

# Homework 1

Topics in Finite Fields (Fall 2013)

Rutgers University

Swastik Kopparty

Last modified: Tuesday 8<sup>th</sup> October, 2013

Recommended number of points to attempt for this problem set:  $\geq 6$  points.

1. **(2 points)** Let  $p, q$  be primes  $\equiv 1 \pmod{4}$ .

(a) Let  $W$  be the set of roots of  $X^p - 1$  in  $\overline{\mathbb{F}}_q$ . Show that there is an element  $\omega \in W$  such that  $W = \{1, \omega, \omega^2, \dots, \omega^{p-1}\}$ . Such an  $\omega$  is called a primitive  $p$ th root of unity.

(b) What is the degree of  $\omega$  over  $\mathbb{F}_q$ ? (i.e. What is the degree of the minimal polynomial of  $\omega$  over  $\mathbb{F}_q$ ).

(c) Show that:

$$\sum_{0 \leq x < p} \omega^x = 0.$$

(d) Define

$$S = \sum_{0 \leq x < p} \omega^{x^2}.$$

Show that  $S^2 = p$ .

(e) Show that  $S \in \mathbb{F}_q$  iff  $q$  is a quadratic residue mod  $p$ .

(f) Conclude that  $p$  is a quadratic residue mod  $q$  if and only if  $q$  is a quadratic residue mod  $p$ . Note where the  $1 \pmod{4}$  condition got used.

2. **(2 points)** Let  $\beta_1, \dots, \beta_n$  be a basis for  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . Having chosen a basis, this gives a  $\mathbb{F}_q$ -vector space isomorphism  $\varphi: \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q^n$ : for  $\alpha \in \mathbb{F}_{q^n}$ , if  $\alpha = \sum c_i \beta_i$ , we define:

$$\varphi(\alpha) = (c_1, \dots, c_n).$$

(a) Show that  $\varphi$  is an  $\mathbb{F}_q$ -linear map.

(b) For an element  $\alpha \in \mathbb{F}_{q^n}$ , consider the linear map  $M_\alpha: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  defined by:

$$M_\alpha(x) = \varphi(\alpha \cdot \varphi^{-1}(x)),$$

(where  $\cdot$  represents multiplication in  $\mathbb{F}_{q^n}$ ). We also denote by  $M_\alpha$  the corresponding  $n \times n$  matrix. In words: if you represent elements of  $\mathbb{F}_{q^n}$  by vectors in  $\mathbb{F}_q^n$ , then  $M_\alpha$  is the matrix you multiply with when you want to multiply by  $\alpha \in \mathbb{F}_{q^n}$ .

(c) Write some equations between the entries of  $M_\alpha$  and the basis  $b_1, \dots, b_n$ .

(d) Show that for  $a, b \in \mathbb{F}_q$ ,  $\alpha, \beta \in \mathbb{F}_{q^n}$ ,

$$aM_\alpha + bM_\beta = M_{a\alpha + b\beta}.$$

(e) Everything we did above depended on the choice of  $b_1, \dots, b_n$ . Suppose we choose a different basis  $b'_1, \dots, b'_n$ , and get matrices  $M'_\alpha$  for each  $\alpha \in \mathbb{F}_{q^n}$ .

Show that there is an invertible matrix  $U$  such that for all  $\alpha \in \mathbb{F}_{q^n}$ ,

$$M'_\alpha = UM_\alpha U^{-1}.$$

(Recall that two matrices  $A, B$  are called similar if  $A = UBU^{-1}$  for some invertible matrix  $U$ , and that similarity preserves the characteristic polynomial.)

- (f) Thus conclude that  $\text{Tr}(M'_\alpha) = \text{Tr}(M_\alpha)$ ,  $\det(M'_\alpha) = \det(M_\alpha)$ , and the eigenvalues of  $M'_\alpha$  and  $M_\alpha$  are the same.

3. (4 points) Pick a basis  $b_1, \dots, b_n$  for  $\mathbb{F}_q^n$  over  $\mathbb{F}_q$ .

- (a) Let  $\alpha \in \mathbb{F}_q^n$ . Let  $M_\alpha$  be the  $n \times n$   $\mathbb{F}_q$ -matrix which represents multiplication by  $\alpha$  (as in the previous problem). What are the eigenvalues of  $M_\alpha$ ? What is the trace of  $M_\alpha$ ? What is the determinant of  $M_\alpha$ ?

