

Math 55 — Discrete Mathematics — Spring 2003

Quiz 7 Solutions

(a) Write out the code matrix for the single-error correcting Reed-Solomon code over \mathbb{Z}_5 with 3 message symbols and 5 code symbols.

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

(b) Using this code, you receive the vector $\mathbf{r} = [2 \ 3 \ 2 \ 1 \ 4]$ (version 1) or $[1 \ 1 \ 4 \ 2 \ 1]$ (version 2). Find a solution of the key equation

$$Q(i) = \mathbf{r}_i E(i), \quad i = 0, 1, \dots, 4$$

with $\deg E(t) \leq 1$, $\deg Q(t) \leq 3$.

For reference, here are the polynomials $C_k(t) = t(t-1)\cdots(t-k+1)/k!$ expanded out (mod 5):

$$\begin{aligned} C_0(t) &= 1 \\ C_1(t) &= t \\ C_2(t) &= 2t + 3t^2 \\ C_3(t) &= 2t + 2t^2 + t^3 \end{aligned}$$

Following the improved method, make difference tables (mod 5) for the sequences \mathbf{r}_i and $i\mathbf{r}_i$. I'll do version 1 in detail and give the corresponding results for version 2 afterwards.

$$\begin{array}{cccccc} 2 & 3 & 2 & 1 & 4 & & 0 & 3 & 4 & 3 & 1 \\ 1 & 4 & 4 & 3 & & & 3 & 1 & 4 & 3 & \\ 3 & 0 & 4 & & & & 3 & 3 & 4 & & \\ 2 & 4 & & & & & 0 & 1 & & & \\ 2 & & & & & & 1 & & & & \end{array},$$

The matrix equation for the unknown coefficients of $E(t) = v_0 + v_1 t$ comes from the last rows of the two difference tables:

$$\begin{bmatrix} 2 & 1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} = \mathbf{0}.$$

Taking $v_1 = 1$ and solving (mod 5) gives the solution $E(t) = t + 2$. To find $Q(t)$, make a difference table for the sequence $\mathbf{r}_i E(i)$:

$$\begin{array}{cccccc} 4 & 4 & 3 & 0 & 4 & \\ 0 & 4 & 2 & 4 & & \\ 4 & 3 & 2 & & & \\ 4 & 4 & & & & \end{array}$$

Then $Q(t) = 4C_0(t) + 0C_1(t) + 4C_2(t) + 4C_2(t) = 4 + t + 4t^3$.

In version 2, the equation for $E(t)$ is

$$\begin{bmatrix} 4 & 1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} = \mathbf{0},$$

giving $E(t) = t + 4$. The difference table for $\mathbf{r}_i E(i)$ is

$$\begin{array}{cccc} 4 & 0 & 4 & 4 & 3 \\ 1 & 4 & 0 & 4 & \\ 3 & 1 & 4 & & \\ 3 & 3, & & & \end{array}$$

so $Q(t) = 4C_0(t) + 1C_1(t) + 3C_2(t) + 3C_2(t) = 4 + 3t + 3t^3$.

(c) Where is the error and what were the transmitted code vector and the original message vector?

Version 1: The message polynomial is $P(t) = Q(t)/E(t) = 2 + 2t + 4t^2$, the message vector is $[2 \ 2 \ 4]$, the transmitted code vector was $[2 \ 3 \ 2 \ 4 \ 4]$, and the error is in \mathbf{r}_3 (the fourth symbol).

Version 2: The message polynomial is $P(t) = 1 + 3t + 3t^2$, the message vector is $[1 \ 3 \ 3]$, the transmitted code vector was $[1 \ 2 \ 4 \ 2 \ 1]$, and the error is in \mathbf{r}_1 (the second symbol)