

Project No. 2
Due 4:00pm, June 27, 2023

You are expected to produce a computer program capable of decoding the (63, 42) Reed-Solomon code over $\text{GF}(2^6)$, which was used in Cinema Digital Sound. This code consists of all vectors (C_0, \dots, C_{62}) , with each $C_i \in \text{GF}(2^6)$, such that

$$\sum_{i=0}^{62} C_i \alpha^{ij} = 0, \quad \text{for } j = 1, 2, \dots, 21$$

where α is a primitive element in $\text{GF}(2^6)$ satisfying $\alpha^6 + \alpha + 1 = 0$. Assume that the first 21 characters C_0, \dots, C_{20} are the parity-check characters, and the last 42 characters C_{21}, \dots, C_{62} are the information characters.

The deliverable will consist of three parts:

- **Part I, Demonstration.** At the time of demonstration, we will test your program by giving it several garbled codewords of the form (R_0, \dots, R_{62}) , differing from a codeword by t_0 erasures and t_1 errors. If $t_0 + 2t_1 \leq 21$, your program should find the codeword; but if $t_0 + 2t_1 > 21$, your program should output an appropriate failure message.

The elements of $\text{GF}(2^6)$ will be encoded as integers in the range 0 to 63, with integer 0 corresponding to [000000], 1 corresponding to [000001], 2 corresponding to [000010], ..., and 63 corresponding to [111111]. (Here $[a_5 a_4 a_3 a_2 a_1 a_0]$ corresponds to the element $a_5 \alpha^5 + a_4 \alpha^4 + a_3 \alpha^3 + a_2 \alpha^2 + a_1 \alpha + a_0$ in $\text{GF}(2^6)$.) An erasure will be represented by a * sign. The input to the program will be a file consisting of several garbled codewords in the following format:

```
45 63 * 0 2 ... 15    (the first garbled codeword)
...
13 0 5 * * ... 0      (the last garbled codeword)
```

- **Part II, Report.** When the project is due (and after the demonstration is passed), you need to hand in a *report* (in a hard copy), which should include, among other things, description of your project, discussions, etc. Your computer program *with comments* should be attached at the end of the report.
- **Part III, Program file.** You also need to submit, before the deadline, your program file. Please put all of your programs into a single file with your registration number and `proj2` as the file name, say, `105064851_proj2.c` or `105064851_proj2.cpp`. (If, after all kinds of attempts, you are still unable to put all of your programs in a single file, please compress your files into a single `rar` or `zip` file and use your registration number along with `proj2` as the file name, say, `105064851_proj2.rar` or `105064851_proj2.zip`.) Upload your file to the *ee*class system.

The coefficients of the generator polynomial for the (63, 42) RS code:

$g[0]=58$	$g[11]=43$
$g[1]=62$	$g[12]=44$
$g[2]=59$	$g[13]=27$
$g[3]=7$	$g[14]=7$
$g[4]=35$	$g[15]=53$
$g[5]=58$	$g[16]=39$
$g[6]=63$	$g[17]=62$
$g[7]=47$	$g[18]=52$
$g[8]=51$	$g[19]=41$
$g[9]=6$	$g[20]=44$
$g[10]=33$	$g[21]=1$

The values of the polynomial:

