^{-1} = \omega(x,p_1).\omega(u,q_1).\omega(x,p_1)^{-1}$, onde $p_1 \in Q_i$, $q_1 \in Q_{i-1}$, $x, u \in X$. Usando o fato que ω é homomorfismo de grupos e a operação (6) do grupo extensão $X_{\phi\varsigma}Q$ obtemos $q.p.q^{-1} = \omega(x_1, p_1.q_1.p_1^{-1}) \in Q_i$, pois $p_1.q_1.p_1^{-1} \in Q_{i-1}$.
3. Dado $q \in Q_{i+1}$ existem $p \in Q_i$ e $x \in X$ tal que $\omega(x,p) = q$. Como $Q_i = Q_{i-1}$, $p \in Q_{i-1}$. Logo $\omega(x,p) = q \in Q_i$.
4. Em outro caso, pelos items (1) e (3), $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_{|Q|}$. Considere a sequência $\{q_i\} \subset Q$ definida por $q_i \in Q_i$ e $q_i \notin Q_{i-1}$. Então, $\{e_Q, q_1, q_2, \ldots, q_{|Q|}\}$ seria um subconjunto de Q com $|Q| + 1$ elementos. Contradição. ■

Considere o estado inicial $q_0 \in Q$ e uma sequência de letras de informaçào não-codificadas(entradas) $\{x_i\}_{i=1}^{\infty}$, $x_i \in X$, para cada $i \in \mathbb{N}$. Então esta sequência produz no codificador M sequências de estados e letras de informação codificadas(saídas) via as iterações

$$\begin{array}{ll} q_1 = & \omega(x_1, q_0) \\ q_2 = & \omega(x_2, q_1) \\ \vdots & \vdots \\ q_i = & \omega(x_i, q_{i-1}) \\ \vdots & \vdots \\ y_1 = & \nu(x_1, q_0) \\ y_2 = & \nu(x_2, q_1) \\ \vdots & \vdots \\ y_i = & \nu(x_i, q_{i-1}) \\ \vdots & \vdots \end{array}$$

$\{q_i\}_{i=1}^{\infty}$ é dita a sequência de estados internos de M e $\{y_i\}_{i=1}^{\infty}$ chamada de **palavra código**. A classe de todas

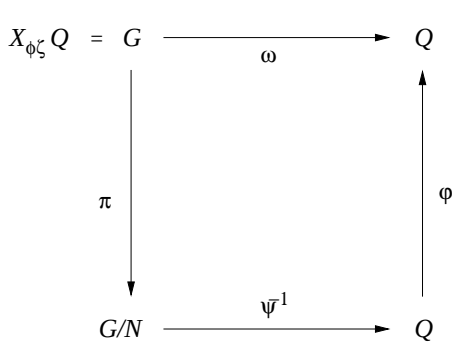

Fig. 1. O homomorfismo de estados ω

as palavras código é chamada sistema ou código convolucional asociado ao codificador M e o mesmo é denotado por $\mathcal{C}$=$\{$palavras código $\{y_i\}_{i=1}^{\infty}\}$. Para $y \in \mathcal{C}$ e $I \subset \mathbb{N}$, seja $y|_I = \{y_k \ ; \ k \in I\}$, por exemplo se $I = [k, \infty) = \{k, k+1, \ldots \infty\}$ teremos $y|_{[k,\infty]} = \{y_k, y_{k+1}, \ldots\}$.

Adaptamos a seguinte definição de [4], onde as palavras são consideradas bi-infinitas, para o caso da indexação em $\mathbb{N}$. Esta adaptação é possível, pois $\mathbb{N} \subset \mathbb{Z}$, o conjunto dos números inteiros.

Definição 2: Um código $\mathcal{C}$ é controlável quando para cada $k \in \mathbb{N}$ e para cada par de palavras código y, $y\prime$ existir uma palavra código $y\prime\prime$ tal que $y\prime\prime|_{(1,k)} = y|_{(1,k)}$ e $y\prime\prime|_{[k+l,\infty)} = y\prime|_{[k+l,\infty)}$, para algum $l \geq 1$.

