******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.

S61 $C_1 = \{(0,0,0,0),(0,1,1,1),(0,2,2,2)\}$ has parameters $[4,1,3]$, and $|C_1| = 3$. C_2 has check matrix $\begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$, so parameters $[4,2,3]$ and $|C_2| = 3^2$. In $\mathbb{F}_3^4$, we have $|S(\mathbf{x},1)| = 1 + 4 \times 2 = 9$. So this, and $|C_1|$ and $|C_2|$, all divide $|\mathbb{F}_3^4| = 81$. Note that since for both codes $d = 3$, the $S(\mathbf{c},1)$ are disjoint. Since $|S(\mathbf{c},1)||C_2| = 81$, these spheres round the codewords of C_2 exactly fill the space, and C_2 is perfect. However for C_1, with fewer spheres, of the same size, the space is not filled. △

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.

S62 If $t = 0$, then $|S(\mathbf{x},t)| = \sum_{k=0}^{t} \binom{n}{k}(q-1)^k = 1$, and we take $C = \mathbb{F}_q^n$. This is a $(n,q^n,1)$ code so we cannot detect or correct any errors. If $t = n$, any sphere $S(x,t) = \mathbb{F}_q^n$, and we have just one codeword. △

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.)

S63 This code has just two codewords. Since $d = n$, the spheres $S(\mathbf{c},t)$ are disjoint. The number of words in the sphere, $|S(\mathbf{c},t)| = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$, which is exactly half of the sum of the n^{th} row in Pascal's triangle. The whole row has sum 2^n, so $|S(\mathbf{c},t)| = 2^{n-1}$. Thus both spheres together cover all of $\mathbb{F}_2^n$. △

64 Let $\text{Ham}_2(3)$ 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 $\mathbf{y}_2 = (1,0,1,0,1,0,1)$.

S64 Using $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ we get $S(\mathbf{y}_1) = (1,0,1)$ which is 5 written in base 2. So we alter the 5th digit and decode to $((0,0,1,0,1,1,0)$. But $S(\mathbf{y}_2) = (0,0,0)$, so $\mathbf{y}_2$ is in the code. △

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) $\text{Ham}_5(2)$ b) $\text{Ham}_3(3)$

S65 a) For $\text{Ham}_5(2)$, two of the $L_{\mathbf{v}}$ sets would be $L_{(1,0)} = \{(1,0),(2,0),(3,0),(4,0)$ and $L_{(1,2)} = \{(1,2),(2,4),(3,1),(4,3)$. One possible check-matrix would be $H = \begin{pmatrix} 4 & 2 & 2 & 0 & 4 & 1 \\ 0 & 2 & 3 & 1 & 3 & 3 \end{pmatrix}$.
b) For $\text{Ham}_3(3)$, two of the $L_{\mathbf{v}}$ sets would be $L_{(1,0,2)} = \{(1,0,2),(2,0,1)\}$ and $L_{(1,1,2)} = \{(1,1,2),(2,1,1)\}$. Two possible check-matrix would be

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \end{pmatrix}, H_2 = \begin{pmatrix} 1 & 2 & 2 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 1 & 1 & 0 & 0 & 2 & 2 & 0 & 2 & 1 & 1 & 1 \end{pmatrix}.$$

△

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 $\mathbf{y}_2 = (0, 6, 0, 5, 0, 4, 0, 3)$.

S66 For a Hamming code, we decode the received words by first calculating their syndromes. We therefore have $S(\mathbf{y}_1) = \mathbf{y}_1 H^t = (1 + 2 + 9 + 20, 2 + 3 + 4) = (4, 2)$. Since this is not 0, $\mathbf{y}_1$ is not itself a codeword. Since the Hamming code is perfect with minimum distance 3, each received word lies in a sphere of radius 1 around some codeword, so we must have $\mathbf{y}_1 = \mathbf{c}_1 + \lambda \mathbf{e}_i$, where $\mathbf{e}_i$ is a standard basis vector, respresenting our error of weight 1.

