ON THE NUMBER OF RATIONAL POINTS ON CURVES OVER FINITE FIELDS WITH MANY AUTOMORPHISMS

ANTONIO ROJAS-LEÓN

Abstract. Using Weil descent, we give bounds for the number of rational points on two families of curves over finite fields with a large abelian group of automorphisms: Artin-Schreier curves of the form $y^q - y = f(x)$ with $f \in \mathbb{F}_{q^r}[x]$, on which the additive group $\mathbb{F}_q$ acts, and Kummer curves of the form $y^{\frac{q-1}{e}} = f(x)$, which have an action of the multiplicative group $\mathbb{F}_q^\star$. In both cases we can remove a $\sqrt{q}$ factor from the Weil bound when q is sufficiently large.

1. Introduction

Let $k = \mathbb{F}_q$ be a finite field of characteristic p and C a geometrically connected smooth curve of genus g in $\mathbb{P}^2_k$. The well known Weil bound gives the following estimate for the number of points N_r of C rational over $\mathbb{F}_{q^r}$ for every $r \geq 1$:

$$|N_r - q^r - 1| \leq 2gq^{\frac{r}{2}}$$

This bound is sharp in general if we fix C and take variable $\mathbb{F}_{q^r}$, in the sense that

$$\limsup_{r\geq 1} \log_q |N_r - q^r - 1| = \frac{r}{2}$$

and

$$\limsup_{r\geq 1} \frac{|N_r - q^r - 1|}{q^{\frac{r}{2}}} = 2g.$$

However, for some curves it is possible to improve this bound for large values of q if we keep r under control. In the article [6] it was proven that this was the case for the affine Artin-Schreier curve A_f defined by

$$y^q - y = f(x)$$

with $f \in k[x]$, whose singular model has genus $(d-1)(q-1)/2$ and only one point at infinity. For A_f one can get an estimate of the form

$$|N_r - q^r| \leq C_{d,r} q^{\frac{r+1}{2}}$$

under certain generic conditions on f (where N_r is now the number of points on the *affine* curve A_f). In this formula $C_{d,r}$ is independent of q (more

Partially supported by P08-FQM-03894 (Junta de Andalucía), MTM2007-66929 and FEDER.

precisely, it is a polynomial in d of degree r) so it gives a great improvement of the Weil bound if q is large. This estimate was obtained by writing $N_r - q^r$ as a sum of additive character sums

$$N_r - q^r = \sum_{t\in k}\sum_{x\in k^r} \psi(\mathrm{Tr}_{k_r/k}(f(x))),$$

each of them bounded by $(d-1)q^{\frac{r}{2}}$, and then showing that there is some cancellation on the outer sum so that the total sum is bounded by $O_q(q^{\frac{r+1}{2}})$.

In this article we take a different approach: since

$$N_f = q\cdot \#\{x\in k_r | \mathrm{Tr}_{k_r/k}(f(x)) = 0\},$$

using Weil descent we construct a hypersurface in $\mathbb{A}^r_k$ whose number of rational points is precisely the number of $x\in k_r$ such that $\mathrm{Tr}_{k_r/k}(f(x)) = 0$. Under certain conditions the projective closure of this hypersurface is smooth, so we can use Deligne's bound to estimate its number of rational points and deduce the bound

$$|N_r - q^r| \leq (d-1)^r q^{\frac{r+1}{2}}. \tag{1}$$

This method is certainly less powerful than the one used in [6]. In particular, the hypotheses we need f to satisfy in order to get (1) are more restrictive than those in [6, Corollary 3.4, Corollary 4.2], and the constant $(d-1)^r$ is also slightly worse (notice that the coefficient of the leading term of $C_{d,r}$ in [6, Corollary 3.4] decreases rapidly as r grows). On the other hand, this method works even when f is defined only over k_r, not just over k, thus giving a positive answer to one of the questions posed in the introduction of [6].

We also apply the same procedure to study the other example proposed in the introduction of [6]: Kummer curves, a particular type of superelliptic curves of the form

$$E_f : y^{\frac{q-1}{e}} = f(x)$$

where e is a positive divisor of $q-1$. These curves can have genus anywhere between $\left(\frac{q-1}{e}-1\right)(d-2)/2$ and $\left(\frac{q-1}{e}-1\right)(d-1)/2$, but in any case for fixed e the Weil estimate gives

$$|N_r - q^r| = O(q^{\frac{r}{2}+1}).$$

Here we also have a large abelian group acting faithfully on E_f, namely the multiplicative group $k^\star/\mu_e$ of non-zero elements of k modulo the subgroup of e-th roots of unity, so one also expects to be able to remove a $\sqrt{q}$ factor from the bound. We can write

$$N_f = \delta + \frac{q-1}{e}\sum_{\lambda^e=1} \#\{x\in k_r | \mathrm{N}_{k_r/k}(f(x)) = \lambda\}$$

where δ is the number of roots of f in k_r. Again using Weil descent we will construct a hypersurface (or rather a one-parameter family of hypersurfaces) W_λ in $\mathbb{A}^r_k$ such that the number of rational points of W_λ over k is $\#\{x\in$

$k_r|\mathrm{N}_{k_r/k}(f(x)) = \lambda\}$. The hypersurfaces W_λ are highly singular at infinity, so this case requires a detailed study of the cohomology of this family, which takes most of the length of this article.

The descent method works surprisingly well in this case, and we get the estimate

$$|N_f - q^r - \delta + 1| \leq r(d-1)^r(q-1)q^{\frac{s-1}{2}}$$

under the only hypothesis that f is square-free of degree prime to p.

The fact that the descent method works well in the Kummer case and not so well in the Artin-Schreier case has an explanation: for Artin-Schreier curves, we can write $N_r - q^r$ as a "sum of additive character sums", parameterized by the set of non-trivial additive characters of k. Upon choosing a non-trivial character ψ, this set can be identified with the set of k-points of the scheme $\mathbb{G}_m = \mathbb{A}^1 - \{0\}$, and the corresponding exponential sums are the local Frobenius traces of the r-th Adams power of some geometrically semisimple ℓ-adic sheaf on $\mathbb{G}_m$. In order to get a good estimate (i.e., of the form $O(q^{\frac{r+1}{2}})$), we need (all components of) this Adams power to not have any invariants when regarded as representations of $\pi_1(\mathbb{G}_m)$. When doing Weil descent, what we are really looking at is the invariant space of the (Frobenius twisted) r-th tensor power of this sheaf, which is a much larger object. In particular, we may get some undesired additional invariants. In this case the monodromy group is semisimple, and therefore its determinant has some finite order N. Then its N-th tensor power is definitely going to have non-zero invariant space, which (in general) would not be present if we just considered the Adams power.

On the other hand, for the Kummer case we can write $N_r - q^r$ as a sum of multiplicative character sums, parameterized by the set of all non-trivial multiplicative characters χ of $k^\star$ of order divisible by $\frac{q-1}{e}$. Even though it is not possible to realize these sums as the Frobenius traces of an ℓ-adic sheaf on a scheme, recent work of Katz ([5], especially remark 17.7) shows that these sums are approximately distributed like traces of random elements on a compact Lie group. For generic f, this group is the unitary group U_{d-1}. In particular, all tensor powers of this "representation" (the standard $(d-1)$-dimensional representation of U_{d-1}) have zero invariant space, and this makes our method work well.

