FINITE FIELDS AND APPLICATIONS
Characters and character sums (9 lectures)

Ana Zumalacárregui
a.zumalacarregui@unsw.edu.au

May 12, 2016

Contents

**

Exponential sums and character sums have many applications in number theory and combinatorial number theory. Many famous and interesting problems have been studied by means of exponential sums techniques: Goldbach ternary conjecture (Vinogradov), Waring Problem (Hardy, Littlewood, Vaughan, Vinogradov, Wooley), Distribution of prime numbers (Ford, Hardy, Korobov, Linnik,...) as well as many other interesting questions.

The applications of these techniques are so wide, that they represent a very active research area nowadays. In this short introductory course we will discuss some basic theory of characters, focusing on the finite field case, and show some classic examples of character sums as well as some applications.

Notation: From now on, we will denote by $\mathbf{e}(x) := e^{2\pi i x}$ and, for some positive integer n, $\mathbf{e}_n(x) := \mathbf{e}(\frac{x}{n}) = e^{2\pi i x/n}$. Note that for any $x, y \in \mathbb{R}$ and a positive integer n we have

$$\mathbf{e}\left(x+y\right) = \mathbf{e}\left(x\right)\mathbf{e}\left(y\right) \quad \text{and} \quad \mathbf{e}_n\left(x+y\right) = \mathbf{e}_n\left(x\right)\mathbf{e}_n\left(y\right).$$

For a ring R (or field) we denote by $R^\times$ the group of units or set of invertible elements in R, depending on the context.

Along the text p will denote a prime number, q will be a power of the prime p and $\mathbb{F}_q$ will denote the finite field of q elements. In many occasions we will identify the elements in the prime field $\mathbb{F}_p$ with its corresponding residues in $\{0, 1, \ldots, p-1\}$. The cyclic group of n elements will be denoted by $\mathbb{Z}_n$.

Let $\mathbb{F}_q^m/\mathbb{F}_q$ be a finite extension of finite fields. The *trace map* from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ is the $\mathbb{F}_q$-linear map

$$\begin{array}{rccc} \mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q}: & \mathbb{F}_q^m & \to & \mathbb{F}_q \\ & x & \mapsto & x + x^q + \cdots + x^{q^{m-1}} \end{array}.$$

1 Characters

Let G be a finite abelian group (written multiplicatively) of order $|G|$ with identity element 1_G. A *character* χ of G is a homomorphism from G into the multiplicative group of the complex numbers $\mathbb{C}^\times$, that is $\chi : G \to \mathbb{C}^\times$ with

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2).$$

Clearly, $\chi(1_G) = \chi(1_G)\chi(1_G)$ which implies that $\chi(1_G) = 1$. Furthermore,

(i) For every $g \in G$,

$$(\chi(g))^{|G|} = \chi\left(g^{|G|}\right) = \chi(1_G) = 1,$$

so the values of χ are $|G|$th roots of unity.

(ii) For every $g \in G$ and every character χ, we have that $\chi(g)\chi(g^{-1}) = \chi(1_G) = 1$ and so $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$, where the bar denotes the complex conjugation.

Among the characters of G we have the *trivial* character, denoted by χ_0, defined by $\chi(g) = 1$ for every $g \in G$: all the other characters are called nontrivial.

Proposition 1.1. *The set $\widehat{G}$ of characters of G forms a finite abelian group with respect to the operation $\cdot$ given by*

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g) \quad \text{for every } g \in G.$$

Proof. Left as an exercise.

Example 1. *Let G be the cyclic group of order n and let g be a generator of G. For a fixed integer j, $0 \le j \le n-1$, the function*

$$\chi_j(g^k) = \mathbf{e}(k/n), \quad k = 0, 1, \ldots, n-1,$$

defines a character of G. In fact, those are all the characters in $\widehat{G}$ (see Corollary 1.5).

Theorem 1.2. *Let H be a subgroup of a finite abelian group G and let ψ be a character of H. Then ψ can be extended to a character of G: i.e. there exists a character $\chi \in \widehat{G}$ with $\chi(h) = \psi(h)$ for every $h \in H$.*

Proof. Suppose that H is a proper subgroup of G, since otherwise there is nothing to prove. Choose $a \in G \setminus H$ and let H_1 be the subgroup generated by H and a. Let m be the minimum integer such that $a^k \in H$. Then, for every $g \in H_1$ there exist a unique representation of the form

$$g = a^k h \quad \text{where} \quad k \in \{o, 1, \ldots, m-1\},\ h \in H.$$

Define a function $\psi_1 : H_1 \to \mathbb{C}^\times$ by $\psi_1(g) = \omega^k \psi(h)$ where ω is a fixed complex number satisfying

$$\omega^m = \psi(a^m). \tag{1}$$

We claim that ψ_1 is a character in H_1 whose restriction to H is precisely ψ. Let $g_1 = a^k h_1, g_2 = a^s h_2 \in H_1$, then $g_1 g_2 = a^{k+s} h_1 h_2$. If $k + s < m$ then

$$\psi_1(g_1 g_2) = \omega^{k+s}\psi(h_1 h_2) = \omega^k \psi(h_1)\omega^s \psi(h_2) = \psi_1(g_1)\psi_1(g_2),$$

if $k + s \ge m$, then since $a^m \in H$, we have that

$$\psi_1(g_1 g_2) = \omega^{k+s-m}\psi(h_1 h_2 a^m) = \omega^{k+s-m}\psi(a^m)\psi(h_1 h_2) = \omega^{k+s}\psi(h_1 h_2) = \psi_1(g_1)\psi_1(g_2)$$

from (1).