In terms of this error vector, we have $S(\mathbf{y}_1) = S(\mathbf{c}_1 + \lambda e_i) = S(\mathbf{c}_1) + \lambda S(e_i) = \lambda \mathbf{h}_i$, where $\mathbf{h}_i$ is the i^{th} column of H, and where we've used linearity of the syndrome, and that all codewords have syndrome 0. We therefore need to find λ and i, such that $\lambda \mathbf{h}_i = (4, 2)$. Since all of the columns of H end in a 1, we immediately see that we must have $\lambda = 2$, and therefore $i = 4$, as $(4, 2) = 2(2, 1)$. We can therefore decode $\mathbf{y}_1$ as $\mathbf{c}_1 = \mathbf{y}_1 - 2e_4 = (1, 0, 2, 5, 3, 0, 4, 0)$.

The process is the same for decoding $\mathbf{y}_2 = (0, 6, 0, 5, 0, 4, 0, 3)$. We first calculate $S(\mathbf{y}_2) = (10 + 16 + 18, 6 + 5 + 4 + 3) = (2, 4) = 4(4, 1)$. So we have $\lambda = 4$, $i = 6$, and we decode $\mathbf{y}_2$ as $\mathbf{c}_2 = \mathbf{y}_2 - 4\mathbf{e}_6 = (0, 6, 0, 5, 0, 0, 0, 3)$. △

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

S67 Since, by construction, no column in the check-matrix is a multiple of another, we know that $d($ Ham$_q(r)) \geq 3$. So spheres of radius 1 are disjoint. For a codeword $\mathbf{c}$, how many words have $d(\mathbf{v}, \mathbf{c}) = 1$? Choose a position to change, and then choose a different symbol, so $n(q - 1)$. Thus $|S(\mathbf{c}, 1)| = 1 + n(q - 1) = 1 + q^r - 1 = q^r$. But $|\text{Ham}_q(r)| = q^k = q^{n-r}$. So the disjoint union of all the $|S(\mathbf{c}, 1)|$ contains $q^{n-r} q^r = q^n$ words. This is all of $\mathbb{F}_q^n$, as required. △

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

S68 Since Ham$_q(r)$ has $d = 3$ and is perfect, any word $\mathbf{y}$ in $\mathbb{F}_q^n$ is in exactly one $S(\mathbf{c}, 1)$. So $\mathbf{y} = \mathbf{c} + \mathbf{x}$, with $w(\mathbf{x}) \leq 1$. If $w(\mathbf{x}) = 0$, then $\mathbf{y}$ is a codeword. If $w(\mathbf{x}) = 1$, then $\mathbf{x} = \lambda \mathbf{e}_i$ for some $\lambda \in \mathbb{F}_q$ and standard basis vector $\mathbf{e}_i, 1 \leq i \leq n$. So $\mathbf{y} = \mathbf{c} + \lambda \mathbf{e}_i$. Now $S(\mathbf{y}) = S(\mathbf{c}) + S(\lambda \mathbf{e}_i) = \lambda S(\mathbf{e}_i) = \lambda \cdot$ column i of H. By the construction of the check-matrix H, for any $S(\mathbf{y})$ there is just one λ and one i which make this work. We then subtract the error $\lambda \mathbf{e}_i$ to get $\mathbf{c}$. △

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.

S69 Since $q = 5, r = 2$, a Hamming code Ham$_5(2)$ would have $n = \frac{5^2 - 1}{5 - 1} = 6$. But C has $n = 5$, so it is not a Hamming code. Alternatively, C is not a Hamming code because no column is from $L_{(1,4)}$. We find that $S(\mathbf{y}_1) = (3, 1) = 3(1, 2)$. Since this is 3 times column 4 of H, we can assume the error-vector was $(0, 0, 0, 3, 0)$ and decode to $\mathbf{c}_1 = (3, 3, 1, 2, 4)$. But $S(y_2) = (2, 3) = 2(1, 4)$, and this is not a multiple of any column. So there cannot be an error-vector of weight 1. No $S(\mathbf{c}, 1)$ contains y_2; unlike a Hamming code, C is not perfect. However, since $S(y_2) = 2(1, 0) + 3(0, 1)$, one possible error-vector of weight 2 is $(2, 3, 0, 0, 0)$ and we could decode to a nearest neighbour

$\mathbf{y}_2 - (2,3,0,0,0) = (4,4,1,0,0) \in C$. But there are many other possible error-vectors of weight 2, so many other nearest neighbours. Since $d(C) = 3$ (by Theorem 4.11.), a word can easily be at distance 2 from several codewords. △

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.)

