ECE 405/511 Assignment 3 SPRING 2026 SOLUTIONS

① the order of an element of GF(81) must divide 80

$$80 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$$

the possible orders are

$$\{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$$

order	# elements with order
1	$\phi(1) = 1$
2	$\phi(2) = 1$
4	$\phi(4) = 2$
5	$\phi(5) = 4$
8	$\phi(8) = 4$
10	$\phi(10) = 4$
16	$\phi(16) = 8$
20	$\phi(20) = 8$
40	$\phi(40) = 16$
80	$\phi(80) = 32$
total	80 = # of nonzero elements

2. representation of GF(32) using $x^5 + x^3 + 1$

let α be a root of $x^5 + x^3 + 1$
so that $\alpha^5 + \alpha^3 + 1 = 0$ or $\alpha^5 = \alpha^3 + 1$

power	polynomial	vector
$\alpha^{-\infty} = 0$	0	00000
$\alpha^0 = 1$	1	10000
α^1	α	01000
α^2	α^2	00100
α^3	α^3	00010
α^4	α^4	00001
α^5	$1 + \alpha^3$	10010
α^6	$\alpha + \alpha^4$	01001
α^7	$1 + \alpha^2 + \alpha^3$	10110
α^8	$\alpha + \alpha^3 + \alpha^4$	01011
α^9	$1 + \alpha^2 + \alpha^3 + \alpha^4$	10111
α^{10}	$1 + \alpha + \alpha^4$	11001
α^{11}	$1 + \alpha + \alpha^2 + \alpha^3$	11110
α^{12}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4$	11111
α^{13}	$1 + \alpha^2 + \alpha^4$	10101
α^{14}	$1 + \alpha$	11000
α^{15}	$\alpha + \alpha^2$	01100
α^{16}	$\alpha^2 + \alpha^3$	00110
α^{17}	$\alpha^3 + \alpha^4$	00011
α^{18}	$1 + \alpha^3 + \alpha^4$	10011

power	polynomial	vector
α^{19}	$1\ \alpha\ \ \alpha^3\ \alpha^4$	11011
α^{20}	$1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4$	11111
α^{21}	$1\ \alpha\ \alpha^2\ \ \ \alpha^4$	11101
α^{22}	$1\ \alpha\ \alpha^2$	11100
α^{23}	$\alpha\ \alpha^2\ \alpha^3$	01110
α^{24}	$\alpha^2\ \alpha^3\ \alpha^4$	00111
α^{25}	$1\ \ \ \ \ \alpha^4$	10001
α^{26}	$1\ \alpha\ \ \alpha^3$	11010
α^{27}	$\alpha\ \alpha^2\ \ \alpha^4$	01101
α^{28}	$1\ \ \alpha^2$	10100
α^{29}	$\alpha\ \ \ \alpha^3$	01010
α^{30}	$\alpha^2\ \ \ \alpha^4$	00101

$\alpha^{31} = 1$ as expected

3. GF(8) arithmetic using Table B.3 page 346

(a) $\alpha^4 + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = 1$

(b) $(\alpha^3 + \alpha^2)(\alpha^6 + \alpha^3)$

$= (\alpha^2 + \alpha + 1)(\alpha^{2+1} + \alpha + 1)$

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

$= \alpha^5 \cdot \alpha^4 = \alpha^9 = \alpha^7 \cdot \alpha^2 = \alpha^2$

(c) $\alpha^6(\alpha^5 + \alpha^4) + \alpha^2 = \alpha^{11} + \alpha^{10} + \alpha^2 = \alpha^4 + \alpha^3 + \alpha^2$

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

(d) $(\alpha^3 x^2 + \alpha x + 1)(\alpha^5 x^3 + x + \alpha^2)$

$= \alpha^8 x^5 + \alpha^6 x^4 + (\alpha^3 + \alpha^5) x^3 + (\alpha + \alpha^5) x^2 + (\alpha^3 + 1) x + \alpha^2$

$= \alpha x^5 + \alpha^6 x^4 + \alpha^2 x^3 + \alpha^6 x^2 + \alpha x + \alpha^2$

