Mathematical Research Letters **6**, 613–624 (1999)

SPACE FILLING CURVES OVER FINITE FIELDS

Nicholas M. Katz

Introduction

In this note, we construct curves over finite fields which have, in a certain sense, a "lot" of points, and give some applications to the zeta functions of curves and abelian varieties over finite fields. In fact, we found the basic construction, given in Lemma 1, of curves in $\mathbb{A}^n$ which go through every rational point, as part of an unsuccessful attempt to find curves of growing genus over a fixed finite field with lots of points in the sense of the Drinfield-Vladut bound [2]. The idea of applying that construction along the lines of this note grew out of an August 1996 conversation with Ofer Gabber about whether every abelian variety over a finite field was a quotient of a Jacobian, during which he constructed, on the fly, a proof of that fact. A variant of his proof appears here in Theorem 11. It is a pleasure to acknowledge my debt to him.

The basic constructions

Lemma 1. *Let k be a finite field, p its characteristic, $\bar{k}$ an algebraic closure of k, E/k a finite extension inside $\bar{k}$, and $n \geq 1$ an integer. There exists a smooth, geometrically connected curve C/k and a closed immersion of k-schemes*

$$C \subset \mathbb{A}^n \otimes_{\mathbb{Z}} k$$

which induces a bijection of E-valued points

$$C(E) = \mathbb{A}^n(E).$$

Construction-proof. If $n = 1$, take $C = \mathbb{A}^n \otimes_{\mathbb{Z}} k$. If $n = r + 1$ with $r \geq 1$, choose a sequence of r nonzero polynomials in one variable over k, $f_1(X), \dots, f_r(X)$, with the following three properties:

1) For each i, $f_i(x) = 0$ for every $x \in E$.
2) For each i, the degree d_i of f_i is prime to p.
3) The degrees are strictly increasing: $d_1 < d_2 < \cdots < d_r$.

[Here is a simple way to make such a choice. Write $q := \#E$, and pick a strictly increasing sequence of r positive integers each of which is prime to p, say $e_1 < e_2 < \cdots < e_r$. Then take each $f_i(X) := (X^q - X)X^{e_i}$.]

Received March 4, 1999.

In $\mathbb{A}^{r+1} \otimes k$ with coordinates $X, Y_1, \dots, Y_r$, consider the closed subscheme C/k defined by the r equations

$$(Y_i)^q - Y_i = f_i(X), \qquad i = 1, \dots, r.$$

It is obvious from these equations that every E-valued point of $\mathbb{A}^n$ lies in C. We must see that C/k is a smooth curve which is geometrically connected.

First of all, C/k is a smooth curve, for it is the fibre product over $\mathbb{A}^1 \otimes k$ of r finite etale galois coverings $\mathcal{E}_i \to \mathbb{A}^1 \otimes k$, with $\mathcal{E}_i$ the affine plane curve $(Y)^q - Y = f_i(X)$ in $\mathbb{A}^2 \otimes k$.

It remains to see that $C \otimes_k \bar{k}$ is connected. This results from Artin-Schreier theory. On $\mathbb{A}^1 \otimes \bar{k}$, or indeed on any smooth, affine, connected scheme $S/\bar{k}$, the Artin-Schreier sequence relative to q,

$$0 \to E \to \mathcal{O}_S \xrightarrow{f \mapsto \mathcal{P}(f) := f^q - f} \mathcal{O}_S \to 0$$

gives, via the long exact cohomology sequence, an isomorphism of E-vector spaces

$$H^0(S, \mathcal{O}_S)/\mathcal{P}(H^0(S, \mathcal{O}_S)) \cong H^1_{\mathrm{et}}(S, E) = \mathrm{Hom}(\pi_1(S), E).$$

Given f in $H^0(S, \mathcal{O}_S)$, the covering of S defined by $Y^q - Y = f$ (in $\mathbb{A}^1 \times S$) is finite etale galois with group E (α in E translates Y), so “is” an element $\mathrm{Class}(f)$ in $\mathrm{Hom}(\pi_1(S), E)$.

Now return to the case when S is $\mathbb{A}^1 \otimes \bar{k}$ and take any nontrivial $\mathbb{C}$-valued character ψ of E. If f in $\bar{k}[X]$ has degree d prime to p, then the composite homomorphism is known [1, 3.5.4] to have Swan conductor d at ∞.

Our $C \otimes_k \bar{k}$ is a finite etale galois covering of $\mathbb{A}^1 \otimes \bar{k}$ with group $E \times E \times \cdots \times E = E^r$, corresponding to the r-tuple $(f_1, f_2, \dots, f_r)$ via

$$\left(\bar{k}[X]/\mathcal{P}(\bar{k}[X])\right)^r \cong H^1_{\mathrm{et}}(\mathbb{A}^1 \otimes \bar{k}, E^r) = \mathrm{Hom}(\pi_1(S), E^r).$$