S70 Multiplying the 2nd, 4th and 5th column of G_1 by 2 gives G_2, so they are equivalent. By Proposition 5.9, we can write down $\widehat{G_1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$ and $\widehat{G_2} = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}$. (You just have to make the rows add to 0.) Because every column in $\widehat{G_1}$ has one zero, one non-zero, it is easy to see what weights codewords of $\widehat{C_1}$ can have: any codeword in $\widehat{C_1}$ is $(a,b)\widehat{G_1}$, and these have weights 0, 3, and 6 as both, one, or neither of a and b are 0, respectively. Similarly, $\widehat{C_2}$ has words of weight 0, 2, 4, and 6. So $d(\widehat{C_1}) = 3$, $d(\widehat{C_2}) = 2$, and they are not equivalent. △

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.

S71 The punctured code have generator-matrices $G^{\{5\}} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}$ and $G^{\{p\}} = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 \end{pmatrix}$ respectively. Then $C^{\{5\}}$ has check-matrix $\begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 4 & 3 \end{pmatrix}$, and so $d(C^{\{5\}}) = 3$. For $C^{\{3\}}$ we row-reduce $G^{\{3\}}$ to $\begin{pmatrix} 1 & 0 & 4 & 4 \\ 0 & 1 & 2 & 2 \end{pmatrix}$, so $C^{\{3\}}$ has check-matrix $\begin{pmatrix} 1 & 3 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix}$, and $d(C^{\{3\}}) = 2$. So they cannot be 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 $(I|A)$.

S72 a) By the definition of an extended code, $\widehat{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$, (and since col.s 1,3, and 4 add to 0, $d(\widehat{C}) = 3$). By Proposition 4.5, since H is in form $(I \mid A)$, we have $G = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$. So by Proposition 5.9, $\widehat{C}$ has a generator matrix $\begin{pmatrix} 2 & 2 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 & 2 \end{pmatrix}$.

b) Applying EROs $P_{1,2}$ then $A_{2,1}(1)$ gives $\widehat{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 2 & 2 & 1 & 0 & 1 \end{pmatrix}$, which is also a generator matrix for $\widehat{C}$. We can then puncture this at each position:

$G_{p1} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$, so $H_{p1} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}$, and $d(C_{p1}) = 2$.

$G_{p2} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$, so $H_{p2} = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}$, and $d(C_{p2}) = 3$.

$G_{p3} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}$, so $H_{p3} = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, and $d(C_{p3}) = 2$.

$G_{p4} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 1 & 1 \end{pmatrix} \xrightarrow{A_{1,2}(2)} G'_{p4} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$, so $H_{p4} = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, and $d(C_{p4}) = 2$.

$G_{p5} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 2 & 1 & 0 \end{pmatrix} \xrightarrow{P_{1,2}} \begin{pmatrix} 2 & 2 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \xrightarrow{A_{1,2}(2)} \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$, $H_{p5} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$, $d(C_{p5}) = 3$.

Since all six check-matrices are in RREF, we know that we cannot turn one into another by row operations, so different matrices do give different codes. As they have the same check-matrix, $C_{p5} = C$, as we would expect; puncturing in the last position has reversed the extending process. Also, since multiplying col.4 of H_{p5} by 2 gives H_{p2}, C_2 is also equivalent to these (see Q59). Swapping col.s 1 and 2 of G_{p1} gives G'_{p4}, so C_1 and C_4 are equivalent. But even though it has the same $d(C)$, it seems that C_3 is not equivalent to these, as H_{p3} and H_{p4} match apart from their last columns which are not multiples of each other. (I don't think we have the theory to prove this rigorously!) △

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 $\widehat{C}$?

S73 a) $H = (-2 \;\; 1)$ and $G = (1 \;\; 2)$.

b) $\widehat{C} = \{\mathbf{x} \in \mathbb{R}^3 \mid \mathbf{x}\widehat{H}^t = 0\} = \{\lambda \widehat{G} \mid \lambda \in \mathbb{R}\}$, where $\widehat{H} = \begin{pmatrix} -2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ and $\widehat{G} = (1 \;\; 2 \;\; -3)$.

c) Deleting the last co-ordinate z projects $\widehat{C}$ back to C in the x-y plane. But deleting x or y gives different lines: $3y + 2z = 0$ in the y-z plane or $3x + z = 0$ in the x-z plane. (It all works very much like extending and puncturing a code over $\mathbb{F}_q$, except that over $\mathbb{R}$ there is no such thing as a minimum distance for 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.

