******The following questions are concerned with Chapter 3 of the notes - Codes as Images.******

28 Let code $C_5 \subseteq \mathbb{F}_5^4$ be the span of the set $\{(0,1,2,3),(1,1,1,1),(3,1,4,2)\}$. Find a generator-matrix for C_5. What is the dimension of C_5?

S28 We make a matrix with these vectors and row-reduce in $\mathbb{F}_5$:

$$\begin{pmatrix}1&1&1&1\\0&1&2&3\\0&3&1&4\end{pmatrix} \xrightarrow{A_{1,3}(2)} \begin{pmatrix}1&1&1&1\\0&1&2&3\\0&3&1&4\end{pmatrix} \xrightarrow{A_{2,1}(4),A_{2,3}(2)} \begin{pmatrix}1&0&4&3\\0&1&2&3\\0&0&0&0\end{pmatrix}.$$

So we remove the all-zero row, to get $G = \begin{pmatrix}1&0&4&3\\0&1&2&3\end{pmatrix}$, and $\dim(C_5) = 2$. △

29 Let code $C_7 \subseteq \mathbb{F}_7^4$ be the span of the set $\{(0,1,2,3),(1,1,1,1),(3,1,4,2)\}$. Find a generator-matrix for C_7. What is the dimension of C_7? (- so, identical to the previous question, except that we are over a different field.)

S29 Over $\mathbb{F}_7$, $\begin{pmatrix}1&1&1&1\\0&1&2&3\\0&3&1&4\end{pmatrix} \xrightarrow{A_{1,3}(4)} \begin{pmatrix}1&1&1&1\\0&1&2&3\\0&5&1&6\end{pmatrix} \xrightarrow{A_{2,1}(6),A_{2,3}(2)} \begin{pmatrix}1&0&6&5\\0&1&2&3\\0&0&5&5\end{pmatrix}$

$\xrightarrow{M_3(3)} \begin{pmatrix}1&0&6&6\\0&1&2&3\\0&0&1&1\end{pmatrix} \xrightarrow{A_{3,1}(1),A_{3,2}(5)} \begin{pmatrix}1&0&0&5\\0&1&0&1\\0&0&1&1\end{pmatrix} = G$, so $\dim(C_7) = 3$. △

30 For each of the codes above, C_5 and C_7, write down an alternative generator-matrix.

S30 If two matrices are related by EROs, they generate the same code. So, for C_7, any of the matrices in the row-reduction is also a generator-matrix. For C_5 we could do $A_{1,2}(1)$ to G, to get $\begin{pmatrix}1&0&4&3\\1&1&1&1\end{pmatrix}$. △

31 a) Draw 49 points in a square grid, to represent $\mathbb{F}_7^2$. (You could label just the "axes", $S((0,0),1)$). Find the points corresponding to the code C with generator-matrix $(2\ 1)$. Does it look like a "line" in a "plane"? Can you think of a better way to draw (or model?) these vector spaces?
b) Perhaps on a new grid, draw the code C' with generator-matrix $(1\ 3)$. Can you see two different ways to draw the "line"? Is one better than the other?

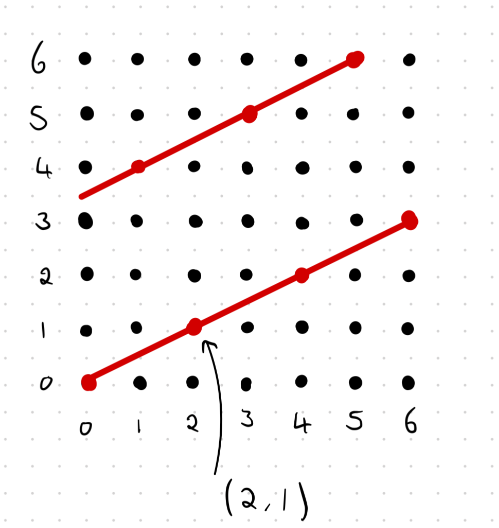

FIGURE 1. The 49 points of $\mathbb{F}_7^2$ in the plane, with the points corresponding to the code $C = \langle\{(2,1)\}\rangle$ drawn in red and joined by a line.

