A potential analogue of Schinzel's hypothesis for polynomials with coefficients in $\mathbf{F}_q[t]$

Andreas O. Bender*
Korea Institute for Advanced Study
Seoul 130-722
Korea
andreas@kias.re.kr

Olivier Wittenberg
Laboratoire de mathématiques, Bâtiment 425
Université Paris-Sud
F-91405 Orsay
France
olivier.wittenberg@ens.fr

July 1, 2005

1 Introduction

The Schinzel hypothesis essentially claims that finitely many irreducible polynomials in one variable over $\mathbf{Z}$ simultaneously assume infinitely many prime values unless there is an obvious reason why this is impossible.

We prove that under a restriction on the characteristic and a smoothness assumption, finitely many irreducible polynomials in one variable over the ring $\mathbf{F}_q[t]$ assume simultaneous prime values after a sufficiently large extension of the field of constants.

1.1 The Schinzel hypothesis over Z

Let $f_1(x), \ldots, f_r(x)$ be irreducible polynomials with coefficients in $\mathbf{Z}$. Assume that the leading coefficient of every $f_i(x)$ is positive and that for each prime p, there exists an integer x_p such that no $f_i(x_p)$ is divisible by p. Then $f_1(x), \ldots, f_r(x)$ are simultaneously prime for infinitely many integer values of x.
In its present generality, this conjecture was first stated in [12].

1.2 The Schinzel hypothesis over $\mathbf{F}_q[t]$

A naïve analogon to the Schinzel hypothesis over the coefficient ring $\mathbf{F}_q[t]$ can be formulated as follows:

Let $f_1(x), \ldots, f_r(x)$ be non-constant polynomials in $\mathbf{F}_q[t, x]$ which are irreducible in $\mathbf{F}_q(t)[x]$ and assume that for each prime $\mathfrak{p}$ of $\mathbf{F}_q[t]$, there is an $x_\mathfrak{p}$ in $\mathbf{F}_q[t]$

*The first author acknowledges financial support provided by the Japan Society for the Promotion of Science (JSPS) as well as through the European Community's Human Potential Programme under contracts HPRN-CT-2000-00120 [AAG] and HPRN-CT-2000-00114 [GTEM].

such that no $f_i(x_{\mathfrak{p}})$ is divisible by $\mathfrak{p}$. Then $f_1(x), \dots, f_r(x)$ are simultaneously prime for infinitely many values of x in $\mathbf{F}_q[t]$.

In this form, the hypothesis is known to be false; counterexamples are described in [3], one of them being the following: With p the characteristic of $\mathbf{F}_q$, choose an integer b with $1 < b < 4q$ and $(b, p(q-1)) = 1$ (e.g., $b = 2q-1$). Let $f(x) = x^{4q} + t^b$. Then $f(g)$ is reducible for all $g \in \mathbf{F}_q[t]$ (see [3, Section 4]).

In [1], Bateman and Horn formulated a quantitative version of the Schinzel hypothesis, which specifies the conjectural proportion of integers for which the polynomials assume prime values.

In [3, (1.2),(1.8)], Conrad, Conrad and Gross presented an analogue to the Bateman–Horn conjecture for the case of one polynomial over $\mathbf{F}_q[t]$, supported by good agreement with numerical evidence. As for the qualitative case, this conjecture implies that the naïve function field version of the Schinzel hypothesis enunciated above does in fact hold for one separable polynomial.

For polynomials with coefficients in either $\mathbf{Z}$ or $\mathbf{F}_q[t]$, Dirichlet's theorem about primes in arithmetic progressions and its analogue for function fields is the only case in which the Schinzel hypothesis is known to hold; see [10] or [11, Theorem 4.7] for the case of $\mathbf{F}_q[t]$. Note that in that case of one polynomial of degree 1, these results amount to the quantitative statements of the conjectures of Bateman–Horn and of Conrad, Conrad and Gross, respectively.

The goal of this note is to prove the following theorem.

