SOBRE A CAPACIDADE DE CANAL DE UM SISTEMA DE COMUNICAÇÃO COM UM LASER DE CO_2 CAÓTICO

Bartolomeu F. Uchôa Filho
GPqCOM/EEL/UFSC
Florianópolis-SC 88040-900
uchoa@eel.ufsc.br

Cecilio Pimentel
CODEC/DES/UFPE
Recife-PE 50711-970
cecilio@npd.ufpe.br

Renato M. de Moraes
ECE/Univ. of Maryland
College Park, MD, 20742
rmariz@zipmail.com

RESUMO

Pimentel apresentou um procedimento para se determinar a capacidade de canais discretos (sem ruído) com restrições de seqüências permitidas. Este procedimento, que se utiliza de técnicas combinatoriais, difere daquele desenvolvido por Shannon por não necessitar da descrição do canal através de diagrama de estados finitos (ou matriz de transição). Neste artigo, mostramos que este procedimento pode ser facilmente adaptado para o caso de alfabetos com símbolos de durações distintas, que tem como exemplo um sistema de comunicação com um laser de CO_2 caótico. A partir das restrições de seqüências do laser, que são conhecidas, determinamos a capacidade de canal deste sistema. Na literatura, estas restrições são simplificadas para tornar possível o cálculo da capacidade. Os nossos resultados comprovam que estas simplificações são aceitáveis.

1. INTRODUÇÃO

O *canal discreto sem ruído* (DNC, do inglês *discrete noiseless channel*) foi primeiramente estudado por Shannon em seu aclamado artigo de 1948 [2]. O DNC admite a transmissão sem ruído de *certas* seqüências de símbolos de durações possivelmente distintas pertencentes a um alfabeto q-ário. Seja $\mathcal{A}$ um conjunto de q símbolos representando este alfabeto. Suscintamente, diremos seqüências sobre $\mathcal{A}$. O conjunto de todas as seqüências sobre $\mathcal{A}$ permitidas pelo DNC será denotado por $\mathcal{S}$. Shannon considerou apenas os conjuntos $\mathcal{S}$ que pudessem ser descritos de maneira compacta, através de um grafo com um determinado número de estados, com ramos orientados interconectando estados, cada ramo rotulado com um símbolo de $\mathcal{A}$. $\mathcal{S}$ é então o conjunto de todas as possíveis seqüências obtidas a partir de caminhos no grafo.

O trabalho de C. Pimentel recebeu suporte parcial do CNPq através do processo No 300987/96-0

A capacidade do DNC, denotada por C, foi definida por Shannon como [2]:

$$C = \lim_{T\to\infty} \frac{\log_2 N(T)}{T} \text{ (bits/s)}, \tag{1}$$

onde $N(T)$ é o número de seqüências de duração T segundos em $\mathcal{S}$. C representa a taxa máxima de transmissão de informação (em bits por segundo) através do DNC. Shannon propôs uma técnica para determinar $N(T)$ (e daí C) que usa uma matriz, denominada matriz de transição, definida a partir do grafo que representa o DNC. A capacidade é dada por $\log_2 \lambda$, onde λ é o maior autovalor positivo dessa matriz de transição.

Em certas situações práticas, um grafo que represente $\mathcal{S}$ pode não estar disponível ou não ser facilmente obtido. Alternativamente, o DNC pode ser representado por uma lista finita de L sub-seqüências (ou "strings") proibidas sobre $\mathcal{A}$, descritas pelo conjunto $\mathcal{F} = \{\mathbf{f}_1, \cdots, \mathbf{f}_L\}$ (ver, por exemplo, Lind e Marcus [4], Seção 1.2). Nesta nova representação, $\mathcal{S}$ é formado por todas as seqüências sobre $\mathcal{A}$ que não possuem como sub-seqüência nenhum dos "strings" em $\mathcal{F}$.

Recentemente, Pimentel [1] apresentou um procedimento para se determinar a capacidade do DNC quando este é representado pelo conjunto proibido $\mathcal{F}$. Através deste procedimento, que se utiliza de técnicas combinatoriais, a capacidade é expressa pela maior raiz real positiva de um polinômio cujos coeficientes são determinados diretamente a partir do alfabeto $\mathcal{A}$, das durações de cada símbolo em $\mathcal{A}$, e do conjunto proibido $\mathcal{F}$, que definem o DNC. Em [1], apenas o caso de símbolos de mesma duração foi considerado.