It follows from the definition of ψ_1 that $\psi_1(h) = \psi(h)$ for every $h \in H$.

If $H_1 = G$ the result follows. Otherwise, we can always repeat the process for a new element $b \in G \setminus H_1$ and in a finite number of steps (since our group is finite) this algorithm ends and for some iteration we will have $H_t = G$. □

Corollary 1.3. *For any $h \neq 1_G$, there exists a character χ in G for which $\chi(g) \neq 1$.*

Proof. Let H be the subgroup of G generated by h, which is cyclic of order m for some $m \geq 2$. It follows from Example 1 that

$$\psi(h^k) = \mathbf{e}(k/m)$$

defined a character in H with $\psi(h) = \mathbf{e}(1/m) \neq 1$ (since $m \geq 2$). It follows from Theorem 1.2 that ψ can be extended to a character in G. □

Remark 1. *The previous result implies that the group of characters discriminate between distinct elements in the group: if $g_1 \neq g_2$ in G then there must exist a character $\chi \in \widehat{G}$ with $\chi(g_1) \neq \chi(g_2)$.*

Theorem 1.4 (Orthogonality of the characters)**.** *Let G be a finite abelian group. Then, for any $\chi \in \widehat{G}$*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

And for any given $g \in G$ we have

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |\widehat{G}| & \text{if } g = 1_E, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Proof. Clearly, if $\chi = \chi_0$ the equality in (2) holds. Let us assume that $\chi \neq \chi_0$. Since χ is nontrivial, there exist an element $h \in G$ with $\chi(h) \neq 1$. Then

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g),$$

because if g runs through G, so does hg. Thus we have

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0,$$

which already implies (2).

For the second part, once again we will assume that $g \neq 1_G$, since otherwise the result is trivial. Note that the function $\widehat{g}(\chi) = \chi(g)$ is a character for the group $\widehat{G}$. This character is nontrivial if $g \neq 1_G$, since from Corollary 1.3 there exist some $\chi \in \widehat{G}$ with $\widehat{g}(\chi) = \chi(g) \neq 1$.

Therefore, the equality in (3) follows from (2) applied to the group $\widehat{G}$:

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \widehat{g}(\chi) = 0.$$

□

Corollary 1.5. *Let G be a finite abelian group. Then $|\widehat{G}| = |G|$.*

Proof. It follows from the orthogonality properties of the characters that

$$|G| = \sum_{g \in G} \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) = |\widehat{G}|.$$

□

$$- \star -$$

In a finite field $\mathbb{F}_q$ there are two finite abelian groups: the additive group $(\mathbb{F}_q, +)$ and the multiplicative group of the field $(\mathbb{F}_q^\times, \cdot)$. In this context, we will consider additive and multiplicative characters in $\mathbb{F}_q$. From now on additive characters will be denoted by the Greek letter φ while the letter χ will be reserved to multiplicative ones.

1.1 Additive characters

Let p be the characteristic of $\mathbb{F}_q$, that is $q = p^n$ for some positive integer n. Then the prime field contained in $\mathbb{F}_q$ is $\mathbb{F}_p$, which we identify with $\mathbb{Z}_p$.

Let $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q|\mathbb{F}_p}$ be the trace function from $\mathbb{F}_q$, $q = p^n$, to $\mathbb{F}_p$ defined before. Recall that

$$\mathrm{Tr}(c) = c + c^p + c^{p^2} + \cdots + c^{p^{n-1}} \in \mathbb{F}_p.$$

Then the function φ_1 defined by

$$\varphi_1(c) = \mathbf{e}_p\left(\mathrm{Tr}(c)\right) = e^{2\pi i \mathrm{Tr}(c)/p} \quad \text{for all } c \in \mathbb{F}_q \tag{4}$$

is a character of the additive group of $\mathbb{F}_q$, since $\mathrm{Tr}(a+b) = \mathrm{Tr}(a) + \mathrm{Tr}(b)$ for every $a, b \in \mathbb{F}_q$, and furthermore φ_1 is a nontrivial character. The character defined in (4) will be called the *canonical additive character* in $\mathbb{F}_q$.

All characters of $\mathbb{F}_q$ can be expressed in terms of φ_1.

Theorem 1.6. *For a given $b \in \mathbb{F}_q$, the function φ_b with $\varphi_b(c) := \varphi_1(cb)$ for every $c \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$. Furthermore, every additive character of $\mathbb{F}_q$ is obtained in this way.*

Proof. For any $c_1, c_2 \in \mathbb{F}_q$ we have,

$$\varphi_b(c_1 + c_2) = \varphi_1(bc_1 + bc_2) = \varphi_1(bc_1)\varphi_1(bc_2) = \varphi_b(c_1)\varphi_b(c_2),$$

and the first part is established. Since φ_1 is a nontrivial character, for every $a, b \in \mathbb{F}_q$, $a \neq b$, we have

$$\frac{\varphi_a(c)}{\varphi_b(c)} = \frac{\varphi_1(ac)}{\varphi_1(bc)} = \varphi((a-b)c) \neq 1,$$

for suitable $c \in \mathbb{F}_q$, and so φ_a and φ_b are distinct characters. From Corollary 1.5 it follows that $\mathbb{F}_q$ has exactly q characters, so the list of characters is complete. □

By setting $b = 0$ in (4) we obtain the trivial character $\varphi_0(c) = \varphi_1(0 \cdot c) = \varphi_1(0) = 1$ for every $c \in \mathbb{F}_q$.

