HW #11 Math 4280 4/11/08

5.4, 5.5, 5.9, 5.10

Hi Bri,
Please grade 5.5. 10pts & 5.9 10pts
-Kate.

5.5) How large can a subset $\mathcal{C} \subseteq \mathbb{F}_2^3$ be if $d(\vec{u},\vec{v}) \geq 2$ for all $\vec{u} \neq \vec{v}$ in $\mathcal{C}$. Describe geometrically all sets obtaing this bound. What is the analogoous bound for subsets of $\mathbb{F}_2^n$?

Claim: The largest such sets $\mathcal{C}$ have 4 elemts,
$\mathcal{C} = \{000, 011, 101, 110\}$ and $\{100, 010, 001, 111\}$.

Proof Let $\vec{u} = u_1u_2u_3 \in \mathcal{C}$,

Clearly, $\mathcal{C} \subseteq \mathbb{F}_2^3 \setminus \{\vec{v} \in \mathbb{F}_2^3 \mid d(\vec{u},\vec{v}) = 1\} = D$

From problem 5.4) $|\{\vec{v} \in \mathbb{F}_2^3 \mid d(\vec{u},\vec{v}) = 1\}| = 3$

So $|\mathcal{C}| \leq |D| = 8 - 3 = 5$

That is $\mathcal{C}$ has at most 5 elemts.
If $|\mathcal{C}| = 5$, then

$$\mathcal{C} = D = \{\vec{v} \in \mathbb{F}_2^3 \mid d(\vec{u},\vec{v}) = 0, 2 \text{ or } 3\}$$

From Problem 5.4 again D has 3 elemts distance 2 from $\vec{u}$, and one elemt distance 3 from $\vec{u}$.

Let $\vec{v}_2$ & $\vec{v}_3$ be s.t. $d(\vec{u},\vec{v}_2) = 2$, $d(\vec{u},\vec{v}_3) = 3$.

5.5 cont. 1.

Since $d(\vec{u},\vec{v}_3)=3$ $\vec{u}=u_1u_2u_3$ $\vec{v}_3=v_{3_1}v_{3_2}v_{3_3}$.

$\Rightarrow$ $u_i \neq v_{3_i}$ for all i. $1 \leq i \leq 3$.

Since $d(\vec{u},\vec{v}_2)=2$ $\vec{u}=u_1u_2u_3$ $\vec{v}_2=v_{2_1}v_{2_2}v_{2_3}$.

$\Rightarrow$ $u_k \neq v_{2_k}$, $u_\ell \neq u_{2_\ell}$ for distinct k & ℓ $1 \leq k < \ell \leq 3$.

There are 2 possibilities for each of the u_i's, v_{2_i}'s & v_{3_i}'s.

So $v_{2_k} \neq u_k$ and $v_{3_k} \neq u_k$ $\Rightarrow$ $v_{2_k} = v_{3_k}$.

and

$v_{2_\ell} \neq u_\ell$ and $v_{3_\ell} \neq u_\ell$ $\Rightarrow$ $v_{2_\ell} = v_{3_\ell}$.

$\Rightarrow$ $d(\vec{v}_2, \vec{v}_3) \leq 1$.

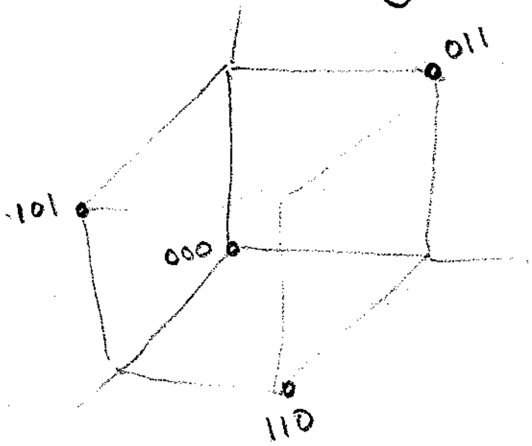
$\mathcal{D} = \{\vec{v} \in \mathbb{F}_2^3 \mid d(\vec{u},\vec{v})=0, 2 \text{ or } 3\}$ does not have the desired property. any and set $\mathcal{C}$ with $\vec{u} \in \mathcal{C}$ and the desired property is a proper subset of $\mathcal{D}$

$\Rightarrow |\mathcal{C}| < |\mathcal{D}| = 5$ $\Rightarrow$ $|\mathcal{C}| \leq 4$.

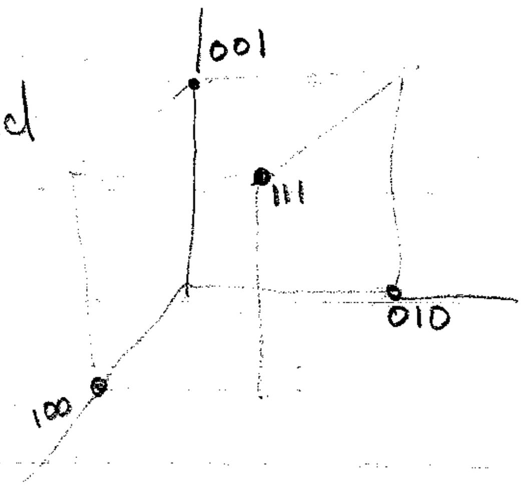
and because we have 2 examples with $|\mathcal{C}|=4$, 4 is the maximum.

