Exercises for CQC S'22, Set #3 (not collected or graded)

.

A. ***Reed-Solomon codes***

1. Study the example in the notes for Lecture 5 (posted to ELMS).

(a) Retrace the steps of the decoding algorithm, matching them to the description of the algorithm in the lectures.

(b) Take the codeword decoded by the algorithm in the example, insert two errors in it, and run the algorithm to see how it functions.

B. ***Geometric notions for codes on curves***

2. Let V_n be the set of $(n+1)$-dim vectors over $\mathbb{F} = ff_q$ (some finite field). Call vectors $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ equivalent if $\boldsymbol{x}_1 = \lambda \boldsymbol{x}_2$ for some constant $\lambda \in \mathbb{F}\backslash\{0\}$.

(a) Show that this is indeed an equivalence relation.

(b) Assume that $x_{n+1} = 0$ corresponds to points at infinity, and show that the affine points in $\mathbb{P}^n\mathbb{F}$ can be represented uniquely by $(x_1 : x_2 : \cdots : x_n : 1)$. The set of affine points is called the n-dim affine space $\mathbb{A}^n\mathbb{F}_q$.

(c) Show that $|\mathbb{P}^n\mathbb{F}| = q^n + q^{n-1} + \cdots + q + 1$ of which $q^{n-1} + \cdots + q + 1$ are points at infinity.

3. Let $g(x_1, \ldots, x_{n+1})$ be a homogeneous polynomial of degree d over $\mathbb{F}$ (some finite field) and let $f(x_1, \ldots, x_n)$ be any polynomial. We denote by f^H the homogeneous polynomial obtained from f.

Show that

(a) If $\alpha \in \mathbb{F}$ then $g(\alpha x_1, \ldots, \alpha x_{n+1}) = \alpha^d g(x_1, \ldots, x_{n+1}$.

(b) $f(x_1, \ldots, x_n) = 0$ if and only if $f^H(x_1, \ldots, x_n, 1) = 0$.

(c) For all points $(x_1 : x_2 : \cdots : x_n : x_{n+1})$ in an equivalence class (problem 2a) either $g(x_1 : x_2 : \cdots : x_n : x_{n+1}) = 0$ or not simultaneously.

(d) There is a bijection between the sets $\{f : \deg(f) = d)\}$ and $\{g : \deg(g) = d\}$, where f and g are as defined above.

Thus: zeros of f in the affine space $\mathbb{A}^n\mathbb{F}$ can be viewed as the affine points in $\mathbb{P}^n\mathbb{F}$ that are zeros of the homogeneous polynomial f^H (which may very well have other zeros at infinity). Moreover, points in $\mathbb{P}^n\mathbb{F}$ can be viewed as zeros of a homogeneous polynomial. Roughly speaking, this extends to points on curves.

4. Consider the "Fermat curve" $\mathcal{F}_3(\mathbb{F}_q)$ of degree 3, i.e., a plane curve defined by the projective equation $x^3 + y^3 + z^3 = 0$.

(a) For $q = 2$ the curve has three projective points $(x : y : z)$. Find them.

(b) For $q = 4$ the curve has 9 projective points $(x : y : z)$. Find them.

(c) For $q = 8$ the curve has 9 projective points $(x : y : z)$. Find them.

5. Let

$$f(x, y) = 1 + x + y - x^2 - y^2 - 2x^2y + xy^2 - y^3 + x^4 - 2x^3y + x^2y^2 + 2xy^3 \in \mathbb{F}_5[x].$$

Show that $(1, 2) \in \mathbb{F}_5^2$ is a root of f of multiplicity 3.