EE/Ma 127a Error-Correcting Codes R. J. McEliece

Draft of November 7, 2000 162 Moore

Homework Assignment 4, Solutions

Problem 1.

n=8, $x^8-1=(x+1)^8$

(n,k)	*g(x)*
(8,8)	1
(8,7)	$x+1$
(8,6)	$(x+1)^2$
(8,5)	$(x+1)^3$
(8,4)	$(x+1)^4$
(8,3)	$(x+1)^5$
(8,2)	$(x+1)^6$
(8,1)	$(x+1)^7$
(8,0)	$(x+1)^8$

n=9, $x^9-1=(x+1)(x^2+x+1)(x^6+x^3+1)$

(n,k)	g(x)
(9,9)	1
(9,8)	$x+1$
(9,7)	x^2+x+1
(9,6)	$(x+1)(x^2+x+1)$
(9,3)	x^6+x^3+1
(9,2)	$(x+1)(x^6+x^3+1)$
(9,1)	$(x^2+x+1)(x^6+x^3+1)$
(9,0)	$(x+1)(x^2+x+1)(x^6+x^3+1)$

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

(n,k)	g(x)
(10,10)	1
(10,9)	$x+1$
(10,8)	$(x+1)^2$
(10,6)	$x^4+x^3+x^2+x+1$
(10,5)	$(x+1)\ (x^4+x^3+x^2+x+1)$
(10,4)	$(x+1)^2(x^4+x^3+x^2+x+1)$
(10,2)	$(x^4+x^3+x^2+x+1)^2$
(10,1)	$(x+1)\ (x^4+x^3+x^2+x+1)^2$
(10,0)	$(x+1)^2(x^4+x^3+x^2+x+1)^2$

Problem 2.

$x^9-1=(x+1)(x^2+x+1)(x^6+x^3+1)$, $g(x)= (x+1)(x^2+x+1)=1+x^3$

$h(x)= 1+x^3+x^6$, $\tilde{h}(x) = 1 + x^3 + x^6$

$$G_1=\begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ x^3g(x) \\ x^4g(x) \\ x^5g(x) \end{bmatrix}=\begin{pmatrix} 1&0&0&1&0&0&0&0&0\\ 0&1&0&0&1&0&0&0&0\\ 0&0&1&0&0&1&0&0&0\\ 0&0&0&1&0&0&1&0&0\\ 0&0&0&0&1&0&0&1&0\\ 0&0&0&0&0&1&0&0&1 \end{pmatrix}$$

$$H_1=\begin{bmatrix} \tilde{h}(x) \\ x\tilde{h}(x) \\ x^2\tilde{h}(x) \end{bmatrix}=\begin{pmatrix} 1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1 \end{pmatrix}$$

For i=0,1,…,8, $x^i \bmod g(x) = x^i \bmod (x^3+1) = x^{i \bmod 3}$

$$G_2=\begin{pmatrix} 1&0&0&1&0&0&0&0&0\\ 0&1&0&0&1&0&0&0&0\\ 0&0&1&0&0&1&0&0&0\\ 1&0&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0&0&1 \end{pmatrix} \quad H_2=\begin{pmatrix} 1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1 \end{pmatrix}$$

Problem 3.
$g(x)=x^8+x^7+x^6+x^4+1$, $h(x)=(x^{15}-1)/g(x)=x^7+x^6+x^4+1$.
The three different shift-register encoders are:

(1) The non-systematic encoder of the form in figure 8.1, “Chapter 8” handout.
(2) The systematic encoder of the form in figure 8.5, “Chapter 8” handout.
(3) The systematic encoder of the form in figure 8.7, “Chapter 8” handout.

Problem 4.
(a)

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

$H=[A|I_5]$
(b) The decoding circuit is of the form in figure 8.8, “Chapter 8” handout.

Problem 5.

(a) C_k is the dual code of the (n, n-k) cyclic Hamming code, so $n=2^k-1$.

(Note: The proof needs the condition that C_k is the dual code of a Hamming code, without which we cannot complete the proof. However, the problem doesn't clearly state that you can use that condition, so I won't deduct any point for this sub-problem.)

(b) $n=2^k-1$, so $r=n-k>k$ except for the trivial case $k=2$. So an encoder of the form in figure 8.7, "Chapter 8" is preferred because it uses fewer components than the encoders in figure 8.5 or figure 8.1.

(c) The set of cyclic shifts of the first row of G_1 are: $[x^i g(x)]_n$ $(i=0,1,2,\ldots,n-1)$, each of which is a non-zero codeword. Since there are exactly 2^k-1 non-zero codewords, and $n=2^k-1$, we just need to prove that no two distinct cyclic shifts of the first row are the same. And we prove it by contradiction.
WLOG, suppose there exist i and j s.t. $0\le i<j\le n-1$, $[x^i g(x)]_n=[x^j g(x)]_n$.
Then $[x^j g(x)-x^i g(x)]_n=0 \Rightarrow (x^n-1)|(x^j g(x)-x^i g(x)) \Rightarrow g(x)h(x)|x^i(x^{j-i}-1)g(x)$
$\Rightarrow h(x)|x^i(x^{j-i}-1)$. Since h(x) is primitive, h(x) is irreducible. So either $h(x)|x^i$ or $h(x)|(x^{j-i}-1)$. However, since h(x) is primitive, and $0<j-i<n=2^k-1$, h(x) can divide neither x^i nor $x^{j-i}-1$. So there is a contradiction.

For C_4 with $h(x)=x^4+x+1$, $g(x)=x^{11}+x^8+x^7+x^5+x^3+x^2+x+1$. So the first row of G_1 is [1 1 1 1 0 1 0 1 1 0 0 1 0 0 0]. By listing all the 15 non-zero codewords we found that they are just the 15 cyclic shifts of the first row of G_1.

(d) Since C_k is a simplex code, all its non-zero codewords have weight $(n+1)/2$. So the weight enumerator is:
$A(z)=1+(2^k-1)z^{(n+1)/2}$

Problem 6.

For b=1, there are n ordinary bursts of length b.

For $2\le b\le n$, there are $n-b+1$ possibilities for the location of the ordinary burst. The b-2 bits between the first 1 and last 1 in the burst pattern can be arbitrary, and there are 2^{b-2} such strings. So the number of ordinary bursts is $(n-b+1)\,2^{b-2}$.