We conjecture that one should get a similar estimate for Kummer hypersurfaces of the form

$$y^{\frac{q-1}{e}} = f(x_1, \ldots, x_n)$$

where $f \in k_r[x_1, \ldots, x_n]$ is in some Zariski open set, namely one should have

$$|N_r - q^{nr}| \leq C_{n,d,e,r} q^{\frac{nr+1}{2}}$$

for some $C_{n,d,e,r}$ independent of q. However, the conditions in this case should necessarily be more restrictive, as shown by the example

$$y^{q-1} = x_1 x_2 + 1$$

in which $f(x_1, x_2) = x_1x_2 + 1$ is as smooth as it can be but it is easy to check that

$$N_r = q^{2s} + (q-2)q^r$$

for every odd q and every r.

The author would like to thank Daqing Wan for pointing out some mistakes in an earlier version of this article.

2. The Artin-Schreier case

Let $k = \mathbb{F}_q$ be a finite field of characteristic p, $k_r = \mathbb{F}_{q^r}$ the extension of k degree r inside a fixed algebraic closure $\bar{k}$, and $f \in k_r[x]$ a polynomial of degree d prime to p. Let A_f be the Artin-Schreier curve defined in $\mathbb{A}^2_{k_r}$ by the equation

$$y^q - y = f(x) \tag{2}$$

and denote by N_f its number of k_r-rational points. The group of k-rational points of the affine line $\mathbb{A}^1$ acts on $A_f(k_r)$ by $\lambda \cdot (x, y) = (x, y + \lambda)$.

By the general Artin-Schreier theory, an element $z \in k_r$ can be written as $y^q - y$ for some $y \in k_r$ if and only if $\mathrm{Tr}_{k_r/k}(z) = 0$, and in that case there are exactly q such y's. Therefore

$$N_f = q \cdot \#\{x \in k_r | \mathrm{Tr}(f(x)) = 0\}$$

where $\mathrm{Tr} = \mathrm{Tr}_{k_r/k}$ is the trace map $k_r \to k$.

Let us recall the Weil descent setup (cf. for instance [3]). Fix an basis $\mathcal{B} = \{\alpha_1, \dots, \alpha_r\} \subseteq k_r$ of k_r over k, and consider the polynomial $S(x_1, \dots, x_r) = \sum_{j=1}^r f^{\sigma^j}(\sigma^j(\alpha_1)x_1 + \cdots + \sigma^j(\alpha_r)x_r) \in k_r[x_1, \dots, x_r]$, where $\sigma \in \mathrm{Gal}(k_r/k)$ is the Frobenius automorphism and f^{σ^j} means applying σ^j to the coefficients of f. Since the coefficients of S are invariant under the action of $\mathrm{Gal}(k_r/k)$, $S \in k[x_1, \dots, x_r]$.

Let V be the subscheme of $\mathbb{A}^r_k$ defined by the polynomial S. Notice that a point $(x_1, \dots, x_r) \in k^r$ is in $V(k)$ if and only if $\sum_{j=1}^r f^{\sigma^j}(\sigma^j(\alpha_1)x_1 + \cdots + \sigma^j(\alpha_r)x_r) = \sum_{j=1}^r \sigma^j(f(\alpha_1x_1 + \cdots + \alpha_rx_r)) = 0$, if and only if $\mathrm{Tr}(f(\alpha_1x_1 + \cdots + \alpha_rx_r)) = 0$. Since $\{\alpha_1, \dots, \alpha_r\}$ is a basis of k_r over k, we conclude that

$$N_f = q \cdot \#\{x \in k_r | \mathrm{Tr}(f(x)) = 0\} = q \cdot \#V(k). \tag{3}$$

On the other hand, $V \otimes k_r$ is isomorphic, under a linear change of variable, to the hypersurface defined by $f^\sigma(x_1) + f^{\sigma^2}(x_2) + \cdots + f^{\sigma^r}(x_r) = 0$ in $\mathbb{A}^r_{k_r}$. Since d is prime to p, V has at worst isolated singularities, and its projective closure has no singularities at infinity. In particular, we get:

Theorem 2.1. *Let $f \in k_r[x]$ be a polynomial of degree d prime to p. If the hypersurface defined in $\mathbb{A}^r_k$ by $f^\sigma(x_1) + f^{\sigma^2}(x_2) + \cdots + f^{\sigma^r}(x_r) = 0$ is non-singular, the number N_f of k_r-rational points on C_f satisfies the estimate*

$$|N_f - q^r| \leq \frac{(d-1)^{r+1} - (-1)^r(d-1)}{d} q^{\frac{r+1}{2}} + \frac{(d-1)^r - (-1)^{r-1}(d-1)}{d} q^{\frac{r}{2}} \leq$$

$$\leq (d-1)^r q^{\frac{r+1}{2}}.$$

Proof. If $\bar{V}$ is the projective closure of V in $\mathbb{P}^r_k$ and $V_0 = \bar{V} - V$, we have

$$\#V(k) - q^{r-1} = \#\bar{V}(k) - \#V_0(k) - (\#\mathbb{P}^{r-1}(k) - \#\mathbb{P}^{r-2}(k)) =$$

$$= (\#\bar{V}(k) - \#\mathbb{P}^{r-1}(k)) - (\#V_0(k) - \#\mathbb{P}^{r-2}(k))$$

so

$$|N_r - q^r| = q \cdot |\#V(k) - q^{r-1}| \leq$$

$$\leq q \cdot (|\#\bar{V}(k) - \#\mathbb{P}^{r-1}(k)| + |\#V_0(k) - \#\mathbb{P}^{r-2}(k)|) \leq$$

$$\leq \frac{(d-1)^{r+1} - (-1)^r(d-1)}{d} q^{\frac{r+1}{2}} + \frac{(d-1)^r - (-1)^{r-1}(d-1)}{d} q^{\frac{r}{2}}$$

since $\bar{V}$ and V_0 are non-singular of degree d and dimension $r-1$ and $r-2$ respectively. □

As noted in [6, end of section 3], the non-singularity condition is generic in every linear space of polynomials of degree d that contains the constants: if $\lambda \in k_r$ is such that $\mathrm{Tr}_{k_r/k}(\lambda)$ is not a critical point of $f^\sigma(x_1) + \cdots + f^{\sigma^r}(x_r)$, then $f - \lambda$ satisfies the condition. The order of magnitude of the constant is polynomial in d of degree r, essentially the same as in [6]. However, the leading coefficient there decreases rapidly with r, whereas here it is always 1.

