******The following questions are concerned with Chapter 2 of the notes - Linear Codes.******

17 Write out an addition table and a multiplication table for $\mathbb{Z}/5$ and $\mathbb{Z}/6$. Use your tables to show that $\mathbb{Z}/6$ is not a field.

S17

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The last table shows that 2, 3 and 4 do not have multiplicative inverses in $\mathbb{Z}/6$, so it is not a field. △

18 Let $C = \{(0,0,2),(1,1,0),(2,2,1)\} \subseteq \mathbb{F}_3^3$. Is C a linear code? Find its span, $\langle C\rangle$, a ternary $[n,k,d]$ code. What are n, k, and d?

S18 C is not linear. There are many ways to check this; to start with, a linear code should contain $(0,0,0)$. We can add in all multiples of the given vectors to get $\{(0,0,2),(1,1,0),(2,2,1),(0,0,1),(2,2,0),(1,1,2),(0,0,0)\}$, and if we then take sums of these, we find that the new vectors we get are only $(1,1,1)$ and $(2,2,2)$. So $\langle C\rangle = \{(0,0,2),(1,1,0),(2,2,1),(0,0,1),(2,2,0),(1,1,2),(0,0,0),(1,1,1),(2,2,2)\}$. Clearly, $n = 3$ and $d = 1$. And $k = 2$, because $M = 3^k = 9$, or else because $\{(1,1,0),(0,0,1)\}$ is a basis. △

19 Show that a q-ary $[n,k,d]$ MDS code satisfies $d = n - k + 1$. Use this to check that the code $C = \{000, 111\} \subset \mathbb{F}_2^3$ is MDS.

S19 Recall that a code is MDS if it satisfies the Singleton bound, $M = q^{n-d+1}$. By Proposition 2.3, for a linear $[n,k,d]_q$ code, we have $M = q^k$, and hence the Singleton bound can be written as $q^k \leq q^{n-d+1}$. Since q is an integer greater than 1, this can be written as $k \leq n - d + 1$ or $d \leq n - k + 1$. An MDS code saturates the Singleton bound, and so satisfies $d = n - k + 1$.

The code C is a $[3,1,3]_2$ code, and so we have $n - k + 1 = 3 - 1 + 1 = 3 = d$, and hence C is MDS. △

20 Let $C = \langle\{(0,1,0,1,0),(1,0,1,1,0),(0,1,1,1,0),(1,0,0,1,0)\}\rangle \subseteq \mathbb{F}_2^5$. Find a basis for C, and its dimension.

S20 If we put these vectors as rows in a matrix, and row-reduce, then the RREF form is $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

So we remove the all-zero row, and the remaining rows form a basis, so the dimension is 3. (In terms of Ch 3, we have also found a generator-matrix for C.) △

21 Show that, for a prime p, the p-ary code $C = \{(0,1),(1,1),\ldots,(p-1,1)\} \subseteq F_p^2$, is a $(2,p,1)$ code but not a $[2,1,1]$ code.

S21 Block length is 2, $d(C) = 1, M = p$. But for no prime p is $\vec{0} \in C$, hence C is not linear. △

22 Show that, in a decoding array constructed according to the algorithm given, every possible received word $\mathbf{y} \in \mathbb{F}_q^n$ appears exactly once. (Hint: Show first that the same $\mathbf{y}$ cannot appear twice in the same row, and then that the same $\mathbf{y}$ cannot appear twice in *different* rows. (This contradiction argument is similar to the proof of Proposition 2.10.))

S22 The top row has each codeword just once, and the lefthand column (of errors) has no repeats by construction. So we now consider the main body of the array.

$\mathbf{0}$	$\mathbf{c}_1$	$\mathbf{c}_2$
$\mathbf{e}$	$\mathbf{y}$	$\mathbf{y}$

$\mathbf{0}$	$\mathbf{c}_2$	$\mathbf{c}_1$
$\mathbf{e}_1$		$\mathbf{y}$
$\mathbf{e}_2$	$\mathbf{y}$	

If $\mathbf{y}$ appears twice in the same row (first picture), then $\mathbf{y} = \mathbf{e} + \mathbf{c}_1 = \mathbf{e} + \mathbf{c}_2$. So $\mathbf{c}_1 = \mathbf{c}_2$, and in fact $\mathbf{y}$ only appears once. If $\mathbf{y}$ appears twice in the different rows (second picture), we have $\mathbf{e}_2 + \mathbf{c}_2 = \mathbf{e}_1 + \mathbf{c}_1$. WLOG assume $\mathbf{e}_1$ is above $\mathbf{e}_2$. Then $\mathbf{e}_2 = \mathbf{e}_1 + \mathbf{c}_1 - \mathbf{c}_2$. But then, as $\mathbf{c}_1 - \mathbf{c}_2 \in C$, $\mathbf{e}_2$ is in $\mathbf{e}_1$'s row, and was not available to be chosen for the first column. Contradiction. So no word is repeated in the table. But we have q^{n-k} rows, each with q^k entries, so q^n distinct words in all. These are all of $\mathbb{F}_q^n$. △

23 Make a decoding array for the code $C_2 = \{(0,0,0),(1,1,1)\} \subseteq \mathbb{F}_2^3$. If C_2 is transmitted over a symmetric binary channel with symbol-error probability p, use Proposition 2.11 to find the probability that a codeword $\mathbf{c} \in C_2$ will be successfully decoded.