The total space $C \otimes_k \bar{k}$ of this covering is connected if and only if the corresponding homomorphism

$$\mathrm{Class}(f_1, f_2, \dots, f_r) : \pi_1(\mathbb{A}^1 \otimes \bar{k}) \to E^r$$

is surjective, or equivalently (Pontrajagin duality!) if and only if for every nontrivial $\mathbb{C}$-valued additive character $(\psi_1, \psi_2, \dots, \psi_r)$ of E^r, the composite homomorphism

$$(\psi_1, \psi_2, \dots, \psi_r) \circ \mathrm{Class}(f_1, f_2, \dots, f_r) : \pi_1(\mathbb{A}^1 \otimes \bar{k}) \to \mathbb{C}^\times,$$

is nontrivial. But this composite is just the product

$$(\psi_1, \psi_2, \dots, \psi_r) \circ \mathrm{Class}(f_1, f_2, \dots, f_r) = \prod_i \mathcal{L}_{\psi_i}(f_i).$$

In this product, $\mathcal{L}_{\psi_i}(f_i)$ is trivial if ψ_i itself is trivial, and $\mathcal{L}_{\psi_i}(f_i)$ has $\mathrm{Swan}_\infty = d_i$ if ψ_i is nontrivial. Because the d_i are all distinct, and at least one ψ_i is nontrivial, we have

$$\mathrm{Swan}_\infty\left(\prod_i \mathcal{L}_{\psi_i}(f_i)\right) = \mathrm{Sup}_{i \text{ with } \psi_i \text{ nontriv}}(d_i) > 0.$$

Hence $\prod_i \mathcal{L}_{\psi_i}(f_i)$ must be nontrivial. □

Lemma 2. *Let k be a finite field, X/k projective (resp. quasi-projective), smooth, and geometrically connected of dimension $n \geq 1$. Let E/k be a finite extension. There exists an affine (resp. quasi-affine) open set $U \subset X$ which contains all the E-valued points of X, i.e., $U(E) = X(E)$.*

Proof. To fix ideas, say $X \subset \mathbb{P}^N \otimes k$. We need only construct an affine open set U in $\mathbb{P}^N \otimes k$ which contains all the E-valued points of $\mathbb{P}^N \otimes k$, for then $X \cap U$ is the desired affine (resp. quasi-affine) open set of X. To do this, denote by K/E the field extension of degree $N+1$, and pick a basis $\alpha_0, \alpha_1, \ldots, \alpha_N$ of K/E. Denote by H the form of degree $N+1$ in $X_0, \ldots, X_N$ with coefficients in E defined by

$$H(X\text{'s}) := \mathrm{Norm}_{K/E}\left(\alpha_0 X_0 + \cdots + \alpha_N X_N\right).$$

Then H is nonzero at every E-valued point of $\mathbb{P}^N$. For each σ in $\mathrm{Gal}(E/k)$, the form H^σ has the same property (indeed, if we extend σ to an element $\tilde{\sigma}$ in $\mathrm{Gal}(K/k)$ which induces σ, then $\tilde{\sigma}(\alpha_0, \alpha_1, \ldots, \alpha_N)$ is another basis of K/E, and H^σ is its norm form to E). So $\mathrm{Norm}_{E/k}(H)$ is a form with coefficients in k which is nonzero at every E-valued point of $\mathbb{P}^N$. We may take for U the affine open set $(\mathbb{P}^N \otimes k)\left[1/\mathrm{Norm}_{E/k}(H)\right]$. □

Lemma 3. *Let k be a finite field, U/k a quasi-affine, smooth, and geometrically connected of dimenstion $n \geq 1$. Let E/k be a finite extension. There exists an open set $V \subset U$ which contains all the E-valued points of U and which admits an etale map to $\mathbb{A}^n \otimes k$.*

Proof. Say U is open in the affine scheme $\bar{U}$. First view $U(E)$ as a finite closed subscheme Z of U, by grouping its points into orbits under $\mathrm{Gal}(E/k)$. More precisely, Z is the disjoint union of the finitely many closed points of U the degree over k of whose residue fields divides $\deg(E/k)$, with its reduced structure. Thus, Z is a closed subscheme of U which is finite etale over k. This same Z is closed in $\bar{U}$, since we may describe it as the disjoint union of the finitely many closed points of $\bar{U}$ whose residue field degrees over k divide $\deg(U/k)$ and which lie in U. Denote by A the coordinate ring of $\bar{U}$, $I \subset A$ the ideal defining Z. At each point P in Z, pass to the local ring $\mathcal{O}_{\bar{U},P}$ of P in $\bar{U}$, and pick n elements $f_{1,P}, f_{2,P}, \ldots, f_{n,P}$ which form a $k(P)$-basis of $\mathbf{m}/\mathbf{m}^2$, $\mathbf{m}$ the maximal ideal. The ring A/I^2 is just the product ring $\prod_{P \in Z} \mathcal{O}_{\bar{U},P}/\mathbf{m}^2$. So, we can find functions $f_1, \ldots, f_n$ in A such that, for each i and each P, f_i induces $f_{i,P}$ in $\mathcal{O}_{\bar{U},P}/\mathbf{m}^2$. Restrict each function f_i to U, and view $(f_1, \ldots, f_n)$ as a map π of U to $\mathbb{A}^n$. This map π is etale at each point P in Z by construction. Thus, the set V of points of U at which π is etale is open, and contains Z. □