Theorem 1.1. *Let $\mathbf{F}_q$ be a finite field of characteristic p and cardinality q. Let $f_1, \dots, f_n \in \mathbf{F}_q[t, x]$ be irreducible polynomials whose total degrees $\deg(f_i)$ satisfy $p \nmid \deg(f_i)(\deg(f_i) - 1)$ for all i. Assume that the curves $C_i \subset \mathbf{P}^2_{\mathbf{F}_q}$ defined as the Zariski closures of the affine curves*

$$f_i(t, x) = 0$$

are smooth. Then, for any sufficiently large $s \in \mathbf{N}$, there exist $a, b \in \mathbf{F}_{q^s}$ such that the polynomials $f_1(t, at + b), \dots, f_n(t, at + b) \in \mathbf{F}_{q^s}[t]$ are all irreducible.

Acknowledgements: A preliminary manuscript about this topic, written solely by the first author, contained some gaps; he is grateful to Jean-Louis Colliot-Thélène, Jürgen Klüners and Sir Peter Swinnerton-Dyer for pointing them out.

We had very useful discussions about the contents of this paper with Jean-Louis Colliot-Thélène; previous versions benefited from comments made by Ido Efrat, Bert van Geemen, Pierre Dèbes, Moshe Jarden, and Fumiharu Kato. We also thank Keith Conrad for corresponding with us about the results contained in [3] and Ofer Gabber for pointing out that Lemma 2.3 could be used instead of [13, Proposition 4.4.6].

This research was carried out while the first author was staying at the University of Pavia and Collegio Ghislieri, the University of Padova, at Ben-Gurion University of the Negev, the Hebrew University of Jerusalem, with the major part having been done at Kyoto University. To all these institutions, he expresses his gratitude for their hospitality.

Notations. We denote by $|S|$ the cardinality of a set S and by $\mathfrak{S}(S)$ the symmetric group on S. Let k be a field and X be a k-scheme. If k' is a field extension of k, the scheme $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$ will often be denoted $X_{k'}$. We write $\kappa(x)$ for the residue field of $x \in X$, and $\kappa(X)$ for the function field of X when X is integral. Finally, when Y is an X-scheme, $\mathrm{Aut}_X(Y)$ denotes the group of X-automorphisms of Y.

2 A preliminary result about generic covers of $\mathbf{P}^1$

If k is a field, a finite k-scheme X will be said to have *at most one double point* if $n(X) \geq r(X) - 1$, where $r(X)$ and $n(X)$ respectively denote the rank and the geometric number of points of X.

The following definition was introduced by Hurwitz [7] in his proof of connectedness of the moduli spaces for curves of genus g over $\mathbf{C}$.

Definition 2.1. *A finite morphism $f\colon C \to \mathbf{P}^1_k$ is called generic if $f^{-1}(x)$ has at most one double point for all $x \in \mathbf{P}^1_k$.*

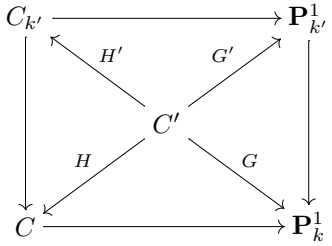
Note that if the characteristic of k is not 2, f is generic and C is an integral curve, then f is separable (in the sense that the field extension $\kappa(C)/\kappa(\mathbf{P}^1_k)$ is separable).

Proposition 2.2. *Let C be a regular, complete, geometrically irreducible curve over a field k, endowed with a finite separable generic morphism $f\colon C \to \mathbf{P}^1_k$. Let C' be a regular, complete, irreducible curve over k, and $g\colon C' \to C$ be a finite morphism. Assume that the finite extension $\kappa(C')/\kappa(\mathbf{P}^1_k)$ is a Galois closure of the subextension $\kappa(C)/\kappa(\mathbf{P}^1_k)$. We denote respectively by G and H the Galois groups of $\kappa(C')/\kappa(\mathbf{P}^1_k)$ and $\kappa(C')/\kappa(C)$. Then C' is geometrically irreducible over k and the morphism*

$$G \longrightarrow \mathfrak{S}(H\backslash G)$$

induced by right multiplication is an isomorphism. Moreover, all the ramification indices of $\kappa(C')/\kappa(\mathbf{P}^1_k)$ are ≤ 2.

