TOPICS IN DISCRETE MATHEMATICS 3/4: SOLUTIONS SHEET 1

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

1. Linear Algebra Revision

(1) None of these sets have multiplicative inverses e.g. in all three sets F we can check that $2 \cdot a \neq 1$ for all $a \in F$.

(2) No - for many reasons e.g. there is no additive identity (the all zeros matrix isn't invertible).

(3) Firstly we need an irreducible polynomial in $\mathbb{F}_3[x]$ of degree 2. Well if $f(x) = x^2+1$ then $f(0,1,2) \neq 0$ and so is irreducible. It follows that

$$\mathbb{F}_9 = \mathbb{F}_{3^2} = \{a + \alpha b \,|\, a, b \in \mathbb{F}_3\},$$

where $f(\alpha) = 0$.

(4) (a) We need to check that W is closed under the vector space operations of addition, and multiplication by scalars in F. But this is clear as $\deg(\lambda \cdot f)$, $\deg(f+g) \leq 3$, for all $f, g \in F[x]$ with $\deg(f), \deg(g) \leq 3$ and all $\lambda \in F$.

(b) No. Suppose that $\{f_1, \ldots, f_l\}$ is a finite collection of polynomials in V. Clearly if $f \in \langle f_1, \ldots, f_l \rangle_F$ then $\deg(f) \leq \max\{\deg(f_i) \,|\, 1 \leq i \leq l\}$. Therefore, as the polynomials in V have unbounded degree, $\{f_1, \ldots, f_l\}$ cannot span the whole space and is not a basis by definition. As l was chosen arbitrarily, it follows that no finite basis can exist.

(5) The vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly independent if and only if the matrix

$$M := \begin{pmatrix} \leftarrow \mathbf{v}_1 \rightarrow \\ \leftarrow \mathbf{v}_2 \rightarrow \\ \leftarrow \mathbf{v}_3 \rightarrow \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 0 & -1 \end{pmatrix}.$$

has non-zero determinant. Well $\det(M) = -10$ and so the vectors are linearly independent over $\mathbb{R}$ but not over $\mathbb{F}_5$. In particular, treated as vectors in $\mathbb{F}_5^3$, $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_3$

(6) There are many choices: $\{(1,1,2,0), (1,0,1,1), (0,0,1,0), (0,0,0,1)\}$ is just one of them.

(7) Firstly, we check that the rows of M are linearly independent and hence $\text{nullity}(M) = 4 - \text{rank}(M) = 1$. Now let $\mathbf{v} \in \mathbb{F}_2^4$. By definition $\mathbf{v} = (v_1, v_2, v_3, v_4) \in \text{NullSpace}(M)$ if and only if

$$M\mathbf{v}^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = 0.$$

Date: February 11, 2019.

This is equivalent to $v_1 = v_2 = v_3$ and consequently, $2v_1 = v_4$. Letting $v_1 = 1$ gives vector $(1, 1, 1, 0) \in$NullSpace(M). But we only need this single basis vector (as the space is 1-dimensional) and so we're done.

(8) By the rank-nullity theorem, as $\dim(\text{RowSpace}(M)) = 2$ it follows that $\dim(\text{NullSpace}(M)) = 2$ also. It therefore suffices to show that $\mathbf{v}_1 = (1, 1, 1, 1)$ and $\mathbf{v}_2 = (0, 1, 0, 1) \in$ NullSpace(M). But it's easy to check that indeed $M\mathbf{v}_1^T = M\mathbf{v}_2^T = 0$.

2. Error-correcting codes

(1) A single error in a component (x, y, z, a, b, c, d) produces a unique pattern of failures in the check-sums. I.e.

Error in:	x	y	z	a	b	c	d
$x + y = a$	×	×	✓	×	✓	✓	✓
$x + z = b$	×	✓	×	✓	×	✓	✓
$y + z = c$	✓	×	×	✓	✓	×	✓
$x + \cdots + c = d$	×	×	×	×	×	×	×

E.g. if there is an error in the 4th co-ordinate (the "a" position) then the 1st and 4th check-sums fail. Hence given any codeword with a single error, we simply check which check-sums fail, identify the co-ordinate position, and bit-flip accordingly.

(2) The first two properties are clear so we shall check the triangle inequality: let $\mathbf{u}, \mathbf{v}, \mathbf{s} \in A^n$ and recall that $d(\mathbf{u}, \mathbf{v})$ is exactly the number of co-ordinates in $\mathbf{u}$ we need to change to get $\mathbf{v}$. Well we could make these changes via the point $\mathbf{s}$ i.e. start with $\mathbf{u}$, make $d(\mathbf{u}, \mathbf{s})$ changes to get $\mathbf{s}$ and then $d(\mathbf{s}, \mathbf{v})$ changes to get $\mathbf{v}$. It follows that $d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{s}) + d(\mathbf{s}, \mathbf{v})$. NB: We have equality if we change each ith position $(1 \leq i \leq n)$ at most once.

(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) $n = 4, d = 1$ and $|\mathcal{C}| = 3$. This code is non-linear.
   (b) $\mathcal{C}$ is a $[4, 1, 4]_3$-linear code. Hence $|\mathcal{C}| = 3^1 = 3$.
   (c) $\mathcal{C}$ is a $[3, 2, 1]_3$-linear code. Hence $|\mathcal{C}| = 3^2 = 3$.
   (d) These three vectors are linearly independent and hence form a basis of $\mathcal{C}$ as a $[4, 3, 2]_3$-linearly code.