4. Factoring x^n+1 into binary irreducible polynomial

(a) x^5+1

$x+1$ is a factor

$$
\begin{array}{r|l}
x+1 & x^5+0x^4+0x^3+0x^2+0x+1 \\
 & x^4+x^3+x^2+x+1 \\
\hline
 & x^5+x^4 \\
\hline
 & x^4+0x^3 \\
 & x^4+x^3 \\
\hline
 & x^3+0x^2 \\
 & x^3+x^2 \\
\hline
 & x^2+0x+1 \\
 & x^2+x \\
\hline
 & x+1 \\
 & x+1 \\
\hline
 & 0
\end{array}
$$

$x^4+x^3+x^2+x+1$ is irreducible

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

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

$x^6+x^5+x^4+x^3+x^2+x+1$ is NOT irreducible

- it must have a factor of degree 2 or 3
- the only irreducible degree 2 polynomial is x^2+x+1.

$$
\begin{array}{r}
x^4 \qquad\qquad +x \\
x^2+x+1 \;\overline{)\; x^6+x^5+x^4+x^3+x^2+x+1} \\
\underline{x^6+x^5+x^4} \\
x^3+x^2+x+1 \\
\underline{x^3+x^2+x} \\
1 \leftarrow \text{nonzero remainder}
\end{array}
$$

$\therefore$ $x^6+x^5+x^4+x^3+x^2+x+1$ is the product of two degree 3 irreducible polynomials

$$(x^7+1) = (x+1)(x^3+x+1)(x^3+x^2+1)$$

(c) $x^{15}-1 = (x+1)(x^{14}+x^{13}+\cdots+x+1)$

all the nonzero elements of GF(16) are factors of $x^{15}-1$

- there are $\phi(15) = 8$ primitive elements in GF(16)

these elements correspond to the primitive polynomials

x^4+x+1 and x^4+x^3+1

- there are $\phi(3) = 2$ elements of order 3

there is only one irreducible polynomial of degree 2

x^2+x+1

- there are $\phi(5) = 4$ elements of order 5

these are roots of the irreducible polynomial

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

$\therefore\ x^{15}-1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

5. Cyclic code generated by $g(x) = x^5 + x^4 + x^2 + 1$

a) $g(x)$ must be a factor of $x^{15}+1$

$$
\begin{array}{r|l}
x^5+x^4+x^2+1 & x^{10}+x^9+x^8+x^6+x^5+x^2+1 \\
\hline
 & x^{15}+1 \\
 & x^{15}+x^{14}+x^{12}+x^{10} \\
\hline
 & x^{14}+x^{12}+x^{10}+1 \\
 & x^{14}+x^{13}+x^{11}+x^9 \\
\hline
 & x^{13}+x^{12}+x^{11}+x^{10}+x^9+1 \\
 & x^{13}+x^{12}+x^{10}+x^8 \\
\hline
 & x^{11}+x^9+x^8+1 \\
 & x^{11}+x^{10}+x^8+x^6 \\
\hline
 & x^{10}+x^9+x^6+1 \\
 & x^{10}+x^9+x^7+x^5 \\
\hline
 & x^7+x^6+x^5+1 \\
 & x^7+x^6+x^4+x^2 \\
\hline
 & x^5+x^4+x^2+1 \\
 & x^5+x^4+x^2+1 \\
\hline
 & 0
\end{array}
$$

$\therefore$ $g(x)$ is a factor of $x^{15}+1$

(b) $h(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$

from part (a)

$h^*(x) = x^{10} h(x^{-1}) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

(c) $\deg(g(x)) = n - k = 5$

$\therefore\ k = n - (n-k) = 15 - 5 = 10$

the number of codewords is

$2^k = 2^{10} = 1024$

6. For C in problem 5

find G and H

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

$$G = \begin{bmatrix} 1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0 \\ \vdots \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0 \end{bmatrix}$$

10 rows

15 columns

from 5.1 $h(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$

$h^*(x) = x^{10} h(x^{-1}) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$H = \begin{bmatrix} 1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1 \end{bmatrix}$$

5 rows

7. $x^{33}-1$ factors into

1 polynomial of degree 1

1 " " 2

3 " " 10

The possible dimensions are

$\{32, 31, 30, 23, 22, 21, 20, 13, 12, 11, 10, 3, 2, 1.\}$