S74 a) A code is perfect if we have equality in the Hamming bound, $M|S(c,t)| = q^n$. If $d = 5$, then we have $t = \lfloor \frac{d-1}{2} \rfloor = 2$, and so as in the proof of Proposition 1.15, spheres of radius 2 are disjoint. So, we now check whether these spheres cover the space (i.e. whether the Hamming bound is satisfied).

$$|S(c,t)| = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j = \sum_{j=0}^{2} \binom{90}{j} = 4096 = 2^{12}.$$

So in total, the spheres cover $2^{12}M$ words. But in a linear code $M = q^k$, so the spheres cover 2^{12+k} words. This code is therefore perfect if $2^{12+k} = 2^{90}$, which is true if $k = 78$.

b) Consider the words $(0, x_2, x_3, \ldots, x_n)$, $(1, x_2, x_3, \ldots, x_n)$. Clearly, if the first word has odd weight, the second word has even weight, and vice versa. Every word of $\mathbb{F}_2^r$ is of one of these two forms, and for each word of $\mathbb{F}_2^r$ with a zero in the first position, there is a word with a 1 in the first position (and vice versa), so the number of words of each form must be equal. Therefore half of the vectors of $\mathbb{F}_2^r$ have odd weight, which is a total of $\frac{1}{2}2^r = 2^{r-1}$ words.

c) Columns of H are of length $n - k = 12$, so $\mathbf{h}_i \in \mathbb{F}_2^{12}$ for $1 < i < 90$. If H is a check matrix for a code of minimum distance 5, then by Theorem 4.11, any 4 columns of H must be linearly independent. We therefore **cannot** have:

- $\mathbf{h}_i = 0$ – otherwise $d = 1$
- $\mathbf{h}_i = \mathbf{h}_j$ for $i \neq j$ – otherwise $d = 2$
- $\mathbf{h}_i = \mathbf{h}_j + \mathbf{h}_k$ for i, j, k distinct – otherwise $\mathbf{h}_i - \mathbf{h}_j - \mathbf{h}_k = \mathbf{0} \implies d = 3$
- $\mathbf{h}_i + \mathbf{h}_j = \mathbf{h}_k + \mathbf{h}_l$ for i, j, k, l distinct – otherwise $\mathbf{h}_i + \mathbf{h}_j - \mathbf{h}_k - \mathbf{h}_l = \mathbf{0} \implies d = 4$.

d) Let $X = \{\mathbf{0}\} \cup \{\mathbf{h}_i \mid 1 \leq i \leq 90\} \cup \{\mathbf{h}_i + \mathbf{h}_j \mid 1 \leq i < j \leq 90\}$. Since the three sets $\{\mathbf{0}\}$, $\{\mathbf{h}_i\}$, $\{\mathbf{h}_i + \mathbf{h}_j\}$ have no elements in common by part c), the size of X is therefore the sum of the sizes of these constituent sets. We therefore have $|X| = 1 + 90 + \binom{90}{2} = 4096 = 2^{12} = |\mathbb{F}_2^{12}$. So since $\mathbf{h}_i \in \mathbb{F}_2^{12}$, we have $X \subseteq \mathbb{F}_2^{12}$ and therefore $X = \mathbb{F}_2^{12}$.

e) If m of the $\mathbf{h}_i$ have odd weight, then $90 - m$ have even weight. By Lemma 5.16, $w(\mathbf{h}_i + \mathbf{h}_j) = w(\mathbf{h}_i) + w(\mathbf{h}_j) - 2w(\mathbf{h}_i \cap \mathbf{h}_j)$. We therefore have that $\mathbf{h}_i + \mathbf{h}_j$ has odd weight if one of $\mathbf{h}_i$ or $\mathbf{h}_j$ has odd weight and the other has even weight. There are then $m(90 - m)$ $\mathbf{h}_i + \mathbf{h}_j$ of odd weight, and therefore a total of $m + m(90 - m) = m(91 - m)$ vectors in X of odd weight. Now if m is even, then $91 - m$ is odd, and vice versa, so this is therefore an odd number times an even number. However, in part b) we showed that the number of odd weight vectors in $\mathbb{F}_2^{12}$ was 2^{11}, which certainly has no odd factors, and we therefore have a contradiction. Hence no such code can exist. $\triangle$

