EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2011

Solution to Assignment 3

1. Let $g(X)$ be the generator polynomial of a binary cyclic code of length n.

   (a) Show that if $g(X)$ has $X+1$ as a factor, the code contains no codewords of odd weight.

   Solution: Since every code polynomial in a cyclic code is a multiple of the generator polynomial $g(X)$, every code polynomial has $X+1$ as a factor. This implies that $c(1) = 0$ for a code polynomial $c(X)$ which in turn requires $c(X)$ to have an even number of terms. So every codeword is of even weight.

   (b) If n is odd and $X+1$ is not a factor of $g(X)$, show that the code contains a codeword consisting of all ones.

   Solution: The oddness of n is in fact not required for the existence of a codeword consisting of all ones. We know that the generator polynomial $g(X)$ divides $X^n + 1$. We have

   $$a(X)g(X) = X^n + 1 = (X+1)(X^{n-1} + X^{n-2} + \cdots + X + 1). \tag{1}$$

   Since $X+1$ appears on the right hand side and is not a factor of $g(X)$, it has to be a factor of $a(X)$. Let $a(X) = (X+1)b(X)$. This implies

   $$b(X)g(X) = X^{n-1} + X^{n-2} + \cdots + X + 1. \tag{2}$$

   So $g(X)$ divides $X^{n-1} + X^{n-2} + \cdots + X + 1$ and hence the all ones codeword is contained in this code.

   (c) Show that the code has a minimum weight of at least 3 if n is the smallest integer such that $g(X)$ divides $X^n + 1$.

   Solution: For this question to be well defined n has to be at least 3. In the minimum weight calculation of a code, we consider only nonzero codewords. So it is enough to show that weight one and weight two codewords do not exist.

   If a weight one codeword exists, its corresponding code polynomial will be of the form X^i for $0 \leq i \leq n-1$ which has to be divisible by $g(X)$. The generator polynomial of a cyclic code has a nonzero constant term. We have $g(X) \neq 1$ because otherwise $g(X)$ would divide $X+1$ which is not equal to $X^n + 1$ for $n \geq 3$. So $g(X)$ has at least two terms which implies that any polynomial multiple of $g(X)$ has at least two terms. Thus X^i cannot be a multiple of $g(X)$. In fact, X^i and $g(X)$ have no factors in common because if they do the common factor will have to be of the form X^j for $1 \leq j \leq i$. Such a factor has zero as a root but zero is not a root of $g(X)$ because it has a nonzero constant term.

If a weight two codeword exists, its corresponding code polynomial will be of the form $X^i + X^j$ for $0 \leq i < j \leq n-1$ which has to be divisible by $g(X)$. So $X^j(X^{i-j}+1)$ has to be divisible by $g(X)$. Since $g(X)$ and X^j have no factors in common, $X^{i-j}+1$ has to be divisible by $g(X)$ but this is not possible since $i-j \leq n-1$.

Since no weight one or two codewords exist, the minimum weight is at least three.

2. (a) For a cyclic code, if an error pattern $e(X)$ is detectable, show that its ith cyclic shift $e^{(i)}(X)$ is also detectable.

Solution: If an error pattern $e(X)$ is detectable, $e(X) \neq 0 \mod g(X)$. The ith cyclic shift $e^{(i)}(X)$ is equal to $X^i e(X) \mod X^n+1$ where n is the blocklength of the cyclic code. Let $a(X)$ be the quotient when $X^i e(X)$ is divided by X^n+1. Then $X^i e(X) = a(X)(X^n+1) + e^{(i)}(X)$ which implies $e^{(i)}(X) = X^i e(X) + a(X)(X^n+1)$. If we divide both sides by $g(X)$, we get

$$\begin{aligned} e^{(i)}(X) \mod g(X) &= X^i e(X) \mod g(X) + a(X)(X^n+1) \mod g(X) \\ &= X^i e(X) \mod g(X) \end{aligned}$$

where the second equality is obtained by the fact that $g(X)$ divides X^n+1. The error pattern $e^{(i)}(X)$ is undetectable if and only if $e^{(i)}(X) \mod g(X)$ is equal to zero which happens if and only if $X^i e(X) \mod g(X)$ is equal to zero. Since $g(X)$ and X^i have no factors in common (see solution to question 1(c)), $g(X)$ would need to divide $e(X)$. But this is not possible as $e(X) \mod g(X)$ is not equal to zero.

