8.4 Linear Block Codes

Consider binary n tuples under XOR addition, AND for scalar mult. It forms a vector space.

By analogy with $\mathbb{R}^n$, we'll write it as $\mathbb{B}^n$

An (n,k) <u>linear block code</u> $\mathcal{C}$ is a subspace of $\mathbb{B}^n$ of dimension k.

<u>generator matrix</u> G $k \times n$ has k n-vectors as its rows.

so $\underline{c} = \underline{i}\, G$ defines the code,

where $\underline{i}$ is length k row vector of info, $\underline{c}$ is row vect code word

<u>ex</u> (7,4) Hamming code:

$$\underline{c} = (i_1, i_2, i_3, i_4) \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

a <u>systematic code</u> has $G = [I \mid P]$ (like the Hamming (7,4) above) so that the first part of the code word is $\underline{i}$ itself.

$$\underline{c} = [\underline{i} \mid \underline{i}P]$$

The subspace $\mathcal{C}$ has orthog comp subspace $\mathcal{C}^\perp$ of dimension $m = n - k$. Put m basis vectors of $\mathcal{C}^\perp$ into rows of <u>parity check matrix</u> H $m \times n$

every $\underline{c} \in \mathcal{C}$ is orthog to every row of H

$$H\underline{c}^t = \underline{0} \leftarrow m \text{ dim}$$

$$HG^t\underline{i}^t = \underline{0} \implies HG^t = \underline{0} \leftarrow m \times k$$

ex for Hamming (7,4)

$$H = \begin{bmatrix} 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{bmatrix}$$

the syndrome of a vector $\underline{r}$ is length m row vector

$$\underline{s} = \underline{r} H^t \qquad \underline{s}^t = H \underline{r}^t$$

since only 2^m distinct syndromes, B^n is partitioned into 2^m disjoint sets (called cosets) each of size 2^k vectors.

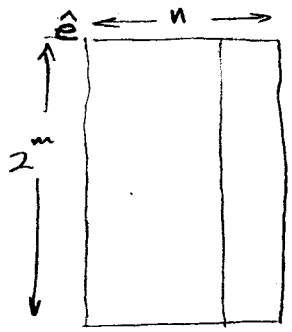
Decoding:

send $\underline{c}$, get $\underline{r} = \underline{c} + \underline{e}$.

calculate syndrome $\underline{s} = \underline{r} H^t = (\underline{c} + \underline{e}) H^t = \underline{e} H^t$
depends only on $\underline{e}$

each syndrome value could have been generated by 2^k possible error patterns. which one? Choose the one with least weight, since it's most probable.

Store a table of length 2^m, indexed by $\underline{s}$, containing the lowest weight error patterns of length n.
Add $\hat{\underline{e}}$ to $\underline{r}$: $\hat{\underline{c}} = \underline{r} + \hat{\underline{e}} = \underline{c} + \underline{e} + \hat{\underline{e}} = \underline{c}$ (we hope)



actually, width k is enough if it's systematic — why correct parity bits?

get $\underline{r}$
$\underline{s} := \underline{r} H^t$
$\hat{\underline{c}} := \underline{r} + \hat{\underline{e}}[\underline{s}]$

incomplete decoding: suppose we want to correct only single errors, request repeat if > 1. Then store only the n corresponding syndromes, with the associated lowest weight error patterns.

$$\begin{bmatrix} \underline{s}_1 & \underline{e}_1 \\ \underline{s}_2 & \underline{e}_2 \\ \vdots & \\ \underline{s}_n & \underline{e}_n \end{bmatrix}$$

get $\underline{r}$; calculate $\underline{s}$; if it's in the table, then correct, else retry.

Hamming codes If we want to correct all single errors, using m parity bits, then each of the n possible single error patterns must have a unique syndrome.

$$m \begin{bmatrix} & \overset{n}{H} & \end{bmatrix} \begin{bmatrix} \\ \underline{e}^t \\ \\ \end{bmatrix}$$

This is guaranteed if columns of H are distinct.

eg $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ cols are all $2^3 - 1$ non-zero bit patterns

(note $\underline{s}$ is the binary coded index of error location)

generalizing we have the $(2^m - 1, 2^m - 1 - m)$ Hamming codes, all single error correcting, all perfect.

(3,1) (7,4) (15,11) (31,26) etc

↑ the repetition code