HW6 Solution

1 Shortened Cyclic Code

Sol: a) To prove that the shortened cyclic code is linear, it's equivalent to prove that if c_1 and c_2 are codewords in the shortened cyclic code, so is $c_1 + c_2$. Let $C_1(x)$ and $C_2(x)$ be the *generating function* of c_1 and c_2 respectively, by the definition of shortened cyclic code, $C_i(x)$ $(i = 1, 2)$ are multiples of $g(x)$ with degree $\leq n_o - 1$. Hence, clearly, $C_1(x) + C_2(x)$ is a multiple of $g(x)$, with degree $\leq n_o - 1$, which is exactly the generating function of $c_1 + c_2$.
b) Let

$$G_1 = \left\{ \begin{array}{c} g(x) \\ xg(x) \\ \vdots \\ x^9 g(x) \end{array} \right\}.$$

Since each row in G_1 is a codeword in shortened cyclic code, and it has dimension 10, it must be the generator matrix of the shortened cyclic code. Hence,

$$G_1 = \left\{ \begin{array}{cccccccccccccccc}
1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1
\end{array} \right\}.$$

Since the shortened cyclic code is the subset of original code which has all zeros at the bits from 17 to 21, its parity check matrix can be obtained by deleting the last five columns of the original parity check matrix H. So,

$$H_1 = \left\{ \begin{array}{cccccccccccccccc} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{array} \right\}.$$

2 Wicker 5.9

Sol: By Theorem 5.4-5.6 in Wicker, we have:

b	Detectable fraction
4	1
5	1
6	15/16
7	31/32
8	31/32

3 Problem 3

Sol: a) Since all the columns are nonzero and distinct, the minimum distance $d \geq 3$. Now if $a, b, c \in 1, \ldots, F$, $a + b + c = 0$, then $f(a) + f(b) + f(c) = T(a+b+c)+3y = 0+y \neq 0$, this means no three columns will sum up to zero, so $d \geq 4$. On the other hand, $1+2+4+7$=0 and $f(1)+f(2)+f(4)+f(7) = T(1+2+4+7)+4y = 0$, so there are four columns summing to 0. Hence $d = 4$.
b) The dimension of the code $k = n - r$, where r is the dimension of the parity check matrix. We can find out the dimension of H by either looking at the column vectors or row vectors. To simplify, let's first do some row operations on H: deduct $T*$ *the first four rows* from *the last four rows*. This operation doesn't change the rank of the matrix, and the new formed matrix H' is

$$H' = \begin{pmatrix} 1 & 2 & 3 & \ldots & D & E & F \\ y & y & y & \ldots & y & y & y \end{pmatrix}.$$

Clearly each of the last four rows is either all 1 or all 0, and at least there is one all 1 because y is nonzero. Hence the rank of H' is the same as the rank of the 5×15 matrix H^*

$$H^* = \begin{pmatrix} 1 & 2 & 3 & \dots & D & E & F \\ 1 & 1 & 1 & \dots & 1 & 1 & 1 \end{pmatrix}.$$

The rank of H^* is at most 5. On the other hand, we have a submatrix

$$\begin{pmatrix} 1 & 2 & 4 & 8 & F \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

has nonzero determinant. So the rank of H^* is 5. Hence the dimension of the code is 10.