Bull. Aust. Math. Soc. **98** (2018), 196–202
doi:10.1017/S0004972718000448

A SIMPLE PROOF OF CHEBOTAREV'S DENSITY THEOREM OVER FINITE FIELDS

STEVE MEAGHER

(Received 15 December 2017; accepted 4 May 2018; first published online 12 July 2018)

Abstract

We present a simple proof of the Chebotarev density theorem for finite morphisms of quasi-projective varieties over finite fields following an idea of Fried and Kosters for function fields. The key idea is to interpret the number of rational points with a given Frobenius conjugacy class as the number of rational points of a twisted variety, which is then bounded by the Lang–Weil estimates.

2010 *Mathematics subject classification*: primary 11G25; secondary 14G15.

Keywords and phrases: Chebotarev density theorem, quasi-projective variety, Frobenius conjugacy class, Lang–Weil bounds.

1. Introduction

Let G be a finite group and let X/k be a quasi-projective variety, that is, a geometrically irreducible, integral separated scheme of finite type over a field k, of dimension d with a G-action. Let $Y = X/G$ be the quotient and $f : X \longrightarrow Y$ be the quotient morphism. Assume that f is étale and k is finite.

For any closed point $\bar{y} \in Y$ and any point $\bar{x} \in f^{-1}(\bar{y})$, the decomposition group is $D(\bar{x}) = \{g \in G \mid g(\bar{x}) = \bar{x}\}$. For a closed point $\bar{x} \in X$, let $k(\bar{x})$ denote the residue field of $\bar{x}$. There is a natural epimorphism $D(\bar{x}) \to \mathrm{Gal}(k(\bar{x})/k(\bar{y}))$ (see [7, Proposition 2.5, page 342]), which is an isomorphism because f is étale. We call the preimage $\varphi_{\bar{y}}$ of the field automorphism of $k(\bar{x})$ given by $\alpha \mapsto \alpha^{|k(\bar{y})|}$ the Frobenius of $\bar{y}$. Its choice depends on $\bar{x}$ and altering the choice of $\bar{x}$ to $\bar{x}' \in f^{-1}(\bar{y})$ corresponds to conjugating $\varphi_{\bar{y}}$ by a $g \in G$ such that $\bar{x}' = g\bar{x}$. Thus, the conjugacy class of $\varphi_{\bar{y}}$ is well defined.

A point $y \in Y(\mathbf{F}_q)$ is a morphism of schemes, $y : \mathrm{Spec}(\mathbf{F}_q) \longrightarrow Y$. We let $\{\bar{y}\}$ denote the image, so that $\bar{y}$ is a closed point. With this notation, if the base of Y is $\mathbf{F}_q$, then $k(\bar{y}) = \mathbf{F}_q$.

THEOREM 1.1 (Chebotarev). *With notation as above, for a conjugacy class $C \subset G$,*

$$|\{y \in Y_{\mathbf{F}_q}(\mathbf{F}_q) \mid \varphi_{\bar{y}} \in C\}| = \frac{|C|}{|G|} q^d + O(q^{d-(1/2)}),$$

where the implied constant depends only on $|C|/|G|$ and the degree, dimension and ambient dimension of an embedding of X into projective space.

The proof interprets the set of rational points with fixed Frobenius conjugacy class as the set of rational points on a certain twist of X. Using the Lang–Weil bounds, Theorem 1.1 follows. In the case of function fields, this idea goes back to Fried [2], who used the cyclic case as a special first case, and to Kosters [4], who obtained a formula in the case of non étale covers which are cyclic. Our only contribution is to present a geometric proof for varieties of any dimension which is independent of the structure of G. Lang's original proof [6] uses fibrations by curves. For a more modern proof using étale sheaves and L-functions, see [1, Theorem 4.1].

