ALGEBRAIC VARIETIES OVER PAC FIELDS

BY

János Kollár

Princeton University, Princeton NJ 08544-1000, USA
e-mail: kollar@math.princeton.edu

ABSTRACT

The paper answers problems 2 and 3 of the list of open problems in the
2005 edition of *Field Arithmetic* by M. D. Fried and M. Jarden.

A field is called *PAC* (pseudo algebraically closed) if every geometrically integral k-variety has a k-point. (A k-variety X is called geometrically integral if $X_{\bar{k}}$ is irreducible and reduced where $\bar{k}$ is an algebraic closure of k. This notion is also frequently called "absolutely irreducible.") These fields were introduced and studied in [Ax68]; see [FJ05] for an exhaustive and up to date treatment.

The aim of this paper is to settle questions 2 and 3 of the list of Open Problems in [FJ05, Sec. 32.2] about algebraic varieties over PAC fields.

THEOREM 1: *For a field k the following are equivalent:*

(1) *k is PAC.*
(2) *every absolutely irreducible homogeneous polynomial $f(x, y, z) \in k[x, y, z]$ has a nontrivial zero in k^3.*
(3) *every geometrically integral plane curve $C \subset \mathbb{P}^2_k$ has infinitely many k-points.*

THEOREM 2: *Let k be a PAC field, $\bar{k}$ an algebraic closure and v a nontrivial valuation of $\bar{k}$. Let X be a geometrically integral k-variety. Then $X(k)$ is dense in $X(\bar{k})$ in the v-adic topology.*

It is clear that (1.1) implies (1.2). The equivalence of (1.1) and (1.3) is known (cf. [FJ05, Sec. 11.2]). Thus we need to show that if k is not PAC then there is a geometrically integral plane curve $C \subset \mathbb{P}^2$ such that $C(k) = \emptyset$. This is done in Section 1.

The proof of Theorem 2 relies on a trick of Prestel (cf. [FJ05, 11.5.3]), which was used to show that $\mathbb{P}^1(k)$ is v-adically dense in $\mathbb{P}^1(\bar{k})$. The general case is proved in Section 2.

1. A characterization of PAC fields

We prove Theorem 1 in 6 steps.

STEP 1:   Finite fields.

If k is finite then (1.2) never holds. This is shown in [FJ05, 11.2.9]. For instance, $x^{q-1} + y^{q-1} + z^{q-1} = 0$ has no solutions in $\mathbb{F}_q$ whenever $q > 3$. So in the sequel we assume that k is an infinite field and there is a geometrically integral k-variety X such that $X(k) = \emptyset$.

STEP 2:   Reduction to a nonsingular projective curve.

This is known (cf. [Fre73]) but here is another short argument.

Let X be a geometrically integral k variety X such that $X(k) = \emptyset$. We may assume that X is affine. A general hypersurface section is a geometrically integral curve B such that $B(k) = \emptyset$. Let $\bar{B} \supset B$ denote a projective model. The problem is that $\bar{B} \setminus B$ may contain k-points.

The k-points of $\bar{B} \times \bar{B}$ are all contained in the finite set $(\bar{B} \setminus B) \times (\bar{B} \setminus B)$, thus a general hypersurface section $C_1 \subset \bar{B} \times \bar{B}$ is a geometrically integral projective curve such that $C_1(k) = \emptyset$. We can replace C_1 with its normalization $C \to C_1$ to get a nonsingular projective curve without k-points.

STEP 3:   Projecting to the plane.

If k is perfect then C is smooth. Embed C into some projective space $\mathbb{P}^n$ and project generically to $\mathbb{P}^2$. By a classical result (cf. [Har77, IV.3.10]), the general projection is a plane curve with only nodes as singularities.

If k is not perfect then C is nonsingular, but $C_{\bar{k}}$ may be singular, so it is more complicated to state the precise result. I thank M. Jarden for pointing out that I originally overlooked this. (I follow the terminology of [Har77, p. 177], according to which "nonsingular" means that the local rings are regular and "smooth" means that the module of differentials has the same dimension as the variety. If k is perfect, the two notions coincide.)

Choose a very ample line bundle L on C such that

$$h^0(C_{\bar{k}}, L(-p_1 - p_2 - p_3)) = h^0(C_{\bar{k}}, L) - 3 \quad \text{for every } p_i \in C_{\bar{k}},$$

and embed $C \hookrightarrow \mathbb{P}^n$ using the global sections of L. This condition implies that no 3 points of C are contained in a line and that no tangent line at a smooth

point has another intersection point with C. Let $\pi \colon C \to C' \subset \mathbb{P}^2$ be a general projection.

