Trigonometric Sums

Andrew Gordon

1 Notation

- This paper be concerned, almost exclusively, with algebraic geometry over finite fields. To that end, q will be a prime power p^n, $\mathbb{F}_q$ the finite field with q elements, and $\mathbb{F}$ an algebraic closure.
- If Y_0 is a scheme, sheaf or other object defined over $\mathbb{F}_q$, dropping the 0 subscript and writing Y will denote the object over $\mathbb{F}$ coming from Y_0 by extending scalars.
- For Y_0 a scheme over $\mathbb{F}_q$, $F : Y_0 \to Y_0$ is the Frobenius morphism which acts as the identity on the underlying topological space of Y_0 and acts by raising to the qth power on the structure sheaf of Y_0.

  We will also use F to denote the extension by scalars to a morphism on Y. Acting on Y, F is not the identity on the inderlying topological space, and in fact $Y^F = Y(\mathbb{F}_q)$
- ℓ is a prime distinct from p, and E_λ is a finite extension of the field $\mathbb{Q}_\ell$. The etale cohomology groups we will encounter will be E_λ vector spaces, not complex ones, and we will frequently, but often not explicitly, use an embedding $E_\lambda \hookrightarrow \mathbb{C}$ to make sense of statements of the form

  "The eigenvalues of F^* acting on $H^i(X, \mathcal{F})$ have absolute value $q^{i/2}$"
- For $\mathcal{A}^\bullet$ a graded vector space and T an endomorphism we abbreviate

$$\mathrm{Tr}(T, \mathcal{A}^*) = \sum_i (-1)^i \,\mathrm{Tr}(T, \mathcal{A}^i)$$

  This will always be used in the context of Y a scheme over $\mathbb{F}$, $\mathcal{F}$ a sheaf of E_Λ vector spaces on Y to abbreviate the sum

$$\mathrm{Tr}(T^*, H^*(Y, \mathcal{F})) = \sum_i (-1)^i \,\mathrm{Tr}(T^*, H^i(Y, \mathcal{F})$$

  In the above we mean the cohomology of $\mathcal{F}$ computed on the etale site of Y, though we will make use of the same notation for the compactly supported cohomology as well, when we write H_c^*

2 Introduction

The notion of a trigonometric sum does not have, or need, a precise definition, but it would do at the outset to give a general idea of what we will be considering in this paper. As a preliminary example, and one we will explore in detail, let f be a polynomial in $\mathbb{F}_p[x]$. Consider what can be said about value of

$$\sum_{n=1}^{p} e^{2\pi i f(n)/p}$$

Note first that this is well defined even though f does not properly take values in $\mathbb{C}$ because for an integer y, $e^{2\pi i y/p}$ depends only on the residue class of y mod p.

Naively, this sum must have absolute value less that p, since it is a sum of p terms of magnitude 1. However we would hope for the sum to be a great deal smaller. If, for example $f(x) = x$, then the above sum would be zero. We shall see what can be said for a general class of f.

The central trick will be two related results which shall not be proven here but can be found (along with most of the other material in this paper) in [1].

Theorem 1. *Lefschetz Trace Formula For X_0 a separated scheme of finite type over* $\mathrm{Spec}(\mathbb{F}_q)$*, and $\mathcal{F}_0$ a sheaf of E_λ vector spaces. Then*

$$\sum_{x \in X^F} \mathrm{Tr}(F_x^*, \mathcal{F}) = \mathrm{Tr}(F^*, H_c^*(X, \mathcal{F}))$$

We will use this by finding a scheme X_0 and a sheaf $\mathcal{F}$ such that the left hand side of this equation is out 'trigonometric sum'. Then, to bound it we use the following result

Theorem 2. *Riemann Hypothesis For X_0 an affine smooth scheme over $\mathbb{F}_q$ of pure dimension n and $\mathcal{F}_0$ a pure of weight* m[1] *sheaf on X_0, the eigenvalues of F^* acting on $H_c^i(X, \mathcal{F}$ are algebraic integers all of whose complex conjugates have magnitude less than or equal to* $q^{n+m/2}$

So we can achieve bounds on the trigonometic sums by finding $\dim H_c^i(X, \mathcal{F})$. These numbers are very hard to come by in general, but in certain cases are accessible to us.

