Study Problems
CMSC 442/653

Dr. Lomonaco

April 11, 2009

Problem 1. Let V be the binary linear cyclic code of length $n = 9$ given by the generator polynomial

$$g(x) = x^6 + x^3 + 1$$

i) Use $g(x)$ to compute a generator matrix G for V.

$Dim\,(V) = codeg\,(g) = 9 - \deg(g) = 3$. Hence, G has 3 rows. Since $n = 9$, G has 9 columns. Thus,

$$G = \begin{pmatrix} x^2 g(x) \\ x g(x) \\ g(x) \end{pmatrix} = \begin{pmatrix} x^8 + x^5 + x^2 \\ x^7 + x^4 + x \\ x^6 + x^3 + 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

ii) Find the parity check polynomial $h(x)$ of V.

$$h(x) = \frac{x^n - 1}{g(x)} = \frac{x^9 - 1}{x^6 + x^3 + 1} = x^3 + 1$$

iii) Use $h(x)$ to compute a generator matrix of $V^!$.

$Dim\left(V^!\right) = codeg\,(h) = \deg\,(g) = 6$, and $n = 9$

$$\text{Hence } G_! = \begin{pmatrix} x^5 h(x) \\ x^4 h(x) \\ x^3 h(x) \\ x^2 h(x) \\ x h(x) \\ h(x) \end{pmatrix} = \begin{pmatrix} x^8 + x^6 \\ x^7 + x^4 \\ x^6 + x^3 \\ x^5 + x^2 \\ x^4 + x \\ x^3 + 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

iv) Use $h(x)$ to find a generator polynomial for $V^{\perp}$.

The generator polynomial for $V^{\perp}$ is is the dual (a.k.a., reciprocal) polynomial $h^*(x) = x^{\deg(h)} h\left(x^{-1}\right) = x^3\left(x^{-3} + 1\right) = x^3 + 1$. This can also be computed by reversing the order of the bits of $h(x)$.

Remark

$$\begin{array}{ccccc} (g(x)) = V & & \longleftrightarrow & & V^{\perp} = (h^*(x)) \\ & \searrow\nwarrow & & \swarrow\nearrow & \\ & & V^! = (h(x)) & & \end{array}$$

where $h(x) = (x^7 - 1)/g(x)$ and $h^*(x) = x^{\deg(h)} h(x^{-1})$ and that

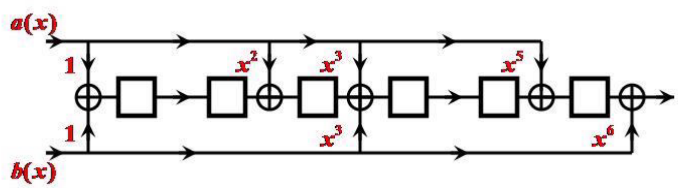
$$V^{\perp} = \{f(x) \in \mathcal{R}_9 : f(x) \cdot h(c) \quad \forall h(x) \in \mathcal{R}_9\} \quad \text{and} \quad V^! = \{f(x) \in \mathcal{R}_9 : f(x) \circ h(c) \quad \forall h(x) \in \mathcal{R}_9\}$$

where "$f(x) \cdot h(c)$" denotes vector inner product, and where "$f(x) \circ h(c)$" denotes ring product in the ring $\mathcal{R}_9 = GF(2)[x]/(x^9 - 1)$.

Problem 2.

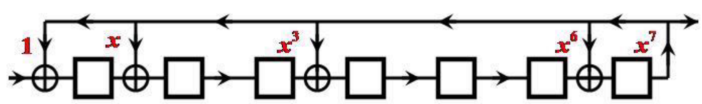
a) Draw a linear sequential circuit (LSC) that takes two polynomial inputs $a(x)$ and $b(x)$ and produces as output the polynomial:

$$\left(1 + x^2 + x^3 + x^5\right) a(x) + \left(1 + x^3 + x^6\right) b(x)$$



b) Draw a linear sequential circuit (LSC) that takes as input an arbitrary polynomial input $a(x)$, and produces as output:

$$\frac{a(x)}{1 + x + x^3 + x^6 + x^7}$$



Remark. Please refer to the handout on linear sequential circuits(a.k.a., linear switching circuits)

Problem 3. Let ξ be the primitive element of $GF(2^6)$ such that:

$$1+\xi+\xi^6=0$$

Use the attached antilog/log table (based on $p(x)=1+x+x^6$) of $GF(2^6)$ to find the minimum polynomial $m_{36}(x)$ of ξ^{36} .