Example 2. *Prime fields $\mathbb{F}_p$. The additive group of $\mathbb{F}_p$ is a cyclic group of p elements and clearly, in this case, the trace function is simply the identity $\mathrm{Tr}(c) = c$ for every $c \in \mathbb{F}_p$.*

In this setting all additive characters in $\mathbb{F}_p$ are given by

$$\varphi_a(c) = \mathbf{e}_p(ac) = e^{2\pi i ac/p} \quad \text{for every } c \in \mathbb{F}_p,$$

where $a \in \mathbb{F}_p$ is the element which index the character. With this characterization it is clear that $G = (\mathbb{Z}_p, +) \cong \widehat{G}$, with the isomorphism $a \mapsto \varphi_a$.

1.2 Multiplicative characters

The characters of the multiplicative group $\mathbb{F}_q^\times$ of $\mathbb{F}_q$ are called *multiplicative characters* of $\mathbb{F}_q$. Since $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$ and its characters can be easily determined.

Theorem 1.7. *Let g be a fixed primitive element of $\mathbb{F}_q$. For each $j = 0, 1, \ldots, q-2$ the function χ_j with*

$$\chi_j\left(g^k\right) = e^{2\pi i jk/(q-1)} \quad \text{for } k = 0, 1, \ldots, q-2 \tag{5}$$

defines a multiplicative character of $\mathbb{F}_q$. Furthermore, every multiplicative character of $\mathbb{F}_q$ is obtained in this way.

Proof. The result follows from Example 1 and Corollary 1.5. □

Remark 2. *It is clear from the definition of χ_j that the group of multiplicative characters of $\mathbb{F}_q$ is cyclic of order $q-1$ with identity element χ_0.*

Remark 3. *For every j relatively prime to $q-1$ we have that g^j is another primitive element of $\mathbb{F}_q$. Thus, the character χ_j is a new generator of the group of multiplicative characters $\widehat{G} = \widehat{(\mathbb{F}_q^\times, \cdot)}$.*

Example 3. *Legendre symbol: let us consider, for a given finite field $\mathbb{F}_q$ with odd characteristic, the character defined in* (5) *for* $j = (q-1)/2$.

Such character $\chi_{(q-1)/2}$ is called the quadratic character of $\mathbb{F}_q$ and coincides with the known as Legendre symbol, usually denoted by $\left(\frac{\cdot}{q}\right)$, and satisfies for $c \in \mathbb{F}_q^\times$

$$\chi_{(q-1)/2}(c) = \left(\frac{c}{q}\right) = \begin{cases} 1 & \text{if } c \text{ is a square in } \mathbb{F}_q^\times, \\ -1 & \text{otherwise.} \end{cases}$$

It is called the quadratic character because it is the only character χ of $\mathbb{F}_q$ with $\chi^2 \equiv \chi_0$.

It will be convenient for some applications to extend multiplicative characters in $\mathbb{F}_q^\times$ to the complete field by imposing $\chi(0) = 0$ if $\chi \neq \chi_0$ and $\chi_0(0) = 1$. With this definition, we have then

$$\sum_{c \in \mathbb{F}_q} \chi(c) = \begin{cases} q & \text{if } \chi \text{ is trivial,} \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Furthermore, this extension is compatible with the character structure: $\chi(c \cdot 0) = \chi(c)\chi(0)$ for every $c \in \mathbb{F}_q$.

2 Complete and incomplete character sums

For most of the applications, we will be interested in the behaviour in sums of the form:

$$\sum_{a \in A} \psi(f(a)), \tag{7}$$

where $A \subseteq \mathbb{F}_q$ is a set, ψ a character (additive o multiplicative) in $\mathbb{F}_q$ and f is some interesting function in $\mathbb{F}_q$ as well. Whenever $A = \mathbb{F}_q$, we will say that the sum is *complete* otherwise we say that it is an *incomplete* character sum.

In some cases, very few of them, we might obtain closed formulas for the value of certain character sums, but in general our only aim is to obtain any bound better than trivial for the quantity in (7): *i.e.* anything upper bound better than

$$\left| \sum_{a \in A} \psi(f(a)) \right| \leq \sum_{a \in A} \left| \psi(f(a)) \right| = |A|.$$

The objective of our study will be to obtain bounds of the form:

$$\left| \sum_{a \in A} \psi(f(a)) \right| \leq \Delta |A|$$

where either $\Delta < 1$ is a constant or $\Delta = \Delta(|A|)$ is a quantity that tends to zero as $|A|$, q tend to infinity.

2.1 Complete sums

The following result, which follows from the orthogonality of the characters, suggests that one might use character sums to count solutions to certain congruences.

Corollary 2.1. *Let ψ_a, ψ_b be two additive (resp. multiplicative) characters in $\mathbb{F}_q$. Then,*

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \psi_a(c)\overline{\psi_b(c)} = \begin{cases} 0 & \text{if } a \neq b, \\ 1 & \text{if } a = b. \end{cases}$$

Furthermore, summing up over all possible characters, we have that

$$\frac{1}{q} \sum_{\psi} \psi(c)\overline{\psi(d)} = \begin{cases} 0 & \text{if } c \neq d, \\ 1 & \text{if } c = d. \end{cases}$$

Proof. Observe that the character $\psi_a \cdot \overline{\psi_b} = \psi_a \cdot \psi_b^{-1} = \psi_0$ if and only if $a = b$ and that for any character ψ we have that $\psi(c)\overline{\psi(d)} = \psi(c-d)$ if ψ is additive (resp. $\psi(cd^{-1})$ if ψ is multiplicative). The result follows from Theorem 1.4 and the previous observations. □

In particular, for any function f we have that:

$$\frac{1}{q}\sum_{a\in\mathbb{F}_q}\psi_a(f(c))\overline{\psi_a(d)} = \begin{cases} 0 & \text{if } f(c)\neq d \\ 1 & \text{if } f(c)=d, \end{cases}$$

which implies that

$$\#\{c : f(c) = d\} = \sum_{c\in\mathbb{F}_q}\sum_{a\in F_q}\psi_a(f(c))\overline{\psi_a(d)}.$$

So we can encode many problems in these terms and exploit the techniques we will discuss in the following sections to obtain results.

