EE 605: Error Correction Codes

Assignment 1

Due: Friday, Aug 27th, 2021

General rules: I am ok if you discuss the homework with other students, but it is mandatory to write the answers on your own and mention at the start who all you have discussed the homework with. Failure to do so might lead to a straight rejection of the homework submission.

---

1. Consider a $(5, 3)$-linear code over $GF(4)$, defined by the following generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix}$$

   (a) Find the parity check matrix of this code.

   (b) Characterize the error-correcting and error-detection capabilities of the code.

   (c) Is this a perfect code? Justify your answer

2. What is the erasure correcting capability z of a $(7, 4)$-Hamming code over GF(2)? Derive a procedure for correcting upto z erasures for this code.

3. Using a counting argument, show that there might exist a perfect double-error correcting $(11, 6)$-linear code over GF(3) . (Such a code was actually found by Golay)

4. (a) Show that the set of integers under the usual subtraction operation does not form a group.

   (b) Solve the set of equations $2x + y = 3, x + 2y = 3$ over $GF(4)$.

   (c) Consider a set of four elements $\{0, 1, 2, 3\}$. Does this set with the $+$ and . operations defined below constitute a field?

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

5. Let p be a prime number and consider the set $\{0, 1, \ldots, p-1\}$ with mod-p arithmetic. Show that every non-zero element in the set has a multiplicative inverse.

6. (a) Find the probability of undetected error for the $(8, 4)$- extended Hamming code and the $(8, 7)$-simple parity check code, when used over the BSC(p) channel. Compare the two quantities for $p = 1/2$.

   (b) Consider the (5,1)-binary repetition code. List the vectors which will be decoded to (00000) under nearest neighbor decoding. Also, assuming both messages to be equally likely, what will be the probability of error if this code is used over a BSC(p) channel?

7. Consider a $(5, 3)$-binary code C with generator matrix as follows:

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

   (a) Convert G to systematic form.

   (b) Find the parity check matrix of the code C

   (c) List all the codewords of the dual code of C

8. Consider a $(6, 3)$-binary code C with parity check matrix as follows:

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

   (a) Construct the coset decomposition of this code, choosing the lowest weight available vector as each coset leader.

   (b) Construct the syndrome decoding table.

   (c) Use syndrome decoding to decode the received vectors $r_1 = (000011)$ and $r_2 = (111100)$.

9. Recall that each element h in a finite group G is associated with a cyclic subgroup. We will say the group G is cyclic if it is equal to the cyclic subgroup generated by one of its elements g, so that $G = \{e, g, g^2, \ldots, g^{n-1}\}$. In other words, there is an element with order n, where n is the size of the group G.

   (a) Show that any cyclic group G is abelian.

   (b) Show that a group of size 3 will be cyclic.

   (c) Is the same true for groups of size 4?

   (d) Is the group $\{0, 1, \ldots, 7\}$ with mod-8 arithmetic a cyclic group? If yes, identify all elements whose cyclic subgroup generates the group. *Remark: Other than doing this in a brute-force way by enumerating all the cyclic subgroups, you might want to try to show that the order of element g^i in a cyclic subgroup generated by g is $n/gcd(i, n)$.*