COM 5140 Error-Correcting Codes — Chi-chao Chao
Fall 2019

Project No. 2
Due 5:00pm, January 21, 2020

You are expected to produce a computer program capable of decoding the $(31, 15)$ Reed-Solomon code over GF(2^5). This code consists of all vectors $(C_0, \ldots, C_{30})$, with each $C_i \in$ GF(2^5), such that

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

where α is a primitive element in GF(2^5) satisfying $\alpha^5 + \alpha^2 + 1 = 0$. Assume that the first 16 characters $C_0, \ldots, C_{15}$ are the parity-check characters, and the last 15 characters $C_{16}, \ldots, C_{30}$ 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 $(R_0, \ldots, R_{30})$, differing from a codeword by t_0 erasures and t_1 errors. If $t_0 + 2t_1 \leq 16$, your program should find the codeword; but if $t_0 + 2t_1 > 16$, your program should output an appropriate failure message.

  The elements of GF(2^5) will be encoded as integers in the range 0 to 31, with integer 0 corresponding to [00000], 1 corresponding to [00001], 2 corresponding to [00010], ..., and 31 corresponding to [11111]. (Here $[a_4 a_3 a_2 a_1 a_0]$ corresponds to the element $a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ in GF(2^5).) An erasure will be represented by a $*$ sign. The input to the program will be a file consisting of several garbled codewords similar to the following format:

  ```
  25 27 * 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 as the file name, say, `105064851.c` or `105064851.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 as the file name, say, `105064851.rar` or `105064851.zip`.) Upload your file to the iLMS system.

Additional Details on Project No. 2

As a partial check, 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

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