Exam TMA4185 Cryptography

Suggested solutions

June 11, 2016

Problem 1

a.

We build a 4×6 matrix and proceed using Gaussian elimination to find a linearly independent set of rows, which will be our generator matrix:

$$\begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 & 2 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We find three linearly independent rows, which means that the code has dimension 3 and one generator matrix is

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

b.

It is clear from the calculations in the previous problem that no generator matrix on standard form exists. However, we can go from the generating matrix we got above to a generator matrix for a permutation equivalent code by multiplying two rows by 1, then taking the columns in the order $(1,3,5,2,4,6)$, and finally completing the Gaussian elimination:

$$\begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 2 \end{pmatrix}$$

From the generator matrix on standard form, we trivially get a parity check matrix

$$H_0^T = \begin{pmatrix} 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

for the permutation-equivalent code. To get a parity check matrix for $\mathscr{C}$, we invert the permutation and get

$$H^T = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

c.

Our generator matrix G contains a row of weight 3, so the minimum distance cannot be greater than 3.

We see that no row of H is zero, so there will be no code words of weight 1. We see that no two rows of H sum to zero, so there will be no code words of weight 2.

The minimum distance is 3.

A code is perfect if it satisfies the sphere bound, and a quick calculation shows that

$$3^3 = 27 \neq \frac{3^6}{1 + \binom{6}{1} \cdot 2} = \frac{3^6}{1 + 6 \cdot 2}.$$

The code is not perfect.

A linear MDS code satisifies the linear singleton bound $k \leq n - d + 1$, but since $3 < 6 - 3 + 1$, our code is not an MDS code.

d.

Since the errors of weight one all consist of vectors with a single 1 or 2, the table consists of all the rows of H and all the rows of H multiplied by 2.

We compute $(1,0,1,2,1,1)H = (2,0,0)$, which corresponds to twice the second row in H, which means that the error is $(0,2,0,0,0,0)$. The nearest code word is then $(1,1,1,2,1,1)$.

e.

The definition can be found in the textbook.

Without loss of generality, we can consider the puncture to be in the last coordinate. Consider two code words $\mathbf{x} = (x_1, x_2, \ldots, x_{n-1})$ and $\mathbf{y} = (y_1, y_2, \ldots, y_{n-1})$ in the punctured code. By the definition of punctured code, x_n and y_n exist such that $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ are in the code. Then for any $a \in \mathbb{F}$, $(ax_1, \ldots, ax_n)$ and $(x_1 + y_1, \ldots, x_n + y_n)$ are also in the code, so $(ax_1, \ldots, ax_{n-1})$ and $(x_1 + y_1, \ldots, x_{n-1} + y_{n-1})$ will be in the punctured code. Hence, the punctured code is linear.

The generator matrix we found above contains a code word of weight three with a non-zero value in the fourth coordinate. Hence, the punctured code will have minimum distance 2.

For the punctured code to have fewer code words than the original code, there must be two code words in the original code that only differ in the fourth coordinate. But the original code has minimum distance 3, so the punctured code still has dimension 3.

Problem 2

a.

The code has dimension 3. We know that such a code with 4 consecutive zeros has minimum distance at least 5, which means that the code can correct up to two errors.

This is a Reed-Solomon code which is an MDS code (since $5 = 7 - 3 + 1$), for which any set of three coordinates is an information set, so it can correct up to 4 erasures.

After a tedious calculation we find that

$$g(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4) = X^4 + \alpha^2 X^3 + \alpha^3 X^2 + X + \alpha^3.$$

b.

We know that any code word $c(X) = \sum c_i X^i$ can be expressed as $g(X)m(X)$, where $m(X)$ is a polynomial of degree at most 2, that is, $m(X) = m_0 + m_1 X + m_2 X^2$. Comparing coefficients in front of X, X^4 and X^5, we get the following system of equations:

$$\begin{aligned} \alpha^2 &= m_1 + m_2\alpha^2 \\ \alpha^2 &= m_0 + m_1\alpha^2 + m_2\alpha^2 \\ 1 &= m_0 + m_1\alpha^3 \end{aligned}$$

Linear algebra follows:

$$\begin{pmatrix} 0 & 1 & \alpha^2 & \alpha^2 \\ 1 & \alpha^2 & \alpha^3 & \alpha^2 \\ 1 & \alpha^3 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha^3 & \alpha^3 \\ 1 & \alpha^3 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & \alpha^2 & \alpha^2 \\ 0 & 0 & 1 & 1 \\ 1 & \alpha^3 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & \alpha^3 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

from which it follows that $m_0 = 1$, $m_1 = 0$ and $m_2 = 1$.

Finally, we see that the coefficient in front of X^6 is $m_2 = 1$, while the constant term is $\alpha^3 m_0 = \alpha^3$.

Problem 3

The Gilbert bound says that a linear code exists with not less than

$$\frac{8^{35}}{1 + \binom{35}{1}\cdot 7 + \binom{35}{2}\cdot 7^2 + \binom{35}{3}\cdot 7^3 + \binom{35}{4}\cdot 7^4 + \binom{35}{5}\cdot 7^5 + \binom{35}{6}\cdot 7^6} \approx 8^{22.5}$$

code words. (An exact calculation may be a bit tricky on an ordinary calculator, but it is clear that the final term dominates the sum and therefore the logarithm, which is sufficient for our purposes.)

