Códigos para o Canal Aditivo com Dois Usuários Binários

Maria de Lourdes M.G. Alcoforado e Valdemar C. da Rocha Jr.,
Grupo de Pesquisa em Comunicações - CODEC
Departamento de Eletrônica e Sistemas
Universidade Federal de Pernambuco
Caixa Postal 7800, CEP 50.711-970 Recife PE BRASIL
Tel.: (081) 271-8213, Fax: (081) 271-8215
vcr@npd.ufpe.br

Resumo – Códigos para o canal aditivo com dois usuários binários (2-BAC) são investigados neste trabalho, na situação em que o código empregado por um dos usuários é linear e não há ruído no sistema. Especificamente é apresentada uma dedução mais simples para a taxa de transmissão de códigos lineares fortemente ortogonais, são introduzidos os códigos lineares fortemente ortogonais balanceados e os códigos de paridade repetida, com as respectivas taxas de transmissão. O algoritmo de Cabral, para a construção linear de códigos para o 2-BAC, foi implementado pela primeira vez e alguns dos códigos construídos são aqui apresentados.

1. Introdução

O mais simples modelo de canal de acesso múltiplo é o representado pelo *canal aditivo com dois usuários binários* (2-BAC), na ausência de ruído [1]. Neste sistema dois usuários geograficamente separados tentam enviar dados binários através de um mesmo canal de comunicações. A função utilizada neste canal para combinar os dois usuários é a adição sobre os reais, onde cada usuário tem como alfabeto o conjunto $F_2 = (0, 1)$. A entrada do canal consiste, portanto, de duplas binárias x_i, w_i e a saída $y_i = x_i + w_i$, consiste de símbolos do alfabeto $\{0, 1, 2\}$.

Um dos principais objetivos dos pesquisadores que investigam o 2-BAC é obter códigos unicamente decodificáveis com taxas de transmissão tão próximas à fronteira da região de capacidade [1] quanto possível. Cabral [2] determinou um algoritmo para, a partir de um código C_1 linear específico, produzir um código C_2 com o maior número possível de palavras-código. Mais especificamente, Cabral determinou condições que dois conjuntos de vetores binários devem satisfazer para garantir sua decodibilidade única sobre o 2-BAC, dando ênfase ao caso em que um dos conjuntos de vetores é um código de bloco linear. Os resultados obtidos por Cabral permitem dividir a busca de vetores para C_2 no espaço das n-uplas binárias, i.e., $C_2 \in F_2^n$, em buscas em subconjuntos de F_2^n, de menor cardinalidade e independentes entre si.

Na *Seção 2* apresentamos a caracterização do 2-BAC, tratando da decodibilidade única e dos códigos lineares para o 2-BAC. Na *Seção 3* apresentamos uma revisão sucinta de códigos fortemente ortogonais [2] e uma dedução mais simples para a taxa de transmissão dos mesmos. Nas *Seções 4* e *5* introduzimos os códigos lineares fortemente ortogonais balanceados e os códigos de paridade repetida [3], respectivamente, acompanhados de expressões analíticas para as correspondentes taxas de transmissão. Na *Seção 6* apresentamos alguns dos códigos obtidos da construção linear de Cabral, implementada pela primeira vez. Finalmente na *Seção 7* apresentamos as conclusões finais e alguns comentários.

2. Canal 2-BAC

Consideramos no que segue que os dois usuários utilizam códigos binários de mesmo comprimento n, operam na mesma freqüência, transmitem ao mesmo tempo, operam com sincronismo de palavra e existe um único decodificador. Supomos que os dois usuários escolhem independentemente as respectivas palavras-código a serem transmitidas. O usuário 1 envia palavras-código de um código de bloco C_1; o usuário 2 envia palavras-código de um código de bloco C_2. Representamos por (C_1, C_2) um código de comprimento n para dois usuários, onde o código constituinte C_1 tem L palavras $\{x_1, x_2, \ldots, x_L\}$ e o código constituinte C_2 tem M palavras $\{w_1, w_2, \ldots, w_M\}$. A taxa de transmissão conjunta R do par (C_1, C_2) é dada por:

$$R = R_1 + R_2 = \frac{\log_2 L}{n} + \frac{\log_2 M}{n}$$

Para pontos (R_1, R_2) dentro da região de capacidade do canal, existem os codificadores e o decodificador tais que cada remetente pode se comunicar com o receptor com probabilidade de erro zero ou muito pequena.

