******The following questions are concerned with Chapter 4 of the notes - Codes as Kernels.******

44 Let $C \subseteq \mathbb{F}_5^6$ have generator-matrix $G = \begin{pmatrix} 1 & 4 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 & 2 \end{pmatrix}$. Find a basis for its dual code $C^\perp$.

S44 Using the algorithm, we note that G has a leading 1 in columns 1 and 4, so our basis is $\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_6\}$. We construct these vectors in two stages, *:

$$\mathbf{v}_2 = (\ \ , 1, 0, \ \ , 0, 0) \quad \mathbf{v}_3 = (\ \ , 0, 1, \ \ , 0, 0) \quad \mathbf{v}_5 = (\ \ , 0, 0, \ \ , 1, 0) \quad \mathbf{v}_6 = (\ \ , 0, 0, \ \ , 0, 1)$$

Then step **:

$$\mathbf{v}_2 = (1, 1, 0, 0, 0, 0) \quad \mathbf{v}_3 = (3, 0, 1, 0, 0, 0) \quad \mathbf{v}_5 = (2, 0, 0, 1, 1, 0) \quad \mathbf{v}_6 = (4, 0, 0, 3, 0, 1).$$

△

45 Let $C \subseteq \mathbb{F}_7^6$ have generator-matrix $G = \begin{pmatrix} 2 & 1 & 2 & 1 & 1 & 2 \\ 3 & 0 & 6 & 0 & 3 & 4 \\ 0 & 1 & 5 & 5 & 0 & 1 \end{pmatrix}$. Find a generator-matrix for $C^\perp$.

S45 Row-reduce G to $\begin{pmatrix} 1 & 0 & 2 & 0 & 1 & 6 \\ 0 & 1 & 5 & 0 & 4 & 3 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{pmatrix}$. Then for the algorithm $L = \{1, 2, 4\}$, so we make vectors $\mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_6$ as above, and put them as rows in the matrix $H = \begin{pmatrix} 5 & 2 & 1 & 0 & 0 & 0 \\ 6 & 3 & 0 & 5 & 1 & 0 \\ 1 & 4 & 0 & 6 & 0 & 1 \end{pmatrix}$ △

46 Let $C \subseteq \mathbb{F}_3^5$ have generator-matrix $G = \begin{pmatrix} 0 & 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 2 & 1 \end{pmatrix}$. Using the $G \leftrightarrow H$ algorithm, find a generator-matrix for $C^\perp$. Could you have used Proposition 4.5? Would you have got the same answer?

S46 To use the $G \leftrightarrow H$ algorithm, we first need to put G into RREF. Row reducing gives

$$\begin{pmatrix}0&1&2&2&0\\1&1&0&2&0\\2&0&1&2&1\end{pmatrix} \xrightarrow{P_{12}} \begin{pmatrix}1&1&0&2&0\\0&1&2&2&0\\2&0&1&2&1\end{pmatrix} \xrightarrow{A_{13}(1)} \begin{pmatrix}1&1&0&2&0\\0&1&2&2&0\\0&1&1&1&1\end{pmatrix}$$
$$\xrightarrow[A_{23}(2)]{A_{21}(2)} \begin{pmatrix}1&0&1&0&0\\0&1&2&2&0\\0&0&2&2&1\end{pmatrix} \xrightarrow{M_3(2)} \begin{pmatrix}1&0&1&0&0\\0&1&2&2&0\\0&0&1&1&2\end{pmatrix} \xrightarrow[A_{32}(1)]{A_{31}(2)} \begin{pmatrix}1&0&0&2&1\\0&1&0&0&2\\0&0&1&1&2\end{pmatrix} = H',$$

which is a check-matrix for $C^{\perp}$. We now apply the algorithm to find a generator matrix for $C^{\perp}$. We have $L = \{1,2,3\}$, so we need vectors $\vec{v}_4, \vec{v}_5$. Following the algorithm, these are given by

$$\mathbf{v}_4 = (1,0,2,1,0)$$
$$\mathbf{v}_5 = (2,1,1,0,1),$$

and so a generator matrix for $C^{\perp}$ is

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

Since H' is in standard form, $H' = (I \mid A)$, by Proposition 4.5 a generator matrix is also given by $(-A^t \mid I)$. This gives the same generator matrix G' as found above. △

47 Prove the following (which we might call Proposition 4.5 a):
If $C \subseteq \mathbb{F}_q^n$ has generator-matrix $G = (A \mid I_k)$, then it has a check-matrix $H = (I_{n-k} | -A^t)$. (*Hint:* Consider the code C' which has generator-matrix $H = (I_{n-k} | -A^t)$, and use Propositions 4.5 and 4.7.)