Neste artigo (Seção 2), mostramos que o procedimento apresentado em [1] para se obter a capacidade do DNC pode ser facilmente adaptado de modo a considerar alfabetos com símbolos de durações distintas, que é o caso, por exemplo, de um sistema de comunicação com um laser operando em uma região (ou janela) caótica ([10], Sec. 2.1). A Seção 3 descreve as questões fundamentais de tal sistema, no que diz respeito ao cálculo de capacidade obtido em [8][10]. Veremos que as restrições das seqüências produzidas pelo laser são naturalmente representadas por conjuntos proibidos $\mathcal{F}$, o que torna o procedimento da Seção 2 para cálculo da capacidade mais atraente do que aquele proposto por Shannon. Em [8][10], foram construídos grafos a partir dos conjuntos proibidos, e a capacidade foi então calculada usando o procedimento de Shannon. Para tornar simples a construção dos grafos, de Moraes [8][10] considerou certas simplificações nas restrições das seqüências, o que provoca uma perda na capacidade de canal. Usando o procedimento da Seção 2, quantificamos esta perda e mostramos que ela é aceitável, principalmente se considerarmos que as simplificações nas restrições das seqüências implicam em uma correspondente simplificação na construção de códigos satisfazendo as restrições. Discutimos estas questões na Seção 4. Finalmente, na Seção 5, concluimos o artigo.

2. CÁLCULO DA CAPACIDADE — O CASO DE SíMBOLOS DE DURAÇÕES DISTINTAS

Nesta seção adaptamos o procedimento apresentado em [1] para se determinar a capacidade do DNC, quando este é representado pelo conjunto proibido $\mathcal{F}$, para o caso de símbolos de durações distintas. Vamos supor que sejam dados os conjuntos $\mathcal{A}$, $\mathcal{S}$ e $\mathcal{F}$, e a duração $\tau(a)$ (pertencente aos reais) de cada símbolo $a \in \mathcal{A}$. A duração de qualquer seqüência $\sigma = a_1 a_2 \cdots a_n$ de comprimento n em $\mathcal{S}$ (ou em $\mathcal{F}$) é $\tau(\sigma) = \tau(a_1) + \tau(a_2) + \cdots \tau(a_n)$. Definimos a série geradora de $\mathcal{S}$, usando a transformada discreta de Laplace [3] (DLT, do inglês *discrete Laplace transform*) na base 2, como[1]:

$$C(s) = \sum_{\sigma \in \mathcal{S}} 2^{-s\,\tau(\sigma)} = \sum_{T \geq 0} N(T) 2^{-s\,T}, \qquad (2)$$

para $s \geq 0$. Para a classe de canais em apreço, $C(s)$ pode ser expressa por $C(s) = P(s)/Q(s)$, onde $P(s)$ e $Q(s)$ são polinômios relativamente primos na variável 2^{-s}. A seguir, apresentamos uma expressão explícita para $C(s)$.

Definição 1 *A DLT para o conjunto $\mathcal{A}$ é dada por:*

$$P_A(s) = \sum_{a \in \mathcal{A}} 2^{-s\,\tau(a)}.$$

Definição 2 *Sejam $\mathbf{f}_i$ e $\mathbf{f}_j$ duas "strings" em $\mathcal{F}$. Se $\mathbf{f}_i$ e $\mathbf{f}_j$ podem ser segmentadas como $\mathbf{f}_i = \mathbf{ab}$, $\mathbf{f}_j = \mathbf{bc}$, para "strings" $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ de comprimentos não nulos, o* produto de concatenação com superposição*, denotado por $\otimes$, é definido como $\mathbf{f}_i \otimes \mathbf{f}_j = \mathbf{abc}$. Note que para o mesmo par $\mathbf{f}_i$ e $\mathbf{f}_j$ pode haver mais de um produto. O conjunto de todos os possíveis produtos $\mathbf{f}_i \otimes \mathbf{f}_j$ é denotado por $\mathcal{G}_{i,j}$, para $i, j \in \{1, 2 \cdots, L\}$. Definimos $\mathbf{C}(s)$ como uma matriz $L \times L$ cujo elemento (i,j), denotado por $[\mathbf{C}(s)]_{i,j}$, é:*

$$[\mathbf{C}(s)]_{i,j} = \sum_{\mathbf{f}_i \otimes \mathbf{f}_j \in \mathcal{G}_{i,j}} 2^{-s\,\tau(\mathbf{a})}.$$

Uma expressão explícita para $C(s)$ é dada no próximo teorema.

