10 pts

Math/CS 4240/6240 – Spring 2023 – Exam 1 Name:_____

(1) (a) How many $(n, 2, n)_3$-codes are there?

$$\frac{3^n 2^n}{2} = \boxed{3^n 2^{n-1}}$$

(b) How many $(n, 2, n)_q$-codes are there?

$$\frac{q^n (q-1)^n}{2}$$

18 pts

(2) What is the smallest possible length n for which a $(n, 6, 3)_2$-code may exist? Why?

n+1 words total

So $6(n+1) \geq 2^n$ must be true.

n	$6(n+1)$	2^n
3	24	8
4	30	16
5	36	32
(6)	42	64

↑ Smallest length with $6(n+1) \geq 2^n$

(b) For the value of n determined in (a), does an $(n, 6, 3)_2$-code actually exist? Why?

Here is an actual $(6, 6, 3)_2$-code. It is a subset of the $(6, 8, 3)_2$-code discussed in class.

000 000,
001 110,
010 101,
100 011,
110 110,
101 101

16 pts

(3) A symmetric binary communication channel has $p(0|0) = p(1|1) = .95$ and $p(0|1) = p(1|0) = .05$. If this channel is used to transmit code words of length 7, then what is the probability that a code word received has at most one bit in error from the code word that was actually transmitted? What is the same probability when code words of length 15 are transmitted?

length 7

probability of no error $(.95)^7 \approx .6983$

probability of one error $7(.95)^6(.05) \approx .2572$

$+$

$.9556$

95.56%

length 15

probability of no error $(.95)^{15}$

probability of one error $15(.95)^{14}(.05)$

$+$

$.8290$

82.90%

20 pts

(4) Consider the finite field $\mathbb{F}_8 = \dfrac{\mathbb{F}_2[x]}{(x^3 + x^2 + 1)}$.

(a) What is the order of $a \in \mathbb{F}_8$ when $a \neq 0$ and $a \neq 1$?

order of a divides 7 so order is 7.

(b) Is $\alpha = x$ a primitive element of $\mathbb{F}_8$?

yes.

(b) Calculate $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7$ as a polynomial in α of degree less than three.

$\alpha^3 + \alpha^3 + 1 = 0$ reduction relation

α

α^2

$\alpha^3 = \alpha^2 + 1$

$\alpha^4 = \alpha^3 + \alpha$

$= \alpha^2 + \alpha + 1$

$\alpha^5 = \alpha^3 + \alpha^2 + \alpha$

$= \alpha + 1$

$\alpha^6 = \alpha^3 + \alpha$

$\alpha^7 = \alpha^3 + \alpha^2 + 1$

18 pts

(5) $x^3 + 2x + 1 \in \mathbb{F}_3[x]$ is a primitive polynomial. The powers of primitive element $\alpha = x$ are given in the table below.

(a) Calculate the cyclotomic cosets of 3 mod 26.

(b) Calculate the minimal polynomials for α, α^2, α^3, and α^6.

α	$\alpha^{14} = 2\alpha$
α^2	$\alpha^{15} = 2\alpha^2$
$\alpha^3 = \alpha + 2$	$\alpha^{16} = 2\alpha + 1$
$\alpha^4 = \alpha^2 + 2\alpha$	$\alpha^{17} = 2\alpha^2 + \alpha$
$\alpha^5 = 2\alpha^2 + \alpha + 2$	$\alpha^{18} = \alpha^2 + 2\alpha + 1$
$\alpha^6 = \alpha^2 + \alpha + 1$	$\alpha^{19} = 2\alpha^2 + 2\alpha + 2$
$\alpha^7 = \alpha^2 + 2\alpha + 2$	$\alpha^{20} = 2\alpha^2 + \alpha + 1$
$\alpha^8 = 2\alpha^2 + 2$	$\alpha^{21} = \alpha^2 + 1$
$\alpha^9 = \alpha + 1$	$\alpha^{22} = 2\alpha + 2$
$\alpha^{10} = \alpha^2 + \alpha$	$\alpha^{23} = 2\alpha^2 + 2\alpha$
$\alpha^{11} = \alpha^2 + \alpha + 2$	$\alpha^{24} = 2\alpha^2 + 2\alpha + 1$
$\alpha^{12} = \alpha^2 + 2$	$\alpha^{25} = 2\alpha^2 + 1$
$\alpha^{13} = 2$	$\alpha^{26} = 1$

$C_0 = 0$ $\quad C_7 = 7, 21, 11$ (4)

