MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 8 (15pts)

5.4 1; 2pts *Show that the ISBN code detects the interchange of two digits.*

Suppose the digits x_i and x_j in the i-th and j-th positions are interchanged, replacing $x_1 \ldots x_{10}$ with $x'_1 \ldots x'_{10}$. Then,

$$\sum_{k=1}^{10} x_i - \sum_{k=1}^{10} x'_i = \big((11-i)x_i + (11-j)x_j\big) - \big((11-i)x_j + (11-j)x_i\big) = (i-j)(x_j - x_i).$$

Since $-9 \le i-j \le 9$ and $-10 \le x_j - x_i \le 10$, the difference above is divisible by 11 if and only if either $x_i = x_j$ or $i = j$ (which in turn implies $x_i = x_j$). Since the first sum above is divisible by 11, the second one is thus divisible by 11 if and only if $x_i = x_j$ (same digits are "interchanged").

5.4 3; 4pts *Let $f : \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^9$ be the coding function given by*

$$f(abc) = abcabc\bar{a}\bar{b}\bar{c}, \qquad \textit{where} \qquad \bar{0} = 1, \quad \bar{1} = 0.$$

List the eight codewords of f. Show that f is not a group/linear code. How many errors does f detect/correct?

The code is not linear because $f(000) = 000000111 \neq 00000000$. The distance between two codewords is

$$d\big(f(abc), f(xyz)\big) = d\big(abcabc\bar{a}\bar{b}\bar{c}, xyzxyz\bar{x}\bar{y}\bar{z}\big) = 3d(abc, xyz).$$

Thus, the minimal distance between two distinct codewords is 3. It follows that f can detect $3-1=2$ errors and correct $\lfloor (3-1)/2 \rfloor = 1$ error. The 8 words and associated codewords are

000	000000111	001	001001110	010	010010101	011	011011100
100	100100011	101	101101010	110	110110001	111	11111000

Problem D (3pts)

Show that there is no 2-error-correcting code with 15 message bits and 8 check bits.

The number of codewords is 2^{15}, i.e. the number of words in $\mathbb{Z}_2^{15}$. The number of codewords with one mutation in any of $15+8$ bits is $23 \cdot 2^{15}$, if they are all distinct (as the case would be for a 1-error-correcting code). The number of codewords with two mutations in any of the 23 bits is $\binom{23}{2} \cdot 2^{15}$, if they are all distinct (as the case would be for a 2-error-correcting code). Thus, the number codewords, codewords with one mutation, and codewords with two mutations is

$$\big(1 + 23 + 23 \cdot 11\big) \cdot 2^{15} = 277 \cdot 2^{15}\,,$$

if all of these are distinct (as the case would be for a 2-error-correcting code). However,

$$277 \cdot 2^{15} > 256 \cdot 2^{15} = 2^8 \cdot 2^{15} = 2^{23}\,.$$

Since the total number of words in $\mathbb{Z}_2^{23}$ is 2^{23}, the codewords for words in $\mathbb{Z}_2^{15}$, codewords with one mutation, and codewords with two mutations cannot be all distinct in $\mathbb{Z}_2^{23}$. Thus, there is no 2-error-correcting code with 15 message bits and 8 check bits.

5.4 7; 6pts *A linear coding function* $f\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^6$ *is given by the generator matrix*

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

A message is encoded using

000	blank	100	A	010	E	001	T
110	N	101	R	011	D	111	H

and is received as

$$011011 \quad 110000 \quad 010110 \quad 100000 \quad 110110 \quad 110111 \quad 011111.$$

Write down a two-column coset decoding table for f *and decode the message.*

Multiplying the seven received words above by the decoding/parity-check matrix

$$D = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we obtain the seven associated syndromes

$$110 \qquad 011 \qquad 000 \qquad 101 \qquad 101 \qquad 100 \qquad 010\,.$$

This means that the third codeword was (likely) transmitted without an error, while the other six had errors. Since all rows of D are distinct, the errors are in the positions corresponding to the rows of the above syndromes (assuming only one error). Thus, the 1st codeword has an error in position 2, the 2nd in position 3, the 4th and 5th in 1, 6th in 4, and 7th in 5. Thus, the sent codewords (before the errors) were

$$001011 \quad 111000 \quad 010110 \quad 000000 \quad 010110 \quad 110011 \quad 011101.$$

The associated "words" are given by the first three bits in each case:

$$001 = \text{T}, \qquad 111 = \text{H} \qquad 010 = \text{E} \qquad 000 = \text{blank} \qquad 010 = \text{E} \qquad 110 = \text{N} \qquad 011 = \text{D}.$$

A two-column coset decoding table for f is on p315 in the book; the last entry in this table is not unique. Subtracting the coset leaders associated with the syndromes computed above, we obtain the sent codewords; the last row of the table (which corresponds to two errors) is not used. The first approach to decoding is more systematic.

Note: the first edition of the textbook had no Chapter 6, so this exercise was indeed the end.