Teorema 1 *A DLT $C(s)$ para o conjunto $\mathcal{S}$ é dada por:*

$$\begin{aligned} C(s) &= \frac{P(s)}{Q(s)} \qquad (3) \\ &= (1 - P_A(s) + \sum_{1 \leq i,j \leq L} [(\mathbf{I} + \mathbf{C}(s))^{-1}\,\mathbf{\Phi}(s)]_{i,j})^{-1}, \end{aligned}$$

onde $\mathbf{\Phi}(s) = diag(2^{-s\,\tau(\mathbf{f}_1)}, 2^{-s\,\tau(\mathbf{f}_2)}, \cdots, 2^{-s\,\tau(\mathbf{f}_L)})$ é uma matrix diagonal.

Prova: A prova, no que diz respeito ao uso de técnicas combinatórias, segue os mesmos passos da prova do Teorema 1 em [1]. Para acomodar o caso de símbolos de durações distintas, a função $w_1(\sigma)$, definida em ([1], Seção 2.1) como sendo o comprimento da seqüência σ, foi simplesmente substituida por $\tau(\sigma)$, ou seja, pela duração de σ. As Definições 1 e 2 e a definição da matriz $\mathbf{\Phi}(s)$ já se apresentam na nova forma. Isto basta para que (3) seja uma expressão válida visto que, à parte do emprego de propriedades combinatórias, a contagem das seqüências feita em [1] depende unicamente da propriedade elementar de multiplicação polinomial: $x^a x^b = x^{a+b}$, onde x^a e x^b representam as funções geradoras de duas seqüências com características a e b, respectivamente, e x^{a+b} a função geradora da seqüência concatenada, que tem característica $(a+b)$. Obviamente, a propriedade vale quer a característica represente o comprimento quer represente a duração da seqüência. **Q.E.D.**

Comentário 1 *Nas funções geradoras em [1], x representa o núcleo de uma transformada, cuja forma específica é irrelevante no que tange à contagem das seqüências. Aqui estamos usando $x = 2^{-s}$ por conveniência.*

A capacidade do DNC é dada no próximo teorema, cuja prova é fornecida no Apêndice A.

Teorema 2 *A capacidade do DNC é dada por:*

$$C = \alpha \quad \text{bits/s},$$

[1] Usamos a base 2 aqui para que a capacidade seja expressa em bits/s. Em [3] a base adotada é $e = 2,71828\ldots$, e a capacidade é expressa em nats/s.

onde α é a maior raiz real positiva de $Q(s)$. Uma expressão explicita para $Q(s)$ segue do Teorema 1:

$$Q(s) = (1 - P_A(s)) \det(\mathbf{I} + \mathbf{C}(s)) + \sum_{1 \le i,j \le L} [\mathrm{cof}(\mathbf{I} + \mathbf{C}(s))^T \, \mathbf{\Phi}(s)]_{i,j}$$

onde $\mathrm{cof}(\mathbf{X})$ *denota a matriz dos cofatores de* $\mathbf{X}$.

Para ilustrar o método, vamos determinar a capacidade do canal telegráfico de Shannon [2], definido por $\mathcal{A} = \{d, D, s, S\}$, denotando "dot", "dash", "letter space" e "word space", respectivamente, com durações $\tau(d) = 2$, $\tau(D) = 4$, $\tau(s) = 3$ e $\tau(S) = 6$. A restrição é de que dois "spaces" consecutivos não sejam permitidos. Assim, o conjunto proibido será dado por $\mathcal{F} = \{ss, sS, Ss, SS\}$. A DLT para $\mathcal{A}$ é:

$$P_A(s) = 2^{-2s} + 2^{-4s} + 2^{-3s} + 2^{-6s}. \tag{4}$$

Os conjuntos $\mathcal{G}_{i,j}$'s são:

$$\begin{array}{lll}
\mathcal{G}_{1,1} = \{sss\} & \mathcal{G}_{1,2} = \{ssS\} & \mathcal{G}_{1,3} = \emptyset \\
\mathcal{G}_{1,4} = \emptyset & \mathcal{G}_{2,1} = \emptyset & \mathcal{G}_{2,2} = \emptyset \\
\mathcal{G}_{2,3} = \{sSs\} & \mathcal{G}_{2,4} = \{sSS\} & \mathcal{G}_{3,1} = \{Sss\} \\
\mathcal{G}_{3,2} = \{SsS\} & \mathcal{G}_{3,3} = \emptyset & \mathcal{G}_{3,4} = \emptyset \\
\mathcal{G}_{4,1} = \emptyset & \mathcal{G}_{4,2} = \emptyset & \mathcal{G}_{4,3} = \{SSs\} \\
\mathcal{G}_{4,4} = \{SSS\} & &
\end{array}$$

