IV054-2021 Homework 1 solutions

1.

Statement is false, proof by finding a specific case where statement is false.

Let C be a binary (2,2,2) code, where C = {00,11}. Let C' be a code obtained from C by adding a parity bit, therefore C' = {000,110}. C' is not a (n+1,M,d+1) code, but a (3,2,2,) code, therefore statement is false.

2.

Proof that $A_2(5,4) = 2$: Let C be a code containing codeword 00000. To satisfy $d = 4$, all other codewords in C must have at least four ones (their distance from the codeword 00000 must be larger than four). Two codewords of length 5 containing four ones have distance at most 2, therefore we can't construct code $(5,3,4)$.

3.

ISBN can correct a single digit error, thanks to the last digit used as a checksum so that: $\sum_{i=1}^{10}(11-i)x_i \equiv 0 \; mod \; 11$.

For the code 0444851x33, we need to solve the following equation:

$$\begin{aligned} 0\cdot 1+4\cdot 2+4\cdot 3+4\cdot 4+8\cdot 5+5\cdot 6+1\cdot 7+x\cdot 8+3\cdot 9+3\cdot 10 &\equiv 0 \; mod \; 11 \\ 0+8+12+16+40+30+7+8x+27+30 &\equiv 0 \; mod \; 11 \\ 170+8x &\equiv 0 \; mod \; 11 \\ 5+8x &\equiv 0 \; mod \; 11 \\ x &= 9 \end{aligned}$$

The ISBN code 0444851933 is **The Theory Of Error-Correcting Codes** by F. J. Macwilliams and N. J. Sloane

4.

Writing out M codewords on $\log_2 M$ bits produces a "code" with Hamming distance equal to 1. We can create each new code by adding trailing zeroes to it, then:

$$\forall n \in \mathbb{N} > \log_2 M : \; d(n) = 1$$

- such a function is **increasing** (although not *strictly increasing*, but that's not the question, right?)
- such a function is also **decreasing** so let's show that we can also create non-decreasing increasing function:

Let us create each new code by repeating the elements of the original code e.g.

$$for \; M = 8 : x_1x_2x_3 \; in \; C_3 \rightsquigarrow x_1x_2x_3x_1 \; in \; C_4 \rightsquigarrow ... \rightsquigarrow x_1x_2x_3x_1x_2x_3x_1 \; in \; C_7 \rightsquigarrow ...$$

for such a code:

$$\forall k,n \in \mathbb{N}; k \geq 1, n \in [k\log_2 M, (k+1)\log_2 M) : \; d(n) = k$$

This function is **increasing** and even **non-decreasing**!

5.

(a) Not a linear code: $111 + 111 = 000$ and $000 \notin C_a$

(b) Not a linear code: let's have a ternary linear code $C_1 = \{000, 111, 222\}$, then $C_b = \{000111, 111222, 222000\}$. We can see that C_b is not a linear code since $000111 + 111222 = 111000$ and $111000 \notin C_b$.

(c) Is a linear code: the result of applying addition operation on two linear codes is a linear superset code of those two codes.

(d) Not a linear code: if $C_1 = \{000, 001, 100, 101\}$ and $C_2 = \{000, 111, 222\}$, then $101 + 222 = 020 \in C_d$, but $020 + 001 = 021 \notin C_d$

6.

(a) Standard generator matrix for C:

$$H_{norm} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \sim \left[\begin{array}{cc|ccc} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

$$H_{norm} = [\,-A^T \mid I_{n-k}]$$
$$\text{G} = [\, I_k \mid \text{A} \,]$$
$$\text{G} = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right].$$

(b) The minimal distance of C, h(C) = w(C), where w(C) is the smallest weight of non-zero code words of C.

$$\text{C} = \{00000,\ 10011,\ 01110,\ 11101\}.$$
$$\mathbf{h(C) = w(C) = 3}.$$

(c) Syndrome decoding table:

l(z)	z
00000	000
10000	110
01000	001
00100	100
00010	101
00001	011
10100	010
10110	111

w = 10111
w $\cdot H^T =$ e $\cdot H^T = 100$
l(100) = 00100
Decoded word is w + l(z) = 10111 + 00100 = **10011**.

7.

