Algebraic Geometry for Theoretical Computer Science

Assignment 3

Lecturer: Gil Cohen *Hand in date: November 20, 2014*

Instructions: Please write your solutions in LaTeX / Word or exquisite handwriting. Submission can be done individually or in pairs.

1. In this exercise we will learn about two important functions – the *trace* and the *norm* of finite field extensions. Let L/K be a finite field extension, and let $\mathrm{Aut}(L/K)$ denote the Galois group of L/K. The trace function $\mathrm{Tr}_{L/K} \colon L \to K$ is defined by
$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Aut}(L/K)} \sigma(x)\,.$$
If K, L are clear from context, then we omit them from the subscript, and write $\mathrm{Tr}(x)$. In this course we care mainly about finite fields and finite field extensions.

   (a) Let q be a prime power, and $n \geq 1$ an integer. Show that
$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \sum_{i=0}^{n-1} x^{q^i}\,.$$

   (b) Prove that $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is an $\mathbb{F}_q$-linear function. Namely, for all $x, y \in \mathbb{F}_{q^n}$ and $a \in \mathbb{F}_q$, it holds that $\mathrm{Tr}(x + ay) = \mathrm{Tr}(x) + a\mathrm{Tr}(y)$.

   (c) Prove that $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ has indeed range $\mathbb{F}_q$.

   (d) Consider the representation of $\mathbb{F}_8$ as $\mathbb{F}_2[\omega]/(\omega^3 + \omega + 1)$. What is $\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}$?

   The trace function got its name for the following reason. Fix $x \in \mathbb{F}_{q^n}$, and consider the function $m_x \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, defined by $m_x(y) = xy$. Note that m_x is a linear function. Therefore, it can also be represented as an $n \times n$ matrix M_x over $\mathbb{F}_q$, once a representation for $\mathbb{F}_{q^n}$ has been fixed. As it turns out, regardless of the way we choose to represent $\mathbb{F}_{q^n}$, the "matrix-theory trace" of M_x (namely, sum of entries on the diagonal) is exactly $\mathrm{Tr}(x)$ as defined above.

   (e) Consider again $\mathbb{F}_8$ represented as $\mathbb{F}_2[\omega]/(\omega^3 + \omega + 1)$. What is the matrix that corresponds to multiplication by the element $x = a + b\omega + c\omega^2$, in terms of a, b and c ? Verify that this matrix's trace is the same as the one you computed in the previous item.

   (f) We finish the discussion on the trace function with the following useful characetrization of the kernel of Tr. Show that $\mathrm{Tr}(x) = 0 \iff \exists y \in \mathbb{F}_{q^n}$ such that $x = y^q - y$.

A second important function in our course will be the *norm* function, which we now define. Let L/K be a finite field extension. The norm function $\mathrm{N}_{L/K}\colon L \to K$ is defined by

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Aut}(L/K)} \sigma(x)\,.$$

When $L = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$, where q is a prime power, and $n \geq 1$ an integer, we have that

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \prod_{i=0}^{n-1} x^{q^i} = x^{1+q+q^2+q^3+\cdots+q^{n-1}}.$$

It is worth mentioning that $\mathrm{N}(x)$ is the determinant of the matrix M_x defined above. We conclude this exercise with the following item, which will also be useful later in the course.

(g) How many solutions does the equation $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y)$ have over $\mathbb{F}_{q^n}$?

2. Let $f(x, y) = y^2 + y - x^3 - x - 1$ be a polynomial over $\mathbb{F}_2$, and let C_f be the affine plane curve associated with f.

   (a) What is the homogenization F of f, and the projective closure $\widehat{C_f}$ of C_f?

   (b) Prove that $\widehat{C_f}$ is nonsingular.

   (c) Find all points in $\widehat{C_f}$ over $\mathbb{F}_2$.

   (d) Find all points in $\widehat{C_f}$ over $\mathbb{F}_4$.

   (e) Find all points in $\widehat{C_f}$ over $\mathbb{F}_8$.