Proof. Let k' denote the algebraic closure of k in $\kappa(C')$. We denote respectively by G' and H' the subgroups of G defined by the subfields $\kappa(\mathbf{P}^1_{k'})$ and $\kappa(C_{k'})$ of $\kappa(C')$, so that we have a canonical commutative diagram as follows, where the labels indicate the Galois groups of the generic fibres:



Let us endow $H\backslash G$ (resp. $H'\backslash G'$) with the action of G (resp. G') by right multiplication. The equality $H \cap G' = H'$ of subgroups of G yields a natural injective G'-equivariant map $H'\backslash G' \to H\backslash G$, which is even bijective since $|H\backslash G|$ and $|H'\backslash G'|$ are both equal to $\deg(f)$. Hence a commutative square

$$\begin{array}{ccc} G' & \longrightarrow & \mathfrak{S}(H'\backslash G') \\ \downarrow & & \| \\ G & \longrightarrow & \mathfrak{S}(H\backslash G), \end{array}$$

where the horizontal arrows are induced by right multiplication. The bottom horizontal arrow is injective, in virtue of the equality $\bigcap_{a\in G} aHa^{-1} = 1$, itself a consequence of the hypothesis that $\kappa(C')/\kappa(\mathbf{P}^1_k)$ is a Galois closure of $\kappa(C)/\kappa(\mathbf{P}^1_k)$. For the first part of the proposition, it only remains to be shown that the top horizontal arrow is surjective; indeed, this will imply not only that the bottom horizontal arrow is an isomorphism, but also that $G' = G$, hence $k' = k$, which is equivalent

to C' being geometrically irreducible over k. The second part will follow from the first once we know that all ramification indices of $\kappa(C')/\kappa(\mathbf{P}^1_{k'})$ are ≤ 2.

We shall now make use of the following classical result. A very similar lemma is stated and proven in [13, Proposition 4.4.6].

Lemma 2.3. *Let X be a regular, complete, geometrically irreducible curve over a field K, endowed with a finite and generically Galois morphism $X \to \mathbf{P}^1_K$ with group G. Then G is generated by the inertia subgroups above closed points of $\mathbf{P}^1_K$ and their conjugates.*

Proof. Let $H \subseteq G$ denote the normal subgroup generated by the inertia subgroups and their conjugates. The map $X \to \mathbf{P}^1_K$ can be factored as $X \to Y \to \mathbf{P}^1_K$, where Y is a regular, complete, irreducible curve over K whose function field is the subfield of $\kappa(X)$ fixed by H. The curve Y is geometrically irreducible over K, since X is, and it follows from Lemma 5.1 that it is étale over $\mathbf{P}^1_K$; therefore $Y = \mathbf{P}^1_K$ (see [6, IV.2.5.3]), hence $H = G$. □

Let us consider the cover $C' \to \mathbf{P}^1_{k'}$. It is generically Galois with group G'. Let $I \subseteq G'$ be the inertia subgroup of G' associated with a point of C' whose image by $f \circ g$ will be denoted x. By Lemma 5.1, the geometric number of points of $f^{-1}(x)$ is $|H'\backslash G'/I|$. Moreover, the rank of $f^{-1}(x)$ is $|H'\backslash G'|$. The hypothesis that $f^{-1}(x)$ has at most one double point thus leads to the inequality

$$|H'\backslash G'/I| \geq |H'\backslash G'| - 1,$$

thereby proving that every non-trivial inertia subgroup of G' has order 2 and acts as a transposition on $H'\backslash G'$. Applying Lemma 2.3 to $X = C'$ and $K = k'$ now yields that G' is generated by elements which act on $H'\backslash G'$ as transpositions. The image of $G' \to \mathfrak{S}(H'\backslash G')$ is therefore a transitive subgroup of $\mathfrak{S}(H'\backslash G')$ which is generated by transpositions; but the only such subgroup is $\mathfrak{S}(H'\backslash G')$ itself (see [13, Lemma 4.4.4]), hence the result. □

