Solutions to problem set 3.

Mathematics 342, Term 2, 2018. Instructor: Reichstein.

(1) Is 0131160938 a valid ISBN number?

Solution: No, because

$$1 \cdot 0 + 2 \cdot 1 + 3 \cdot 3 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 6 + 7 \cdot 0 + 8 \cdot 9 + 9 \cdot 3 + 10 \cdot 8 \equiv 4 \pmod{11}.$$

(2) Problem 4.4.

Solution: First we check that if $\mathbf{u} = \mathbf{0}$ then $\mathbf{u}$ and $\mathbf{v}$ are linearly dependent. Indeed, in this case $1 \cdot \mathbf{u} + 0 \cdot \mathbf{v} = \mathbf{0}$. Similarly, if $\mathbf{v} = \mathbf{0}$ then $\mathbf{u}$ and $\mathbf{v}$ are linearly dependent.

Next we check that is one of these vectors is a scalar multiple of the other, say, if $\mathbf{u} = c\mathbf{v}$, then $\mathbf{u}$ and $\mathbf{v}$ are linearly dependent. Indeed, in this case we have $1 \cdot \mathbf{u} - c \cdot \mathbf{v} = \mathbf{0}$.

Conversely, suppose that $\mathbf{u}$ and $\mathbf{v}$ are linearly dependent, i.e., $a\mathbf{u} + b\mathbf{v} = \mathbf{0}$ for some scalars a and b such that one of the is non-zero. Consider two cases.

(i) $b = 0$. In this case $a \neq 0$ and thus $\mathbf{u} = 0$.

(ii) $b \neq 0$. In this case $\mathbf{v} = \dfrac{a}{b}\mathbf{u}$ is a scalar multiple of $\mathbf{u}$.

(3) Problem 4.5.

Solution: (a) After renumbering the vectors, we may assume that $i = 1$. Let c be a non-zero element of the field F_q. We need to show that

(i) $\mathrm{Span}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) = \mathrm{Span}(c \cdot \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$, and

(ii) $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ are linearly dependent if and only if $c \cdot \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ are linearly dependent.

To prove (i), recall that $\mathrm{Span}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$ consists of linear combinations

$$\mathbf{v} = s_1\mathbf{x}_1 + s_2\mathbf{x}_2 + \cdots + s_n\mathbf{x}_n\,,$$

where $s_1, \dots, s_n$ are elements of F_q. Any such $\mathbf{v}$ is a linear combination

$$\mathbf{v} = s_1c^{-1}(c \cdot \mathbf{x}_1) + s_2\mathbf{x}_2 + \cdots + s_n\mathbf{x}_n\,.$$

of $c\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$. Conversely, every linear combination

$$\mathbf{w} = t_1(c \cdot \mathbf{x}_1) + t_2\mathbf{x}_2 + \cdots + t_n\mathbf{x}_n$$

of $c \cdot \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ can be rewritten as a linear combination

$$\mathbf{w} = (t_1c) \cdot \mathbf{x}_1 + t_2\mathbf{x}_2 + \cdots + t_n\mathbf{x}_n$$

of $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$. This proves (i).

To prove (ii), assume that $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ are linearly dependent. That is,

$$s_1\mathbf{x}_1 + s_2\mathbf{x}_2 + \cdots + s_n\mathbf{x}_n = \mathbf{0}$$

for some $s_1, \dots, s_n$ in F_q, such that $(s_1, \dots, s_n) \neq (0, \dots, 0)$. Then

$$s_1c^{-1}(c \cdot \mathbf{x}_1) + s_2\mathbf{x}_2 + \cdots + s_n\mathbf{x}_n = \mathbf{0}$$

and $(s_1c^{-1}, s_2, \dots, s_n) \neq (0, 0, \dots, 0)$. This shows that if $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ are linearly dependent, then $c \cdot \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ are also linearly dependent.

Conversely, suppose $c \cdot \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ are linearly dependent, i.e.,

$$t_1(c \cdot \mathbf{x}_1) + t_2\mathbf{x}_2 + \cdots + t_n\mathbf{x}_n = \mathbf{0}$$

where at least one of the coefficients is non-zero. Then we can rewrite this identity as

$$(t_1 c) \cdot \mathbf{x}_1 + u_2 \mathbf{x}_2 + \cdots + t_n \mathbf{x}_n = \mathbf{0}\,.$$

Since $c \neq 0$, at least one of the coefficients $ct_1, t_2, \ldots, t_n$ is non-zero We conclude that if $c \cdot \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ are linearly dependent, then $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ are also linearly dependent, as claimed.

