EE/Ma 127b Error-Correcting Codes — R. J. McEliece
draft of January 3, 2001 — 162 Moore

Details of Class Project #1 (Version 1.0)
Due date: Midterms week

You (and/or your team; maximum of three students per team) are expected to produce a program capable of decoding the $(31, 15)$ RS code over GF(32). This code consists of all vectors $(C_0, \ldots, C_{30})$, with each $C_i \in \mathrm{GF}(32)$, such that

$$\sum_{i=0}^{30} C_i \alpha^{ij} = 0, \qquad \text{for } j = 1, 2, \ldots, 16,$$

where α is a primitive root in GF(32) satisfying $\alpha^5 = \alpha^2 + 1$. Assume that the first 15 characters $C_0, \ldots, C_{14}$ are the information characters, and the last 16 characters $C_{15}, \ldots, C_{30}$ are the parity-check characters.

I will test your program by giving it several garbled codewords of the form $(R_0, \ldots, R_{30})$, differing from a codeword by t_0 erasures and t_1 errors. If $2t_0 + t_1 \le 16$, your program should find the codeword; but if $2t_0 + t_1 > 16$, your program should output an appropriate error message.

I will encode the elements of GF(32) as integers in the range 0 to 31, with the integer 0 corresponding to [00000], 1 corresponding to [00001], ..., and 31 corresponding to [11111]. (Alternatively, you may wish to use an alphanumeric code. If so, please use the correspondence `A` $\to$ [`00000`], `B` $\to$ [`00001`], ..., `Z` $\to$ [`11001`], `1` $\to$ [`11010`], ..., `6` $\to$ [`11111`].)

As a partial check of the correctness of your program, you may find it helpful to know that the generator polynomial

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{16})$$

has the representation

$$g(x) = g_0 + g_1 x + \cdots + g_{16} x^{16}$$

where

$g_0 = 14$	$g_6 = 16$	$g_{12} = 13$
$g_1 = 3$	$g_7 = 20$	$g_{13} = 1$
$g_2 = 21$	$g_8 = 25$	$g_{14} = 28$
$g_3 = 15$	$g_9 = 24$	$g_{15} = 15$
$g_4 = 29$	$g_{10} = 2$	$g_{16} = 1$
$g_5 = 15$	$g_{11} = 8$	

Also, here is a table of the values of α^i and $g(\alpha^i)$, for $i = 0, 1, \ldots, 30$.

i	α^i	$g(a^i)$
0	1	20
1	2	0
2	4	0
3	8	0
4	16	0
5	5	0
6	10	0
7	20	0
8	13	0
9	26	0
10	17	0
11	7	0
12	14	0
13	28	0
14	29	0
15	31	0
16	27	0
17	19	6
18	3	1
19	6	11
20	12	26
21	24	20
22	21	18
23	15	17
24	30	1
25	25	23
26	23	1
27	11	30
28	22	7
29	9	29
30	18	8

Finally, here are five sample codewords $C^{(1)}, \ldots, C_i^{(5)}$:

i	$C_i^{(1)}$	$C_i^{(2)}$	$C_i^{(3)}$	$C_i^{(4)}$	$C_i^{(5)}$
0	3	14	29	31	14
1	2	21	16	6	1
2	21	20	18	19	22
3	8	17	8	11	18
4	20	0	17	1	28
5	24	15	12	5	26
6	10	2	23	2	27
7	13	6	6	5	23
8	31	29	25	21	21
9	19	5	8	0	30
10	8	1	18	6	5
11	30	10	28	31	27
12	16	31	19	4	22
13	28	1	31	24	19
14	18	15	15	10	11
15	17	11	28	11	13
16	6	8	26	28	14
17	7	1	11	5	15
18	20	6	8	26	28
19	29	7	1	11	5
20	18	20	6	8	26
21	3	29	7	1	11
22	0	18	20	6	8
23	25	3	29	7	1
24	30	0	18	20	6
25	31	25	3	29	7
26	12	30	0	18	20
27	21	31	25	3	29
28	10	12	30	0	18
29	27	21	31	25	3
30	24	10	12	30	0