Two Study Problems for Exam II
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

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

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

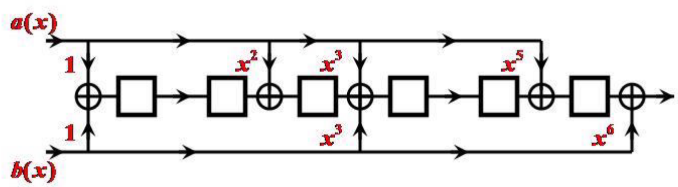
$$V^{\perp} = \{f(x) \in \mathcal{R}_9 : f(x) \cdot h(c) \quad \forall h(x) \in \mathcal{R}_9\} \quad \text{and} \quad V^! = \{f(x) \in \mathcal{R}_9 : f(x) \circ h(c) \quad \forall h(x) \in \mathcal{R}_9\}$$

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.

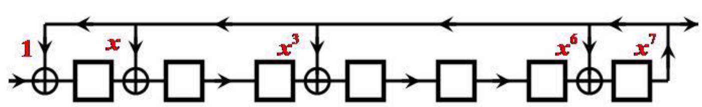
a) Draw a linear sequential circuit (LSC) that takes two polynomial inputs $a(x)$ and $b(x)$ and produces as output the polynomial:

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



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)