Lemma 4. *Let k be a finite field, V/k smooth and geometrically connected of dimension $n \geq 1$, and*

$$\pi : V \to \mathbb{A}^n \otimes k$$

an etale map of k-schemes. For each integer $r \geq 1$, denote by k_r the extension field of k inside $\bar{k}$ of degree r over k. For each $r \geq 1$, apply Lemma 1 with $E := k_r$ to produce a closed immersion

$$i_r : C_r/k \hookrightarrow \mathbb{A}^n \otimes k,$$

with C_r/k a smooth, geometrically connected curve such that

$$C_r(k_r) = \mathbb{A}^n(k_r).$$

Form the fibre product

$$\begin{array}{ccc} D_r := C_r \times_{\mathbb{A}^n \otimes k} V & \xrightarrow{i} & V \\ \downarrow & & \downarrow \pi \\ C_r & \xhookrightarrow{i_r} & \mathbb{A}^n \otimes k. \end{array}$$

1) *For every r, D_r/k is a smooth curve, space-filling in V for k_r, i.e., via the closed immersion*

$$i : D_r := C_r \times_{\mathbb{A}^n \otimes k} V \longrightarrow V,$$

we have

$$D_r(k_r) = V(k_r).$$

2) *For all sufficiently large r, D_r/k is geometrically connected.*

Proof. 1) is obvious from the cartesian diagram defining D_r, in which π is etale, C_r/k is a smooth curve, and i_r is surjective on k_r-valued points.

To prove 2), we argue as follows. The etale map π need not be finite etale, but there is a dense open set $j : W \hookrightarrow \mathbb{A}^n \otimes k$ over which π is finite etale (just because π is finite etale over the generic point of $\mathbb{A}^n \otimes k$). Take the entire diagram

$$\begin{array}{ccc} D_r := C_r \times_{\mathbb{A}^n \otimes k} V & \xrightarrow{i} & V \\ \downarrow & & \downarrow \pi \\ C_r & \xhookrightarrow{i_r} & \mathbb{A}^n \otimes k. \end{array}$$

in the category of $\mathbb{A}^n \otimes k$-schemes, and pull it back to the open set W, i.e., base change it by $j : W \hookrightarrow \mathbb{A}^n \otimes k$. We get a diagram

$$\begin{array}{ccc} D_{r,W} & \xrightarrow{i_W} & V_W \\ \downarrow & & \downarrow \pi \\ C_{r,W} & \xhookrightarrow{i_{r,W}} & W \\ \downarrow j_r & & \downarrow j \\ C_r & \xhookrightarrow{i_r} & \mathbb{A}^n \otimes k \end{array}$$

In this diagram, both W and V_W are smooth over k and geometrically connected, π is finite etale, and $i_{r,W} : C_{r,W} \hookrightarrow W$ is spacefilling for k_r. Now $C_{r,W}$ is open in C_r, so it is either dense and open in C_r and itself geometrically connected, or it is empty. For large r, $C_{r,W}$ is not empty, because $W(k_r)$ is nonempty for large r (by Lang-Weil, because W/k is geometrically irreducible), and $i_{r,W} : C_{r,W} \hookrightarrow W$ is spacefilling for k_r. Let us temporarily admit the truth of

Lemma 5. *Let k be a finite field, $\mathcal{E}/k$ and W/k two smooth, geometrically connected k-schemes of the same dimension $n \geq 1$, and*

$$\begin{array}{c} \mathcal{E} \\ \downarrow{\scriptstyle \pi} \\ W \end{array}$$

a finite etale k-morphism. Suppose given an integer $r_0 \geq 1$, and for all integers $r \geq r_0$, a smooth, geometrically connected curve $\mathcal{C}_r/k$ and a closed k-immersion $i_r : \mathcal{C}_r \to W$ which is spacefilling for k_r, i.e., $\mathcal{C}_r(k_r) = W(k_r)$. Form the fibre product

$$\begin{array}{ccc} \mathcal{D}_r & \xrightarrow{i_{r,\mathcal{E}}} & \mathcal{E} \\ \downarrow & & \downarrow{\scriptstyle \pi} \\ \mathcal{C}_r & \xrightarrow{i_{r,W}} & W \end{array}$$

Then for r sufficiently large, the curve $\mathcal{D}_r/k$ is geometrically connected.

Applying this lemma to our situation ($\mathcal{E}$ is V_W, $\mathcal{C}_r$ is $C_{r,W}$), we find that for large r, $D_{r,W}$ is geometrically connected. We wish to infer that D_r/k itself is geometrically connected. If it is not, then $D_r \otimes_k \bar{k}$ is a union of two or more connected components, each of which is etale over $C_r \otimes_k \bar{k}$. But as etale maps are open, the image of each connected component meets the dense open set $C_{r,W} \otimes_k \bar{k}$, and hence $D_{r,W} \otimes_k \bar{k}$ is not connected, contradiction. QED for Lemma 4 modulo Lemma 5. □