3 Constructing the correct sheaf

3.1 Torsors

For A an group and X a scheme, an A-torsor on X is a sheaf T on X with a right action of A such that T is etale locally isomorphic (as sheaves with an A action) to the constant sheaf $\underline{A}$.

[1] This is a requirement on the eignevalues of F on the stalks of $\mathcal{F}$, which the sheaves we will consider will satisfy

One concrete way of presenting a torsor on X is giving an etale cover $\{U_i \to X\}_i$ and identifications $T_{U_i} \simeq \underline{A}$. Then we need transition data. The endomorphisms of A as a right A-set (not as a group) are exactly right multiplipication by elements of A. So our transition data is a collection of elements of A satisfying cocycle conditions.

This makes it clear that if $\phi : A \to B$ is a homomorphism of groups, and T an A-torsor on X we can produce a unique B torsor T' and a map $\phi : T \to T'$ such that $\phi(ta) = \phi(t)\phi(a)$. The construction is to give T' the same trivializing cover as T and apply ϕ to the transition data.

This will be used primarily in the context that $B = \mathrm{GL}(V)$ for V a finite E_λ vector space.

Given S a $\mathrm{GL}(V)$ torsor on X, there is a unique sheaf of E_λ-sheaf $\mathcal{F}$, smooth of rank $\dim(V)$, with an isomorphism $\underline{Isom}(V, \mathcal{F}) \simeq S$, by once again giving $\mathcal{F}$ the same trivializing cover as S, and reinterpreting the transition data of S as transition data of an E_λ sheaf.

Putting this together, given an A-torsor T for A an abelian group, and a character $\phi : A \to E_\Lambda^\times$, we get a rank one line bundle on X. We will call the torsor $\chi(T)$. This construction will work for any representation and possibly nonabelain A, but in the abelian-character case there is also a never zero morphism

$$\chi : T \to \chi(T)$$

satisfying

$$\chi(ta) = \chi(a)\chi(t)$$

For S a scheme and G a connected group scheme over S, we can produce an A-torsor on G from an extension of group schemes

$$0 \longrightarrow A \longrightarrow G' \xrightarrow{\pi} G \longrightarrow 0$$

The sheaf of sections of π is an A-torsor.

3.2 The Lang Torsor

For G_0 a group scheme over $\mathbb{F}_q$ we define the Lang isogeny

$$\mathcal{L}_0 : G_0 \to G_0 \quad x \mapsto Fxx^{-1}$$

This map is etale and surjective, and its kernel is $G_0(\mathbb{F}_q)$.

We define the Lang torsor L_0 as the torsor of local sections of this map.

Our computations to come rely heavily on understanding the action of F on the stalks of L at the points of $G(\mathbb{F}_q)$.

We can identify the fiber L_x with $\mathcal{L}^{-1}(x)$. If $\gamma \in G(\mathbb{F}_q)$ and $\mathcal{L}(g) = \gamma$, then $Fg = Fgg^{-1}g = \gamma g$.

So for $x \in G(\mathbb{F}_q)$ the map $F^* : L_x \to L_x$ sends $g \mapsto gx^{-1}$

Note then that if χ is a character of $G_0(\mathbb{F}_q)$, then F^* acts by multiplication by $\chi(x^{-1})$ on the fiber of $\chi(L_0)_x$

Now we can define the line bundles that will be used to determine sums.

