S-72.341 CODING METHODS

Tutorial 1, Solutions

1. (This problem appeared in a coding course at California Institute of Technology.)

   a) Since

$$\begin{aligned}\sum_{i=1}^{10} i x_i &= 2\cdot 4 + 3\cdot 7 + 4\cdot 1 + 6\cdot 6 + 7\cdot 2 + 8\cdot 5 + 9\cdot 9 + 10x_{10} \\ &= 204 + 10x_{10} \\ &= 6 + 10x_{10} = 0 \bmod 11\end{aligned}$$

   we note that $x_{10} = 6$ satisfies the check equation. The complete ISBN is 0-471-06259-6. The book is Elements of Information Theory by Cover and Thomas, Wiley, 1991.

   b) If a valid ISBN number is altered by exchanging two digits x_i and x_j (assume $x_i \neq x_j$, since otherwise the check bit doesn't change for sure) then the difference between the checksum for the new number and the original ISBN is

$$\left(jx_i + ix_j\right) - \left(ix_i + jx_j\right) = (j-i)\left(x_i - x_j\right).$$

   This is the product of two nonzero numbers less than 11, because

$$0 < |j-i| \leq 9 \text{ and } 0 < \left|x_i - x_j\right| \leq 9\,.$$

   Since 11 is prime and does not divide either factor, 11 does not divide the product, so the checksum difference is nonzero modulo 11.

   c) This is very similar to the a part. The missing digit x_6 satisfies the equation

$$\begin{aligned}0 &= 2\cdot 1 + 3\cdot 3 + 4\cdot 2 + 5\cdot 8 + 6x_6 + 7\cdot 7 + 8\cdot 9 + 9\cdot 6 + 10\cdot 10 \\ &= 6x_6 + 334 = \left(6x_6 + 4\right) \bmod 11.\end{aligned}$$

   We see that $x_6 = 3$ is the solution. The complete ISBN is 0-13-283796-X. The student was frustrated in the book Error Control Coding by Lin and Costello, Prentice-Hall, 1983 (The second edition to be published soon!).

2. In both parts we apply the good old contradiction proof. Note that "." is not the usual multiplication, but the operation associated with the group.

   a) Suppose that there exist *two* identity elements $e_1, e_2 \in G$, $e_1 \neq e_2$, such that $a \cdot e_1 = e_1 \cdot a = a$ and $a \cdot e_2 = e_2 \cdot a = a$ for all $a \in G$. Then

   $$e_1 = e_2 \cdot e_1 = e_1 \cdot e_2 = e_2,$$

   which is a contradiction.

   b) Assume that there exist *two* inverses a_1^{-1} and a_2^{-1}, $a_1^{-1} \neq a_2^{-1}$ for a group element $a \in G$. Then

   $$a_1^{-1} = e \cdot a_1^{-1} = \left(a_2^{-1} \cdot a\right) \cdot a_1^{-1} = a_2^{-1} \cdot \left(a \cdot a_1^{-1}\right) = a_2^{-1} \cdot e = a_2^{-1}.$$

   This contradicts our assumption.

3. Addition table for GF(5):

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication table for GF(5):

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

4. The key to this problem is to recall that when two vectors $\mathbf{c}$ and $\mathbf{h}$ are orthogonal their inner product is zero, i.e. $\mathbf{c}^T\mathbf{h} = 0$. The same thing for two basis: Suppose column vectors of $\mathbf{G}$ are a basis for space S and column vectors of $\mathbf{H}$ are a basis for space D. Then the two spaces are orthogonal (dual) if $\mathbf{G}^T\mathbf{H} = \mathbf{0}$, i.e. every vector in S is orthogonal to every vector in D.

   a) Let $\mathbf{G}$ denote the matrix whose column vectors form the given basis. We shall find the dual space by manipulating $\mathbf{G}^T$ using elementary row operations in the following way:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \Leftrightarrow \quad \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \Leftrightarrow \quad \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right].$$