LEMMA 3: *Let k be an infinite field and $C \subset \mathbb{P}^n$ a nonsingular curve such that no 3 points of C are contained in a line and no tangent line at a smooth point of C intersects C in any other point. Let $\pi \colon C \to C' \subset \mathbb{P}^2$ be a general projection and $Q \subset C'_{\bar{k}}$ the set of points with at least 2 preimages (over $\bar{k}$). Then*

(1) *Q is finite,*

(2) *for every smooth point $q \in C' \setminus Q$, $k(\pi^{-1}(q)) = k(q)$,*

(3) *for every nonsmooth point $q \in C' \setminus Q$, $k(\pi^{-1}(q)) = k$ iff $k(q) = k$ and*

(4) *for every $q \in Q$, its preimage $\pi^{-1}(q)$ consists of 2 smooth points q_1, q_2 such that $k(q_i)/k(q)$ is separable and of degree ≤ 2.*

Proof: The center of the projection is a general linear space $M^{n-3} \subset \mathbb{P}^n$. We show how a general choice of M assures the above properties.

The secant lines fill out a 3-dimensional subset, and the general M intersects only finitely many secant lines, proving (1).

The tangent lines at smooth points of $C_{\bar{k}}$ fill out a surface, so M can be taken to be disjoint from it. Thus π is unramified at all smooth points of C which implies (2).

There are finitely many singular points $c_i \in C_{\bar{k}}$ (no such points if k is perfect). Let L_i be the smallest linear subspace defined over k such that $c_i \in L_i$. Since C is nonsingular, c_i is not a k-point thus $\dim L_i \geq 1$. Then $\pi(c_i)$ is a k-point iff $\pi(L_i)$ is a k-point iff $M \cap L_i$ has codimension 1 in L_i. For M general, $M \cap L_i$ has codimension 3 in L_i, proving (3).

Given $p_1, p_2, p_3 \in C_{\bar{k}}$, their linear span is a plane P. Thus $\pi(p_1) = \pi(p_2) = \pi(p_3)$ only if $\dim(P \cap M) \geq 1$. For each P, the latter condition is satisfied by a codimension 4 subset of all M^{n-3}. The triplets (p_1, p_2, p_3) are parametrized by C^3, so all together we get a codimension 1 subset of all M^{n-3} where ≥ 3 points have the same image. This shows that every point in Q has at most 2 preimages. Secant lines of C which pass through at least one singular point of $C_{\bar{k}}$ fill out a 2-dimensional subset, and the general M is disjoint from it. Thus every point in Q has smooth preimages.

We already saw that π is unramified at all smooth points of C, thus $k(q_i)/k(q)$ is separable for every $q \in Q$. Since there are at most 2 preimages, $\deg k(q_i)/k(q) \leq 2$. This completes (4).   ∎

STEP 4:   Quadratically closed fields.

Assume that k does not have any degree 2 separable field extensions and let $\pi\colon C \to C'$ be a projection as in Lemma 3. We claim that $C'(k) = \emptyset$.

Indeed, we know that $C'(k) \subset Q$ by Lemma 3 (2) and (3). If $q \in C'(k) \cap Q$ with preimages $q_1, q_2 \subset C_{\bar{k}}$ then $\deg k(q_i)/k(q) = \deg k(q_i)/k \leq 2$ by Lemma 3 (4), thus $k(q_i) = k$ by our assumption. This contradicts $C(k) = \emptyset$.

If k does have a degree 2 separable field extension, then the projected curve C' may well have k-points at its nodes. We next use the existence of a degree 2 separable field extension to first get a plane curve birational to C with a unique k-point and then to get rid of that single k-point using a non-birational map.

STEP 5:   Reduction to a plane curve with a unique k-point.

More generally, we prove the following

LEMMA 4: *Let k be an infinite field which has a degree 2 separable field extension. Let $C \subset \mathbb{P}^2$ be a plane curve with only finitely many k points. Then there is a birational map $\Phi\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ which transforms C into $C' := \Phi_* C \subset \mathbb{P}^2$ such that C' has at most one k-point.*

The proof uses some explicit birational maps of $\mathbb{P}^2$ which we review first.

