Linear Code

John McCall

February 4, 2014

1 Background

A *linear code* is a type of error-correcting code in which any linear combination of codewords is also a codeword. Usually linear codes are partitioned into block codes and convolutional codes. Linear codes are more efficient algorithms for encoding or decoding than other types of codes.

Linear codes are used in *forward error correction* and applied in methods for symbol transmission (for example: bits) over a communication channel. They are used so that if there are errors in the transmission, they can be corrected or detected by the receiver. The codewords used in linear codes are blocks of symbols which are encoded using more symbols than the original value.

2 Definitions

A linear code of length n and rank k is a linear subspace C with dimension k of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with q elements. These are called q-ary codes. If $q = 2$ or $q = 3$ the code is called a *binary code*, or a *ternary code* respectively. The vectors in C are the *codewords*. The *size* of a code is the number of codewords and equals q^k.

The *weight* of a codeword is the number of non-zero elements it contains. The distance between two codewords is the *Hamming distance* between them. The distance d of a linear code is the minimum distance between distinct codewords. A linear code of length n, dimension k, and distance d is called an $[n,k,d]$ code.

3 Examples