75 Prove Lemma 5.12.

S75 i) The positions where $\mathbf{x}$ and $\mathbf{y}$ both have 1 are counted twice in $w(\mathbf{x})+w(\mathbf{y})$, not at all in $w(\mathbf{x}+\mathbf{y})$.
ii), iii) Calculated in $\mathbb{Z}$, $\mathbf{x}\cdot\mathbf{y} = w(\mathbf{x}\cap\mathbf{y})$. △

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 $1 \le i < j \le 6$. (Again, there are only a few cases to consider.)
c) Show that if $\mathbf{c} \in \mathcal{G}_{12}, \mathbf{c} \ne \mathbf{0}$, then $w(\mathbf{c}) \ge 6$. 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.

S76 We write the rows of G as $\mathbf{g}_i = (\mathbf{e}_i, \mathbf{a}_i)$. a) We first show that $\mathcal{G}_{12} \subseteq \mathcal{G}_{12}^{\perp}$, by showing that $(\mathbf{e}_i, \mathbf{a}_i)\cdot G = 0$, or equivalently that $(\mathbf{e}_i, \mathbf{a}_i)\cdot(\mathbf{e}_j, \mathbf{a}_j) = 0$ for any $1 \le i \le j \le 6$.

Note that $(\mathbf{e}_i, \mathbf{a}_i).(\mathbf{e}_j, \mathbf{a}_j) = \mathbf{e}_i \cdot \mathbf{e}_j + \mathbf{a}_i \cdot \mathbf{a}_j$, that A is symmetric, and that the lower-right 5×5 submatrix of A is cyclic; each row is the one above with the entries permuted one place to the right. Now consider the following cases:

(1) If $i = j$, then $\mathbf{e}_i \cdot \mathbf{e}_i = 1$ and $\mathbf{a}_i \cdot \mathbf{a}_i = w(a_i) = 5$. Therefore $(\mathbf{e}_i, \mathbf{a}_i).(\mathbf{e}_i, \mathbf{a}_i) = 0 \in \mathbb{F}_3$ for all $1 \le i \le 6$.
(2) Consider $(\mathbf{e}_1, \mathbf{a}_1).(\mathbf{e}_j, \mathbf{a}_j)$ for $2 \le j \le 6$. We have $\mathbf{e}_1 \cdot \mathbf{e}_j = 0$. The first term of $\mathbf{a}_1 \cdot \mathbf{a}_j$ is zero, and the other terms which get summed in this product are always 0,1,2,2 and 1, in some order depending on the cyclic shift of $\mathbf{a}_j$. So again we have $(\mathbf{e}_1, \mathbf{a}_1).(\mathbf{e}_j, \mathbf{a}_j) = 0 \in \mathbb{F}_3$.
(3) Next, consider $(\mathbf{e}_2, \mathbf{a}_2).(\mathbf{e}_j, \mathbf{a}_j)$ for $3 \le j \le 6$. Again, the product $\mathbf{e}_2 \cdot \mathbf{e}_j = 0$. $\mathbf{a}_1 \cdot \mathbf{a}_j$ has two terms involving 0s, two terms where the entries of the $\mathbf{a}$ match and so contribute a 1, and two terms where the entries of the $\mathbf{a}$ differ and so contribute a 2. We therefore have $\mathbf{a}_1 \cdot \mathbf{a}_j = 0$ and hence $(\mathbf{e}_2, \mathbf{a}_2).(\mathbf{e}_j, \mathbf{a}_j) = 0 \in \mathbb{F}_3$.
(4) Finally, if we consider any two other rows of G, the $\mathbf{e}_i$ will also be orthogonal, and the $\mathbf{a}_i$ will be the same as a pair already consider up to a cyclic permutation, and hence we've already checked that the inner product will be 0.

