# D-MATH HS 2018 Prof. Emmanuel Kowalski
# Exponential sums over Finite Fields. Exercise Sheet 3

October 23, 2018

**Definition 1.** Let $p$ be a prime number and let $a \in \mathbb{F}_p^\times$. The *Heilbronn sum* $H(a;p)$ is defined by

$$H(a;p) := \sum_{x \in \mathbb{F}_p^\times} e\Big(\frac{ax^p}{p^2}\Big). \tag{1}$$

The goal of this exercise sheet is to prove the following

**Theorem 1.** *We have*

$$H(a;p) \ll p^{11/12},$$

*for all primes $p$ and $a \in \mathbb{F}_p^\times$, where the implied constant is absolute.*

**Exercise 1.** Show that for any $n, m \in \mathbb{Z}$ such that $m \equiv n \mod p$, one has

$$e\Big(\frac{am^p}{p^2}\Big) = e\Big(\frac{an^p}{p^2}\Big),$$

and conclude that $H(a;p)$ is well-defined.

**Exercise 2.** Let $p$ be a prime number. Define the polynomial

$$L_p := X + \frac{X^2}{2} + \cdots + \frac{X^{p-1}}{p-1} \in \mathbb{F}_p[X],$$

and let

$$\mathcal{N}_r(\mathbb{F}_p) := \{x \in \mathbb{F}_p \setminus \{0,1\} : L(x) = r\},$$

for any $r \in \mathbb{F}_p$. The goal of this exercise is to show that, for any $a \in \mathbb{F}_p^\times$, one has

$$|H(a;p)| \leq (p-1)^{1/2} + \mathcal{N}(\mathbb{F}_p)^{1/4} p^{3/4},$$

where

$$\mathcal{N}(\mathbb{F}_p) := \max_{r \in \mathbb{F}_p} |\mathcal{N}_r(\mathbb{F}_p)|.$$

Proceed as follows

*i)* Assume $p \neq 2$. Show that

$$|H(a;p)|^2 = p - 1 + \sum_{x \in \mathbb{F}_p^\times} \sum_{u \in \mathbb{F}_p \setminus \{0,1\}} e\Big(\frac{a(x^p(1-(1-u)^p))}{p^2}\Big).$$

*ii*) Prove that for any $1 \leq j \leq p-1$ one has

$$\binom{p}{j} \equiv (-1)^{j-1}\frac{p}{j},$$

and conclude that

$$|H(a;p)|^2 = p-1+\sum_{x\in\mathbb{F}_p^\times}\sum_{u\in\mathbb{F}_p\setminus\{0,1\}} e\Big(\frac{ax^p(u^p+pL_p(u))}{p^2}\Big).$$

*iii*) Show that

$$|H(a;p)|^2 = p-1+\sum_{x\in\mathbb{F}_p^\times}\sum_{u\in\mathbb{F}_p\setminus\{0,1\}} e\Big(\frac{a(xu)^p(1-pL_p(u^{-1}))}{p^2}\Big),$$

and deduce that

$$|H(a;p)|^2 = p-1+\sum_{r\in\mathbb{F}_p} H(a(1-pr);p)|\mathcal{N}_r(\mathbb{F}_p)|.$$

*iv*) Prove that

$$\sum_{r\in\mathbb{F}_p}|\mathcal{N}_r(\mathbb{F}_p)| = p-2, \qquad \sum_{r\in\mathbb{F}_p}|H(a(1-pr);p)|^2 = p(p-1),$$

and conclude the exercise.

**Exercise 3.** Let $K$ be a field of characteristic $p>0$, $f\in K[X]$ a polynomial and $0\leq m\leq p$. Prove that an element $x\in K$ is a zero of $f$ of order $\geq m$ if and only if

$$f(x)=f'(x)=\cdots=f^{m-1}(x)=0.$$

If $x\neq 1,0$, then $x\in K$ is a zero of $f$ of order $\geq m$ if and only if

$$f(x)=\delta f'(x)=\cdots=\delta^{m-1}f(x)=0,$$

where $\delta$ is the linear map

$$\delta : \begin{array}{ccc} K[X] & \to & K[X] \\ f & \mapsto & X(1-X)f' \end{array}.$$

**Exercise 4.** We denote by $\Phi$ the $\mathbb{F}_p$-linear map

$$\Phi : \begin{array}{ccc} \mathbb{F}_p[A,B,C] & \to & \mathbb{F}_p[X] \\ F & \mapsto & F[X,X^p,L_p(X)] \end{array},$$

where $L_p$ is as before. The goal of this exercise is to prove the following: for $F\in\mathbb{F}_p[A,B,C]$ and $G=F[X,X^p,L_p(X)]\in\mathbb{F}_p[X]$, we have

$$\delta G = X(1-X)G' = \partial(F)(X,X^p,L_p(X)) = \Phi(\partial(F)),$$

where $\partial$ denotes the map

$$\partial : \begin{array}{ccc} \mathbb{F}_p[A,B,C] & \to & \mathbb{F}_p[A,B,C] \\ F & \mapsto & A(1-A)\frac{\partial F}{\partial A}+(A-B)\frac{\partial F}{\partial C} \end{array}.$$

Proceed as follows

*i)* Reduce to the case when $F = A^a B^b C^c$.