The same procedure can be applied to Artin-Schreier hypersurfaces. Let $f \in k_r[x_1, \ldots, x_n]$ be a Deligne polynomial, that is, its degree d is prime to p and its highest homogeneous form defines a non-singular projective hypersurface. Let B_f be the Artin-Schreier hypersurface defined in $\mathbb{A}^{n+1}_{k_r}$ by the equation

$$y^q - y = f(x_1, \ldots, x_n) \tag{4}$$

and denote by N_f its number of k_r-rational points. Like in the previous case, we have

$$N_f = q \cdot \#\{(x_1, \ldots, x_n) \in k_r^n | \mathrm{Tr}(f(x_1, \ldots, x_n)) = 0\}$$

where Tr is the trace map $k_r \to k$. Let $S \in k_r[\{x_{i,j} | 1 \leq i \leq n, 1 \leq j \leq r\}]$ be the polynomial

$$\sum_{j=1}^{r} f^{\sigma^j} \left(\sum_{i=1}^{r} \sigma^j(\alpha_i) x_{1,i}, \ldots, \sum_{i=1}^{r} \sigma^j(\alpha_i) x_{n,i} \right)$$

which has coefficients in k, and V the subscheme of $\mathbb{A}^{nr}_k$ defined by S. Again $N_f = q \cdot \#V(k)$, and $V \otimes k_r$ is isomorphic to the hypersurface defined by $f^\sigma(x_{1,1}, \ldots, x_{n,1}) + \cdots + f^{\sigma^r}(x_{1,r}, \ldots, x_{n,r}) = 0$. Since this hypersurface is non-singular at infinity, we get

Theorem 2.2. *Let $f \in k_r[x_1, \dots, x_n]$ be a Deligne polynomial of degree d prime to p. If the hypersurface defined in $\mathbb{A}_k^{nr}$ by $f^\sigma(x_{1,1}, \dots, x_{n,1}) + \cdots + f^{\sigma^r}(x_{1,r}, \dots, x_{n,r}) = 0$ is non-singular, the number N_f of k_r-rational points on C_f satisfies the estimate*

$$|N_r - q^{nr}| \leq \frac{(d-1)^{nr+1} - (-1)^{nr}(d-1)}{d} q^{\frac{nr+1}{2}} + \frac{(d-1)^{nr} - (-1)^{nr-1}(d-1)}{d} q^{\frac{nr}{2}} \leq$$

$$\leq (d-1)^{nr} q^{\frac{nr+1}{2}}.$$

3. The Kummer case

Fix a positive integer e which divides $q-1$. Let E_f be the Kummer curve defined in $\mathbb{A}_{k_r}^2$ by the equation

$$y^{\frac{q-1}{e}} = f(x) \tag{5}$$

and denote by N_f its number of k_r-rational points. The group $k^\star$ of k-rational points of the torus $\mathbb{G}_m$ acts on $E_f(k_r)$ by $\lambda \cdot (x, y) = (x, \lambda^e y)$.

A non-zero element $z \in k_r$ can be written as $y^{\frac{q-1}{e}}$ for some $y \in k_r$ if and only if $\mathrm{N}_{k_r/k}(z)^e = 1$, and in that case there are exactly $\frac{q-1}{e}$ such y's. Therefore

$$N_f = \#Z(k_r) + \frac{q-1}{e} \cdot \#\{x \in k_r | \mathrm{N}(f(x))^e = 1\}$$

where N is the norm map $k_r \to k$ and Z is the subscheme of $\mathbb{A}_{k_r}^1$ defined by $f = 0$.

If we apply the Weil descent method to identify the set $\{x \in k_r | \mathrm{N}(f(x))^e = 1\}$ with the set of k-rational points on a scheme over k like we did in the Artin-Schreier case we get a scheme geometrically isomorphic to the one defined by $(f^\sigma(x_1) \cdots f^{\sigma^r}(x_r))^e = 1$, which is highly singular at infinity. In particular, its higher cohomology groups do not vanish. However, these cohomology groups are relatively easy to control as we will see.

Fix an basis $\mathcal{B} = \{\alpha_1, \dots, \alpha_r\} \subseteq k_r$ of k_r over k, and consider the polynomial $T(x_1, \dots, x_r) = \prod_{j=1}^r f^{\sigma^j}(\sigma^j(\alpha_1)x_1 + \cdots + \sigma^j(\alpha_r)x_r) \in k_r[x_1, \dots, x_r]$, where $\sigma \in \mathrm{Gal}(k_r/k)$ is the Frobenius automorphism and f^{σ^j} means applying σ^j to the coefficients of f. The coefficients of T are invariant under the action of $\mathrm{Gal}(k_r/k)$, so $T \in k[x_1, \dots, x_r]$.

For any $\lambda \in k$, let W_λ be the subscheme of $\mathbb{A}_k^r$ defined by $T = \lambda$. A point $(x_1, \dots, x_r) \in k^r$ is in $W_\lambda(k)$ if and only if $\prod_{j=1}^r f^{\sigma^j}(\sigma^j(\alpha_1)x_1 + \cdots + \sigma^j(\alpha_r)x_r) = \prod_{j=1}^r \sigma^j(f(\alpha_1 x_1 + \cdots + \alpha_r x_r)) = \lambda$, if and only if $\mathrm{N}(f(\alpha_1 x_1 + \cdots + \alpha_r x_r)) = \lambda$. Since $\{\alpha_1, \dots, \alpha_r\}$ is a basis of k_r over k, we conclude that

$$N_f = \#Z(k_r) + \frac{q-1}{e} \cdot \#\{x \in k_r | \mathrm{N}(f(x))^e = 1\} = \tag{6}$$

$$= \#Z(k_r) + \frac{q-1}{e} \sum_{\lambda^e = 1} \#\{x \in k_r | \mathrm{N}(f(x)) = \lambda\} = \#Z(k_r) + \frac{q-1}{e} \sum_{\lambda^e = 1} \#W_\lambda(k).$$

Now $W_\lambda \otimes k_r$ is isomorphic, under a linear change of variables, to the hypersurface defined by $f^\sigma(x_1)f^{\sigma^2}(x_2)\cdots f^{\sigma^r}(x_r) = \lambda$. This hypersurface is highly singular at infinity, so in general we are not going to obtain good bounds for its number of rational points. For instance, in the simplest case $f(x) = x$, the hypersurface is a product of $r-1$ tori. In particular, it has non-zero cohomology with compact support in all degrees between $r-1$ and $2r-2$.

In order to understand the cohomology of these hypersurfaces, it will be convenient to consider the entire family $f^\sigma(x_1)\cdots f^{\sigma^r}(x_r) = \lambda$ parameterized by λ and study the relative cohomology sheaves. We will do this in a more general setting. Let $f_1, \ldots, f_s \in k_r[x]$ be polynomials of degree d, and let $F_s : \mathbb{A}^s_{k_r} \to \mathbb{A}^1_{k_r}$ be the map defined by $F_s(x_1, \ldots, x_s) = f_1(x_1)\cdots f_s(x_s)$. Fix a prime $\ell \neq p$ and an isomorphism $\iota : \bar{\mathbb{Q}}_\ell \to \mathbb{C}$, and let $K_s := \mathrm{R}F_{s!}\bar{\mathbb{Q}}_\ell \in \mathcal{D}^b_c(\mathbb{A}^1_{k_r}, \bar{\mathbb{Q}}_\ell)$ be the relative ℓ-adic cohomology complex with compact support of F_s. For dimension reasons, $\mathcal{H}^j(K_s) = 0$ for $j < 0$ and $j > 2s-2$.

