Review Week 08

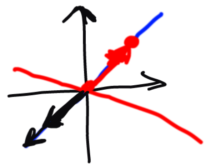
2022-11-14

Reminder: COURSEWORK
Week 10 (timed online test)
Material up to and incl. Week 09

Hamming and simplex codes + useful facts

M.J.E. Golay (1949)

Hamming code $\mathrm{Ham}(r,q)$ **for prime power** q



Def Projective space, $\mathbb{P}_{n-1}(\mathbb{F}_q)$:
- a line in $\mathbb{F}_q^n$ is a 1-dimensional subspace of $\boxed{\mathbb{F}_q^n}$.
- a representative vector of a line is any non-zero vector from that line (it spans the line)
- $\mathbb{P}_{n-1}(\mathbb{F}_q) = \{\text{all lines in } \mathbb{F}_q^n\}$

Check matrix for $\mathrm{Ham}(r,q)$**: - take one representative** $\boxed{\text{column}}$ **vector from **each line in** $\mathbb{F}_q^r$ **- this guarantees** $d=3$

Construct a check matrix H **for** $\mathrm{Ham}(3,2)$

$\begin{bmatrix}1\\0\\0\end{bmatrix}$ represents $\left\{\begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}\right\}$ r ($\mathbb{F}_2 = \{0,1\}$) q

$$\left.\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}\right\} r=3$$

Construct a check matrix H **for** $\mathrm{Ham}(2,3)$

$r=2$ $\quad \mathbb{F}_3^2 = \{$

$\begin{bmatrix}0\\0\end{bmatrix}$ — $\begin{bmatrix}1\\0\end{bmatrix}$ — $\begin{bmatrix}2\\0\end{bmatrix}$

$\begin{bmatrix}0\\1\end{bmatrix}$ — $\begin{bmatrix}0\\2\end{bmatrix}$

$\begin{bmatrix}1\\1\end{bmatrix}$ — $\begin{bmatrix}2\\2\end{bmatrix}$

$\begin{bmatrix}1\\2\end{bmatrix}$ — $\begin{bmatrix}2\\1\end{bmatrix}$

4 lines $\Rightarrow H = \underbrace{\begin{bmatrix} 1 & \cancel{2}\,1 & 1 & 0 \\ 2 & \cancel{1}\,2 & 0 & 1 \end{bmatrix}}_{4 \text{ columns}}$

Parameters of $\mathrm{Ham}(r,q)$

- n length $\# \mathbb{P}_{r-1}(\mathbb{F}_q) = \dfrac{q^r - 1}{q-1} = q^{r-1} + q^{r-2} + \dots + q + 1$
- k $n - \dim \mathrm{Ham}(r,q)^\perp = n - r$
- d $d=3 \Rightarrow t = \left[\frac{d-1}{2}\right] = 1$

$\boxed{\text{Ham}(r,q) \text{ is a perfect code}}$

The decoder for $\mathrm{Ham}(r,q)$

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

$\underline{a} = 0000000 \qquad S(\underline{a}) = 000$

$\underline{a} = 1000000 \qquad S(\underline{a}) = 100$

$\underline{a} = 0100000 \qquad S(\underline{a}) = 010$

$0010000 \qquad 110$

n vectors of wt $= 1$ $\qquad 2^r - 1$

$\#$ columns $= 2^r - 1$

$\underline{y} \in \mathbb{F}_2^n$ received

$S(\underline{y}) = \underline{\begin{bmatrix} * \\ * \\ * \end{bmatrix}} = S(e_i)$ $\qquad e_i := 00\ldots0\underset{i}{1}0\ldots0$

$S(\underline{y}) = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$; $5_2 = 101 \Rightarrow \text{Decode}(\underline{y}) = \underline{y} - \underline{e_5}$

$q \neq 2$: $S(\underline{y}) = \lambda \underline{h}_i$, $\text{Decode}(\underline{y}) = \underline{y} - \lambda \underline{e}_i$

The MacWilliams identity

$C \neq D$ but $W_C(x,y) = W_D(x,y)$

$\Downarrow$

$W_{C^\perp}(x,y) = W_{D^\perp}(x,y)$

THM $\quad W_{C^\perp}(x,y) = \frac{1}{\#C} W_C(x+(q-1)y,\, x-y)$

The Average Weight Equation

e.g. if we know $W_{C^\perp}$ for $C = \text{Ham}(2,3)$ we can calculate $W_C(x,y)$

$\frac{1}{\#C}\sum_{\underline{c}\in C} w(\underline{c}) = (n-z)(1-\frac{1}{q})$

The Plotkin bound

average weight $= n(1-q^{-1})$ if G has no zero columns

$C \subseteq \mathbb{F}_2^n$ linear, $d = d(C) > \frac{n}{2} \Rightarrow$

$\#C \leq \frac{d}{d - n/2}$

The simplex code $\Sigma(r,q)$

Def The simplex code: $\Sigma(r,q) = \mathrm{Ham}(r,q)^{\perp}$ $\cancel{\ast}$

THM $\Sigma(r,q)$, of length $n = (q^r - 1)/(q-1)$ and dimension r, has the property that the Hamming distance between each pair of codevectors is q^{r-1}.

Find the average weight of a codevector of $\Sigma(3,2)$ in three ways.

Bonus question: does $\Sigma(3,2)$ attain the Plotkin bound?

$\underline{c} \in \Sigma(r,q) \setminus \{\underline{0}\}, w(\underline{c}) = q^{r-1}$