2. Proof of Theorem 1.1

Let $g \in G$ be an element of order m and let $C(g)$ be the conjugacy class of g. In this situation, given $y \in Y(\mathbf{F}_q)$ such that $\varphi_{\bar{y}} \in C(g)$, there exists $x \in X(\mathbf{F}_{q^m})$ such that $f(x) = y$. Let Frob denote the q-power Frobenius of $\mathbf{F}_{q^m}$.

We define the twist[1] X^g of X to be the $\mathbf{F}_q$ variety associated to the 1-cocycle $a_\sigma : \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q) \to G$ given by Frob $\mapsto g$. As a variety, X^g is the quotient

$$X \times_{\mathrm{Spec}(\mathbf{F}_q)} \mathrm{Spec}(\mathbf{F}_{q^m})/\langle (g^{-1}, \mathrm{Spec}(\mathrm{Frob}))\rangle$$

endowed with an $\mathbf{F}_q$ structure. An $\mathbf{F}_q$ rational point of X^g corresponds to a unique $\mathbf{F}_{q^m}$ rational point $x : \mathrm{Spec}(\mathbf{F}_{q^m}) \longrightarrow X_{\mathbf{F}_q}$ such that $g \circ x = x \circ \mathrm{Spec}(\mathrm{Frob})$. This means that if $\{\bar{x}\}$ is the image of x in X, then $g\bar{x} = \bar{x}$ and the image of g in $\mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q)$ is Frob. Thinking of G as a constant group scheme, we likewise twist G by a_σ to obtain a group scheme G^g whose $\mathbf{F}_{q^s}$ rational points are

$$G^g(\mathbf{F}_{q^s}) = \{h \in G \mid g^s h = h g^s\}.$$

The twist X^g is equipped with a G^g action, which is fixed-point free. Again Y is the quotient and we denote the quotient morphism by f^g. Let

$$Y(g, q) = \{y \in Y_{\mathbf{F}_q}(\mathbf{F}_q) \mid \varphi_{\bar{y}} \in C(g)\}.$$

By construction of X^g and f^g, we have $Y(g, q) = f^g(X^g(\mathbf{F}_q))$. If $Z(g) \subset G$ is the centraliser of g, then by definition $G^g(\mathbf{F}_q) = Z(g)$. Therefore,

$$X^g(\mathbf{F}_q)/Z(g) = X^g(\mathbf{F}_q)/G^g(\mathbf{F}_q) = f^g(X^g(\mathbf{F}_q)) = Y(g, q). \tag{2.1}$$

Here, we use the fact that since f^g is a quotient morphism for the algebraic group G^g, the $\mathbf{F}_q$ rational points of a fibre form a $G^g(\mathbf{F}_q)$ orbit. This fact follows because G^g acts freely on X^g [10, Theorem (B), page 105].

Putting together (2.1) and the identity $|Z(g)| = |G|/|C(g)|$,

$$|Y(g, q)| = \frac{|C(g)|}{|G|} |X^g(\mathbf{F}_q)|. \tag{2.2}$$

[1] The reader new to twists should consult the Appendix.

https://doi.org/10.1017/S0004972718000448 Published online by Cambridge University Press

Since X^g is itself a variety of the same dimension d as $Y_{\mathbf{F}_q}$, the Lang–Weil bounds [8] and (2.2) yield

$$\left| |Y(g, q)| - \frac{|C(g)|}{|G|} q^d \right| \leq A q^{d-(1/2)} + B q^{d-1},$$

where A depends only on the degree of an embedding of X^g into projective space and $|C(g)|/|G|$ and B depend only on the degree, dimension, ambient dimension of the embedding and $|C(g)|/|G|$. We fix a degree-δ embedding of X into $\mathbf{P}^N$ such that G acts on X via projective linear maps. Then X^g also has a degree-δ embedding into $\mathbf{P}^N_{\mathbf{F}_q}$ (see the Appendix). Therefore,

$$A = \frac{|C(g)|}{|G|}(\delta - 1)(\delta - 2) \quad \text{and} \quad B = \frac{|C(g)|}{|G|} B',$$

where B' depends only on δ, d and N [8].