Lemma 3.1. *Suppose that f_i is square-free for every $i = 1, \ldots, s$. Then*

1. *$\mathcal{H}^j(K_s)_{|\mathbb{G}_m} = 0$ for $j < s-1$.*
2. *If $s \geq 2$, $\mathcal{H}^{2s-2}(K_s)_{|\mathbb{G}_m}$ is the Tate-twisted constant sheaf $\bar{\mathbb{Q}}_\ell(1-s)$.*
3. *$\mathcal{H}^j(K_s)_{|\mathbb{G}_m}$ is geometrically constant of weight $2(j-s+1)$ for $s \leq j \leq 2s-3$.*
4. *$\mathcal{H}^{s-1}(K_s)_{|\mathbb{G}_m}$ contains a subsheaf $\mathcal{F}_s$ which is the extension by direct image of a smooth sheaf on an open subset $V \hookrightarrow \mathbb{G}_m$ of rank $s(d-1)^s$, pure of weight $s-1$, unipotent at 0 and totally ramified at infinity, such that the quotient $\mathcal{H}^{s-1}(K_s)_{|\mathbb{G}_m}/\mathcal{F}_s$ is geometrically constant of rank $d^s - (d-1)^s$ and weight 0.*
5. *$\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$ is pure of weight 0 and dimension $(d-1)^s$.*

If all f_i split completely in k_r one can replace "geometrically constant" by "Tate-twisted constant" everywhere and $\mathrm{Gal}(\bar{k}_r/k_r)$ acts trivially on $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$.

Proof. We will proceed by induction on s, as in [1, Théorème 7.8]. For $s = 1$, (1), (2) and (3) are empty, so we only need to prove (4) and (5). In this case, $K_1 = f_{1!}\bar{\mathbb{Q}}_\ell[0]$. There is a natural trace map $f_{1!}\bar{\mathbb{Q}}_\ell \to \bar{\mathbb{Q}}_\ell$, let $\mathcal{F}_1$ be its kernel. Since d is prime to p, the inertia group I_∞ at infinity acts on $\mathcal{F}_1$ via the direct sum of all its non-trivial characters of order divisible by d. In particular, $\mathcal{F}_1$ is totally ramified at infinity, and is clearly pure of weight 0. Now from the exact sequence $0 \to \mathcal{F}_1 \to f_{1!}\bar{\mathbb{Q}}_\ell \to \bar{\mathbb{Q}}_\ell \to 0$ we get $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_1) \hookrightarrow \mathrm{H}^1_c(\mathbb{G}_m, f_!\bar{\mathbb{Q}}_\ell) = \mathrm{H}^1_c(U_1, \bar{\mathbb{Q}}_\ell) = \mathrm{H}^0_c(Z_1, \bar{\mathbb{Q}}_\ell)$ which is pure of weight 0, where $Z_1 \subseteq \mathbb{A}^1$ is the subscheme defined by $f_1 = 0$ and $U_1 = \mathbb{A}^1 - Z_1$. Moreover, $\dim \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_1) = \dim \mathrm{H}^1_c(\mathbb{G}_m, f_{1!}\bar{\mathbb{Q}}_\ell) - \dim \mathrm{H}^1_c(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell) = \dim \mathrm{H}^1_c(U_1, \bar{\mathbb{Q}}_\ell) - \dim \mathrm{H}^1_c(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell) = d-1$ since f_1 has d distinct roots in $\bar{k}$. If f_1 splits completely in k_r, then $U_1(k_r) = U_1(\bar{k}_r)$ and therefore $\mathrm{Gal}(\bar{k}_r/k_r)$ acts trivially on $\mathrm{H}^1_c(U_1, \bar{\mathbb{Q}}_\ell)$ and a fortiori on $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_1)$.

From now on let us denote $K(f_1) = K_1$ and $\mathcal{F}(f_1) = \mathcal{F}_1$ in order to keep track of the polynomial from which they arise. We move now to the

induction step, so suppose the lemma has been proved for $s-1$. Since F_s is the composition of $F_{s-1}\times f_s$ and the multiplication map $\mu:\mathbb{A}^2_{k_r}\to\mathbb{A}^1_{k_r}$, we get $K_s=\mathrm{R}\mu_!(\mathbb{A}^1\times\mathbb{A}^1,K_{s-1}\boxtimes K(f_s))$. In particular, $K_{s|\mathbb{G}_m}=\mathrm{R}\mu_!(\mathbb{G}_m\times\mathbb{G}_m,K_{s-1}\boxtimes K(f_s))$. From the distinguished triangles

$$\mathcal{F}(f_s)[0]\to K(f_s)\to\bar{\mathbb{Q}}_\ell[0]\to$$

and

$$\mathcal{F}_{s-1}[2-s]\to K_{s-1}\to L_{s-1}\to$$

where L_{s-1} is the "constant part" of K_{s-1}, we get the distinguished triangles

$$\mathrm{R}\mu_!(K_{s-1}\boxtimes\mathcal{F}(f_s)[0])\to K_{s|\mathbb{G}_m}\to\mathrm{R}\mu_!(\pi_1^\star K_{s-1})\to, \tag{7}$$

$$\mathrm{R}\mu_!(\pi_1^\star\mathcal{F}_{s-1})[2-s]\to\mathrm{R}\mu_!(\pi_1^\star K_{s-1})\to\mathrm{R}\mu_!(\pi_1^\star L_{s-1})\to \tag{8}$$

and

$$\mathrm{R}\mu_!(\mathcal{F}_{s-1}\boxtimes\mathcal{F}(f_s))[2-s]\to\mathrm{R}\mu_!(K_{s-1}\boxtimes\mathcal{F}(f_s)[0])\to\mathrm{R}\mu_!(L_{s-1}\boxtimes\mathcal{F}(f_s)[0])\to \tag{9}$$

where $\pi_1,\pi_2:\mathbb{G}_m\times\mathbb{G}_m\to\mathbb{G}_m$ are the projections.

Let $\sigma:\mathbb{G}_m\times\mathbb{G}_m\to\mathbb{G}_m\times\mathbb{G}_m$ be the automorphism given by $(u,v)\mapsto(u,uv)$. Then $\mu=\pi_2\circ\sigma$ and $\pi_1=\pi_1\circ\sigma$, so

$$\mathrm{R}\mu_!(\pi_1^\star\mathcal{F}_{s-1})=\mathrm{R}\pi_{2!}(\pi_1^\star\mathcal{F}_{s-1})=\mathrm{R}\Gamma_c(\mathbb{G}_m,\mathcal{F}_{s-1})$$

where the last object is seen as a geometrically constant object (in fact constant if $f_1,\dots,f_{s-1}$ split in k_r) in $\mathcal{D}^b_c(\mathbb{G}_m,\bar{\mathbb{Q}}_\ell)$. By part (4) of the induction hypothesis, we have $\mathrm{H}^1_c(\mathbb{G}_m,\mathcal{F}_{s-1})=0$ for $i=0,2$, so $\mathrm{R}\Gamma_c(\mathbb{G}_m,\mathcal{F}_{s-1})[2-s]=\mathrm{H}^1_c(\mathbb{G}_m,\mathcal{F}_{s-1})[1-s]$. Similarly, using the automorphism $(u,v)\mapsto(uv,v)$ we get

$$\mathrm{R}\mu_!(L_{s-1}\boxtimes\mathcal{F}(f_s))=\mathrm{R}\Gamma_c(\mathbb{G}_m,L_{s-1}\otimes\mathcal{F}(f_s))$$

and

$$\mathrm{R}\mu_!(\pi_1^\star L_{s-1})=\mathrm{R}\Gamma_c(\mathbb{G}_m,L_{s-1})$$

which are both geometrically constant (and constant if $f_1,\dots,f_s$ split in k_r).