3 Proof of Theorem 1.1

To prove Theorem 1.1, we may and will assume that the polynomials $(f_i)_{1\leq i\leq n}$ are pairwise non-proportional. Let $\mathbf{F}$ denote an algebraic closure of $\mathbf{F}_q$. The symbol $\mathbf{F}_{q^s}$ will now be understood to refer to the unique subfield of $\mathbf{F}$ with cardinality q^s. Let $M_0 \in \mathbf{P}^2(\mathbf{F}_q)$ denote the point at infinity with coordinates $x = 1$, $t = 0$.

Proposition 3.1. *There exists a non-empty open subset $U \subset \mathbf{P}^2_{\mathbf{F}_q} \setminus \{M_0\}$, disjoint from C_i for all $i \in \{1, \ldots, n\}$, such that every line D in $\mathbf{P}^2_{\mathbf{F}}$ which meets U satisfies the following properties:*

1. *For all $i \in \{1, \ldots, n\}$, the scheme-theoretic intersection $(C_i)_{\mathbf{F}} \cap D$ has at most one double point (as a finite $\mathbf{F}$-scheme).*
2. *The line D is not tangent to more than one of the curves $(C_i)_{\mathbf{F}}$, $i \in \{1, \ldots, n\}$.*

Proof. It is enough to prove that there are finitely many lines D in $\mathbf{P}^2_{\mathbf{F}}$ not satisfying the above properties. Indeed, once this is known, we can take for U any non-empty open subset disjoint from the curves C_i and from all these lines.

We shall use the duality theory of plane curves. To every irreducible plane curve $C \subset \mathbf{P}^2$ over some field is associated an irreducible curve $C^\star \subset (\mathbf{P}^2)^\star$, called its dual, together with a canonical rational map $\rho\colon C \dashrightarrow C^\star$, called the Gauss map, which sends a smooth point of C to its tangent line. Here $(\mathbf{P}^2)^\star$ denotes the dual projective plane. The reader is referred to [9] for an overview of this theory, of

which we shall only use the following two results. Firstly, the Monge-Segre-Wallace criterion (see [9, p. 169]) ensures that the equality $C^{\star\star} = C$ of closed subsets of $\mathbf{P}^2$ holds as soon as ρ is separable. Secondly, it follows from Corollaire 3.5.0 and Corollaire 3.2.1 of [8] that if ρ is separable, then there are only finitely many lines D in $\mathbf{P}^2$ such that the scheme-theoretic intersection $C \cap D$ does not have at most one double point.

Let us apply these results to the smooth curves $(C_i)_{\mathbf{F}} \subset \mathbf{P}^2_{\mathbf{F}}$. A line in $\mathbf{P}^2_{\mathbf{F}}$ which is tangent to more than one of the curves $(C_i)_{\mathbf{F}}$, $i \in \{1, \ldots, n\}$, corresponds to a point in $(C_i)^\star_{\mathbf{F}} \cap (C_j)^\star_{\mathbf{F}}$ for distinct i, j. Now if the Gauss maps $\rho_i \colon C_i \to C_i^\star$ and $\rho_j \colon C_j \to C_j^\star$ are separable, this intersection is finite. Indeed, the curves $C_i^\star$ and $C_j^\star$ being irreducible, they would otherwise be equal; but the separability of ρ_i and ρ_j implies that $C_i^{\star\star} = C_i$ and $C_j^{\star\star} = C_j$, and we have assumed that $C_i \neq C_j$.