A matriz $\mathbf{C}(s)$ é então:

$$\mathbf{C}(s) = \begin{bmatrix} 2^{-3s} & 2^{-3s} & 0 & 0 \\ 0 & 0 & 2^{-3s} & 2^{-3s} \\ 2^{-6s} & 2^{-6s} & 0 & 0 \\ 0 & 0 & 2^{-6s} & 2^{-6s} \end{bmatrix} \tag{5}$$

e $\mathbf{\Phi}(s) = diag(2^{-6s}, 2^{-9s}, 2^{-9s}, 2^{-12s})$.

Substituindo-se (4), (5) e a matriz $\mathbf{\Phi}(s)$ na expressão (3), encontramos:

$$\begin{aligned} C(s) &= \frac{P(s)}{Q(s)} \\ &= \frac{1 + 2^{-3s} + 2^{-6s}}{1 - 2^{-2s} - 2^{-4s} - 2^{-5s} - 2^{-7s} - 2^{-8s} - 2^{-10s}} \end{aligned}$$

A capacidade[2] é portanto a maior raiz real positiva de $Q(s) = 1 - 2^{-2s} - 2^{-4s} - 2^{-5s} - 2^{-7s} - 2^{-8s} - 2^{-10s}$, ou seja, 0.538936 bits, que é o mesmo valor encontrado por Shannon [2].

3. SISTEMA DE COMUNICAÇÃO COM UM LASER CAÓTICO

"Comunicações com caos" tem recebido uma crescente atenção nos últimos anos. Um dos métodos de se trasmitir informação utilizando sistemas caóticos foi proposto por Hayes, Grebogi e Ott [5]. Eles usaram a idéia de *controle de caos* por *pequenas perturbações* [6] com o propósito de gerar órbitas caóticas controladas cuja representação simbólica correponde à codificação de uma messagem desejada. Em [5], foi demonstrado que na ausência de controle, ou seja, quando o sistema caótico evolui livremente, certas seqüências de símbolos representando as órbitas no atrator nunca são produzidas. Diz-se então que o sistema caótico possui uma gramática, ou linguagem própria. As trajetórias correspondentes às seqüências de símbolos permitidas desenham o atrator. Para que o controle de caos seja eficiente, ou seja, usando-se apenas pequenas perturbações, de modo que a estrutura topológica básica do atrator não seja alterada, é necessário que as seqüências de símbolos codificadas façam parte da mesma gramática do sistema livre de controle. Normalmente, considera-se que este sistema de comunicação é livre de ruído. Como podemos observar, este sistema de comunicação corresponde a um caso particular de DNC, abordado na Seção 2.

Recentemente, o laser de CO_2 com absorvedor saturável [7] foi analisado segundo o médtodo de comunicação com caos proposto por Hayes, Grebogi e Ott [5]. As quatro equações diferenciais não lineares que descrevem o comportamento do laser de CO_2 [7][10] foram simuladas numericamente [8] por de Moraes, e através de implementação em circuitos analógicos [9] por de Moraes, Oliveira Neto e Rios Leite, em três janelas caóticas, cuja seleção é feita através da variação de um parâmetro de controle: a taxa de bombeamento [7]. Os conjuntos proibidos para as janelas caóticas $C^{(1)}$, $C^{(2)}$ e $C^{(3)}$ obtidos por de Moraes foram, respectivamente:

- $\mathcal{F}_1 = \{10100\}$
- $\mathcal{F}_2 = \{120, 201, 202, 2000, 2001\}$
- $\mathcal{F}_3 = \{0010, 0100, 0101, 0201, 1021, 1201, 1211, 2011, 2013, 2101, 2112, 2121\}$

As durações dos símbolos são $\tau(0) = 1$, $\tau(1) = 1 + 2/3$, $\tau(2) = 1 + 4/3$ e $\tau(3) = 3$, onde por questão de simplicidade as durações foram normalizadas pela duração do símbolo "0", que no caso do laser de CO_2 real é de aproximadamente $10 \mu s$.