(b) Let $v(X)$ be a code polynomial in a cyclic code of length n. Let i be the smallest integer such that $v^{(i)}(X) = v(X)$. Show that if $i \neq 0$, i is a factor of n.

Solution: Since n cyclic shifts of a codeword of length n returns the codeword to the initial state, $v^{(n)}(X) = v(X)$. If i is not a factor of n, divide n by i to get a quotient q and remainder r $(0 \leq r < i)$, $n = qi + r$. We get

$$v(X) = v^{(n)}(X) = v^{(qi+r)}(X) = v^{(i+[q-1]i+r)}(X) = v^{([q-1]i+r)}(X) = \cdots = v^{(r)}(X)$$

Since i is the smallest integer such that $v(X) = v^{(i)}(X)$ and $0 \leq r < i$, we must have $r = 0$. Thus i divides n.

3. Consider a binary (n,k) cyclic code C generated by $g(X)$. Let $g^*(X) = X^{n-k}g(X^{-1})$ be the reciprocal polynomial of $g(X)$.

(a) Show that $g^*(X)$ also generates an (n,k) cyclic code.

Solution: Since any polynomial which divides X^n+1 generates an (n,k) cyclic code, we need to prove that $g^*(X)$ divides X^n+1. Since $g(X)$ generates an (n,k) cyclic code it has degree $n-k$ and it divides X^n+1. Let $g(X)h(X) = X^n+1$ where the degree of $h(X)$ is k. We get

$$\begin{aligned} g(X^{-1})h(X^{-1}) &= X^{-n}+1 \\ \Rightarrow X^n g(X^{-1})h(X^{-1}) &= X^n(X^{-n}+1) = 1+X^n \\ \Rightarrow X^{n-k} g(X^{-1}) X^k h(X^{-1}) &= 1+X^n. \end{aligned}$$

Both $X^{n-k}g(X^{-1})$ and $X^k h(X^{-1})$ are polynomials in X since $g(X)$ has degree $n-k$ and $h(X)$ has degree k. From the above expression, we see that $g^*(X) = X^{n-k}g(X^{-1})$ divides $X^n + 1$ and as a consequence it generates an (n, k) cyclic code.

(b) Let C^* be the cyclic code generated by $g^*(X)$. Show that C and C^* have the same weight distribution. (*Hint:* If $v(X)$ is a code polynomial in C, then $X^{n-1}v(X^{-1})$ is a code polynomial in C^*).

Solution: Any codeword in C corresponds to a code polynomial $v(X) = u(X)g(X)$ where the degree of $u(X)$ is at most $k-1$. The number of terms in $v(X)$ corresponds to the weight of the corresponding codeword. The polynomial $X^{n-1}v(X^{-1})$ has the same number of terms as $v(X)$ albeit in reverse order. We will show that for every code polynomial in C there is a code polynomial in C^* with the same number of terms. This will in turn prove that for every codeword in C there is an equal weight codeword in C^*. So the weight distributions of these two codes will have to be the same. We have

$$\begin{aligned} v(X) &= u(X)g(X) \\ X^{n-1}v(X^{-1}) &= X^{n-1}u(X^{-1})g(X^{-1}) \\ X^{n-1}v(X^{-1}) &= X^{k-1}u(X^{-1})X^{n-k}g(X^{-1}) \\ X^{n-1}v(X^{-1}) &= X^{k-1}u(X^{-1})g^*(X) \end{aligned}$$

Since the degree of $u(X)$ is at most $k-1$, $X^{k-1}u(X^{-1})$ is a polynomial. Thus $X^{n-1}v(X^{-1})$ is a polynomial multiple of $g^*(X)$. It is thus a code polynomial in C^*. So for every code polynomial in C there is a code polynomial in C^*.