S47 By Proposition 4.5, if C' has generator-matrix $H = (I_{n-k} | -A^t)$, then $(C')^{\perp}$ has generator-matrix $(-(-A^t)^t \mid I_{n-(n-k)}) = (A \mid I_k)$. So in fact $(C')^{\perp} = C$, so $C' = C^{\perp}$. Then by Proposition 4.7, the generator-matrix for $C^{\perp}$ is a check-matrix for C.

△

48 A code is a subspace of a vector space. The first example of this you ever met was lines through the origin in $\mathbb{R}^2$, which can be written as $ax + by = 0$. Later you learned that such a line could also be given as any multiple of some vector, $\lambda\binom{c}{d}$.
a) Explain how these two ways correspond to specifying a code using either a generator- or a check-matrix.
b) Give two ways to specify a line through $(0,0,0)$ in $\mathbb{R}^3$, and explain how these also correspond to generator and check-matrices.
c) What about planes in $\mathbb{R}^3$?

S48 a) The line $ax+by=0$ is $\{\mathbf{x}\in\mathbb{R}^2 \mid \mathbf{x}H^t=\mathbf{0}\}$, with $H=\begin{pmatrix}a & b\end{pmatrix}$. The line $\lambda\binom{c}{d}$ is $\{\mathbf{x}G \mid \mathbf{x}\in\mathbb{R}\}$, with $G=\begin{pmatrix}c & d\end{pmatrix}$.

b) A line in $\mathbb{R}^3$ through the origin in direction (d,e,f) is $\{\mathbf{x}G \mid \mathbf{x}\in\mathbb{R}\}$, with $G=\begin{pmatrix}d & e & f\end{pmatrix}$. This can also be written as $\frac{x}{d}=\frac{y}{e}=\frac{z}{f}$, so we have $fx-dz=0$ and $fy-ez=0$ (each of these defines a plane, and the line is the intersection of these two planes). So the line is also $\{\mathbf{x}\in\mathbb{R}^3 \mid \mathbf{x}H^t=\mathbf{0}\}$, with

$$H=\begin{pmatrix}f & 0 & -d\\ 0 & f & -e\end{pmatrix}.$$

c) A plane in $\mathbb{R}^3$ through $\mathbf{0}$ can be written as $ax+by+cz=0$, so it is $\{\mathbf{x}\in\mathbb{R}^3 \mid \mathbf{x}H^t=\mathbf{0}\}$, with $H=\begin{pmatrix}a & b & c\end{pmatrix}$. It is also the span of two linearly independent vectors in the plane. For the plane above we could choose $\mathbf{v}_1=(c,0,-a)$ and $\mathbf{v}_2=(0,c,-b)$, and then the plane is $\{\mathbf{x}G \mid \mathbf{x}\in\mathbb{R}^3\}$, with

$$G=\begin{pmatrix}c & 0 & -a\\ 0 & c & -b\end{pmatrix}.$$

△

49 In each case, find a check-matrix and then a generator-matrix for the code.
a) $C=\{(x_1,x_2,x_3,x_4)\in\mathbb{F}_2^4 \mid x_1+x_2+x_4=0,\ x_3+x_4=0\}$
b) $C=\{(x_1,x_2,x_3,x_4,x_5)\in\mathbb{F}_7^5 \mid x_1+x_2+x_3+x_4+x_5=0,\ x_1+2x_2+3x_3+4x_4+5x_5=0\}$
c) $C=\{(x_1,x_2,x_3,x_4,x_5)\in\mathbb{F}_5^5 \mid x_1+x_3=0,\ x_2+x_4=0,\ 2x_1+3x_2+x_5=0\}$

