Topics in Coding Theory: Locality and Interaction **Winter 2020**

Exercise 1

Publish Date: November 05, 2019 *Due Date: November 16, 2019*

Exercise 1.1 *Let* $G \in M_{5\times 3}(\mathbb{F}_2)$*:*

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

And let $\mathcal{C} = Im(G)$ *be the code generated by* G.

a) *What is the rate of* $\mathcal{C}$*?*

b) *Find* H*, the parity check matrix of* $\mathcal{C}$.

c) *What is the distance of* $\mathcal{C}$*?*

d) *Find another generator matrix* G_0 *for the same code* $\mathcal{C}$ *that represents a systematic encoding; that is, so that the encoding map* $x \to G_0 x$ *has the form* $(x_1, x_2, x_3) \to (x_1, x_2, x_3, a, b)$ *for some* $a, b \in \mathbb{F}_2$.

Exercise 1.2 *Let* $\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ *be a family of binary codes with relative distance* δ *and relative rate* ρ *(that means that* $\lim_{n\to\infty} \delta_n = \delta$*, and* $\lim_{n\to\infty} \rho_n = \rho$*). Prove that* $\rho + H(\frac{\delta}{2}) \leq 1$.

Exercise 1.3 *Let* $\mathbb{F}_2$ *be the field with two elements. Denote by* α *an element that satisfy the polynomial equation* $\alpha^2 + \alpha + 1 = 0$ *over* $\mathbb{F}_2$*. Denote by* $\mathbb{F}_4 = \{a\alpha + b \mid a, b \in \mathbb{F}_2\}$.

a) *Prove that* $\mathbb{F}_4$ *is a field.*

b) *Let* $Tr(x) = x^2 + x \in \mathbb{F}_4[x]$*. Show that* $Tr(x)$ *is linear with respect to* $\mathbb{F}_2$ *elements, i.e. for every* $a, b \in \mathbb{F}_2$*,* $\beta \in \mathbb{F}_4$ *it holds that* $Tr(a\beta + b) = aTr(\beta) + Tr(b)$.

   Deduce that for every $\beta \in \mathbb{F}_4$*,* $Tr(\beta) \in \mathbb{F}_2$.

c) *Let* $\{R_i\}_{i\in\mathbb{N}}$ *be a sequence of independent random variables, each is uniformly distributed over* $\mathbb{F}_4$ *except that* R_1 *is fixed to* $R_1 = \alpha$*. Let*

$$S_k(x) = \sum_{i=1}^{k} R_{k+1-i} x_i,$$

   where addition and multiplication are performed in $\mathbb{F}_4$*. We defined in class a tree code with a coloring function given by* $T(x)_k = S_k(x)$*. We proved that with a positive probability, this code has a distance that is bounded away from zero.*

   In this exercise we will show an alternative construction for a tree code. Show that the tree code defined with the following coloring function

$$T'(x)_k = \begin{cases} S_k(x), & k \equiv_2 0; \\ Tr(S_k(x)), & \text{otherwise.} \end{cases}$$

   also has distance that is bounded away from 0, with positive probability.