

1. Publicação nº <i>INPE-2828-PRE/380</i>	2. Versão	3. Data <i>Julho, 1983</i>	5. Distribuição ☐ Interna ☒ Externa ☐ Restrita
4. Origem <i>DTL/DST</i>	Programa <i>TESP/TTC</i>		
6. Palavras chaves - selecionadas pelo(s) autor(es) <i>EQUIVOCAÇÃO</i> <i>ENTROPIA</i> <i>CANAL GAUSSIANO</i>			
7. C.D.U.: <i>621.391.8</i>			
8. Título <i>LIMITANTES DA EQUIVOCAÇÃO EM</i> <i>CANAIS GAUSSIANOS ADITIVOS</i>		10. Páginas: <i>17</i>	
		11. Última página: <i>10</i>	
9. Autoria <i>Max Henrique Machado Costa</i>		12. Revisada por <i>P. Tissi</i> <i>Plínio Tissi</i>	
		13. Autorizada por <i>Parada</i> <i>Nelson de Jesus Parada</i> <i>Diretor Geral</i>	
Assinatura responsável <i>Max Henrique Machado Costa</i>			
14. Resumo/Notas A equivocação em um canal gaussiano aditivo é definida como $H(X X + Z_t)$, ou seja, como a entropia condicional da entrada X, dada a saída $X + Z_t$ do canal. A equivocação é obviamente uma função da potência t do ruído gaussiano adicionado Z_t. Neste trabalho obtêm-se limitantes inferiores e superiores para a equivocação como função da potência de ruído t. O limitante inferior decorre da concavidade da potência de entropia em função da potência do ruído adicionado. Este limitante encontra aplicação na teoria de informação de múltiplos usuários: ele permite que se estabeleça a otimalidade de dois pontos extremos da região de taxas atingíveis do canal de interferência gaussiano geral. O limitante superior é uma consequência da Desigualdade da Potência de Entropia de Shannon. Este limitante estabelece que o crescimento mais rápido possível da equivocação é logarítmico.			
15. Observações <i>Submetido para apresentação no I Simpósio Brasileiro de Telecomunicações, PUC/RJ, 5 a 9 de setembro de 1983.</i>			

ABSTRACT

The equivocation in a Gaussian additive channel is defined by $H(\underline{X}|\underline{X} + \underline{Z}_t)$, i.e., the conditional entropy of the input $\underline{X}$, given the channel output $\underline{X} + \underline{Z}_t$. The equivocation is obviously a function of the added Gaussian noise power t . In this paper, we obtain lower and upper bounds for the equivocation as a function of the noise power t . The lower bound follows from the concavity of entropy power as a function of the added noise power. This bound finds an application in multi-user information theory: it can be used to prove the optimality of two extreme points of the achievable rate region of the general Gaussian interference channel. The upper bound is a consequence of Shannon's Entropy Power Inequality. It establishes that the fastest possible growth of equivocation is logarithmic.

SUMÁRIO

	<u>Pág.</u>
LISTA DE FIGURAS	v
1. <u>INTRODUÇÃO</u>	1
2. <u>LIMITANTE INFERIOR</u>	5
3. <u>LIMITANTE SUPERIOR</u>	7
REFERÊNCIAS	10

LISTA DE FIGURAS

	<u>Pág.</u>
1 - Codificador e canal de ruído gaussiano aditivo	2
2 - Família de curvas de equivocação como função da potência do ruído adicionado	4
3 - Limitantes da equivocação	9

LIMITANTES DA EQUIVOCAÇÃO EM CANAIS GAUSSIANOS ADITIVOS

Max Henrique M. Costa

Conselho Nacional de Desenvolvimento Científico e Tecnológico-CNPq
Instituto de Pesquisas Espaciais - INPE
São José dos Campos, SP

RESUMO

A equivocação em um canal gaussiano aditivo é definida como $H(\underline{X} | \underline{X} + \underline{Z}_t)$, ou seja, como a entropia condicional da entrada $\underline{X}$, dada a saída $\underline{X} + \underline{Z}_t$ do canal. A equivocação é obviamente uma função da potência t do ruído gaussiano adicionado $\underline{Z}_t$. Neste trabalho obtêm-se limitantes inferiores e superiores para a equivocação como função da potência de ruído t . O limitante inferior decorre da concavidade da potência de entropia em função da potência do ruído adicionado. Este limitante encontra aplicação na teoria de informação de múltiplos usuários: ele permite que se estabeleça a otimalidade de dois pontos extremos da região de taxas atingíveis do canal de interferência gaussiano geral. O limitante superior é uma consequência da Desigualdade da Potência de Entropia de Shannon. Este limitante estabelece que o crescimento mais rápido possível da equivocação é logarítmico.