$\alpha^0 = 1$	$g(\alpha^0) = 34$	$\alpha^{32} = 9$	$g(\alpha^{32}) = 22$
$\alpha^1 = 2$	$g(\alpha^1) = 0$	$\alpha^{33} = 18$	$g(\alpha^{33}) = 20$
$\alpha^2 = 4$	$g(\alpha^2) = 0$	$\alpha^{34} = 36$	$g(\alpha^{34}) = 28$
$\alpha^3 = 8$	$g(\alpha^3) = 0$	$\alpha^{35} = 11$	$g(\alpha^{35}) = 17$
$\alpha^4 = 16$	$g(\alpha^4) = 0$	$\alpha^{36} = 22$	$g(\alpha^{36}) = 13$
$\alpha^5 = 32$	$g(\alpha^5) = 0$	$\alpha^{37} = 44$	$g(\alpha^{37}) = 19$
$\alpha^6 = 3$	$g(\alpha^6) = 0$	$\alpha^{38} = 27$	$g(\alpha^{38}) = 14$
$\alpha^7 = 6$	$g(\alpha^7) = 0$	$\alpha^{39} = 54$	$g(\alpha^{39}) = 56$
$\alpha^8 = 12$	$g(\alpha^8) = 0$	$\alpha^{40} = 47$	$g(\alpha^{40}) = 25$
$\alpha^9 = 24$	$g(\alpha^9) = 0$	$\alpha^{41} = 29$	$g(\alpha^{41}) = 45$
$\alpha^{10} = 48$	$g(\alpha^{10}) = 0$	$\alpha^{42} = 58$	$g(\alpha^{42}) = 10$
$\alpha^{11} = 35$	$g(\alpha^{11}) = 0$	$\alpha^{43} = 55$	$g(\alpha^{43}) = 46$
$\alpha^{12} = 5$	$g(\alpha^{12}) = 0$	$\alpha^{44} = 45$	$g(\alpha^{44}) = 45$
$\alpha^{13} = 10$	$g(\alpha^{13}) = 0$	$\alpha^{45} = 25$	$g(\alpha^{45}) = 8$
$\alpha^{14} = 20$	$g(\alpha^{14}) = 0$	$\alpha^{46} = 50$	$g(\alpha^{46}) = 12$
$\alpha^{15} = 40$	$g(\alpha^{15}) = 0$	$\alpha^{47} = 39$	$g(\alpha^{47}) = 14$
$\alpha^{16} = 19$	$g(\alpha^{16}) = 0$	$\alpha^{48} = 13$	$g(\alpha^{48}) = 44$
$\alpha^{17} = 38$	$g(\alpha^{17}) = 0$	$\alpha^{49} = 26$	$g(\alpha^{49}) = 14$
$\alpha^{18} = 15$	$g(\alpha^{18}) = 0$	$\alpha^{50} = 52$	$g(\alpha^{50}) = 17$
$\alpha^{19} = 30$	$g(\alpha^{19}) = 0$	$\alpha^{51} = 43$	$g(\alpha^{51}) = 26$
$\alpha^{20} = 60$	$g(\alpha^{20}) = 0$	$\alpha^{52} = 21$	$g(\alpha^{52}) = 31$
$\alpha^{21} = 59$	$g(\alpha^{21}) = 0$	$\alpha^{53} = 42$	$g(\alpha^{53}) = 22$
$\alpha^{22} = 53$	$g(\alpha^{22}) = 16$	$\alpha^{54} = 23$	$g(\alpha^{54}) = 59$
$\alpha^{23} = 41$	$g(\alpha^{23}) = 13$	$\alpha^{55} = 46$	$g(\alpha^{55}) = 29$
$\alpha^{24} = 17$	$g(\alpha^{24}) = 43$	$\alpha^{56} = 31$	$g(\alpha^{56}) = 52$
$\alpha^{25} = 34$	$g(\alpha^{25}) = 41$	$\alpha^{57} = 62$	$g(\alpha^{57}) = 31$
$\alpha^{26} = 7$	$g(\alpha^{26}) = 48$	$\alpha^{58} = 63$	$g(\alpha^{58}) = 57$
$\alpha^{27} = 14$	$g(\alpha^{27}) = 15$	$\alpha^{59} = 61$	$g(\alpha^{59}) = 48$
$\alpha^{28} = 28$	$g(\alpha^{28}) = 11$	$\alpha^{60} = 57$	$g(\alpha^{60}) = 45$
$\alpha^{29} = 56$	$g(\alpha^{29}) = 52$	$\alpha^{61} = 49$	$g(\alpha^{61}) = 51$
$\alpha^{30} = 51$	$g(\alpha^{30}) = 33$	$\alpha^{62} = 33$	$g(\alpha^{62}) = 13$
$\alpha^{31} = 37$	$g(\alpha^{31}) = 1$		