De Moraes considerou duas simplificações nas restrições das seqüências do laser, nas janelas caóticas $C^{(2)}$ e $C^{(3)}$, que resultaram nos seguintes conjuntos proibidos simplificados:

- $\tilde{\mathcal{F}}_2 = \{20\}$
- $\tilde{\mathcal{F}}_3 = \{01, 21\}$

[2] Devemos observar que se as durações dos símbolos fossem dadas em segundos, a capacidade seria expressa em bits/s

Pode-se verificar facilmente que as restrições $\mathcal{F}_2$ e $\mathcal{F}_3$ ainda são satisfeitas. Por exemplo, note que se a "string" "20" não ocorre em uma dada seqüência, então nenhuma das "strings" em $\mathcal{F}_2$ ocorre nesta mesma seqüência. Para $\tilde{\mathcal{F}}_2$ e $\tilde{\mathcal{F}}_3$, de Moraes encontrou as seguintes capacidades de canal[3]: $\tilde{C}_2 = 0.8974$ bits e $\tilde{C}_3 = 0.9052$ bits.

4. CAPACIDADE DO LASER — ANÁLISE COMPARATIVA

Nesta seção usamos o método da Seção 2 para determinar a capacidade dos canais com conjuntos proibidos $\mathcal{F}_2$ e $\mathcal{F}_3$, apresentados na seção anterior. Assim, podemos quantificar as perdas de capacidade em [8][10], onde foram usadas as restrições simplificadas $\tilde{\mathcal{F}}_2$ e $\tilde{\mathcal{F}}_3$.

Cálculo para $\mathcal{F}_2$

Neste caso, $\mathcal{A} = \{0, 1, 2\}$, $\tau(0) = 1$, $\tau(1) = 1 + 2/3$, $\tau(3) = 1 + 4/3$ e $\mathcal{F}_2 = \{120, 201, 202, 2000, 2001\}$. A DLT para $\mathcal{A}$ é:

$$P_A(s) = 2^{-\tau(0)s} + 2^{-\tau(1)s} + 2^{-\tau(2)s}. \qquad (6)$$

Os conjuntos $\mathcal{G}_{i,j}$'s não vazios são:

$\mathcal{G}_{1,2} = \{1201\}$ $\quad\mathcal{G}_{1,3} = \{1202\}$ $\quad\mathcal{G}_{1,4} = \{12000\}$
$\mathcal{G}_{1,5} = \{12001\}$ $\quad\mathcal{G}_{2,1} = \{20120\}$ $\quad\mathcal{G}_{3,2} = \{20201\}$
$\mathcal{G}_{3,3} = \{20202\}$ $\quad\mathcal{G}_{3,4} = \{202000\}$ $\quad\mathcal{G}_{3,5} = \{202001\}$
$\mathcal{G}_{5,1} = \{200120\}$.

A matriz $\mathbf{C}(s)$ é então:

$$\mathbf{C}(s) = \begin{bmatrix} 0 & \Psi_1(s) & \Psi_1(s) & \Psi_1(s) & \Psi_1(s) \\ \Psi_2(s) & 0 & 0 & 0 & 0 \\ 0 & \Psi_2(s) & \Psi_2(s) & \Psi_2(s) & \Psi_2(s) \\ 0 & 0 & 0 & 0 & 0 \\ \Psi_3(s) & 0 & 0 & 0 & 0 \end{bmatrix} \qquad (7)$$

e

$$\mathbf{\Phi}(s) = diag(\Psi_4(s), \Psi_4(s), \Psi_5(s), \Psi_6(s), \Psi_7(s)),$$

onde
$\Psi_1(s) = 2^{-s\tau(1)}$, $\Psi_2(s) = 2^{-s(\tau(0)+\tau(2))}$,
$\Psi_3(s) = 2^{-s(2\tau(0)+\tau(2))}$, $\Psi_4(s) = 2^{-s(\tau(1)+\tau(2)+\tau(0))}$,
$\Psi_5(s) = 2^{-s(2\tau(2)+\tau(0))}$, $\Psi_6(s) = 2^{-s(3\tau(0)+\tau(2))}$ e
$\Psi_7(s) = 2^{-s(\tau(2)+2\tau(0)+\tau(1))}$.