We therefore see that all codewords in $\mathcal{G}_{12}$ are orthogonal to every other codeword of $\mathcal{G}_{12}$ by linearity, and hence $\mathcal{G}_{12} \subseteq \mathcal{G}_{12}^{\perp}$. Since we also have $\dim \mathcal{G}_{12}^{\perp} = 12 - 6 = 6 = \dim \mathcal{G}_{12}$, and hence $|\mathcal{G}_{12}| = |\mathcal{G}_{12}^{\perp}|$, we therefore have $\mathcal{G}_{12} = \mathcal{G}_{12}^{\perp}$.

Since $G = (I_6 \mid A)$ is a generator matrix for $\mathcal{G}_{12}$, $H = (-A^t \mid I_6) = (-A \mid I_6)$ is a check-matrix for $\mathcal{G}_{12}$, and hence a generator matrix for $\mathcal{G}_{12}$. But since $\mathcal{G}_{12} = \mathcal{G}_{12}^{\perp}$, this is also a generator matrix for $\mathcal{G}_{12}$. So the rows of B are $\mathbf{b}_i = -\mathbf{a}_i$.

b) For $i \ne j$, $\mathbf{a}_i \pm \mathbf{a}_j$ has two non-zero entries where $\mathbf{a}_i$ or $\mathbf{a}_j$, but not both, has a zero. In the other 4 positions, both $\mathbf{a}_i$ and $\mathbf{a}_j$ have non-zero entries, and they match in two positions and differ in two positions. We have that $\mathbf{a}_i + \mathbf{a}_j$ is non-zero where they match and zero where they differ, and vice versa for $\mathbf{a}_i - \mathbf{a}_j$. We therefore have $w(\mathbf{a}_i \pm \mathbf{a}_j) = 4$ for all $i \neq j$.

c) Consider $\mathbf{c} \in \mathcal{G}_{12}$, $\mathbf{c} \neq \mathbf{0}$, and suppose that $1 \leq w(c) \leq 5$. If we write $\mathbf{c}$ as $(\mathbf{l}, \mathbf{r})$, then we have $w(\mathbf{c}) = w(\mathbf{l}) + w(\mathbf{r})$, and hence we must have one of $\mathbf{l}$, $\mathbf{r}$ with weight either 1 or 2. If $w(\mathbf{l}) = 1$, then since $\mathbf{c}$ is a linear combination or rows of G, we must have $\mathbf{c} = (\mathbf{e}_i, \mathbf{a}_i)$ and so $w(\mathbf{c}) = 6$. If $w(\mathbf{r}) = 1$, then since $\mathbf{c}$ is a linear combination of rows of H, we must have that $\mathbf{c} = (-\mathbf{a}_i, \mathbf{e}_i)$ and so $w(\mathbf{r}) = 6$. If $w(\mathbf{l}) = 2$, then $\mathbf{c}$ is either the sum or difference of two rows of G, so $\mathbf{c} = \pm(\mathbf{e}_i, \mathbf{a}_i) \pm (\mathbf{e}_j, \mathbf{a}_j)$ with $i \neq j$, and so $w(\mathbf{c}) = 6$ using part b). If $w(\mathbf{r}) = 2$, then similarly $w(\mathbf{c}) = 6$, by considering the sum/difference of two rows of H. Hence there is no such $\mathbf{c} \in \mathcal{G}_{12}$ with $1 \leq w(\mathbf{c}) \leq 6$, and so all non-zero words must have weight ≥ 6.

d) Firstly, we see that $\mathcal{G}_{12}$ has block length 12, dimension 6. By part c) the minimum distance of $\mathcal{G}_{12}$ is ≥ 6, but since the rows of G have weight 6, then $\mathcal{G}_{12}$ certainly contains words of weight 6, and so $d(\mathcal{G}_{12}) = 6$. Hence $\mathcal{G}_{12}$ is a $[12, 6, 6]_3$ code.

We now puncture $\mathcal{G}_{12}$ in the last position to obtain $\mathcal{G}_{11}$. By Proposition 5.11, $\mathcal{G}_{11}$ has $n = 11$ and $k = 6$, and since $\mathcal{G}_{12}$ has a word of weight 6 with a non-zero entry in the final position (all but the last row of G for instance), we have $d(\mathcal{G}_{11}) = 5$, and so $\mathcal{G}_{11}$ is a $[11, 6, 5]_3$ code. Plugging these parameters into the Hamming bound shows that this code is perfect. $\triangle$

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?

