Códigos para o Canal T-Usuários via Ação de Grupos

Coding for T-User Multiple Access Channel for Action Groups

João Bosco Batista Lacerda
Departamento de Matemática
Universidade Federal da Paraíba – UFPB, João Pessoa, PB
boscolacerda@mat.ufpb.br

Resumo: Neste artigo é apresentada uma generalização, via ação de grupos, dos Códigos Corretores de Erros para o Canal Aditivo Binário T - Usuários, obtidos em [1]. Também é determinado um limite superior para o número de códigos equivalentes ao código determinado por uma matriz diferença A bem como para o estabilizador G_A, onde G é um grupo finito.

Palavras-chave: ação; canal; código; grupo.

Abstract: This study presents a generalization, through action groups, of Error-Correcting Codes for T - User Binary Adder Channel, got in [1]. It is also determined an upper limit for the number of codes which are equivalent to the determined code by $A =$ difference matrix, and stabilizer G_A, when $G =$ finite group.

Key words: action; channel; code; group.

1 Introdução

Códigos para o Canal Aditivo Binário de Múltiplo Acesso com dois usuários (2-BAC) na ausência de ruídos foram estudados por Kasami e Lin [2, 3]. Chang e Weldon [4] apresentam uma classe de códigos denominados de Códigos Univocamente Decodificáveis para o Canal de Múltiplo Acesso T-Usuários. Fergunson [5] generaliza os códigos de Chang e Weldon via ação de grupos e obtém classes de códi-

Recebido em 07/07/2011 - Aceito em 23/02/2012.

gos equivalentes univocamenrte decodificáveis. Wilson [6] generaliza os códigos de Chang e Weldon através do produto de Kronecker e obtém uma classe de códigos corretores de erro para o Canal Aditivo Binário T-Usuários. Mais recentemente, Rocha Jr. e Alcoforado [7], apresentaram uma classe de códigos para o canal 2-BAC denominados de Códigos Fortemente Ortogonais Balanceados e verificaram que esses códigos possuem a mais alta taxa de transmissão atingível com a construção linear.

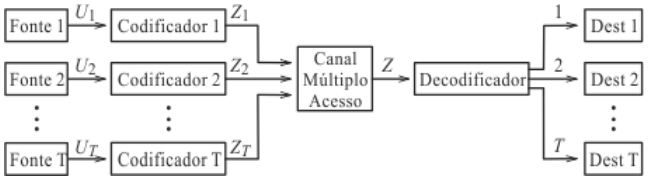

Figura 1. Sistema de Comunicação Múltiplo Acesso

O principal objetivo deste trabalho é generalizar os códigos obtidos [1] via a noção de ação de grupos. O sistema de comunicação considerado é o Canal de Múltiplo Acesso T-Usuários onde T fontes, estatisticamente independentes, transmitem dados para T destinatários sobre um canal comum sem memória, veja figura 1. A cada um dos T usuários é dado um código constituinte C_i consistindo de dois vetores binários X_i e Y_i de comprimento N [4]. Um vetor Z_i é escolhido e transmitido por cada usuário. Se o canal é sem ruído, o vetor recebido é o vetor $Z = Z_1 + Z_2 + \cdots + Z_T$, onde o sinal $+$ indica a adição de vetores.

2 Resultados básicos

Nesta seção, apresento alguns resultados básicos sobre Grupos e Ação de Grupos que serão necessários para o desenvolvimento deste trabalho. O leitor interessado em mais detalhes pode consultar [8].

Definição 1 Seja G um grupo e X um conjunto não vazio qualquer, uma ação à esquerda do grupo G em X é uma função $* : G \times X \to X$, com $*(a,x) = a * x$, satisfazendo as seguintes condições:

1. $a*(b*x) = (ab)*x$, para todos $a, b \in G$ e $x \in X$;

2. $e_G * x = x$, para todo $x \in X$, onde e_G denota o elemento identidade de G.

Se G é um grupo finito com $|G| = n$ dizemos que n é o grau da ação de G em X ou que X é um G-conjunto de grau n. Analogamente, define-se uma ação à direita de G em X.

Sejam X e Y dois G-conjuntos não vazios. Uma função $\varphi : X \to Y$ é um G-hom*omorfismo* se

$$\varphi(gx) = g\varphi(x), \forall \quad g \in G \quad \text{e} \quad x \in X.$$

Um G-homomorfismo $\varphi : X \to Y$ é um G-isomorfismo se φ é bijetora. Neste caso, dizemos que X e Y são G-isomorfos e escrevemos $X \simeq Y$.

Proposição 1 Seja X um G-conjunto não vazio transitivo. Então $X \simeq \frac{G}{G_x}$, $\forall\, x \in X$, em que $G_x = \{a \in G : ax = x\}$ é o estabilizador de x.

Corolário 1 Seja X um G-grupo não vazio. Então $\mathcal{O}(x) \simeq \frac{G}{G_x}, \forall\, x \in X$, em que $\mathcal{O}(x)$ é a órbita do elemento x.