Substituindo-se (6), (7) e a matriz $\mathbf{\Phi}(s)$ na expressão (3), encontramos $C(s) = P(s)/Q(s)$ onde: $P(s) = 1 + 2^{-(10/3)s} - 2^{-5s} - 2^{-6s}$ e $Q(s) = 1 - 2^{-(28/3)s} - 2^{-6s} - 2^{-(25/3)s} - 2^{-(13/3)s} - 2^{-s} - 2^{-(5/3)s} - 2^{-(7/3)s} - 2^{-(16/3)s} - 2^{-(10/3)s}$.

A capacidade é portanto a maior raiz real positiva de $Q(s)$, ou seja, $C_2 = 0,9031$ bits. Comparando este valor com $\tilde{C}_2 = 0,8974$ bits, obtido em [8][10], vimos que a perda de capacidade é de apenas 0,63116 %, que é aceitável.

Cálculo para $\mathcal{F}_3$

Neste caso, $\mathcal{A} = \{0, 1, 2, 3\}$, $\tau(0) = 1$, $\tau(1) = 1 + 2/3$, $\tau(2) = 1 + 4/3$, $\tau(3) = 3$ e $\mathcal{F}_3 = \{0010, 0100, 0101, 0201, 1021, 1201, 1211, 2011, 2013, 2101, 2112, 2121\}$. A DLT para $\mathcal{A}$ é:

$$P_A(s) = 2^{-\tau(0)s} + 2^{-\tau(1)s} + 2^{-\tau(2)s} + 2^{-\tau(3)s}. \qquad (8)$$

Os conjuntos $\mathcal{G}_{i,j}$'s não vazios são fornecidos no Apêndice B. Dada a complexidade deste caso, não foi possível se obter uma expressão para $C(s)$. Porém, com o auxílio do programa de cálculo simbólico MAPLE, conseguimos determinar a capacidade, dada por $C_3 \approx 1,04$ bits. Comparando este valor com $\tilde{C}_3 = 0,9052$ bits, obtido em [8][10], vimos que a perda de capacidade é de aproximadamente 12,96 %, que ainda assim é aceitável, sobretudo se considerarmos que a simplificação trazida por $\tilde{\mathcal{F}}_3$ implica em uma correspondente simplificação na construção de códigos satisfazendo as restrições.

5. CONCLUSÕES

Neste trabalho, generalizamos o procedimento em [1] para se determinar a capacidade de canais discretos (sem ruído) com restrições de seqüências permitidas para o caso de alfabetos com símbolos de durações distintas. Em seguida, consideramos um sistema de comunicação com um laser de CO_2 caótico e calculamos as suas capacidades em duas janelas caóticas. Estes valores foram comparados com aqueles obtidos por de Moraes [8][10], que adotou simplificações nas restrições. Concluimos que as perdas de capacidade devidas a essas simplificações são aceitáveis, sobretudo se considerarmos que com as simplificações nas restrições consegue-se uma correpondente simplificação na construção de códigos satisfazendo as restrições.

APÊNDICE A

Neste apêndice provaremos o Teorema 2. A prova é, em grande medida, baseada no artigo [3]. Sem perda de generalidade, podemos supor que $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ e que $0 \le \tau(a_1) \le \tau(a_2) \le \cdots \le \tau(a_q) < \infty$, onde q é finito. Para qualquer inteiro $n \ge 0$, defina:

$$\mathcal{T}_n = \{T = n_1\tau(a_1) + n_2\tau(a_2) + \cdots + n_q\tau(a_q) : \\ n_i \in \mathcal{Z}^+, \text{ p/ } i = 1, 2, \ldots, q, T < n\}.$$

[3] Por causa da normalização das durações dos símbolos, a capacidade real é obtida dividindo-se estes valores por $10\mu s$.

Dentre os valores que os n_i's podem assumir, o maior valor, denotado por $n_{i,\max}$, é limitado superiormente por:

$$n_{i,\max} \leq \max\{n_1 : T \in \mathcal{T}_n\} = \left\lfloor \frac{n}{\tau(a_1)} \right\rfloor.$$

Isto implica que $|\mathcal{T}_n| \leq n_{i,\max}^q$.

Seja $\mathcal{T} = \cup_{n=0}^{\infty} \mathcal{T}_n$ o conjunto dos comprimentos de todas as possíveis seqüências sobre $\mathcal{A}$.

