

Error-correcting codes: an introduction

César A. W. Dainezi (IC)

Abstract

In early 1950's, Richard Hamming established the foundations of the theory of Error-Correcting Codes, which are indispensable for any form of telecommunication (such as internet, cellphone, satellite) or physical data storage (such as hard drive, DVD) nowadays. Our study focused on linear codes, which can be seen as the image of a linear transformation, and on cyclic codes, which are isomorphic to ideals of a ring. Some special linear codes were also studied, such as Reed-Solomon codes.

Key words: error-correcting codes, information theory, discrete mathematics.

Introduction

Error-correcting codes are methods of "introducing more information" into a message, in order to it become redundant in some sense. So, after noise is introduced to it, the original message can still be retrieved or the error existence can be detected. See the example below.

Say that there are 4 possible messages that are likely to be transmitted (such as the directions for a robot to move: north, south, east or west). Thinking on binary as natural source codification, one is likely to define "north" as "00", "south" as "11", "east" as "10" and "west" as "01". However, noise could be introduced to the message and turn "00" into "01", so "north" could be received as "west".

To avoid that, error correcting codes take place and codify "00" to "00 00 00", "11" to "11 11 11", "10" to "10 10 10" and "01" to "01 01 01". Now, if an error is introduced to "00 00 00", it would become something such as "00 10 00" and can still be interpreted as "north" by the receiver.

This example is known as *triple repetition code* and is an extremely simple code that can be found in [1] and [2]. There are many other simple error-correcting codes used daily. Examples are the CPF's and ISBN's verifying digits.

Results and Discussion

An error-correcting code, generally speaking, is a subset of A^n , where A is a finite set. There's a notion of distance (or metric) in this set, which is the Hamming metric. From that, there can be defined a minimum distance of the code, which is related to the capability of detecting or correcting errors.

The first kind of code studied were the linear codes. They can be understood as the image of a linear transformation T which maps K^k to K^n , where K is a finite field. In other words, a linear code C is a linear space given by $T(K^k)$. The orthogonal complement, of C , and is also a code, called the dual code of C . It has a very important role on decodifying the codewords of C . The codes C and C' have generator matrices, G and H respectively, that when written in some particular basis, they satisfy the relation $H^t G = 0$.

On cyclic codes, they are defined by a code that every word translated is still a word, this means if (c_0, c_1, \dots, c_n) is a word of the code, then (c_1, \dots, c_n, c_0) is also a word of the code. There can be shown that a cyclic code is isomorphic to an ideal of the ring of residual classes of $K[X] \text{ mod } X^n - 1$.

Conclusions

Error correcting codes are essential to this modern world we live in. They are an unnoticed, but very important component of something that is getting more and more ordinary in a worldwide proportion: the telecommunication.

Acknowledgement

This project was supported by PIBIC/CNPq, who I would like to thank.

I also would like to thank the Prof. Dr. Sueli Costa, who oriented me through the study on the subject.

¹ Lavor, C. C.; Alves, M. M. S.; Siqueira, R. M. e Costa, S. I. R. *Uma introdução à teoria de códigos*. SBMAC: São Carlos, SP, 2006.

² Hefez, A.; Villela, M. L. T. *Códigos corretores de erros*. 2. ed. IMPA: Rio de Janeiro, RJ, 2008. .