Homework 2

Topics in Finite Fields (Fall 2013)
Rutgers University
Swastik Kopparty
Last modified: Sunday 20th October, 2013

Recommended number of points to attempt for this problem set: ≥ 10 points.

1. **(3 points)** We will generalize the Mordell argument from class to all fields.

   Let $\mathbb{F}_q$ be a field of characteristic p. Let ψ be a nontrivial additive character of $\mathbb{F}_q$.

   (a) A polynomial $R(X) \in \mathbb{F}_q[X]$ is said to be p-free if it is an $\mathbb{F}_q$ linear combination of the monomials $\{X^i : p \text{ does not divide } i\}$.
   Let $d < \sqrt{q}$. Let $P(X) \in \mathbb{F}_q[X]$ be a polynomial of degree $\leq d$. Show that there exists a unique p-free polynomial $R(X)$ of degree $\leq d$ such that for every $x \in \mathbb{F}_q$, $\psi(R(x)) = \psi(P(x))$.
   Show that $R(X)$ is a constant if and only if $P(X)$ can be written in the form $Q(X)^p - Q(X) + c$, for some $Q(X) \in \mathbb{F}_q[X]$ and $c \in \mathbb{F}_q$.

   (b) Let $S = \{1 \leq i \leq t : p \not| i\}$. Let $s_1 < s_2 < \ldots < s_k$ be the elements of S. Let $z_1, \ldots, z_t \in \mathbb{F}_q$ be distinct.
   For each $j \in [t]$, define $v_j \in \mathbb{F}_q^k$ by $v_j = (z_j^{s_1}, z_j^{s_2}, \ldots, z_j^{s_k})$.
   Show that there is no nonzero $\mathbb{F}_p$-linear combination of the v_j which equals 0.

   (c) Let $R(X)$ be a nonconstant p-free polynomial. Adapt the Mordell argument to show that:

   $$|\sum_{x \in \mathbb{F}_q} \psi(R(x))| \leq O(d \cdot q^{1-\frac{1}{2d}}).$$

   (d) Use this to deduce a bound on:

   $$|\sum_{x \in \mathbb{F}_q} \psi(P(x))|,$$

   for every $P(X) \in \mathbb{F}_q[X]$.

2. **(3 points)**

   (a) Show that if $\mathbb{F}_q$ has proper subfields, there are nontrivial multiplicative subgroups $H \subseteq \mathbb{F}_q$ and nontrivial additive characters ψ with:

   $$|\sum_{x \in H} \psi(x)| = |H|.$$

   Thus it is not reasonable to always expect cancellation in $|\sum_{x \in H} \psi(x)|$.

   (b) Suppose $H \subseteq \mathbb{F}_q$ is a nontrivial multiplicative subgroup and ψ is a nontrivial additive character such that:

   $$|\sum_{x \in H} \psi(x)| = |H|.$$

   Show that H must be contained in a proper subfield of $\mathbb{F}_q$.

   (c) The bound for the Waring problem that we proved in class implies that for every $\delta > 1/2$: For every prime power q, if H is a multiplicative subgroup of $\mathbb{F}_q$ of size $\geq q^\delta$, then every element of $\mathbb{F}_q$ can be written as the sum of c_δ elements of H.
   Show that this theorem is not true for any $\delta < 1/2$.

3. **(3 points)** We will see some relations between Fourier coefficients and uniform distribution in subspaces/APs.

   (a) Suppose $T \subseteq \mathbb{F}_q$ is such that for all nonzero $a \in \mathbb{F}_q$, $|\hat{1_T}(a)| \leq \frac{\epsilon|T|}{q}$.
   Show that for every subspace or AP S in $\mathbb{F}_q$, we have:

$$\left| \frac{|T \cap S|}{|T|} - \frac{|S|}{q} \right| \leq O(\epsilon \cdot \log q).$$

   (That is: the right fraction of T lies in S.)

   (b) Let $q = 2^n$. Suppose $T \subseteq \mathbb{F}_q$ is such that for every subspace S, we have:

$$\left| \frac{|T \cap S|}{|T|} - \frac{|S|}{q} \right| \leq \epsilon.$$

   Show that for every $a \neq 0$, the additive Fourier coefficient $|\hat{1_T}(a)| \leq 2\frac{\epsilon|T|}{q}$.

   (c) Let q be prime. Suppose $T \subseteq \mathbb{F}_q$ is such that for every AP S, we have:

$$\left| \frac{|T \cap S|}{|T|} - \frac{|S|}{q} \right| \leq \epsilon.$$

   Show that for every $a \neq 0$, the additive Fourier coefficient $|\hat{1_T}(a)| \leq O\left(\frac{\epsilon|T|}{q}\right)$.

4. **(2 points)** Let S be an AP or subspace in $\mathbb{F}_q$ of size $\gg q^{0.9}$, and let $P(X), Q(X), R(X)$ be polynomials of degree at most 100. Give conditions on P, Q, R which guarantee that $|\{x \in \mathbb{F}_q \mid (P(x), Q(x), R(x)) \in S^3\}|$ is about $\frac{|S|^3}{q^3} \cdot q$. Give examples of P, Q, R where this set is abnormally small and where this set is abnormally large.

5. **(2 points)** A squarefree polynomial $F(X)$ is a polynomial which is not divisible by $R(X)^2$ for any $R(X)$ with degree ≥ 1.

   Define

$$H(s) = \sum_{F(X) \in \mathbb{F}_q[X],\ \text{monic, squarefree}} \frac{1}{|F(X)|^s}.$$

   Find a Euler-like factorization of $H(s)$. Use this to find a relation between $H(s)$ and $\zeta(s)$. Thus compute the number of monic, squarefree polynomials of degree d.

6. **(2 points)** Let ψ be a nontrivial additive character and and let χ be a nontrivial multiplicative character of $\mathbb{F}_q$. Define the character $\Delta : \mathbb{F}_q[T] \to \mathbb{C}$ by:

$$\Delta(\sum_{i=0}^{d} a_i T^{d-i}) = \psi(a_1/a_0)\chi(a_d/a_0),$$

   where $a_0 \neq 0$.

   Show that all the zeroes of the L-function $L(s, \Delta)$ are of the form $\frac{1}{2} + it$.