   The last matrix is in the form $\begin{bmatrix} \mathbf{I}_{3\times 3} & \mathbf{P}_{3\times 2} \end{bmatrix}$. We can now find a basis for the dual space by setting $\mathbf{H}^T = \begin{bmatrix} -\mathbf{P}_{2\times 3}^T & \mathbf{I}_{2\times 2} \end{bmatrix}$, since then

$$\mathbf{G}^T\mathbf{H} = \begin{bmatrix} \mathbf{I}_{3\times 3} & \mathbf{P}_{3\times 2} \end{bmatrix} \begin{bmatrix} -\mathbf{P}_{3\times 2} \\ \mathbf{I}_{2\times 2} \end{bmatrix} = \mathbf{0}.$$

   Notice that in GF(2) $1 = -1$. Thus *a* basis for the dual space is

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{3\times 2} \\ \mathbf{I}_{2\times 2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

NOTE: In these tutorials we shall use in a routine fashion the equality $1 = -1$ when working in GF(2). Be alert!

We shall see later in the course that the generator matrix $\mathbf{G}$ of a systematic block code has the form shown here. $\mathbf{P}$ is the parity part and $\mathbf{I}$ is the systematic part. The matrix $\mathbf{H}$ is called parity-check matrix.

b) This could be solved similarly to the part a. However, here we shall apply the standard procedure for solving $\mathbf{Ax} = \mathbf{0}$ for rectangular $\mathbf{A}$. Again, $\mathbf{G}$ is the matrix whose columns form the given basis. By using row operations $\mathbf{G}^T$ can be manipulated to form

$$\begin{bmatrix} 1 & 2 & 3 & 2 & 2 \\ 1 & 4 & 3 & 1 & 2 \\ 4 & 1 & 2 & 3 & 3 \end{bmatrix} \quad \Leftrightarrow \quad \begin{bmatrix} 1 & 2 & 3 & 2 & 2 \\ 0 & 2 & 0 & 4 & 0 \\ 0 & 3 & 0 & 0 & 0 \end{bmatrix} \Leftrightarrow \ldots \Leftrightarrow \begin{bmatrix} 1 & 2 & 3 & 2 & 2 \\ 0 & 2 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 \end{bmatrix} = \mathbf{G}_{rr}^T.$$

(Subtract row 1 from row 2, add row 1 to row 3, then add row 2 to row 3.) Next we have to solve $\mathbf{G}_{rr}^T\mathbf{h} = \mathbf{0}$, $\mathbf{h} = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 & h_5 \end{bmatrix}^T$. Free variables are h_3 and h_5. The two solutions can be found by setting $h_3 = 1$, $h_5 = 0$, and $h_3 = 0, h_5 = 1$. Since $h_1 = -3h_3 - 2h_5 = 2h_3 + 3h_5$ we conclude that the solutions $\mathbf{h}_1$ and $\mathbf{h}_2$ are

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1 & \mathbf{h}_2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

5. By theorem 2-12 the elements of GF(11) have order 1,2,5, or 10. Our strategy is to find a primitive element in GF(11) and then apply theorem 2-11 to find other elements. One primitive element is 2, since $2^{10} = 1$, and $2^2 = 4 \neq 1$ and $2^5 = 10 \neq 1$. By theorem 2-11 the other primitive elements are equal to 2^i, where i satisfies GCD(10,i)=1 ($i = 1,2,...,10$), i.e. the indices that are relatively prime to 10. They are $i = 1,3,7,9$. Thus, the other primitive elements are $2^3 = 8, 2^7 = 7, 2^9 = 6$.

   Similarly, the elements of order 5 are the ith powers of 2, where i satisfies GCD(10,i)=2. These are $i = 2,4,6,8$. The multiplicative orders of all elements of GF(11) are listed in the table below. The only element having order 2 is 10 ($10^2 = 1$). The identity element has always order 1.

i	2^i	order
1	2	10
2	4	5
3	8	10
4	5	5
5	10	2
6	9	5
7	7	10
8	3	5
9	6	10
10	1	1

   All nonzero elements of GF(11) can be expressed as powers of a primitive element. The primitive elements are 2,6,7,8. In the table nonzero elements of GF(11) are presented as powers of 2.