With these ingredients we can now start proving the lemma. We have already seen that $\mathrm{R}\Gamma_c(\mathbb{G}_m,\mathcal{F}_{s-1})[2-s]$ only has non-zero cohomology in degree $s-1$. By induction, L_{s-1} only has non-zero cohomology in degrees $\geq s-2$. Since a constant object has obviously no punctual sections in $\mathbb{G}_m$, we deduce that $\mathrm{R}\Gamma_c(\mathbb{G}_m,L_{s-1}\otimes\mathcal{F}(f_s))$ and $\mathrm{R}\Gamma_c(\mathbb{G}_m,L_{s-1})$ only have cohomology in degrees $\geq s-1$.

For the first term in the triangle (9) we have

$$\mathrm{R}\mu_!(\mathcal{F}_{s-1}\boxtimes\mathcal{F}(f_s))=\mathrm{R}\pi_{2!}((\pi_1\circ\sigma^{-1})^\star\mathcal{F}_{s-1}\otimes(\pi_2\circ\sigma^{-1})^\star\mathcal{F}(f_s))=$$

$$=\mathrm{R}\pi_{2!}(\pi_1^\star\mathcal{F}_{s-1}\otimes(\pi_2\circ\sigma^{-1})^\star\mathcal{F}(f_s))$$

Its fibre over a geometric point $t\in\mathbb{G}_m$ is $\mathrm{R}\Gamma_c(\mathbb{G}_m,\mathcal{F}_{s-1}\otimes\sigma_t^\star\mathcal{F}(f_s))$, where $\sigma_t(u)=t/u$ is an automorphism of $\mathbb{G}_m$. Since $\mathcal{F}_{s-1}\otimes\sigma_t^\star\mathcal{F}(f_s)$ has no punctual sections, it does not have cohomology in degree 0, and therefore

$\mathrm{R}\mu_!(\mathcal{F}_{s-1} \boxtimes \mathcal{F}(f_s))[2-s]$ only has cohomology in degrees $\geq s-1$. Using the distinguished triangles 7, 8 and 9 this proves (1).

Since $\mathcal{F}_{s-1}$ is totally ramified at infinity, $\mathrm{H}^2_c(\mathbb{G}_m, \mathcal{F}_{s-1}) = 0$, so $\mathrm{R}\mu_!(\pi_i^\star \mathcal{F}_{s-1})[2-s] = \mathrm{R}\Gamma_c(\mathbb{G}_m, \mathcal{F}_{s-1})[2-s]$ has no cohomology in degree $\geq s$ (and in particular in degree $2s-2$). On the other hand, since $\mathcal{F}(f_s)$ is totally ramified at infinity, so are all cohomology sheaves of $L_{s-1} \otimes \mathcal{F}(f_s)$. Since L_{s-1} only has cohomology in degrees $\leq 2s-4$, the spectral sequence $\mathrm{H}^i_c(\mathbb{G}_m, \mathcal{H}^j(L_{s-1}) \otimes \mathcal{F}(f_s)) \Rightarrow \mathrm{H}^{i+j}_c(\mathbb{G}_m, L_{s-1} \otimes \mathcal{F}(f_s))$ implies that $L_{s-1} \otimes \mathcal{F}(f_s)$ only has non-zero cohomology in degrees $\leq 2s-3$. Finally, since $\mathcal{F}(f_s)$ is smooth at 0 (because f_s is square-free and therefore étale over 0), $\sigma_t^\star \mathcal{F}(f_s)$ is unramified at infinity and therefore $\mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)$ is totally ramified at infinity. In particular, $\mathrm{H}^2_c(\mathbb{G}_m, \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)) = 0$ and $\mathrm{R}\mu_!(\mathcal{F}_{s-1} \boxtimes \mathcal{F}(f_s))[2-s]$ has no cohomology in degree $\geq s$ (in particular in degree $2s-2$). From the triangles 7 and 8 we get then isomorphisms

$$\mathcal{H}^{2s-2}(K_{2|\mathbb{G}_m}) \cong \mathrm{R}^{2s-2}\mu_!(\pi_1^\star K_{s-1}) \cong \mathrm{R}^{2s-2}\mu_!(\pi_1^\star L_{s-1}) \cong$$

$$\cong \mathrm{H}^2_c(\mathbb{G}_m, \mathcal{H}^{2s-4}(L_{s-1})) \cong \mathrm{H}^2_c(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell(2-s)) = \bar{\mathbb{Q}}_\ell(1-s)$$

by the induction hypothesis and the spectral sequence $\mathrm{H}^i_c(\mathbb{G}_m, \mathcal{H}^j(L_{s-1})) \Rightarrow \mathrm{H}^{i+j}_c(\mathbb{G}_m, L_{s-1})$, where the last two objects are regarded as constant sheaves on $\mathbb{G}_m$. This proves (2).

For (3), we have already seen that the left hand side of triangle 9 only has cohomology in degree $s-1$. Similarly, the left hand side of triangle 8 $\mathrm{R}\Gamma_c(\mathbb{G}_m, \mathcal{F}_{s-1})[2-s] = \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1})[1-s]$ only has cohomology in degree $s-1$. Since the other two ends of 8 and 9 are geometrically constant, we conclude that $\mathcal{H}^j(K)_{|\mathbb{G}_m}$ is geometrically constant for $j \geq s$ using triangle 7.

Let $s \leq j \leq 2s-3$. For any geometrically constant object L, we have $\mathrm{R}\Gamma_c(\mathbb{G}_m, L) = L \otimes \mathrm{R}\Gamma_c(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell) \cong L[-1] \oplus L(-1)[-2]$. In particular

$$\mathcal{H}^j(\mathrm{R}\Gamma_c(\mathbb{G}_m, L_{s-1})) \cong \mathcal{H}^{j-1}(L_{s-1}) \oplus \mathcal{H}^{j-2}(L_{s-1})(-1)$$

is pure of weight $2(j-s+1)$ by induction. Similarly $\mathcal{H}^j(\mathrm{R}\Gamma_c(\mathbb{G}_m, L_{s-1} \otimes \mathcal{F}(f_s))) = \mathcal{H}^j(L_{s-1} \otimes \mathrm{R}\Gamma_c(\mathbb{G}_m, \mathcal{F}(f_s))) \cong \mathcal{H}^{j-1}(L_{s-1}) \otimes \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}(f_s))$ is pure of weight $2(j-s+1)$ since $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}(f_s))$ is pure of weight 0. Using triangle 7 this proves that $\mathcal{H}^j(K)_{|\mathbb{G}_m}$ is pure of weight $2(j-s+1)$.