(4) (a) $n = 3, k = 2, |\mathcal{C}| = 5^2$ and $d = 2$.
   (b) Row reducing the parity check matrix gives

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 4 & 4 & 3 \\ 0 & 0 & 2 & 0 & 0 \end{pmatrix}.$$

As this has 5 columns and 3 rows, the code $\mathcal{C}$ that it defines has $n = 5$ and dimension $k = 5 - 3 = 2$. It follows that $|\mathcal{C}| = 5^2$. Now we need to find 2 distinct vectors $\mathbf{v} = (v_1, \ldots, v_5) \neq 0$ such that $H\mathbf{v}^T = 0$ and these will form a basis of $\mathcal{C}$. Well $H\mathbf{v}^T = 0$ implies that

$$v_1 + v_2 + v_4 = v_2 + 4v_3 + 4v_4 + 3v_5 = 2v_3 = 0.$$

This system has general solution $(3\alpha+3\beta, \alpha+2\beta, 0, \alpha, \beta)$ for $\alpha, \beta \in \mathbb{F}_5$. Letting $(\alpha, \beta) \in \{(1,0),(0,1)\}$ then gives basis vectors $(3,1,0,1,0)$ and $(3,2,0,0,1)$. To see that $d = 3$, note from the general form code-word $(3\alpha + 3\beta, \alpha + 2\beta, 0, \alpha, \beta)$ that the minimum weight is 3, and apply Lem 3.13 from lectures. Alternatively, spot that every pair of columns in H is linearly independent, but that columns 2 and 5 add to give column 4. The result then follows by Prop. 4.4 in lectures.

(5) (a) $n = 10, k = 9$, $|\mathcal{C}| = 10^9$ and $d = 2$ by Prop. 4.4 in lectures.

(b) $a = 8, b = 3, c = 9$.

(6) (a) As $\mathcal{C}$ is linear, it contains the zero vector, and so 0 is in the image of f. Then, noting that $f(\mathbf{c}) \equiv \text{wt}(\mathbf{c}) \mod 2$, it is clear that f is surjective if and only if $\mathcal{C}$ contains a codeword of weight $1 \mod 2$.

(b) A neat solution to this problem applies the rank-nullity theorem to the map f defined in the previous section. Recall that the rank-nullity theorem says the following: Let $\phi : V \to W$ be a linear transformation between two vector spaces V and W, such that V is finite dimensional. Then $\text{rank}(\phi) + \text{nullity}(\phi) = \dim(V)$. If W is also finite dimensional, and we pick bases for the spaces, we can describe f by a matrix (this is how we gave the R-N theorem in lectures - see Thm 2.14).

So, it's easy to check that $f(\lambda\mathbf{c} + \mu\mathbf{c}') = \lambda f(\mathbf{c}) + \mu f(\mathbf{c}')$ for all $\mathbf{c}, \mathbf{c}' \in \mathcal{C} \leq \mathbb{F}_2^n$ and all $\lambda, \mu \in \mathbb{F}_2$. Hence f is a linear transformation by definition. In fact, we have matrix representation $f(\mathbf{c}) = M\mathbf{c}^T$ where $M = (1, \ldots, 1)$. Now as $\mathcal{C}$ contains an odd-weight code-word, f is surjective onto the vector space $\mathbb{F}_2$. In particular, $\text{rank}(f) = \dim(\mathbb{F}_2) = 1$ and it follows by rank-nullity that

$$\text{nullity}(f) = \dim(\text{NullSpace}(f)) = \dim(\mathcal{C}) - 1 = k - 1.$$

But $\text{NullSpace}(f) \leq \mathcal{C}$ is the subspace of code-words satisfying $f(\mathbf{c}) \equiv \text{wt}(\mathbf{c}) \equiv 0 \mod 2$, and we're done.

Alternative Solution

Let $\mathcal{C}_0, \mathcal{C}_1 \subseteq \mathcal{C}$ denote the set of code-words of even, and odd weights, respectively. Both of these subsets are non-empty ($\mathcal{C}_1$ by assumption, and $\mathcal{C}_0$ as it contains the zero vector). Now suppose that $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_0$ and consider $\mathbf{c} + \mathbf{c}'$. Well

$$\text{wt}(\mathbf{c} + \mathbf{c}') = \text{wt}(\mathbf{c}) + \text{wt}(\mathbf{c}') - 2|\{i | c_i = c_i'\}|, \tag{1}$$

which is even. So $\mathcal{C}_0$ is closed under addition (and clearly also multiplication by $0, 1 \in \mathbb{F}_2$) and hence $\mathcal{C}_0 \leq \mathcal{C}$. It therefore remains to show that $2|\mathcal{C}_0| = |\mathcal{C}|$. Well similarly to (1), it is easy to check that adding an odd and even-weight codeword yields an odd-weight result. Lastly, odd plus odd gives even. Hence if $\mathbf{c} \in \mathcal{C}_1$ is a fixed code-word of odd weight, the set

$$\mathbf{c} + \mathcal{C}_0 = \{\mathbf{c} + \mathbf{c}' | \mathbf{c}' \in \mathcal{C}_0\} \subset \mathcal{C}_1$$

contains $|\mathcal{C}_0|$ distinct vectors. So $|\mathcal{C}_0| \leq |\mathcal{C}_1|$. The reverse inequality follows in a similar manner and hence

$$2|\mathcal{C}_0| = |\mathcal{C}_0| + |\mathcal{C}_1| = |\mathcal{C}|.$$

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