1. INTRODUÇÃO

Seja R um número real não negativo e seja n um número inteiro muito maior que 1. Suponha que e^{nR} mensagens equiprováveis $W \in \{1, \dots, e^{nR}\}$ são mapeadas biunivocamente em suas palavras de códigos associadas $\underline{X}$, e transmitidas através de um canal de ruído gaussiano aditivo (independente de $\underline{X}$) de variância (potência) t , como mostrado na Figura 1. As e^{nR} palavras de código $\underline{X}$ são vetores n -dimensionais representados por pontos em $\mathbb{R}^n$.

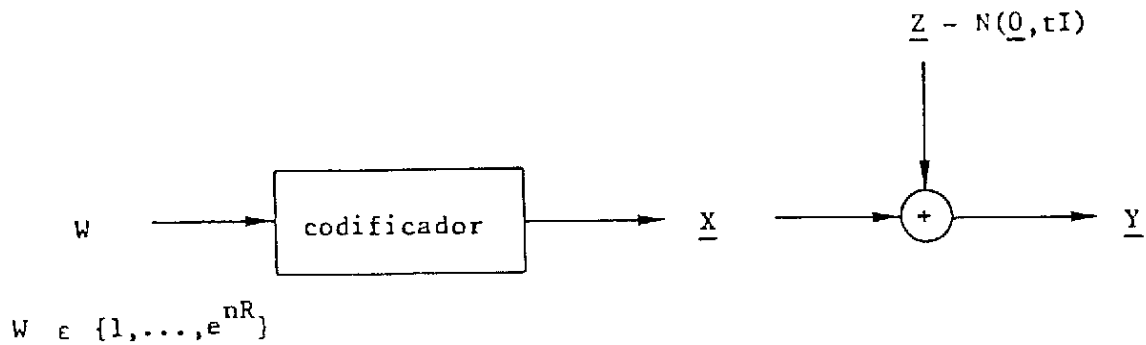


Fig. 1 - Codificador e canal de ruído gaussiano aditivo.

A equivocação de $\underline{X}$ na saída do canal $\bar{e}$ é dada por $H(\underline{X} | \underline{X} + \underline{Z}_t)$, isto é, pela entropia condicional de $\underline{X}$, dado $\underline{X} + \underline{Z}_t$. Neste trabalho estuda-se a equivocação $H(\underline{X} | \underline{X} + \underline{Z}_t)$ como função da potência de ruído t . A cada livro de código, isto é, a cada escolha das e^{nR} palavras de código, corresponde um gráfico de equivocação como função de t . A equivocação $H(\underline{X} | \underline{X} + \underline{Z}_t)$ possui as seguintes propriedades, facilmente constatáveis:

- i) $H(\underline{X} | \underline{X} + \underline{Z}_t)$ é uma função monótona crescente de t ;
- ii) para $t = 0$, $H(\underline{X} | \underline{X} + \underline{Z}_0) = H(\underline{X} | \underline{X}) = 0$;
- iii) $\lim_{t \rightarrow \infty} H(\underline{X} | \underline{X} + \underline{Z}_t) = H(\underline{X}) = nR$.

Se os pontos (palavras de código) $\underline{X}$ são esparsamente distribuídos em R^n , a adição de um vetor gaussiano de pequena variância não chega a confundir um observador à saída do canal, e a equivocação $\bar{e}$ é pequena. Se não há limitações na escolha das palavras de código $\underline{X}$, elas podem ser tomadas tão esparsamente quanto se queira, o que permite que a equivocação, para um valor fixado de t , seja arbitrariamente pequena. No entanto, é comum que o código precise satisfazer a uma limitação de potência, por exemplo, a de que todas as palavras $\underline{X}$ estejam inscritas na esfera n -dimensional de raio $\sqrt{P}$. Neste caso, as e^{nR} palavras de código não podem estar arbitrariamente esparsas. No entanto, a mágica do Teorema da Codificação de Shannon [1] para o canal gaussiano garante que, para determinados valores de t e crescentes valores de n , a equivocação por dimensão $H(\underline{X} | \underline{X} + \underline{Z}_t)/n$ pode ser feita arbitrariamente pequena.

