Álgebra Linear e a Teoria de Códigos

André Badenas dos Santos *
Engenharia de Computação - UTFPR
andre_1994_11@hotmail.com

Profa. Mari Sano (Orientadora)
Departamento Acadêmico de Matemática - UTFPR
marisano@utfpr.edu.br

Palavras-chave: Código, Código de Hamming,Capacidade de Shannon.

Resumo: Códigos de correção de erros começaram a surgir nos anos 50 e estão difundidos nas mais variadas áreas, como computação e espacial, economia, aeronáutica, e, principalmente, comunicação. Para garantir que o destinatário receba uma mensagem segura, de forma que ninguém seja capaz de ler, utiliza-se criptografia, porém, isso não garante que o meio pelo qual a mensagem foi enviada contenha ou não ruídos e/ou interferências, fazendo com que a mensagem possa ser recebida de duas formas:

- O destinatário percebe que tem um erro, porém não consegue consertar, deixando a mensagem ilegível.
- O destinatário não percebe que tem um erro, assim ele interpreta a mensagem de outra forma diferente da original.

Para esses problemas foram criados os códigos de correção de erros, que consistem basicamente em enviar uma mensagem maior ao receptor, na qual os caracteres a mais têm a função de corrigir uma certa quantidade de erros. Aqui serão tratadas cadeias de quatro caracteres com no máximo um erro. Para resolvê-lo, é introduzido um código que utilize uma quantidade mínima de caracteres, chamado código de Hamming.

Seja $abcd$ uma palavra de 4 caracteres binários. O código de Hamming transforma essa palavra em $abcdefg$, tal que $e := a + b + c$, $f := a + b + d$ e $g =: a + c + d$. Esse código é capaz de corrigir exatamente um erro e resolver os problemas listados acima. Esse fato será mostrado usando a teoria da Álgebra linear.

Além da correção de erros em mensagens, deve-se anular mensagens que possam parecer ambíguas quando enviadas. Para enviar o número máximo de mensagens possíveis sem ambiguidade serão introduzidos os conceitos de capacidade de Shannon e o guarda-chuva de Lovasz.

*Bolsista do PICME

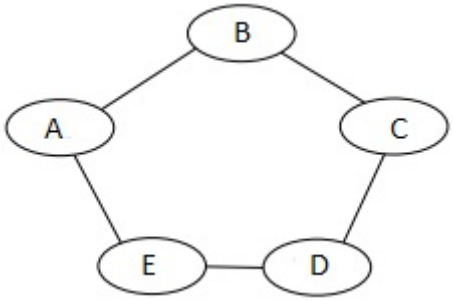

Figura 1: Grafo que representa os canais de transmissão e as ambiguidades presentes.

Seja um modelo de transmissão conforme a figura 1. Cada canal A, B, C, D, E é capaz de transmitir um caractere por dia, de forma que canais ligados por arestas são intercambiáveis, isto é, ambíguos. Será calculado o número máximo de mensagens distintas capazes de serem enviadas em k dias. Em uma rápida análise, nota-se que é possível enviar pelo menos dois caracteres por dia, escolhendo canais não adjacentes. Com isso temos, em k dias, um limite inferior de 2^k mensagens. Para limite superior, pode-se perceber que não é possível encontrar 3 canais não adjacentes entre si, logo o valor é menor que 3^k mensagens distintas. Para calcular esse valor, serão utilizados alguns conceitos da Teoria de Grafos e principalmente Álgebra linear, bem como uma representação ortogonal interessante chamada de guarda-chuva de Lovasz, representado na figura 2.

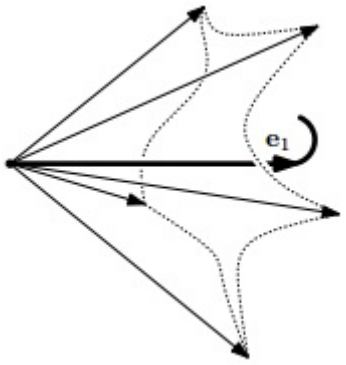

Figura 2: Guarda-chuva de Lovasz.

Por fim, vale salientar que o mesmo problema, porém para sete canais de transmissão, não foi resolvido até hoje, pois pode ser reduzido a um problema NP-completo.

Referências:

[1] Matousek,J.; **Thirty-Three Miniatures:Mathematical and Algorithmic Applications of Linear Alguebra**,Amer. Math. Soc., 2010, e-book. Disponível em:
<http://kam.mff.cuni.cz/ matousek/stml-53-matousek-1.pdf>. Acesso em 28/09/2015.

[2] Boguszak,M.;Error-Correcting Codes, 2005. Disponível em:
<http://cc.pima.edu/mboguszak/ErrorCorrectingCodes.pdf>. Acesso em 28/09/2015.

[3] L. Lovasz "On the Shannon capacity of a graph", IEEE Trans. Inf. Theory, vol. 25, no. 1, p. 1-7 1979. Disponível em:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1055985>. Acesso em 28/09/2015.