2.1. Decodibilidade única

Consideremos uma extensão para o 2-BAC onde cada entrada é uma n-upla binária, denotadas respectivamente por $\mathbf{x}$ e $\mathbf{w}$ sendo

$$\begin{aligned} \mathbf{x} &= (x_1, x_2, \ldots, x_n) \\ \mathbf{w} &= (w_1, w_2, \ldots, w_n) \end{aligned}$$

a saída para o 2-BAC será então,

$$\mathbf{y} = (x_1 + w_1, x_2 + w_2, \ldots, x_n + w_n)$$

Definindo as operações de adição e multiplicação binárias sobre n-uplas binárias como as respectivas operações sobre F_2, aplicadas componente a componente temos que,

$$\begin{aligned} \mathbf{x} \oplus \mathbf{w} &= (x_1 \oplus w_1, x_2 \oplus w_2, \ldots, x_n \oplus w_n) \\ \mathbf{x}.\mathbf{w} &= (x_1.w_1, x_2.w_2, \ldots, x_n.w_n) \end{aligned}$$

Nas referências [2] e [4] foi mostrado que

$$\mathbf{x}+\mathbf{w}=\mathbf{x}\oplus\mathbf{w}+2\mathbf{x}.\mathbf{w},$$

resultado este que permitiu tratar a síntese de códigos binários para o 2-BAC considerando apenas as operações lógicas $\oplus$ (ou-exclusivo) e . (e-lógico). Nosso interesse no canal 2-BAC é construir um par de códigos C_1 e C_2 de modo que:

Condição 1 *O decodificador deve ser capaz de decodificar o vetor* $\mathbf{y}$ *recebido, sem ambigüidade, nas duas palavras-código que foram transmitidas pelos usuários 1 e 2. Isto é, se para quaisquer* $\mathbf{x_1}\in C_1, \mathbf{x_2}\in C_1$ *e* $\mathbf{w_1}\in C_2, \mathbf{w_2}\in C_2$ *tais que* $\mathbf{x_1}\neq\mathbf{x_2}$, *e* $\mathbf{w_1}\neq\mathbf{w_2}$, *então* $\mathbf{x_1}+\mathbf{w_1}\neq\mathbf{x_2}+\mathbf{w_2}$.

Condição 2 *As taxas* (R_1,R_2), *respectivamente de* C_1 *e* C_2, *devem situar-se dentro da região de capacidade e tão próximas à fronteira quanto possível.*

Um par de códigos (C_1,C_2) que satisfaz a *Condição 1* acima é dito ser unicamente decodificável. Eventualmente faremos referência ao par (C_1,C_2) como "o código" (C_1,C_2).

2.2. Códigos lineares

Um caso de interesse no estudo de códigos para o 2-BAC é aquele em que apenas um dos códigos constituintes é linear.

Definição 1 *Um código* (C_1,C_2) *de comprimento* n *para o 2-BAC é dito ser um código linear se um dos códigos constituintes for um código linear de parâmetros* (n,k).

O teorema a seguir, provado por Weldon [5], estabelece limitantes para as taxas alcançáveis por códigos lineares.

Teorema 1 *Seja* C_1 *um código constituinte linear com parâmetros* (n,k_1), *então a região de capacidade para um par* (C_1,C_2) *unicamente decodificável é limitada superiormente por* $(R_1,R_2)\leq(k_1/n,(1-k_1/n)\log 3)$.

Decorre do *Teorema 1* que códigos lineares para o 2-BAC possuem a desvantagem de não atingirem a capacidade quando o código constituinte linear tiver taxa maior que $(\log_2 3-1)/\log_2 3$. Rocha [6] observou que na demonstração do fererido teorema não é feito uso da linearidade de C_1 e, portanto, o resultado do *Teorema 1* é válido num contexto mais geral, quando C_1 é apenas um código sistemático, podendo ser também não linear.