S77 a) Clearly $\mathbf{a}_i$ and the right $w(\mathbf{a}_i)$ of the $\mathbf{e}_j$ from I_5 make a linearly dependent set of size $w(\mathbf{a}_i) + 1$. So we need all the $w(\mathbf{a}_i)$ to be ≥ 4; no more than one zero in any $\mathbf{a}_i$.
b) If $w(\mathbf{a}_i + \mathbf{a}_j)$ or $w(\mathbf{a}_i - \mathbf{a}_j)$ is ≤ 2, then $\mathbf{a}_i$ and $\mathbf{a}_j$ with at most two of the $\mathbf{e}_j$s would make a linearly dependent set of size 3 or 4, so we must avoid this.
c) Suppose we have $w(\mathbf{a}_i)$ and $w(\mathbf{a}_j) = 5$, with $\mathbf{a}_i = (x_1, \ldots, x_5)$ and $\mathbf{a}_j = (y_1, \ldots, y_5)$. The x_k and the y_k are either 1 or 2. For a given k, if they match, we have $x_k - y_k = 0,\ x_k + y_k \neq 0$; if they differ we have $x_k + y_k = 0,\ x_k - y_k \neq 0$. Thus $w(\mathbf{a}_i + \mathbf{a}_j) + w(\mathbf{a}_i - \mathbf{a}_j) = 5$. It follows that either $w(\mathbf{a}_i + \mathbf{a}_j)$ or $w(\mathbf{a}_i - \mathbf{a}_j) \leq 2$, which we must avoid. So there can be only one column of H with no zeros.
d) If $\mathbf{a}_i$ and $\mathbf{a}_j$ each have a single zero, in the same position, then arguing as for c) we have that $w(\mathbf{a}_i + \mathbf{a}_j) + w(\mathbf{a}_i - \mathbf{a}_j) = 4$. So again either $w(\mathbf{a}_i + \mathbf{a}_j)$ or $w(\mathbf{a}_i - \mathbf{a}_j) \leq 2$, which we must avoid.
e) Where $\mathbf{a}_j$ has a 2, $\mathbf{a}_1 + \mathbf{a}_j$ has a 0; where $\mathbf{a}_j$ has a 1, $\mathbf{a}_1 - \mathbf{a}_j$ has a 0. By b) we cannot have more than two 0s in either one. It follows that we must have two 1s and two 2s in $\mathbf{a}_j$.
f) So $w(\mathbf{a}_i + \mathbf{a}_j)$ and $w(\mathbf{a}_i - \mathbf{a}_j)$ are ≥ 2, but we still need $\mathbf{a}_i$ and $\mathbf{a}_j$ to differ in at least one other position, to make $w(\mathbf{a}_i - \mathbf{a}_j) \geq 3$, and match in at least one other position, to make $w(\mathbf{a}_i + \mathbf{a}_j) \geq 3$.
g) There are still many ways to do this. If we keep the last 5 columns symmetrical across both

diagonals, we can get

$$H = \begin{pmatrix} 1 & & & & & 1 & 1 & 1 & 2 & 2 & 0 \\ & 1 & & 0 & & 1 & 1 & 2 & 1 & 0 & 2 \\ & & 1 & & & 1 & 2 & 1 & 0 & 1 & 2 \\ & 0 & & 1 & & 1 & 2 & 0 & 1 & 2 & 1 \\ & & & & 1 & 1 & 0 & 2 & 2 & 1 & 1 \end{pmatrix},$$

h) For example, $2\mathbf{e}_1 + 2\mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{a}_7 = \mathbf{0}$.
i) a) rules out $n_a = 1$, b) rules out $n_a = 2$. It still seems possible that four $\mathbf{a}_j$, or three $\mathbf{a}_j$ and an $\mathbf{e}_i$, might be linearly dependent. There are only $\binom{6}{4} = 15$ and $\binom{6}{3} \times 5 = 100$ cases to check, respectively (and we might be able to cut this down further using symmetries...). △