Definition 1. *For $f_0 : X_0 \to G_0$ a morphism, and $\chi : G_0(\mathbb{F}_q) \to E_\lambda^\times$ a character, we define*

$$\mathfrak{F}(\chi, f_0) := \chi^{-1}(f_0^*(L_0)) = f_0^*\chi^{-1}(L_0))$$

For $x \in X_0(\mathbb{F}_q)$, $f_0^*(L_0)_x = (L_0)_{f_0(x)}$, so the trace of F^* on $\mathfrak{L}(\chi, f_0)_x$ is $\chi^{-1}(f_0(x)^{-1}) = \chi(f_0(x))$

Then we can begin to study the sums in question via the equality

$$\sum_{x \in X_0(\mathbb{F}_q)} \chi(f_0(x)) = \sum_{x \in X_0(\mathbb{F}_q)} \mathrm{Tr}(F_*, \mathfrak{F}(\chi, f_0)_x) = Tr(F^* H_c^*(X, \mathfrak{F}(\chi, f_0))$$

Choose some integer $n > 1$ and for a group scheme G_0 defined over $\mathrm{Spec}(\mathbb{F}_q)$ denote by G_1 the extension to $\mathrm{Spec}\,\mathbb{F}_{q^n}$.

On G_1 we have L_1, the extension by scalars of the Lang torsor L_0 on G_0, which is a $G_1(\mathbb{F}_q) = G_0(\mathbb{F}_q)$ torsor. This is the torsor defined by the map $\mathcal{L} : G_1 \to G_1$ taking $g \mapsto Fgg^{-1}$.

But we can also define a map $\mathcal{L}^{(n)} : G_1 \to G_1$ that takes $g \mapsto F^n g$. The torsor of local sections of $\mathcal{L}^n$ is a $G_1(\mathbb{F}_{q^n})$ torsor, which we will denote $L_1^{(n)}$

We have a map $N : G_1 \to G_1$ that sends g to $\prod_{i=0}^{n-1} F^i(g)$. This induces a group homomorphism $N : G_1(\mathbb{F}_{q^n}) \to G_1(\mathbb{F}_q)$ which as we've seen allows us to produce a $G_1(\mathbb{F}_q)$ torsor from a $G_1(\mathbb{F}_{q^n})$ torsor. The following theorem says however that this construction gives us nothing new

Theorem 3. *L_1 and $N(L_1^{(n)})$ are isomorphic*

Proof. Note first that $\mathcal{L}^{(n)} = \mathcal{L} \circ N$, and that for $g \in G_1(\mathbb{F}_q^n)$, $Ng = \prod_{i=0}^{n-1} F^i(g)$, so we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G_1(\mathbb{F}_{q^n}) & \longrightarrow & G_1 & \xrightarrow{\mathcal{L}^{(n)}} & G_1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle id} & & \\
0 & \longrightarrow & G_1(\mathbb{F}_q) & \longrightarrow & G_1 & \xrightarrow{\mathcal{L}} & G_1 & \longrightarrow & 0
\end{array}$$

Thus on any open set the set of sections of $\mathcal{L}$ is the same as N applied to the set of sections of $\mathcal{L}^{(n)}$, proving the result. $\square$

As an important corollary, for a map $f_0 : X_0 \to G_0$, and χ a character of $G_0(\mathbb{F}_q)$, the base change of $(F)(\chi, f_0)$ to the scheme $(X_0)_{\mathbb{F}_{q^n}}$ is isomorphic to the line bundle $\mathfrak{F}(\chi \circ N, (f_0)_{\mathbb{F}_{q^n}})$.

4 Trigonometric Sums

4.1 Note on cohomological computations

The crux of nearly every argument to come will be the computation of certain etale cohomology groups. Full proofs of these computations are too lengthy for a note of this size, so they will be reproduced here only as facts, with a sketch of an argument when that can be done in a succinct and enlightening manner. Full arguments can be found in [**?**], and when citing a fact I will endeavor to list its exact location.