Proof of Lemma 5. Fix a geometric point ω in $W \otimes_k \bar{k}$, and view the finite etale covering $\pi : \mathcal{E} \to W$ as an action of the group $\pi_1(W, \omega)$ on the finite set $S := \pi^{-1}(\omega)$, i.e., a homomorphism

$$\rho : \pi_1(W, \omega) \to \mathrm{Aut}(S).$$

The geometric connectedness of $\mathcal{E}$ means precisely that via this action, the subgroup

$$\pi_1^{\mathrm{geom}}(W, \omega) := \pi_1(W \otimes_k \bar{k}, \omega) \subset \pi_1(W, \omega)$$

acts transitively on S. Recall the short exact sequence

$$1 \to \pi_1^{\mathrm{geom}}(W,\omega) \to \pi_1(W,\omega) \xrightarrow{\text{degree}} \mathrm{Gal}(\bar{k}/k) \to 1$$
$$\| $$
$$\hat{\mathbb{Z}}$$

Denote by

$$\Gamma_{\mathrm{geom}} \subset \Gamma \subset \mathrm{Aut}(S)$$

the images in $\mathrm{Aut}(S)$ of $\pi_1^{\mathrm{geom}}(W,\omega)$ and of $\pi_1(W,\omega)$ respectively under ρ. The quotient $\Gamma/\Gamma_{\mathrm{geom}}$ is cyclic, say of order N, generated by $\rho(F)$ for any fixed element F in $\pi_1(W,\omega)$ of degree 1. For each i in $\mathbb{Z}/N\mathbb{Z}$, denote by $\Gamma(i) \subset \Gamma$ the set of elements whose degree mod N is i, i.e., $\Gamma(i)$ is the coset $\rho(F^i)\Gamma_{\mathrm{geom}}$.

By Chebotarev (cf., [5, 9.7.13]) for every $r \gg 0$, we have:

($**r$, $\mathcal{E}/W$) The images under ρ of all degree r Frobenius elements in $\pi_1(W,\omega)$, i.e., all elements in all Frobenius conjugacy classes

$$\mathrm{Frob}_{k_r,w} \text{ in } \pi_1(W,\omega)$$

attached to k_r-valued points w of W, fill the coset $\Gamma(r)$.

We will show that for any $r \geq r_0$ large enough that ($**r$, $\mathcal{E}/W$) holds, $\mathcal{D}_r$ is geometrically connected. To see this, pick a geometric point c_r in $\mathcal{C}_r$, take for ω its image in W, and consider the composite homomorphism

$$\pi_1(\mathcal{C}_r, c_r) \xrightarrow{\pi_1(i_{r,W})} \pi_1(W,\omega) \xrightarrow{\rho} \Gamma \subset \mathrm{Aut}(S),$$

which we label

$$\rho_r : \pi_1(\mathcal{C}_r, c_r) \to \Gamma \subset \mathrm{Aut}(S).$$

Now $\mathcal{D}_r/k$ is geometrically connected if and only if the subgroup

$$\rho_r\left(\pi_1^{\mathrm{geom}}(\mathcal{C}_r, c_r)\right) \subset \mathrm{Aut}(S)$$

acts transitively on S. A sufficient condition for this transitivity is that

$$(*r) \qquad \rho_r\left(\pi_1^{\mathrm{geom}}(\mathcal{C}_r, c_r)\right) = \Gamma_{\mathrm{geom}},$$

(because the geometric connectedness of $\mathcal{E}$ means that Γ_{geom} acts transitively).

A sufficient condition for

$$\rho_r(\pi_1^{\mathrm{geom}}(\mathcal{C}_r, c_r)) = \Gamma_{\mathrm{geom}},$$

is that the condition ($**r$, $\mathcal{D}_r, \mathcal{C}_r$) hold:

($**r$, $\mathcal{D}_R, \mathcal{C}_r$) The images under ρ_r of all the Frobenius elements of degree r in $\pi_1(\mathcal{C}_r, c_r)$ fill $\Gamma(r)$.

Indeed, every element in $\Gamma_{\mathrm{geom}} := \Gamma(0)$ is of the form $A^{-1}B$ with A and B in $\Gamma(r) = \rho(F^r)\Gamma_{\mathrm{geom}}$, and hence every element of Γ_{geom} will be the image under ρ_r of a ratio $(\mathrm{Frob}_{k_r,x})^{-1}(\mathrm{Frob}_{k_r,y})$ for two points x and y in $\mathcal{C}_r(k_r)$. Such a ratio lies in $\pi_1^{\mathrm{geom}}(\mathcal{C}_r, c_r)$.

But $\mathcal{C}_r(k_r) = W(k_r)$ by assumption, so every degree r Frobenius element in $\pi_1(W,\omega)$ is the image under $\pi_1(i_{r,W})$ of a degree r Frobenius element in

$\pi_1(\mathcal{C}_r, c_r)$. Therefore $(**r,\ \mathcal{D}_r/\mathcal{C}_r)$ is equivalent to $(**r,\ \mathcal{E}/W)$. In particular, for large r, $(**r,\ \mathcal{D}_r/\mathcal{C}_r)$ and hence $(*r)$ hold. □

With an eye to later applications, we extract from the proof of Lemma 5 the following variant.