3. Examples of Theorem 1.1

3.1. Zeros of degree-n polynomials. Assume that n is coprime to q. Let $p(z) \in \mathbf{F}_q[z]$ be monic of degree n so that

$$p(z) = z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0.$$

The zeros of $p(z)$ are all defined over $\mathbf{F}_{q^{n!}}$. For a divisor d of $n!$, one can ask what proportion of degree-n polynomials defined over $\mathbf{F}_q$ has zeros defined over $\mathbf{F}_{q^d}$ and no smaller extension.

The coefficients of $p(z)$ are the standard symmetric polynomials in the zeros of $p(z)$. Let $f : \mathbf{A}^n \longrightarrow \mathbf{A}^n$ be the morphism given by the standard symmetric polynomials, so that $f^{-1}(a_0, \ldots, a_{n-1})$ is the set of all permutations of the ordered zeros of $p(z)$. Moreover, f is the quotient morphism for $\mathbf{A}^n$ equipped with the natural action of S_n (the symmetric group on n letters). In this case f is not étale. However, by removing the diagonal of $\mathbf{A}^n$ one obtains an étale morphism g, which corresponds to assuming that $p(z)$ has no repeated zeros.

Then $\mathbf{F}_{q^d}$ is the extension generated by the zeros of $p(z)$ if and only if the Frobenius element φ_a of $a = (a_0, \ldots, a_{n-1})$ is an order-d element of S_n. Let $C_d \subset S_n$ be the set of elements of order m, so that C_d is closed under conjugation. Note that C_d is empty unless d is the least common multiple of the $d_i \leq n$ such that $\sum d_i = n$. Of course if C_d is empty there are no such polynomials.

So, the proportion of degree-n polynomials, without repeated zeros, whose zeros generate $\mathbf{F}_{q^d}$ is approximately $|C_d|/n!$. In particular, the proportion of polynomials whose zeros are defined over $\mathbf{F}_q$ and do not repeat is $1/n!$.

3.2. Legendre elliptic curves. Let $X = \mathbf{A}^1 - \{0, 1\}$ be the affine line minus 0 and 1 and let $Y = \mathbf{A}^1$ be the affine line. The set of Möbius transformations which permute $0, 1$ and ∞ in the projective line is isomorphic to S_3. Therefore, S_3 acts on X and the quotient is Y. Then, for q large, approximately $1/6$ of the $j \in Y(\mathbf{F}_q)$ will have a rational

https://doi.org/10.1017/S0004972718000448 Published online by Cambridge University Press

point $\lambda \in X(\mathbf{F}_q)$ lying above them,[1] 1/2 will have an element $\lambda \in Y(\mathbf{F}_{q^2})$ lying above them, and 1/3 will have an element $\lambda \in X(\mathbf{F}_{q^3})$ lying above them. In fact, the elements of Y can be interpreted as j-invariants of elliptic curves and an element $\lambda \in X(\mathbf{F}_{q^s})$ lying above j as a Legendre elliptic curve, $y^2 = x(x-1)(x-\lambda)$ with j-invariant j. So, for q large, the 'probability' that an $\mathbf{F}_q$ rational j-invariant is realised by an $\mathbf{F}_q$ rational Legendre elliptic curve is approximately 1/6.

3.3. *L*-functions of curves. Chavdarov [1] proved a conjecture of Katz that the proportion of curves whose L-function is irreducible in an algebraic family over $\mathbf{F}_q$ approaches 1 as q approaches infinity (provided the family has so-called 'big monodromy'). By combining Chebotarev's theorem and sieve theory, Kowalski obtained more precise bounds on the number of hyperelliptic curves in a family over $\mathbf{A}^1$ over $\mathbf{F}_q$ whose L function is not irreducible [5, page 178], making more explicit the results of Chavdarov. In addition, Kowalski gave bounds on the number of curves in such families whose number of $\mathbf{F}_q$ rational points is a square [5, page 193].