In the examples below we will be computing $H^i_c(C, \mathcal{F})$ for C a smooth conntected affine curve. Our general result will always be that, with some hypotheses on $\mathcal{F}$, these groups will be 0 for $i \neq 1$ and the rank of $H^i_c(C, \mathcal{F})$ can be computed directly via formula.

If $C \hookrightarrow \overline{C}$ is a compactification with $\overline{C}$ a smooth projective curve of genus g. We define the euler characteristic $\chi(C) = 2 - 2g - \#S$ where $S := \overline{X} - X$[2]. It is possibly familiar that

$$\chi(C) = \sum_i (-1)^i \dim(H^i_c(C, E_\Lambda))$$

This fact generalizes. For $\mathcal{F}$ an E_λ sheaf on C we also define

$$\chi(\mathcal{F}) = \sum_i (-1)^i \dim(H^i_c(C, \mathcal{F}))$$

Fact 1.

$$\chi(\mathcal{F}) = \mathrm{Rk}(\mathcal{F})\chi(C) - \sum_{s \in S} Sw_s(\mathcal{F})$$

where $Sw_s(\mathcal{F})$ is the Swan conductor of $\mathcal{F}$, a measure of wild ramification.

Since[3] $H^i_c(C, \mathcal{F}) = 0$ for i out of the range $[0, 2]$, all that remains is the computation of the 0th and 2nd cohomology groups.

$H^0_c(C, \mathcal{F})$ is the group of sections of $\mathcal{F}$ with compact support, which can easily be seen to be 0 when C is noncomplete.

Fact 2. *Poincare Duality, Sommes Trigonométriques 1.18c: For $\mathcal{F}$ smooth, the vector spaces $H^i_c(C, \mathcal{F}$ and $H^{2-i}(C, \mathcal{F}^\vee)$ are dual, up to a twist*

Fact 3. *For $\mathcal{F} = \mathfrak{F}(\psi, f)$ for $f : C \to G$ nonconstant and ψ a nontrivial character of $G(\mathbb{F}_q)$, $H^i_c(C\mathcal{F}) \simeq H^i(C, \mathcal{F})$*

The above two facts let us conclude that $H^2_c(C, \mathcal{F})$ is 0 if $H^0_c(C, \mathcal{F})$ is, so the rank of $H^1_c(C, \mathcal{F})$ is determined by the euler characteristic.

[2]Note by my lack of subscript the assumption that the field of definition of C is algebraically closed
[3]another fact

4.2 Gauss Sums

For $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ characters we define the gauss sum

$$\tau(\chi, \psi) = -\sum_{x \in \mathbb{F}_q^*} \psi(x)\chi^{-1}(x)$$

We can get characters of $\mathbb{F}_{q^n}^\times$ and $\mathbb{F}_{q^n}$ by precomposing χ or ψ with the norm map and trace map to $\mathbb{F}_q$, respectively. Note that this is exactly the homomorphism $N : \mathbb{G}_m \times \mathbb{G}_a(\mathbb{F}_{q^n}) \to \mathbb{G}_m \times \mathbb{G}_a(\mathbb{F}_q)$

As a first application

Theorem 4. *Hasse-Davenport, 1935*

$$\tau(\chi \circ Nm, \psi \circ Tr) = \tau(\chi, \psi)^n$$

Proof. To prove this, We use the following result

Fact 4. *Sommes Trigonométriques 4.2 For $\iota : \mathbb{G}_m \to \mathbb{G}_m \times \mathbb{G}_a$ the diagonal embedding, $H_c^i(\mathbb{G}_m, \mathfrak{F}(\chi^{-1}\psi, \iota))$ is a one dimensional vector space when $i = 1$, and 0 otherwise, for chi and ψ not both trivial.*

Hasse and Davenport were working with complex characters, but since the values of χ and ψ are algebraic, we can assume they are contained in some number field E, and prove the equality in the completion E_λ at some place of E of characteristic ℓ.