Lemma 6. *Let k be a finite field, W/k a smooth, geometrically connected k-scheme, and w a geometric point of W. Suppose given an integer $r_0 \geq 1$, and, for each integer $r \geq r_0$, a smooth geometrically connected k-scheme $\mathcal{C}_r/k$ and a k-morphism*

$$f_r : \mathcal{C}_r \to W$$

which is surjective on k_r-valued points. For each $r \geq r_0$, pick a geometric point c_r in $\mathcal{C}_r$, and a "chemin" from $f_r(c_r)$ to w.

Suppose that G is either

1) *a finite group, or,*
2) $\mathrm{GL}(n, \mathcal{O}_\lambda)$ *for some positive integer n and for $\mathcal{O}_\lambda$ the ring of integers in a finite extension of $\mathbb{Q}_l$, for some prime number l.*
3) $\mathrm{GL}(n, \bar{\mathbb{Q}}_l)$ *for some n and some prime l.*

Suppose given a continuous group homomorphism

$$\rho : \pi_1(W, w) \to G.$$

We denote

$$\rho_r : \pi_1(\mathcal{C}_r, c_r) \to G$$

the composite homomorphism

$$\pi_1(\mathcal{C}_r, c_r) \xrightarrow{f_*} \pi_1(W, f(c_r)) \xrightarrow{\text{chemin}} \pi_1(W, w) \xrightarrow{\rho} G.$$

Then we have:

a) *For r sufficiently large, we have an equality of images of geometric fundamental groups*

$$\rho_r(\pi_1^{\text{geom}}(\mathcal{C}_r, c_r)) = \rho(\pi_1^{\text{geom}}(W, w))$$

(equality inside G).

b) *Suppose in addition that, for each $r \geq r_0$, f_r is also surjective on k_s-valued points for all divisors s of r. Then for r sufficiently large and sufficiently divisible, we have an equality of images of fundamental groups*

$$\rho_r(\pi_1(\mathcal{C}_r, c_r)) = \rho(\pi_1(W, w))$$

(equality inside G).

Proof. In case 1), G finite, we put $\Gamma := \rho(\pi_1(W, w))$, $\Gamma_{\text{geom}} := \rho(\pi_1^{\text{geom}}(W, w))$, denote by N the order of the cyclic group $\Gamma/\Gamma_{\text{geom}}$, and denote by $\Gamma(i)$ the set of elements in Γ of degree $i \mod N$. By Chebotarev, for $r \gg 0$, the Frobenii of k_r-valued points of W fill the coset $\Gamma(r)$, hence by the surjectivity of the map f_r on k_r-valued points, so do the Frobenii of k_r-valued points of $\mathcal{C}_r$ for $r \gg 0$. For these r, the $A^{-1}B$ argument shows that ratios $A^{-1}B$ of such Frobenii fill Γ_{geom}, whence a).

For b), we argue as follows. For each integer i in $[0, N-1]$ pick an integer $d_i \equiv i \mod N$ and sufficiently large that the Frobenii of k_{d_i}-valued points of W fill the coset $\Gamma(i)$. Then for any $r \geq r_0$ which is divisible by $\prod_i d_i$, the Frobenii of the points on $\mathcal{C}_r$ with values in k_{d_i} for $i = 0, 1, \ldots, N-1$ fill Γ.

For case 2), put $K :=$ the image $\rho(\pi_1^{\mathrm{geom}}(W, w))$ in $\mathrm{GL}(n, \mathcal{O}_\lambda)$. By Pink's Lemma [4, 8.18.3], there exists an integer $d \geq 1$ such that a closed subgroup H of K is equal to K if and only if H and K have the same image in $\mathrm{GL}(n, \mathcal{O}_\lambda / l^d \mathcal{O}_\lambda)$.

For each integer $r \geq r_0$, put $H_r :=$ the image $\rho_r(\pi_1^{\mathrm{geom}}(\mathcal{C}_r, c_r))$ in $\mathrm{GL}(n, \mathcal{O}_\lambda)$. Thus H_r is a closed subgroup of K. By case 1), applied to the reduction mod l^d of ρ, for $r \gg 0$, H_r and K have the same image in $\mathrm{GL}(n, \mathcal{O}_\lambda / l^d \mathcal{O}_\lambda)$. So by Pink's Lemma $H_r = K$ for all such r.

For b), apply Pink's Lemma to $L :=$ the image $\rho(\pi_1(W, w))$ in $\mathrm{GL}(n, \mathcal{O}_\lambda)$ and the subgroups $J_r :=$ the image $\rho_r(\pi_q(\mathcal{C}_r, c_r))$ in $\mathrm{GL}(n, \mathcal{O}_\lambda)$ to reduce b) to case 1).

For case 3), use the fact [5, 9.0.7] that any compact subgroup of $\mathrm{GL}(n, \bar{\mathbb{Q}}_l)$, in particular the image $\rho(\pi_1(W, w))$, is conjugate to a closed subgroup of $\mathrm{GL}(n, \mathcal{O}_\lambda)$ for $\mathcal{O}_\lambda$ the ring of integers in some finite extension E_λ of $\mathbb{Q}_l$ to reduce to case 2). □

As an immediate consequence of case 3) of Lemma 6, we get the following result of Bertini type.