From triangles 7 and 9 we get exact sequences

$$0 \to \mathrm{R}^{s-1}\mu_!(K_{s-1} \boxtimes \mathcal{F}(f_s)[0]) \to \mathcal{H}^{s-1}(K_{s|\mathbb{G}_m}) \to \tag{10}$$

$$\to \mathrm{R}^{s-1}\mu_!(\pi_1^\star K_{s-1}) \to \mathrm{R}^s\mu_!(K_{s-1} \boxtimes \mathcal{F}(f_s)[0])$$

and

$$0 \to \mathrm{R}^1\mu_!(\mathcal{F}_{s-1} \boxtimes \mathcal{F}(f_s)) \to \mathrm{R}^{s-1}\mu_!(K_{s-1} \boxtimes \mathcal{F}(f_s)[0]) \to$$

$$\to \mathrm{H}^{s-1}_c(\mathbb{G}_m, L_{s-1} \otimes \mathcal{F}(f_s)) \to 0.$$

We have already shown that $\mathrm{R}^s\mu_!(K_{s-1} \boxtimes \mathcal{F}(f_s)[0])$ is pure of weight $2(s-s+1) = 2$. On the other hand, from triangle 8 we get an exact

sequence

$$\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1}) \to \mathrm{R}^{s-1}\mu_!(\pi_1^\star K_{s-1}) \to \mathcal{H}^{s-1}(\mathrm{R}\Gamma_c(\mathbb{G}_m, L_{s-1}))$$

where the left hand side has weight 0 by part (5) of the induction hypothesis and the right hand side $\mathcal{H}^{s-1}(\mathrm{R}\Gamma_c(\mathbb{G}_m, L_{s-1})) \cong \mathcal{H}^{s-1}(L_{s-1}[-1] \oplus L_{s-1}(-1)[-2]) = \mathcal{H}^{s-2}(L_{s-1}) \oplus \mathcal{H}^{s-3}(L_{s-1})(-1) = \mathcal{H}^{s-2}(L_{s-1})$ also has weight 0 by part (4) of the induction hypothesis. Therefore $\mathrm{R}^{s-1}\mu_!(\pi_1^\star K_{s-1})$ is pure of weight 0, and the last arrow in sequence (10) is trivial:

$$0 \to \mathrm{R}^{s-1}\mu_!(K_{s-1} \boxtimes \mathcal{F}(f_s)[0]) \to \mathcal{H}^{s-1}(K_{s|\mathbb{G}_m}) \to \mathrm{R}^{s-1}\mu_!(\pi_1^\star K_{s-1}) \to 0$$

Let $\mathcal{F}_s := \mathrm{R}^1\mu_!(\mathcal{F}_{s-1} \boxtimes \mathcal{F}(f_s))$ (the multiplicative convolution of $\mathcal{F}(f_1), \dots, \mathcal{F}(f_s)$). Then $\mathcal{F}_s \hookrightarrow \mathcal{H}^{s-1}(K_{s|\mathbb{G}_m})$, and the quotient sits inside an exact sequence

$$0 \to \mathrm{H}^{s-1}_c(\mathbb{G}_m, L_{s-1} \otimes \mathcal{F}(f_s)) \to \mathcal{H}^{s-1}(K_{s|\mathbb{G}_m})/\mathcal{F}_s \to \mathrm{R}^{s-1}\mu_!(\pi_1^\star K_{s-1}) \to 0$$

whose extremes are already known to be geometrically constant by triangle 8. The rank of this quotient is

$$\begin{aligned}
&\dim \mathrm{H}^{s-1}_c(\mathbb{G}_m, L_{s-1} \otimes \mathcal{F}(f_s)) + \dim \mathrm{R}^{s-1}\mu_!(\pi_1^\star K_{s-1}) \\
&= (\dim \mathcal{H}^{s-2}(L_{s-1}))(\dim \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}(f_s))) + \dim \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1}) + \dim \mathrm{H}^{s-1}_c(\mathbb{G}_m, L_{s-1}) \\
&= (d^{s-1} - (d-1)^{s-1})(d-1) + (d-1)^{s-1} + \dim \mathcal{H}^{s-2}(L_{s-1}) + \dim \mathcal{H}^{s-3}(L_{s-1}) \\
&= d^s - d^{s-1} - (d-1)^s + (d-1)^{s-1} + (d^{s-1} - (d-1)^{s-1}) \\
&= d^s - (d-1)^s
\end{aligned}$$

by parts (4) and (5) of the induction hypothesis.

By [4, Corollary 6 and Proposition 9], $\mathcal{H}^{s-1}(K_s)$ (and in particular its subsheaf $\mathcal{F}_s$) does not have punctual sections in $\mathbb{A}^1$. Let $j_0 : \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ be the inclusion. We claim that $\mathrm{H}^1_c(\mathbb{A}^1, j_{0\star}\mathcal{F}_s) = 0$. This will prove both that $\mathcal{F}_s$ is the extension by direct image of its restriction to any open set $j_V : V \hookrightarrow \mathbb{G}_m$ on which it is smooth and that it is totally ramified at infinity, since from the exact sequences

$$0 \to j_{0\star}\mathcal{F}_s \to j_{0\star}j_{V\star}j_V^\star\mathcal{F}_s \to \mathcal{Q} := j_{V\star}j_V^\star\mathcal{F}_s/\mathcal{F}_s(\text{punctual}) \to 0$$

and

$$0 \to j_{\infty!}j_{0\star}\mathcal{F}_s \to j_{\infty\star}j_{0\star}\mathcal{F}_s \to \mathcal{F}_s^{I_\infty} \to 0$$

where $j_\infty : \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ is the inclusion, we get injections $\mathcal{Q} \hookrightarrow \mathrm{H}^1_c(\mathbb{A}^1, j_{0\star}\mathcal{F}_s)$ and $\mathcal{F}_s^{I_\infty} \hookrightarrow \mathrm{H}^1_c(\mathbb{A}^1, j_{0\star}\mathcal{F}_s)$.

Let $i_0 : \{0\} \hookrightarrow \mathbb{A}^1$ be the inclusion. From the exact sequence

$$0 \to j_{0!}\mathcal{F}_s \to j_{0\star}\mathcal{F}_s \to i_{0\star}i_0^\star j_{0\star}\mathcal{F}_s \to 0$$

and the fact that $\mathcal{F}_s$ has no punctual sections we get

$$0 \to \mathcal{F}_s^{I_0} \to \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s) \to \mathrm{H}^1_c(\mathbb{A}^1, j_{0\star}\mathcal{F}_s) \to 0$$

where $\mathcal{F}_s^{I_0}$ is the invariant space of $\mathcal{F}_s$ as a representation of the inertia group I_0. So it suffices to show that $\dim \mathcal{F}_s^{I_0} \geq \dim \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$ (and then we will automatically have equality). By definition of $\mathcal{F}_s$, $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s) = \mathrm{H}^2_c(\mathbb{G}_m \times \mathbb{G}_m, \mathcal{F}_{s-1} \boxtimes \mathcal{F}(f_s)) = \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1}) \times \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}(f_s))$. Therefore

$\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$ is pure of weight 0 and dimension $(d-1)^{s-1}(d-1) = (d-1)^s$ by induction, thus proving (5). If $f_1, \dots, f_s$ split in k_r then $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$ is a trivial $\mathrm{Gal}(\bar{k}_r/k_r)$-module, also by induction.