Assuming the fact, then

$$\tau(\chi, \psi) = -\sum_{x \in \mathbb{F}_q^*} \psi(x)\chi^{-1}(x) = -\sum_{x \in \mathbb{G}_m(\mathbb{F}_q)} \mathrm{Tr}(F^*, \mathfrak{F}(\chi^{-1}\psi, \iota)_x) = \mathrm{Tr}\left(F^*, H_c^1(\mathbb{G}_m, \mathfrak{F}(\chi^{-1}\psi, \iota)\right)$$

We denote the eigenvalue of the action of F^* on the one diemnsional space $H_c^1(\mathbb{G}_m, \mathfrak{F}(\chi^{-1}\psi, \iota)$ as γ.

But then, using the last results of the previous section

$$\tau(\chi \circ Nm, \psi \circ Tr) = -\sum_{x \in \mathbb{G}_m(\mathbb{F}_q^n)} \mathrm{Tr}((F^*)^n, \mathfrak{F}((\chi^{-1}\psi) \circ N, \iota)_x) = \mathrm{Tr}\left((F^*)^n, H_c^1(\mathbb{G}_m, \mathfrak{F}(\chi^{-1}\psi, \iota)\right) = \gamma^n$$

To prove the fact, we use the arguement outlined in the preceding section. All that remains is the computation of

$$\mathrm{Rk}(\mathcal{F})\chi(C) - \sum_{s \in S} Sw_s(\mathcal{F})$$

$\mathfrak{F}(\chi^{-1}\psi), \iota)$ is unramified away from 0 and ∞. Its swan conductor at 0 is 0, and at ∞ it is 1. So the euler characteristic is

$$(1)(2) - 0 - 1 = 1$$

□

When χ is nontrivial Poincare Duality for etale sheaves gives a perfect pairing $H^1_c(\mathbb{G}_m, \mathfrak{F}(\chi^{-1}\psi, \iota))$ and $H^1_c(\mathbb{G}, \mathfrak{F}(\chi\psi^{-1}))$, valued in the tate twist $E_\lambda(-1)$. We know that F^* acts on $E_\lambda(-1)$ by multiplication by q, so considering F^* equivariance of the pairing

$$H^1_c(\mathbb{G}_m, \mathfrak{F}(\chi^{-1}\psi, \iota)) \times H^1_c(\mathbb{G}, \mathfrak{F}(\chi\psi^{-1})) \to E_\lambda(-1)$$

we discover a new proof of the statement that $|\tau(\chi, \psi)| = q$

5 Single variable sums

For a character $\psi : \mathbb{F}_q \to E_\lambda$, and X_0 a smooth connected curve and f_0 a morphism $X_0 \to \mathbb{P}^1$, i.e. a rational function on X_0, we can consider the sum

$$S'_f = \sum_{x \in X_0(\mathbb{F}_q), f_0(x \neq \infty} \psi(f_0(x))$$

Note that $S'_f = 0$ if $f = g^q - g$ for some rational function g, and that S'_f is unchanged if we add a function of the form $g^q - g$ to f.

For every point where it is defined, $\psi(f_0(x)) = \psi(f(x) + g^p(x) - g(x))$. We define $v_x(f)$ to be the order of the pole of f at x (so zero for $f(x) \neq \infty$) and then $v^*_x(f) = \inf_g v(f + g^q - g)$. Then we can modify our sum S'_f to

$$S_f = \sum_{x \in X_0(\mathbb{F}_q), v^*_x(f) \neq 0} \psi(f(x))$$

Here, $\psi(f(x))$ is shorthhand for $\psi(f(x) + g^p(x) - g(x))$ for *some* g that makes this value make sense. Our goal then will be to prove the following

Theorem 5. *Let ψ be a nontrivial character, and f a rational function not of the form $g^p - g + C$ for g a rational function and C a constant*

$$|S_f| \leq \left(2 - 2g + \sum_{v^*_x(f) \neq 0} [k(x) : \mathbb{F}_q](1 + v^*_x(f)) \right) q^{1/2}$$