Theorem 2.2. *The polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

$$\sum_{c\in\mathbb{F}_q}\varphi(f(c)) = 0 \tag{8}$$

for all non-trivial additive characters φ of $\mathbb{F}_q$.

Proof. If f is a permutation polynomial of $\mathbb{F}_q$ and φ is a non-trivial additive character, then

$$\sum_{c\in\mathbb{F}_q}\varphi(f(c)) = \sum_{c\in\mathbb{F}_q}\varphi(c) = 0$$

from the orthogonality of characters. Conversely, if φ_0 denotes the trivial additive character of $\mathbb{F}_q$ and (8) holds for all $\varphi \neq \varphi_0$, then for any $a \in \mathbb{F}_q$ the number N of solutions to $f(x) = a$ in $\mathbb{F}_q$ is given by

$$N = \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{\varphi}\varphi(f(c))\overline{\varphi(a)} = 1 + \frac{1}{q}\sum_{\varphi\neq\varphi_0}\overline{\varphi(a)}\sum_{c\in\mathbb{F}_q}\varphi(f(c)) = 1,$$

hence f is a permutation polynomial of $\mathbb{F}_q$. □

2.2 Incomplete sums

The first non-trivial example of a general bound for incomplete character sums in prime fields is the following result, where the set A is an interval modulo p.

Proposition 2.3. *For any prime p and any integer $0 \leq N \leq p-1$*

$$\sum_{\varphi}\left|\sum_{x=0}^{N-1}\varphi(x)\right| = O\left(p\log p\right),$$

where the sum is taken over all additive characters of $\mathbb{F}_p$.

Proof. See question (6) in tutorial questions 7. □

Observe that the trivial bound for the sum appearing in Proposition 2.3 is precisely pN, which means that the obtained bound is non-trivial as long as N is greater than some constant times $\log p$.

Remark 4. *For any complex number $x \in \mathbb{C}^\times$ we have: $|x|^2 = x\cdot\overline{x}$. Therefore, for any additive character φ and any subset $\mathcal{X}$ of $\mathbb{F}_q$ we have:*

$$\left|\sum_{a\in\mathcal{X}}\varphi(a)\right|^2 = \left(\overline{\sum_{a\in\mathcal{X}}\varphi(a)}\right)\cdot\left(\sum_{b\in\mathcal{X}}\varphi(b)\right) = \sum_{a,b\in\mathcal{X}}\varphi(b-a). \tag{9}$$

Let $\mathcal{X}$ and $\mathcal{Y}$ be arbitrary subsets of $\mathbb{F}_q$. For a given an additive character φ let us define the sum

$$W_\varphi = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} \varphi(xy).$$

Trivially we have that $|W_\varphi| \le |\mathcal{X}||\mathcal{Y}|$ and clearly the equality is attained for $\varphi = \varphi_0$ the trivial character.

Theorem 2.4. *For any sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_q$,*

$$\max_{\varphi\neq\varphi_0} |W_\varphi| \le (|\mathcal{X}||\mathcal{Y}|q)^{1/2}.$$

This bound improves the trivial bound for very *sparse* sets as long as $|\mathcal{X}||\mathcal{Y}| \ge q$.

Proof. We have

$$|W_\varphi| = \left|\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} \varphi(xy)\right| \le \sum_{x\in\mathcal{X}}\left|\sum_{y\in\mathcal{Y}} \varphi(xy)\right|.$$

From the Cauchy-Schwarz inequality[1] it follows that

$$|W_\varphi|^2 \le |\mathcal{X}| \sum_{x\in\mathcal{X}}\left|\sum_{y\in\mathcal{Y}} \varphi(xy)\right|^2 \le |\mathcal{X}| \sum_{x\in\mathbb{F}_q}\left|\sum_{y\in\mathcal{Y}} \varphi(xy)\right|^2.$$

Now observe that it follows from (9)

$$\sum_{x\in\mathbb{F}_q}\left|\sum_{y\in\mathcal{Y}} \varphi(xy)\right|^2 = \sum_{x\in\mathbb{F}_q}\sum_{y_1,y_2\in\mathcal{Y}} \varphi(x(y_1-y_2)) = \sum_{y_1,y_2\in\mathcal{Y}}\sum_{x\in\mathbb{F}_q} \varphi(x(y_1-y_2)).$$

Now observe that from Theorem 1.6 and by (3)

$$\sum_{x\in\mathbb{F}_q} \varphi(x(y_1-y_2)) = \sum_{\psi} \psi(y_1-y_2) = q$$

if $y_1 = y_2$ and 0 otherwise, and the sum is taken over all additive characters. Therefore

$$|W_\varphi|^2 \le |\mathcal{X}||\mathcal{Y}|q.$$

□

3 Some famous examples

3.1 Gauss sums

Let φ be an additive character and χ a multiplicative character of $\mathbb{F}_q$, then the Gaussian sum $G(\varphi,\chi)$ is defined by

$$G(\varphi,\chi) = \sum_{c\in\mathbb{F}_q} \varphi(c)\chi(c),$$

Recall that φ_0 and χ_0 denote the trivial additive and multiplicative characters respectively.