S49 In each case, we write down an "acting check-matrix" A such that $C=\{\mathbf{x}\in\mathbb{F}_q^n \mid \mathbf{x}A^t=0\}$. We row-reduce it to RREF to be sure we have a check-matrix H, and can then use the $G\leftrightarrow H$ algorithm to find a generator-matrix G. Note that in all three cases, it turns out that A did have linearly independent rows, and so was in fact also a check-matrix for C.
a) $A=\begin{pmatrix}1&1&0&1\\0&0&1&1\end{pmatrix}=H$ (already in RREF). Then put vectors $\mathbf{v}_2$ and $\mathbf{v}_4$ into $G=\begin{pmatrix}1&1&0&0\\1&0&1&1\end{pmatrix}$.
b) $A=\begin{pmatrix}1&1&1&1&1\\1&2&3&4&5\end{pmatrix}$ and $H=\begin{pmatrix}1&0&6&5&4\\0&1&2&3&4\end{pmatrix}$. Using Proposition 4.5, $G=\begin{pmatrix}1&5&1&0&0\\2&4&0&1&0\\3&3&0&0&1\end{pmatrix}$.
c) $A=\begin{pmatrix}1&0&1&0&0\\0&1&0&1&0\\2&3&0&0&1\end{pmatrix}=(B\mid I_3)$. So by Proposition 4.5 in reverse, $G=(I_2\mid -B^t)=\begin{pmatrix}1&0&4&0&3\\0&1&0&4&2\end{pmatrix}$.

△

50 Until 2007, an ISBN (International Standard Book Number) was ten digits $x_1\ldots x_{10}$, with $0\le x_i\le 9$ for $1\le i\le 9$, and $0\le x_{10}\le 10$, but writing X for 10. It was also required that $x_1+2x_2+\cdots+10x_{10}\equiv 0$ mod 11. We can regard the ISBN numbers as a code $C_{ISBN}\subseteq\mathbb{F}_{11}^{10}$.
a) Why is C_{ISBN} not a linear code?
b) By thinking about codewords (that is, ISBN numbers) show that $d(C_{ISBN})\le 2$, and then show that $d(C_{ISBN})\ne 1$.
c) If instead we allow $0\le x_i\le 10$ for $1\le i\le 10$, we have a linear code $C\subseteq\mathbb{F}_{11}^{10}$. Write down its check-matrix, and show using Theorem 4.11 that $d(C)=2$.
d) One particularly common human error is to swap two adjacent digits. This is an error of weight two. Show that, nonetheless, for C (or C_{ISBN}) this error will be detected. What about swapping non-adjacent digits?

S50 a) For example , we have $\mathbf{c} = (2,9,0,0,0,0,0,0,0,0) \in C_{ISBN}$ but $5\mathbf{c} = (X,1,0,0,0,0,0,0,0,0) \neq C_{ISBN}$. (The problem is the restriction "$0 \leq x_i \leq 9$ for $1 \leq i \leq 9$".)
b) We know $d(C)$ is the minimum weight of a codeword, and above we have $w(\mathbf{c}) = 2$. Suppose we had $\mathbf{c}'$ with $w(\mathbf{c}') = 1$. Then $\mathbf{c}'$ has $x_j \neq 0$ but $x_i = 0$ for $i \neq j$. So the equation gives $jx_j = 0$, which is impossible because 11 is prime.
c) $H = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ X)$. No zero columns, but any two columns are linearly dependent (eg $3+8=0$), so $d(C) = 2$.
d) Suppose $\mathbf{c} = (c_1,\dots,c_j,c_{j+1},\dots,c_{10})$ is received as $\mathbf{y} = (c_1,\dots,c_{j+1},c_j,\dots,c_{10})$, with $c_j \neq c_{j+1}$. Then the error-vector is $\mathbf{e} = \mathbf{y} - \mathbf{c} = (0,\dots,c_{j+1}-c_j, c_j - c_{j+1},\dots,0)$. So $\mathbf{y}H^t = \mathbf{e}H^t = j(c_{j+1}-c_j) + (j+1)(c_j - c_{j+1}) = c_j - c_{j+1} \neq 0$. So $S(\mathbf{y}) \neq 0$, and the swap is detected. This also works for non-adjacent digits. △

51 Let $C = \subseteq \mathbb{F}_2^5$ have check-matrix $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$. Make a syndrome look-up table for C, and decode the received words $\mathbf{y}_1 = (1,0,0,1,1)$ and $\mathbf{y}_2 = (0,1,1,1,0)$. Show how a different syndrome look-up table could decode $\mathbf{y}_2$ differently. Why could this not happen for $\mathbf{y}_1$?