The roots of $m_{36}(x)$ consist of ξ^{36} and all its conjugates. Hence, the roots of $m_{36}(x)$ are

$$\xi^{36}, \quad \xi^9, \quad \xi^{18}$$

Thus, $m_{36}(x)$ is of degree 3, i.e., $m_{36}(x)=x^3+a_2x^2+a_1x+a_0$. We will now determine the unknown coefficients:

$$\begin{aligned} 0 &= m_{36}(\xi^9)=(\xi^9)^3+a_2(\xi^9)^2+a_1(\xi^9)^1+a_0(\xi^9)^0 \\ \\ &= \xi^{27}+a_2\xi^{18}+a_1\xi^9+a_0 \end{aligned}$$

So,

$$a_2\xi^{18}+a_1\xi^9+a_0=\xi^{27}$$

Using the attached antilog/log table for $GF(2^6)$, we have

$$a_2\begin{pmatrix}1\\1\\1\\1\\0\\0\end{pmatrix}+a_1\begin{pmatrix}0\\0\\0\\1\\1\\0\end{pmatrix}+a_0\begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\1\\1\\1\\0\\0\end{pmatrix}$$

which can be rewritten as

$$\begin{pmatrix}a_2+a_0\\a_2\\a_2\\a_2+a_1\\a_1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\1\\1\\0\\0\end{pmatrix}$$

Thus, to determine $m_{36}(x)$ we need to solve the following system of equations over $GF(2)$

$$\begin{cases} a_2 \quad\quad + a_0 = 0 \\ a_2 \quad\quad\quad\quad = 1 \\ a_2 \quad\quad\quad\quad = 1 \\ a_2 + a_1 \quad\quad = 1 \\ \quad\quad a_1 \quad\quad = 0 \\ \quad\quad\quad\quad 0 = 0 \end{cases}$$

Solving this system, we find that

$$a_2 = 1, \quad a_1 = 0, \quad a_0 = 1$$

So finally we have

$$m_{36}(x) = x^3 + a_2x^2 + a_1x + a_0 = x^3 + 1 \cdot x^2 + 0 \cdot x + 1 = x^3 + x^2 + 1$$

Problem 4. Let α be the primitive element of $GF(2^6)$ which is the zero of the primitive polynomial:

$$1 + x + x^6$$

Let $g(x)$ be the polynomial of smallest degree having the following zeros:

$$\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \alpha^7,\ \alpha^8, \alpha^9, \alpha^{10}$$

Let $V = (g(x))$ be the corresponding cyclic code of smallest length.

a) Write $g(x)$ as a product of minimal polynomials $m_i(x)$, where $m_i(x)$ is the minimal polynomial of α^i. (**Do not explicitly compute the $m_i(x)$'s.**)

1	2	4	8	16	32	$m_1 = m_2 = m_4 = m_8$	(deg = 6)
3	6	12	24	48	33	$m_3 = m_6$	(deg = 6)
5	10	20	40	17	34	$m_5 = m_{10}$	(deg = 6)
7	14	28	56	49	35	m_7	(deg = 6)
9	18	36				m_9	(deg = 3)

Hence,

$$g(x) = LCM\,(m_1, m_2, \ldots, m_{10}) = LCM\,(m_1, m_3, m_5, m_7, m_9) = m_1m_3m_5m_7m_9$$

b) What is the degree of $g(x)$?

$$\deg(g) = \deg(m_1) + \deg(m_3) + \deg(m_5) + \deg(m_7) + \deg(m_9) = 6+6+6+6+3 = 27$$

c) What is the length n of V ?

$$n = LCM\left(ord\,(\alpha)\,, ord\left(\alpha^2\right), \ldots, ord\left(\alpha^{10}\right)\right) = ord\,(\alpha) = 63$$

d) What is the dimension of V ?

$$Dim\,(V) = codeg\,(g) = n - \deg(g) = 63 - 27 = 36$$

Problem 5. Let ξ be a primitive element of $GF(2^4)$ defined by

$$\xi = x \bmod p(x)$$

for the primitive polynomial

$$p(x) = 1 + x + x^4$$

Let $g(x)$ be the binary polynomial of smallest degree having

$$\xi \text{ and } \xi^3$$

as roots. Let $V = (g(x))$ be the cyclic code of smallest length having $g(x)$ as a generator polynomial. Use the enclosed table for $GF(2^4)$ to answer the following questions:

a) What is the length n of V?

$$n = LCM\left(ord\left(\xi\right), ord\left(\xi^3\right)\right) = LCM\left(15, 5\right) = 15$$

b) What is the dimension of $V^\perp$?