Definition 5 (Cremona transformations):   The standard **Cremona transformation** of $\mathbb{P}^2$ with base points at the "coordinate vertices" $(0 : 0 : 1)$, $(0 : 1 : 0), (1 : 0 : 0)$ is given by

$$\phi\colon (x : y : z) \mapsto (yz : zx : xy).$$

It is best to think of ϕ as the map given by the 3-dimensional vector space of quadrics that vanish at the three coordinate vertices.

Note that ϕ is an involution and it gives an automorphism of $\mathbb{P}^2 \setminus (xyz = 0)$.

Let $C \subset \mathbb{P}^2$ be a plane curve not contained in $(xyz = 0)$ and $\phi_* C \subset \mathbb{P}^2$ the closure of its image. Assume that none of the coordinate vertices is in C. Then $C \to \phi_* C$ is a morphism and $\phi_* C$ is obtained from C as follows:

(1) $\phi_* C \cap (\mathbb{P}^2 \setminus (xyz = 0))$ is isomorphic to $C \cap (\mathbb{P}^2 \setminus (xyz = 0))$,
(2) $C \cap (x = 0)$ is mapped to $(1 : 0 : 0)$, $C \cap (y = 0)$ is mapped to $(0 : 1 : 0)$ and $C \cap (z = 0)$ is mapped to $(0 : 0 : 1)$.

Similarly, if P_1, P_2, P_3 are 3 non-collinear points in $\mathbb{P}^2$ then there is a 3-dimensional vector space of quadrics that vanish at P_1, P_2, P_3. By choosing a basis Q_1, Q_2, Q_3 we get a Cremona transformation

$$\phi_{(P,Q)}\colon (x : y : z) \mapsto (Q_1(x, y, z) : Q_2(x, y, z) : Q_3(x, y, z)).$$

For us it is especially useful to consider the case when P_1, P_2 are conjugate over k and P_3 is a k-point. In this case the vector space of quadrics that vanish at P_1, P_2, P_3 is defined over k and $\phi_{(P,Q)}$ is also defined over k.

To get a concrete example, let $q(x, y)$ be a k-irreducible, separable, degree 2, homogeneous polynomial with roots $P_1, P_2 \in \mathbb{P}^1$ and consider the Cremona transformation

$$\phi_q \colon (x : y : z) \mapsto (xz : yz : q(x, y)).$$

Its base points are $P_3 = (0 : 0 : 1)$ and $P_1, P_2 \in \mathbb{P}^1$ where we think of $\mathbb{P}^1$ as the line at infinity $(z = 0) \subset \mathbb{P}^2$.

The line $(z = 0)$ is mapped to $(0 : 0 : 1)$ and the conjugate pair of lines $(q(x, y) = 0)$ to the conjugate pair of points $(q(x, y) = z = 0)$.

Now we return to the proof of (4). Assume that $C(k)$ has at least 2 points Q_1, Q_2. By assumption, there is a k-irreducible, separable, degree 2, homogeneous polynomial $q(x, y)$. Since k is infinite, there is a coordinate system on $\mathbb{P}^2$ such that

(1) $(0 : 0 : 1) \notin C$,
(2) the points $(z = q(x, y) = 0)$ are not on C and
(3) Q_1, Q_2 are on the line at infinity $(z = 0)$.

Apply the Cremona transformation ϕ_q. It is an isomorphism outside $(zq(x, y) = 0)$, so no new k-points are created there.

None of the three base points are on C, so the only new points of $C' := (\phi_q)_*(C)$ are the three base points. Two of these, corresponding to the two conjugate linear factors of $q(x, y)$, are conjugate over k. The third one, $(0 : 0 : 1)$, is in k.

Thus $C(k) \to C'(k)$ is surjective and the two points $Q_1, Q_2 \in C(k)$ have the same image, thus $|C(k)| > |C'(k)|$. Repeating this procedure, we eventually end up with a unique k point on the birational transform of C. ∎

STEP 6:   Removing the unique k-point by a degree 2 cover.

Again we prove a more general result.

LEMMA 6: *Let k be an infinite field which has a degree 2 separable field extension. Let $C \subset \mathbb{P}^2$ be a geometrically integral plane curve with exactly one k point. Then there is a degree 2 map $g \colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ such that $C'' := g^{-1}(C) \subset \mathbb{P}^2$ is geometrically integral, closed and $C''(k) = \emptyset$.*

The plan is to write down a quadric surface $Q \subset \mathbb{P}^3$ and two projections $\pi \colon Q \to \mathbb{P}^2$ and $\rho \colon Q \dashrightarrow \mathbb{P}^2$. Here π is a projection from a k-point outside Q.

