EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2010

Solutions to Assignment 5 — Prepared by Sravan Kumar Jatavath

1. Given: (8,7) single parity check code.

   Single parity check codewords are all of even parity. Let A_i be the number of codewords of Hamming weight i.

   $\mathrm{A}_0 = 1$ (trivial, codeword of all zeros)
   $\mathrm{A}_1 = 0$
   $\mathrm{A}_2 = 8_{C_2} = \frac{8\times 7}{2} = 28$
   $\mathrm{A}_3 = 0$
   $\mathrm{A}_4 = 8_{C_4} = 70$
   $\mathrm{A}_5 = 0$
   $\mathrm{A}_6 = 8_{C_6} = 28$
   $\mathrm{A}_7 = 0$
   $\mathrm{A}_8 = 1$

   Now, error is undetected when error pattern is a codeword.

   If $\mathrm{P}_u(\mathrm{E})$ = probablity of undetected error,

   $\mathrm{P}_u(\mathrm{E}) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$
   $\mathrm{P}_u(\mathrm{E}) = 28p^2(1-p)^6 + 70p^4(1-p)^4 + 28p^6(1-p)^2 + p^8$

2. (15,11) Hamming Code

   The parity check matrix of a Hamming code consists of all non-zero n-tuples as columns.

   In a systematic form,

$$H = \begin{bmatrix} I_m & Q \end{bmatrix}$$

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

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Now, consider

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Note that there are no zero columns and no two columns add up to zero (no two identical colums). Furthermore, no three columns will add up to zero because the last row of the sum of three columns will always be 1.

There exist 4 columns which add up to zero (columns 1,2,3,11).

$\therefore\ d_{min} > 3$ but $d_{min} \leq 4$

$\Rightarrow d_{min} = 4$

$\Rightarrow$ number of errors that can be corrected $= \lfloor \frac{d_{min}-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$.

When a single error occurs, the syndrome is equal to a column of H_1 which always has a 1 in the last row. When two errors occur, the syndrome is a sum of two columns which has a 0 in the last row. So when the decoder sees a 1 in the last row of the syndrome it will try to correct the error. When it sees a 0 in the last row of the syndrome it will declare an uncorrectable number of errors and give up. Specifically two errors can be detected. In fact, any even number of errors can be detected.

In this new code, $n = 16$, $k = 16 - 5 = 11$ and the rate of the code $= \frac{11}{16}$.

Sol 4 a) g(X) $= 1 + X + X^4$
and h(X) $= \frac{1+X^{15}}{1+X+X^4}$
$\therefore$ h(X) $= 1 + X + X^2 + X^3 + X^5 + X^7 + X^8 + X^{11}$

b) Generator polynomial for the dual code
$= \mathrm{X}^{11}.\mathrm{h}(\mathrm{X}^{-1})$
$= \mathrm{X}^{11}[1 + X + X^2 + X^3 + X^5 + X^7 + X^8 + X^{11}] = 1 + X^3 + X^4 + X^6 + X^8 + X^9 + X^{10} + X^{11}$

c) n=15 and k=11
$b_0(X) = \frac{X^{15-11}}{g(X)} = X + 1$
Similarly finding $b_1(X), b_2(X), \ldots\ldots b_{10}(X)$ where $b_i(X)$ is the remainder of X^{n-k-i} when divided by g(X), where $i = 0, 1, 2, 3, \ldots, k-1$. Now $X^{n-k-i} = a_i(X)g(X) + b_i(X) \Rightarrow X^{n-k-i} + b_i(X) = a_i(X)g(X)$ is a multiple of $g(X)$. Therefore it is a codeword for $i = 0, 1, \ldots, k-1$. These codewords are k linearly independent since each of them have a power of X which none of the others have, namely X^{n-k-i}. So they can be arranged as the rows of a generator matrix for the code.
$b_0(X) = X + 1$
$b_1(X) = X^2 + X$
$b_2(X) = X^3 + X^2$
$b_3(X) = X^3 + X + 1$
$b_4(X) = X^2 + 1$
$b_5(X) = X^3 + X$
$b_6(X) = X^2 + X + 1$
$b_7(X) = X^3 + X^2 + X$
$b_8(X) = X^3 + X^2 + X + 1$
$b_9(X) = X^3 + X^2 + 1$
$b_{10}(X) = X^3 + 1$

$$G = [P \;\; I_{11}] = \left[\begin{array}{cccccccccccccccc} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

and $H = [I_4 \;\; P^T]$

Sol 5 $g(X)$ = generator polynomial of binary cyclic code of length n.

