******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 $C^\perp$.

**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 $C^\perp$.

**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?

**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 $H = (I_{n-k} \mid -A^t)$. (*Hint:* Consider the code $C'$ which has generator-matrix $H = (I_{n-k} \mid -A^t)$, and use Propositions 4.5 and 4.7.)

**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 $\mathbb{R}^3$?

**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) $C = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_5^5 \mid x_1 + x_3 = 0,\ x_2 + x_4 = 0,\ 2x_1 + 3x_2 + x_5 = 0\}$

**50** Until 2007, an ISBN (International Standard Book Number) was ten digits $x_1 \dots x_{10}$, with $0 \leq x_i \leq 9$ for $1 \leq i \leq 9$, and $0 \leq x_{10} \leq 10$, 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 $d(C_{ISBN}) \leq 2$, and then show that $d(C_{ISBN}) \neq 1$.
c) If instead we allow $0 \leq x_i \leq 10$ for $1 \leq i \leq 10$, 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?

**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 $\mathbf{y}_1$?

**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?

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

**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) $d > m$ ?

**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) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^3 \mid \mathbf{x}H^t = \mathbf{0}\}$

**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) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^4 \mid \mathbf{x}H^t = \mathbf{0}\}$

**57** Using Theorem 4.11, find yet another proof that $d \leq n - k + 1$ (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.)

**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 $M_{2,3}(\mathbb{F}_2)$)

**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.

**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?