Homework 3

Curves over finite fields, Autumn 2017, Leiden

Deadline: Monday 11 December 2017

Problem 1. Consider the curve $\mathcal{C} = \mathbb{P}^1$ over $\mathbb{F}_{2^\ell} = \{x_1, \ldots, x_{2^\ell}\}$ with coordinates $(X : Y)$. Consider the points $P_i = (x_i : 1) \in \mathcal{C}(\mathbb{F}_{2^\ell})$ for $i = 1, \ldots, 2^\ell$, and, moreover, let D be the divisor $r \cdot (1 : 0)$ for some $r \geq 0$. Let C_r be the Goppa code associated with $(\mathcal{C}, D)$ inside $\mathbb{F}_{2^\ell}^{2^\ell}$ (using all the P_i).

(a) Find the length and the minimum distance of C_r.

(b) Suppose that $r < 2^\ell - 1$. Prove that C_r is dual to $C_{2^\ell - r - 2}$.

The function $\pi := \frac{Y}{X} \in \mathbb{F}_{2^\ell}(\mathcal{C})$ has a simple zero at $(1 : 0)$. For each $f \in \mathcal{L}(D)$, we can evaluate the function $f \cdot \pi^r$ in $P_{2^\ell+1} = (1 : 0)$. With abuse of notation, we call this value $f((1 : 0))$. Let E_r be obtained by extending the Goppa code C_r to $\mathbb{F}_{2^\ell}^{2^\ell+1}$ by putting $f((1 : 0))$ on the the last coordinate, i.e. E_r is the image of

$$\varphi \colon \mathcal{L}(D) \to \mathbb{F}_{2^\ell}^{2^\ell+1} \colon f \mapsto (f(P_i))_{i=1}^{2^\ell+1}.$$

(c) Prove that E_r is an MDS code.

Problem 2. Do Exercise 23 from the coding theory lecture notes:

(a) Construct an isomorphism between $V \otimes W$ and the space constructed in Remark 21 of the notes.

(b) Prove that the map $\varphi : V \times W \to V \otimes W : (v, w) \mapsto v \otimes w$ is bilinear.

(c) Prove that $V \otimes W$ and φ satisfy the following universal property: for any K-vector space T and any bilinear map $\rho : V \times W \to T$ there exists a unique linear map $\eta : V \otimes W \to T$, such that the following diagram commutes (i.e. $\eta \circ \varphi = \rho$):

$$\begin{tikzcd} V \times W \arrow[r, "\varphi"] \arrow[rr, bend right, "\rho"'] & V \otimes W \arrow[r, dashed, "\eta"] & T \end{tikzcd}$$

Problem 3. Do Exercises 40 and 41 from the coding theory lecture notes. Download your worksheet from `https://sage.math.leidenuniv.nl/` and hand it in by e-mail. Put enough comments in your code, or hand in a separate explanation of your code with your homework solutions.

(a) Use `Magma` to construct an $[n, k, d]$-code using algebraic geometry with $k, d \geq 200$ and $n \leq 450$, just as we did in the lecture notes. Generate a random code word, randomly change 10 entries of the vector and try to decode the word (stop if it takes too long).

(b) Use `Magma` again to repeat the procedure, but this time use the specific algebraic-geometric procedures that are implemented in `Magma`. Look up the functions `AGDualCode` and `AGDecode` in the `Magma` handbook.

Problem 4. Let E be a classical elliptic curve over $\mathbb{F}_q$, i.e. a smooth projective curve inside $\mathbb{P}^2$ given by a Weierstraß equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Let $O = (0 : 1 : 0)$ be the chosen point on E.

(a) For each $n \in \mathbb{Z}_{\geq 0}$ give a basis for $\mathcal{L}(n \cdot O)$.

(b) Prove that E has genus 1 by using Riemann-Roch.

Now suppose that E' is an elliptic curve over $\mathbb{F}_q$, i.e. a smooth projective curve of genus 1, together with an $\mathbb{F}_q$-rational point O'.

(c) Prove that there exist functions x and y in $\mathbb{F}_q(E')$, having a pole of order 2 and 3 at O' and no other poles, respectively.

(d) Prove that the map

$$\varphi\colon E' \to \mathbb{P}^2 \colon P \mapsto (x(P) : y(P) : 1)$$

is well-defined and injective.

(e) Prove that the points in the image of φ satisfy an equation of the shape

$$Y^2Z + a_1XYZ + a_3YZ^2 = a_0X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

for some $a_0, a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$.

Problem 5. Let E be the classical elliptic curve over $\mathbb{F}_5$ given by the equation $Y^2Z + YZ^2 = X^3 + XZ^2$ inside $\mathbb{P}^2$ with coordinates $(X : Y : Z)$. Let $P := (0 : 0 : 1) \in E(\mathbb{F}_5)$.

(a) Compute the number of $\mathbb{F}_5$-rational points on E.

(b) Compute $2 \cdot P$ and $3 \cdot P$.

(c) Determine the order of P.

Let $Q := (1 : 1 : 1) \in E(\mathbb{F}_5)$, $O := (0 : 1 : 0) \in E(\mathbb{F}_5)$ and let D be the divisor $P + Q$.

(d) Compute $\operatorname{div}((Y^2 + 4YZ)/Z^2)$.

(e) Let $f \in \mathcal{L}(D)$. Prove that $f \cdot (Y^2 + 4YZ)/Z^2 \in \mathcal{L}(6O)$.

(f) Use this to compute a basis for $\mathcal{L}(D)$. *Hint: use the results of* **4(a)**.

Let P_1 and P_2 be two other rational points of $E(\mathbb{F}_5)$ of your choice.

(g) Indicate your choice of P_1 and P_2 and describe a basis for the Goppa code associated with (E, D) inside $\mathbb{F}_5^2$ (using the points P_1 and P_2).