Tópicos Avançados em Ciência da Computação I:
Introdução à Teoria de Códigos para Criptografia Pós-Quântica
Prof. Daniel Panario

Lista de Exercícios I
Entrega: Sexta Feira 24 de janeiro de 2020
Valor no curso: 20%

1. (25 pontos) Caracterizações de corpos finitos.

(a) (5 pontos) Prove que para qualquer corpo finito, o anel $\mathbb{F}_q[x]/(x^4 + x^3 + x + 1)$ nunca é um corpo.

(b) (5 pontos) Prove que $f(x)^q = f(x^q)$ para todo $f \in \mathbb{F}_q[x]$.

(c) (5 pontos) Desenhe a grade de subcorpos de $\mathbb{F}_{5^{30}}$. Responda: $\mathbb{F}_9$ um subcorpo de $\mathbb{F}_{27}$? Explique.

(d) (10 pontos) Prove que a soma de todos os elementos de um corpo finito é 0, exceto para $\mathbb{F}_2$.

2. (20 pontos) Cálculos à mão em corpos finitos.

(a) (5 pontos) Construa as tabelas de soma e produto de $\mathbb{F}_3[x]/(x^2 + 2x + 2)$. Determine se esse anel é um corpo.

(b) (5 pontos) Calcule o inverso de x^3+x+1 em $\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(x^4+x+1)$ usando o algoritmo estendido de Euclides.

(c) (5 pontos) Encontre um elemento primitivo em $\mathbb{F}_{17}$. Então, usando o método mostrado na aula, determine todos os elementos primitivos de $\mathbb{F}_{17}$.

(d) (5 pontos) Seja $\mathbb{F}_{25} \cong \mathbb{F}_5[x]/(x^2 + 2x + 3)$. Encontre a ordem de x.

3. (15 pontos) Considere o código linear $(5, 2)$ sobre $\mathbb{F}_2$ com matriz de paridade

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

Determine todas as palavras de código e a distância mínima do código. Dê uma matriz geradora do código. Construa a matriz para a decodificação por síndrome e decodifique os vetores: $11111, 01101$ and 01100.

4. (15 pontos) Considere uma função binária de codificação que mapeia (a_1, a_2, a_3) em $(a_1, a_2, a_3, a_1 + a_2, a_1 + a_3, a_2 + a_3)$. Primeiro, dê uma matriz geradora do código. Depois, dê a matriz de paridade, comprimento n, dimensão k e distância mínima do código. Finalmente, construa a matriz para a decodificação por síndrome e decodifique três vetores de sua escolha.

5. (15 pontos) Prove que um código linear pode detectar s ou menos erros se e somente se a sua distância mínima d_C satisfaz $d_C \geq s + 1$.

6. (10 pontos)

(a) (5 pontos) Se um código linear (n, k) sobre $\mathbb{F}_q$ tem distância mínima d, vimos que $k + d - 1 \leq n$. Deduzir uma cota para o número de palavras-códigos M em termos de n, d, q.

(b) (5 pontos) Comparar a sua cota da parte (a) com a cota de Hamming para códigos binários. Mostre pares d e n tais que a sua cota é melhor que a cota de Hamming.

Ajuda: divida a análise em dois casos, t par e t ímpar (onde t aparece na cota de Hamming).