EE/Ma 127a Error-Correcting Codes - Homework Assignment 4

Ling Li, ling@cs.caltech.edu

November 3, 2000

4.1 Possible binary cyclic codes.

(a) $x^8 - 1 = (x+1)^8$.

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

(b) $x^9 - 1 = (x+1)(x^2+x+1)(x^6+x^3+1)$.

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

(c) $x^{10} - 1 = (x+1)^2(x^4+x^3+x^2+x+1)^2$.

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

4.2 The generator polynomial is $g(x) = (x+1)(x^2+x+1) = x^3+1$, the parity-check polynomial is $h(x) = (x^9-1)/(x^3+1) = x^6+x^3+1$. Thus for the $(9,6)$ cyclic code with $g(x)$:

$$
\begin{aligned}
G_1 &= \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ x^3g(x) \\ x^4g(x) \\ x^5g(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \\
H_1 &= \begin{bmatrix} \tilde{h}(x) \\ x\tilde{h}(x) \\ x^2\tilde{h}(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

$$
G_2 = \begin{bmatrix} x^3 - x^3 \bmod g(x) \\ x^4 - x^4 \bmod g(x) \\ x^5 - x^5 \bmod g(x) \\ x^6 - x^6 \bmod g(x) \\ x^7 - x^7 \bmod g(x) \\ x^8 - x^8 \bmod g(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}
$$

$$
\begin{aligned}
H_2 &= [1, x, x^2, x^3 \bmod g, x^4 \bmod g, x^5 \bmod g, x^6 \bmod g, x^7 \bmod g, x^8 \bmod g] \\
&= \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

It happens that $H_2 = H_1$.

4.3 $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, $h(x) = \left(x^{15} - 1\right)/g(x) = 1 + x^4 + x^6 + x^7$. Three encoding circuits are shown in Figure 1.

4.4 Since $g(x) = x^5 + x^2 + 1$, we have

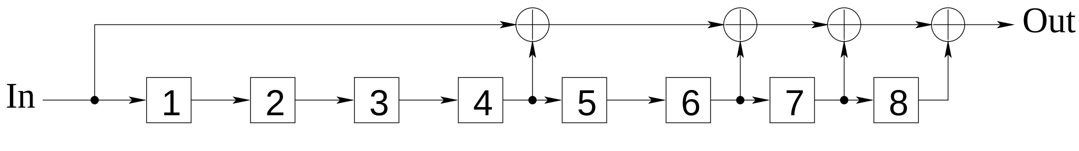
$$
\begin{aligned}
h(x) &= \left(x^{31} - 1\right)/g(x) \\
&= 1 + x^2 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{20} + x^{21} + x^{23} + x^{26}.
\end{aligned}
$$

(a) One parity-check matrix for this code is

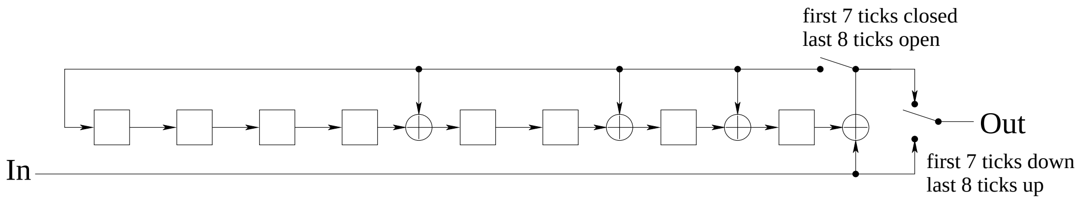
$$
H_1 = \begin{bmatrix} 1001011001111100011011101010000 \\ 0100101100111110001101110101000 \\ 0010010110011111000110111010100 \\ 0001001011001111100011011101010 \\ 0000100101100111110001101110101 \end{bmatrix}.
$$

Let

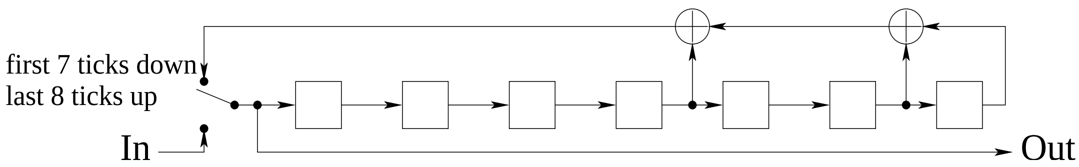
$$
P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix},
$$



(a) a nonsystematic encoder with $g(x)$



(b) An n-tick systematic encoder with $g(x)$



(c) A systematic shift-register encoder with $h(x)$

Figure 1: Three encoding circuits for the $(15, 7)$ binary cyclic code with $g(x) = 1+x^4+x^6+x^7+x^8$.

which is the inverse matrix of last 5 columns of H_1. Let

$$H = PH_1 = \begin{bmatrix} 1001011001111100011011101010000 \\ 0100101100111110001101110101000 \\ 1011001111100011011101010000100 \\ 0101100111110001101110101000010 \\ 0010110011111000110111010100001 \end{bmatrix}.$$

Since H is from H_1 via some row-transformations, and

$$GH^T = GH_1^T P^T = 0P^T = 0,$$

H is also a parity-check of the code $(31, 26)$. And, this is a systematic one.