3. Códigos fortemente ortogonais

Cabral [2] introduziu códigos lineares fortemente ortogonais e determinou analiticamente a taxa de transmissão (vide *Teorema 2*) destes códigos.

Definição 2 *Um código de bloco linear binário* C_1, *tendo sua matriz geradora* G *na forma sistemática, é definido como fortemente ortogonal se para a i-ésima linha de* G, *denotada por* $\mathbf{c}_i$ *e considerada como um vetor, tivermos:* $\mathbf{c}_i.\mathbf{c}_j=0,\ i\neq j,\ i,j\in\{1,2,\ldots,k\}$.

Teorema 2 *A taxa* R_2 *do código* C_2, *obtido a partir do código fortemente ortogonal* C_1 (n,k) *é dada por*

$$R_2=\frac{\log_2(\sum_{i=0}^{k}(2^i N_i)+l_{k+1})}{k+\sum_{i=1}^{k}l_i+l_{k+1}} \qquad (1)$$

$$G=\left[\begin{array}{cccccc}
\overbrace{10\,..\,0}^{k} & \overbrace{11\,..\,1}^{l_1} & \overbrace{00\,..\,0}^{l_2} & \ldots & \overbrace{0\,..\,0}^{l_k} & \overbrace{0\,..\,0}^{l_{k+1}}\\
01\,..\,0 & 00\,..\,0 & 11\,..\,1 & \ldots & 0\,..\,0 & 0\,..\,0\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
00\,..\,1 & 00\,..\,0 & 00\,..\,0 & \ldots & 1\,..\,1 & 0\,..\,0
\end{array}\right]$$

Figura 1: Matriz geradora

$$G'=\left[\begin{array}{cccccc}
\overbrace{11\,..\,1}^{l_1+1} & \overbrace{00\,..\,0}^{l_2+1} & \overbrace{00\,..\,0}^{l_3+1} & \ldots & \overbrace{0\,..\,0}^{l_k+1} & \overbrace{0\,..\,0}^{l_{k+1}}\\
00\,..\,0 & 11\,..\,1 & 00\,..\,0 & \ldots & 0\,..\,0 & 0\,..\,0\\
00\,..\,0 & 00\,..\,0 & 11\,..\,1 & \ldots & 0\,..\,0 & 0\,..\,0\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
00\,..\,0 & 00\,..\,0 & 00\,..\,0 & \ldots & 1\,..\,1 & 0\,..\,0
\end{array}\right]$$

Figura 2: Matriz geradora equivalente

onde os l_i's estão ilustrados na *Figura 1* e N_i é dado por

$$N_i=\sum_{s_1=1}^{k}\sum_{s_2=s_1+1}^{k}\ldots\sum_{s_i=s_{i-1}+1}^{k}(2^{l_{s_1}}-1)(2^{l_{s_2}}-1)\ldots(2^{l_{s_i}}-1).$$

Apresentamos a seguir uma dedução alternativa e mais simples do *Teorema 2*.

3.1. Análise de códigos fortemente ortogonais

É conveniente representarmos a matriz geradora do código linear fortemente ortogonal C_1 na forma sistemática mostrada na *Figura 1*. Outra forma de representação da matriz geradora é obtida quando a retiramos da forma sistemática, agrupando todas as $l_j,\ 1\leq j\leq k+1$, colunas idênticas, inclusive as k colunas mais à esquerda. Podemos visualizar esta representação através da *Figura 2*.

Neste momento faz-se necessário utilizarmos a construção de Weldon [5] para códigos unicamente decodificáveis, onde 0^n e 1^n denotam respectivamente as n-uplas toda zero e toda 1.

Construção 1 *Seja* $C_1=(0^n,1^n)$ *e seja* C_2 *constituído por todas as* n*-uplas exceto* 1^n.

