******The following questions are concerned with Chapter 5 of the notes - Perfect Codes.******

61 Let $C_1 = \langle(0,1,1,1)\rangle$, and $C_2 = \langle(0,1,1,1,),(1,0,1,2,)\rangle$, both codes in $\mathbb{F}_3^4$. Find parameters $[n,k,d]$ for each code, and find $|S(\mathbf{x},1)|$ for $\mathbf{x} \in \mathbb{F}_3^4$. Show that $|C_1|$, $|C_2|$ and $|S(\mathbf{x},1)|$ all divide $|\mathbb{F}_3^4|$, but only one of the codes is perfect.

62 For $\mathbf{x} \in \mathbb{F}_q^n$, find $|S(\mathbf{x},t)|$ for $t = 0$ and $t = n$. Show that there is a perfect code for each value of t, and give parameters (n,M,d) if possible. Are these "trivial" codes linear? Explain why they are not useful.

63 A binary repetition code is $C_n = \{(0,\ldots,0),(1,\ldots,1)\} \subset \mathbb{F}_2^n$. If $n = 2t+1$ is odd, show that C_n is perfect. (*Hint*: Use well-known properties of Pascal's triangle.)

64 Let Ham$_2(3)$ have the standard check-matrix described in the lecture. Use the algorithm to decode the received words $\mathbf{y}_1 = (0,0,1,0,0,1,0)$ and $\mathbf{y}_2 = (1,0,1,0,1,0,1)$.

65 Construct check-matrices for these two Hamming codes: (In each case, write out a couple of the $L_{\mathbf{v}}$ sets, but you do not have to list them all.) a) Ham$_5(2)$ b) Ham$_3(3)$

66 Let C be the Ham$_7(2)$ code with check-matrix $H = \begin{pmatrix} 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$. Decode the received words $\mathbf{y}_1 = (1,0,2,0,3,0,4,0)$ and $\mathbf{y}_2 = (0,6,0,5,0,4,0,3)$.

67 Show that Ham$_q(r)$ is perfect.

68 Explain why the decoding algorithm for q-ary Hamming codes works.

69 Let $C \subseteq \mathbb{F}_5^5$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \end{pmatrix}$. Show that C is not a Hamming code. Nonetheless, try to use the Hamming decoding algorithm to decode received words $\mathbf{y}_1 = (3,3,1,0,4)$ and $\mathbf{y}_2 = (1,2,1,0,0)$. Why does the algorithm only sometimes work? When it doesn't, can you still use the syndrome to find a nearest neighbour in the code for that word? Explain.

70 Let C_1 and C_2 in $\mathbb{F}_3^5$ have generator-matrices $G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 \end{pmatrix}$. Show that these codes are (monomially) equivalent. Write down generator matrices for the extended codes $\widehat{C_1}$ and $\widehat{C_2}$, and show that these codes have different $d(\widehat{C_i})$, and so are not equivalent. (You could find check-matrices and use Theorem 4.11., or you could just think about possible weights of codewords.)

71 Let $C \subseteq \mathbb{F}_5^5$ have generator-matrix $G = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 0 & 1 & 1 \end{pmatrix}$. By finding their minimum distances, show that the codes $C^{\{5\}}$ and $C^{\{3\}}$ are not equivalent.

72 Let $C \subseteq \mathbb{F}_3^4$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$.

a) Find a generator-matrix G for C, and check- and generator-matrices $\widehat{H}$ and $\widehat{G}$ for the extended code $\widehat{C}$.
b) Now puncture $\widehat{C}$ at each position in turn, to give generator-matrices $G_{p1},\ G_{p2},\ G_{p3},\ G_{p4},\ G_{p5}$ for codes $C_{p1},\ C_{p2},\ C_{p3},\ C_{p4},\ C_{p5}$.
c) Which of the six codes $C,\ C_{p1},\ \ldots,\ C_{p5}$ have the same minimum distance? Which are equivalent? Which are actually the same code?
Hint: There are many ways to do all this, and you may find different matrices. But you should get the same answers for c). It might save you work to use a $\widehat{G}$ in form $(A|I)$ or $(I|A)$.

73 Can we "extend" and "puncture" over $\mathbb{R}$? Let C be the line $y = 2x$ in $\mathbb{R}^2$.
a) Find H and G such that $C = \{\mathbf{x} \in \mathbb{R}^2 \mid \mathbf{x}H^t = 0\} = \{\lambda G \mid \lambda \in \mathbb{R}\}$.
b) Now, in $\mathbb{R}^3$, consider the intersection of the plane $y = 2x$ with the plane $x + y + z = 0$.
Find a check-matrix $\widehat{H}$ and a generator-matrix $\widehat{G}$ for this line $\widehat{C}$.
c) Puncturing $\widehat{C}$ in each position gives three different lines, back in $\mathbb{R}^2$ again. Specify them; in geometric terms, how are they related to $\widehat{C}$?