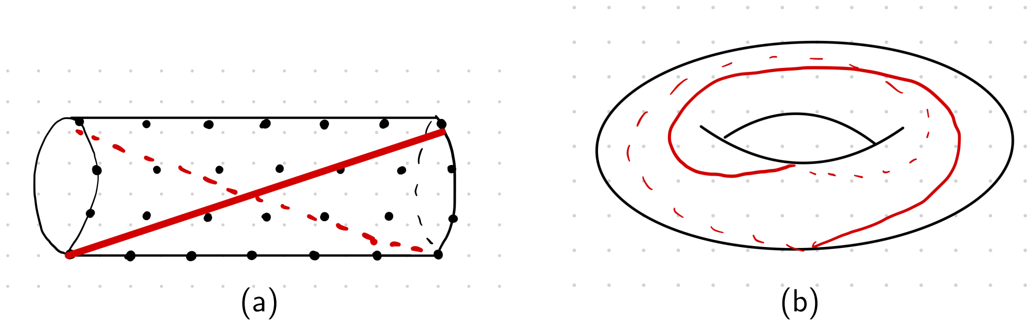

FIGURE 2. The points of $\mathbb{F}_7^2$ drawn on (a) a cylinder, and (b) a torus.

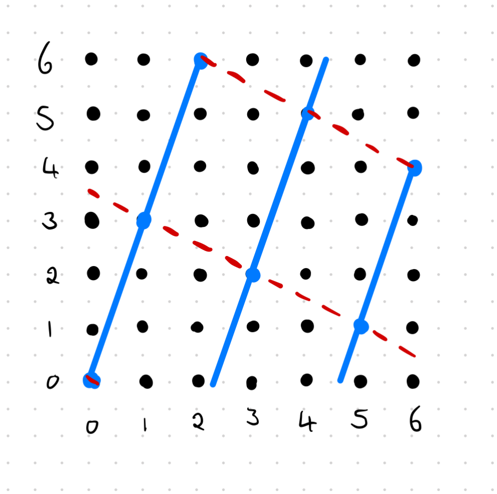

FIGURE 3. The 49 points of $\mathbb{F}_7^2$ in the plane, with the points corresponding to the code $C = \langle\{(1,3)\}\rangle$ drawn in blue and joined with 2 'different' lines, one in blue and one dashed red.

S31 a) The situation is shown in Figure 1. The code does look like a line in the plane, but we should note that, i) the code consists of only the 7 points highlighted (there is nothing 'in between' the points), ii) the 'line' is made up of 2 disjoint sections.

We could perhaps improve this picture, by first rolling the plane into a cylinder, as show in Figure 2(a), and then joining the ends of the cylinder to form a torus as shown in Figure 2(b). On the torus, where again we should remember that $\mathbb{F}_7^2$ consists of only a discrete set of 49 points, the line now becomes a continuous cycle.

b) This time, the situation is as shown in Figure 3. The blue line shows the points joined 'in order' as multiples of $(1, 3)$. However, drawn in this way, each codeword looks to have 'closer' codewords, and the line joining each codeword to this 'closest' codeword is shown in dashed red. This notion of 'closer' is Euclidian though, and so is irrelevant to the code, which measures distance using the Hamming distance - with this measure, each codeword is distance exactly 2 from each other codeword. The red line is generated by $(2, -1)$, but over $\mathbb{F}_7$, this is the same as $(2, 6) = 2(1, 3)$. △

32 The code $C \subseteq \mathbb{F}_7^5$ has generator matrix $G_1 = \begin{pmatrix} 1 & 2 & 3 & 3 & 3 \\ 0 & 2 & 1 & 5 & 5 \\ 4 & 5 & 0 & 6 & 3 \end{pmatrix}$.