Este código é unicamente decodificável pois todos as palvras-código de C_2 são distintas e todas as n-uplas para o 2-BAC serão da forma (0^n+c_{2j}) ou (1^n+c_{2j}), onde c_{2j} denota as palavras-código de C_2, donde verificamos que $(0^n+c_{2j})\cap(1^n+c_{2j})=\phi$. O número total de palavras-código obtidas para C_2 é $|C_2|=2^n-1$ e o número de palavras-código de C_1 é $|C_1|=2$. Analisando a matriz da *Figura 2* vemos que podemos representá-la como sendo formada por $k+1$ submatrizes geradoras, da seguinte forma

$$G'=\left[\begin{array}{c} G_1G_2G_3\ldots G_{k+1}\end{array}\right]$$

Vemos que cada uma das submatrizes geradoras $G_i,\ 1\leq i\leq k$, gera um código de bloco linear com parâmetros $(l_i,1)$

e cada uma delas gera duas palavras-código $(0^{l_i}, 1^{l_i})$. Vamos denotar por C_{1i}, o código gerado pela submatriz geradora G_i e por C_{2i}, o código encontrado com o máximo número de palavras-código possível, de modo a obtermos a decodibilidade única de (C_{1i}, C_{2i}) no 2-BAC. Observamos que o código C_{2i} encontrado através do algoritmo implementado é o mesmo obtido pela *Construção 1*.

Vamos a partir de agora analisar a submatriz geradora G_{k+1}. Vemos que ela gera um código cujo vetor nulo é sua única palavra-código. O código $C_{2,k+1}$ portanto pode ter qualquer uma das l_{k+1}-uplas como palavras-código, incluindo o vetor nulo. Portanto o máximo $|C_{2,k+1}|$ é $2^{l_{k+1}}$. Como temos as $k+1$ submatrizes lado a lado, formando a matriz geradora G, as palavras-código de C_2 resultam da concatenação das palavras-código dos C_{2i} e portanto o máximo número de palavras-código pertencentes ao código C_2 é

$$|C_2| = \prod_{l_i=1}^{k} (2^{l_i} - 1) 2^{l_{k+1}}$$

Podemos sintetizar o resultado obtido acima no seguinte teorema.

Teorema 3 *A partir do código binário linear fortemente ortogonal C_1 encontramos um código C_2, de máxima cardinalidade, contendo $|C_2| = \prod_{l_i=1}^{k}(2^{l_i}-1)2^{l_{k+1}}$ palavras-código, de tal modo que o par (C_1, C_2) é unicamente decodificável no 2-BAC.*

Observamos que os resultados dos *Teoremas 2* e *3* e são idênticos. Para taxas R_1 maiores que 1/2, necessariamente alguns dos l_i's na *Figura 1* serão iguais a zero. Considerando o caso particular em que $l_{k+1} = 0$ e cada um dos demais l_i's, $1 \leq i \leq k$, é igual a 1 ou a 0, resulta que $\sum_{i=1}^{k} l_i = n-k$ e portanto

$$|C_2| = (2^2 - 1)^{n-k}.$$

A taxa R neste caso resulta igual a

$$R = \frac{k}{n} + \frac{(n-k)}{n} \log_2 3$$

que coincide com o limitante superior do *Teorema 1*. Introduzimos a seguir os códigos lineares fortemente ortogonais balanceados.

4. Códigos fortemente ortogonais balanceados

Definição 3 *Seja C_1 um código de bloco linear sobre F_2 de parâmetros (n, k), com matriz geradora G na forma sistemática. Denominando a i-ésima linha da matriz G por $\mathbf{c}_i$ e considerando-a como um vetor em F_2^n, dizemos que C_1 é um código linear fortemente ortogonal balanceado se $\mathbf{c}_i.\mathbf{c}_j = 0$, $i, j \in (1, 2, \ldots, k)$, com $i \neq j$; e cuja matriz geradora tem a mesma quantidade de 1's em cada uma de suas linhas.*