The absolute value of $G(\varphi,\chi)$ is trivially $\le q$. The equality is attained at $\varphi = \varphi_0$ and $\chi = \chi_0$, but in most cases this quantity will be considerably smaller.

Remark 5. *It follows from* (6) *that $G(\varphi_0,\chi) = 0$, if $\chi \neq \chi_0$, and from* (2) *that $G(\varphi,\chi_0) = 0$, if $\varphi \neq \varphi_0$.*

The interesting phenomena occurs when one considers nontrivial characters.

[1] For any $2n$ complex numbers $x_1, y_1, \ldots, x_n, y_n$ we have $|\sum_{i=1}^n x_i\overline{y_i}|^2 \le \sum_{i=1}^n |x_i|^2 \sum_{i=1}^n |y_i|^2$.

Theorem 3.1. *Let φ be an additive character and χ a multiplicative character in $\mathbb{F}_q$. If $\varphi \neq \varphi_0$ and $\chi \neq \chi_0$, then*

$$|G(\varphi,\chi)| = q^{1/2}.$$

Proof.

$$|G(\varphi,\chi)|^2 = \overline{G(\varphi,\chi)}G(\varphi,\chi) = \sum_{b\in\mathbb{F}_q^\times}\sum_{a\in\mathbb{F}_q^\times} \overline{\varphi(b)}\,\overline{\chi(b)}\,\varphi(a)\,\chi(a) = \sum_{b\in\mathbb{F}_q^\times}\sum_{a\in\mathbb{F}_q^\times} \varphi(a-b)\chi(ab^{-1}).$$

In the inner sum we substitute $ab^{-1} = c$, and so $a - b = b(c-1)$. Then

$$\begin{aligned}|G(\varphi,\chi)|^2 &= \sum_{b\in\mathbb{F}_q^\times}\sum_{c\in\mathbb{F}_q^\times} \varphi(b(c-1))\chi(c)\\ &= \sum_{c\in\mathbb{F}_q^\times}\chi(c)\left(\sum_{b\in\mathbb{F}_q}\varphi(b(c-1)) - \varphi(0)\right) = \sum_{c\in\mathbb{F}_q^\times}\chi(c)\sum_{b\in\mathbb{F}_q}\varphi(b(c-1)), \qquad (10)\end{aligned}$$

since from Theorem 1.4 it follows that $\sum_{c\in\mathbb{F}_q^\times}\chi(c)\varphi(0) = 0$. From Theorem 1.4 it follows that the inner sum

$$\sum_{b\in\mathbb{F}_q}\varphi(b(c-1)) = \begin{cases} q & \text{if } c = 1,\\ 0 & \text{if } c \neq 1.\end{cases}$$

Plugging the above equality into (10) we obtain $|G(\varphi,\chi)|^2 = \chi(1)q = q$. □

Gaussian sums, as defined before, have several applications in connecting additive and multiplicative characters and sometimes it allow us to estimate certain exponential sums.

Corollary 3.2. *For any prime $p \leq 3$ and any integer a with $\gcd(a,p) = 1$, we have*

$$\Big|\sum_{x=0}^{p-1}\mathbf{e}_p(ax^2)\Big| = p^{1/2}.$$

Proof. Let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol described in Example 3 and recall that $\mathbf{e}_p(ac) = \varphi_a(c)$ is a nontrivial additive character if $\gcd(a,p) = 1$.

Note that the quantity $\left(\left(\frac{c}{p}\right)+1\right) \in \{0,1,2\}$ counts the number of solutions to $x^2 \equiv c \pmod p$, for every fixed $c \in \mathbb{F}_p$. Therefore, we have

$$\sum_{x=0}^{p-1}\mathbf{e}_p(ax^2) = \sum_{c\in\mathbb{F}_p}\varphi_a(c)\left(\left(\tfrac{c}{p}\right)+1\right) = G\big(\varphi,\left(\tfrac{\cdot}{p}\right)\big) + \sum_{c\in\mathbb{F}_p}\varphi_a(c) = G\big(\varphi_a,\left(\tfrac{\cdot}{p}\right)\big),$$

since from Equation (2) it follows that $\sum_{c\in\mathbb{F}_p}\varphi_a(c) = 0$ as long as $\gcd(a,p) = 1$. The result follows now from Theorem 3.1. □

3.2 Jacobi sums

For two given multiplicative characters χ, ψ in $\mathbb{F}_q$, the *Jacobi sum* associated to ψ and χ is given by

$$J(\psi,\chi) = \sum_{c\in\mathbb{F}_q}\chi(c)\psi(1-c) = \sum_{x+y=1}\chi(x)\psi(y).$$

These sums turn out, rather surprisingly, to be expressible in terms of general Gauss sums.

Theorem 3.3. *Let χ and ψ be two non-trivial multiplicative characters in $\mathbb{F}_q$ wich that $\chi\cdot\psi$ is also non-trivial. For any non-trivial additive character φ in $\mathbb{F}_q$, we have*

$$J(\chi,\psi) = \frac{G(\varphi,\chi)G(\varphi,\psi)}{G(\varphi,\chi\psi)}.$$

Proof. Observe that the denominator $G(\varphi, \chi\psi) \neq 0$ by hypothesis. Therefore, we have

$$J(\chi,\psi)G(\varphi,\chi\psi) = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q^\times} \chi(x)\psi(1-x)\chi(y)\psi(y)\varphi(y).$$

