DOI: 10.20396/revpibic2720191611

Uma introdução a Códigos Corretores de Erros e Teoria da Informação

Lucas Bertoloto Pereira*, Sueli Irene Rodrigues Costa.

Resumo
Nesse trabalho de iniciação científica foi feito um estudo introdutório de códigos corretores de erros, incluindo a associação destes a reticulados e alguns tópicos de teoria da informação. Enfatizamos especialmente o estudo de conceitos básicos de códigos corretores de erros, alguns códigos em especial, como o de Hamming, Golay e Reed Solomon; conceitos básicos de reticulados e algumas aplicações, como em criptografia; e uma introdução à teoria da informação, com foco no estudo de entropias e os dois teoremas de Shannon.

Palavras-chave:
Códigos corretores de erros, reticulados, teoria da informação.

Introdução

O trabalho teve como objetivo fazer uma introdução à área de telecomunicações, em especial abordando códigos corretores de erros e reticulados, temas relacionados a transmissão confiável e segura de informação. Depois, foi realizada uma introdução à teoria da informação, que estuda o armazenamento e transmissão de informação.

Resultados e Discussão

Inicialmente, os estudos foram focados em códigos corretores de erros. A grande motivação desses códigos é a transmissão de informação de forma confiável por meio de canais que introduzem ruídos nas mensagens enviadas. Para isso, a mensagem é mapeada para uma palavra código, que é transmitida pelo canal e decodificada pelo receptor. Pela palavra recebida, dependendo da quantidade de erros e do tipo de código, o receptor consegue detectar se houveram erros e possivelmente corrigi-los para recuperar a mensagem original. Entre os códigos estudados, estão os de Hamming, Golay e Reed Solomon. As principais referências dessa parte foram [1], [3] e [4].

Depois, foi feito um estudo de reticulados, conjuntos que podem ser utilizados para construir códigos, além de possuir aplicações na área de criptografia, em especial na criptografia pós-quântica. Essa área, em especial, é importante para a transmissão segura de informações depois que computadores quânticos, que podem quebrar bem mais facilmente as formas de criptografia atual, forem amplamente utilizados. As principais referências dessa parte foram [1] e [5].

Por fim, foi realizada uma introdução à área de teoria da informação, que analisa o armazenamento e transmissão de informação. Suas principais medidas são as entropias, relacionadas ao grau de indeterminação de algo. Os resultados dos estudos de teoria da informação permitem provar qual o máximo que um sinal pode ser comprimido e o quanto de informação é possível transmitir em um canal, tendo uma taxa de erro arbitrariamente baixa. As principais referências foram [2] e [6], e o software Mathematica foi utilizado para exemplos e ilustrações de diversos tópicos desse conteúdo.

Conclusão

Na Iniciação Científica, o aluno teve contato introdutório com as áreas de códigos corretores de erros, reticulados e teoria da informação, permitindo continuar um estudo aprofundado desses temas, visando suas aplicações à área de telecomunicações.

Agradecimentos

Esse trabalho foi desenvolvido com o suporte da bolsa de Iniciação Científica FAPESP número 2018/06884-1, “Uma introdução a Códigos Corretores de Erros, Reticulados e Aplicações”, associada ao Projeto Temático FAPESP número 2013/25977-7, “Segurança e Confiabilidade da Informação: Teoria e Aplicações”

---

[1] Lavor, C. C.; Akves, M. M. e Costa, S. I. R.: Uma Introdução à Teoria de Códigos – e Notas em Matemática Aplicada; SBMAC: 2006.
[2] Cover, T. and Thomas, J.: Elements of Information Theory; Wiley: 2006.
[3] Justesen, J. and Hoholdt, T.: A Course in Error-Correcting Codes; European Mathematical Society: 2004.
[4] Huffman, G. and Pless, V.: Fundamentals of Error-Correcting Codes; Cambridge University Press: 2003.
[5] Costa, S. I. R.; Oggier, F.; Campello, A.; Belfiore, J. C. and Viterbo, E.: Lattices Applied to Coding for Reliable and Secure Communications; Springer Verlag: 2017.
[6] Haykin, S.: Communication Systems; Wiley: 2009.