Thus $\pi\colon Q \to \mathbb{P}^2$ is everywhere defined and it has degree 2. We arrange that $C' := \pi^{-1}(C)$ is a geometrically integral curve without k points. On the other hand, $\rho\colon Q \dashrightarrow \mathbb{P}^2$ is a projection from a k-point on Q, hence birational and not everywhere defined. Again we arrange that $C'' := \rho(C')$ still has no k-points. Thus $g := \pi \circ \rho^{-1}$ is the required degree 2 map.

The characteristic 2 case behaves somewhat differently, thus we leave it to the end. We start with a simple general position result.

LEMMA 7: *Let k be an infinite field, char $k \neq 2$ and $C \subset \mathbb{A}_k^2$ a geometrically reduced plane curve. Then there is a hyperbola $(ax + by)(cx + dy) = e$, with $a, b, c, d, e \in k$ which intersects every irreducible component of C transversally in at least one point.*

Proof: Pick a smooth point $P \in C$ different from the origin. First we show that there is a hyperbola over $\bar{k}$ which intersects C transversally at P. This implies that the assertion of the lemma holds for a Zariski open set of all hyperbolas. Since k is infinite there is also such a hyperbola defined over k.

We can assume that $P = (1, 0)$. Then we can normalize the equation to $(x + by)(x + dy) = 1$. Its gradient at $(1, 0)$ is $(2, b + d)$. Since char $k \neq 2$, we can make $(2, b + d)$ transversal to the gradient of C at $(1, 0)$. ∎

Let us now prove Lemma 6 in the char $k \neq 2$ case. By Lemma 7 we can choose coordinates $(x : y : z)$ in $\mathbb{P}^2$ such that the following hold

(1) $(0 : 0 : 1)$ is the unique k-point of C and
(2) the hyperbola $H := (xy = z^2)$, intersects C transversally in at least one point.

By assumption there is an $a \in k$ which is not a square. Consider the smooth quadric

$$Q := (xy = z^2 - at^2) \subset \mathbb{P}^3$$

and let $\pi\colon Q \to \mathbb{P}^2(x : y : z)$ be the coordinate projection. Note that the ramification locus of π is the hyperbola H.

The preimage of $(0 : 0 : 1)$ is given by the solutions of $at^2 = 1$, hence it is a conjugate pair of points. Therefore $C'(k) = \emptyset$ where $C' := \pi^{-1}(C)$.

The projection $C' \to C$ is a double cover, ramifying at most at the points in $H \cap C$. Thus either C' is geometrically integral, or, over $\bar{k}$, it is the union of two copies of C mapping isomorphically onto C. Since H is transversal to C in at least one point, $C' \to C$ has at least one simple ramification point, thus C' is geometrically integral.

Note further that $q := (1 : 0 : 0 : 0) \in Q$ and the two lines through q are given by $(y = z^2 - at^2 = 0)$, hence they are conjugate over k.

Let us now project the quadric Q from the point q to get $\rho \colon Q \dashrightarrow \mathbb{P}^2 (y : z : t)$. ρ is everywhere defined on C' since q is not on C' (since $C'(k) = \emptyset$). Set $C'' := \rho(C') \subset \mathbb{P}^2$. Note that ρ is an isomorphism away from the two lines $(y = z^2 - at^2 = 0)$ and these lines are mapped to a conjugate pair of points. In particular, $C''(k) = \emptyset$. We can take $g := \pi \circ \rho^{-1}$. This completes the proof when char $k \neq 2$.

Only minor modifications are needed in the char $k = 2$ case. Choose coordinates $(x : y : z)$ in $\mathbb{P}^2$ such that the following hold

(1) the line $L := (z = 0)$, intersects C transversally in at least one point and
(2) $(0 : 0 : 1)$ is the unique k-point of C.

By assumption there is a k-irreducible polynomial $z^2 + tz + at^2$. Consider the quadric

$$Q := (xy = z^2 + tz + at^2) \subset \mathbb{P}^3$$

and let $\pi \colon Q \to \mathbb{P}^2$ be the coordinate projection. Set $C' := \pi^{-1}(C)$ and note that the ramification locus of π is the line L.

