HW 5 MTH 416 POCOCK

1) Find a minimum distance decision rule for binary code

$C := \{0000, 1100, 0011, 1111\}$

↳ $\sigma(z) = \begin{cases} 0000, & \text{if @ least 3 coords are zero} \\ 1100, & \text{if there are 2 zero coords, next to eachother} \\ 0011, & \text{if there are 2 zero coords, not next to eachother} \\ 1111, & \text{if @ most one coord is zero} \end{cases}$

ignore, for practice & visualizing

→ $F_{1111} = \{0000, 0001, 0010, 1000, 0100\}$, $F_{0000} = \{1111, 1110, 1101, 1011, 0111\}$

$F_{0011} = \{0011, 1001, 1100\}$, $F_{1100} = \{1010, 0101, 0110\}$

$M_{0000} = \Gamma_{0000,1111} + \Gamma_{0000,1110} + \Gamma_{0000,1101} + \Gamma_{0000,1011} + \Gamma_{0000,0111}$

$= e^4 + e^3(1-e) + e^3(1-e) + e^3(1-e) + e^3(1-e) = e^3(4(1-e)+e$

$= e^3(4-3e)$

2) $D := \{00000, 11100, 10011\}$. Find all $a \in B^5 \setminus D$ st $D \cup \{a\}$ is a 1-error-correcting binary code

$a = \{01111\}$.

↳ WORK ON DIFF pg.. basically

$D \cup \{a\} = \{00000, 11100, 10011, 01111\}$

has $d(D \cup \{a\}) = 3$ since it is 1-error-correcting binary code & every other code in a has $d \leq 3$ which doesnt hold □

3) Let C be a 3-error correcting code w/ $C \subseteq B^{12}$ & $|C| = 8$. Determine $|N_3(C)|$

↳ $C \subseteq B^{12}$, $\dim(C) = |C| = 8 \geq 2 \cdot 3 = r \in \mathbb{N}$ ✓.

$N_3(C) = \{ y = B^{12} \mid d(x,y) \leq 3 \ \exists x \in X \}$

Let $a, b \in C$ w/ $a \neq b$; then $N_3(a) \cap N_3(b) \neq \emptyset$

Also $|N_3(C)| \leq |C| \sum_{i=0}^{r} \binom{n}{i}$

$\leq (8) \sum_{i=0}^{r} \binom{12}{i}$

Now by thm 5.2.3;

$|N_3(C)| \leq (8) \sum_{i=0}^{r} \binom{12}{i} \leq 2^{12}$

≤ 4096

So $|N_3(C)| \leq 4{,}096$

HW 5 CONT

4) Let n & r be positive $\mathbb{Z}$'s. let $D \subseteq \mathbb{B}^n$ be an r-error-correcting code & let $a \in \mathbb{B}^n \setminus D$. Show $D \cup \{a\}$ is an r-error-correcting code iff $a \notin N_{2r}(D)$.

$\hookrightarrow \Rightarrow$ Assume $a \notin N_{2r}(D)$. Since r is any positive $\mathbb{Z}$; $N_{2r}(D)$ will be the set of positive products of 2 w/ integer 2; multiples of 2. $\therefore$ So $N_{2r}(D)$ is neighboring of D w/ radius ≥ 2 st $2 \mid$ radius. Now, $a \in \mathbb{B}^n \setminus D$ implies a's codewords are same length as D's codewords. For

5) Let $n \in \mathbb{N}$ & suppose $C \subseteq \mathbb{B}^n$ is a perfect, 1-error-correcting binary code. Show there exists $l \in \mathbb{N}$ st $n = 2^l - 1$ & $|C| = 2^{2^l - l - 1}$

↳ Let $C \subseteq \mathbb{B}^n$ be a perfect 1-error-correcting binary code for $n \in \mathbb{N}$, Let it be linear; then C is a hamming code (6.4.8).

By thm 6.4.9, Hamming code $\Rightarrow n = 2^{l-1}$ & columns of standard $m \times n$ check matrix H are the non-zero vectors of $\mathbb{F}_2^m$.

Now, bc C is Hamming code; $|C|(1+l) = 2^l$ & H in standard form $\Rightarrow \dim(C) = n - l$. So

① $|C| = 2^{n-l}$. Thus $|C|(1+n) = 2^n \Leftrightarrow 2^{n-l}(1+n) = 2^n$ ①
$\Leftrightarrow 1 + n = 2^l \Leftrightarrow n = 2^l - 1$.