So we know that a code of dimension 23 exists. (Bigger codes exist, so other answers would also work.)

Furthermore $8^{22.5} > 2^{28}$.

(Strictly speaking, there was a mistake in the problem text, where 2^{28} should have been 8^{28}. In that case, the sphere packing bound would have shown that such a code was impossible. However, with the mistake, the Gilbert bound is sufficient to answer both questions, so there was no need to correct the text.)

Problem 4

a.

The two polynomials have $1+D$ as a common factor, which means that it is a catastrophic encoder.

A better encoder is $(1+D, 1+D+D^3)$. Encoding 101100 corresponding to $1+D^2+D^3$ gives us

$$(1+D)(1+D^2+D^3) = 1+D+D^2+D^4,$$
$$(1+D+D^3)(1+D^2+D^3) = 1+D+D^2+D^3+D^4+D^5+D^6.$$

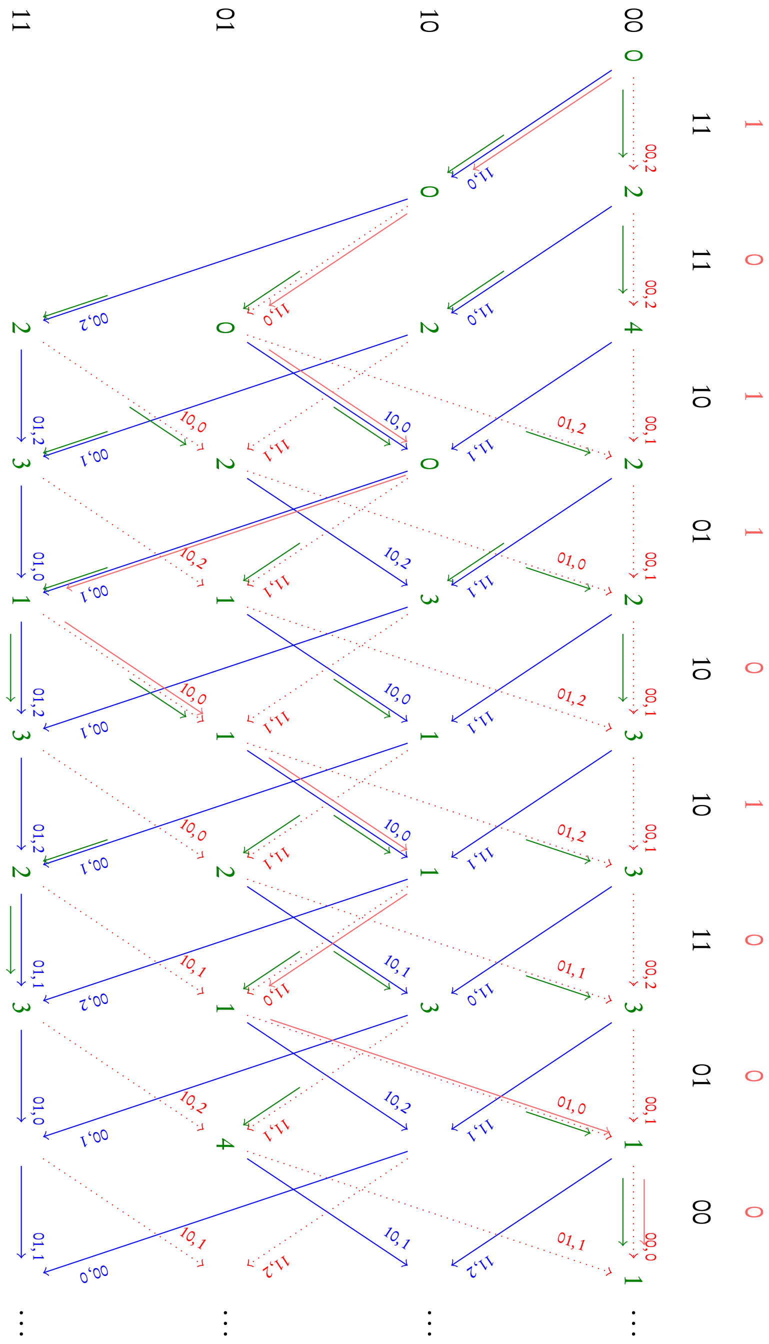
We get 11111101110101.

If you use a state machine or circuit diagram to encode, you do not get the final two bits, since the encoder does not return to its all-zero state.

Either method is ok.

b.

We use the following Trellis diagram. The received bits are written along the top of the diagram. The weight of each edge is indicated above the edge. The numbers in green indicate the minimum weight of a path to that state, while the green arrows indicate where the minimum weight path came from (where there are multiple paths, only one is indicated). The minimum weight path that ends with two zeros is indicated by pink arrows, and the corresponding message is written in pink above the diagram.



00
10
01
11
11
11
10
01
10
10
11
01
00
1
0
1
1
0
1
0
0
0