The rest of the proof works as before. ∎

Remark 8: Lemmas 4 and 6 also hold if k has a degree 2 inseparable field extension. In this case we have degenerate Cremona transformations where two of the base points coincide. The geometric language needs to be modified but the algebraic side remains unchanged.

Our proof of Theorem 1 starts with a curve C such that $C(k) = \emptyset$ and finds a double cover of C which is birational to a plane curve without k-points. It is, however, possible that C itself is birational to a plane curve without k-points.

QUESTION 9: *Let k be a field and C a projective curve over k such that $C(k) = \emptyset$. Is C birational to a plane curve $C' \subset \mathbb{P}^2$ such that $C'(k) = \emptyset$?*

Poonen remarked that a generic projection from a sufficiently high degree embedding $C \hookrightarrow \mathbb{P}^3$ should be such if k is Hilbertian.

The general case, however, seems to have a different flavor. Consider, for instance, the case when $k = \mathbb{R}$ and let $C \subset \mathbb{P}^n$ be a real curve such that $C(\mathbb{R}) = \emptyset$. If $P, \bar{P} \in C$ is a conjugate point pair, the line L connecting them is real. Thus if we project from a center intersecting L, the image of C has a real singular point. Moreover, this real singular point is usually stable under small perturbations of the projection. Thus we get real singular points for a

(Euclidean) open subset of all projections. I do not know the answer to (9) for real curves.

On the other hand, it may also be of interest to find for an integral, projective curve C over an infinite field k a birational morphism $\phi\colon C \to C' \subset \mathbb{P}^2$ such that $\phi(k)\colon C(k) \to C'(k)$ is a bijection.

Such a ϕ could exist even if k is algebraically closed, since C' may have only unibranch singularities. While I do not know any smooth counter examples, there are singular curves for which no such morphism exists.

Example 10:   (1) By a result of [Ton05], if a rational curve $C' \subset \mathbb{P}^2$ has only unibranch singularities, then the total number of singular points is at most 8. Take $k = \mathbb{C}$ and let $C \subset \mathbb{P}^N$ be a rational curve with at least 9 cusps. Then every projection must have some non-unibranch singularities.

(2) Okounkov suggested that that there are counter examples over $\mathbb{R}$ coming from graph theory. For instance, the complete bipartite graph $K_{4,4}$ on $4 + 4$ vertices can not be embedded into $\mathbb{RP}^2$. Following any Euler path, $K_{4,4}$ can be realized by the real points of a rational curve C with 8 nodes. Thus any projection $C \to C' \subset \mathbb{P}^2$ has new real singular points.

2. Density of k-points

Definition 11:   The convention we use is that a valuation of a field K is a map $v\colon K \to \Gamma \cup \infty$, where $(\Gamma, <)$ is an ordered group, satisfying the properties
  (1) $v(ab) = v(a) + v(b)$,
  (2) $v(a + b) \geq \min\{v(a), v(b)\}$ and
  (3) $v(a) = \infty$ iff $a = 0$.
With this convention, $a, b \in K$ should be thought of as near each other if $v(a-b)$ is large. A valuation determines a topology on K^n whose basis is given by the "balls of radius γ":

$$B_\gamma(a_1, \ldots, a_n) := \{(x_1, \ldots, x_n) : v(x_i - a_i) > \gamma \forall i\}.$$

This induces a topology on the K-points of any affine variety, and this is independent of the embedding chosen. Thus we get a well-defined topology on $X(K)$ where X is any K-variety.

The continuous dependence of the roots of a monic polynomial on the coefficients implies the following result that we need later:

LEMMA 12: *Let K be an algebraically closed field with a valuation v and $F\colon D \to B$ a nonconstant morphism between integral curves. Let $W \subset B$ be any subset. Then*

$$F^{-1}(\overline{W}) = \overline{F^{-1}(W)},$$

where $\overline{}$ denotes closure in the v-adic topology.

Plan of the proof of Theorem 2: Consider the special case when $X = C$ is a plane curve with equation $g(x, y) = 0$ and we want to prove that a point $(0, b) \in C(\bar{k})$ is in the closure of $C(k)$.

Following a trick of Prestel (cf. [FJ05, 11.5.3]), consider the surface in 4-space

$$T := (g(x_1, y_1) = g(x_2, y_2) = 0)$$

and the family of curves on T:

$$B_a := T \cap (x_1 x_2 = a^2).$$

It can happen that every B_a is reducible (for instance, when $g = x - y^2$), but this is not hard to avoid. Thus assume that B_a is geometrically integral for some a with $v(a)$ large. Then the system of equations

$$g(x_1, y_1) = g(x_2, y_2) = x_1 x_2 - a^2 = 0$$

has a solution in k and either $v(x_1) \geq v(a)$ or $v(x_2) \geq v(a)$. In either case, $g(x, y) = 0$ has a solution in k such that $v(x) \geq v(a)$.