On the other hand, $\mathcal{H}^{s-1}(K_s)_{|\mathbb{G}_m}$ contains $\mathcal{F}_s$ plus a geometrically constant part of dimension $d^s - (d-1)^s$. So $\dim \mathcal{H}^{s-1}(K_s)^{I_0} = \dim \mathcal{F}_s^{I_0} + (d^s - (d-1)^s)$. Since $\mathcal{H}^{s-1}(K_s)$ has no punctual sections, there is an injection $\mathcal{H}^{s-1}(K_s)_0 \hookrightarrow \mathcal{H}^{s-1}(K_s)^{I_0}$, so $\dim \mathcal{H}^{s-1}(K_s)^{I_0} \geq \dim \mathcal{H}^{s-1}(K_s)_0$. By base change, $\mathcal{H}^{s-1}(K_s)_0 = \mathrm{H}^{s-1}_c(\{f_1(x_1)\cdots f_s(x_s) = 0\}, \bar{\mathbb{Q}}_\ell) = \mathrm{H}^s_c(\{f_1(x_1)\cdots f_s(x_s) \neq 0\}, \bar{\mathbb{Q}}_\ell) = \mathrm{H}^s_c(U_1 \times \cdots \times U_s, \bar{\mathbb{Q}}_\ell) = \mathrm{H}^1_c(U_1, \bar{\mathbb{Q}}_\ell) \times \cdots \times \mathrm{H}^1_c(U_s, \bar{\mathbb{Q}}_\ell)$, where $U_i \subseteq \mathbb{A}^1$ is the open set defined by $f_i(x) \neq 0$ (since the U_i only have non-zero cohomology in degrees 1 and 2), so $\dim \mathcal{H}^{s-1}(K_s)_0 = d^s$. We conclude that $\dim \mathcal{F}_s^{I_0} = \dim \mathcal{H}^{s-1}(K_s)^{I_0} - (d^s - (d-1)^s) \geq \dim \mathcal{H}^{s-1}(K_s)_0 - (d^s - (d-1)^s) = (d-1)^s = \dim \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$.

To prove (4) it only remains to show that $\mathcal{F}_{s|V}$ is pure of weight $s-1$ and rank $s(d-1)^s$ and has unipotent monodromy action at 0. Let $t \in \mathbb{G}_m$ be a geometric point which is not the product of a non-smoothness point of $\mathcal{F}_{s-1}$ and a non-smoothness point of $\mathcal{F}(f_s)$. The fibre of $\mathcal{F}_s$ over t is $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s))$. By the choice of t, at every point of $\mathbb{G}_m$ at least one of $\mathcal{F}_{s-1}$, $\sigma_t^\star \mathcal{F}(f_s)$ is smooth. Therefore if $\mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)$ is smooth in the open set $j_W : W \hookrightarrow \mathbb{G}_m$, $j_{W\star} j_W^\star(\mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)) = (j_{W\star} j_W^\star \mathcal{F}_{s-1}) \otimes (j_{W\star} j_W^\star \sigma_t^\star \mathcal{F}(f_s)) = \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)$. Given that $\mathcal{F}_{s-1}$ (respectively $\sigma_t^\star \mathcal{F}(f_s)$) is pure of weight $s-2$, unipotent at 0 and totally ramified at ∞ (resp. pure of weight 0, unramified at ∞ and totally ramified at 0), $\mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)$ is pure of weight $s-2$ and totally ramified at both 0 and ∞, so $\mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)) = \mathrm{H}^1(\mathbb{P}^1, j_{\infty\star} j_W^\star(\mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)))$ is pure of weight $s-1$, where $j_\infty : W \hookrightarrow \mathbb{P}^1$ is the inclusion.

As for the rank, since $\mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)$ has no punctual sections and is totally ramified at 0 and ∞, $\dim \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)) = -\chi(\mathbb{G}_m, \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s))$. By the Ogg-Shafarevic formula, for each of $\mathcal{F}_{s-1}$, $\sigma_t^\star \mathcal{F}(f_s)$ its Euler characteristic is (-1 times) a sum of local terms for the points of $\mathbb{P}^1$ where they are ramified. The local terms at 0, ∞ are the Swan conductors, which get multiplied by D upon tensoring with a unipotent sheaf of rank D. The local terms corresponding to ramified points in $\mathbb{G}_m$ (Swan conductor plus drop of the rank) are multiplied by D upon tensoring with an unramified sheaf of rank D. Since at every point of $\mathbb{G}_m$ at least one of $\mathcal{F}_{s-1}$, $\sigma_t^\star \mathcal{F}(f_s)$ is unramified, we conclude that $-\chi(\mathbb{G}_m, \mathcal{F}_{s-1} \otimes \sigma_t^\star \mathcal{F}(f_s)) = -(d-1)\chi(\mathbb{G}_m, \mathcal{F}_{s-1}) - (s-1)(d-1)^{s-1}\chi(\mathbb{G}_m, \mathcal{F}(f_s)) = (d-1)(d-1)^{s-1} + (s-1)(d-1)^{s-1}(d-1) = s(d-1)^s$.

Finally, since $\mathcal{F}_s^{I_0} \cong \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_s)$ has weight 0 and $\mathcal{F}_s$ is pure of weight $s-1$, for every Frobenius eigenvalue of $\mathcal{F}_s^{I_0}$ there is a unipotent Jordan block of size s for the monodromy of $\mathcal{F}_s$ at 0 by [2, Section 1.8]. Since its rank is $s(d-1)^s$, these Jordan blocks fill up the entire space, and therefore the I_0 action is unipotent. This finishes the proof of (4) and of the lemma. □

Now let $T : \mathbb{A}^r_{k_r} \to \mathbb{A}^1_{k_r}$ be the map defined by the polynomial T, and $K'_r := \mathrm{R}T_!\bar{\mathbb{Q}}_\ell \in \mathcal{D}^b_c(\mathbb{A}^1_k, \bar{\mathbb{Q}}_\ell)$. After extending scalars to k_r, K'_r becomes isomorphic to K_r for $f_j = f^{\sigma^j}$, $j = 1, \dots, r$. Since the results of the lemma are invariant under finite extension of scalars, they also hold for K'_r. In particular, for every $r-1 \leq j \leq 2r-2$ there exist $\beta_{j,1}, \dots, \beta_{j,d_j} \in \mathbb{C}$ of absolute value 1, where $d_j = \operatorname{rank} \mathcal{H}^j(K_r)$ (or the rank of the constant part if $j = r-1$) such that for every finite extension k_m of k of degree m and every $\lambda \in k_m^\star$

$$\#\{(x_1, \dots, x_r) \in k_m^r | T(x_1, \dots, x_r) = \lambda\} = \tag{11}$$

$$= \sum_{j=r-1}^{2r-2} (-1)^j \sum_{l=1}^{d_j} q^{m(j-r+1)} \beta_{j,l}^m + (-1)^{r-1} \mathrm{Tr}(\mathrm{Frob}_{k_m,\lambda} | \mathcal{F}_r).$$

Taking the sum over all $\lambda \in k_m^\star$ and using the trace formula:

$$\#\{(x_1, \dots, x_r) \in k_m^r | T(x_1, \dots, x_r) \neq 0\} =$$

$$= \sum_{j=r-1}^{2r-2} (-1)^j \sum_{l=1}^{d_j} (q^m - 1) q^{m(j-r+1)} \beta_{j,l}^m + (-1)^{r-1} \sum_{\lambda \in k_m} \mathrm{Tr}(\mathrm{Frob}_{k_m,\lambda} | \mathcal{F}_r) =$$

$$= \sum_{j=r-1}^{2r-2} (-1)^j \sum_{l=1}^{d_j} (q^m - 1) q^{m(j-r+1)} \beta_{j,l}^m + (-1)^r \mathrm{Tr}(\mathrm{Frob}_{k_m} | \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_r)).$$