Teorema 1: Considere os subgrupos de estados Q_j definidos em (7). Se $Q_i = Q_{i+1} \subsetneq Q$, para algum $i \in \mathbb{N}$ então o código não é controlável

Prova.- Seja $q \in Q$ tal que $q \notin Q_i$. Teremos que para qualquer sequência $\{x_i\}_{i=1}^{n}$,

$$q \neq \omega(x_n, \omega(x_{n-1}(x_{n-2}, \ldots, \omega(x_1, e_Q)\ldots)))$$

■

Definição 3: Dado um grupo G e um subgrupo $H \subset G$ é dito **subgrupo caraterístico** quando $\sigma(H) \subset H$ para todo $\sigma \in Aut(G)$.

Teorema 2: Se $Q_i \subsetneq Q$ é um subgrupo característico de Q e então o código não é controlável.

Prova.- Seja $\omega : G \to Q$ um homomorfismo sobrejetor da definição de codificador convolucional. Então, se $\pi : G \to G/N$ é o homomorfismo natural e $\psi : Q \to G/N$ é o homomorfismo usado em (1), temos que ω depende de $\varphi \in Aut(Q)$. Isto é, $\omega = \varphi_o \psi_o^{-1} \pi$, vide Figura 1. Logo, $\omega(x, Q_i) = \varphi_o \psi_o^{-1} \pi(x, Q_i) = Q_i$, para todo $x \in X$. ■

Exemplo 2: Considere a extensão $G \cong \mathbb{Z}_{2\phi_\varsigma} D_8$ do Exemplo 1. Considere o codificador $M = (\mathbb{Z}_2, Y, D_8, \omega, \nu)$, onde $\omega : \mathbb{Z}_{2\phi_\varsigma} D_8 \to D_8$ é definida por

$(0, R_0) \mapsto R_0$	$(1, R_0) \mapsto R_2$	$(0, R_2) \mapsto R_0$	$(1, R_2) \mapsto R_2$
$(0, R_1) \mapsto R_1$	$(1, R_1) \mapsto R_3$	$(0, R_3) \mapsto R_1$	$(1, R_3) \mapsto R_3$
$(0, d_1) \mapsto d_1$	$(1, d_1) \mapsto d_2$	$(0, d_2) \mapsto d_1$	$(1, d_2) \mapsto d_2$
$(0, H) \mapsto V$	$(1, H) \mapsto H$	$(0, V) \mapsto V$	$(1, V) \mapsto H$

O homomorfismo de codificação ν não tem importância en este caso. Temos,

$$Q_1 = \omega(X, R_0) = \{\omega(x, R_0) \ ; \ x \in \mathbb{Z}_2\} = \{R_0, R_2\}$$

Más $Q_1 = \{R_0, R_2\}$ é um grupo característico de D_8, logo o código associado a M é não controlável, vide a treliça do código na Figura 2.

IV. Conclusões

Neste artigo temos apresentado um critério seguro que permite descartar grupos abastratos associados a extensões do grupo das entradas(informações) e o grupo dos estados. Este descarte permite desconsiderar grupos cujos codificadores produzam códigos não controláveis. Isto facilitaria, usando alguma rotina no sistema GAP [6], por exemplo, a busca de códigos convolucionais que efetivamente sejam controláveis fato que por sua vez pode ser de utilidade na escolha dos parámetros que são de interesse como distância do código ou perfomance, quando o código é analizado sob o ponto de vista geométrico.

Referências

[1] Hall M. Jr..; *The Theory of Groups*, MacMillan, New York, 1959.

[2] Rotman J. J.; *An Introduction to the Theory of the Groups*, Fourth Ed., Springer Verlag 1995.