Use this to encode the message $(3, 2, 1) \in \mathbb{F}_7^3$ to a codeword $\mathbf{c}$. Also, channel-decode codeword $\mathbf{c}' = (4, 5, 0, 0, 2)$ to find the corresponding message. (You will need to solve a set of five equations - possibly by row-reducing a suitable augmented matrix.)

S32 We encode $(3, 2, 1)$ to $\mathbf{c} = (3, 2, 1)G_1 = (0, 1, 4, 4, 1)$. To channel decode (4,5,0,0,2) we must solve $\mathbf{x}G_1 = (4, 5, 0, 0, 2)$, or, taking transposes, $G_1^t(x_1, x_2, x_3)^t = (4, 5, 0, 0, 2)^t$. So we row-reduce the augmented matrix $\begin{pmatrix} 1 & 0 & 4 & | & 4 \\ 2 & 2 & 5 & | & 5 \\ 3 & 1 & 0 & | & 0 \\ 3 & 5 & 6 & | & 0 \\ 3 & 5 & 3 & | & 2 \end{pmatrix}$, losing two all-zero rows , to get $\begin{pmatrix} 1 & 0 & 0 & | & 2 \\ 0 & 1 & 0 & | & 1 \\ 0 & 0 & 1 & | & 4 \end{pmatrix}$. So $\mathbf{x} = (2, 1, 4)$. △

33 For the code C of Q32, find an alternative generator-matrix, G_2, in RREF. Use this to encode the message $(3, 2, 1)$. Also, use G_2 to channel-decode the codeword $(2, 1, 1, 4, 0)$.

S33 We first need to row reduce over $\mathbb{F}_7$ to put G_1 into RREF. We find

$$\begin{pmatrix}1&2&3&3&3\\0&2&1&5&5\\4&5&0&6&3\end{pmatrix} \xrightarrow{A_{1,3}(3)} \begin{pmatrix}1&2&3&3&3\\0&2&1&5&5\\0&4&2&1&5\end{pmatrix} \xrightarrow[A_{2,3}(5)]{A_{2,1}(6)} \begin{pmatrix}1&0&2&5&5\\0&2&1&5&5\\0&0&0&5&2\end{pmatrix}$$

$$\xrightarrow[M_3(3)]{M_2(4)} \begin{pmatrix}1&0&2&5&5\\0&1&4&6&6\\0&0&0&1&6\end{pmatrix} \xrightarrow[A_{3,2}(1)]{A_{3,1}(2)} \begin{pmatrix}1&0&2&0&3\\0&1&4&0&5\\0&0&0&1&6\end{pmatrix} = G_2$$

Now we can encode $(3,2,1)$ as $(3,2,1)G_2$.

$$(3,2,1)\begin{pmatrix}1&0&2&0&3\\0&1&4&0&5\\0&0&0&1&6\end{pmatrix} = (3,2,0,1,4).$$

We can also decode $(2,1,1,4,0)$ just by looking at positions $1,2$ and 4. Explicitly, we have

$$(2,1,4)\begin{pmatrix}1&0&2&0&3\\0&1&4&0&5\\0&0&0&1&6\end{pmatrix} = (2,1,1,4,0),$$

so $(2,1,1,4,0)$ should be decoded as $(2,1,4)$.

△

34 There is a code C' which is permutation equivalent to code C of Q32 but has a generator matrix G_3 in standard form. Use this matrix to encode $(3,2,1)$ to a codeword of C', and channel-decode the codeword $(2,1,4,1,0)$.

