ON SOME APPLICATIONS OF ALGEBRA AND GEOMETRY IN CODING THEORY.

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF SCIENCE DEGREE OF THE UNIVERSITY OF NAIROBI IN PURE MATHEMATICS.

BEN OBIERO

August 16, 2011
Declarations

I, the undersigned, declare that this dissertation is my original work and to the best of my knowledge has not been presented for the award of a degree in any other University/College.

Ben Obiero

I56/78951/2009

Signature Date

Declaration by Supervisor

This project has been submitted for examination with my approval as supervisor.

Mw. Achola Claudio

Signature Date
Abstract

The fundamental problem that led to the development of the theory of error correcting codes was that of having a reliable communication over unreliable channels. A communication channel can be as simple as the air between the voicebox of one addressing an audience and the ears of the listeners. Copper wires connecting telephones or modems can also be considered as channels. In the case of data storage, say in a magnetic tape or disc, the magnetized field in the magnetic tape or disc is the channel.

One property of these channels is their capacity to distort the information. For instance, the copper wires connecting telephones may get heated resulting in background interruptions. Magnetisation on the tape may re-align over time, or the head of the drive reading the tape or disc may be ill positioned and the right magnetisation be misread! Such distortions to our good information will be referred to as noise.

There are two main ways of handling noise; physical means and system means. Under physical means, one "targets" the cause of noise and seeks to eliminate it. For instance if the drive head misreads the magnetisation, then a better drive is used as a replacement for the "now faulty drive". As for system means, one "sandwiches" the channel between two devices; an encoder and a decoder (see figure 1) so that any form of noise can be detected and possibly corrected. The theory of error correcting codes is involved in this.

For our purpose we will consider an abstract communication channel called the Binary Symmetric Channel (BSC). In BSC, information to be transmitted is encoded as a string of 0's and 1's. An error is then considered as an interchange between the binary digits in the sent and received information symbols.

Figure 1: A simple Communications Channel
Below is a diagramatic representation of a binary symmetric channel.

Until 1948, encoding with minimal error was done at the expense of information rates. Information symbols to be transmitted were repeated several times with more efficiency gained by higher order repetitions. If $n$, say is the order of repetition, then each bit represented $1/n$ of the information and this value approaches zero as the order of repetition becomes very large. Shanons ground breaking work [?] created a platform for the launch of error correcting codes (see history of coding in the introduction). Since then, various mathematical disciplines have lead to the development of this theory. In this Dissertation, we will consider the "contributions" from Algebra and Geometry in Coding Theory.