Final Exam

Duration : 3 hours

Exercise 1 – Consider the projective curve $\mathrm{X}_1 \subset \mathbb{P}^2$ defined over $k = \mathbb{F}_2$ as the projective closure of the affine curve $\subset \mathbb{A}^2$ given by:

$$y^2 + y = x^3 + x.$$

1.1. Give an equation of X_1, and prove that X_1 is smooth.

1.2. Show that $\#\mathrm{X}_1(\mathbb{F}_{16}) = 25$. *You may use without proof that* X_1 *has genus* 1.

Let $\mathrm{P} \in \mathrm{X}_1(\mathbb{F}_{16})$ be one of these 25 points, and $a, b \geqslant 1$ be two integers. Consider the divisor $\mathrm{D} = a \cdot \mathrm{P}$ on $\mathrm{X}_1/\mathbb{F}_{16}$, and choose b points $\mathrm{P}_1, \ldots, \mathrm{P}_b$ in $\mathrm{X}_1(\mathbb{F}_{16}) \smallsetminus \{\mathrm{P}\}$.

We denote by $\Gamma_{a,b}$ the Goppa code over $\mathbb{F}_{16}$ associated to this data $\mathrm{X}_1, \mathrm{D}, \{\mathrm{P}_1, \ldots, \mathrm{P}_b\}$.

1.3. Estimate the invariants n, k, d of $\Gamma_{a,b}$ in terms of a, b (give the exact values of n and k, and a lower bound on d). What inequalities restrict the possible choices of a, b?

1.4. Among the following, which can be realized as a $\Gamma_{a,b}$? If so, give suitable values of a, b.

(a) A $[n, k, d]$-code over $\mathbb{F}_{16}$ with $n = 21$, $k = 11$ and $d \geqslant 10$.

(b) A code over $\mathbb{F}_{16}$ of dimension 24.

(c) A code over $\mathbb{F}_{16}$ of length 22 which corrects at least 4 errors. *Hint: use the Singleton bound.*

(d) A code over $\mathbb{F}_{16}$ which corrects at least 12 errors.

1.5. From a suitable $\Gamma_{a,b}$ over $\mathbb{F}_{16}$, explain how to deduce a $[84, 32, \geqslant 13]$-code over $\mathbb{F}_2$.

Let $\mathrm{X}_2 \subset \mathbb{P}^2$ be the smooth projective curve of genus 1 defined over $\mathbb{F}_{16}$ by $x^3 + y^3 + z^3 = 0$.

1.6. Can a Goppa code obtained from X_2 have bigger length than the longest $\Gamma_{a,b}$?

Exercise 2 – Let $k = \mathbb{F}_5$, and consider the smooth projective curve $\mathrm{C} \subset \mathbb{P}^2$ defined over $\mathbb{F}_5$ by

$$\mathrm{C}/\mathbb{F}_5 \ : \qquad x^4 + y^4 + z^4 = 0.$$

It can be shown that C is smooth and has genus 3.

For any integer $d \geqslant 1$ coprime to q, we denote by μ_d the group of d-th roots of unity in $\overline{\mathbb{F}_5}$.

2.1. For what values of d do we have $\mu_d \subset \mathbb{F}_5^\times$? and $\mu_d \subset \mathbb{F}_{25}^\times$?

2.2. Show that $\#\mathrm{C}(\mathbb{F}_5) = 0$.

2.3. Let $\xi \in \mathbb{F}_{25}^\times$ be a primitive 8-th root of unity. Considering points of the form $\mathrm{P}_k = [0 : 1 : \xi^k] \in \mathbb{P}^2$ (for suitable $k \geqslant 0$) and points obtained from P_k by permuting the coordinates, prove that $\#\mathrm{C}(\mathbb{F}_{25}) \geqslant 3 \cdot 4 = 12$.

2.4. Now let $\zeta \in \mathbb{F}_{25}^\times$ be a primitive 12-th root of unity.

For $a \in \{0, 1, 2\}$ and $k, \ell \geqslant 0$, let $\mathrm{Q}_{a,k,\ell} = [1 : \zeta^{a+3k} : \zeta^{3-a+3\ell}] \in \mathbb{P}^2$. Exhibit $2 \cdot 4 \cdot 4 = 32$ more points in $\mathrm{C}(\mathbb{F}_{25})$.

Hint: ζ^4 is a primitive 3*-rd of unity.*

The Serre bound gives that $\#\mathrm{C}(\mathbb{F}_{25}) \leqslant 56$, and a more detailed analysis would show that $\#\mathrm{C}(\mathbb{F}_{25}) \leqslant 55$.