Lema 1 *Se $0 \leq \rho < 1$, então a série $\sum_{T \in \mathcal{T}} \rho^T$ converge.*

Prova: Se $0 \leq \rho < 1$, então temos

$$\begin{aligned}
\sum_{T \in \mathcal{T}} \rho^T &\leq \sum_{T \in \mathcal{T}} \rho^{\lfloor T \rfloor} \\
&= \sum_{n=0}^{\infty} \sum_{T \in (\mathcal{T}_{n+1} \setminus \mathcal{T}_n)} \rho^{\lfloor T \rfloor} \\
&= \sum_{n=0}^{\infty} \sum_{T \in (\mathcal{T}_{n+1} \setminus \mathcal{T}_n)} \rho^n \\
&\leq \sum_{n=0}^{\infty} \sum_{T \in \mathcal{T}_{n+1}} \rho^n \\
&\leq \sum_{n=0}^{\infty} \rho^n \left\lfloor \frac{n+1}{\tau(a_1)} \right\rfloor^q \\
&< \infty,
\end{aligned}$$

onde $\mathcal{A} \setminus \mathcal{B}$ denota o conjunto dos elementos em $\mathcal{A}$ que não pertencem a $\mathcal{B}$. **Q.E.D.**

Repetimos (2) aqui por conveniência:

$$C(s) = \frac{P(s)}{Q(s)} = \sum_{T \geq 0} N(T) 2^{-sT},$$

onde $s \geq 0$ é um número real. Vamos supor que α seja a maior raiz real positiva de $Q(s)$, ou seja, α é o maior polo real de $C(s)$. Da teoria, α determina a região de convergência da série $C(s)$, de modo que $C(s)$ converge para todo $s > \alpha$ e diverge para todo $s < \alpha$. Queremos provar que

$$\alpha = C = \lim_{T \to \infty} \frac{\log_2 N(T)}{T}.$$

Podemos reescrever $C(s)$ como:

$$C(s) = \sum_{T \geq 0} 2^{-T(s - \log_2 N(T)/T)}. \tag{9}$$

Se $s < C$, então $\lim_{T \to \infty}(s - \log_2 N(T)/T) < 0$, o que implica que haverá um número infinito de termos > 1 em (9). $C(s)$ então digerve para $s < C$.

Se $s > C$, então existe $\epsilon > 0$ tal que $s - \epsilon > C$. Assim, teremos que $\log_2 N(T)/T < s - \epsilon$ exceto para um número finito de T's. Mas quando $s - \epsilon > \log_2 N(T)/T$, o termo correspondente em (9) é $\leq 2^{-\epsilon T} = \rho^T$, onde $\rho = 2^{-\epsilon} < 1$. Portanto, do Lema 1, segue que $C(s)$ converge para $s > C$. Como a região de convergência é única, devemos ter $\alpha = C$.

APÊNDICE B

Para $\mathcal{F}_3 = \{0010, 0100, 0101, 0201, 1021, 1201, 1211, 2011, 2013, 2101, 2112, 2121\}$, os conjuntos $\mathcal{G}_{i,j}$'s não vazios são:

