Honours Algebra 2, Assignment 1

Michael Snarski & Jamie Klassen

February 5, 2012

Question 1. *Solve $Ax = y$ over $\mathbb{Z}_2$, where*

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, y = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Solution Plug this into an augmented matrix and row-reduce via the one real operation you have: add rows together (why?). Otherwise, since $\det(A) \neq 0$, the unique solution is (by inspection) $x = (1, 0, 0)$.

Question 2. *Solve the linear equation $Ax = y$ over $\mathbb{Z}_2$ where*

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Solution By inspection there are two linearly independent columns, and the vector $x = (1, 1, 1)$ is in $\text{null}(A)$. The number of solutions is determined by the number of elements in the kernel, so, 2: the previous $(1, 0, 0)$ and $(1, 1, 1) + (1, 0, 0) = (0, 1, 1)$. (If you're not 100% comfortable with this, read the first solution to the next question.)

Question 3. *Show that the number of distinct solutions of a system of linear equations (in any number of equations or unknowns) over $\mathbb{Z}_p$ is either 0 or a power of p.*

Solution There are two solutions I've seen of this, one linear-algebraic and the other group-theoretic, the latter being due to Simon Szatmari.

Suppose we have at least one solution x_0 to the equation $Ax = y$. The first thing is to notice that it suffices to check the homogenous equation $(y = 0)$ for the number of solutions. To see this, let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be a basis for the nullspace of A, i.e. $Av_i = 0$ for each $i = 1 \ldots n$. Then for each $\alpha_i \in \mathbb{F}, v_i \in \mathcal{B}$, given $Ax_0 = y$, $A(x_0 + \sum_i \alpha_i v_i) = Ax_0 + \sum_i \alpha_i (Av_i) = y$, so we have at least $\#\mathcal{B}$ solutions. These are all the solutions, for if $Ax_0 = Ax_1 = y$, $A(x_1 - x_0) = 0$, and $x_1 = x_0 + (x_1 - x_0)$, so $x_1 = x_0 + \sum_i \alpha_i v_i$.

So how many elements are there in $\mathcal{B}$? As in question 4 of assignment 2, we have p choices for each of the n scalars, so p^n choices. If there were no fundemental solution x_0 to begin with, the system is overdetermined and has no solution. If $\text{null}(A) = \{0\}$, $\dim(\text{null}(A)) = 0$ and $p^0 = 1$, so there is a unique solution.

Question 4. *Show that there is no error-correcting code of dimension 5 in $\mathbb{Z}_2^7$, so that the example constructed in class is in some sense optimal, in the sense that it is the error-correcting code of largest possible dimension in $\mathbb{Z}_2^7$.*

Solution Let $C \subset \mathbb{Z}_2^7$ be a linear code of dimension k. Let B be the standard basis for $\mathbb{Z}_2^7$; there must be an injection $B \hookrightarrow \mathbb{Z}_2^7/C \cong \mathbb{Z}_2^{7-k}$ so that the different bits can be distinguished in order to correct at least one error. Thus we must have $7 = |B| \leq |\mathbb{Z}_2^{7-k}| = 2^{7-k}$ so $7 - k \geq \lceil \log_2 7 \rceil = 3$ so $k \leq 4$. Therefore there is no error-correcting code of dimension 5 in $\mathbb{Z}_2^7$.

Question 5. *What is the largest dimension of a linear code in $\mathbb{Z}_2^{15}$ that can detect and correct a single bit (i.e. one-bit) error?*

Solution Since $2^4 = 16 = 15 + 1$, we need at least four entries in $\mathbb{Z}_2$ to have enough combinations (excluding the zero vector) to distinguish 15 different vectors. Thus we need to save four dimensions, and the rest can be in the kernel – that is, the largest dimension a linear code can have is 11.

Question 6. *Let V be the vector space of polynomials of degree at most 5 over $\mathbb{R}$, and let $T\colon V \to V$ be defined by*

$$T(f) = \frac{d^3}{dx^3} f + \frac{d^2}{dx^2} f.$$

Describe the kernel of T, and its image. What are the dimensions of these subspaces? What is the subspace of V generated by $\ker(T)$ and $\operatorname{im}(T)$?