Using the "symmetries" of C, one can show that $\#\mathrm{C}(\mathbb{F}_{25}) \equiv 8 \bmod 12$.

2.5. Conclude that $\#\mathrm{C}(\mathbb{F}_{25}) = 44$.

2.6. It is known that $\#\mathrm{C}(\mathbb{F}_{125})$ attains the upper bound of Serre. Deduce that

$$\mathrm{Z}(\mathrm{C}/\mathbb{F}_5, \mathrm{T}) = \frac{125\mathrm{T}^6 - 150\mathrm{T}^5 + 135\mathrm{T}^4 - 68\mathrm{T}^3 + 27\mathrm{T}^2 - 6\mathrm{T} + 1}{(1 - \mathrm{T})(1 - 5\mathrm{T})}.$$

Exercise 3 – Let $k = \mathbb{F}_2$ be the finite field with 2 elements. For any finite extension $\mathbb{F}_q$ of $\mathbb{F}_2$ (with $q = 2^m$), we denote by $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ the trace map, defined by $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{2^i}$, for all $x \in \mathbb{F}_q$.

We identify $\mathbb{F}_2$ with $\{0, 1\} \subset \mathbb{Z}$; in particular, $(-1)^{\mathrm{Tr}(x)}$ makes sense, for all $x \in \mathbb{F}_q$.

3.1. Show that the map $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ is $\mathbb{F}_2$-linear, and surjective.

3.2. Prove that $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(x)} = 0$, and deduce that the following probabilistic statement holds:

"the probability that a randomly chosen $x \in \mathbb{F}_q$ has trace 0 is 1/2."

3.3. Consider the $\mathbb{F}_2$-linear map $s : \mathbb{F}_q \to \mathbb{F}_q$, $y \mapsto y^2 - y$. Compute the kernel of s, and show that $\mathrm{Tr} \circ s = 0$.

3.4. Deduce that, for all $z \in \mathbb{F}_q$,

$$\#\{y \in \mathbb{F}_q \ : \ y^2 - y = z\} = 1 + (-1)^{\mathrm{Tr}(z)} = \begin{cases} 0 & \text{if } \mathrm{Tr}(z) \neq 0 \\ 2 & \text{if } \mathrm{Tr}(z) = 0. \end{cases}$$

Given $\mathrm{A}, \mathrm{B} \in \mathbb{F}_2$, we set $f(x) := x^3 + \mathrm{A}x + \mathrm{B} \in \mathbb{F}_2[x]$. For any extension $\mathbb{F}_q/\mathbb{F}_2$, we define the sum

$$\Sigma_{\mathrm{A},\mathrm{B}}(q) := \sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(f(x))}.$$

3.5. Prove that the sequence $\left(2^{-m} \cdot \Sigma_{\mathrm{A},\mathrm{B}}(2^m)\right)_{m \geqslant 1}$ is bounded.

For $\mathrm{A}, \mathrm{B} \in \mathbb{F}_2$, consider the affine curve $\mathrm{C}_{\mathrm{aff}} \subset \mathbb{A}^2$ defined over $\mathbb{F}_2$ by

$$\mathrm{C}_{\mathrm{aff}}/\mathbb{F}_2 : \qquad y^2 - y = f(x) = x^3 + \mathrm{A} \cdot x + \mathrm{B}.$$

Denote by $\mathrm{C}/\mathbb{F}_2$ the projective closure of $\mathrm{C}_{\mathrm{aff}}$ in $\mathbb{P}^2$. You may use without proof that the curve C has genus 1.

3.6. Give an equation of $\mathrm{C} \subset \mathbb{P}^2$, and check that C is smooth.

3.7. Given any finite extension $\mathbb{F}_q/\mathbb{F}_2$, prove that $\#\mathrm{C}_{\mathrm{aff}}(\mathbb{F}_q) = q + \Sigma_{\mathrm{A},\mathrm{B}}(q)$.

3.8. For any extension $\mathbb{F}_q/\mathbb{F}_2$, show that $|\Sigma_{\mathrm{A},\mathrm{B}}(q)| \leqslant 2 \cdot \sqrt{q}$.

Deduce that the sequence $\left(2^{-m} \cdot \Sigma_{\mathrm{A},\mathrm{B}}(2^m)\right)_{m \geqslant 1}$ tends to 0 as $m \to \infty$.

3.9. Conclude that the following statement is true:

"the probability that $\mathrm{Tr}(x^3 + 1) = 0$ for a random $x \in \mathbb{F}_{2^m}$ tends to 1/2, when $m \to \infty$."