Recall that we have extended the multiplicative characters to $\mathbb{F}_q$ by imposing that $\chi(0) = \psi(0) = 0$ (since both are non-trivial), thus we may restrict the sum to $x \neq \{0,1\}$. Then we can define $u = xy$ and $v = y - xy$ and we obtain a bijective change of variable from $(x,y) \in \big(\mathbb{F}_q \setminus \{0,1\}\big) \times \mathbb{F}_q^\times$ to

$$\{(u,v) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times : u + v \neq 0\}.$$

since we can recover x and y by $y = u + v, x = u/(u+v)$. We derive

$$\begin{aligned} J(\chi,\psi)G(\varphi,\chi\psi) &= \sum_{\substack{u,v\in\mathbb{F}_q^\times\\ u+v\neq 0}} \chi(u)\psi(v)\varphi(u+v) \\ &= G(\varphi,\chi)G(\varphi,\psi) - \sum_{u\in\mathbb{F}_q^\times} \chi(u)\psi(-u) \\ &= G(\varphi,\chi)G(\varphi,\psi) - \psi(-1)\sum_{u\in\mathbb{F}_q^\times} \chi\psi(u) \\ &= G(\varphi,\chi)G(\varphi,\psi), \end{aligned}$$

since $\chi\cdot\psi$ is non-trivial. □

Corollary 3.4. *Let χ and ψ be two non-trivial multiplicative characters in $\mathbb{F}_q$ wich that $\chi\cdot\psi$ is also non-trivial. Then,*

$$|J(\chi,\psi)| = q^{1/2}.$$

Proof. It follows from Theorem 3.1 that for any non-trivial φ, χ additive and multiplicative characters $|G(\varphi,\chi)| = q^{1/2}$, thus the result follows from Theorem 3.3. □

3.3 Kloosterman sums

Let $n \geq 1$ be an integer, $a, b \in \mathbb{Z}$. We define the *Kloosterman sum* $K(a,b:n)$ as follows

$$K(a,b:n) = \sum_{x\in\mathbb{Z}_n^\times} \mathbf{e}\left(\frac{ax+bx^*}{n}\right), \tag{11}$$

where x^* denotes the residue class of the inverse of x modulo n. Observe that, whenever n is a prime the previous sum can be expressed in terms of additive characters in $\mathbb{F}_p$:

$$K(a,b;p) = \sum_{c\in\mathbb{F}_p^\times} \varphi_a(c)\varphi_b(c^{-1}).$$

In this case, we will consider a generalization of the Kloosterman sums defined in (11) for a finite field $\mathbb{F}_q$. Let φ, ψ be two additive characters of $\mathbb{F}_q$, the associated *Kloosterman sum* $K(\varphi,\psi)$ is defined by

$$K(\varphi,\psi) = \sum_{c\in\mathbb{F}_q^\times} \varphi(c)\psi(c^{-1}). \tag{12}$$

Remark 6. *We note that $K(\varphi,\psi)$ is always a real number, since*

$$\overline{K(\varphi,\psi)} = \sum_{c\in\mathbb{F}_q^\times} \overline{\varphi(c)\psi(c^{-1})} = \sum_{c\in\mathbb{F}_q^\times} \varphi(-c)\psi(-c^{-1}) = \sum_{d\in\mathbb{F}_q^\times} \varphi(d)\psi(d^{-1}) = K(\varphi,\psi),$$

by using the change of variable $d = -c$.

Remark 7. *For every $b \in \mathbb{F}_q^\times$ we have that $K(\varphi,\psi) = K(\varphi_b, \psi_{b^{-1}})$, where $\varphi_b(x) = \varphi(bx)$ and $\psi_{b^{-1}}(x) = \psi(b^{-1}x)$.*

Theorem 3.5 (Kloosterman)**.** *Let φ, ψ be two nontrivial additive characters in $\mathbb{F}_p$. Then*

$$|K(\varphi,\psi)| < 2p^{3/4}.$$

The idea of the proof to this result is to try to understand Kloosterman sums globally, and not individually. More preciselly, the idea is to use the following fact: if we can prove an average bound for the $k-$th moments

$$M_k = \sum_{\varphi, psi \neq \varphi_0} |K(\varphi,\psi)|^{2k} \leq M$$

for some $k \geq 1$ and $M \geq 0$, then for any pair φ, ψ we can deduce from Remark 7 that

$$(q-1)|K(\varphi,\psi)|^{2k} = \sum_{b \in \mathbb{F}_q^\times} |K(\varphi_b, \psi_{b^{-1}})|^{2k} \leq M,$$

and hence

$$|K(\varphi,\psi)| \leq \left(\frac{M}{q-1}\right)^{1/2k} \tag{13}$$

for every fixed φ, ψ.

Now, for any $k \geq 1$ we have

$$M_k = \sum_{\varphi,\psi} |K(\varphi,\psi)|^{2k} - 2\sum_{\varphi \neq \varphi_0} |K(\varphi,\varphi_0)|^{2k} - |K(\varphi_0,\varphi_0)|^{2k}$$

and clearly $\varphi \neq \varphi_0$ implies that $K(\varphi,\varphi_0) = -1$ by Corollary 2.1. Thus

$$M_k = \sum_{\varphi,\psi} |K(\varphi,\psi)|^{2k} - 2(q-1) - (q-1)^{2k}.$$

In order to prove Theorem 3.5 we will need the following auxiliary result.