4. Draw the Meggitt decoder circuit for the $(7, 3)$ binary cyclic code generated by $g(X) = (X+1)(X^3+X+1)$

Solution: For the Meggitt decoder, we need to identify all correctable error patterns which have a one in the last location, i.e. the corresponding polynomial representation has the term X^6. For this code $n = 7$ and $k = 3$, so there are $2^{n-k} = 2^4 = 16$ correctable error patterns. These can be found by constructing the standard array. First we calculate the eight codewords and find that the minimum weight of the nonzero codewords is four. So if we take weight one coset leaders the cosets will contain vectors of weight at least three. So after we choose all weight one vectors as coset leaders we are free to choose any weight two vector as a coset leader for the ninth coset because it has not appeared so far in the standard array. But we choose those weight two vectors as coset leaders which have a one in the last location so that the Megitt decoder can immediately correct it. When weight two vectors are chosen as coset leaders other weight two vectors can appear in the coset and hence care must be taken to make sure that they are not chosen as coset leaders for the subsequent cosets. There are $\binom{7}{2} = 21$ weight two vectors of length 7 and they all appear within the first 15 cosets. For the last coset, the coset leader has to be of weight three and we choose it to be 0100011 because it has a one in the last location. We could also have chosen 0001101 or 1010001.

Once we have constructed the standard array, we see that the coset leaders of cosets 2, 9, 10, 11, 12, 13, 14 and 16 have a one in the last location i.e. their corresponding

1	0000000	1011100	0101110	0010111	1110010	1001011	0111001	1100101
2	0000001	1011101	0101111	0010110	1110011	1001010	0111000	1100100
3	0000010	1011110	0101100	0010101	1110000	1001001	0111011	1100111
4	0000100	1011000	0101010	0010011	1110110	1001111	0111101	1100001
5	0001000	1010100	0100110	0011111	1111010	1000011	0110001	1101101
6	0010000	1001100	0111110	0000111	1100010	1011011	0101001	1110101
7	0100000	1111100	0001110	0110111	1010010	1101011	0011001	1000101
8	1000000	0011100	1101110	1010111	0110010	0001011	1111001	0100101
9	0000011	1011111	0101101	0010100	1110001	1001000	0111010	1100110
10	0000101	1011001	0101011	0010010	1110111	1001110	0111100	1100000
11	0001001	1010101	0100111	0011110	1111011	1000010	0110000	1101100
12	0010001	1001101	0111111	0000110	1100011	1011010	0101000	1110100
13	0100001	1111101	0001111	0110110	1010011	1101010	0011000	1000100
14	1000001	0011101	1101111	1010110	0110011	0001010	1111000	0100100
15	0100010	1111110	0001100	0110101	1010000	1101001	0011011	1000111
16	0100011	1111111	0001101	0110100	1010001	1101000	0011010	1000110

polynomials have a X^6 term. So the error pattern detection circuit of the Megitt decoder should output a one when the syndromes corresponding to these coset leaders appears in the syndrome register. The truth table of the error pattern detection circuit is given in the last two columns of the following table. If the syndrome is represented as the bit string $abcd$, using Karnaugh map minimization we get the error pattern detection circuit to be equal to $bd + (b + c)(a\bar{c} + \bar{a}c)$.

	Coset leader	Syndrome	Syndrome (binary)	
1	0	0	0000	0
2	X^6	X^3+X^2+X	0111	1
3	X^5	X^2+X+1	1110	0
4	X^4	X^3+X^2+1	1011	0
5	X^3	X^3	0001	0
6	X^2	X^2	0010	0
7	X	X	0100	0
8	1	1	1000	0
9	X^6+X^5	X^3+1	1001	1
10	X^6+X^4	$X+1$	1100	1
11	X^6+X^3	X^2+X	0110	1
12	X^6+X^2	X^3+X	0101	1
13	X^6+X	X^3+X^2	0011	1
14	X^6+1	X^3+X^2+X+1	1111	1
15	X^5+X	X^2+1	1010	0
16	X^6+X^5+X	X^3+X+1	1101	1