S34 C' has generator matrix

$$G_3 = \begin{pmatrix}1&0&0&2&3\\0&1&0&4&5\\0&0&1&0&6\end{pmatrix},$$

found by applying the permutation $(3\ 4)$ to G_2. Then

$$(3,2,1)\begin{pmatrix}1&0&0&2&3\\0&1&0&4&5\\0&0&1&0&6\end{pmatrix} = (3,2,1,0,4),$$

and if $\mathbf{x}G_3 = (2,1,4,1,0)$, then $\mathbf{x} = (2,1,4)$. △

35 Equivalent codes have the same rank, redundancy and rate. Find these values for C' and C above.

S35 rank $= k = 3$, redundancy $= n-k = 5-3 = 2$, rate $= k/n = 0.6$. △

36 Let C be an (n,M,d) over an alphabet of order q, not necessarily linear. If C_2 is equivalent to C_1, show that C_2 is also an (n,M,d) code over an alphabet of order q.

S36 If two q-ary codes, not necessarily linear, are *equivalent*, then we can transform one to the other by permuting the n positions of all codewords simultaneously, and by permuting the q symbols in a given position in all codewords simultaneously. Clearly neither kind of transformation changes the block length of codes. Now by considering two codewords $\mathbf{c}_1,\ \mathbf{c}_2\ \in C_1$, we see that changing the order of the positions of the codewords, and permuting the symbols in a given position, can't change the total number of positions in which the two codewords agree. So all distances between codewords are preserved between equivalent codes, and hence the minimum distance is preserved. But also, if the distances between words is fixed, two different words in C_1 cannot become the same word in C_2, and so the total number of codewords is fixed. $\triangle$

37 The codes C_1 and C_2 in $\mathbb{F}_5^6$ have generator-matrices G_1 and G_2 respectively, where

$$G_1 = \begin{pmatrix} 0 & 3 & 1 & 0 & 3 & 1 \\ 1 & 4 & 0 & 2 & 3 & 4 \\ 2 & 0 & 3 & 4 & 3 & 0 \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} 3 & 1 & 4 & 1 & 0 & 0 \\ 4 & 4 & 0 & 1 & 4 & 1 \\ 0 & 0 & 2 & 1 & 3 & 2 \end{pmatrix}.$$

Show that C_1 and C_2 are monomially equivalent.

S37 We have

$$G_1 = \begin{pmatrix} 0 & 3 & 1 & 0 & 3 & 1 \\ 1 & 4 & 0 & 2 & 3 & 4 \\ 2 & 0 & 3 & 4 & 3 & 0 \end{pmatrix} \xrightarrow[(2\ 1\ 6)(4\ 5)]{\text{Apply}} \begin{pmatrix} 3 & 1 & 1 & 3 & 0 & 0 \\ 4 & 4 & 0 & 3 & 2 & 1 \\ 0 & 0 & 3 & 3 & 4 & 2 \end{pmatrix} \xrightarrow[\substack{\text{3 by 4} \\ \text{4 by 2} \\ \text{5 by 2}}]{\text{Multiply Cols:}} \begin{pmatrix} 3 & 1 & 4 & 1 & 0 & 0 \\ 4 & 4 & 0 & 1 & 4 & 1 \\ 0 & 0 & 2 & 1 & 3 & 2 \end{pmatrix} = G_2.$$

So the two generators are related by a monomial transformation, and hence C_1 and C_2 are monomially equivalent.

The relevant monomial matrix here can easily be check to be

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

so that $G_1 M = G_2$. $\triangle$

38 Given a code $C \subseteq \mathbb{F}_q^n$, prove that $\mathrm{PAut}(C)$ is a group.

S38 In order to be a group, the set $\mathrm{PAut}(C)$ must: i) Be closed under composition of permutations; ii) Contain an identity permutation; iii) Have an inverse permutation $\rho^{-1} \in \mathrm{PAut}(C)$ for each $\rho \in \mathrm{PAut}(C)$; iv) Satisfy the associativity property $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in \mathrm{PAut}(C)$. Since we know (from Linear Algebra I or elsewhere) that the set of all permutations on n objects form a group (the Symmetric group, S_n), we are really trying to show that $\mathrm{PAut}(C)$ is a subgroup of S_n.