5.5 cont. 2

Geometrically they are



and



Such a set in $\mathbb{F}_2^{\,n}$?

Certainly the sets

$$\mathcal{C}_0 = \{ \vec{u} = u_1 u_2 \cdots u_n \mid \textstyle\sum u_i \text{ is even} \}$$
$$\mathcal{C}_1 = \{ \vec{u} = u_1 u_2 \cdots u_n \mid \textstyle\sum u_i \text{ is odd} \}$$

have distance at least 2 between all distinct pairs of elements. As 'if $d(\vec{u},\vec{v}) = 1$, then $\sum u_i$ is odd & $\sum v_i$ is even.'

or $\sum u_i$ is even & $\sum v_i$ is odd.

It remains to show that no larger sets can exist.

$$|\mathcal{C}_0| = |\mathcal{C}_1| = 2^{n-1}$$

5.5 cont 3

<u>Claim</u> If $d(\vec{u},\vec{v}) \geq 2$ for all $\vec{u},\vec{v} \in \mathcal{C}$ $\vec{u} \neq \vec{v}$.

$\mathcal{C} \subseteq \mathbb{F}_2^n$, then $|\mathcal{C}| \leq 2^{n-1}$.

Let $|\mathcal{C}| = M$. For each $u_i \in \mathcal{C}$,

Let $S_i = \{\vec{v} \in \mathbb{F}_2^n \mid d(\vec{u}_i,\vec{v}) = 1\}$.

then $\bigcup_{u_i \in \mathcal{C}} S_i \subseteq \mathcal{C}^c$, the complement of $\mathcal{C}$ in $\mathbb{F}_2^n$.

and $|S_i| = n$. The S_i's need not be disjoint, but each $\vec{v} \in \mathbb{F}_2^n$ is in at most n of the S_i's. So $\sum_{u_i \in \mathcal{C}} |S_i|$ over counts each element of $\bigcup S_i$ at most n times $\Rightarrow$

$$|\bigcup S_i| \geq \frac{1}{n} \sum_{u_i \in \mathcal{C}} |S_i| = \frac{1}{n} \cdot M \cdot n = M$$

So $|\mathcal{C}^c| \geq |\bigcup S_i| \geq M$

$$\Rightarrow \quad 2^n = |\mathbb{F}_2^n| = |\mathcal{C}| + |\mathcal{C}^c| \geq M + M = 2M$$

$\Rightarrow \quad M \leq 2^{n-1}$ as claimed.

5.9) A binary channel Γ always transmits 0 correctly, but transmits 1 as 1 or 0 with probabilities P and $Q = \overline{P}$ with $0 < P < 1$.

① Write down the channel matrix, and describle the maximum likelyhood rule.

$$M = \begin{bmatrix} 1 & 0 \\ Q & P \end{bmatrix}$$, since $1 > Q$, $\Delta(0) = 0$ and since $P > 0$, $\Delta(1) = 1$

is the maximum likelyhood rule.

② If the input probabilities are p and $\bar{p}$ find the probability of error.

$$R_{ij} = \begin{bmatrix} p & 0 \\ \bar{p}Q & \bar{p}P \end{bmatrix}$$, so for the maximum likelyhood rule.

$Pr_C = p + \bar{p}P$ and $Pr_E = \bar{p}Q$.

③ To improve reliability 0 and 1 are encoded as 000 and 111. Describe the resulting maximum likelyhood decoding.

channel matrix:

$$\begin{array}{c} \\ 000 \\ 111 \end{array} \begin{array}{c} \begin{array}{cccccccc} 000 & 001 & 010 & 100 & 011 & 101 & 110 & 111 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ Q^3 & Q^2P & Q^2P & Q^2P & Q^2P & Q^2P & Q^2P & P^3 \end{bmatrix} \end{array}$$

So maximum likelihood decoding sends $\Delta(000) = 000$ and $\Delta(\vec{u}) = 111$ for all $\vec{u} \in \mathbb{F}_2^3$, $\vec{u} \neq 000$.

④ It is not the same as majority decoding or nearest neighboor decoding.

(5) Find the resulting rate and error-probability

rate, $R = \frac{\log_2 2}{3} = \frac{1}{3}$

and error probability $= \bar{p} Q^3$.

(6) What happens if instead we use the binary repetition code R_n and let $n \to \infty$?

rate $R = \frac{1}{n}$ and error probability $= \bar{p} Q^n$.
both $\to 0$ as $n \to \infty$.