Proposition 3.6. *The first normalised moments for Kloosterman sums are*

$$\frac{M_0}{(q-1)^2} = 1, \quad \frac{M_1}{(q-1)^2} = \frac{q^2-q-1}{q-1} \quad \textit{and} \quad \frac{M_2}{(q-1)^2} = \frac{2q^3-3q^2-3q-1}{(q-1)}.$$

Proof. The equality for M_0 is trivial, so let us start with M_1. Once again, it follows from (9) that

$$\begin{aligned} M_1 &= \sum_{\varphi,\psi} \sum_{c,d \in \mathbb{F}_q^\times} \varphi(c-d)\psi(c^{-1}-d^{-1}) - 2(q-1) - (q-1)^2 \\ &= \sum_{c,d \neq 0} \Big(\sum_{\varphi} \varphi(c-d)\Big)\Big(\sum_{\psi} \psi(c^{-1}-d^{-1})\Big) - 2(q-1) - (q-1)^2 \\ &= q^2(q-1) - 2(q-1) - (q-1)^2 = (q-1)\big(q^2-q-1\big) \end{aligned}$$

since

$$\Big(\sum_{\varphi} \varphi(c-d)\Big)\Big(\sum_{\psi} \psi(c^{-1}-d^{-1})\Big) = \begin{cases} q^2 & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases}$$

Now let us show the formula for M_2. Note that

$$\begin{aligned} M_2 &= \sum_{\varphi,\psi} \sum_{a,b,c,d, \in \mathbb{F}_q^\times} \varphi(a+c-b-d)\psi(a^{-1}+c^{-1}-b^{-1}-d^{-1}) - 2(q-1) - (q-1)^4 \\ &= \sum_{a,b,c,d, \in \mathbb{F}_q^\times} \Big(\sum_{\varphi} \varphi(a+c-b-d)\Big)\Big(\sum_{\psi} \psi(a^{-1}+c^{-1}-b^{-1}-d^{-1})\Big) - 2(q-1) - (q-1)^4. \end{aligned}$$

Once again, by orthogonality of the characters, we have that the product of sums

$$\Big(\sum_{\varphi}\varphi(a+c-b-d)\Big)\Big(\sum_{\psi}\psi(a^{-1}+c^{-1}-b^{-1}-d^{-1})\Big)$$

is q^2 if $a,b,c,d\in\mathbb{F}_q^\times$ satisfy

$$\begin{cases} a+c=b+d \\ \frac{1}{a}+\frac{1}{c}=\frac{1}{b}+\frac{1}{d}\end{cases} \tag{14}$$

and zero otherwise. Let us now count the number of solutions in (14):

1. Clearly, if $\{c,d\}=\{a,b\}$ the quadruple (a,b,c,d) satisfies (14). There are exactly $2(q-1)^2-(q-1)$ of such quadruples.
2. If $a=-c$, then $a+c=b+d=0$ and we have $(q-1)^2$ of these pairs:
$$(x,y,-x,-y)\quad x,y\in\mathbb{F}_q^\times$$
but $2(q-1)$ of them were counted in the previous case (those of the form $(x,x,-x-x)$ and $(x,-x,-x,x)$ for some $x\in\mathbb{F}_q^\times$). Thus, we must add $(q-1)^2-2(q-1)$ to the final count.
3. Suppose that (a,b,c,d) is a solution not counted before: $a+c\neq 0$ and $\{a,b\}\neq\{c,d\}$. Then it follows from (14) that
$$\begin{gathered} a+c=b+d,\\ bd(a+c)=ac(b+d).\end{gathered}$$
Eliminating a we are left with
$$bd(b+d)=c(b+d-c)(b+d)$$
whence $bd=c(b+d-c)$. This implies $b(d-c)=c(d-c)$, which contradicts the fact that $c\neq b,d$ by assumption.

Thus, the total number of pairs satisfying (14) is $3(q-1)^2-3(q-1)$. Therefore,

$$M_2=(q-1)\big(3q^2(q-2)-2-(q-1)^3\big)=(q-1)\big(2q^3-3q^2-3q-1\big).$$

□

Proof of Theorem 3.5 It follows from (13) and Proposition 3.6 that

$$\big|K(\varphi,\psi)\big|\le\big((q-1)M_2\big)^{1/4}=\big(2q^3-(3q^2+3q+1)\big)^{1/4}<2q^{3/4}$$

for any pair of non-trivial characters φ,ψ. □

The best known bound, which we will not prove, is due to Weil and was obtained by means of algebraic geometry arguments.

Theorem 3.7 (Weil)**.** *Let p be a prime number and a,b integers coprime with p. Then we have the upper bound*

$$|K(\varphi,\psi)|\le 2\sqrt{q}.$$

This result is in some sense best possible, as the following result shows.

Corollary 3.8. *For at least one pair of non-trivial additive characters φ,ψ, we have*

$$|K(\varphi,\psi)|>\sqrt{2q-2}.$$

Proof. Observe that by definition of the quantities M_1,M_2 it follows that

$$M_2\le\big(\max_{\varphi,\psi\neq\varphi_0}|K(\varphi,\psi)|^2\big)M_1,$$

and therefore there exists a pair of non-trivial characters φ,ψ for which

$$|K(\varphi,\psi)|^2\ge\frac{M_2}{M_1}=\frac{2q^3-3q^2-3q-1}{q^2-q-1}>2q-2,$$

from Proposition 3.6. □

4 Pólya-Vinogradov bound

The following result, which dates back to 1918, is another example of an incomplete sum: the multiplicative analogue of Proposition 2.3 or the incomplete version of the original Gauss sum $G(\varphi_0, \chi_{p-1/2})$.

Theorem 4.1 (Polya-Vinogradov)**.** *For any integer N, $1 \leq N \leq p-1$ and any non-trivial multiplicative character χ*

$$\sum_{x=1}^{N} \chi(x) = O\left(p^{1/2} \log p\right).$$

Proof. For a given $a \in \mathbb{F}_p$ let us denote by $S(a)$ the following Gaussian sum

$$S(a) = G(\varphi_a, \chi) = \sum_{c=1}^{p-1} \varphi_a(c)\chi(c).$$

It follows from Theorem 3.1 that $|S(a)| = p^{1/2}$ if $a \neq 0$ and from the orthogonality of the characters that $S(0) = 0$.