Corollary 7. *Let k be a finite field, W/k a smooth, geometrically connected k-scheme, and w a geometric point of W. Suppose given an integer $r_0 \geq 1$, and, for each integer $r \geq r_0$, a smooth, geometrically connected k-scheme $\mathcal{C}_r/k$ and a k-morphism*

$$f_r : \mathcal{C}_r \to W,$$

which is surjective on k_r-valued points. For each $r \geq r_0$, pick a geometric point c_r in $\mathcal{C}_r$, and a "chemin" from $f_r(c_r)$ to w. Let l be a prime number, and $\mathcal{F}$ a lisse $\bar{\mathbb{Q}}_l$-sheaf on W of rank denoted n, corresponding to a continuous homomorphism

$$\rho : \pi_1(W, w) \to \mathrm{GL}(n, \bar{\mathbb{Q}}_l).$$

Denote by $G_{\mathrm{geom}, \mathcal{F} \text{ on } W}$ the Zariski closure of $\rho(\pi_1^{\mathrm{geom}}(W, w))$ in $\mathrm{GL}(n) \otimes \bar{\mathbb{Q}}_l$. Then for r sufficiently large, the pullback sheaf $(f_r)^*(\mathcal{F})$ on $\mathcal{C}_r$ has the same G_{geom}:

$$G_{\mathrm{geom},\, (f_r)^*\mathcal{F} \text{ on } \mathcal{C}_r} = G_{\mathrm{geom},\, \mathcal{F} \text{ on } W}.$$

Moreover, if $\mathcal{F}$ on W has the property that $\rho(\pi_1(W, w))$ lies in $G_{\mathrm{geom},\, \mathcal{F} \text{ on } W}(\bar{\mathbb{Q}}_l)$, then for r sufficiently large the pullback sheaf $(f_r)^*(\mathcal{F})$ on $\mathcal{C}_r$ has the same property, that $\rho(\pi_1(\mathcal{C}_r, c_r))$ lies in $G_{\mathrm{geom},\, (f_r)^*\mathcal{F} \text{ on } \mathcal{C}_r}(\bar{\mathbb{Q}}_l)$.

Theorem 8. *Let k be a finite field, X/k smooth and quasi-projective and geometrically connected, of dimension $n \geq 1$. Let E/k be a finite extension. There exists a smooth, geometrically connected curve C_0/k, and an immersion $\pi : C_0 \to X$ which is bijective on E-valued points.*

Proof. First apply Lemmas 2 and 3 to find an open set V in X which contains all the E-valued points and which admits an etale map π to $\mathbb{A}^n \otimes k$. Let $d :=$ degree(E/k), so E is k_d. For each $r \geq 1$, use Lemma 1 to find a smooth, geometrically connected curve C_{rd}/k in $\mathbb{A}^n \otimes k$ which is spacefilling for k_{rd}. Take D_{rd}/k in V to be the fibre product

$$D_{rd} := C_{rd} \times_{\mathbb{A}^n \otimes k} V.$$

By Lemma 4, for large r this closed subscheme D_{rd} of V is a smooth, geometrically connected curve over k which is spacefilling for k_{rd}. Taking the $\mathrm{Gal}(k_{rd}/k_d)$-invariants on both sides of the equality $D_{rd}(k_{rd}) = V(k_{rd})$, we get $D_{rd}(k_d) = V(k_d)$, or in other words D_{rd} is spacefilling in V for E. The composite inclusion $D_{rd} \subset V \subset X$ is the desired immersion. □

Corollary 9. *Let k be a finite field, X/k projective, smooth, and geometrically connected, of dimension $n \geq 1$. Let E/k be a finite extension. There exists a proper, smooth, geometrically connected curve C/k, and a k-morphism $\pi : C \to X$ which is surjective on E-valued points. Moreover,*

1) *there is an open dense set U in C such that $\pi|U : U \to X$ is bijective on E-valued points,*
2) *π is birationally an isomorphism of C with its image $\pi(C)$ taken with the induced reduced structure.*

Proof. Apply Theorem 8 to get $\pi : C_0 \to X$, and then take C/k to be the complete nonsingular model of C_0/k. Take U to be C_0. Because X/k is proper, the map π extends to a k-morphism $\bar{\pi} : C \to X$ with all the asserted properties. □

Question 10. Given X/k projective, smooth, and geometrically connected of dimension $n \geq 2$, and E/k a finite extension, is there always a closed subscheme Y in X, $Y \neq X$, such that $Y(E) = X(E)$ and such that Y/k is smooth and geometrically connected? What, if any, is the obstruction to the existence of such Y? For example, take for X an odd dimensional projective space $\mathbb{P}^{2n+1}$, $n \geq 1$ with homogeneous coordinates X_i and Y_i for $i = 1, \ldots, n+1$. Write $q := \mathrm{Card}(E)$ and take for Y the smooth hypersurface $\mathrm{Hyp}(2n+1, q)$ of degree $q+1$:

$$\mathrm{Hyp}(2n+1, q) : \sum_i (X_i(Y_i)^q - (X_i)^q Y_i) = 0.$$

But what to do for $\mathbb{P}^{2n}$? Take the "easy" case $k = E$ $(= \mathbb{F}_q)$. One idea is to view $\mathbb{P}^{2n}$ as an $\mathbb{F}_q$-rational hyperplane section $L = 0$ of $\mathbb{P}^{2n+1}$, and then take its Y to be $L \cap \mathrm{Hyp}(2n+1, q)$. This idea does not work, because the Gauss map for $\mathrm{Hyp}(2n+1, q)$ is

$$(X_i, Y_i)\text{'s} \mapsto ((Y_i)^q, -(X_i)^q)\text{'s} = \mathrm{Frob}_q((Y_i, -X_i)\text{'s}).$$