Let b be the degree of a splitting field of f over k_r. Then the (geometrically constant) cohomology sheaves of K'_r become constant after extending scalars to k_{br}. In particular all $\beta_{j,l}$ are br-th roots of unity. If m is any positive integer congruent to 1 modulo br we have then

$$\#\{(x_1, \dots, x_r) \in k_m^r | T(x_1, \dots, x_r) \neq 0\} =$$

$$= \sum_{j=r-1}^{2r-2} (-1)^j \sum_{l=1}^{d_j} (q^m - 1) q^{m(j-r+1)} \beta_{j,l} + (-1)^r \mathrm{Tr}(\mathrm{Frob}_{k_m} | \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_r)) =$$

$$= \left(\sum_{l=1}^{d_{2r-2}} \beta_{2r-2,l} \right) q^{mr} + \sum_{j=r-1}^{2r-2} (-1)^{j-1} \left(\sum_{l=1}^{d_{j-1}} \beta_{j-1,l} + \sum_{l=1}^{d_j} \beta_{j,l} \right) q^{m(j-r+1)} +$$

$$+ (-1)^r \mathrm{Tr}(\mathrm{Frob}_{k_m} | \mathrm{H}^1_c(\mathbb{G}_m, \mathcal{F}_r)).$$

Since m is prime to r, $\mathcal{B}$ is a basis of k_{mr} over k_m, and thus $T(x_1, \dots, x_r) = N_{k_{mr}/k_m}(f(\alpha_1 x_1 + \cdots + \alpha_r x_r))$. Therefore

$$\#\{(x_1, \dots, x_r) \in k_m^r | T(x_1, \dots, x_r) \neq 0\} =$$

$$= \#\{x \in k_{mr} | \mathrm{N}_{k_{mr}/k_m}(f(x)) \neq 0\} = \#\{x \in k_{mr} | f(x) \neq 0\}$$

and in particular

$$|\#\{(x_1, \dots, x_r) \in k_m^r | T(x_1, \dots, x_r) \neq 0\} - q^{mr}| \leq d.$$

Substituting in the formula above, we get

$$\left|\left(\sum_{l=1}^{d_{2r-2}}\beta_{2r-2,l}-1\right)q^{mr}+\sum_{j=r-1}^{2r-2}(-1)^{j-1}\left(\sum_{l=1}^{d_{j-1}}\beta_{j-1,l}+\sum_{l=1}^{d_j}\beta_{j,l}\right)q^{m(j-r+1)}+\right.$$
$$\left.+(-1)^r\mathrm{Tr}(\mathrm{Frob}_{k_m}|\mathrm{H}^1_c(\mathbb{G}_m,\mathcal{F}_r))\right|\leq d$$

Letting $m\to\infty$ and using that $|\mathrm{Tr}(\mathrm{Frob}_{k_m}|\mathrm{H}^1_c(\mathbb{G}_m,\mathcal{F}_r))|\leq(d-1)^r$ is bounded by a constant, we conclude that $\sum_{l=1}^{d_{2r-2}}\beta_{2r-2,l}=1$ and

$$\sum_{l=1}^{d_{j-1}}\beta_{j-1,l}+\sum_{l=1}^{d_j}\beta_{j,l}=0$$

for every $r\leq j\leq 2r-2$, so $\sum_{l=1}^{d_j}\beta_{j,l}=(-1)^j$ for every $r-1\leq j\leq 2r-2$.

Theorem 3.2. *Let $f\in k_r[x]$ be a square-free polynomial of degree d prime to p and $e|q-1$. Then the number N_f of k_r-rational points on the curve*

$$y^{\frac{q-1}{e}}=f(x)$$

satisfies the estimate

$$|N_f-q^r-\delta+1|\leq r(d-1)^r(q-1)q^{\frac{r-1}{2}}$$

where $0\leq\delta\leq d$ is the number of roots of f in k_r.

Proof. Substituting the computed values for $\sum_{l=1}^{d_j}\beta_{j,l}$ in equation 11 for $m=1$ we get

$$\#W_\lambda(k)=\#\{(x_1,\dots,x_r)\in k^r|T(x_1,\dots,x_r)=\lambda\}=$$
$$=\sum_{j=r-1}^{2r-2}q^{j-r+1}+(-1)^{r-1}\mathrm{Tr}(\mathrm{Frob}_{k,\lambda}|\mathcal{F}_r)=\sum_{j=0}^{r-1}q^j+(-1)^{r-1}\mathrm{Tr}(\mathrm{Frob}_{k,\lambda}|\mathcal{F}_r).$$

So, by equation 6, we have

$$N_f=\#Z(k_r)+\frac{q-1}{e}\sum_{\lambda^e=1}\#W_\lambda(k)=$$
$$=\delta+\frac{q-1}{e}\sum_{\lambda^e=1}\left(\sum_{j=0}^{r-1}q^j+(-1)^{r-1}\mathrm{Tr}(\mathrm{Frob}_{k,\lambda}|\mathcal{F}_r)\right)=$$
$$=\delta+(q^r-1)+(-1)^{r-1}\frac{q-1}{e}\sum_{\lambda^e=1}\mathrm{Tr}(\mathrm{Frob}_{k,\lambda}|\mathcal{F}_r),$$

so

$$|N_f-q^r-\delta+1|\leq\frac{q-1}{e}\sum_{\lambda^e=1}r(d-1)^rq^{\frac{r-1}{2}}=r(d-1)^r(q-1)q^{\frac{r-1}{2}}$$

since $\mathcal{F}_r$ is pure of weight $r-1$ and generic rank $r(d-1)^r$ by the lemma, and its rank can only drop at ramified points. □

Remark 3.3. The condition that f is square-free is necessary, as shown by the example

$$y^{q-1} = x^d$$

in which

$$N_r = 1 + \#\{x \in k_r | N_{k_r/k}(x^d) = 1\} = 1 + \sum_{t \in k, t^d = 1} \#\{x \in k_r | N_{k_r/k}(x) = t\} =$$

$$= 1 + \mu_d \cdot (q^{s-1} + q^{r-2} + \cdots + q + 1)$$

where $\mu_d \geq 1$ is the number of d-th roots of unity in k.

References

[1] Deligne, P., *Applications de la formule des traces aux sommes trigonométriques*, in *Cohomologie Étale, Séminaire de Géométrie Algébrique du Bois-Marie (SGA $4\frac{1}{2}$)*,Lecture Notes in Mathematics 569, Springer-Verlag.

[2] Deligne, P., *La conjecture de Weil II*, Publ. Math. IHES, 52(1980), 137-252.

[3] Katz, N., *Estimates for Soto-Andrade sums*, J. reine angew. Math. 438 (1993), 143–161.

[4] Katz, N., *A semicontinuity result for monodromy under degeneration*, Forum Math. 15 (2003), 191–200.

[5] Katz, N., *Sato-Tate Theorems for Finite-Field Mellin Transforms*, preprint (2010)

[6] Rojas-León, A. and Wan, D., *Big improvements of the Weil bound for Artin-Schreier curves*, preprint (2010), arXiv:1004.2224 [math:AG].

Departamanto de Álgebra, Universidad de Sevilla, Apdo 1160, 41080 Sevilla, Spain

E-mail: arojas@us.es