(a) Generator matrix of polynomial $1 + x^2 + x^3 + x^4$ in R_7:

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

(b) To find parity-check matrix, first we need to find check polynomial $h(x) = \frac{(x^n - 1)}{g(x)}$:

$$(x^7 - 1)/(x^4 + x^3 + x^2 + 1) = 1 + x^2 + x^3$$

From the result, we obtain parity-check matrix H:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = H_{norm}$$

We can also get the same parity matrix by transposition from G_{norm} ...

(c) codeword 1010 cannot be encoded by this code as maximum length of message word this polynomial can encode is 3. Best we can do is 101 which is encoded as:

$$\begin{aligned} (1 + x^2 + x^3 + x^4)(1 + x^2) &= (1 + x^2 + x^3 + x^4) + x^2(1 + x^2 + x^3 + x^4) \\ &= (1 + x^2 + x^3 + x^4) + (x^2 + x^4 + x^5 + x^6) \\ &= 1 + x^3 + x^5 + x^6 \end{aligned}$$

thus 101 will be encoded as 1001011 (same result can be obtained by using generator matrix)

8.

(a)

$$n(3,3) \geq 3 + n(2,2)$$
$$n(2,2) \geq 2 + n(1,1)$$
$$n(1,1) = 1$$

The lower bound of n for $k = 3, d = 3$ is 6, since $n(3,3) \geq 3 + (2+1) \implies n(3,3) \geq 6$.

(b) Since $n = 6$ and $k = 3$, the generator matrix will be 3×6. It's left half will be identity matrix I_3, and we choose the right half such that all it's rows contain exactly two 1s. The [6,3,3] linear code's generator matrix is:

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

The resulting code $C = \{000000, 100110, 010101, 110011, 001011, 101101, 011110, 111000\}$.

(c)

$$10 \geq d + n(2, \lceil d/2 \rceil)$$
$$n(2, \lceil d/2 \rceil) = \lceil d/2 \rceil + n(1, \lceil \lceil d/2 \rceil /2 \rceil)$$
$$n(1, \lceil \lceil d/2 \rceil /2 \rceil = \lceil \lceil d/2 \rceil /2 \rceil + n(0, \lceil \lceil \lceil d/2 \rceil /2 \rceil /2 \rceil)$$
$$n(0, \lceil \lceil \lceil \lceil d/2 \rceil /2 \rceil /2 \rceil /2 \rceil) = 0$$

$10 = d + \lceil d/2 \rceil + \lceil \lceil d/2 \rceil /2 \rceil + 0 \implies d = 5$. The upper bound for d is 5.

9.

(a) All binary cyclic codes C of length 10 can be described using irreducible polynomials of $x^{10}-1$:

$$x^{10}-1=(x+1)(x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+x^2+x+1)$$

We can therefore construct $2^4=16$ cyclic codes from these irreducible polynomials. But since some of these irreducible polynomials are equal, some cyclic codes will be equal. In the end, we can build 9 different cyclic codes:

$$1$$

$$(x+1)$$

$$(x^4+x^3+x^2+x+1)$$

$$(x+1)(x^4+x^3+x^2+x+1)=x^5+1$$

$$(x+1)(x+1)=x^2+1$$

$$(x^4+x^3+x^2+x+1)(x^4+x^3+x^2+x+1)=x^8+x^6+x^4+x^2+1$$

$$(x+1)(x+1)(x^4+x^3+x^2+x+1)=x^6+x^5+x+1$$

$$(x^4+x^3+x^2+x+1)(x^4+x^3+x^2+x+1)(x+1)=x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

$$(x^4+x^3+x^2+x+1)(x^4+x^3+x^2+x+1)(x+1)(x+1)=x^{10}+1$$

(b) To construct the smallest binary code with the codewords (0110000000) and (1010000000), we will use the previous question and choose $C=<1+x>$. Let's see if this code contains both codewords (0110000000) and (1010000000) :

- By shifting (0110000000) 1 bit to the left, we obtain the codeword (1100000000) which can be constructed with $1+x$.
- The codeword (1010000000) can be constructed using $1+x^2$ which is $(x+1)(x+1)=1+x^2$

Therefore, the smallest binary code containing both codewords is $C=<1+x>$.