Hint for one approach: you can choose any basis you like; by the previous problem, the answer does not depend on the choice of basis. Choose a convenient basis that depends on  $\alpha$ . It may help to initially assume that  $\alpha$  has degree  $n$  over  $\mathbb{F}_q$ .

Hint for another approach: The eigenvalues of  $M$  are those  $\lambda \in \overline{\mathbb{F}_q}$  for which there exists  $x$  with  $Mx = \lambda x$ . Use the relationship between the entries of  $M_\alpha$  and the basis  $b_1, \dots, b_n$ .

- (b) Let  $F$  be the  $n \times n$   $\mathbb{F}_q$ -matrix that represents the map:  $\alpha \mapsto \alpha^q$ . What are the eigenvalues of  $F$ ? What is the trace of  $F$ ? What is the determinant of  $F$ ?
- (c) Let  $f(n, k)$  be the largest possible dimension of a linear space  $V$  of  $n \times n$   $\mathbb{F}_q$ -matrices such that every nonzero  $M \in V$  has rank  $\geq n - k + 1$ . Show that  $f(n, k) = nk$ .

The problem of finding  $f(n, k)$  over  $\mathbb{R}$  is significantly more difficult. (For  $k = 1$ , look up Radon-Hurwitz numbers.)

- (d) Show that there exists an  $n \times n$   $\mathbb{F}_q$ -matrix  $A$  and a point  $x \in \mathbb{F}_q^n$ , such that

$$\{A^k \cdot x \mid k \geq 0, k \in \mathbb{Z}\} = \mathbb{F}_q^n \setminus \{0\}.$$

Not for credit: Can you find a real orthogonal matrix  $A$  and a point  $x$  on the unit sphere of  $\mathbb{R}^n$ , such that  $\{A^k x \mid k \geq 0, k \in \mathbb{Z}\}$  is dense in the unit sphere?

4. (2 point) Let  $\alpha, \beta \in \mathbb{F}_q$ . Show that the polynomial  $P(X) = X^q - \alpha X - \beta$  is irreducible if and only if  $\beta \neq 0$ ,  $\alpha = 1$  and  $q$  is prime.

In the cases where  $P(X)$  is reducible, find the degrees of all its irreducible factors.

5. (3 points) This problem will study whether curves can parametrize product sets.

- (a) Let  $\gamma, \delta$  be a basis for  $\mathbb{F}_{q^2}$  over  $\mathbb{F}_q$ . Define  $P(X) = (\gamma X)^q + \gamma X$  and  $Q(X) = (\delta X)^q + \delta X$ . Show that:

$$\{(P(\alpha), Q(\alpha)) \mid \alpha \in \mathbb{F}_{q^2}\} = \mathbb{F}_q \times \mathbb{F}_q.$$

- (b) **This part of the problem was corrected.** Let  $q$  be prime. Let  $S, T \subseteq \overline{\mathbb{F}_q}$  with  $|S| = |T| = n$ , with  $n \leq q$ . Suppose we have  $n^2$  elements  $(\alpha_{ij})_{i,j \in [n]}$  of  $\mathbb{F}_{q^2}$  and polynomials  $P(X), Q(X)$  of degree  $\leq n$  such that

$$\{(P(\alpha_{ij}), Q(\alpha_{ij})) \mid i, j \in [n]\} = S \times T.$$

First observe that  $\deg(P), \deg(Q)$  cannot be  $< n$ . Show that  $P, Q$  must be of the form  $X^q + \alpha X + \beta$ , and that  $S, T$  are 1-dimensional  $\mathbb{F}_q$ -affine subspaces of  $\overline{\mathbb{F}_q}$ .

- (c) If  $q$  is not prime, show that the previous problem is false.
- (d) (4 bonus points, maybe more) I suspect that the previous theorem can be generalized to characterize for all  $n, q$ , which sets  $S, T \subseteq \overline{\mathbb{F}_q}$  with  $|S| = |T| = n$  are such that  $S \times T$  can be parametrized by  $n^2$  evaluations of two polynomials  $(P, Q)$  of degree  $n$ . Conjecture:  $S, T$  must be  $\mathbb{F}_p$ -affine subspaces of  $\overline{\mathbb{F}_q}$ , where  $p$  is the characteristic of  $q$ .

6. (1 point) Let  $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^n}$ . Show that they are linearly independent over  $\mathbb{F}_q$  if and only if the  $k \times k$  matrix  $M$  with  $M_{ij} = \alpha_i^{q^{j-1}}$  is nonsingular.