Uma propriedade interessante de códigos fortemente ortogonais balanceados pode ser observada com o auxílio da *Figura 1*, considerando $l_i + 1 = l, 1 \leq i \leq k$ e $l_{k+1} = s$ e grupando as $kl + s$ colunas em k blocos de l colunas idênticas não-nulas e um bloco com s colunas toda zero. A matriz resultante G' gera um código $C_{1'}$ equivalente a C_1 no sentido de que um é obtido do outro através de uma permutação de coordenadas. Aplicando o *Teorema 3* para matrizes fortemente ortogonais balanceadas, encontramos que,

$$|C_2| = |C_{2i}|^k 2^s = (2^l - 1)^k 2^s$$

pois cada palavra-código de C_2 será formada pela combinação das $(2^l - 1)$ palavras-código de cada um dos C_{2i}, $1 \leq i \leq k$, e das palavras-código de $C_{2,s}$. Neste caso temos que,

$$R_2 = \frac{\log_2 (2^l - 1)^k 2^s}{kl + s} = \frac{k}{kl + s} \log_2 (2^l - 1) + \frac{s}{kl + s}$$

$$R = R_1 + R_2 = \frac{k}{kl+s} + \frac{k}{kl+s} \log_2(2^l - 1) + \frac{s}{kl+s},$$

que para $s = 0$ e $l = 2$ reduz-se a

$$R = \frac{1}{2} + \frac{1}{2} \log_2 3$$

ou seja, para $s = 0$ e $l = 2$ estes códigos atingem o limitante de Weldon [5] para códigos lineares (*Teorema 1*).

5. Códigos de paridade repetida

Um outro caso de interesse é aquele em que a matriz geradora do código C_1 possui uma propriedade que denominamos de *paridade repetida*, a qual nos permite calcular o número de palavras-código pertencentes a C_2.

Definição 4 *Códigos de paridade repetida (n, k) são aqueles que possuem metade das palavras-código com os $n - k$ dígitos de paridade todos iguais a 0 e a outra metade das palavras-código com os $n-k$ dígitos de paridade todos iguais a 1.*

Exemplo 1 *O código C = (10111, 01111, 11000, 00000), no qual $n = 5$ e $k = 2$, é um código de paridade repetida pois, além de linear, tem metade das palavras-código com dígitos de paridade* 000 *e metade com* 111*, respectivamente.*

Nosso objetivo é, a partir da matriz geradora do código de paridade repetida C_1, determinar o máximo número de palavras-código de C_2, de modo a termos o par (C_1, C_2) unicamente decodificável no 2-BAC. O próximo teorema [3] fornece esta resposta.

Teorema 4 *Seja C_1 um código de paridade repetida. Quando a matriz geradora de C_1 possui*

1. *um número par de linhas em que os $n - k$ dígitos de paridade são 1's, o código C_2 construído a partir de C_1 tem um número máximo de $2^{n-k+1} - 2$ palavras-código.*

2. *um número ímpar de linhas em que os $n-k$ dígitos de paridade são 1's, o código C_2 construído a partir de C_1 tem um número máximo de $2^{n-k+1} - 1$ palavras-código.*

6. Resultados

O algoritmo de Cabral [2] permite encontrar o conjunto de maior cardinalidade de palavras-código para um código C_2 a partir de um código linear C_1 dado, de modo a garantir a decodibilidade única no 2-BAC. A nossa implementação do algoritmo de Cabral consiste dos seguintes passos.

1. É solicitada a matriz geradora de C_1, com k linhas e n colunas, e a partir desta são geradas todas as palavras-código de C_1.

2. Particionamos o conjunto das n-uplas binárias em classes laterais do espaço vetorial n-dimensional em relação a C_1, i.e., construímos o arranjo padrão segundo C_1.

3. Para cada classe lateral obtemos o conjunto $S_{v \oplus C_1} = \{\mathbf{x_3} \in C_1; \mathbf{x_3}.(\mathbf{x_1} \oplus \mathbf{w_2}) = 0, \mathbf{x_1} \in C_1\} \subseteq C_1\}$.