Appendix

This appendix establishes the result needed for the implicit constant, namely that for some N there is an embedding of X into $\mathbf{P}^N$ of degree δ such that all the twists X^g also admit embeddings into $\mathbf{P}^N$ of degree δ.

In this section k will be a field, K/k a finite Galois extension, X/k a quasi-projective variety and $G \subset \mathrm{Aut}(X_K)$ a finite group. We will call a variety X'/k a G-twist of X if for some finite Galois extension K/k there is an isomorphism

$$\Psi : X'_K \longrightarrow X_K$$

inducing a 1-cocycle

$$a_\sigma : \mathrm{Gal}(K/k) \to G : \sigma \mapsto ({}^\sigma\Psi) \circ \Psi^{-1}.$$

The cocycle a_σ defines a twisted action of $\mathrm{Gal}(K/k)$ on $X \times_{\mathrm{Spec}(k)} K$ by letting σ act as (a_σ, σ), and the quotient by this action is X'_K. Moreover, each 1-cocycle defines a twist of X (by [12, Ch. III, Proposition 5], as X is quasi-projective). If $G \subset \mathrm{Aut}(X_k)$ is considered as a constant group scheme over k, then a_σ defines a twisted action of $\mathrm{Gal}(K/k)$ on $G \times_{\mathrm{Spec}(k)} K$, which defines a twisted algebraic group G'/k isomorphic to G over K. The action of $G'(S)$ on $X'(S)$ is exactly the same as that of $G(S_K)$ on $X(S_K)$ as the former are respective subsets of the latter. There is an isomorphism between the quotients[2] $(X'/G')_K$ and $(X/G)_K$ induced by Ψ and the universal property of quotients, which descends to k as the action of G is trivial on the quotients.

Propositions A.1 and A.2 establish that there is an N so that if X' is any twist then X and X' both embed into $\mathbf{P}^N$ and are isomorphic over K under an element of $\mathbf{GL}_{N+1}(K)$.

[1] For λ being $\mathbf{F}_q$ rational means that φ_j is the identity element, so $|C| = 1$ and $|G| = 6$. Likewise λ being $\mathbf{F}_{q^2}$ rational means that φ_j is a 2-cycle, so $|C| = 3$, etc.

[2] That the quotients exist is shown on [10, page 105].

https://doi.org/10.1017/S0004972718000448 Published online by Cambridge University Press

Proposition A.1 is slightly more general than what we need, as it also applies to cases where some of the automorphisms of X are not defined over k (but are all defined over K).

Proposition A.1. *Let $\varphi : X \longrightarrow \mathbf{P}_k^N$. Let $\rho : G \longrightarrow \mathbf{GL}_{N+1}(K)$ be a group homomorphism compatible with φ. If X' is a G-twist of X, then there is an embedding of X' into $\mathbf{P}_K^N$ and an element $\gamma \in \mathbf{GL}_{N+1}(K)$ inducing an isomorphism between X'_K and X_K. In particular, if X has degree δ under φ, then X' does too.*

Proof. Let $\Psi : X'_K \longrightarrow X_K$ be an isomorphism and let a_σ be the corresponding 1-cocycle. It follows that X' is determined, up to k-isomorphism, by the class of $a_\sigma \in \mathrm{H}^1(\mathrm{Gal}(K/k), G)$. It therefore suffices to show two things:

(i) every element of $\mathrm{H}^1(\mathrm{Gal}(K/k), G)$ has the form $({}^\sigma\gamma)\gamma^{-1}$ for some $\gamma \in \mathbf{GL}_{N+1}(K)$;

(ii) if $a_\sigma = ({}^\sigma\gamma)\gamma^{-1}$, then there is an embedding $X' \subset \mathbf{P}_k^N$ and γ gives an isomorphism between X'_K and X_K.

For (i), ρ induces a morphism

$$\mathrm{H}^1(\mathrm{Gal}(K/k), G) \to \mathrm{H}^1(\mathrm{Gal}(K/k), \mathbf{GL}_{N+1}(K))$$

and the latter is trivial by Hilbert's theorem 90 [11, Proposition 3, page 151].