Proof. The reason for expanding the sum is that S_f is related to a nice sheaf. If $j : U \hookrightarrow \overline{X}$ is the inclusion of the open set where $f \neq \infty$ then

$$S_f = \sum_{x \in \overline{X_0}(\mathbb{F}_q)} \mathrm{Tr}(F^*, j_* \mathfrak{F}(\psi, f)_x) = Tr(F^*, H^*(X, j_* \mathfrak{F}(\psi, f))$$

If $v_x(f) = 0$, then it is clear that $\mathrm{Tr}(F^*, j_* \mathfrak{F}(\psi, f)_x) = \psi(f(x))$.

Suppose $v_x(f) \neq 0$ but $v^*_x(f) = 0$. Let g be such that $f + g^p - g$ has no pole at x. Then, on the open subset $k : V \hookrightarrow U$ where f and g are both regular, the torsor $(f + g^p - g)^* L$

is equal to the sum (in $H^1(\mathbb{F}_q, \mathrm{Aut}(X))$) of the torsors f^*L and $(g^p - g)^*L$, but the latter torsor is trivial. Therefore (ψ, f) and $(\psi, f + g^p - g)$ are isomorphic on V. Then

$$j_*(F)(\psi, f) \simeq j_* k_*(F)(\psi, f + g^p - g)$$

so it is clear that for $v_x^*(f) = 0$, $\mathrm{Tr}(F^*, j_*\mathfrak{F}(\psi, f)_x) = \psi(f(x))$. Finally, it turns out to be the case that if $v_x^*(f) \neq 0$ then $j_*\mathfrak{F}(\psi, f)_x = 0$, though the proof involves ramification theory and will not be given here. See [2] for more details.

Once again we observe, or take on faith, that the groups $H^i(X, j_*\mathfrak{F}(\psi, f))$ are 0 unless $i = 1$

Then the sum S_f is the trace of F^* on the vector space $H^1(X, j_*\mathfrak{F}(\psi, f))$. By the Riemann Hypothesis, all eigenvalues of F^* have absolute value $q^{1/2}$. In this particular case we can compute $Sw_x(f) = [k(x) : \mathbb{F}_q](1 + v_x^*(f))$ and the formula follows □

5.1 Example: Simple Kloosterman sum

As an example, consider

$$K_a(\psi) := \sum_{x \in \mathbb{F}_q^\times} \psi(x + \frac{a}{x})$$

for ψ a nontrivial character of $\mathbb{F}_q$. Then if we define $f : \mathbb{G}_m \to \mathbb{G}_a$ by sending $x \mapsto x + \frac{a}{x}$ the above sum is exactly S_f for the character ψ.

f is ramified at 0 and ∞, with swan conductor 1 in both places. So the euler characteristic is

$$2 - 2g + \sum_{v_x^*(f) \neq 0} [k(x) : \mathbb{F}_q](1 + v_x^*(f)) = -2$$

This implies $|K_a(\psi)| \leq 2\sqrt{q}$.

However, we can do even better

Fact 5. *Sommes Trigonométriques 3.6 If X has an involfution σ such that $f(\sigma(x)) = -f(x)$ then if α is an eigenvalue of F^* on $H_c^1(X, \mathfrak{F}(\psi, f)$ so is $\frac{q}{\alpha}$*

Putting this together with work in the previous sections we have

$$\sum_{x \in \mathbb{F}_{q^n}^\times} \psi(x + \frac{a}{x}) = \alpha^n + \left(\frac{q}{\alpha}\right)^n$$

for some $|\alpha| = \sqrt{q}$

References

[1] P. Deligne, "Cohomologie Etale"

[2] J. P Serre, "Sur les corps locaux à corps résiduel algébriquement clos"