This implies that at least one of the solutions of $g(0, y) = 0$ is in the closure of $C(k)$. Thus if we can choose $C \to \mathbb{A}_x^1$ to be Galois, then every solution of $g(0, y) = 0$ is in the closure of $C(k)$ and we are done.

13 (Proof of Theorem 2): Every point of $X(\bar{k})$ is contained in a geometrically integral curve $C \subset X$ and it is enough to prove that $C(k)$ is dense in $C(\bar{k})$. We can replace C by a projective model, also denoted by C.

STEP 1: Reduction to the Galois case.

The above discussion suggests that we should replace C with its Galois closure $D \to C \to \mathbb{A}_x^1$. The main theorem on the "stability of fields" (cf. [FJ05, 18.9.3]) says that for every geometrically integral curve C (over any field) one can always choose $C \to \mathbb{P}^1$ such that its Galois closure $D \to C \to \mathbb{P}^1$ is also geometrically integral. We need our map $C \to \mathbb{P}^1$ to satisfy certain additional properties which are easy to establish in the PAC case.

For any point $p \in C(\bar{k})$ there is an effective Cartier divisor $P \subset C$ such that $p \in \operatorname{Supp} P$. Since k is PAC, $C(k)$ is infinite. Thus there is a $t > 0$ and distinct points $q_i \in C(k)$ such that $\mathcal{O}_C(\sum_{i=0}^{t} q_i - P)$ is very ample. In particular, there is a rational function f on C with simple poles at $q_1, \ldots, q_t$ and vanishing on P. This gives a morphism $f \colon C \to \mathbb{P}^1$ such that

(1) $p \in f^{-1}(0 : 1)$,
(2) f is smooth above $(1 : 0)$ and
(3) $f^{-1}(1 : 0) = \{q_1, \ldots, q_t\}$ is a union of t different k-points.

Let $F \colon D \to \mathbb{P}^1$ denote the normalization of $\mathbb{P}^1$ in the Galois closure of $k(C)/k(\mathbb{P}^1)$. By the next Lemma, D is geometrically integral.

LEMMA 14: *Let C be an integral k-curve and $f \colon C \to \mathbb{P}^1$ a morphism such that*

(1) *f is smooth above $(1 : 0)$ and*
(2) *$f^{-1}(1 : 0) = \{q_1, \ldots, q_t\}$ is a union of t different k-points.*

Let $F \colon D \to \mathbb{P}^1$ denote the normalization of $\mathbb{P}^1$ in the Galois closure of $k(C)/k(\mathbb{P}^1)$. Then D is geometrically integral and F is smooth above $(1 : 0)$

Proof: We can also realize D as the normalization of an irreducible component of the t-fold fiber product

$$f^{(t)} : C^{(t)} := C \times_{\mathbb{P}^1} C \times_{\mathbb{P}^1} \cdots \times_{\mathbb{P}^1} C \to \mathbb{P}^1.$$

Since f is smooth above $(1 : 0)$ and $f^{-1}(1 : 0)$ is a union of k-points, we see that $f^{(t)}$ is smooth above $(1 : 0)$ and $(f^{(t)})^{-1}(1 : 0)$ is also a union of k-points. Thus every irreducible component of $C^{(t)}$ contains a smooth k-point hence they are geometrically integral. ∎

STEP 2: The auxiliary curves B_a.

Consider now the product map

$$F \times F \colon D \times D \to \mathbb{P}^1 \times \mathbb{P}^1,$$

and let $(x_i : y_i)$ for $i = 1, 2$ be coordinates on the two copies of $\mathbb{P}^1$. As shown by the next Lemma, in our case the curves B_a are almost all geometrically integral.

LEMMA 15: *Let D be a geometrically integral, projective k-curve and $F \colon D \to \mathbb{P}^1$ a morphism which is smooth above $(1 : 0)$. Then, for all but finitely many $(s : t) \in \mathbb{P}^1(k)$, the preimage*

$$B_{(s:t)} := (F \times F)^{-1}(sx_1x_2 = ty_1y_2) \subset D \times D$$

is a geometrically integral curve.