For (ii), let $a_\sigma = ({}^\sigma\gamma)\gamma^{-1}$ be a 1-cocycle, let $x_0, \dots, x_N$ be the homogeneous coordinate functions of $\mathbf{P}_k^N$, let $I_1 \subset k[x_0, \dots, x_N]$ be the homogeneous ideal defining the closure of X_k and let I_2 be the homogeneous ideal defining the closed variety $Z_k \subset \mathbf{P}_k^N$ such that $X_k = \bar{X}_k - Z_k$. Note that if $g \in \rho(G)$ and $F \in I_\epsilon$, then $F(gx_0, \dots, gx_N) \in I_\epsilon$, where $\epsilon \in \{1, 2\}$. Consider the twisted $\mathrm{Gal}(K/k)$ action on $K[x_0, \dots, x_N]$ given by letting $\sigma \in \mathrm{Gal}(K/k)$ act on x_i by $x_i \mapsto ({}^\sigma\gamma)\gamma^{-1}(x_i)$ and on $\lambda \in K$ by $\lambda \mapsto \sigma(\lambda)$. Let $y_i = \gamma^{-1}x_i$. Then y_i is invariant under the twisted action of $\mathrm{Gal}(K/k)$. Let $\{F_{1,\epsilon}, \dots, F_{m_\epsilon,\epsilon}\} \subset I_\epsilon$ be a set of $\rho(G)$-invariant generators. Put

$$H_{i,\epsilon}(y_0, \dots, y_N) = F_{i,\epsilon}(\gamma y_0, \dots, \gamma y_N).$$

Let X''_K be the variety defined by the locus of the $H_{i,1}$ with the locus of the $H_{i,2}$ removed. The set of $H_{i,\epsilon}$ is invariant under the twisted action of $\mathrm{Gal}(K/k)$ as

$$\begin{aligned}
\sigma(H_{i,\epsilon}(y_0, \dots, y_N)) &= \sigma(F_{i,\epsilon}(\gamma y_0, \dots, \gamma y_N)) \\
&= F_{i,\epsilon}(\sigma(\gamma)y_0, \dots, \sigma(\gamma)y_N) \\
&= F_{i,\epsilon}(({}^\sigma\gamma)\gamma^{-1}x_0, \dots, ({}^\sigma\gamma)\gamma^{-1}x_N) \\
&= F_{j,\epsilon}
\end{aligned}$$

for some j as $({}^\sigma\gamma)\gamma^{-1} \in \rho(G)$. Thus, X''_K descends to a variety X'' defined over k. Moreover, X''_K is isomorphic to X_K via γ and has a 1-cocycle a_σ. Therefore, $X'' \cong_k X'$. □

Proposition A.2. *There exists an N, an embedding $\varphi : X \longrightarrow \mathbf{P}_k^N$ and a group homomorphism $\rho : G \longrightarrow \mathbf{GL}_{N+1}(k)$ compatible with φ if the quotient X/G is a quasi-projective variety.*

https://doi.org/10.1017/S0004972718000448 Published online by Cambridge University Press

Proof. Let $f : X \longrightarrow Y$ be the quotient morphism. Since Y is quasi-projective, it has an ample line bundle L. The morphism f is finite (see, for example, [10, page 105]) and therefore f^*L is also an ample line bundle. This is because ample means that $\mathcal{F} \otimes (f^*L)^{\otimes n}$ is globally generated for sufficiently large n, but, as L is ample, $f_*\mathcal{F} \otimes L^{\otimes n}$ is globally generated and therefore so is $f^*f_*\mathcal{F} \otimes f^*L^{\otimes n}$. But the latter surjects onto $\mathcal{F} \otimes f^*L^{\otimes n}$ as f is finite and hence affine (see [9, page 39]).