$\mathcal{G}_{1,1} = \{0010010\}$ $\mathcal{G}_{1,2} = \{00100, 0010100\}$
$\mathcal{G}_{1,3} = \{00101, 0010101\}$ $\mathcal{G}_{1,4} = \{0010201\}$
$\mathcal{G}_{1,5} = \{001021\}$ $\mathcal{G}_{2,1} = \{010010, 0100010\}$
$\mathcal{G}_{2,2} = \{0100100\}$ $\mathcal{G}_{2,3} = \{0100101\}$
$\mathcal{G}_{2,4} = \{0100201\}$ $\mathcal{G}_{3,2} = \{010100\}$
$\mathcal{G}_{3,3} = \{010101\}$ $\mathcal{G}_{3,5} = \{0101021\}$
$\mathcal{G}_{3,6} = \{0101201\}$ $\mathcal{G}_{3,7} = \{0101211\}$
$\mathcal{G}_{4,2} = \{020100\}$ $\mathcal{G}_{4,3} = \{020101\}$
$\mathcal{G}_{4,5} = \{0201021\}$ $\mathcal{G}_{4,6} = \{0201201\}$
$\mathcal{G}_{4,7} = \{0201211\}$ $\mathcal{G}_{4,8} = \{02011\}$
$\mathcal{G}_{4,9} = \{02013\}$ $\mathcal{G}_{5,5} = \{1021021\}$
$\mathcal{G}_{5,6} = \{1021201\}$ $\mathcal{G}_{5,7} = \{1021211\}$
$\mathcal{G}_{5,10} = \{102101\}$ $\mathcal{G}_{5,11} = \{102112\}$
$\mathcal{G}_{5,12} = \{102121\}$ $\mathcal{G}_{6,2} = \{120100\}$
$\mathcal{G}_{6,3} = \{120101\}$ $\mathcal{G}_{6,5} = \{1201021\}$
$\mathcal{G}_{6,6} = \{1201201\}$ $\mathcal{G}_{6,7} = \{1201211\}$
$\mathcal{G}_{6,8} = \{12011\}$ $\mathcal{G}_{6,9} = \{12013\}$
$\mathcal{G}_{7,5} = \{121021\}$ $\mathcal{G}_{7,6} = \{1211201\}$
$\mathcal{G}_{7,7} = \{1211211\}$ $\mathcal{G}_{7,11} = \{12112\}$
$\mathcal{G}_{8,5} = \{2011021\}$ $\mathcal{G}_{8,6} = \{2011201\}$
$\mathcal{G}_{8,7} = \{2011211\}$ $\mathcal{G}_{10,2} = \{210100\}$
$\mathcal{G}_{10,3} = \{210100\}$ $\mathcal{G}_{10,5} = \{2101021\}$
$\mathcal{G}_{10,6} = \{2101201\}$ $\mathcal{G}_{10,7} = \{2101211\}$
$\mathcal{G}_{11,6} = \{211201\}$ $\mathcal{G}_{11,7} = \{211211\}$
$\mathcal{G}_{11,8} = \{2112011\}$ $\mathcal{G}_{11,9} = \{2112013\}$
$\mathcal{G}_{11,10} = \{2112101\}$ $\mathcal{G}_{11,11} = \{2112112\}$
$\mathcal{G}_{11,12} = \{2112121\}$ $\mathcal{G}_{12,5} = \{2121021\}$
$\mathcal{G}_{12,6} = \{2121201\}$ $\mathcal{G}_{12,7} = \{2121211, 21211\}$
$\mathcal{G}_{12,10} = \{212101\}$ $\mathcal{G}_{12,11} = \{212112\}$
$\mathcal{G}_{12,12} = \{212121\}$.

REFERÊNCIAS

[1] C. Pimentel, "The Enumeration of constrained codes", *Anais do XVII Simósio Brasileiro de Telecomunicações*, Setembro, 1999, Vitória, ES.

[2] C. E. Shannon, "A mathematical theory of communication", *The Bell System Technical Journal*, vol. 27, pp.379-423, July 1948.

[3] A. Khandekar, R. McEliece and E. Rodemich, "The discrete noiseless channel revisited," International Symposium on Communication Theory and Applications (ISCTA'99), Ambleside, England, pp. 164-166, July 1999.

[4] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge University Press, Cambridge, 1995.

[5] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos", *Phys. Rev. Lett*, vol. 70, no. 20, pp. 3031-3034, May 1993.

[6] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos", *Phys. Rev. Lett.*, vol 64, no. 11, pp. 1196-1199, Mar. 1990.

[7] M. Lefranc, D. Hennequin, and D. Dangoisse, "Homoclinic chaos in a laser containing a saturable absorber", *J. Opt. Soc. Am. B*, vol. 8, no. 2, pp. 239-249, Feb. 1991.

[8] R. M. de Moraes "Codificação e capacidade de canal de um laser caótico", M.Sc. Thesis, Universidade Estadual de Campinas, Ago. 1998.

[9] R. M. de Moraes, L. de B. Oliveira Neto, and J. R. Rios Leite, "Analog circuits simulation of communication with chaotic lasers", *Appl. Phys. Lett.*, vol. 70, no. 11, pp. 1357-1359, Mar. 1997.

[10] R. Palazzo, R. M. de Moraes, J. R. Rios Leite, and B. F. Uchôa Filho, "Determinação da taxa de transmissão de Sinais Caóticos nos regimes $C^{(n)}$ do laser de CO_2", *Anais do XV Simósio Brasileiro de Telecomunicações*, Setembro, 1997, Recife, PE.