S23 Firstly, note that C_2 is a binary $[3,1,3]$ code. We therefore know that the completed array should contain $q^{n-k} = 4$ rows, and by following the algorithm we can obtain the following array:

$(0,0,0)$	$(1,1,1)$
$(0,0,1)$	$(1,1,0)$
$(1,0,0)$	$(0,1,1)$
$(0,1,0)$	$(1,0,1)$

For this question, this array is fixed up to permutations of the bottom 3 rows.

If a codeword of C_2 is sent over a ternary symmetric channel with symbol-error probability p, we will decode the received word correctly if the error which occurs in transmission is one of the 4 words in the leftmost column of our array. Since there is one word of weight 0 and 3 words of weight 1 in this column we have $\alpha_0 = 1$, $\alpha_1 = 3$, $\alpha_2 = 0$ and $\alpha_3 = 0$, so by Proposition 2.11 the probability that we decode correctly is

$$\begin{aligned}\mathbb{P}(c \text{ decoded correctl}) &= \sum_{i=0}^{n} \alpha_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i} \\ &= \sum_{i=0}^{3} \alpha_i (p)^i (1-p)^{3-i} \\ &= (1-p)^3 + 3p(1-p)^2\end{aligned}$$

△

24 Make a decoding array for the code $C_3 = \{(0,0,0),(1,1,1),(2,2,2)\} \subseteq \mathbb{F}_3^3$. Use it to decode the words $(1,2,1)$ and $(1,2,0)$. If C_3 is transmitted over a symmetric ternary channel with symbol-error probability p, use Proposition 2.11 to find the probability that a codeword $c \in C_3$ will be successfully decoded.

S24

$(0,0,0)$	$(1,1,1)$	$(2,2,2)$
$(0,0,1)$	$(1,1,2)$	$(2,2,0)$
$(0,0,2)$	$(1,1,0)$	$(2,2,1)$
$(0,1,0)$	$(1,2,1)$	$(2,0,2)$
$(0,2,0)$	$(1,0,1)$	$(2,1,2)$
$(1,0,0)$	$(2,1,1)$	$(0,2,2)$
$(2,0,0)$	$(0,1,1)$	$(1,2,2)$
$(1,2,0)$	$(2,0,1)$	$(0,1,2)$
$(0,2,1)$	$(1,0,2)$	$(2,1,0)$

We decode $(1,2,1)$ and $(1,2,0)$ to $(1,1,1)$ and $(0,0,0)$ respectively: the codeword at the top of its column. Our decoding is successful if and only if the error that occurred is one of those in the first column (including $(0,0,0)$). The probability of one of these errors occurring is $(1-p)^3 + 6\frac{p}{2}(1-p)^2 + 2(\frac{p}{2})^2(1-p)$. (This is also given by Proposition 2.11, with $\alpha_0 = 1$ (as always!), $\alpha_1 = 6$, $\alpha_2 = 2$.) △

25 In making your array for Q24, when did you have to make arbitrary choices? Which of these choices will affect decoding? Which words may be decoded differently by different arrays? Explain by considering a different (but still correct!) array for C_3. Is the situation the same for C_2 of Q23?

S25 Call the words in the first column the "errors". The six errors of weight 1 could have been chosen in any order, but this would have only re-ordered the rows, and not changed any decoding. Then for the eighth error, there are six words of weight 2 to chose from (all the words using 0 and 1 and 2), and for the last error, the remaining three of these. For example, we could have

$(0,0,0)$	$(1,1,1)$	$(2,2,2)$
$\vdots$	$\vdots$	$\vdots$
$(1,0,2)$	$(2,1,0)$	$(0,2,1)$
$(2,0,1)$	$(0,1,2)$	$(1,2,0)$

This array decode $(1,2,1)$ and $(1,2,0)$ to $(1,1,1)$ and $(2,2,2)$ respectively. The decoding did not change for $(1,2,1)$ which (probably) suffered only one symbol-error. But it did change for $(1,2,0)$ which must have suffered two.

For C_2 in Q24, the errors are exactly the words of weight ≤ 1. So different arrays can only have re-ordered rows, and will all decode identically. △

26 Suppose we have a decoding array for a q-ary $[n,k,2t+1]$ code C (t any integer). For $\mathbf{c} \in C$ and $r \leq t$, where in the array would we find the the words of the sphere $S(\mathbf{c},r)$? (Look at Q25, and/or draw a general, schematic array).

S26 These words are of the form $\mathbf{c}+\mathbf{e}$, with $w(\mathbf{e}) \leq r$. And since $r \leq t$, they are not in any other $S(\mathbf{c}',r)$. They will be found in a top part of the column headed by $\mathbf{c}$, from $\mathbf{c}$ itself at the top, down to the last row which starts with an error of weight r. △

27 In terms of the definition of a perfect code ("there is some t such that...."), what words are in the first column of a decoding array for a perfect code? Explain why, for perfect codes, all arrays will decode identically.

S27 If the code is perfect, the spheres $S(\mathbf{c},t)$ partition $\mathbb{F}_q^n$. So the errors for the array are exactly the words of weight $\leq t$ (- which are the words in $S(\mathbf{0},t)$). Our only choices are in the order of these, which does not affect decoding. △