S51 We could make the table:

Syndrome $S(\mathbf{x})$	Error-vector $\mathbf{x}$
$(0,0,0)$	$(0,0,0,0,0)$
$(0,1,1)$	$(1,0,0,0,0)$
$(1,0,1)$	$(0,1,0,0,0)$
$(1,1,0)$	$(0,0,1,0,0)$
$(1,0,0)$	$(0,0,0,1,0)$
$(0,0,1)$	$(0,0,0,0,1)$
$(0,1,0)$	$(1,0,0,0,1)$
$(1,1,1)$	$(1,0,0,1,0)$

To decode $\mathbf{y}_1$, we calculate $S(\mathbf{y}_1) = (1,1,0)$. Using the above lookup table we should then decode $\mathbf{y}_1$ as $\mathbf{y}_1 - (0,0,1,0,0) = (1,0,1,1,1) = \mathbf{c}_1$. Similarly, we have $S(\mathbf{y}_2) = (1,1,1)$ and so should decode $\mathbf{y}_2$ as $\mathbf{y}_2 - (1,0,0,1,0) = (1,1,1,0,0) = \mathbf{c}_2$.

An alternate syndrome lookup table would be to replace the last two rows with

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

This would not affect $\mathbf{y}_1$, as it is only distance 1 away from $\mathbf{c}_1$, which is its unique nearest neighbour. However, using the alternate table we would decode $\mathbf{y}_2$ as $\mathbf{y}_2 - (0,0,1,0,1) = (0,1,0,1,1) = \mathbf{c}_3$. Both $\mathbf{c}_2$ and $\mathbf{c}_3$ are nearest neighbours of $\mathbf{y}_2$. By looking at H we can see that $d(C) = 3$ using Theorem 4.11, so we know that C can detect 2 errors, but can only uniquely correct 1 error. △

52 Let $C = \{\mathbf{x} \in \mathbb{F}_5^4 \mid \mathbf{x}H^t = 0\}$, where $H = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 1 \end{pmatrix}$.
a) Make a shortened syndrome look-up table for C, and decode the received words $\mathbf{y}_1 = (1,2,3,4)$, $\mathbf{y}_2 = (3,1,2,0)$, and $\mathbf{y}_3 = (2,4,3,1)$.
b) A normal look-up table has q^{n-k} rows. How many rows in this kind of shortened table?

S52 a)

Syndrome $S(\mathbf{x})$	Error-vector $\mathbf{x}$
$(0,0)$	$(0,0,0,0)$
$\lambda(1,0)$	$\lambda(1,0,0,0)$
$\lambda(0,1)$	$\lambda(0,0,1,0)$
$\lambda(2,3)$	$\lambda(0,0,1,0)$
$\lambda(3,1)$	$\lambda(0,0,0,1)$
$\lambda(1,1)$	$\lambda(1,1,0,0)$
$\lambda(1,3)$	$\lambda(1,3,0,0)$

$S(y_1) = y_1 H^t = (4,0) = 4(1,0)$. So we assume the error was $4(1,0,0,0)$, and decode to $(1,2,3,4) - (4,0,0,0) = (2,2,3,4)$.
$S(y_2) = (2,2) = 2(1,1)$. So we decode to $(3,1,2,0) - 2(1,1,0,0) = (1,4,2,0)$.
$S(y_3) = (1,4) = 3(2,3)$. So we decode to $(2,4,3,1) - 3(0,0,1,0) = (2,4,0,1)$.
b) We still have the zero syndrome. But all the q^{n-k} other syndromes are grouped into sets of $q-1$ multiples. So we get $\frac{q^{n-k}-1}{(q-1)} + 1$. For this code, it's $\frac{5^2-1}{5-1} + 1 = 7$ rows. △

53 Show that syndrome decoding is nearest-neighbour decoding. (Do this by contradiction - similar to the proof for array decoding)

S53 We receive $\mathbf{y}$, use the syndrome look-up table to find $\mathbf{x}$ such that $S(\mathbf{x}) - S(\mathbf{y})$, and decode to $\mathbf{c} = \mathbf{y} - \mathbf{x}$. Now suppose (for a contradiction) that $\mathbf{y}$ has a nearer neighbour $\mathbf{c}'$, so $d(\mathbf{y}, \mathbf{c}') < d(\mathbf{y}, \mathbf{c})$. In other words, $\mathbf{y}$ also $= \mathbf{c}' + \mathbf{x}'$, and $w(\mathbf{x}') < w(\mathbf{x})$. Now $S(\mathbf{x}') = S(\mathbf{y}) = S(\mathbf{x})$, but in making the table, $\mathbf{x}'$ would have been considered before $\mathbf{x}$, so the table has the line $S(\mathbf{x}') \mid \mathbf{x}'$, not $S(\mathbf{x}) \mid \mathbf{x}$. So in fact we would have decoded to $\mathbf{c}' = \mathbf{y} - \mathbf{x}'$. △

54 Suppose that matrix A is in $M_{m,n}(\mathbb{F}_q)$. How can we check whether some set of d columns of A is linearly dependent? In general, we could write them as *rows* in a $d \times m$ matrix, and row-reduce. But for some values of d there are other ways. How can we check when:
a) $d = 1$ b) $d = 2$ c) $d = m$ d) $d > m$?

