Goppa Codes

Author: Jbara Abdelhamid
Supervisor: Kiss Sándor

Abstract

Coding theory is an area of mathematics that combines many theoretical concepts with a wide variety of applications. One major tool that this theory provides is Error correcting codes. They are concerned with the transmission of data across noisy channels and the recovery of corrupted messages. They are used in practically all cases of message transmission, especially in data storage where Error correcting codes defend against data corruption. In this expository thesis, we will begin by introducing many of the fundamental ideas in classical error correcting codes. Namely, after presenting some historical background and a motivational introduction, in chapter 3 we start by defining the notions of a code, encoding, and the principle of decoding. In addition, we introduce the crucial concepts of minimum distance and error correcting capability of a code. After that, we study linear codes and their properties, cyclic codes and cyclic codes from roots, and we finish the section by presenting an important class of codes called BCH codes. The reason of choosing this specific class of codes, is that in the literature many consider Goppa codes to be a generalization of it, and in fact we show in what follows how to go back to the former using the latter.

Thus, Goppa codes are the matter of study in section 4. We start by the definition, and the dimension of the code. Next, we present two theorems about the minimum distance, the first is true for all Goppa codes and the second is concerned with binary ones. The last subsection is an explanation of a decoding algorithm for binary Goppa codes.

In the end, we finish the thesis by presenting parts of a program, written in SageMAth programming language, which implements all of the theoretical ideas

presented, and can be used to show a concrete example of error correcting.

The work presented in this thesis was achieved by the guided study of several books and articles from the literature of coding theory suggested by my supervisor Dr.Kiss Sándor.