Since S_n is a group, and hence satisfies associativity, the subset $\mathrm{PAut}(C)$ must also be associative. We therefore just need to check that the subset is *closed*, the identity permutation (which must exist, since S_n is a group) is in $\mathrm{PAut}(C)$, and for each $\rho \in \mathrm{PAut}(C)$, the inverse (which must exist, since S_n is a group) $\rho^{-1} \in \mathrm{PAut}(C)$.

If $\rho, \sigma \in \mathrm{PAut}(C)$, then $\rho(C) = C = \sigma(C)$ by definition of the permutation automorphism group (and where $\rho(C)$ indicates the action of ρ on C). Hence $(\rho \circ \sigma)(C) = \rho(\sigma(C)) = \rho(C) = C$, and so $(\rho \circ \sigma) \in \mathrm{PAut}(C)$ and so $\mathrm{PAut}(C)$ is closed under composition.

Clearly the identity permutation e satisfies $e(C) = C$ (trivially), and so $e \in \mathrm{PAut}(C)$ and so $\mathrm{PAut}(C)$ has an identity (which automatically satisfies $e \circ \rho = \rho \circ e = \rho \quad \forall \rho \in \mathrm{PAut}(C)$ since e is the identity of S_n).

Finally, given $\rho \in \mathrm{PAut}(C)$, since $\rho^{-1} \circ \rho = e$ we have $C = e(C) = (\rho^{-1} \circ \rho)(C) = \rho^{-1}(\rho(C)) = \rho^{-1}(C)$. Hence $\rho^{-1}(C) = C$ and so for all $\rho \in \mathrm{PAut}(C)$, we have $\rho^{-1} \in \mathrm{PAut}(C)$.

We have therefore shown that $\mathrm{PAut}(C)$ is a group.

△

39 Let $C \subseteq \mathbb{F}_3^4$ be the code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

Let $g = (134) \in S_4$. Show that $g \in \mathrm{PAut}(C)$.

S39 We have

$$g(G) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{pmatrix},$$

and so $g \in \mathrm{PAut}(C)$ if $g(G)$ generates the same code C that G generates. Note that G is in RREF, and the RREF form of a generator matrix is unique, so we can put $g(G)$ into RREF and see if this gives us back G. If so $g(G)$ generates the same code as G, since elementary row operations don't change the image of the associated linear map.

$$g(G) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{A_{12}(1)} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} = G,$$

so $g(G)$ is another generator matrix for C and hence $g \in \mathrm{PAut}(C)$ △

40 Consider two maps $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$. Map $\pi_{s(i,j)}$ swaps the i^{th} and j^{th} entry of each vector, and map $\pi_{m(i,\mu)}$ multiplies the i^{th} entry by $\mu \in \mathbb{F}_q$. Show that for each of these maps, and for any $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ and $\lambda \in \mathbb{F}_q$, we have $\pi(\mathbf{x} + \mathbf{y}) = \pi(\mathbf{x}) + \pi(\mathbf{y})$, and $\pi(\lambda \mathbf{x}) = \lambda \pi(\mathbf{x})$. For this reason we say that these maps "preserve linear structure".

S40 Let $\mathbf{x} = (x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_i, \ldots, y_j, \ldots, y_n)$. Then