Now using $n = 2^{l-1}$ & subbing it into ①

$\Rightarrow |C| = 2^{2^l - 1 - l}$

$= 2^{2^l - l - 1}$. $\square$

HW 5

6) Let $n \in \mathbb{N}$

a) Let $a, b, c \in \mathbb{B}^n$. Show $d(a,b) + d(b,c) + d(a,c) \leq 2n$

↳ n = length of codewords a, b, c. By lemma (5.1.11);

* $d(a,c) = d(a,b) + d(b,c) - 2|D(a,b) \cap D(b,c)|$. Now,

if $i \in D(a,b) \cap D(b,c)$ then $a_i \neq b_i \neq c_i$ $\mathbb{B}$ has 2 elements so $a_i = c_i$.

$\Rightarrow d(a,b) + d(b,c) + ^{*}(d(a,b) + d(b,c) - 2|D(a,b) \cap D(b,c)|)$

$\Rightarrow |D(a,b)| + |D(a,c)| + (|D(a,b)| + |D(b,c)| - 2|D(a,b) \cap D(b,c)|)\ldots$

0 1 1 0 < 2. As n increases; the min (d) difference between a, b, c could only increase by 2 since you're adding one value ∴ it will always be less than or equal to the length $(n) \times 2$.

b) Let $C \subseteq \mathbb{B}^n$ be a binary code w/ min distance $= \delta$. Suppose $|C| \geq 3$. Show $d(a,b) \leq 2(n-\delta)$ $\forall a, b \in C$

↳ Let $a, b \in C \subseteq \mathbb{B}^n$. Let $r \in \mathbb{N}$. Then for each $b \in \mathbb{B}^n$; $\exists$ @ most one $a \in C$ w/ $d(a,b) \leq r$. $d(C) = \delta$, because $|C| \geq 3$ we know there exists values in C st their distance $\geq \delta$. So using (a); $d(a,b) \leq 2r$, but we know here $r = n - \delta$ so

$d(a,b) \leq 2(n-\delta)$

□

$\ell = 5$

7) Which are linear codes (subsets of $\mathbb{F}_2^5$)

a) $C_1 := \{00000, 11000, 10011, 11111\}$

↳ a subspace of $\mathbb{F}_2^n$ is a binary linear code of $\ell = n$. So $00000 \in C$ ✓

$$\begin{array}{r} \to 11000 \\ + 10011 \\ \hline 01011 \notin C \end{array}$$

11111

SO NO

b) $C_2 := \{00000, 11000, 00111, 11111, 01010, 10010, 01101, 10100\}$

↳ $00000 \in C$ ✓

$$\begin{array}{r} 11000 \\ +00111 \\ \hline \end{array}, \quad \begin{array}{r} 11000 \\ +01010 \\ \hline 10010 \end{array}, \quad \begin{array}{r} 11000 \\ 10010 \\ \hline 01010 \end{array}, \quad \begin{array}{r} 11000 \\ +01101 \\ \hline 10101 \end{array} \quad \ldots$$

CONT ON DIFF pg

closed under addition

& since $\ell x \in C$ $\forall \ell \in \mathbb{F}_2, x \in \mathbb{F}_2^1$, closed under *

So yes.

c) $C_3 := \{x \in \mathbb{F}_2^5 \mid x_1 + x_2 + x_5 = 0\}$

↳ C consists all even $x \in \mathbb{F}_2^5$; $\vec{0} \in C$ &

If $x, y \in C$ then $\sum_{i=1} (x_i + y_i) =$

So $\sum_{i=1}^n x_i + \sum_{i=1}^n y_i = 0 + 0 = 0$

$x + y \in C$ $\therefore$ yes

8) Let $C \subseteq \mathbb{F}_2^5$ be the linear code w/ generating matrix : $E := \begin{array}{c} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array} \begin{array}{c} a \\ b \\ c \\ d \\ e \end{array}$ [3x7]

$C = \{ xG \mid x \in V[k,q] \}$

a) list all elements of C

$\rightarrow 5 \rightarrow 2^5 = 32$ row vectors [row vector]·[G]

So C = {00000, 00001, 0010, 00011, 00100, 00101, 00110, 00111, 01000, 01001, 01010, 01011, 01100, 01101, 01110, 01111, 10000, 10001, 10010, 10011, 10100, 10101, 10110, 10111, 11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111}

b) determine the min distance of C

a → 1, 2, 1, 2 ; b → 1, 1, 2, 3 ; min distance = 1

c) is C 1-error-correcting?

$[(d-1)/2]$

$(1-1)/2$

0 , no