Solution Probably the easiest way to get everything fully correctly is write the matrix associated to T. To do this, *we must first choose a basis* (As one of my CEGEP professors once said, 'mistaking a linear transformation for its standard matrix would, you know, qualify you for the special olympics or something.') Let $\mathcal{B} = \{e_1, \ldots, e_6\}$ be the standard basis and write $f = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 = (a_0, a_1, a_2, a_3, a_4, a_5)$. Then,

$$T(e_1) = 0, T(e_2) = 0, T(e_3) = 2, T(e_4) = 3 \cdot 2 + 3 \cdot 2x$$
$$T(e_5) = 4!x + 4 \cdot 3x^2, T(e_6) = 5 \cdot 4 \cdot 3x^2 + 5 \cdot 4x^3$$

so the matrix representing T relative to $\mathcal{B}$ is

$$A = \begin{pmatrix} 0 & 0 & 2 & 3 \cdot 2 & 0 & 0 \\ 0 & 0 & 0 & 3 \cdot 2 & 4 \cdot 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \cdot 3 & 5 \cdot 4 \cdot 3 \\ 0 & 0 & 0 & 0 & 0 & 5 \cdot 4 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

From this, it is clear that e_1 and e_2 are two linearly independent basis elements which are in $\ker(T)$. Since there are four linearly independent columns and $6 = \dim V = \dim(\operatorname{im}(T)) + \dim(\ker(T)) = 4 + \dim(\ker(T))$, e_1 and e_2 must span the kernel, and so $\ker(T) = \operatorname{Span}(\{e_1, e_2\})$, while $\operatorname{im}(T) = \operatorname{Span}(\{e_1, e_2, e_3, e_4\})$, which is the subspace of all polynomials of degree at most three, and it is 4-dimensional.

Question 7. *A linear transformation $T : V \to V$ is called a* projection*, or an* idempotent*, if it satisfies $T^2 = T$. Show that V can be expressed as the* direct sum *of* $\ker(T)$ *and* $\text{Image}(T)$*.*

Solution Let $v \in V$ be arbitrary. Write $v = (v - T(v)) + T(v)$. Since

$$T(v - T(v)) = T(v) - T^2(v) = T(v) - T(v) = 0,$$

we have expressed v as a sum of an element of $\ker(T)$ and an element of $\text{Image}(T)$, so $V = \ker(T) + \text{Image}(T)$. To show that the sum is direct we must show $\ker(T) \cap \text{Image}(T) = 0$. To see this, suppose $v \in \ker(T) \cap \text{Image}(T)$. Then $v \in \text{Image}(T)$ so there exists $w \in V$ with $v = T(w)$. Then since $v \in \ker(T)$,

$$0 = T(v) = T^2(w) = T(w) = v,$$

so indeed $\ker(T) \cap \text{Image}(T) = 0$. Hence $V \cong \ker(T) \oplus \text{Image}(T)$ as required.

Question 8. *Let V be a vector space over a field F. A linear transformation $N : V \to V$ is said to be* nilpotent *if $N^k = 0$ for some k. Show that if N is nilpotent, then the linear transformation $1 - N$ (where 1 denotes the identity transformation) is invertible.*

Solution To show invertibility, we need to exhibit a linear transformation $A : V \to V$ which is a two-sided inverse to $1 - N$; that is $A(1 - N) = (1 - N)A = 1$. Inspired by the series

$$\frac{1}{1 - x} = 1 + x + x^2 + x^3 + \cdots$$

we take $A = 1 + N + N^2 + \cdots + N^{k-1}$ (since all of the terms at or after N^k are zero by nilpotency). We check using right distributivity:

$$\begin{aligned} A(1 - N) &= (1 + N + N^2 + \cdots + N^{k-1})(1 - N) \\ &= (1 - N) + (N - N^2) + (N^2 - N^3) + \cdots + (N^{k-1} - N^k) \\ &= 1 + (-N + N) + (-N^2 + N^2) + \cdots + (-N^{k-1} + N^{k-1}) - N^k \\ &= 1 - N^k = 1 \end{aligned}$$

since the inner terms cancel and N is nilpotent. Furthermore by left distributivity:

$$\begin{aligned} (1 - N)A &= (1 - N)(1 + N + N^2 + \cdots + N^{k-1}) \\ &= (1 - N) + (N - N^2) + (N^2 - N^3) + \cdots + (N^{k-1} - N^k) \\ &= 1 + (-N + N) + (-N^2 + N^2) + \cdots + (-N^{k-1} + N^{k-1}) - N^k \\ &= 1 - N^k = 1 \end{aligned}$$

So $1 - N$ is indeed invertible!