Mais especificamente, para $t < P/(e^{2R} - 1)$, a equivocação por dimensão pode ser feita assintoticamente nula, como mostrado a seguir. Usando a regra da cadeia, pode-se escrever

$$H(\underline{X}) + H_d(\underline{X} + \underline{Z}_t | \underline{X}) = H_d(\underline{X} + \underline{Z}_t) + H(\underline{X} | \underline{X} + \underline{Z}_t) \quad , \quad (1)$$

onde $H_d(\cdot)$ denota entropia diferencial.

Assim, têm-se*

$$H(\underline{X} | \underline{X} + \underline{Z}_t) = H(\underline{X}) + H_d(\underline{Z}_t) - H_d(\underline{X} + \underline{Z}_t) \quad (2)$$

$$= nR + \frac{n}{2} \log(2\pi e t) - H_d(\underline{X} + \underline{Z}_t) \quad . \quad (3)$$

Se as palavras de código $\underline{X}$ estão restritas à esfera n-dimensional de raio $\sqrt{P}$, o máximo valor de $H_d(\underline{X} + \underline{Z}_t)$ é dado por $(n/2)\log(2\pi e(P + t))$. Portanto, de (3) a equivocação por dimensão deve satisfazer a desigualdade

$$\frac{1}{n} H(\underline{X} | \underline{X} + \underline{Z}_t) \geq R - \frac{1}{2} \log\left(1 + \frac{P}{t}\right) \quad (4)$$

$$= \frac{1}{2} \log\left(\frac{te^{2R}}{t + P}\right) \quad . \quad (5)$$

Para valores de t superiores a $P/(e^{2R} - 1)$, a desigualdade (5) demonstra que a equivocação não pode ser feita arbitrariamente pequena, por dever ser superior a um número positivo. Por outro lado, de acordo com o Teorema da Codificação de Shannon, equivocações assintoticamente nulas são atingíveis se $t < P/(e^{2R} - 1)$.

Alternativamente, a desigualdade (5) assegura que quando se deseja enviar confiavelmente e^{nR} mensagens para um observador à saída de um canal gaussiano com potência de ruído N , a mínima potência necessária para o código utilizado deve satisfazer a seguinte relação:

$$0 = \frac{1}{2} \log\left(\frac{N e^{2R}}{N + P}\right) \quad , \quad (6)$$

* Os logaritmos usados neste trabalho são naturais.

ou seja,

$$P = N(e^{2R} - 1) \quad (7)$$

Pode-se assim expressar assintoticamente a equivocação (por dimensão) do código que utiliza a menor potência possível para comunicar e^{nR} mensagens através de um canal gaussiano de potência de ruído N :

$$\frac{1}{n} H(\underline{X} | \underline{X} + \underline{Z}_t) = \begin{cases} 0 & \text{para } 0 \leq t \leq N, \\ \frac{1}{2} \log \left(\frac{t e^{2R}}{t + N(e^{2R} - 1)} \right) & \text{para } t > N. \end{cases} \quad (8)$$

A equação (8) define uma família de curvas de equivocação parametrizadas por R e N . A Figura 2 apresenta um membro típico desta família.

