DOI: 10.20396/revpibic2720191879

Códigos Corretores de Erros Quânticos construídos a partir de códigos clássicos.

André Saugo Mazzari*, Sueli I. R. Costa

Resumo

Este projeto de iniciação científica teve por objetivo introduzir o aluno às áreas de teoria da informação, reticulados, códigos corretores de erros e suas aplicações. Após um estudo inicial destes temas, o orientado concentrou-se numa breve abordagem introdutória de codificação quântica, particularmente em códigos corretores de erros quânticos construídos a partir de códigos clássicos.

Palavras-chave:

Códigos corretores de erros, códigos quânticos, teoria da informação.

Introdução

Ao longo deste projeto, o aluno foi apresentado à conceitos básicos da área de teoria de informação, estudou códigos corretores de erros clássicos e suas propriedades, e a associação destes à reticulados, que vem sendo usados na área de comunicação, particularmente na criptografia. Em seguida, o aluno realizou um estudo introdutório aos códigos quânticos, em especial sobre construção destes a partir de códigos corretores de erros clássicos. Dentre os exemplos estudados, destacamos o código de Shor e os códigos CSS.

Resultados e Discussão

Inicialmente, foi realizado um estudo introdutório nas áreas de teoria da informação, reticulados, e códigos corretores de erros e suas aplicações. Esta etapa foi realizada em conjunto com outros alunos que também participaram do projeto temático "Segurança e Confiabilidade da Informação: Teoria e Aplicações". Destaca-se o estudo sobre códigos corretores de erros clássicos e seus conceitos básicos, em especial códigos lineares sobre corpos finitos. Para isto, foi necessário um breve estudo sobre corpos finitos. Alguns exemplos de códigos estudados são o código de Hamming e de Reed-Solomon. Também vale ressaltar o estudo sobre reticulados, com foco na conexão com códigos corretores de erros e criptografia.

Após o estudo destes temas, o aluno concentrou-se na aplicação de códigos corretores de erros em computação quântica, uma área que promete trazer grandes revoluções tecnológicas ao longo do século XXI. Um de seus principais desafios é controlar os erros introduzidos pelo ambiente externo nos sistemas quânticos. Para contornar este problema, uma teoria de códigos corretores de erros quânticos vem sendo desenvolvida. Dentro desta área, os principais tópicos estudados foram o código de Shor, os códigos CSS, um formalismo para modelar ruídos em sistemas quânticos abertos, algumas propriedades gerais de códigos corretores de erros quânticos, e uma introdução aos códigos estabilizadores. Procurou-se ilustrar conceitos e propriedades através da discussão de exemplos específicos usando recursos computacionais(programa Mathematica). Como pré-requisito, foi necessário aprender alguns tópicos de mecânica quântica e computação quântica. As principais referências utilizadas no projeto estão listadas ao final.

Conclusões

O aluno foi introduzido às áreas de teoria da informação, códigos corretores de erros e reticulados. Após um estudo inicial, aprofundou-se na aplicação de códigos corretores de erros na computação quântica, uma área de grande desenvolvimento e relevância atual. Em especial, foram trabalhados exemplos de códigos quânticos construídos a partir de códigos clássicos.

Agradecimentos

Esse trabalho foi desenvolvido com o suporte da bolsa de Iniciação Científica FAPESP, processo 2018/06775-8, "Códigos, Reticulados e Aplicações à Área de Comunicações- Uma Introdução", associada ao Projeto Temático FAPESP 2013/25977-7, "Segurança e Confiabilidade da Informação: Teoria e Aplicações"

---

[1] Costa, S. I. R. F. Oggier, A. Campello, J-C Belfiore, E, Viterbo Lattices Applied to Coding for Reliable and Secure Comunications, Springer 2017

[2] A. Hefez e M.L. Villela , C´odigos Corretores de Erros, IMPA, 2.a Ed. 2017

[3] W. Huffman e V. Pless Fundamentals of Error- Correcting Codes, Cambridge Univ. Press, 2006

[4] C. Lavor, S. I. R. Costa , M. Muniz, R. Siqueira, Uma Introdu¸c˜ao `a Teoria de C´odigos, SBMAC, 2006

[5] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge Press University, 2000

[6] R. Portugal, D. N. Gon¸calves, C´odigos corretores de erros qu^anticos, SBMAC, Volume 65, 2012

[7] R. Portugal, C. C. Lavor, L. M. Carvalho, N. Maculan, Uma Introdu¸c˜ao a Computa¸c˜ao Qu^antica, SBMAC, Volume 8, 2012.