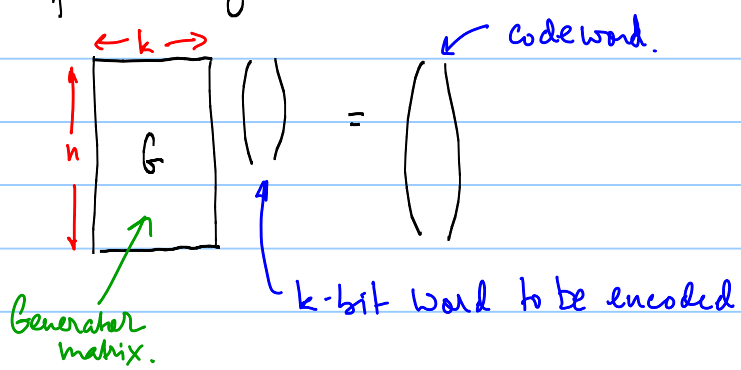
Classical Coding Theory - basic definitions.

Note Title 5/22/2012

Much of classical coding theory concentrates on a class of codes called linear codes.

Suppose we wish to encode k bits using n bits $(n > k)$. The encoding of all k-bit words to codewords is defined by an $n \times k$ matrix G:



All arithmetic is done mod 2 (i.e. over $\mathbb{Z}_2$).

The columns of G are linearly independent so that every v to be encoded is mapped to a unique codeword Gv. Columns of G form a basis for the k-dimensional space of codewords.

Dual matrix P is an $(n-k) \times n$ matrix called the dual matrix. The rows of P form a basis of the subspace orthogonal to the set of all codewords. The rows of P along with the columns of G are linearly independent and span the space of all n-bit strings.

We have $PG = 0$

Since any codeword s can be expressed as Gv

$$PGv = Ps = 0$$

In fact $Ps = 0$ iff s is a codeword.

($\Rightarrow$ direction comes from the fact that the rows of P + columns of G span the whole space of n-bit strings)

P is called the Parity Check Matrix. It can be used to test whether a word is a valid codeword.

The Hamming Distance between two words is the minimum number of bits that must be flipped to turn one into the other. The distance between a + b is the weight (# of 1's) in $(a+b)$.

For a code to correct t errors, the distance between any two codewords must be at least $2t+1$. t errors takes a codeword a distance t from where it started. In order to distinguish between two codewords it is required that the ball of radius t around each codeword do not intersect.

A code that encodes k bits using n bits with a distance d between codewords is a $[n, k, d]$ code.

We can describe a set of errors with a n-bit vector e which has a 1 wherever an error occurs and 0's everywhere else. If the original code is s, after the error it becomes $s' = s + e$. If we apply this to the parity check:

$$Ps' = P(s+e) = \underbrace{\cancel{Ps}}_{=0} + Pe = Pe$$

Ps' is independent of s + depends only on e. If e can be uniquely determined from Pe, we can detect + fix the error. Pe is the error syndrome.

$Pe = Pf$ iff $P(e-f) = 0$. $\Longleftrightarrow$ distance between two codewords can be as small as $wt(e-f)$.

In order for the distance of the code to be d, we must have for any vector $\bar{e}$ of wt $d-1$ or less, $P\bar{e} \neq 0$.

$\Rightarrow$ Any $d-1$ columns of P must be linearly independent.