S54 a) $d = 1$: A single column can only form a dependent set if it is an all-zero column.
b) $d = 2$: Two columns are dependent if and only if one is a multiple of another.
c) $d = m$: make a square matrix of the columns. They are dependent if and only if the determinant is 0.
d) $d > m$: More that m columns of length m must be dependent. △

55 Let $H = \begin{pmatrix} 3 & 4 & 1 \\ 1 & 4 & 2 \end{pmatrix}$. Find the minimum distance of the codes:
a) $C_5 = \{\mathbf{x} \in \mathbb{F}_5^3 \mid \mathbf{x}H^t = \mathbf{0}\}$
b) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^3 \mid \mathbf{x}H^t = \mathbf{0}\}$

S55 By Q54 a) $d \neq 1$, and by d) $d \leq 3$. Over $\mathbb{F}_5$ we have $2\binom{3}{1} = \binom{1}{2}$, so $d(C_5) = 2$.
But over $\mathbb{F}_7$ no pair of columns are multiples, so $d(C_7) = 3$. △

56 Let $H = \begin{pmatrix} 1 & 0 & 4 & 1 \\ 2 & 3 & 0 & 1 \\ 0 & 4 & 3 & 2 \end{pmatrix}$. Find the minimum distance of the codes:
a) $C_5 = \{\mathbf{x} \in \mathbb{F}_5^4 \mid \mathbf{x}H^t = \mathbf{0}\}$
b) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^4 \mid \mathbf{x}H^t = \mathbf{0}\}$

S56 We know $d \le n-k+1 = 4$. No all-zero column, so $d \ne 1$. By the positions of the zeros, no column is a multiple of another, so $d \ne 2$. So the only question is whether $d = 3$ or $d = 4$. We can decide this by finding 3×3 determinants; to do parts a) and b) together, I won't reduce by 5 or 7 until the end.

Expanding by the top row, $\begin{vmatrix} 1 & 0 & 4 \\ 2 & 3 & 0 \\ 0 & 4 & 3 \end{vmatrix} = 1 \times 3 \times 3 + 4 \times 2 \times 4 = 41$, which is $1 \in \mathbb{F}_5, 6 \in \mathbb{F}_7$.

So over both fields, these columns are independent. Expanding by the top row, $\begin{vmatrix} 1 & 0 & 1 \\ 2 & 3 & 1 \\ 0 & 4 & 2 \end{vmatrix} = 1 \times (6-4) + 1 \times 8 = 10$, which is $0 \in \mathbb{F}_5, 3 \in \mathbb{F}_7$. So over $\mathbb{F}_5$, these columns are dependent, so $d(C_5) = 3$. But for $\mathbb{F}_7$ they are independent so we have to go on. Expanding by the middle row, $\begin{vmatrix} 1 & 4 & 1 \\ 2 & 0 & 1 \\ 0 & 3 & 2 \end{vmatrix} = -2 \times (8-3) + -1 \times 3 = -13 = 1 \in \mathbb{F}_7$; and expanding by the top row, $\begin{vmatrix} 0 & 4 & 1 \\ 3 & 0 & 1 \\ 4 & 3 & 2 \end{vmatrix} = -4 \times (6-4) + 1 \times 9 = 1 \in \mathbb{F}_7$. So no set of three columns is dependent over $\mathbb{F}_7$, and we have $d(C_7) = 4$. △

57 Using Theorem 4.11, find yet another proof that $d \le n-k+1$ (the Singleton bound for linear codes). (*Hint*: Although the theorem is also true for acting check-matrices, it helps to consider a proper check-matrix.)