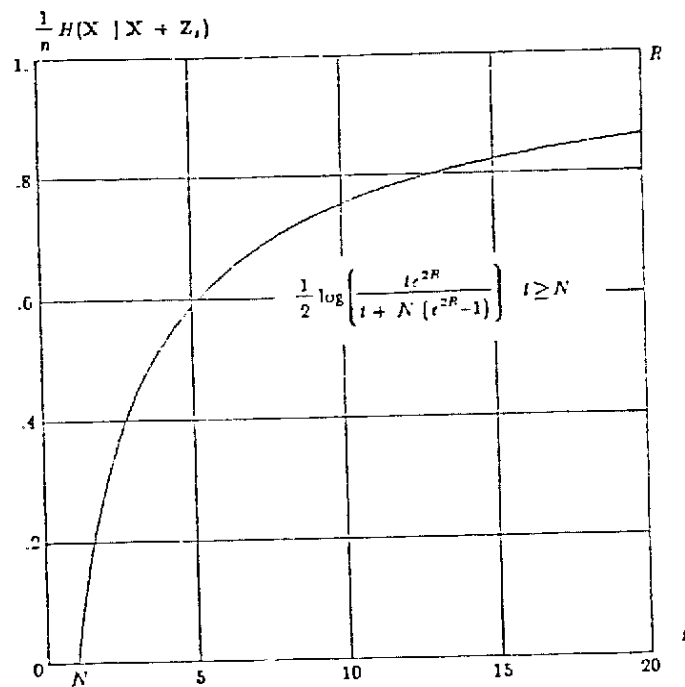


Fig. 2 - Família de curvas de equivocação como função da potência do ruído adicionado.

Como exposto adiante, esta família de curvas de equivocação está ligada a limitantes (inferior e superior) para a equivocação.

2. LIMITANTE INFERIOR

Demonstra-se o seguinte lema:

Lema 1: Seja $0 < t_0 < t_1 \leq t_2$ e $0 \leq \alpha \leq \beta$.

Se

$$\frac{1}{n} H(\underline{X} | \underline{X} + \underline{Z}_{t_0}) \leq \alpha \quad (9)$$

e

$$\frac{1}{n} H(\underline{X} | \underline{X} + \underline{Z}_{t_1}) \geq \beta, \quad (10)$$

então

$$\frac{1}{n} H(\underline{X} | \underline{X} + \underline{Z}_{t_2}) \geq \frac{1}{2} \log \left(\frac{t_2(t_1 - t_0)e^{2(\alpha - \beta)}}{t_1(t_2 - t_0)e^{2\beta} - t_0(t_2 - t_1)e^{2\alpha}} \right). \quad (11)$$

Demonstração: Para facilitar a notação, introduz-se a seguinte definição:

$$\underline{Y}_t \triangleq \underline{X} + \underline{Z}_t.$$

Pode-se mostrar facilmente que o membro direito de (11) é uma função monótona decrescente de α e uma função monótona crescente de β . Assim, para demonstrar o lema acima, é suficiente que se prove a seguinte desigualdade:

$$\frac{1}{n} H(\underline{X} | \underline{Y}_{t_2}) \geq \frac{1}{2} \log \left(\frac{t_2(t_1 - t_0)e^{\frac{2}{n} (H(\underline{X} | \underline{Y}_{t_0}) + H(\underline{X} | \underline{Y}_{t_1}))}}{t_1(t_2 - t_0)e^{\frac{2}{n} H(\underline{X} | \underline{Y}_{t_1})} - t_0(t_2 - t_1)e^{\frac{2}{n} H(\underline{X} | \underline{Y}_{t_0})}} \right). \quad (12)$$

Em [2] e [3] é mostrado que $e^{\frac{2}{n} H(\underline{X} + \underline{Z}_t)}$ é uma função concava de t , para qualquer distribuição da variável n -dimensional $\underline{X}$. Isto implica que

$$e^{\frac{2}{n} H(\underline{Y}_{t_1})} \geq \frac{t_2 - t_1}{t_2 - t_0} e^{\frac{2}{n} H(\underline{Y}_{t_0})} + \frac{t_1 - t_0}{t_2 - t_0} e^{\frac{2}{n} H(\underline{Y}_{t_2})}. \quad (13)$$

Multiplicando ambos os lados desta inequação por

$$\exp \left\{ \frac{2}{n} [2H(\underline{X}) + H(\underline{Z}_{t_0}) + H(\underline{Z}_{t_1}) + H(\underline{Z}_{t_2}) - H(\underline{Y}_{t_0}) - H(\underline{Y}_{t_1}) - H(\underline{Y}_{t_2})] \right\}, \quad (14)$$

e usando (2), tem-se que

$$\begin{aligned} (t_2 - t_0) e^{\frac{2}{n} H(\underline{Z}_{t_1})} e^{\frac{2}{n} (H(\underline{X} | \underline{Y}_{t_0}) + H(\underline{X} | \underline{Y}_{t_2}))} \\ \geq (t_1 - t_0) e^{\frac{2}{n} H(\underline{Z}_{t_2})} e^{\frac{2}{n} (H(\underline{X} | \underline{Y}_{t_0}) + H(\underline{X} | \underline{Y}_{t_1}))} \\ + (t_2 - t_1) e^{\frac{2}{n} H(\underline{Z}_{t_0})} e^{\frac{2}{n} (H(\underline{X} | \underline{Y}_{t_1}) + H(\underline{X} | \underline{Y}_{t_2}))}. \end{aligned} \quad (15)$$