Proof: Note that $B_{(s:t)}$ is defined scheme theoretically.   That is, it is the subscheme of $D \times D$ defined by the equation

$$(sx_1x_2 - ty_1y_2) \circ (F \times F) = 0.$$

Thus our assertion includes the claim that $(sx_1x_2 - ty_1y_2) \circ (F \times F)$ vanishes along $B_{(s:t)}$ with multiplicity 1. Since we use subschemes, the construction of $B_{(s:t)}$ commutes with any field extension. (By contrast, working with the corresponding variety red $B_{(s:t)}$ could introduce extra multiplicities under inseparable field extensions.)

First we reduce the lemma to the case when the base field is algebraically closed and D is smooth.

Let $\bar{k} \supset k$ be an algebraic closure and $D_{\bar{k}}$ the corresponding curve. By assumption, $D_{\bar{k}}$ is integral (that is, irreducible and reduced). The construction of $B_{(s:t)}$ commutes with the field extension, thus $B_{(s:t)}$ is geometrically integral iff $(B_{(s:t)})_{\bar{k}}$ is integral. Therefore we may assume that k is algebraically closed.

Next, let $D' \to D$ be the normalization and $F' \colon D' \to \mathbb{P}^1$ the lifting of F. Set

$$B'_{(s:t)} := (F' \times F')^{-1}(sx_1x_2 = ty_1y_2) \subset D' \times D'.$$

Since D contains a smooth open set so does $D \times D$, thus $D' \times D' \to D \times D$ is an isomorphism over a dense open set. Therefore, for all but finitely many $(s : t)$, the induced morphism $B'_{(s:t)} \to B_{(s:t)}$ is an isomorphism over a dense open set, thus if $B'_{(s:t)}$ is integral then so is $B_{(s:t)}$ for all but finitely many $(s : t)$. Therefore we may also assume that D is smooth.

$|sx_1x_2 - ty_1y_2| =: |H_{(s:t)}|$ is an (incomplete) ample linear system on $\mathbb{P}^1 \times \mathbb{P}^1$ with base points at $((0 : 1), (1 : 0))$ and $((1 : 0), (0 : 1))$. Let $S \to \mathbb{P}^1 \times \mathbb{P}^1$ be the blow up of these base points and $\pi_S \colon S \to \mathbf{P}^1$ the induced morphism given by $|sx_1x_2 - ty_1y_2|$. (Note that $\mathbf{P}^1 \cong \mathbb{P}^1$, but I use the different notation to stress that $\mathbf{P}^1$ is not one of the coordinate factors in $S \to \mathbb{P}^1 \times \mathbb{P}^1$.)
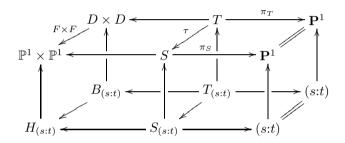
The curves $B_{(s:t)}$ form a linear system which is the pull back of an ample linear system by $F \times F$. Since a $F \times F$ is a finite morphism, the pull back is also ample (cf. [Har77, III.Exrc.5.7(d)]). Therefore, by the lemma of Enriques–Severi–Zariski, every $B_{(s:t)}$ is connected (cf. [Har77, III.7.9]). Thus it is enough to prove that $B_{(s:t)}$ is smooth for all but finitely many $(s : t) \in \mathbf{P}^1$.

The base points of $|B_{(s:t)}|$ are the preimages of $((0 : 1), (1 : 0))$ and $((1 : 0), (0 : 1))$ by $F \times F$. Let $T \to D \times D$ be the blow up of these

base points and $\tau\colon T \to S$ the lifting of $F \times F$. Further, let $\pi_T\colon T \to \mathbf{P}^1$ be the induced morphism given by $|B_{(s:t)}|$. Note that T can be singular.

Our aim is to prove that only finitely many fibers of π_T are singular. Equivalently, π_T has at least one smooth fiber. Let $Z \subset T$ be the set of points $p \in T$ such that $\pi_T^{-1}(\pi_T(p))$ is singular at p. Since π_T is flat, $Z \subset T$ is closed by [Gro65, IV.6.8.7]. For a given $(s:t)$, we analyze the singularities of the fiber $T_{(s:t)} := \pi_T^{-1}(s:t)$ by comparing them to the singularities of the fiber $S_{(s:t)} := \pi_S^{-1}(s:t)$.

The following diagram summarizes the notation.

