Coding Theory: Problem sheet 1

This problem sheet is not for assesment:
solutions will be posted on the web in due course

1. The binary repetition code of length n consists of the words $000\cdots00$ and $111\cdots11$. Let the probability of receiving each bit incorrectly be p, and suppose that these events are independent. What is the probability that "majority vote" decodes a block incorrectly when $n=5$ and when $n=7$? Evaluate these probabilities numerically (to three significant figures) in both cases for $p=0\cdot1$, $p=0\cdot05$ and $p=0\cdot01$.

2. Let $\Omega=\{0,1\}$. Let $\mathbf{a}\in\Omega^n$. We define the *weight* of $\mathbf{a}$ to be the number of ones in $\mathbf{a}$, and denote it as $w(\mathbf{a})$. [For example, $w(01100111)=5$.] Prove that $w(\mathbf{a})=d(000\cdots00,\mathbf{a})$.

   For $\mathbf{a}$, $\mathbf{b}\in\Omega^n$ define $\mathbf{a}\bullet\mathbf{b}$ as the word whose i-th letter is a_ib_i. [This means that $\mathbf{a}\bullet\mathbf{b}$ has a 1 where both $\mathbf{a}$ and $\mathbf{b}$ have 1s and a 0 otherwise; for example, $01100111\bullet10101010=00100010$.] Prove that $d(\mathbf{a},\mathbf{b})=w(\mathbf{a})+w(\mathbf{b})-2w(\mathbf{a}\bullet\mathbf{b})$.

3. Let Ω be an alphabet of size q. Prove that if C is a $(3,M,2)$-code over Ω, then $M\le q^2$. Find a $(3,4,2)$-code with $\Omega=\{0,1\}$ and a $(3,9,2)$-code with $\Omega=\{0,1,2\}$. (This is a special case of the *Singleton bound.*)

   [Hint: consider the first two letters in each of the codewords.]

4. Recall that the binary parity check code P_n is the set of all words of length n over $\{0,1\}$ containing an even number of 1s. Prove that $d(\mathbf{a},\mathbf{b})$ is even for all $\mathbf{a}$, $\mathbf{b}\in P_n$.

   Let C be a code of length m over $\{0,1\}$. We construct a new code C^+ of length $m+1$ as follows. For each $\mathbf{a}=a_1a_2\cdots a_m\in C$ define $\mathbf{a}^+=a_1a_2\cdots a_ma_{m+1}$ where a_{m+1} is chosen to ensure that $\mathbf{a}^+$ contains an even number of 1s. [For example if $\mathbf{a}=1101$ then $\mathbf{a}^+=11011$]. Let C^+ be the set of the $\mathbf{a}^+$ for $\mathbf{a}\in C$. It's clear that the codes C and C^+ have the same size. Compute C^+ for the code $C=\{00000,00111,11100,11011\}$. Prove that if $\mathbf{a}$, $\mathbf{b}\in C$

   $$d(\mathbf{a}^+,\mathbf{b}^+)=\begin{cases} d(\mathbf{a},\mathbf{b}) & \text{if } d(\mathbf{a},\mathbf{b}) \text{ is even,}\\ d(\mathbf{a},\mathbf{b})+1 & \text{if } d(\mathbf{a},\mathbf{b}) \text{ is odd.}\end{cases}$$

   Deduce that if $d(C)$ is odd, then $d(C^+)=d(C)+1$.

   (We say that C^+ is obtained from C by *adding an overall parity check.*)

5. Let C be a code with minimum distance $d(C)$, and suppose that $d(C) \geq r + 1$. Prove that C detects r errors.

6. Recall that a *perfect* code is one giving equality in the sphere-packing bound. Prove that there is no perfect 2-error correcting code of length n over $\{0, 1\}$ with $6 \leq n \leq 10$. (Hint: how many words would such a code have?)

   Prove that there is no perfect 2-error correcting code of length n over $\{0, 1, 2\}$ with $5 \leq n \leq 10$. (As a challenge, think about the case $n = 11$).

7. In each case, construct, if possible, an (n, M, d)-code over $\Omega = \{0, 1\}$ with the following parameter sets (n, M, d): $(7, 2, 7)$, $(5, 3, 4)$, $(6, 4, 4)$, $(4, 7, 2)$, $(8, 29, 3)$. If, in any case, there is no such code, explain why not.

8. Find a $(4, 9, 3)$-code over $\Omega = \{0, 1, 2\}$.

9. (Challenge problem) Prove that there is a $(3, q^2, 2)$-code over any finite alphabet Ω of size q.

RJC 2/10/2007