Neste ponto nota-se que, para $i = 0, 1, 2$,

$$e^{\frac{2}{n} H(\underline{Z}_{t_i})} = 2\pi e t_i. \quad (16)$$

Usando as expressões (16) em (15) e rearranjando termos, encontra-se:

$$e^{\frac{2}{n} H(\underline{X} | \underline{Y}_{t_2})} \geq \frac{t_2(t_1 - t_0) e^{\frac{2}{n} (H(\underline{X} | \underline{Y}_{t_0}) + H(\underline{X} | \underline{Y}_{t_1}))}}{t_1(t_2 - t_0) e^{\frac{2}{n} H(\underline{X} | \underline{Y}_{t_1})} - t_0(t_2 - t_1) e^{\frac{2}{n} H(\underline{X} | \underline{Y}_{t_0})}}. \quad (17)$$

Desta desigualdade, (12) segue imediatamente. Isto conclui a demonstração do Lema 1.

Uma interpretação alternativa para este limitante inferior é dada pela família de funções de equivocação parametrizadas por R e N expressa em (8). Suponha-se que os valores de $H(\underline{X}|\underline{Y}_{t_0})$ e $H(\underline{X}|\underline{Y}_{t_1})$ sejam fixados. Sejam $R = r$ e $N = n_1$ os valores de R e N necessários para que a equivocação dada em (8) coincida com estes valores fixados. O Lema 1 estabelece que o valor desta curva de equivocação é um limitante inferior de $H(\underline{X}|\underline{Y}_t)$ para $t \geq t_1$, isto é,

$$H(\underline{X}|\underline{Y}_t) \geq \frac{1}{2} \log\left(\frac{t e^{2r}}{t + n_1(e^{2r} - 1)}\right) \text{ para } t \geq t_1. \quad (18)$$

Este limitante inferior encontra uma aplicação em Teoria de Informação de múltiplos usuários. Ele permite que se estabeleça a otimalidade de dois pontos extremos na região de taxas atingíveis do canal de interferência gaussiano geral [2], [4].

3. LIMITANTE SUPERIOR

Prova-se o seguinte lema:

Lema 2: Sejam $t_1 \leq t_2$ e $\alpha \geq 0$.

Se

$$\frac{1}{n} H(\underline{X}|\underline{Y}_{t_1}) \leq \alpha \quad (19)$$

então

$$\frac{1}{n} H(\underline{X}|\underline{Y}_{t_2}) \leq \frac{1}{2} \log\left(\frac{t_2}{t_1} e^{2\alpha}\right). \quad (20)$$

Demonstração: Como o membro direito de (20) é uma função monótona crescente de α , é suficiente demonstrar que

$$\frac{1}{n} H(\underline{X}|\underline{Y}_{t_2}) \leq \frac{1}{2} \log\left(\frac{t_2}{t_1} e^{\frac{2}{n} H(\underline{X}|\underline{Y}_{t_1})}\right). \quad (21)$$

A Desigualdade da Potência de Entropia [1, 5, 6], introduzida por Shannon, estabelece que

$$e^{\frac{2}{n} H(\underline{Y}_{t_2})} \geq e^{\frac{2}{n} H(\underline{Y}_{t_1})} + e^{\frac{2}{n} (H(\underline{Z}_{t_2 - t_1}))} \quad (22)$$

Usando (2) e rearranjando termos, obtêm-se:

$$\begin{aligned} t_2 e^{-\frac{2}{n} H(\underline{X} | \underline{Y}_{t_2})} &\geq t_1 e^{-\frac{2}{n} H(\underline{X} | \underline{Y}_{t_1})} + (t_2 - t_1) e^{-\frac{2}{n} H(\underline{X})} \\ &\rightarrow t_1 e^{-\frac{2}{n} H(\underline{X} | \underline{Y}_{t_1})} \end{aligned} \quad (23)$$

Deste ponto, (21) segue de forma trivial.