First we determine the degree of $g(x)$.

$$\begin{array}{cccccc} 1 & 2 & 4 & 8 & m_1 & (\deg = 4) \\ 3 & 6 & 12 & 9 & m_3 & (\deg = 4) \end{array}$$

Thus,

$$g(x) = LCM\left(m_1, m_3\right) = m_1 m_3 \Longrightarrow \deg\left(g(x)\right) = \deg\left(m_1\right) + \deg\left(m_3\right) = 4 + 4 = 8$$

$$Dim\left(V^\perp\right) = n - Dim\left(V\right) = n - codeg\left(g\right) = \deg\left(g\right) = 8$$

c) Use ξ and ξ^3 to construct a parity check matrix H of V. (Do not explicitly compute $g(x)$. Be sure that the rows of your parity check matrix are linearly independent.

$$\begin{aligned} H &= \begin{pmatrix} \xi^{n-1} & \xi^{n-2} & \cdots & \xi^1 & \xi^0 \\ \left(\xi^3\right)^{n-1} & \left(\xi^3\right)^{n-2} & \cdots & \left(\xi^3\right)^1 & \left(\xi^3\right)^0 \end{pmatrix} \\ &= \begin{pmatrix} \xi^{14} & \xi^{13} & \xi^{12} & \xi^{11} & \xi^{10} & \xi^9 & \xi^8 & \xi^7 & \xi^6 & \xi^5 & \xi^4 & \xi^3 & \xi^2 & \xi & 1 \\ \xi^{12} & \xi^9 & \xi^6 & \xi^3 & 1 & \xi^{12} & \xi^9 & \xi^6 & \xi^3 & 1 & \xi^{12} & \xi^9 & \xi^6 & \xi^3 & 1 \end{pmatrix} \end{aligned}$$

Using the Log/AntiLog table for $GF(2^4)$ given below, we have

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

Since $Dim\left(V^{\perp}\right) = 8$, the 8 rows of the above matrix must be linearly independent. Hence, H is a parity check matrix. If the rows of H were not linearly independent, then would need to put the matrix in echelon cannonical form (with all-zero rows deleted) to obtain the parity check. matrix.

$GF(2^4)$	
$p(x) = 1 + x + x^4$	
AntiLog $a_0a_1a_2a_3$	*Log*
0000	$-\infty$
1000	0
0100	1
0010	2
0001	3
1100	4
0110	5
0011	6
1101	7
1010	8
0101	9
1110	10
0111	11
1111	12
1011	13
1001	14

$GF(2^{6)}$	
$p(x) = 1 + x + x^6$	
Antilog $a_0a_1a_2\ a_3a_4a_5$	*Log*
000 000	$-\infty$
100 000	0
010 000	1
001 000	2
000 100	3
000 010	4
000 001	5
110 000	6
011 000	7
001 100	8
000 110	9
000 011	10
110 001	11
101 000	12
010 100	13
001 010	14
000 101	15
110 010	16
011 001	17
111 100	18
011 110	19
001 111	20
110 111	21
101 011	22
100 101	23
100 010	24
010 001	25
111 000	26
011 100	27
001 110	28
000 111	29
110 011	30

$GF(2^{6)}$	
$p(x) = 1 + x + x^6$	
Antilog $a_0a_1a_2\ a_3a_4a_5$	*Log*
101 001	31
100 100	32
010 010	33
001 001	34
110 100	35
011 010	36
001 101	37
110 110	38
011 011	39
111 101	40
101 110	41
010 111	42
111 011	43
101 101	44
100 110	45
010 011	46
111 001	47
101 100	48
010 110	49
001 011	50
110 101	51
101 010	52
010 101	53
111 010	54
011 101	55
111 110	56
011 111	57
111 111	58
101 111	59
100 111	60
100 011	61
100 001	62