Basta observar que G age transitivamente sobre $O(x)$.

Corolário 2 Seja X um G-grupo não vazio. Então $|\mathcal{O}(x)| = \left[G : G_x\right]$.

3 Códigos para o canal T- usuário

Um código para o canal T-usuários é uma T-upla $(C_1, \ldots, C_T)$ em que cada C_i, denominado de código constituinte, é formado por duas palavras códigos

$$C_i = \{X_i, Y_i\}$$

e X_i, Y_i são vetores códigos binários de comprimento N.

Sejam $(C_1, \ldots, C_T)$ um código T-usuários e

$$\mathbf{Z} = (z_1, \ldots, z_N) = \sum_{i=1}^{T} \mathbf{Z}_i$$

onde $z_i \in \{0, 1, \ldots, T\}$ e $\mathbf{Z}_i$ é um vetor código do i-ésimo código constituinte C_i.

A L-distância entre os vetores $\mathbf{Z}$ e $\mathbf{Z}'$, $\mathbf{Z} \neq \mathbf{Z}'$ é definida como sendo

$$d_L(\mathbf{Z}, \mathbf{Z}') = \sum_{i=1}^{N} |z_i - z_i'| = ||\mathbf{Z} - \mathbf{Z}'||.$$

A L-distância mínima $d_{\min}$ do código T-usuários é o menor valor de $d_L(\mathbf{Z},\mathbf{Z}')$ para todo $\mathbf{Z} \neq \mathbf{Z}'$.

Um código T-usuários é δ-decodificável se, e somente se, $d_L(\mathbf{Z},\mathbf{Z}') \geq \delta$ para todo $\mathbf{Z} \neq \mathbf{Z}'$.

Uma matriz diferença é uma matriz com entradas no corpo $\mathbb{F}_3$. Dessa forma, se $(C_1,\ldots,C_T)$ é um código binário T-usuários de comprimento N então o vetor

$$d_i = X_i - Y_i$$

é claramente um vetor diferença. Assim, temos que a matriz

$$D = [d_1,\ldots,d_T]^t$$

em que o símbolo t denota a matriz transposta é a matriz diferença $T \times N$ do código T-usuários $(C_1,\ldots,C_T)$.

De Chang e Weldon [4] temos que um código T-usuários é univocamente decodificável se, e somente se, os vetores linhas da matriz diferença associada ao código T-usuários forem linearmente independentes sobre $\mathbb{F}_3$.

Reciprocamente, dada uma matriz diferença $D_{T\times N}$, tal que os vetores linhas sejam linearmente independentes sobre $\mathbb{F}_3$ então é possível construir um código T-usuários univocamente decodificável $(C_1,\ldots,C_T)$.

Dada a matriz diferença

$$D_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

o código 2-usuários univocamente decodificável associado à matriz D_1 é formado pelos seguintes códigos constituintes [4]:

$$\begin{aligned} C_1 &= \{(1,1),(0,0)\} \\ C_2 &= \{(1,0),(0,1)\} \end{aligned}$$

A seguinte proposição pode ser conferida em [4].

Proposição 2 Para todo inteiro $k \geq 1$ a matriz diferença

$$D_k = \begin{bmatrix} D_{k-1} & D_{k-1} \\ D_{k-1} & -D_{k-1} \\ I_{k-1} & 0_{k-1} \end{bmatrix}$$

define um código univocamente decodificável $(k+2)2^{k-1}$-usuários de comprimento 2^k, onde I_{k-1} e 0_{k-1} são, respectivamente, a matriz identidade e a matriz nula de ordem 2^{k-1}.

Agora, sejam $D_0^{(k)} = D_k$ e

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

então o produto tensorial [9], é uma matriz diferença

$$D_i^{(k)} = D_{i-1}^{(k)} \otimes H$$

que define um código $(k+2).2^{k-1+i}$-usuários de comprimento $N = 2^{k+i}$ e distância mínima $d_{\min} = 2^i$.

Exemplo 3.1 Para $k = i = 1$, o produto tensorial

$$D_1^{(1)} = D_0^1 \otimes H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

define um código 6-usuários de comprimento $N = 4$ e $d_{\min} = 2$.

4 Códigos via ação de grupos

Uma matriz de permutação generalizada de ordem n é uma matriz $P_{n\times n}$ em que cada linha e cada coluna possui um único elemento não nulo que pode ser 1 e -1. O conjunto das matrizes de permutações generalizadas de ordem n formam um grupo multiplicativo finito de ordem $n!2^n$. O leitor interessado em mais detalhes pode consultar [1].

Temos que, se D_0 é uma matriz diferença de ordem $2 \times N_0$ que define um código 2-usuários δ-decodificável de comprimento N_0 e se H é a matriz de Hadamard de ordem q, então o produto de Kronecker $H \otimes D_0$ é uma matriz diferença de ordem $2q \times qN_0$ e define um có digo 2q-usuários de comprimento qN_0 e distância mínima, $d_{\min} = q\delta$ [1].