We are thus reduced to proving that the maps ρ_i are all separable. As the curves C_i are smooth, Euler's formula shows that the Gauss maps ρ_i can be extended to morphisms $r_i : \mathbf{P}^2 \to \mathbf{P}^2$. An application of the projection formula for intersections [6, A.1, A4] then gives

$$r_{i\star}(C_i.r_i^\star D) = (r_{i\star}C_i).D,$$

where D is a line in the target space $\mathbf{P}^2$. The equations of r_i now show that $r_i^\star D$ has degree $\deg(C_i) - 1$. By definition of $r_{i\star}$, we have $r_{i\star}C_i = \deg(\rho_i)C_i^\star$ and so Bézout's theorem implies the following formulae:

$$\deg(C_i)\,(\deg(C_i) - 1) = \deg(\rho_i)\deg(C_i^\star).$$

The hypothesis on the total degrees of the polynomials f_i now implies that $\deg(\rho_i)$ is prime to p, hence ρ_i is separable. □

Let $U \subset \mathbf{P}^2_{\mathbf{F}_q}$ be given by Proposition 3.1 and $s_0 \in \mathbf{N}$ be large enough so that $U(\mathbf{F}_{q^s}) \neq \varnothing$ for all $s \geq s_0$. Let $s \in \mathbf{N}$ be a sufficiently large integer; for the time being, this means that $s \geq s_0$, but another condition on s will be introduced later. For the sake of clarity, we will henceforth denote the field $\mathbf{F}_{q^s}$ by k. Fix $M \in U(k)$ and denote by $\varphi_i \colon (C_i)_k \to \mathbf{P}^1_k$ the k-morphism obtained by composing the inclusion $(C_i)_k \subset \mathbf{P}^2_k \backslash \{M\}$ with the morphism $\mathbf{P}^2_k \backslash \{M\} \to \mathbf{P}^1_k$ defined by projection from M. The morphism φ_i is finite of degree $\deg(f_i)$ and is generic, since $M \in U$. Being generic, it is separable (note that the hypotheses of Theorem 1.1 imply that $p \neq 2$); therefore there exists a smooth, complete, connected curve C_i' over k and a finite morphism $C_i' \to (C_i)_k$, such that the induced field extension $\kappa(C_i')/\kappa(\mathbf{P}^1_k)$ is a Galois closure of $\kappa((C_i)_k)/\kappa(\mathbf{P}^1_k)$. Let us write, for simplicity, $K = \kappa(\mathbf{P}^1_k)$, $K_i = \kappa(C_i')$, $G_i = \mathrm{Gal}(K_i/K)$ and $H_i = \mathrm{Gal}(K_i/\kappa((C_i)_k))$. Proposition 2.2 now shows that for all $i \in \{1, \ldots, n\}$, the curve C_i' is geometrically connected over k, the group G_i is canonically isomorphic to $\mathfrak{S}(H_i \backslash G_i)$ and the ramification indices of K_i/K are ≤ 2.

Let $R_i \subset \mathbf{P}^1_k$ denote the branch locus of the morphism $C_i' \to \mathbf{P}^1_k$.

Proposition 3.2. *The subsets $R_i \subset \mathbf{P}^1_k$ for $i \in \{1, \ldots, n\}$ are pairwise disjoint.*

Proof. We shall need the following well-known lemma, which is a direct consequence of Lemma 5.1.

Lemma 3.3. *Let E/K be a finite separable extension of global fields, and let L be a Galois closure of E/K. Then a finite place of K is unramified in E if and only if it is unramified in L.*

The lemma shows that R_i is also the branch locus of the morphism $(C_i)_k \to \mathbf{P}^1_k$. An $\mathbf{F}$-point of $R_i \cap R_j$ therefore gives rise to a line in $\mathbf{P}^2_{\mathbf{F}}$ which is both tangent to $(C_i)_{\mathbf{F}}$ and $(C_j)_{\mathbf{F}}$, and which contains M. As $M \in U$, there is no such line if $i \neq j$, hence the proposition. □

Let L denote the ring $K_1 \otimes_K \cdots \otimes_K K_n$.