(b) The decoding circuit for this code is similar to Figure 8.8 in Chapter 8.

4.5 Dual codes. (Discussed with Anxiao Jiang)

(a) I can proof that n is a multiply of $(2^k - 1)$, that is, $n = t(2^k - 1)$, where t is a positive integer.

From the definition of primitive polynomial (Wicker, p. 40), the smallest positive integer m for which $h(x)\,|x^m - 1$ is $m = 2^k - 1$. For $h(x)$ is a parity-check polynomial of code (n, k), we have $h(x)\,|x^n - 1$. Thus $h(x)\,|[(x^n - 1) \bmod (x^m - 1)]$, i.e.,

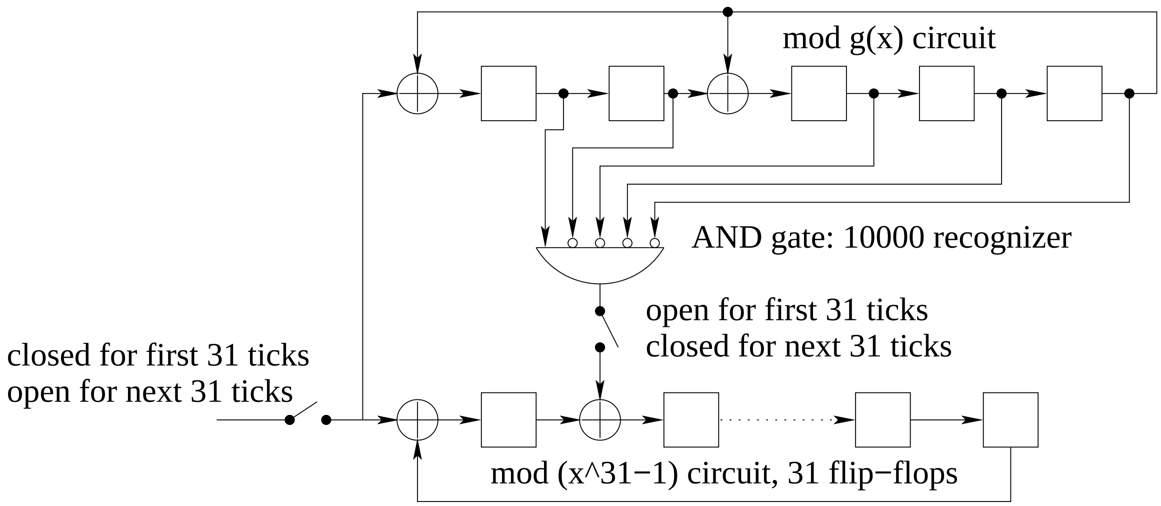


Figure 2: A decoding circuit for the $(31, 26)$ cyclic Hamming code with generator polnomial $g(x) = x^5 + x^2 + 1$.

$h(x)\,|x^{n \bmod m} - 1$. Since m is the smallest positive integer for which $h(x)\,|x^m - 1$, and $n \bmod m < m$, we know $n \bmod m = 0$. Thus $n = tm = t(2^k - 1)$, where t is a positive integer.

However, n is not necessary $2^k - 1$. Here's an example that n is larger than $2^k - 1$: the cyclic code $(6, 2)$, with $n = 6$, $k = 2$, $h(x) = x^2 + x + 1$ is a primitive polynomial. We can calculate the generator polynomial $g(x) = (x + 1)(x^3 + 1)$ and it is easy to verify that $n = 6$ is the smallest n that $g(x)$ divides $x^n - 1$. So this code is also proper. However, $n > 2^k - 1 = 3$.

(b) Usually, $n = t(2^k - 1) \gg k$, thus $r = n - k \gg k$. So a systematic shift-register encoder designed from the parity-check polynomial $h(x)$ will usually have much less adders and flip-flops than those designed from the generator polynomial, thus much more efficient. The encoder has the structure in Figure 8.7 of Chapter 8.

(c) Here $n = 2^k - 1$ is assumed. Let $\mathbf{C}_1 = (C_0, C_1, \ldots, C_{n-1})$ denote the first row of G_1, whose polynomial is $g(x) = C_0 + C_1 x + \cdots + C_{n-k} x^{n-k}$. After i right cyclic shifts, the first row of G_1 becomes $\left[x^i g(x)\right]_n$, which is also a nonzero codeword of $\mathcal{C}_k$.