4. Tendo o conjunto $S_{v \oplus C_1}$ determinamos o conjunto $Z_{v \oplus C_1} = \cup_{i=0}^{m-1} Z_{w_{2_i}} \subseteq v \oplus C_1$, para cada classe lateral, onde $Z_{w_{2_i}} = \{w_2 \oplus x_3 \in v \oplus C_1, \forall x_3 \in S_{v \oplus C_1}, x_3 \neq 0\}$.

5. Determinamos o conjunto $A_{v \oplus C_1}$, formado por todas as palavras-código pertencentes a C_2 em uma determinada classe lateral. O conjunto formado pelos $A_{v \oplus C_1}$'s de todas as classes laterais, acrescido de uma palavra-código em comum com C_1, será o próprio C_2. Denotaremos por M o número de palavras-código de C_2.

Exemplo 2 *Seja C_1 o código $(7,3)$ cuja matriz geradora G é a seguinte*

$$G = \begin{bmatrix} 1\,0\,0 & 0\,0\,1\,1 \\ 0\,1\,0 & 0\,1\,1\,0 \\ 0\,0\,1 & 1\,0\,0\,0 \end{bmatrix}$$

O código C_2 construído a partir do algoritmo de Cabral tem 54 palavras-código, mostradas na Figura 3. As taxas de transmisão de R_1, R_2 e R são as seguintes.

$$\begin{aligned} R_1 &= 0,428 \\ R_2 &= 0,822 \\ R &= R_1 + R_2 = 1,25. \end{aligned}$$

A importância dos códigos fortemente ortogonais balanceados, advém do fato que através de busca exaustiva, para diversos valores dos parâmetros, verificamos que estes códigos possuem a mais alta taxa de transmissão atingível com a construção linear. Consideremos n o comprimento das palavras-código e k a dimensão do código C_1. Seja M o número de palavras-código de C_2, R_1 a taxa de transmissão de C_1, R_2 a taxa de transmissão de C_2 e R a taxa de transmissão conjunta no 2-BAC. Encontramos todas as matrizes geradoras possíveis para alguns valores de n e k. Utilizamos então o algoritmo implementado acima para obtenção das palavras-código de C_2. Apresentamos os resultados nas tabelas seguintes:

```
0000000 0000001 1000010 0000010 0000011 1000000
0000100 0100010 0000101 0100011 1000110 1100000
0000110 0100000 0000111 0100001 1000100 1100010
0001000 0010000 0001001 0010001 1001010 1010010
0001010 0010010 0001011 0010011 1001000 1010000
0001100 0010100 0101010 0110010 0001101 0010101
0101011 0110011 1001110 1010110 1101000 1110000
0001110 0010110 0101000 0110000 0001111 0010111
0101001 0110001 1001100 1010100 1101010 1110010
```

Figura 3: Palavras-código de C_2

1. $n = 4$ e $k = 2$

$\|G\|$	M	R_2	R_1	R
3	4	0,5	0,5	1
9	6	0,646	0,5	1,146
2	7	0,702	0,5	1,202
2	9	0,792	0,5	1,292

2. $n = 6$ e $k = 2$

$\|G\|$	M	R_2	R_1	R
5	16	0,667	0,333	1,000
38	24	0,764	0,333	1,097
40	28	0,801	0,333	1,134
17	30	0,818	0,333	1,151
2	31	0,826	0,333	1,159
60	36	0,862	0,333	1,195
68	42	0,899	0,333	1,232
8	45	0,915	0,333	1,248
12	46	0,921	0,333	1,254
6	49	0,936	0,333	1,269