[3] H.A. Loeliger; "Signal sets matched to groups", *IEEE Transactions on Information Theory* Vol 37, No 6, pp 1675-1682, November 1991.

[4] H.A. Loeliger, Mittelholzer T.; "Convolutional Codes Over Groups", *IEEE Transactions on Information Theory* Vol IT 42, No 6, pp 1659-1687, November 1996.

[5] G.D.Forney, "Geometrically uniform codes" *IEEE Trans. Inform. Theory*; vol. IT-37 No 5, pp. 1241-1260, 1991.

[6] The GAP Group — Groups, Algorithms, and Programming, Version 4.2; Aachen, St Andrews, 1999. (http://www-gap.dcs.st-and.ac.uk/ gap)

[7] G. Ungerboeck; "Channel coding with multilevel phase signal", *IEEE Transactions on Information Theory* Vol IT 25, pp 55-67, Jan 1982.

[8] J. Bali, Rajan, S; "Block-Coded modulation using two-level group-codes over dihedral groups", *IEEE Transactions on Information Theory* Vol IT 44, pp 1620-1631, July 1998.

[9] A. Garcia, Y Lequain, *Álgebra, um Curso de Introdução;* Projeto Euclides 18, IMPA Rio de Janeiro, 1988.

[10] J.C.Willems, "Models for dynamics"em *Dynamics Technical Report* vol. 2, U.Kirchgraber e H.O.Walther, Eds. Wiley and Teubner, 1989.

[11] G.D. Forney and M.D. Trott, "The dynamics of group codes: state spaces, trellis diagrams and canonical encoders", *IEEE Trans. Inform. Theory*, vol IT 39(5):1491-1513, September 1993.

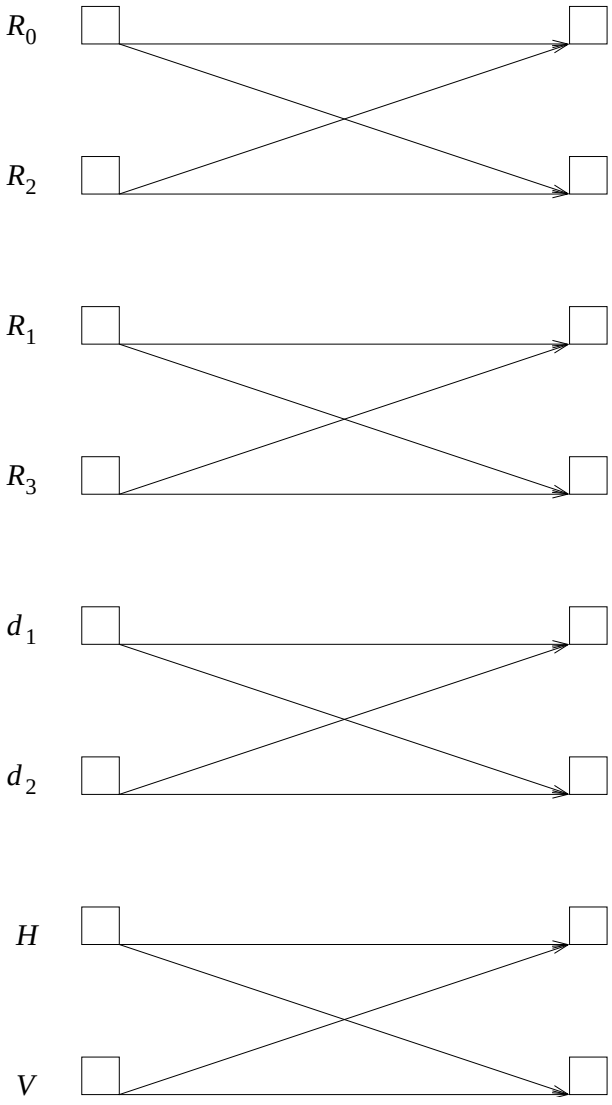

Fig. 2. Seção treliça do codificador M determinado por ω