We claim that for $0 \le i < j < n$, $\left[x^i g(x)\right]_n \ne \left[x^j g(x)\right]_n$. If not so, we can right cyclic shift $\left[x^i g(x)\right]_n$ and $\left[x^j g(x)\right]_n$ for i times, and get $g(x) = \left[x^{j-i} g(x)\right]_n$. Let p denote the greatest common divisor of n and $(j - i)$, then there exist two positive integers a and b such that $a \times (j - i) - b \times n = p$. Thus

$$g(x) = \left[x^{a(j-i)} g(x)\right]_n = \left[x^{bn+p} g(x)\right]_n = \left[(x^{bn} - 1)x^p g(x) + x^p g(x)\right]_n = \left[x^p g(x)\right]_n .$$

That means, $C_{(i+p) \bmod n} = C_i$ for $0 \le i < n$. Considering that $p|n$, we have $C_i = C_{i \bmod p}$. Thus

$$g(x) = \left(C_0 + C_1 x + \cdots + C_{p-1} x^{p-1}\right)\left(1 + x^p + \cdots + x^{n-p}\right) = g'(x) p(x),$$

where $g'(x) = \left(C_0 + C_1 x + \cdots + C_{p-1} x^{p-1}\right)$ is the repeated part of $\mathbf{C}_1$ and $p(x) = (1 + x^p + \cdots + x^{n-p})$ is the repeat factor. Since we have $g(x)h(x) = x^n - 1$, we know that $p(x)$ divides $(x^n - 1)$. Thus

$$g'(x)h(x) = \frac{x^n - 1}{p(x)} = x^p - 1.$$

This contracts that $h(x)$ is a primitive polynomial of degree k and $n = 2^k - 1$ is the smallest positive integer such that $h(x)\,|x^n - 1$ and $0 < p \le j - i < n$. So $\left[x^i g(x)\right]_n \neq \left[x^j g(x)\right]_n$ for $0 \le i < j < n$.

Thus the set of cyclic shifts of $\mathbf{C}_1$ contains n distinct nonzero codewords of $\mathcal{C}_k$. Since $\mathcal{C}_k$ has only 2^k codewords, out of which $2^k - 1 = n$ codewords are nonzero, so the set of nonzero codewords is exactly equal to the set of cyclic shifts of $\mathbf{C}_1$.

For $\mathcal{C}_4$: $n = 2^4 - 1 = 15$, $k = 4$, $h(x) = x^4 + x + 1$. $g(x) = \left(x^{15} - 1\right)/h(x) = 1 + x + x^2 + x^3 + x^5 + x^7 + x^8 + x^{11}$. The first row of G_1 is $\mathbf{C}_1 = 111101011001000$. Below are all the elements in the set of cyclic shifts of $\mathbf{C}_1$:

$$\begin{aligned}
\mathbf{C}_1 &= 111101011001000 \\
x\mathbf{C}_1 &= 011110101100100 \\
x^2\mathbf{C}_1 &= 001111010110010 \\
x^3\mathbf{C}_1 &= 000111101011001 \\
\left[x^4\mathbf{C}_1\right]_n &= 100011110101100 \\
\left[x^5\mathbf{C}_1\right]_n &= 010001111010110 \\
\left[x^6\mathbf{C}_1\right]_n &= 001000111101011 \\
\left[x^7\mathbf{C}_1\right]_n &= 100100011110101 \\
\left[x^8\mathbf{C}_1\right]_n &= 110010001111010 \\
\left[x^9\mathbf{C}_1\right]_n &= 011001000111101 \\
\left[x^{10}\mathbf{C}_1\right]_n &= 101100100011110 \\
\left[x^{11}\mathbf{C}_1\right]_n &= 010110010001111 \\
\left[x^{12}\mathbf{C}_1\right]_n &= 101011001000111 \\
\left[x^{13}\mathbf{C}_1\right]_n &= 110101100100011 \\
\left[x^{14}\mathbf{C}_1\right]_n &= 111010110010001
\end{aligned}$$

It's easy to see that these 15 codewords are distinct.

(d) From (c), we know that all the nonzero codewords are a cyclic shift of $\mathbf{C}_1$, thus have the same weight as $\mathbf{C}_1$. And this code is a dual code to the Hamming code $\left(2^k - 1, 2^k - k - 1\right)$, So the weight enumerator is $1 + (2^k - 1)x^{2^{k-1}}$.

4.6 For bursts of length $b > 1$, let s denote the position of the first 1 and thus the position of the last 1 is $s + b - 1$. From $0 \le s < s + b - 1 \le n - 1$, we have $0 \le s \le n - b$. The bits at positions between s and $s + b - 1$ can be either 0 or 1, so we have 2^{b-2} vectors with such s and b. Thus the number of vectors with bursts of length $b > 1$ is

$$\sum_{e=0}^{n-b} 2^{b-2} = (n - b + 1)2^{b-2}.$$

For $b = 1$, i.e., only one bit is 1, we have the number of different vectors with bursts of length 1 is n.