

Second midterm exam solutions

*Problem 1.* Consider the linear code over  $\mathbb{Z}_5$  with 4 message symbols, 6 code symbols, and code matrix

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 & 1 & 4 \end{bmatrix}.$$

- (a) Show that this code can correct one error.  
 (b) Find and correct the error if the received vector is

$$[2 \ 1 \ 0 \ 4 \ 2 \ 3].$$

- (c) Find and correct the error if the received vector is

$$[3 \ 1 \ 2 \ 2 \ 0 \ 3].$$

Hint on (b) and (c): find the code vector that agrees with the received vector in the first four positions. Then, if necessary, adjust it by adding a multiple of a row of  $C$ .

(a) We must show that the weight of every non-zero code vector  $\mathbf{x}\mathbf{C}$  is at least 3. Since the first four columns of  $C$  form an identity matrix, this is obvious if  $\mathbf{x}$  has 3 or 4 non-zero entries. Since each row of  $C$  has weight 3, we see that  $\mathbf{x}\mathbf{C}$  has weight 3 if  $\mathbf{x}$  has just 1 non-zero entry. It remains to prove that  $\mathbf{y} = \mathbf{x}\mathbf{C}$  has weight at least 3 if  $\mathbf{x}$  has two non-zero entries. In this case  $\mathbf{y}$  has two non-zero entries in the first four columns, so we have to prove that the last two columns of  $\mathbf{y}$  are non-zero.

Since  $\mathbf{x}$  has two non-zero entries, the last two columns of  $\mathbf{y}$  are a linear combination of two of the vectors  $[1 \ 1]$ ,  $[1 \ 2]$ ,  $[1 \ 3]$ , and  $[1 \ 4]$ . Every such linear combination is non-zero, since none of these four vectors is a multiple of another.

- (b) Compute

$$[2 \ 1 \ 0 \ 4] \mathbf{C} = [2 \ 1 \ 0 \ 4 \ 2 \ 0].$$

This is the corrected code vector, since it differs in only one position from the received vector.

- (c) Compute

$$[3 \ 1 \ 2 \ 2] \mathbf{C} = [3 \ 1 \ 2 \ 2 \ 3 \ 4].$$

This differs from the received vector by  $[3 \ 1]$  in the last two positions. To adjust it, observe that  $1 \equiv 2 \cdot 3 \pmod{5}$ , so  $[3 \ 1] = 3 \cdot [1 \ 2]$ . Subtracting 3 times row 2 of  $C$  gives the corrected code vector

$$[3 \ 3 \ 2 \ 2 \ 0 \ 3],$$

which differs in only one position from the received vector.

*Problem 2.* Using a two-error correcting Reed-Solomon code over  $\mathbb{Z}_7$  with 3 message symbols and 7 code symbols, you receive the vector

$$\mathbf{r} = [0 \ 2 \ 4 \ 3 \ 1 \ 0 \ 4].$$

(a) Find an error locator polynomial  $E(t)$  of degree  $\leq 2$  and not identically zero, such that there exists  $Q(t)$  of degree  $\leq 4$  solving the key equation

$$Q(i) \equiv r_i E(i) \pmod{7} \quad \text{for } i = 0, 1, \dots, 6.$$

(b) Locate the possible error positions in  $\mathbf{r}$  by evaluating  $E(t)$ .

This problem does *not* require that you find  $Q(t)$  or the original message.

(a) Let  $E(t) = u_0 + u_1 t + u_2 t^2$ . Compute difference tables of  $r_i$ ,  $ir_i$  and  $i^2 r_i$ , as follows:

```

0 2 4 3 1 0 4
2 2 6 5 6 4
0 4 6 1 5
4 2 2 4
5 0 2
2 2

```

```

0 2 1 2 4 0 3
2 6 1 2 3 3
4 2 1 1 0
5 6 0 6
1 1 6
0 5

```

```

0 2 2 6 2 0 4
2 0 4 3 5 4
5 4 6 2 6
6 2 3 4
3 1 1
5 0

```

This gives the system of linear equations

$$\begin{bmatrix} 2 & 0 & 5 \\ 2 & 5 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix} = \mathbf{0}.$$

Setting  $u_2 = 1$  and solving (mod 7), we find  $u_0 = u_1 = 1$ , so  $E(t) = t^2 + t + 1$ .

(b) Evaluating  $E(i) \pmod{7}$  for  $i = 0, 1, \dots, 6$ , we find  $E(2) = E(4) = 0$ , so the possible errors are in  $r_2$  and  $r_4$ .

*Problem 3.* Prove that  $n^4 - n^2$  is divisible by 12 for every integer  $n$ .

*Proof.* Factoring gives

$$n^4 - n^2 = n^2(n-1)(n+1).$$

One of  $n-1$ ,  $n$  and  $n+1$  is always divisible by 3, so  $3 \mid n^4 - n^2$ .

If  $n$  is odd then  $n-1$  and  $n+1$  are both even and  $(n-1)(n+1)$  is divisible by 4. If  $n$  is even, then  $n^2$  is divisible by 4. In either case,  $4 \mid n^4 - n^2$ .

Since 3 and 4 are relatively prime, their least common multiple is 12, so  $12 \mid n^4 - n^2$ .

An alternative but more tedious proof is to compute  $n^2$  and  $n^4$  for  $n \equiv 0, 1, 2, \dots, 11 \pmod{12}$  and verify that they agree in all twelve cases.

*Problem 4.* Prove that

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3$$

for every positive integer  $n$ .

*Proof.* We proceed by induction on  $n$ . The basis step is  $n = 1$ , where both sides reduce to 2.

For the induction step, assume that

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3.$$

Add  $(n+1)(n+2)$  to both sides to get

$$\begin{aligned} 1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) + (n+1)(n+2) &= n(n+1)(n+2)/3 + (n+1)(n+2) \\ &= (n+1)(n+2)(n+3)/3. \end{aligned}$$