(b) After renumbering the vectors if necessary, we may assume that $i = 1$ and $j = 2$. We need to show that $\mathbf{y_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ form a basis of C, where $\mathbf{y_1} = \mathbf{x_1} + a\mathbf{x_2}$. Since we know that $\dim(C) = k$, it suffices to show that $\mathbf{y_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ span C. Indeed, we can write any given $\mathbf{c} \in C$ as a linear combination of the basis vectors $\mathbf{x_1}, \ldots, \mathbf{x_k}$:

$$\mathbf{c} = a_1 \mathbf{x_1} + a_2 x_2 + \cdots + a_k \mathbf{x_k}\,.$$

Substituting, $\mathbf{x_1} = \mathbf{y_1} - a\mathbf{x_2}$, we see that

$$\mathbf{c} = a_1 \mathbf{y_1} + (a_2 - a a_1)\mathbf{x_2} + \cdots + a_k \mathbf{x_k}$$

is a linear combination of $\mathbf{y_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$. In other words, $\mathbf{y_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ span C.

(4) Let C be the vector subspace of $V(4,5) = (F_5)^4$ spanned by $(1,1,1,1)$, $(1,2,0,3)$ and $(4,0,3,1)$. What is the dimension of C? Construct a generator matrix and a parity check matrix for C.

Solution: Reducing

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

to row echelon form, we obtain

$$A' = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 4 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Here all calculations were carried out mod 5. The row of zeros at the bottom of A' tells us that S is linearly dependent. C is the row space of A which is the same as the row space of A'. The first two rows of A' thus form a basis for C, yielding the generator matrix

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

The dimension of C is the number of rows of G. Here $\dim(C) = 2$.

To construct the parity check matrix, we further reduce G' to standard form,

$$G' = \begin{pmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 4 & 2 \end{pmatrix}.$$

Once again all calculations here were carried out mod 5. Now we can readily construct the parity check matrix. Remembering that $-2 = 3$ and $-4 = 1$ in F_5, we obtain

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

(5) Find a generator matrix and a parity check matrix for the ISBN code.

Solution: Denote the ISBN code by $C \subset V(10,11)$. C is defined by the parity check matrix

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

We will view it as a generator matrix for the dual code $C^\perp$. It is in standard form, with the 1×1 identity matrix on the left. Thus we can use the formula given by Theorem 7.6 to obtain a parity check matrix for $C^\perp$ or equivalently, a generator matrix for C:

$$G = \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -7 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 8 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that generator and parity check matrices are not unique, so other answers are possible.

(6) (a) For which prime numbers q is $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$, a generator matrix for a q-ary linear code C in $V(6,q)$?

(b) If G is a generator matrix for C, determine whether or not the following words lie C: (1 0 1 0 1 0)? (1 1 2 2 3 3)?

Solution: G is a generator matrix for a code C if and only if the rows of G are linearly independent. Let R_1, R_2 and R_3 be the rows of G. If $q = 2$ then $R_1 + R_2 + R_3 = (2,2,2,2,2,2) = (0,0,0,0,0,0)$ and so G is not a generator matrix for any linear code.

If $q \neq 2$, then using row operations, we reduce G to the reduced row echelon form $G' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$, This matrix has a leading term in each row. Hence the rows of G' are linearly independent, and so are the rows of G. Thus for $q \neq 2$, G is a generator matrix.

Moreover, C is the span of the rows of G', i.e., consists of all vectors of the form (a,a,b,b,c,c), where a, b and c lie in F_q. In particular, (1 1 2 2 3 3) lies in C and (1 0 1 0 1 0) does not.

(7) Which of the following codes in F_q^n are linear? For each linear code find a generator matrix and a parity check matrix.

(a) $C_1 = \{(0000), (1111), (1010), (0101)\}, q = 2, n = 4$

(b) $C_2 = \{(0000), (1111), (1010), (0101)\}, q = 3, n = 4$

(c) $C_3 = \{(000), (111), (222)\}, q = 3, n = 3$

Solution: (a) Yes, C_1 is the span of $\mathbf{a} = (1010)$ and $\mathbf{b} = (0101)$.

(b) No. The number of words in a linear code over F_3 should be a power of 3. Another way to see that C_2 is not a linear code, is to notice that (1111) is in C_2 but $2 \cdot (1111)$ is not.

(c) Yes, C_3 is the span of (111).

(8) For each of the following subsets S of $V(n,q) = F_q^n$, find a basis for, and the dimension of, the span of S. Also, determine if the given S is linearly independent.

(a) $S = \{1100, 1010, 1001, 0101\}, q = 2, n = 4$

(b) $S = \{1234, 3142, 2413, 4321\}, q = 5, n = 4$

(c) $S = \{0140, 4322, 1233, 2141\}, q = 5, n = 4$

Solution: (a) Reducing

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

to row echelon form, we obtain

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

The row of zeros at the bottom of A' shows that S is not linearly independent. The span of S is 3-dimensional; the first three (non-zero) rows of A' form a basis.

(b) The last three vectors are scalar multiples of the first. Thus S is linearly dependent, and Span(S) is a 1-dimensional vector space with basis $\{(1234)\}$.

(c) Once again, we row reduce

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

to row echelon form. Start by interchanging the first and the third rows, then clear the non-zero entry under the pivots in colmn 1 and 2 to obtain

$$A' = \begin{pmatrix} 1 & 2 & 3 & 3 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Once again, the zero rows at the bottom of A' indicate that S is not linearly independent. Span(S) = row space of A = row space of A' is 2-dimensional; the non-zero rows of A' form a basis of this space.