7. Conclusões

O canal aditivo com dois usuários binários vem sendo investigado há quase trinta anos e algumas questões básicas ainda não foram respondidas satisfatoriamente como, por exemplo, a região de capacidade com probabilidade de erro zero ainda não é conhecida. Neste trabalho tivemos oportunidade de fazer a implementação computacional, na linguagem *Visual Basic*, de um algoritmo proposto na literatura, mas até então não implementado, para obtenção de um código C_2 de máxima cardinalidade, a partir de um código linear C_1 e assim obtermos um código linear unicamente decodificável para o 2-BAC. Mostramos que a matriz geradora de um código fortemente ortogonal pode ser representada, de modo equivalente, como uma concatenação de matrizes mais simples e assim obtivemos uma expressão bastante concisa para o número de palavras-código de C_2. Introduzimos os *códigos fortemente ortogonais balanceados* e verificamos, através de busca exaustiva para diversos valores dos parâmetros, que estes códigos possuem a mais alta taxa de transmissão atingível com a construção linear. Introduzimos também os *códigos lineares de paridade repetida*, para os quais foram deduzidas as expressões para o número de palavras-código de C_2. Vimos analiticamente que a classe de códigos lineares para o 2-BAC não atinge todos os pontos da região de capacidade para o 2-BAC. Rocha [6] observou que os resultados de Weldon [5] para o 2-BAC são válidos também no caso em que ambos os códigos são não-lineares, sendo um deles sistemático, e conjecturou que a região de capacidade *proibida* para estes códigos não pode ser atingida com códigos unicamente decodificáveis. Dito de outro modo, pela conjectura de Rocha a região atingida não pode, em geral, ser atingida com probabilidade de erro igual a zero. Ahlswede e Balakirsky [11] propuseram recentemente uma classe de códigos não-lineares e não-sistemáticos, unicamente decodificáveis para o 2-BAC. As taxas de transmissão destes códigos, apesar de serem maiores do que as taxas alcançadas por outras construções anteriores, estão dentro da região de taxas atingíveis por códigos binários lineares. Podemos concluir, portanto, que a construção de códigos lineares para o 2-BAC é importante na medida em que alcança probabilidade de erro zero. Para alcançar taxas de transmissão mais elevadas propomos o estudo de classes de códigos, não necessariamente unicamente decodificáveis, mas com probabilidade de erro pequena na decodificação, com taxas de transmissão o mais próximo possível da fronteira da região de capacidade para o 2-BAC.

Referências

[1] T. Kasami and Shu Lin, "Coding for a multiple-access channel", *IEEE Trans. on Inform. Theory*, Vol. IT-22, Number 2, march 1976, pp. 129-137.

[2] H.A. Cabral, "Codificação para Canal de Acesso Múltiplo Síncrono", Dissertação de Mestrado, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brasil, novembro de 1994.

[3] M.L.M.G. Alcoforado, "Implementação algorítmica de códigos lineares para o canal aditivo com dois usuários binrios", Dissertação de Mestrado, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brasil, dezembro de 1999.

[4] H.A. Cabral and V. C. da Rocha, Jr., "Linear code construction for the 2-user binary adder channel", *IEEE Int. Symp. on Info. Theory*, Whistler, Canada, 1995, pp. 497.

[5] E. J. Weldon, Jr., "Coding for a multiple-access channel", *Information and Control*, Vol. 36, 1978, pp. 256-274.

[6] V. C. da Rocha, Jr., "Codificação para o 2-BAC", Seminário de pesquisa, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brasil, 1995.

[7] H.A. Cabral and V. C. da Rocha, Jr., "Coding for the 2-user binary adder channel", Relatório de pesquisa, Grupo de Pesquisa em Comunicações - CODEC, Universidade Federal de Pernambuco, 1995.

[8] V.C. da Rocha, Jr. and J. L. Massey, "A new approach to the design of codes for the binary adder channel", in *Cryptography and Coding III*, (Ed. M.J. Ganley), IMA Conf. Series, New Series Number 45. Oxford: Clarendon Press, 1993, pp. 179-185.

[9] T. Kasami and Shu Lin, "Bounds on the achievable rates of block coding for a memoryless multiple-access channel", *IEEE Trans. on Inform. Theory*, Vol. IT-24, Number 2, march 1978, pp. 187-197.

[10] R. Ahlswede and V. B. Balakirsky, "Construction of uniquely decodable codes for the two-user binary adder channel", *IEEE Trans. Inform. Theory*, Vol. 45, Number 1, January 1999, pp.326-330.

[11] I.N. Herstein, *Topics in Algebra*. New York: Blaisdell Publishing Company, 1964.