There are two distinct ways that a point $p \in T_{(s:t)}$ can be singular: either $\tau(p) \in S_{(s:t)}$ is a singular point, or $\tau\colon T \to S$ is not smooth at p.

Correspondingly, let $Z_1 \subset T$ be the set of points $p \in T$ such that $\pi_S^{-1}(\pi_T(p))$ is singular at $\tau(p)$ and $Z_2 \subset T$ be the set of points $p \in T$ such that τ is not smooth at p. Then $Z \subset Z_1 \cup Z_2$ and $Z_1 \subset Z$, but usually Z_2 is not contained in Z. It is easy to describe Z_1 completely. The linear system $|sx_1x_2 - ty_1y_2|$ has only two singular members corresponding to $(x_1x_2 = 0)$ and $(y_1y_2 = 0)$, hence

$$Z_1 = \tau^{-1}\{((0:1),(0:1)),((1:0),(1:0))\}.$$

Since τ has finite fibers, Z_1 is finite.

Let us consider $B_{(0:1)}$ which is the preimage of $(y_1y_2 = 0)$ by $F \times F$. Thus it is a union

$$B_{(0:1)} = D \times F^{-1}(1:0) \cup F^{-1}(1:0) \times D,$$

and the two components intersect at the points $F^{-1}(1:0) \times F^{-1}(1:0)$ where $B_{(0:1)}$ has ordinary nodes.

Thus we see that $\tau(Z \cap B_{(0:1)}) = ((1:0),(1:0))$ and $Z \cap B_{(0:1)}$ is disjoint from Z_2 since τ is smooth above $((1:0),(1:0))$. Our goal is to prove that $\pi_T(Z)$ is finite. Since Z_1 is finite, it suffices to prove that $\pi_T(Z \cap Z_2)$ is finite. To this end observe that π_T is proper, so $\pi_T(Z \cap Z_2)$ is closed. Thus, $\pi_T(Z \cap Z_2)$

is either finite or all of $\mathbf{P}^1$. The latter possibility is excluded, because $(0 : 1) \notin \pi_T(Z \cap Z_2)$. ∎

STEP 3:   End of the proof.

We are back to the case when k is arbitrary. For $a \in k$, let $B_a \subset D \times D$ denote the affine curve $B_{(1:a^2)} \setminus (y_1 y_2 = 0)$. We change to affine coordinates $X_i = x_i/y_i$ on $(\mathbb{P}^1 \times \mathbb{P}^1) \setminus (y_1 y_2 = 0)$, then the equation of B_a is $X_1 X_2 = a^2$.

Since k is PAC, for all but finitely many $a \in k$ there is a k-point

$$(q_1, q_2) \in B_a(k) \subset D(k) \times D(k).$$

Since $F(q_1)F(q_2) = a^2$, we conclude that either $v(F(q_1)) > v(a)$ or $v(F(q_2)) > v(a)$. In any case we have proved that for all but finitely many $a \in k$ there is a point $q \in D(k)$ such that $v(F(q)) > v(a)$. By [FJ05, 11.5.2], for any $\gamma \in \Gamma$ there are infinitely many $a \in k$ such that $v(a) > \gamma$. Thus, for every $\gamma \in \Gamma$ there is a $q \in D(k)$ such that $v(F(q)) > \gamma$. That is, $(0 : 1) \in \mathbb{P}^1$ is in the v-adic closure of $F(D(k))$.

Since $F \colon D \to \mathbb{P}^1$ is Galois, $F^{-1}(F(D(k))) = D(k)$. Thus, by Lemma 12, $p \in F^{-1}(0 : 1)$ is in the v-adic closure of $F^{-1}(F(D(k))) = D(k)$. ∎

References

[Ax68] J. Ax, *The elementary theory of finite fields,* Annals of Mathematics (2) **88** (1968), 239–271.

[Fre73] G. Frey, *Pseudo algebraically closed fields with non-Archimedean real valuations,* Journal of Algebra **26** (1973), 202–207.

[FJ05] M. D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Spreinger-Verlag, Berlin, 2005.

[Gro65] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II,* Publications Mathématiques de l'Institut des Hautes Études Scientifiques **24** (1965), 231.

[Har77] R. Hartshorne, *Algebraic Geometry,* Springer-Verlag, New York, Graduate Text in Mathematics 52, 1977.

[Ton05] K. Tono, *On the number of the cusps of cuspidal plane curves,* Mathematische Nachrichten **278** (2005), 216–221.