Therefore, for some $n > 0$, the power $M = (f^*L^{\otimes n})$ is very ample. For any line bundle T over a variety Z, we let $[T]$ denote the geometric line bundle corresponding to T. So, $[T]$ is a scheme over Z, with structure morphism $p : [T] \longrightarrow Z$, such that there is an open cover U_i of Z and isomorphisms $\varphi_i : p^{-1}(U_i) \cong U_i \times \mathbf{A}^1$, so that $\varphi_i \circ \varphi^{-1}_{j|U_i \cap U_j} : U_i \cap U_j \times \mathbf{A}^1 \cong U_i \cap U_j \times \mathbf{A}^1$ respects the vector space structure of $\mathbf{A}^1$. The sections of p over any open set U are $T(U)$.

There is an equivalence between the category of geometric line bundles and line bundles. We will use the fact that $[f^*T] \cong [T] \times_Y X$. This follows as $[T]/Y$ is affine, so $[T] = \mathrm{Spec}(\mathcal{A})$ for some quasi-coherent $\mathcal{O}_Y$-algebra $\mathcal{A}$ (actually $\mathcal{A}$ is the symmetric algebra of T). So, $[f^*T] \cong \mathrm{Spec}(f^*\mathcal{A}) \cong \mathrm{Spec}(\mathcal{A}) \times_Y X$. See, for example, [13, Tags 01S5 and 01M1] or [3, Proposition 1.7.11, page 17].

In particular, $[M] \cong [L^{\otimes n}] \times_Y X$. There is an action of G on $[L^{\otimes n}] \times_Y X$ given by $g(a, x) = (a, gx)$, where $(a, x) \in [L^{\otimes n}] \times_Y X(S)$ and S/X is a scheme over X. Therefore, there is an action of G on M. The action on M induces an action of G on $\mathrm{H}^0(X, M)$ and a group homomorphism $\rho : G \longrightarrow \mathbf{GL}_{N+1}(k)$ which is compatible with the embedding

$$X \to \mathbf{P}(\mathrm{H}^0(X, M)) : x \mapsto [s_0(x) : s_1(x) : \cdots : s_N(x)],$$

where $N + 1$ is the dimension of $\mathrm{H}^0(X, M)$ as a k-vector space. □

References

[1] N. Chavdarov, 'The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy', *Duke Math. J.* **87** (1997), 151–180.

[2] M. Fried, 'The nonregular analogue of Tchebotarev's theorem', *Pacific J. Math.* **112** (1984), 303–311.

[3] A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique II. Étude globale élémentaire de quelques classes de morphismes*, Publications Mathématiques, 8 (IHES, Bures-sur-Yvette, 1961).

[4] M. Kosters, 'A short proof of the Chebotarev density theorem for function fields', *Math. Commun.* **22** (2017), 1–7.

[5] E. Kowalski, *The Large Sieve and its Applications: Arithmetic Geometry, Random Walks and Discrete Groups* (Cambridge University Press, Cambridge, 2008).

[6] S. Lang, 'Sur les séries L d'une variété algébrique', *Bull. Soc. Math. France* **84** (1956), 335–407.

[7] S. Lang, *Algebra*, revised third edn (Springer, New York, 2002).

[8] S. Lang and A. Weil, 'Number of points of varieties in finite fields', *Amer. J. Math.* **76**(4) (1954), 819–827.

[9] D. Mumford, *Lectures on Curves on an Algebraic Surface* (Princeton University Press, Princeton, NJ, 1966).

[10] D. Mumford, *Abelian Varieties* (Hindustan Book Agency, New Delhi, 2008).

[11] J.-P. Serre, *Local Fields* (Springer, New York, 1979).

[12] J.-P. Serre, *Cohomologie Galoisienne*, cinquième éd., Lecture Notes in Mathematics, 5 (Springer, Berlin, 1997).
[13] The Stacks Project, http://stacks.math.columbia.edu, 2017.

STEVE MEAGHER, School of Mathematics and Statistics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: sjmeagher@gmail.com

https://doi.org/10.1017/S0004972718000448 Published online by Cambridge University Press