Exemplo 4.1 Sejam D_0 a matriz diferença de ordem 2×4 dada por

$$D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

e H_2 a matriz de Hadamard de ordem 2. Então o produto de Kronecker

$$H_2 \otimes D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

é uma matriz difrença de ordem 4×8 e define um código 4-usuários de comprimento 8 e distância mínima, $d_{\min} = 8$.

Agora, sejam G_1 e G_2 os grupos das matrizes de permutações generalizadas de ordem $2q$ e qN_0, respectivamente. Sejam G o grupo finito

$$G = G_1 \times G_2 = \{(P, Q) : P \in G_1 \quad \text{e} \quad Q \in G_2\}$$

e S o conjunto das matrizes diferenças de ordem $2q \times N_0 q$

$$S = \{A = H_q \otimes D_0 : q = 2 \text{ ou } q \equiv 0 \mod 4\}$$

em que D_0 é uma matriz diferença de ordem $2 \times N_0$, com $N_0 \geq 2$.

Vamos definir a ação do grupo G em S por

$$\begin{array}{rccc} * : & G \times S & \to & S \\ & (P,Q,A) & \longmapsto & PAQ \end{array}.$$

Qualquer matriz $A_{m\times n}$, com entradas em um corpo F, pode ser reduzida através de um número finito de operações elementares sobre as linhas e colunas de A, a uma única matriz $m \times n$ da forma

$$\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}$$

em que I_k é a matriz identidade de ordem k e $k = posto(A) \leq \min\{m,n\}$. Desde que operações elementares de linhas e colunas consistem em multiplicar a matriz A à esquerda e à direita por convenientes matrizes invertíveis [10], então existem matrizes $P \in G_1$ e $Q \in G_2$ tais que

$$PAQ = \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}.$$

É fácil ver que o número de classes de equivalências é menor ou igual a $k = posto(A) = \min\{m,n\}$. Assim, temos que

$$|\mathcal{O}(A)| = posto(A) \leq \min\{m,n\},$$

isto é, o número de matrizes equivalentes a A é menor ou igual ao $\min\{m,n\}$. Por outro lado, pelo colorário 2, temos que

$$|G_A| \leq k\,|G|$$

em que $k = \frac{1}{\min\{m,n\}}$. O exemplo 4.2 ilustra esse resultado.

Exemplo 4.2 Considere a matriz

$$A = H_2 \otimes D_0$$

do exemplo 4.1 e sejam G_1 e G_2 os grupos multiplicativos de matrizes de permutações generalizadas de ordem 4 e 8, respectivamente. Então a matriz A é equivalente a uma matriz da forma

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Dessa forma, temos que o número de matrizes equivalentes a A é igual ao posto $(A) = 4$, isto é, existem 4 códigos 4-usuários de comprimento 8 equivalentes ao código 4-usuários definido pela matriz A.

5 Conclusões

Neste trabalho, apresentei uma classe de códigos equivalentes, por ação de grupos, para o Canal Aditivo Binário T-usuários bem como limitante superior para o número de códigos equivalentes via essa a ção e para o estabilizador G_A, onde A é uma matriz diferença e G é um grupo finito.

6 Agradecimentos

Gostaria de deixar os meus agradecimentos aos Referees pelas valiosas sugestões.

7 Referências

[1] LACERDA, J. B. B. Códigos Corretores de Erros e Algoritmos de Decodificação para o Canal T-Usuário de Múltiplo Acesso. Tese de Doutorado, Universidade de Campinas, UNICAMP, Brasil, 1994.

[2] KASAMI, T.; LIN, S. Coding for a multiple access channel. *IEEE T Inform Theory*, v. IT-22, n. 2, p. 129–137, 1976.

[3] KASAMI, T.; LIN, S. Bounds on the achievable rate of block coding for a memoryless multiple-access channel. *IEEE T Inform Theory*, v. IT-24, n. 1, p. 187–197, 1978.

[4] CHANG, S. C.; WELDON, E. J. Coding for T-user multiple access channels. *IEEE T Inform Theory*, v. 25, n. 6, p. 684–691, 1979.

[5] FERGUNSON, T. J. Generalized T-user codes for multiple-acess channels. *IEEE T Inform Theory*, v. IT-28, n. 5, p. 775–778, 1982.

[6] WILSON, J. H. Error correcting codes for T-user binary adder channel. *IEEE T Inform Theory*, v. IT-34, n. 5, p. 888–890, 1988.

[7] ROCHA JR., V. C.; ALCOFORADO, M. L. M. G. Códigos para o canal aditivo com dois usuários binários. *Rev Soc Bras Telecomunicações*, v. 16, n. 1, p. 46–51, 2001.

[8] GARCIA, A.; LEQUAIN, Y. Elementos de Álgebra. IMPA-Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2003.

[9] LACERDA, J. B. B.; SILVA, A. A. Códigos para o canal T-usuários via o produto tensorial, *Seminário Brasileiro de Análise - SBA*, n. 68, 2008.

[10] BROWN, W. C. Matrices over commutatives rings, Marcel Dekker, Inc.: New York-Basel-Hong Kong, 1993.