Este limitante superior também pode ser expresso em termos da família de funções de equivocação dada em (8). Suponha-se que o valor de $H(\underline{X} | \underline{Y}_{t_1})$ seja fixado. Seja $N = n_2$ o valor de N necessário para que a equivocação dada em (8), com $R = \infty$, coincida com este valor fixado. O Lema 2 estabelece que o valor desta curva de equivocação é um limitante superior de $H(\underline{X} | \underline{Y}_t)$ para $t \geq t_1$, ou seja,

$$H(\underline{X} | \underline{Y}_t) \leq \lim_{R \rightarrow \infty} \frac{1}{2} \log \left(\frac{t e^{2R}}{t + n_2(e^{2R} - 1)} \right) \quad (24)$$

$$= \frac{1}{2} \log \left(\frac{t}{n_2} \right) \quad \text{para } t \geq t_1. \quad (25)$$

Assim, o mais rápido crescimento possível da equivocação $H(\underline{X} | \underline{Y}_t)$ é logarítmico em t , obtido quando $\underline{X}$ tem taxa R infinita.

A Figura 3 é uma ilustração dos limitantes inferior e superior apresentados nos Lemas 1 e 2.

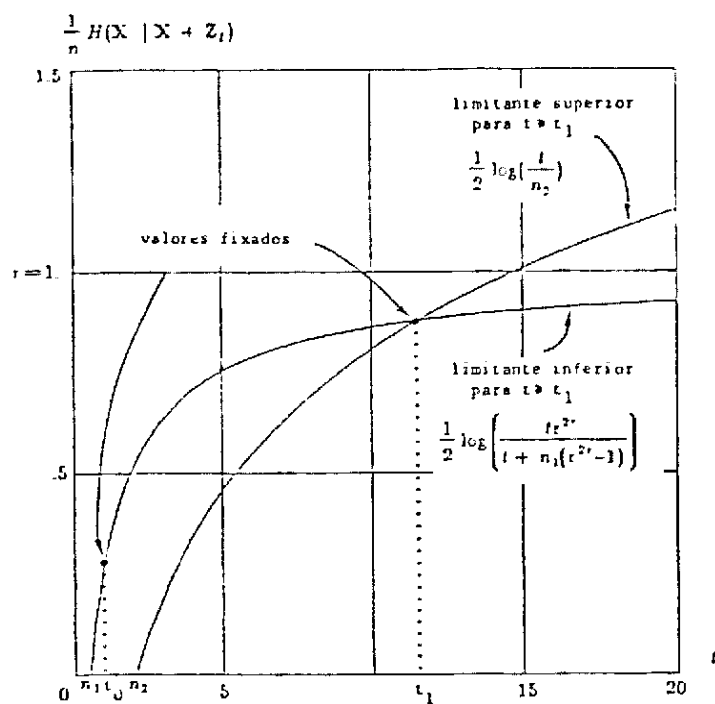


Fig. 3 - Limitantes da equivocação.

AGRADECIMENTOS

O autor agradece a Thomas Cover e a Abbas El Gamal as valiosas discussões.

REFERÊNCIAS

- [1] C. E. Shannon, "A mathematical theory of communication", Bell System Technical Journal, vol. 27, pp. 623-656, out. 1948.
- [2] M. H. M. Costa, "Interference Channels", tese de doutorado, Departamento de Engenharia Elétrica, Stanford University, fev. 1983.
- [3] M. H. M. Costa, "Strengthening the entropy power inequality", submetido para IEEE Transactions on Information Theory.
- [4] M. H. M. Costa, "On the Gaussian interference channel", submetido para IEEE Transactions on Information Theory.
- [5] A. J. Stam, "Some inequalities satisfied by the quantities of information of Fisher and Shannon", Information and Control, vol. 2, pp. 101-112, jun. 1959.
- [6] N. M. Blachman, "The convolution inequality for entropy powers", IEEE Transactions on Information Theory, vol. IT-11, pp. 267-271, abr. 1965.