

ECE 563: Homework 4 - Due November 10, 2022

Problem 1: Bounds on the size of codes. Let C be a linear code with parameters $[n, k, d]$ over an arbitrary finite field alphabet. Prove that $d \leq n - k + 1$.

Problem 2: Bounds on the size of codes. Let C be a binary linear code with parameters $[n, k, d]$ for which $d > \frac{1}{2}n$. Prove that $2^k \leq \frac{2d}{2d-n}$.

Problem 3: Finite fields. Show that for any prime p and any positive integer a that is not a multiple of p one has $a^{p-1} = 1 \pmod{p}$.

Problem 4: Finite fields. Explain how to construct a finite field of order 9. Identify an appropriate primitive polynomial and primitive element and list all the elements, provide an addition and multiplication table.

Problem 5: LDPC codes. Implement the peeling algorithm for BECs discussed in class and use it to decode 3 different codewords of the Hamming $[15, 11, 3]$ code with erasures in the following sets of coordinates: $\{1, 2, 3\}$, $\{3, 4, 9\}$, $\{4, 5, 13\}$. Make sure to specify which parity-check matrix and codewords you are using. Match up each of your chosen three codewords with exactly one erasure pattern and report the outcome of the decoding process.