$$\begin{aligned}
\pi_{s(i,j)}(\mathbf{x}+\mathbf{y}) &= \pi_{s(i,j)}(x_1+y_1, \ldots, x_i+y_i, \ldots, x_j+y_j, \ldots, x_n+y_n) \\
&= (x_1+y_1, \ldots, x_j+y_j, \ldots, x_i+y_i, \ldots, x_n+y_n) \\
&= (x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) + (y_1, \ldots, y_j, \ldots, y_i, \ldots, y_n) \\
&= \pi_{s(i,j)}(\mathbf{x}) + \pi_{s(i,j)}(\mathbf{y}) \ ; \\
\pi_{s(i,j)}(\lambda\mathbf{x}) &= \pi_{s(i,j)}(\lambda x_1, \ldots, \lambda x_i, \ldots, \lambda x_j, \ldots, \lambda x_n) \\
&= (\lambda x_1, \ldots, \lambda x_j, \ldots, \lambda x_i, \ldots, \lambda x_n) \\
&= \lambda(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = \lambda\pi_{s(i,j)}(\mathbf{x}) \ ; \\
\pi_{m(i,\mu)}(\mathbf{x}+\mathbf{y}) &= \pi_{m(i,\mu)}(x_1+y_1, \ldots, x_i+y_i, \ldots, x_n+y_n) \\
&= (x_1+y_1, \ldots, \mu(x_i+y_i), \ldots x_n+y_n) \\
&= (x_1, \ldots, \mu x_i, \ldots, x_n) + (y_1, \ldots, \mu y_i, \ldots, y_n) \\
&= \pi_{m(i,\mu)}(\mathbf{x}) + \pi_{m(i,\mu)}(\mathbf{y}) \ ; \\
\pi_{m(i,\mu)}(\lambda\mathbf{x}) &= \pi_{m(i,\mu)}(\lambda x_1, \ldots, \lambda x_i, \ldots, \lambda x_n) \\
&= (\lambda x_1, \ldots, \mu\lambda x_i, \ldots, \lambda x_n) \\
&= \lambda(x_1, \ldots, \mu x_i, \ldots, x_n) = \lambda\pi_{m(i,\mu)}(\mathbf{x}) \ .
\end{aligned}$$

△

41 Suppose an $[n, k, d]$ code C has a generator-matrix G in RREF. By considering the weights of the rows of G, find a new proof that $d \leq n - k + 1$ (the Singleton bound for linear codes).

S41 Being in RREF, G has k leading 1s, in k columns. So each row has a leading 1 and $k - 1$ zeros, in these columns (though it could also have more zeros). Thus the weight of each row is at most $n - (k - 1)$. Since the rows are codewords, $d(C) \leq \min\{w(\mathbf{c}) \mid \mathbf{c} \in C\} \leq n - k + 1$. △

42 We know that any generator-matrix for a code C can be row-reduced to a generator-matrix G in RREF, and that this RREF generator-matrix is unique. Thus, if C does have a generator-matrix in standard form $(I \mid A)$, it will be this matrix G. Again by considering weights of rows, show that if C is maximum distance separable then it has a generator-matrix in standard form. (Hint: Prove the contrapositive.)

S42 A code is MDS iff it has $d = n - k + 1$. We shall prove the contrapositive: that if C's RREF generator matrix is *not* of form $G = (I \mid A)$, then it has $d < n - k + 1$. If $G \neq (I \mid A)$ then the kth (last) leading 1 is in column $j > k$. In the last row, before this 1, we have $j - 1$ zeros. So $w(\text{last row}) \leq n - (j - 1) \leq n - k$, since $j - 1 \geq k$. But rows of G are codewords, so $d(C) \leq n - k < n - k + 1$. △

43 Show (by example or argument) that the converse of Q42,
"If C has a generator-matrix in standard form then it is MDS."
is false.

S43 *By example*: Let C have generator-matrix $G = (I \mid A) = \begin{pmatrix} 1 & 0 & 0 & 5 & 6 \\ 0 & 1 & 0 & 3 & 4 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix}$. Since the last row has weight 2, $d(C) \leq 2$. But $n - k + 1 = 5 - 3 + 1 = 3$.

By argument: Suppose the $[n, k, d]$-code C has generator-matrix G in RREF, but G is not of form $(I \mid A)$. Then by Q40, $d < n - k + 1$. By Proposition 3.13 there is a monomially equivalent code C' with generator-matrix $G' = (I \mid A)$, and parameters $[n', k', d']$. But monomially equivalent codes have the same parameters, so $d' = d < n - k + 1 = n' - k' + 1$, so C' is a counter-example. (There will be extra zeros in A, as above.) △