S57 A check matrix has $n-k$ rows, so its columns are elements of $\mathbb{F}_q^{n-k}$. The largest possible set of linearly independent vectors in this space is of size $n-k$, so any $n-k+1$ columns must be linearly dependent. So by Theorem 4.11 we have $d \le n-k+1$. △

58 Students sometimes confuse the way to find $d(C)$ from a check-matrix (see Theorem 4.11) with the definition of the rank of a matrix. How are these ideas similar and different? Find two (or more) matrices $H_1, H_2, \ldots$ which have the same rank, but the codes $C_i = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H_i^t = \mathbf{0}\}$, for which they are check-matrices, have different $d(C_i)$. (*Hint:* There are small examples - e.g. in $M_{2,3}(\mathbb{F}_2)$)

S58 The *rank* of a matrix is the largest set of linearly independent columns of a matrix. The minimum distance d is the smallest number of linearly dependent columns of the check-matrix (using Theorem 4.11). As examples of check-matrices with the same rank but whose associated codes have different minimum distances, consider

$$H_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad d(C_1) = 1$$
$$H_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad d(C_2) = 2$$
$$H_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad d(C_3) = 3,$$

all of which have rank 2. △

59 Suppose code C has generator-matrix $G \in M_{k,n}(\mathbb{F}_q)$ and check-matrix $H \in M_{n-k,n}(\mathbb{F}_q)$. If C is monomially equivalent to C' we know we can make a generator-matrix G' for C' by permuting and multiplying columns of G. Can we make a check-matrix H' for C' in a similar way?
Adapting the notation of Q40, let us say that for a matrix $A \in M_{k,n}(\mathbb{F}_q)$, $\pi_{s(i,j)}(A)$ is A with columns i and j swapped, and $\pi_{m(i,\mu)}(A)$ is A with column i multiplied by non-zero $\mu \in \mathbb{F}_q$. Then if C_s has generator-matrix $\pi_{s(i,j)}(G)$,and C_m has generator-matrix $\pi_{m(i,\mu)}(G)$, both these codes are monomially equivalent to C. In terms of $\pi_{s(i,j)}$ and $\pi_{m(i,\mu)}$, find a check-matrix for C_s and for C_m. For each code, justify your answer by showing that any row of the generator matrix is orthogonal to any row of the check matrix.

S59 The check matrix for C_s is $\pi_{s(i,j)}(H)$, and for C_m is $\pi_{m(i,\mu^{-1})}(G)$.
Suppose that $\mathbf{g} = (x_1, \ldots, x_i, \ldots, x_j, \ldots x_n)$ is a row of G , and $\mathbf{h} = (y_1, \ldots, y_i, \ldots, y_j, \ldots y_n)$ is a row of H. Then we know that $\mathbf{g} \cdot \mathbf{h} = x_1 y_x + \cdots + x_i y_i + \cdots + x_j y_j + \cdots + x_n y_n = 0$.
Now, considering C_s, the dot product of the the corresponding rows in $\pi_{s(i,j)}(G)$ and $\pi_{s(i,j)}(H)$ is $\pi_{s(i,j)}\mathbf{g} \cdot \pi_{s(i,j)}\mathbf{h} = x_1 y_x + \cdots + x_j y_j + \cdots + x_i y_i + \cdots + x_n y_n = 0$.
Similarly, for C_m we get $\pi_{m(i,\mu)}\mathbf{g} \cdot \pi_{m(i,\mu^{-1})}\mathbf{h} = x_1 y_x + \cdots + \mu x_i \mu^{-1} y_i + \cdots + x_n y_n = 0$.
We conclude that H needs the *same* permutations of columns as G, but *inverse* multiplications of columns. We can also write a check-matrix version of Proposition 3.9: If two check-matrices are related by permuting or multiplying columns, then the two codes are equivalent. △

60 Consider the code $C' \subseteq \mathbb{F}_{11}^{10}$, $C' = \{\mathbf{x} \in \mathbb{F}_{11}^{10} \mid x_1 + x_2 \cdots + x_{10} = 0\}$. Show that C' is equivalent to the code C of Q50 in two ways:
a) For any word $\mathbf{c} = (c_1, \ldots, c_{10}) \in C$ apply suitable changes to make a word $\mathbf{c}' \in C'$. This shows that C is equivalent to a subset of C'. Now do the same in reverse.
b) Consider check matrices, and see Q59.
c) If C and C' are equivalent, and C' seems simpler, why did we use C for books?

S60 a) Since $\mathbf{c} \in C$, we know that $c_1 + 2c_2 + \cdots + 10c_{10} = 0$. Then if $\mathbf{c}' = (c_1, 2c_2, \ldots + 10c_{10})$, clearly it is in C'. In reverse, if $(u_1, u_2, \ldots, u_n) \in C'$, then $(u_1, 6u_2, 4u_3, \ldots, i^{-1}u_i, \ldots 10u_{10}) \in C$.
b) C has check-matrix $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)$; C' has $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$. Clearly we can multiply the (very short) columns of one to get the other.
d) One common human error is to swap adjacent digits; C detects swapped digits, C' does not. △