(a) If $g(X)$ has X+1 as a factor,

V(X) = a(X).g(X)

$\Rightarrow$ g(X) | V(X)
$\Rightarrow$ (X+1)| V(X) $\Rightarrow$ (X+1) divides all codeword polynomial

V(1)= 0 for all codeword polynomials.

$V_nX^n + V_{n-1}X^{n-1} + \ldots\ldots + V_0 = \text{V(X)}$

$\text{V(1)} = V_n + V_{n-1} + \ldots\ldots + V_0 = 0$

$\Rightarrow$ Codeword has even weight
$\Rightarrow$ No codeword has odd weight

(b) If n is odd & (X+1) $\nmid$ g(X)
(X+1) $\nmid$ g(X)
(X+1) | $X^n + 1$

g(X) | $X^n + 1$

$\Rightarrow$ (X+1) | h(X) $\Rightarrow$ (X+1) | $X^k h(X^{-1})$ (Because 1 is a root of $X^k h(X^{-1})$. Just consider sum of coefficients.)
$\Rightarrow$ Codes in dual space have even parity (from part (a) above)

$\Rightarrow$ With odd n and all 1^s code cannot be in this dual code, since it has odd parity. So $h(X) \nmid 1 + X + X^2 + \ldots + X^{n-1}$. But $(1+X)(1+X+X^2+\ldots+X^{n-1}) = X^n + 1 = g(X)h(X) \Rightarrow g(X) \mid 1 + X + X^2 + \ldots + X^{n-1}$.

(c) n is the smallest integer s.t g(X) | $X^n + 1$
To prove minimum weight ≥ 3, we essentially need to prove W_{min} ¿ 2, i.e., no two columns in G add up to zero.
Let's assume to contrary, two columns in G add up to zero.
i.e., there exists a code of weight 2.
Let that code be V(X) = $X^a + X^b$ a,b <n, a >b

$\Rightarrow$ u(X).g(X) = $X^a + X^b$

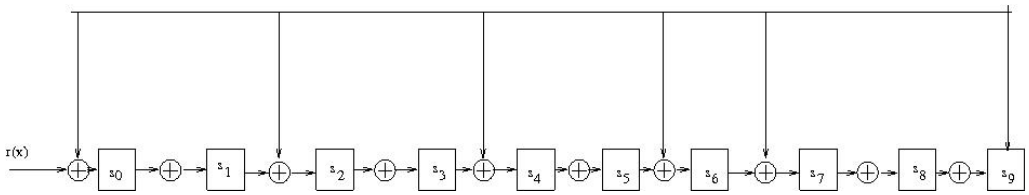
u(X).g(X) = $X^b(X^{a-b} + 1)$

g(X) and X^b are relatively prime.
$\Rightarrow$ g(X) | $X^{a-b} + 1 \Rightarrow$ Contradiction
Since n is the smallest integer s.t g(X) | $X^n + 1$ and a-b <n
Hence proved.

Sol 6

$$g(X) = 1 + X^2 + X^4 + X^6 + X^8 + X^{10} \tag{1}$$

It can be verified that $1+X^2+X^4+X^6+X^8+X^{10}$ divides $X^{21}+1$



Syndrome Computation Circuit:

Feedback branches corresponding to 0 can be just removed (no connections required for those).

$r(X) = 1+X^5+X^{17} = p(X).g(X) + s(X)$

$s(X)$ = remainder $(\frac{r(X)}{g(X)})$ = remainder $\frac{X^{17}+X^5+1}{X^{10}+X^7+X^6+X^4+X^2+1}$

$$\boxed{s(X) = X^8 + X^6 + X^4 + X^3 + 1} \tag{2}$$

Sol 7 Codeword corresponding to u(X) is $v(X) = X^{n-k}u(X) + r(X)$ where $r(X)$ is the remainder obtained by dividing $X^{n-k}u(X)$ by the generator polynomial $g(X)$. For the given $u(X)$,

$v(X) = 1 + X + X^2 + X^4 + X^5 + X^9 + X^{10} + X^{11} + X^{13} + X^{19}$.

V(X) = (1 1 1 0 1 1 0 0 0 1 1 1 0 1 0 0 0 0 0 1)

Encoding Circuit :