Trondheim, June 3, 2013

TMA4185 Coding Theory – answers

For most problems, many other arguments are possible. For several problems, other answers are also possible.

Problem 1

a. Gaussian elimination (add rows I and II to III and row I to IV; swap rows III and IV; back substitution) gives us

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

The dimension of the code is 4.

b. Given G, the transpose of a parity check matrix is

$$H^T = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

No two rows in the parity check matrix sum to zero, so the minimum distance is greater than two. The third row in the generator matrix has weight 3. It follows that the minimum distance is 3.

c. It is obvious that ν is a linear map. Therefore, the image of a subspace is again a subspace, and $\nu(\mathcal{D})$ is a linear code.

Now consider the restriction $\nu|_{\mathcal{D}}$. We know that the kernel of $\nu|_{\mathcal{D}}$ must be contained in the kernel of ν, which has dimension 1. The kernel of $\nu|_{\mathcal{D}}$ therefore has dimension 0 or 1, and its image therefore has the same dimension as $\mathcal{D}$ or 1 lower.

Since the map ν just discards the fifth coordinate, any codeword with a 1 in its fifth coordinate will map to a codeword with weight one less, while any other codeword will map to a codeword with the same weight. If there is a minimal-weight codeword in $\mathcal{D}$ with a 1 in its fifth coordinate, then its image under ν will have weight one less, and the minimum distance of $\nu(\mathcal{D})$ will be one less than the minimum distance of $\mathcal{D}$. Otherwise, their minimum distances will be the same.

We see that $\mathcal{C}$ has no codewords in the kernel of ν, so the dimension of $\nu(\mathcal{C})$ is 4. The third row of G has weight 3 and a 1 in its fifth coordinate, so it will map to a codeword with weight 2. The minimum distance is therefore 2.

d. If we add two vectors with 0 in their fifth coordinate, the fifth coordinate in the sum is also 0. It follows that $\mathcal{D}'$ is closed under addition and multiplication with scalars, so $\mathcal{D}'$ is a subspace.

If there are no codewords in $\mathcal{D}$ with a 1 in the fifth coordinate, $\mathcal{D}'$ will contain the same vectors as $\mathcal{D}$ and have the same dimension.

Suppose there is at least one codeword with a 1 in its fifth coordinate. Now there will be vectors in $\mathcal{D}$ that are not in $\mathcal{D}'$, so the dimension will be lower. Let $\vec{v}_1, \ldots, \vec{v}_k$ be a basis for $\mathcal{D}$. If there is exactly one vector that has a 1 in its fifth coordinate, we are done. Otherwise, choose one vector with a 1 in its fifth coordinate and add it to all the other vectors with a one in their fifth coordinate, to get $\vec{u}_1, \ldots, \vec{u}_{k-1}$. It is obvious that these new vectors are linearly independent, that they are all in $\mathcal{D}'$ and therefore that the dimension of $\mathcal{D}'$ is $k-1$, one lower than the dimension of $\mathcal{D}$.

Applying the map ν to $\mathcal{D}'$ and using the arguments from the previous problem, we see that the dimension of $\nu(\mathcal{D}')$ is the same as the dimension of $\mathcal{D}'$. The minimum distance of $\nu(\mathcal{D}')$ is the same as the minimum distance of $\mathcal{D}'$, which is again the same as $\mathcal{D}$.

Problem 2

a. The dimension is 5 because the generating polynomial has degree 3, the minimum distance is 4 because there are three consecutive zeros in the generating polynomial.

b. We know that $y(x) = c(x) + e_j x^j$ for some e_j. Also,

$$y(\alpha) = c(\alpha) + e_j \alpha^j = e_j \alpha^j \qquad \text{and} \qquad y(\alpha^2) = c(\alpha^2) + e_j \alpha^{2j} = e_j \alpha^{2j}.$$

In other words,

$$y(\alpha^2) = y(\alpha)\alpha^j.$$

A quick computation shows that $y(\alpha^2)/y(\alpha) = 2\alpha + 1 = \alpha^2$, which means that the error was in the x^2-term.

Problem 3

a. The encoding of $m(x) = 1 + x^3 + x^6 + x^7$ is

$$\mathbf{c}(x) = (x^{10} + x^5 + x^4 + x^2 + x + 1, x^{10} + x^9 + x^7 + 1).$$

b. We could use the extended Euclidian algorithm, but is is faster to observe that $(x^2+1) + (x^2+x+1) = x$, $x(x^2+1) + x(x^2+x+1) = x^2$ and $(x+1)(x^2+1) + x(x^2+x+1) = 1$. We get $a(x) = x+1$ and $b(x) = x$.

c. First note that

$$GM = G \begin{bmatrix} a(x) \\ b(x) \end{bmatrix} = a(x)(x^3 + x^2 + x + 1) + b(x)(x^3 + 1).$$

If M is a right-inverse, then the above expression is 1. It is easy to compute that the greatest common divisor of the two elements of G is $x+1$, which means that with polynomials $a(x)$ and $b(x)$, the above expression must be a multiple of $x + 1$ and therefore cannot be 1.

If we allow power series, one right inverse is

$$M = \begin{bmatrix} 1 \\ x/(x+1) \end{bmatrix}.$$

d. Over the field, we can divide G by the "constant" $x+1$ without changing the image, to get

$$G' = \begin{bmatrix} x^2 + 1 \\ x^2 + x + 1 \end{bmatrix}.$$

Now

$$\begin{bmatrix} x+1 \\ x \end{bmatrix}$$

is a right-inverse with polynomial entries.