Proposition 3.4. *The ring L is a field, and k is separably closed in L.*

Proof. For $j \in \{0, \ldots, n\}$, let us write L_j for the K-algebra $K_1 \otimes_K \cdots \otimes_K K_j$ and prove that L_j is a field in which k is separably closed, by induction on j. The case $j = 0$ is trivial, as $L_0 = K$. Assume now that $j > 0$ and that L_{j-1} is a field in which k is separably closed. Let Ω be a field containing $\mathbf{F}$, L_{j-1} and K_j. Consider the subfield $E_j \subset \Omega$ defined as the intersection of the composita $\mathbf{F}L_{j-1}$ and $\mathbf{F}K_j$. Being a finite extension of $\mathbf{F}K$, it is the function field of a connected finite cover of $\mathbf{P}^1_{\mathbf{F}}$. Proposition 3.2 now shows that this cover is unramified; a connected finite étale cover of $\mathbf{P}^1_{\mathbf{F}}$ is necessarily trivial, hence $E_j = \mathbf{F}K$. As $\mathbf{F}K_j$ is Galois and $\mathbf{F}L_{j-1}$ is finite over $\mathbf{F}K$, this is enough to imply that $\mathbf{F}L_{j-1}$ and $\mathbf{F}K_j$ are linearly disjoint subfields of Ω over $\mathbf{F}K$; in other words, $\mathbf{F}L_{j-1} \otimes_{\mathbf{F}K} \mathbf{F}K_j$ is a field. We have $\mathbf{F}L_{j-1} = \mathbf{F} \otimes_k L_{j-1}$ and $\mathbf{F}K_j = \mathbf{F} \otimes_k K_j$ since k is separably closed in L_{j-1} and in K_j, hence $\mathbf{F}L_{j-1} \otimes_{\mathbf{F}K} \mathbf{F}K_j = \mathbf{F} \otimes_k L_j$. As this ring is a field, k is separably closed in L_j. □

Let C' denote a smooth complete connected curve over k with function field L. There is a natural finite morphism $\psi\colon C' \to \mathbf{P}^1_k$, which is generically Galois and therefore separable. We denote by g the genus of C', by G the group $\mathrm{Gal}(L/K)$, by N the degree of ψ, and by $(x, L/K)$ the Artin symbol of the extension L/K above a closed point $x \in \mathbf{P}^1_k$ which does not ramify in L. We would now like to find a rational point of $\mathbf{P}^1_k$ above which the fibre of ψ is integral. To this end, we resort to an effective version of the Čebotarev theorem for function fields, due to Geyer and Jarden. The following is a weak consequence of [5, Proposition 13.4].

Theorem 3.5. *Let c be a conjugacy class in G. We denote by $P(L/K, c)$ the set of rational points $x \in \mathbf{P}^1(k)$ outside the branch locus of $C' \to \mathbf{P}^1_k$ such that $c = (x, L/K)$. Then one has*

$$|P(L/K, c)| \geq \frac{1}{N}\left(q^s - (N + 2g)q^{s/2} - Nq^{s/4} - 2(g + N)\right). \tag{1}$$

Some preparation is in order before applying Theorem 3.5: to be able to deduce from it that $P(L/K, c)$ is non-empty as soon as s is chosen large enough, we need to make sure that the right-hand side of (1) does grow when s goes to infinity. For instance, it suffices to establish that N and g are bounded independently of M and s. The integer N is obviously independent of the choices made: it is equal to $\prod_{i=1}^n (\deg(f_i)!)$. We shall actually prove that g is also independent of M and s.

As C' is geometrically connected over k, Hurwitz's theorem [6, IV.2.4] enables us to express g in terms of the ramification divisor of $C' \to \mathbf{P}^1_k$. The finite extension L/K is tamely ramified, since its ramification indices are ≤ 2 and $p \neq 2$; we can therefore write the ramification divisor in terms of the ramification indices. We finally obtain the equality

$$g - 1 + N = \frac{N}{2} \sum_{i=1}^{n} \deg(R_i), \tag{2}$$

where $R_i \subset \mathbf{P}^1_k$ is now considered as a finite k-scheme with its reduced subscheme structure. Hurwitz's theorem applied to the finite morphism $(C_i)_k \to \mathbf{P}^1_k$ yields

$$\deg(R_i) = 2g_i - 2 + 2\deg(f_i), \tag{3}$$

where g_i denotes the genus of C_i. By combining equations (2) and (3), we end up with

$$g - 1 + N = N \sum_{i=1}^{n} (g_i - 1 + \deg(f_i)), \tag{4}$$

hence the claim: g is independent of M and s.

