TOPICS IN DISCRETE MATHEMATICS 3/4: PROBLEM SHEET 1

Hand in questions: Revision 5, and Error-Correcting Codes 4 and 6.

1. Linear Algebra Revision

(1) Prove that the following sets are not fields: $\mathbb{Z}, \mathbb{N}$, and the integers mod 6 (or indeed modulo any composite number m).

(2) Is $GL_n(\mathbb{C})$ - i.e. the set of invertible $n \times n$ matrices with entries in $\mathbb{C}$ - a field?

(3) Give a construction of the finite field $\mathbb{F}_9 = \mathbb{F}_{3^2}$.

(4) Let $V = F[x]$ - the vector space of polynomials in x over field F.
   (a) Let W denote the set of polynomials $f \in F[x]$ such that $\deg(f) \leq 3$. Prove that $W \leq V$.
   (b) Does V have a finite basis? Remember that scalar multiplication is just by elements in F.

(5) Let $\mathbf{v}_1 = (3, 1, 2), \mathbf{v}_2 = (2, 4, 2)$ and $\mathbf{v}_3 = (0, 0, -1)$. Show that as vectors in $\mathbb{R}^3$, $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly independent. Now consider the $\mathbf{v}_i \in \mathbb{F}_5^3$; are they still linearly independent?

(6) Extend the set $\{(1, 1, 2, 0), (1, 0, 1, 1)\}$ to a basis of $\mathbb{F}_3^4$.

(7) Let
$$M = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in M_{3,4}(\mathbb{F}_2).$$
Compute nullity(M) and find a basis for NullSpace(M).

(8) Let
$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in M_{2,4}(\mathbb{F}_2).$$
Show that RowSpace(M)=NullSpace(M).

2. Error-correcting codes

(1) Recall the simplex code $\mathcal{C}_3 \leq \mathbb{F}_2^7$ as defined in Example 1.2 of lectures. Come up with a scheme for decoding any single error.

(2) Prove that the Hamming distance is a metric.

(3) For the following codes over alphabet $A = \mathbb{F}_3$, find the parameters n, d and $|\mathcal{C}|$. If $\mathcal{C}$ is linear, then also compute its dimension k.
   (a) $\mathcal{C} = \{(0, 0, 0, 0), (1, 1, 2, 1), (1, 1, 0, 1)\}$;
   (b) $\mathcal{C} = \{(0, 0, 0, 0), (1, 1, 2, 1), (2, 2, 1, 2)\}$;
   (c) $\mathcal{C} = \{(0, 0, 0), (1, 1, 1), (2, 2, 2), (1, 0, 0), (2, 0, 0), (2, 1, 1), (0, 2, 2), (0, 1, 1), (1, 2, 2)\}$;

Date: January 31, 2019.

(d) $\mathcal{C} = \langle (0,1,2,0),(1,1,1,1),(1,0,1,2) \rangle_{\mathbb{F}_3}$.

(4) Find the values of n, k, d and $|\mathcal{C}|$ for the following linear codes over $\mathbb{F}_5$. For part (b), find a basis for the code.

(a) The code with generator matrix

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \end{pmatrix}.$$

(b) The code with parity check matrix

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 2 & 2 \\ 3 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

(5) Let's consider a real world example: The International Standard Book Number (ISBN) is a code used to catalogue books. It is a linear code $\mathcal{C} \leq \mathbb{F}_{11}^{10}$ (where in practice, the letter X is used to denote the number 10). The first 9 digits of a codeword tell us information about the book (e.g. country of origin, publisher etc). The tenth digit is a check digit (like in the simplex code where the last 4 entries are check-digits) for error detection.

We define the ISBN code using the parity check matrix

$$H_{ISBN} = \begin{pmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

So for example, "White Teeth" by Zadie Smith has ISBN 0-241-13997-X and we see that

$$10(0) + 9(2) + 8(4) + 7(1) + 6(1) + 5(3) + 4(9) + 3(9) + 2(7) + 1(10) = 165 \equiv 0 \mod 11.$$

(a) Find the values of n, k, d for the ISBN code. How many codewords are there?

(b) Find the missing digits in these ISBN numbers

$$0141184a84; \; 033b727703; \; 184800987c.$$

(6) Let $\mathcal{C} \leq \mathbb{F}_2^n$ be a linear code.

(a) Consider the map $f : \mathcal{C} \to \mathbb{F}_2$ given by $f(\mathbf{c}) = c_1 + \cdots + c_n$. Show that f is surjective if and only if $\mathcal{C}$ contains a code-word of odd weight.

(b) Let $\mathcal{C}$ be an $[n, k]_2$-linear code that contains a code-word of odd weight. Using the above or otherwise, show that the even weight code-words of $\mathcal{C}$ form an $[n, k-1]_2$-linear code.

E-mail address: `alex.malcolm@bristol.ac.uk`