EE 605: Error Correcting Codes (Autumn 2015)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Problem Set 2 Date: August 28, 2015

1. [5 points] Let C be a binary Hamming code of dimension k.
   (a) Find the number of minimum weight nonzero codewords in C in terms of k.
   (b) Find the number of maximum weight codewords in C as a function of k.
2. [5 points] Write down the systematic generator and parity check matrices for the $(15, 11)$ Hamming code. Let the parity check matrix be H. Consider a new parity check matrix H_1 formed by appending a column of zeros to the matrix H and then adding a row of ones. Show that the code with H_1 as the parity check matrix can correct single errors and detect double errors. What is the rate of this new code?
3. [5 points] Let $\mathbf{H}$ be the parity check matrix of a Hamming code of length $n = 2^m - 1$. Consider a matrix $\mathbf{H}'$ obtained by removing all columns of even weight from $\mathbf{H}$. Let C be the code whose parity check matrix is $\mathbf{H}'$?
   (a) Find the length and dimension of C.
   (b) Show that C can correct all single bit errors and detect all two-bit errors.
4. [5 points] Find the generator matrices corresponding to the following Reed-Muller codes.
   (a) $\mathrm{RM}(1, 3)$
   (b) $\mathrm{RM}(2, 3)$
   (c) $\mathrm{RM}(1, 4)$
5. [5 points] Suppose a codeword from the $\mathrm{RM}(2, 4)$ code is transmitted over a noisy channel and the vector $\begin{bmatrix}1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0\end{bmatrix}$ is received. Write down the steps of majority-logic decoding and find the 11-bit transmitted message.
6. [5 points] Show that the binary Reed-Muller codes $\mathrm{RM}(1, 4)$ and $\mathrm{RM}(2, 4)$ are dual codes of each other.
7. [5 points] Let C_1 and C_2 be two cyclic codes of same length n with generator polynomials $g_1(X)$ and $g_2(X)$ respectively. Show that $C_1 \subseteq C_2$ if and only if $g_2(X)$ divides $g_1(X)$.
8. [5 points] Let C_1 and C_2 be two cyclic codes of same length n with generator polynomials $g_1(X)$ and $g_2(X)$ respectively. Show that $C_1 \cap C_2$ is a cyclic code. What is its generator poynomial?
9. [5 points] 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.
   (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.
   (c) Show that the code has a minimum weight of at least 3 if n is the smallest integer such that $g(X)$ divides $X^n + 1$.

10. [5 points] (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.

    (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.

11. [5 points] 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.

    (b) Let C_1 be the cyclic code generated by $g^*(X)$. Find the weight enumerator of C_1 in terms of the weight enumerator $A(z)$ of C.

12. [5 points] For an (n, k) binary cyclic code, show the following.

    (a) The fraction of undetectable bursts of length $n - k + 1$ is $2^{-(n-k-1)}$.

    (b) For $m > n - k + 1$, the fraction of undetectable bursts of length m is $2^{-(n-k)}$.

13. [5 points] Let $g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^10$.

    (a) Show that $g(X)$ generates a $(21, 11)$ cyclic code. Devise a syndrome computation circuit for this code. Compute the syndrome of $r(X) = 1 + X^5 + X^{17}$.

    (b) Devise a systematic encoding circuit for this code. Compute the codeword corresponding to the input $u(X) = 1 + X + X^3 + X^9$.

14. [5 points] Let $\mathbf{g}(X)$ be the generator polynomial of an (n, k) binary cyclic code C. The code polynomials $\mathbf{v}(X)$ are multiples of $\mathbf{g}(X)$ of degree $n - 1$ or less

    $$\mathbf{v}(X) = \mathbf{u}(X)\mathbf{g}(X)$$

    where $\mathbf{u}(X) = u_0 + u_1X + u_2X^2 + \cdots + u_{k-1}X^{k-1}$ is the message polynomial.

    Consider the code polynomials generated by message polynomials of degree $k - l - 1$ or less where $l < k$, i.e. $u_{k-l} = u_{k-l+1} = \cdots = u_{k-1} = 0$. There are 2^{k-l} such code polynomials which have degree $n - l - 1$ or less. They form a $(n - l, k - l)$ linear block code called the shortened cyclic code and it is not a cyclic code.

    If $\mathbf{g}(X) = (X + 1)\mathbf{p}(X)$ where $\mathbf{p}(X)$ is a primitive polynomial of degree m where $n = 2^m - 1$, then show the following.

    (a) The shortened cyclic code can detect all error patterns of odd weight in the codeword of length $n - l$.

    (b) The shortened cyclic code can detect all double-bit error patterns in the codeword of length $n - l$.

    (c) The shortened cyclic code can detect all non-end-around burst errors of length $n - k$ or less in the codeword of length $n - l$.

    Note that the shortening operation destroys the cyclic property of the code. The shortened code loses the ability to detect end-around bursts of length $n - k$ or less. But we gain the ability to have an arbitrary length and still detect double-bit errors.