We can therefore assume that the right-hand side of (1) is ≥ 2, by demanding that s be sufficiently large. The canonical isomorphism $G = G_1 \times \cdots \times G_n = \mathfrak{S}(H_1\backslash G_1) \times \cdots \times \mathfrak{S}(H_n\backslash G_n)$ allows us to choose an element $\sigma \in G$ whose projection in G_i acts transitively on $H_i\backslash G_i$ for every $i \in \{1, \ldots, n\}$. Let $x_0 \in \mathbf{P}^1(k)$ be the point corresponding to the line in $\mathbf{P}^2_k$ passing through M and M_0. Theorem 3.5 now ensures the existence of a rational point $x \in \mathbf{P}^1(k)$ outside $\bigcup_{i=1}^n R_i$, distinct from x_0, and such that $\sigma = (x, L/K)$. As the image of $(x, L/K)$ in G_i is $(x, K_i/K)$, it follows from Lemma 5.1 and the definition of σ that $\varphi_i^{-1}(x)$ is irreducible. Moreover, the k-scheme $\varphi_i^{-1}(x)$ is étale since $x \notin R_i$, and hence it is integral. That $x \neq x_0$ implies that there exist $a, b \in k$ such that for every $i \in \{1, \ldots, n\}$, the scheme $\mathrm{Spec}(k[t]/(f_i(t, at+b)))$ is an open subscheme of $\varphi_i^{-1}(x)$; as the latter scheme is integral, the polynomials $f_1(t, at+b), \ldots, f_n(t, at+b)$ must be irreducible.

4 Application

The following problem was posed in [4]:

PROBLEM: *Let $f(t,x) \in \mathbf{F}_q[t,x]$ be irreducible and set $g(t) = f(t, at+b)$. Count (or estimate) the number of pairs $(a,b) \in \mathbf{F}_q \times \mathbf{F}_q$ such that $g(t)$ is irreducible over $\mathbf{F}_q$.*

As a partial solution of this problem, we have

Proposition 4.1. *Let $\mathbf{F}_q$ be a finite field of characteristic p and cardinality q. Let $f \in \mathbf{F}_q[t,x]$ be an irreducible polynomial whose total degree d satisfies $p \nmid d(d-1)$. Assume that the curve $C \subset \mathbf{P}^2_{\mathbf{F}_q}$ defined as the Zariski closure of the affine curve*

$$f(t,x) = 0$$

is smooth and that $q > 9(d(d-1)d!+2)^2$. Then the polynomial $f(t, at+b) \in \mathbf{F}_q[t]$ is irreducible for at least $\frac{1}{d!}(q - \frac{d^4}{2})(q - 3(d(d-1)d!+2)q^{1/2} - d!)$ pairs $(a,b) \in \mathbf{F}_q \times \mathbf{F}_q$.

Proof. We unfold the proof of Theorem 1.1 for one polynomial and estimate the resulting number of possible pairs (a,b), using only the simplest non-trivial estimates.

The only parts of the proof of Theorem 1.1 which depend on the size of the finite field in relation to the degree d are the applications of Proposition 3.1 and of Theorem 3.5. The case $d = 1$ being trivial, we assume $d \geq 2$.

We use the notation introduced in the proof of Theorem 1.1. As mentioned in the proof of Proposition 3.1, the Gauss map $\varphi\colon C \to C^\star$ is separable. Proposition 3.5 in [8] then implies that as in characteristic 0, the number n of lines $D \subset \mathbf{P}^2_{\mathbf{F}}$ whose scheme-theoretic intersection with $C_{\mathbf{F}}$ does not have at most one double point is bounded by the number of singular points of the dual curve $C^\star_{\mathbf{F}}$. Since $C^\star$ is irreducible of degree $d(d-1)$, we thus obtain $n \leq p_a(C^\star) = \frac{1}{2}(d(d-1)-1)(d(d-1)-2) \leq \frac{1}{2}d^4 - d + 1$. In particular, it follows from our assumption $q > 9(d(d-1)d!+2)^2$ that $q^2 > n$, hence the existence of an $\mathbf{F}_q$-rational line $D_0 \subset \mathbf{P}^2_{\mathbf{F}_q} \setminus \{M_0\}$ whose scheme-theoretic intersection with C has at most one double point.