The map

$$(X_i, Y_i)\text{'s} \mapsto (Y_i, -X_i)\text{'s}$$

is an involution of $\mathrm{Hyp}(2n+1,q)$. Thus $\mathrm{Hyp}(2n+1,q)$ is its own dual variety, cf., [8, XVII, 3.4]. Exactly because $\mathrm{Hyp}(2n+1,q)$ contains all the $\mathbb{F}_q$-valued points in $\mathbb{P}^{2n+1}$, there are no $\mathbb{F}_q$-rational hyperplanes L in $\mathbb{P}^{2n+1}$ which are transverse to $\mathrm{Hyp}(2n+1,q)$!

The simplest form of the question is this: in $\mathbb{P}^2/\mathbb{F}_q$, is there a smooth plane curve $C/\mathbb{F}_q$ which goes through all the $\mathbb{F}_q$-points of $\mathbb{P}^2$?

Applications to abelian varieties and to zeta functions of curves

Theorem 11. *Let k be a field, A/k an abelian variety of dimension $g \geq 1$. There exists a proper, smooth, geometrically connected curve C/k, a k-valued point O_C in $C(k)$, and a k-morphism*

$$\pi : C \to A,$$

which maps the point O_C on C to the origin O_A on A, and whose Albanese map

$$\begin{array}{c} \mathrm{Alb}(\pi) : \mathrm{Alb}(C/k, 0_C) \twoheadrightarrow A \\ \| \\ \mathrm{Jac}(C/k) \end{array}$$

is surjective. Moreover, if the field k is infinite, there exists such data with π a closed immersion.

Proof. We first treat the well known case when the field k is infinite. The proof we give in this case (cf., [6, 10.1] for a variant) is quite simple. We give it both for the reader's convenience and because it conceivably could be made to work over a finite field as well, see Question 13 below. It depends on the following geometric fact:

Lemma 12. *In $\mathbb{P}^N$ over an infinite field k, let X/k be a closed subscheme which is smooth and geometrically connected, of dimension $n \geq 1$. Given an point P in $X(k)$ and an integer $d \geq 2$, there exists a hypersurface H/k of degree d in $\mathbb{P}^N$ such that P lies on H and such that $X \cap H$ is smooth of dimension $n-1$.*

Proof. Denote by $\mathcal{H}$ the projective space of all degree d hypersurfaces in $\mathbb{P}^N$. Inside $\mathcal{H}$, we have two subvarieties of particular interest:

1) the "dual variety" $\check{X}$ (of X for the d-fold Segre embedding, cf., [8, XVII, 2.4]), consisting of those degree d hypersurfaces H such that $X \cap H$ fails to be smooth of dimension $n-1$.
2) the hyperplane $\check{P}$ consisting of those degree d hypersurfaces which contain P.

We claim that $\check{P} - \check{P} \cap \check{X}$ has a k-point. Since $\check{P} - \check{P} \cap \check{X}$ is open in the projective space $\check{P}$ and the field k is infinite, $\check{P} - \check{P} \cap \check{X}$ is either empty or it has a k-point. [This comes down to the fact that if a k-polynomial in some number m of variables vanishes on k^m then it is the zero polynomial, provided k is infinite.] If $\check{P} - \check{P} \cap \check{X}$ is empty, then $\check{P} \subset \check{X}$. But the dual variety is irreducible of codimension at least one, cf., [8, XVII, 3.1.4], so $\check{P} = \check{X}$. Take homogeneous coordinates $X_0, \dots, X_N$ in which the point P is $(1, 0, 0, \dots, 0)$. The hypersurface $(X_0)^d = 0$ lies in $\check{X}$ but not in $\check{P}$, contradiction. □

To exhibit a g-dimensional abelian variety A over an infinite field k as the quotient of a Jacobian, embed A in projective space, pick $g-1$ integers $d_i \geq 2$, and successively intersect A with general hypersurfaces of degrees d_i defined over k which each contain the origin 0_A, to obtain a smooth curve C/k in A, defined over k, which contains 0_A. The "weak Lefschetz theorem" [7, VII, 7.1] on hypersurface sections tells us that for any prime l invertible in k, the restriction map

$$H^i(A \otimes_k \bar{k}, \mathbb{Q}_l) \to H^i(C \otimes_k \bar{k}, \mathbb{Q}_l),$$

is bijective for $i = 0$, so C/k is geometrically connected, and injective for $i = 1$. This injectivity for $i = 1$ implies that the Albanese map

$$\mathrm{Alb}(C, 0_A) \to A$$

is surjective.