*ii)* Show that either $\Delta = \Phi \circ \partial$ or $\Delta = \delta \circ \Phi$ as $\mathbb{F}_p$-linear maps

$$\mathbb{F}_p[A, B, C] \to \mathbb{F}_p[X]$$

satisfy the following version of the Leibniz rule:

$$\Delta(F_1 F_2) = \Phi(F_1)\Delta(F_2) + \Phi(F_2)\Delta(F_1),$$

for $F_1, F_2 \in \mathbb{F}_p[A, B, C]$.

*iii)* Conclude.

**Exercise 5.** Let $r \in \mathbb{F}_p$ be fixed. If $0 \le m < p$ and $a, b, c \ge 1$ are integers such that

$$m(a + b + m - 1) < abc. \tag{2}$$

Then there exists a non-zero polynomial $F \in \mathbb{F}_p[A, B, C]$ such that

$$\deg_A(F) < a, \qquad \deg_B(F) < b, \qquad \deg_C(F) < c,$$

and

$$F(X, X, r) = (\partial F)(X, X, r) = \cdots = (\partial^{m-1} F)(X, X, r) = 0,$$

and in particular such that each $x \in \mathcal{N}_r(\mathbb{F}_p)$ is a zero of

$$G = F(X, X^p, L_p(X))$$

of order $\ge m$.

Proceed as follows

*i)* Fix $a, b, c \ge 1$ and let $\mathcal{V}(a, b, c)$ denote the $\mathbb{F}_p$-subspace of $\mathbb{F}_p[A, B, C]$ of polynomials $F$ such that

$$\deg_A(F) < a, \qquad \deg_B(F) < b, \qquad \deg_C(F) < c,$$

and similarly $\mathcal{H}(d)$ be the subspace of polynomials in $\mathbb{F}_p[X]$ of degree $< d$. Prove that for any $j = 0, ..., m - 1$

$$\Psi \circ \partial^j(\mathcal{V}(a, b, c)) \subset \mathcal{H}(a + b + 2j),$$

where

$$\Psi : \begin{array}{ccc} \mathbb{F}_p[A, B, C] & \to & \mathbb{F}_p[X] \\ F & \mapsto & F(X, X, r) \end{array}.$$

*ii)* Conclude.

**Exercise 6.** Assume $F \in \mathbb{F}_p[A, C]$ is not zero and is of the form

$$F = \sum_{k<c} F_k C^k$$

where $F_k \in \mathbb{F}_p[A]$ has degree $\deg_A(F_k) \le a_k$, $F_{c-1} \neq 0$, and

$$a_0 \ge a_1 \ge \cdots \ge a_{c-1}.$$

Moreover, let us denote

$$d := a_0 + \cdots + a_{c-1}. \tag{3}$$

Our goal is to prove the following claim: if $d + c - 1 \le p$, we have $v(F(X, L_p(X))) \le d + c - 1$, where $v(\cdot)$ denotes the order of vanishing of a polynomial at 0.

Proceed as follows

*i)* Prove the case $c = 1$.

*ii)* Let $c \geq 1$. Prove the statement in the case $d = 0$.

*iii)* Assume that the statement is true for all integers $< c$ and all integers $< d$. Let $F \in \mathbb{F}_p[A, C]$ be given with $\deg_C(C) = c - 1$ and

$$d = a_0 + \cdots + a_{c-1}$$

and satisfying $v(F(X, L_p(X))) \geq c + d$. Prove that

$$(X-1)(F(X, L_p(X)))' \equiv \phi(H) \mod X^{p-1},$$

where
$$H = \sum_{0 \leq k < c-1} \Big((A-1)F_k' - (k+1)F_{k+1}\Big)C^k - (A-1)F_{c-1}'C^{c-1}.$$

Deduce that $v(\Phi(H)) \geq c + d - 1$.

*iv)* Consider the polynomial $\tilde{H} := H - (\deg_A(F_{c-1}))F$, use the inductive step to deduce that $\tilde{H} = 0$, and thus

$$\begin{cases} (A-1)F_{c-1}' - \deg_A(F_{c-1})F_{c-1} = 0, \\ (A-1)F_{c-2}' - \deg_A(F_{c-1})F_{c-2} = (c-1)F_{c-1}. \end{cases}$$

Hence, conclude that $F = 0$, which contradicts our assumption $F_{c-1} \neq 0$.

**Exercise 7.** Let $m \leq p$ and let $a, b, c \geq 1$ be integers such that

$$ac \leq m$$

Then
$$\Phi : \begin{array}{ccc} \mathcal{V}(a,b,c) & \to & \mathbb{F}_p[X] \\ F & \mapsto & F(X, X^p, L_p(X)) \end{array}$$

is injective.

Proceed as follows:

*i)* Let us write

$$\Phi(F) = \sum_j F_j(X, L_p(X))X^{pj}.$$

Prove that if $\Phi(F) = 0$, then
$$v(F_j(X, L_p(X))) \geq p$$

for some $j$.

*ii)* Use the previous exercise to conclude.

**Exercise 8.** Show that
$$\mathcal{N}_r(\mathbb{F}_p) \ll p^{2/3}.$$

Proceed as follows

*i)* Assume that

$$\begin{cases} m < p, \\ m(a+b+m-1) < abc, \\ ac \leq p \end{cases}$$

then prove that

$$\mathcal{N}_r(\mathbb{F}_p) \leq \frac{a + pb + (p-1)c}{m}.$$

*ii)* Choose $m = a = [p^{2/3}]$, $b = 10[p^{1/3}]$ and $c = [p^{1/3}]$ and conclude[1].

**Exercise 9.** Prove Theorem 1.

[1] $[x]$ denotes the integral part of $x$.