Topics in Coding Theory Date of Lecture: 10th March 2021

Lecture 13: Quiz-1 and solutions

Instructor: Dr. Prasad Krishnan *Scribe: Srikar kale*

1 Questions

1 Questions*

(7+13)

1. The dual (or orthogonal) code $\mathcal{C}^{\perp}$ of a $[n,k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is the set of all vectors of $\mathbb{F}_q^n$ which are orthogonal to $\mathcal{C}$, i.e.,

$$\mathcal{C}^{\perp} = \{\underline{v} \in \mathbb{F}^n : \underline{c}.\underline{v}^T = 0\}.$$

It is easy to see that $\mathcal{C}^{\perp}$ is linear and that its dimension is $n-k$. Using the generator matrix of $\mathcal{C}$, show that if $\mathcal{C}$ is an MDS code, then so is $\mathcal{C}^{\perp}$. *(Hint: You can ask me privately for a hint with penalty of 3 marks).*

2. Consider the $[4,2]$ Reed Solomon code over $\mathbb{F}_4$. Obtain the codeword corresponding to the message vector $(1,\alpha)$ where α is primitive in $\mathbb{F}_4$. Assume error in one position *(send me a message privately for which position you have to assume the error in)* when this codeword is transmitted, and run through the algorithm (you have to solve each step) according to the Berlekamp Welch algorithm to decode this.

2 Solutions

2.1 Solution for Question 1

The dual code of a linear MDS code is again a linear MDS code. In other words, the dual of every linear $[n,k,n-k+1]$-code is a linear $[n,n-k,k+1]$ -code over the same field. A code is an MDS code if it meets the Singleton bound with equality, i.e., $d = n-k+1$.

If $C = [n,k,d]_q$ code over F_q, the dual of the code is the set $C^{\perp} = \{x \in F_q^n | \forall y \in C, < x,y >= 0\}$ where $< x,y >$ is the standard dot product. Because $C^{\perp}$ is the space of elements perpendicular to C, the dimension of $C^{\perp}$ is $n-k$. Thus $C^{\perp} = [n,n-k,d]_q$.

Lemma: If G is the generator matrix for C and H is the parity check matrix, then G^T is the parity check matrix for $C^{\perp}$ and H^T is the generator matrix.

Proof: Let x be an element of our message space. We note that the space spanned by xH^T has the right number of dimensions to be a candidate for the space $C^{\perp}$, and $H^T G^T = (GH)^T = 0$. It remains to show that $xH^T, x^{'}G$ are perpendicular for all $x, x^{'}$ in the message space. However,$< xH^T, x^{'}G >= xH^T G^T x^{'} = x(GH)^T x^{'} = 0$ completing the proof of our lemma.

Suppose C is a code with generator matrix G with columns $c_1, c_2, ...c_n$.This is a k by n matrix. Note that in an MDS code, every linear combination of the rows has Hamming weight at least n - k + 1. By the above lemma, $C^{\perp}$ has G^T as its parity check matrix. We wish to show now that if $C = [n, k, n-k+1]$ code, then $C^{\perp} = [n, n-k+1, k+1]$ code. That is,every subset of k columns of G, the generator matrix, is linearly independent.

Suppose that some k columns are linearly dependent. Consider the k by k sub matrix M formed by these columns. Since the columns are linearly dependent, the rank of M is less than k so the rows of M have some linearly dependence. Therefore there exists some linear combination of the rows of M that sums to 0, so we can use this same linear combination on the rows of G whose sum has at least k 0's, and thus has Hamming weight $\leq n-k$. But we've established that any linear combination of the rows of G in an MDS code must have Hamming weight at least n - k + 1. Contradiction.

2.2 Solution for question 2

Given: [4, 2] RS code, finite field $\mathbb{F}_4$, message vector $(1, \alpha)$ where α is a primitive element of $\mathbb{F}_4$. Error position: 3 (can be any 1 position)

Defining e = number of errors (e = 1), the key set of n equations is

$$y_i E(a_i) = E(a_i) M(a_i) \tag{1}$$

Where $E(a_i) = 0$ for the e cases when $y_i \neq M(a_i)$, and $E(a_i) \neq 0$ for the n - e non error cases where $y_i = M(a_i)$. These equations can't be solved directly, but by defining N() as the product of E() and M():

$$N(a_i) = E(a_i) M(a_i) \tag{2}$$

and adding the constraint that the most significant coefficient of $E(a_i) = e_e = 1$, the result will lead to a set of equations that can be solved with linear algebra.

$$y_i E(a_i) = N(a_i) \tag{3}$$

$$y_i E(a_i) - N(a_i) = 0 \tag{4}$$

$$y_i(e_0 + e_1 a_i + e_2 a_i^2 + \cdots + e_e a_i^e) - (n_0 + n_1 a_i + n_2 a_i^2 + \cdots + n_q a_i^q) = 0 \tag{5}$$

where $q = n - e - 1$. Since e_e is constrained to be 1, the equations become:

$$y_i(e_0 + e_1 a_i + e_2 a_i^2 + \cdots + e_{e-1} a_i^{e-1}) - (n_0 + n_1 a_i + n_2 a_i^2 + \cdots + n_q a_i^q) = -y_i a_i^e \tag{6}$$

resulting in a set of equations which can be solved using linear algebra, with time complexity $O(n^3)$.