The proof we give below, over a finite field, is due to Ofer Gabber. We do not know if the proof given above in the infinite field case can be made to work over a given finite field, say by taking the degrees d_i quite large, cf., Question 13 below.

Pick a prime number $l \neq p$, and a finite extension E/k such that each of the l^{2g} points in $A(\bar{k})$ of order dividing l lies in $A(E)$. Apply the previous corollary to produce a proper smooth geometrically connected curve C/k, an open set $U \subset C$, and a k-morphism

$$\pi : C \to A$$

such that $\pi|U$ is bijective on E-valued points: $U(E) \cong A(E)$ by π. Taking $\mathrm{Gal}(E/k)$-invariants, we see that $U(k) \cong A(k)$ by π. Take 0_C in $U(k)$ to be $(\pi|U)^{-1}(0_A)$.

The image of $\mathrm{Alb}(C/k, 0_C)$ in A is an abelian subvariety $B \subset A$. So $B(\bar{k})$ is a subgroup of $A(\bar{k})$. Hence $B(\bar{k}) \cap A(\bar{k})[l] = B(\bar{k})[l]$. But by construction we have

$$A(\bar{k})[l] \subset A(E) \cong \pi(U(E)) \subset \pi(C(\bar{k})) \subset B(\bar{k}).$$

Therefore $B(\bar{k})[l] = A(\bar{k})[l]$, hence $\#(B(\bar{k})[l]) = l^{2g}$. Therefore B has dimension g, so it must be all of A. □

Question 13. Suppose we are in the setting of Lemma 12, but over a finite field k. Thus in $\mathbb{P}^N$ over k, we are given a closed subscheme X/k which is smooth and geometrically connected, of dimension $n \geq 1$. Given a point P in $X(k)$, does there exist an integer $d \geq 2$ and a hypersurface H/k of degree d in $\mathbb{P}^N$ such that P lies on H and such that $X \cap H$ is smooth of dimension $n-1$? Does this hold for all $d \gg 0$?

Corollary 14. *Given a finite field k, and an abelian variety A/k, there exists a proper, smooth, geometrically connected curve C/k such that the characteristic polynomial of Frobenius on (H^1 of) A/k divides the characteristic polynomial of Frobenius on (H^1 of) C/k.*

Proof. Once the Albanese map is surjective, for $l \neq p$ we have a $\mathrm{Gal}(\bar{k}/k)$-equivariant inclusion

$$H^1(A \otimes_k \bar{k}, \mathbb{Q}_l) \subset H^1(\mathrm{Alb}(C/k, 0_C) \otimes_k \bar{k}, \mathbb{Q}_l) = H^1(C \otimes_k \bar{k}, \mathbb{Q}_l),$$

whence a divisibility of characteristic polynomials

$$\det(1 - TF_k | H^1(A \otimes_k \bar{k}, \mathbb{Q}_l) | \det(1 - TF_k | H^1(C \otimes_k \bar{k}, \mathbb{Q}_l)).$$

□

Corollary 15. *Suppose we are given an integer $r \geq 1$, a list of r Weil numbers α_i for $q := \#k$ (each α_i is an algebraic integer which has all its archimedean absolute values equal to* $\mathrm{Sqrt}(q)$*), and a list r positive integers n_i. There exists a proper, smooth, geometrically connected curve C/k whose zeta function has a zero of multiplicity at least n_i at the point $T = 1/\alpha_i$ for each $i = 1, \ldots, r$.*

Proof. By Honda-Tate ([3, 9]), there exists an abelian variety A_i/k on which α_i is an eigenvalue of Frobenius. Apply the previous corollary to the product abelian variety $\prod_i (A_i)^{n_i}$. □

References

[1] P. Deligne, *Application de la formule des traces aux sommes trigonométriques*, in *Cohomologie Étale (SGA $4\frac{1}{2}$)*, Springer Lecture Notes in Mathematics, 569, pp. 168–232, Springer-Verlag, Berlin-New York, 1977.

[2] V. Drinfeld, and S.G. Vladut, *The number of points of an algebraic curve*, Functional Anal. App. **17** (1983), 53–53.

[3] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

[4] N. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, 124, Princeton University Press, Princeton, NJ, 1990.

[5] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, 45, American Mathematical Society, Providence, RI, 1999.

[6] J.S. Milne, *Jacobian varieties*, in *Arithmetic Geometry*, (G. Cornell and J.H. Silverman, eds.), pp. 167–212, Springer, New York, 1986.

[7] *Séminaire de Géométrie Algébrique du Bois-Marie 1965–66*, *Cohomologie l-adique et Fonctions L*, Springer Lecture Notes in Mathematics, 589, Springer, New York, 1977.

[8] *Séminaire de Géométrie Algébrique du Bois-Marie 1967–69*, *Groupes de Monodromie en Géométrie Algébrique*, Springer Lecture Notes in Mathematics, 340, Springer, New York, 1973.

[9] J. Tate, *Classes d'Isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Exposé 352, Séminaire Bourbaki 1968/69.

Fine Hall, Department of Mathematics, Princeton University, Princeton NJ 08544
E-mail address: nmk@math.princeton.edu