EE567: Coding Theory

Homework #1 (due 10/02/14)

Instructor: Arman Shokrollahi *Student: Student's name*

Problem 1

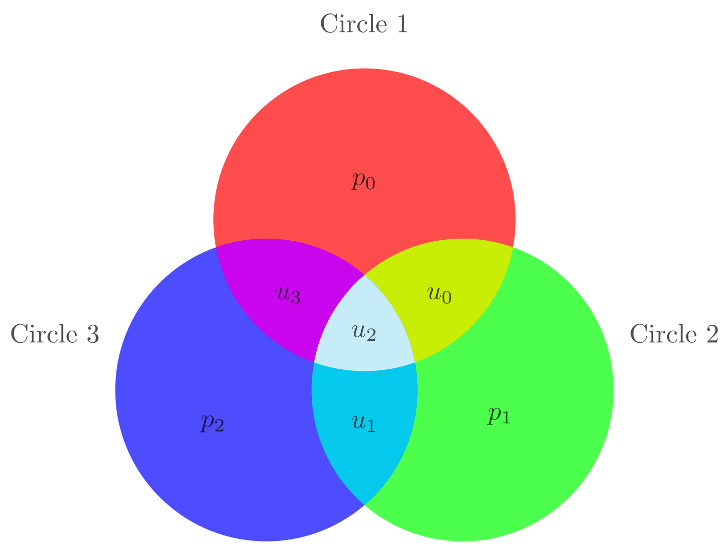
Problem 1.1 *of Ryan/Lin* (We have changed the received word) :

A single error has been added (modulo 2) to a transmitted $(7, 4)$ Hamming codeword, resulting in the received word $r = (1100\,001)$. Using the decoding algorithm described in the chapter, find the error.

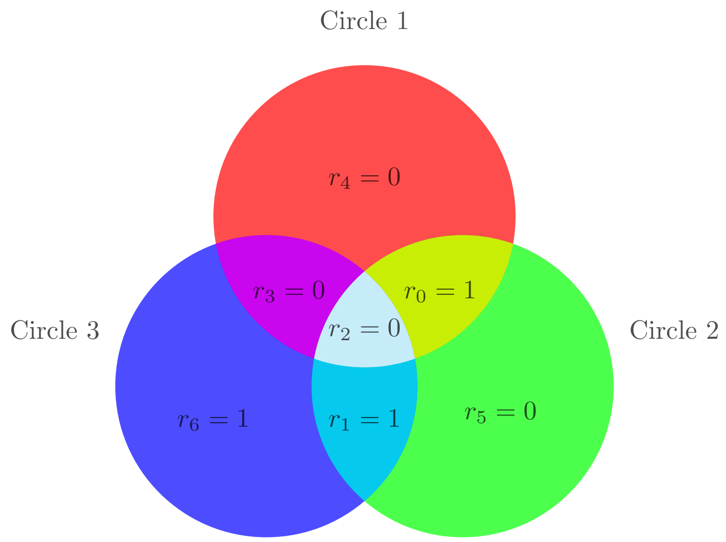
Solution

We want to solve this problem in two ways.

First Way :



We know that $\mathbf{v} = (\mathbf{u}\ \mathbf{p}) = (u_0u_1u_2u_3\ p_0p_1p_2)$ has been transmitted. We have $r = (1100\,001) = (r_0r_1r_2r_3\ r_4r_5r_6)$ as the received word. We rearrange the above Venn diagram as follows



Clearly, Circles 2 and 3, in the figure above, have even numbers of 1's, but Circle 1 does not. We conclude that the error cannot be in Circles 2 and 3, because their rules are satisfied. So it must be $r_4 = 0$ that is in error. Thus, r_4

must be 1. Hence, the decoded codeword is

$$\hat{\mathbf{v}} = (1100\ 101), \tag{0.1}$$

from which the decoded data $\hat{\mathbf{u}} = (1100)$ may be recovered.

Second Way :
We want to solve the problem by some techniques based on generator and parity-check matrices. The parity-check matrix H is helpful in correcting single errors in transmission when

(i) H has no column of 0's,

(ii) no two columns of H are the same.

Consider the following matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & \vdots & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & \vdots & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & \vdots & 0 & 0 & 1 \end{pmatrix}.$$

It is easy to check that H satisfies these two conditions and that for the number of rows ($r = 3$) in H, we have the maximum number of columns possible. If an additional column is added, H will no longer be useful for correcting single errors.
The generator matrix G associated with H is

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \vdots & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & \vdots & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & \vdots & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & \vdots & 1 & 1 & 1 \end{pmatrix}.$$

Consequently we have a $(7, 4)$ group code. The encoding function $E : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$ encodes four-bit messages into seven-bit code words. We realize that because H is determined by three parity-check equations (that is, For all $w = w_1w_2w_3w_4 \in \mathbb{Z}_2^4$, and $E(w) = wG = w_1w_2w_3w_4w_5w_6w_7 \in \mathbb{Z}_2^7$, now try to find $E(w) = wG$. We get some general equations which are called the *parity-check equations*. For more details, see pages 97, 98 of Ryan/Lin), we have now maximized the number of bits we can have in the messages (of course, under our present coding scheme). In addition, the columns of H, read from top to bottom, are the binary equivalents of the integers from 1 to 7. In general, if we start with r parity-check equations, then the parity-check matrix H can have as many as $2^r - 1$ columns and still be used to correct single errors. We denote the transposition of B by B^{tr}. Under these circumstances $H = [B \mid I_r]$, where B is an $r \times (2^r - 1 - r)$ matrix, and $G = [I_m \mid B^{tr}]$ with $m = 2^r - 1 - r$. The parity-check matrix H associated with a $(2^r - 1, 2^r - 1 - r)$ group code.
We want to use some terminologies which can be found on pages 103, 104, and 105 of Ryan/Lin. We now have the matrix H for a Hamming $(7, 4)$ code. It is easy to check that the coset leader for the syndrome (100) is (0000 100). Why we are talking about (100) ? because it is the syndrome corresponding to our received word $r = (1100\ 001)$; note that

$$H \cdot r^{tr} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Finally, if we assume that c is the transmitted word, then $c = (0000\ 100) + (1100\ 001) = (1100\ 101) \overset{0.1}{=} \hat{\mathbf{v}}$.