SECTION B

Answer **TWO** of the three questions in this section (40 marks in total).

If more than TWO questions from this section are attempted, then credit will be given for the best TWO answers.

B5.

(a) Define the minimum distance, $d(C)$, of a code $C \subseteq \mathbb{F}_q^n$.

(b) Prove that a code $C \subseteq \mathbb{F}_q^n$ contains no more that $q^{n+1-d(C)}$ elements.

We say that $C \subseteq \mathbb{F}_q^n$ is an MDS code if $|C| = q^{n+1-d(C)}$.

(c) Define the Hamming code $\mathrm{Ham}(s, q)$.

(d) Write down expressions for the length, n, and the dimension, k, of $\mathrm{Ham}(s, q)$ in terms of s, q.

(e) Let q be given. Describe all values of s such that $\mathrm{Ham}(s, q)$ is an MDS code. You may quote any result from the course without proof.

(f) Write down a generator matrix for $\mathrm{Ham}(3, 2)$ in standard form.

(g) Find $\max\{d(\underline{x}, \underline{y}) : \underline{x}, \underline{y} \in \mathrm{Ham}(3, 2)\}$, that is, the *maximum* distance between two codewords in $\mathrm{Ham}(3, 2)$. Justify your answer.

[20 marks]

B6. Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k.

(a) Define the dual code $C^\perp$ and state the formula for $\dim C^\perp$.

(b) Assume that $q = 2$ and the binary linear code C is self-dual, that is, $C^\perp = C$.

- (i) Show that n is even.
- (ii) Show that every codeword in C has even weight.
- (iii) Show that the vector $11\ldots1$ of weight n belongs to C.

(c) Show that the binary code D with generator matrix $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ is self-dual.

(d) Work out a standard array for the code D.

(e) Assume that the code D is transmitted down a binary symmetric channel with bit error rate r. Let $P_{\mathrm{corr}}(D)$ denote the probability that a received vector is decoded correctly. Show that $P_{\mathrm{corr}}(D) = (1 - r)^2$.

(f) Find a self-dual code $E \subseteq \mathbb{F}_2^4$ such that $E \neq D$. Show that E is linearly equivalent to D.

[20 marks]