$C_1 = 1, 3, 9$ $\quad C_{13} = 13$

$C_2 = 2, 6, 18$ $\quad C_{14} = 14, 16, 22$

$C_4 = 4, 12, 10$ $\quad C_{17} = 17, 25, 23$

$C_5 = 5, 15, 19$ $\quad C_8 = 8, 24, 20$

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

$M^{(2)}(x) = M^{(6)}(x) = (x - \alpha^2)(x - \alpha^6)(x - \alpha^{18})$ (4)

$= x^3 - (\alpha^2 + \alpha^6 + \alpha^{18})x^2 + (\alpha^8 + \alpha^{20} + \alpha^{24})x - \alpha^{26}$

$\alpha^2 = \alpha^2$

$\alpha^6 = \alpha^2 + \alpha + 1$

$+ \alpha^{18} = \alpha^2 + 2\alpha + 1$

2

$\alpha^8 = 2\alpha^2 + 2$

$\alpha^{20} = 2\alpha^2 + \alpha + 1$

$+ \alpha^{24} = 2\alpha^2 + 2\alpha + 1$

1

$\alpha^{26} = 1$

$= x^3 - 2x^2 + x - 1 = x^3 + x^2 + x + 2$ (6)

18 pts

(6) Let $\mathcal{W} = \text{Row}(A)$ be subspace of the binary vector space $\mathbb{F}_2^6$ in which A is given below.

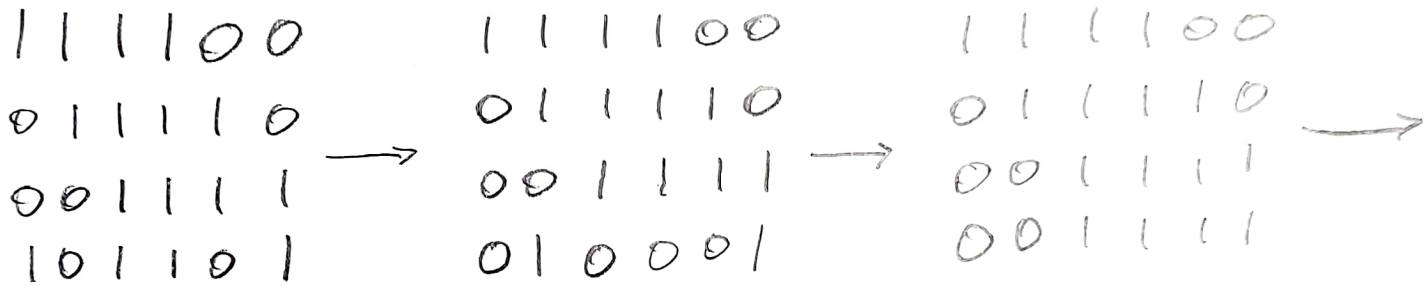
(a) Find a basis for $\mathcal{W}$.

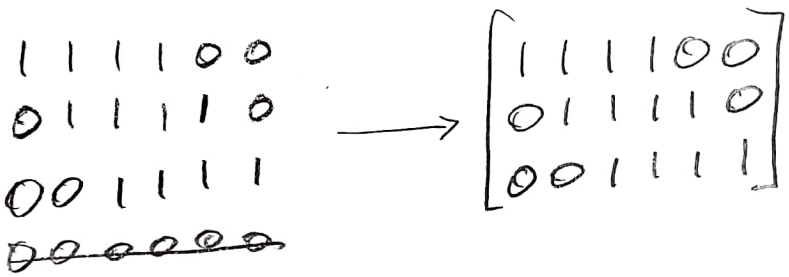
(b) What is $\dim(\mathcal{W})$?

(c) What is $\dim(\mathcal{W}^\perp)$?

(d) Find a basis for $\mathcal{W}^\perp$.

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

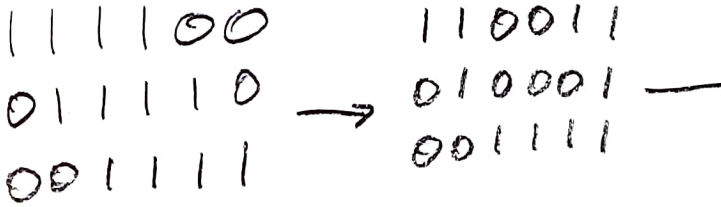




The rows of this matrix are a basis for $\mathcal{W}$.

Thus $\dim(\mathcal{W}) = 3$.

Thus $\dim(\mathcal{W}^\perp) = 6 - 3 = 3$



x_4, x_5, x_6 = free variables

$x_3 + x_4 + x_5 + x_6 = 0$

$x_2 + x_6 = 0$

$x_1 + x_5 = 0$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} x_5 \\ x_6 \\ x_4+x_5+x_6 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = x_4 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_5 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + x_6 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Basis for $\mathcal{W}^\perp$ → 001100, 101010, 011001