Now, from Corollary 2.1 we have that

$$\begin{aligned}
\left|\sum_{c=1}^{N} \chi(c)\right| &= \left|\sum_{c=1}^{p-1} \chi(c)\left[\frac{1}{p}\sum_{a\in\mathbb{F}_p}\sum_{d=1}^{N} \varphi_a(x-y)\right]\right| \\
&= \frac{1}{p}\left|\sum_{a\in\mathbb{F}_p} S(a)\sum_{d=1}^{N} \varphi_a(-y)\right| \\
&\leq \frac{1}{p}\sum_{a\in\mathbb{F}_p} |S(a)|\left|\sum_{d=1}^{N} \varphi_a(-y)\right| \\
&= \frac{p^{1/2}}{p}\sum_{a\in\mathbb{F}_p}\left|\sum_{d=1}^{N} \varphi_a(-y)\right| = O\big(p^{1/2}\log p\big)
\end{aligned}$$

since by Proposition 2.3

$$\sum_{a\in\mathbb{F}_p}\left|\sum_{d=1}^{N} \varphi_a(-y)\right| = \sum_{b\in\mathbb{F}_p}\left|\sum_{d=1}^{N} \varphi_b(y)\right| = O(p\log p)$$

by making the change of variable $a = -b$. □

A direct application of this result is the following (which has already been obtained in the Tutorial 8 by means of additive characters).

Corollary 4.2. *For $1 \leq N \leq p-1$ the interval $[1, N]$ contains $N/2 + O(p^{1/2}\log p)$ quadratic residues.*

Proof. The number of quadratic residues in $[1, N]$ is given by

$$I(N, x^2) = \frac{1}{2}\sum_{x=1}^{N}\left(1 + \left(\frac{x}{p}\right)\right) = \frac{N}{2} + \sum_{x=1}^{N}\left(\frac{x}{p}\right) = \frac{N}{2} + O(p^{1/2}\log p).$$

□

In particular, this implies that if N_0 denotes the smallest quadratic non-residue in $[1, p-1]$, then

$$N_0 = O\big(p^{1/2}\log p\big), \tag{15}$$

since by definition of N_0 we have that $I(N_0, x^2) = N_0 - 1$. Thus

$$N_0 = 1 + I(N_0, x^2) = 1 + \frac{N_0}{2} + O\big(p^{1/2}\log p\big).$$

5 Weil bound for character sums

5.1 Weil bound for additive character sums

Let φ be a nontrivial additive character of $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[x]$ be a polynomial of positive degree. We consider the sums of the form

$$\sum_{c\in\mathbb{F}_q} \varphi(f(c)),$$

which sometimes are referred to as Weil sums.

Remark 8. *Observe that if $f(x) = ax + b$, then the sums can be easily estimated from the orthogonality relations. Also, if f is a quadratic polynomial these sums can be written in terms of Gaussian sums by simply completing squares in $\mathbb{F}_q$.*

For a general polynomial, André Weil proved by means of deep results in algebraic geometry the following result.

Theorem 5.1. *Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $d \geq 1$ with $\gcd(d, q) = 1$ and let ψ be a non-trivial additive character of $\mathbb{F}_q$. Then*

$$\left| \sum_{x\in\mathbb{F}_q} \psi(f(x)) \right| \leq (d-1)q^{1/2}.$$

5.2 Weil bound for multiplicative character sums

The same bound can be obtained for multiplicative characters.

Theorem 5.2. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_q$ of order m and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree $d \geq 1$ which is not an mth power of a polynomial. Then, for every $a \in \mathbb{F}_q$*

$$\left| \sum_{x\in\mathbb{F}_q} \chi(f(x)) \right| \leq (d-1)q^{1/2}.$$

We can use Weil's result to prove the following bound, which was presented when discussing about Equations in finite fields.

Corollary 5.3. *Let $m \in \mathbb{N}$ and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree $d \geq 1$ such that $y^t - f(x)$ is absolutely irreducible where $t = \gcd(m, q-1)$. Then the number N of solutions to $y^m = f(x)$ in $\mathbb{F}_q$ is*

$$|N - q| \leq (t-1)(d-1)q^{1/2}.$$

Proof. Observe that for any given m and a given multiplicative character ψ

$$\sum_{y\in\mathbb{F}_q} \psi(y^m) = \sum_{y\in\mathbb{F}_q} \psi^m(y) = \begin{cases} q & \text{if } \psi^m = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

and $\psi^m = \chi_0$ if and only if the order of ψ divides m. In fact, if $t = \gcd(m, q-1)$ and χ is a multiplicative character of order t, then the only multiplicative characters of order dividing m are

$$\chi, \chi^2, \ldots, \chi^{t-1}, \chi^t = \chi_0.$$

Thus,

$$N = \frac{1}{q} \sum_{\psi} \sum_{x\in\mathbb{F}_q} \psi(f(x)) = \sum_{j=0}^{t-1} \sum_{x\in\mathbb{F}_q} \chi^j(f(x)).$$

Therefore, separating the contribution from $j = 0$ from the rest and applying Theorem 5.2 we have that

$$|N - q| \leq \sum_{j=1}^{t-1} \Big| \sum_{x\in\mathbb{F}_q} \chi^j(f(x) \Big| \leq (t-1)(d-1)q^{1/2}.$$

□