74 a) Show that a binary $[90, k, 5]$-code, if it exists, could be perfect, and that if it is perfect, $k = 78$.
The rest of this questions shows, by contradiction, that there is no such code.
b) Show that, in $\mathbb{F}_2^r$, exactly half the vectors have odd weight, half even. (*Hint:* pair them up...)
c) Suppose that a binary $[90, 78, 5]$-code exists. Then the columns of its check-matrix H are $\mathbf{h}_1, \ldots, \mathbf{h}_{90}$, in $\mathbb{F}_2^{12}$. Now consider the following vectors in $\mathbb{F}_2^{12}$: $\mathbf{0}$; the $\mathbf{h}_i$, $1 \leq i \leq 90$; the $\mathbf{h}_i + \mathbf{h}_j$, $1 \leq i < j \leq 90$. Show that all of these vectors are distinct.
d) Let the set $X = \{\mathbf{0}\} \cup \{\mathbf{h}_i \mid 1 \leq i \leq 90\} \cup \{\mathbf{h}_i + \mathbf{h}_j \mid 1 \leq i < j \leq 90\}$. Show that $X = \mathbb{F}_2^{12}$.
e) Now let m be the number of odd-weight columns of H. In terms of m, how many vectors in X have odd weight? Use b) to reach a contradiction.

75 Prove Lemma 5.12.

76 Let $\mathcal{G}_{12}$ be the ternary code with generator-matrix

$$G = [I_6 \mid A] = \begin{pmatrix} 1 & & & & & & 0 & 1 & 1 & 1 & 1 & 1 \\ & 1 & & & 0 & & 1 & 0 & 1 & 2 & 2 & 1 \\ & & 1 & & & & 1 & 1 & 0 & 1 & 2 & 2 \\ & & & 1 & & & 1 & 2 & 1 & 0 & 1 & 2 \\ & 0 & & & 1 & & 1 & 2 & 2 & 1 & 0 & 1 \\ & & & & & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

We write $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_6$ for the rows of A.
a) Show that $\mathcal{G}_{12}^{\perp} = \mathcal{G}_{12}$, explaining briefly why we do not need to calculate 21 separate dot products. It follows that $\mathcal{G}_{12}$ also has a generator matrix $[B \mid I_6]$; how do the rows of B relate to the $\mathbf{a}_i$?
b) Find the values of $w(\mathbf{a}_i + \mathbf{a}_j)$ and $w(\mathbf{a}_i - \mathbf{a}_j)$ for $1 \leq i < j \leq 6$. (Again, there are only a few cases to consider.)
c) Show that if $\mathbf{c} \in \mathcal{G}_{12}, \mathbf{c} \neq \mathbf{0}$, then $w(\mathbf{c}) \geq 6$. Do this by contradiction, writing $\mathbf{c} = (\mathbf{l}, \mathbf{r})$.
d) To make $\mathcal{G}_{11}$, we puncture the code $\mathcal{G}_{12}$ by removing the last column of G. Show that $\mathcal{G}_{11}$ is an $[11, 6, 5]$ code.

77 Constructing new objects in maths often combines deduction (it must be like this) with convenient choices (try one like this) and checking (does it work?). We shall construct a check-matrix H for $\mathcal{G}_{11}$ as follows:
We can certainly choose to have H in RREF, and (by choosing the right code from the equivalence class) we can assume $H = [I_5 \mid A]$. This time we work with *columns*, not rows: the columns of I_5 are $\mathbf{e}_1, \ldots, \mathbf{e}_5$; let the columns of A be $\mathbf{a}_1, \ldots, \mathbf{a}_6$. By Theorem 4.11. we need to make A so that no four columns of of H are linearly dependent. This requirement tells us a lot about the $\mathbf{a}_i$.

a) Show that all $w(\mathbf{a}_i) \geq 4$.
b) Show that all $w(\mathbf{a}_i + \mathbf{a}_j)$ and all $w(\mathbf{a}_i - \mathbf{a}_j)$ must be ≥ 3.
c) Suppose $w(\mathbf{a}_i) = w(\mathbf{a}_j) = 5$. Show that $w(\mathbf{a}_i + \mathbf{a}_j) + w(\mathbf{a}_i - \mathbf{a}_j) = 5$. Deduce that we can have at most one $\mathbf{a}_i$ of weight 5 in A.
d) Similarly, show that if $\mathbf{a}_i$ and $\mathbf{a}_j$ each have just one 0, these 0s must be in different rows.
Using c) and d), we choose to have our weight 5 column be all 1s, and place the columns in a convenient order, taking

$$H = [I_5 \mid A] = \begin{pmatrix} 1 & & & & & 1 & * & * & * & * & 0 \\ & 1 & & 0 & & 1 & * & * & * & 0 & * \\ & & 1 & & & 1 & * & * & 0 & * & * \\ & 0 & & 1 & & 1 & * & 0 & * & * & * \\ & & & & 1 & 1 & 0 & * & * & * & * \end{pmatrix},$$

where each * is either 1 or 2.

e) Use b) and $\mathbf{a}_1$ to show that each $\mathbf{a}_j, 2 \leq j \leq 6$, must have two 1s and two 2s.
f) For $2 \leq j \leq 6$, $\mathbf{a}_i$ and $\mathbf{a}_j$ will differ in at least two positions, because of their 0s. Show that they must differ in at least one other position, and match in at least one other position.
g) Using e) and f), and working column by column, complete the matrix A.

Do we know that the matrix H we have constructed gives a code with $d = 5$?

h) Find a linearly dependent set of 5 columns.
i) Any linearly dependent set of 4 columns would involve n_e columns from I, and n_a columns from A, with $n_e + n_a = 4$. Which values of n_a have we ruled out? How much more checking would we need to do?