Coding Theory

Sheet 4 Solutions

Spring and Summer 2010

1. In each case, use row operations to get the matrix in upper-triangular form with 1's as far as possible down the main diagonal.

   (a)

$$\begin{matrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{matrix} \rightarrow \begin{matrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{matrix} \rightarrow \begin{matrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{matrix} \rightarrow \begin{matrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

   Hence the subspace has dimension 3.

   (b)

$$\begin{matrix} 1 & 2 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 2 & 1 & 2 \end{matrix} \rightarrow \begin{matrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 \end{matrix} \rightarrow \begin{matrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 \end{matrix} \rightarrow \begin{matrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

   Hence the subspace has dimension 3.

2. To choose a $k-$dimensional subspace, choose k linearly independent vectors to form a basis $\{v_1, \ldots, v_k\}$.

   (a) A non-zero vector v_1 in $V(n, q)$ can be chosen in $q^n - 1$ ways.

   (b) To choose v_2 independent of this, no vector λv_1 can be chosen. Hence there are $q^n - q$ choices for v_2.

   (c) A vector independent of these can be chosen in $q^n - q^2$ ways.

   (d) Continue with this as far as v_k which can be chosen in $q^n - q^{k-1}$ ways.

   So the number of ordered sets of k linearly independent vectors is

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{k-1}).$$

However, the number of ordered sets of k vectors that will give the same subspace is, in the same way,

$$(q^k-1)(q^k-q)\dots(q^k-q^{k-1}).$$

Hence the number of $k-$dimensional subspaces is

$$\begin{aligned}&\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}\\ &= \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}.\end{aligned}$$

3. Take the first four rows of the incidence matrix of the projective plane of order 2:

$$G = \begin{bmatrix} 1&1&0&1&0&0&0\\ 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1 \end{bmatrix} \rightarrow \begin{bmatrix} 1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1\\ 0&0&1&0&1&1&1\\ 0&0&0&1&1&0&1 \end{bmatrix}$$

by row operations only.

4.

$$G = \begin{bmatrix} 1&0&1&1&0&1\\ 1&1&0&1&0&0\\ 0&1&0&0&1&1 \end{bmatrix} \rightarrow \begin{bmatrix} 1&0&1&1&0&1\\ 0&1&1&0&0&1\\ 0&1&0&0&1&1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1&0&1&1&0&1\\ 0&1&1&0&0&1\\ 0&0&1&0&1&0 \end{bmatrix} \rightarrow \begin{bmatrix} 1&0&0&1&1&1\\ 0&1&0&0&1&1\\ 0&0&1&0&1&0 \end{bmatrix}$$

using only row operations.

5. For the ternary $[7,4]$ code,

$$G = \begin{bmatrix} 2 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 & 0 \\ 2 & 1 & 0 & 2 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 & 0 & 2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 0 \\ 0 & 2 & 0 & 1 & 1 & 2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 2 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 0 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 2 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 0 \end{bmatrix}$$

again just using row operations to preserve the code.

6. By row operations,

$$G = \begin{bmatrix} 1 & 0 & 3 & 5 & 4 \\ 0 & 0 & 2 & 3 & 5 \\ 2 & 1 & 0 & 3 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 3 & 5 & 4 \\ 0 & 0 & 2 & 3 & 5 \\ 0 & 1 & 1 & 0 & 6 \\ 0 & 1 & 4 & 2 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 3 & 5 & 4 \\ 0 & 1 & 1 & 0 & 6 \\ 0 & 0 & 2 & 3 & 5 \\ 0 & 1 & 4 & 2 & 3 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 0 & 3 & 5 & 4 \\ 0 & 1 & 1 & 0 & 6 \\ 0 & 0 & 2 & 3 & 5 \\ 0 & 0 & 3 & 2 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 3 & 5 & 4 \\ 0 & 1 & 1 & 0 & 6 \\ 0 & 0 & 1 & 5 & 6 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 3 & 0 & 4 \\ 0 & 1 & 1 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Note In this example, as well as the previous ones, it is easy to check if your answer is correct. Is every row of G a linear combination of the rows of the answer $[I_k\, A]$?

7. If $G = [I_k\, A]$ and $G' = [I_k\, A']$, where the rows of A' are a permutation of the rows of A, then first permute the rows of G' so that A' becomes A; that is, we now have $G'' = [P\, A]$, where P is a *permutation* matrix, with a single 1 in each row and column, and other entries 0. Now permute the columns of P to obtain I_k. Thus, by row and column operations G' becomes G. Hence the code C' generated by G' is equivalent to the code C generated by G.

8. Here,

$$x = x_1 x_2 \ldots x_n \in C \Longrightarrow x' = x_1 x_2 \ldots x_n x_{n+1} \in C',$$

where

$$x_{n+1} = \begin{cases} 1 & \text{if } w(x) \text{ is odd,} \\ 0 & \text{if } w(x) \text{ is even.} \end{cases}$$

Let

$$\begin{aligned} C_0 &= \{x_1 x_2 \ldots x_{n+1} \in V(n+1,2) \mid x_1 x_2 \ldots x_n \in C; x_{n+1} \in \mathbf{F}_2\}, \\ C_1 &= \{x_1 x_2 \ldots x_{n+1} \in V(n+1,2) \mid x_1 + x_2 + \ldots + x_n + x_{n+1} = 0\}. \end{aligned}$$

Then C_0 and C_1 are both subspaces of $V(n+1,2)$, and $C' = C_0 \cap C_1$. Hence C' is a subspace.

Aliter

The weight of x in $V(n,2)$ is $w(x) = \sum_1^n x_i$. Hence, for $x, y \in V(n,2)$,

$$w(x+y) = \sum (x_i + y_i) = \sum x_i + \sum y_i = w(x) + w(y) \pmod 2.$$

To check that C' is linear, only one condition is required: $x', y' \in C' \Rightarrow x' + y' \in C'$. There are three cases.

(a) $w(x)$ even, $w(y)$ even; then $w(x+y)$ is even. So

$$(x+y)' = (x_1 + y_1, \ldots, x_n + y_n, 0) = (x_1, \ldots, x_n, 0) + (y_1, \ldots, y_n, 0) = x' + y'.$$

So the mapping is linear in this case.

(b) $w(x)$ odd, $w(y)$ odd; then $w(x+y)$ is even. So

$$(x+y)' = (x_1 + y_1, \ldots, x_n + y_n, 0) = (x_1, \ldots, x_n, 1) + (y_1, \ldots, y_n, 1) = x' + y'.$$

So the mapping is also linear in this case.

(c) $w(x)$ odd, $w(y)$ even; then $w(x+y)$ is odd. So

$$(x+y)' = (x_1 + y_1, \ldots, x_n + y_n, 1) = (x_1, \ldots, x_n, 1) + (y_1, \ldots, y_n, 0) = x' + y'.$$

So the mapping is linear in this final case.