The elements of $F_4 = \{0, 1, \alpha, \alpha + 1\}$

$$\begin{bmatrix} 1 & \alpha \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix} = \begin{bmatrix} 1 & \alpha+1 & 1+\alpha^2 & 1+\alpha^3 \end{bmatrix} \tag{7}$$

The transmitted code word is

$$c = \begin{bmatrix} 1 & \alpha^2 & \alpha & 0 \end{bmatrix} \tag{8}$$

Let the received code word be (error in position 3)

$$y = \begin{bmatrix} 1 & \alpha^2 & 1 & 0 \end{bmatrix} \tag{9}$$

Using the formula given above, $q = n - e - 1, q = 2, e = 1$, $E(X) = e_0 + X$ as given by the above constraint $e_1 = 1$, $N(X) = n_0 + n_1 X + n_2 X^2$

From here,

$$1(e_0 + 0) = n_0 \tag{10}$$

$$\alpha^2(e_0+1) = n_0 + n_1 + n_2 \tag{11}$$

$$1(e_0+\alpha) = n_0 + n_1\alpha + n_2\alpha^2 \tag{12}$$

$$0(e_0+\alpha^2) = n_0 + n_1\alpha^2 + n_2\alpha^4 = n_0 + n_1\alpha^2 + n_2\alpha^1 \tag{13}$$

Unknowns here are e_0, n_0, n_1, n_2 and we have 4 equations here. Writing them in row echelon form, we get,

$$\begin{bmatrix} 0 & 0 & 1 & -1 \\ 1 & 1 & 1 & -\alpha^2 \\ \alpha^2 & \alpha & 1 & -1 \\ \alpha & \alpha^2 & 1 & 0 \end{bmatrix} \begin{bmatrix} n_2 \\ n_1 \\ n_0 \\ e_0 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha^2 \\ \alpha \\ 0 \end{bmatrix} \tag{14}$$

This can be written as an augmented matrix such as,

$$\begin{bmatrix} 0 & 0 & 1 & -1 & 0 \\ 1 & 1 & 1 & -\alpha^2 & \alpha^2 \\ \alpha^2 & \alpha & 1 & -1 & \alpha \\ \alpha & \alpha^2 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} n_2 \\ n_1 \\ n_0 \\ e_0 \end{bmatrix} \tag{15}$$

Finding the reduced row echelon form of the augmented matrix will give us the solution for the 4 variables

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \frac{\alpha^3+\alpha^2-\alpha-1}{\alpha^4+\alpha^3-\alpha^2-\alpha+1} \\ 0 & 1 & 0 & 0 & \frac{1}{\alpha^4+\alpha^3-\alpha^2-\alpha+1} \\ 0 & 0 & 1 & 0 & -\frac{\alpha\left(\alpha^3+\alpha^2-1\right)}{\alpha^4+\alpha^3-\alpha^2-\alpha+1} \\ 0 & 0 & 0 & 1 & -\frac{\alpha\left(\alpha^3+\alpha^2-1\right)}{\alpha^4+\alpha^3-\alpha^2-\alpha+1} \end{bmatrix} \tag{16}$$

we know, $\alpha^4 = \alpha, \alpha^3 = 1$, and then by simplifying the last column of the reduced row echelon matrix using modulo $1+\alpha+\alpha^2$ (our irreducible polynomial), we get:

$$n_2 = n_0 = e_0 = n_1 = \alpha \tag{17}$$

From this, we can write

$$N(X) = \alpha X^2 + \alpha X + \alpha, E(X) = X + \alpha, M(X) = \frac{\alpha X^2 + \alpha X + \alpha}{X + \alpha} \tag{18}$$

$$M(X) = \alpha X + \alpha + \alpha^2 \tag{19}$$

Verification step:
$E(X) = 0$ only when $X = \alpha$
$M(0) = \alpha + \alpha^2 = 1$
$M(1) = \alpha^2 = 1 + \alpha$
$M(\alpha) = \alpha$
$M(\alpha^2) = 0$
We can see that the code word c $= [M(0)M(1)M(\alpha)M(\alpha^2)]$