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

Exercise 4

Publish Date: 07 January 20 *Due Date: 21 January 20*

Exercise 4.1. *Let $\mathbb{F}_p$ be a prime field. Consider $V = Span\{1, x^2, x^3, x^5, x^6\} \subset \mathbb{F}_p[x]$. Give a bound on p, (for example $p \geq 5$) such that there exists an interpolation set of size 5 for V in $\mathbb{F}_p$.*

Exercise 4.2. *For each vector of nonnegative integers $\vec{k} = (k_1, \ldots, k_m)$, introduce the polynomial*

$$V_{\vec{k}}(x_1, \ldots, x_m) = \prod_{j=1}^{m} (x_j^q - x_j)^{k_j}.$$

(a) For every $\vec{i} = (i_1, \ldots, i_m)$, show that unless $\vec{i} \geq \vec{k}$ coordinate-wise, we have that for every $a \in \mathbb{F}_q^m$:

$$V_{\vec{k}}^{(\vec{i})}(a) = 0,$$

and that

$$V_{\vec{k}}^{(\vec{k})}(a) = (-1)^{wt(\vec{k})}.$$

(b) Let $Q(x_1, \ldots, x_m) \in \mathbb{F}_q[x_1, \ldots, x_m]$ be a polynomial of degree $\leq d$. Prove that Q can be written as

$$Q(x_1, \ldots, x_m) = \sum_{\vec{k}: wt(\vec{k}) \leq \frac{d}{q}} A_{\vec{k}} V_{\vec{k}},$$

for some polynomials $A_{\vec{k}}$ with individual degrees at most $q-1$ and total degree at most $\min(m \cdot (q-1), d - wt(k) \cdot q)$. Conversely, any collection of such $A_{\vec{k}}$ gives Q of degree $\leq d$.

Exercise 4.3. *Let $m \in \mathbb{N}$. Describe sets of vectors $\{v_1, \ldots, v_k\}, \{u_1, \ldots, u_k\} \subset \mathbb{Z}^n$ such that $\langle v_i, u_j \rangle = m \iff i = j$ (Hint: Use Cauchy–Schwarz inequality). Describe how to modify your construction to obtain a matching vector family.*

Exercise 4.4. *Let $p(x, y) \in \mathbb{F}_q[x, y]$ be a degree d polynomial. Let r be the evaluation map of p with δ fraction of errors. Consider a correcting algorithm similar to the one shown in class: Write a set of linear equations $N(\alpha, \beta) = r(\alpha, \beta)E(\alpha, \beta)$ where the coefficients of N, E are the variables. Solve the equations and output $p(x, y) = \frac{N(x,y)}{E(x,y)}$. What is the largest fraction of errors, δ, this algorithm can tolerate?*