Pairs $(a,b) \in \mathbf{F}_q \times \mathbf{F}_q$ such that $f(t, at+b) \in \mathbf{F}_q[t]$ is irreducible correspond bijectively to lines $D \subset \mathbf{P}^2_{\mathbf{F}_q} \setminus \{M_0\}$ such that $C \cap D$ is integral. Let us denote their number by e, and by $e(M)$ the number of such lines which contain a given $M \in (D_0 \cap U)(\mathbf{F}_q)$. For such an M, we have seen in Theorem 3.5 that $e(M) + 1$ is greater than or equal to the right-hand side of (1) with $s = 1$; moreover $N = d!$, and (4) yields

$$g = 1 + \frac{N}{2}(d-2)(d+1),$$

whence

$$e(M) \geq \frac{1}{d!}(q - 3(d(d-1)d! + 2)q^{1/2}).$$

The result now follows in view of the inequalities

$$e \geq \sum_{M \in (D_0 \cap U)(\mathbf{F}_q)} (e(M) - 1)$$

and

$$|(D_0 \cap U)(\mathbf{F}_q)| \geq q + 1 - n - d \geq q - \frac{1}{2}d^4.$$

□

5 Appendix

The following lemma was used several times in the proof of Theorem 1.1. It is essentially well-known, but we state it here and include a sketch of proof for lack of an adequate reference. It is only for technical reasons that we state it in such generality (we need to allow X' to be non-connected in order to be able to reduce to the case of a strictly Henselian base in the proof below).

Lemma 5.1. *Let $u\colon X' \to X$ and $f\colon X \to B$ denote surjective finite flat morphisms of normal schemes. Assume B is the spectrum of a discrete valuation ring. Put $f' = f \circ u$. Let G be a finite subgroup of $\mathrm{Aut}_B(X')$ such that the generic fibre of f' is a torsor under G. Let $m \in X'$ belong to the special fibre of f'. We denote respectively by $D_m \subseteq G$ and $I_m \subseteq G$ the decomposition and inertia subgroups associated with m; in other words, D_m is the stabilizer of m and I_m is the kernel of the natural map $D_m \to \mathrm{Aut}(\kappa(m))$. Let $H = G \cap \mathrm{Aut}_X(X')$. Then the double quotient $H\backslash G/D_m$ is canonically in bijection with the special fibre of f, and the double quotient $H\backslash G/I_m$ is canonically in bijection with the geometric special fibre of f.*

Sketch of proof. Let us first consider the assertion about $H\backslash G/I_m$. To prove it, one easily checks that B may be assumed to be strictly Henselian, by using the fact that for any finite field extension L/k, the group $\mathrm{Aut}_k(L)$ acts freely on $\mathrm{Spec}(L \otimes_k \bar{k})$, where $\bar{k}$ denotes a separable closure of k. Now the assertion about $H\backslash G/I_m$ follows from the one about $H\backslash G/D_m$ since $D_m = I_m$.

We are thus left with the first part of the lemma. Define a map

$$H\backslash G/D_m \longrightarrow f^{-1}(f'(m))$$

by sending the double class $H\sigma D_m$ to $u(\sigma(m))$. The key ingredient for checking that this map is indeed a bijection is the transitivity of the action of G (resp. H) on the fibres of f' (resp. u), and it is a consequence of [2, Ch. 5, §2, Th. 2]. □

References

[1] P. T. Bateman, R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* ***16*** *(1962) 363–367.*

[2] N. Bourbaki, Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations. *Actualités Scientifiques et Industrielles, No. 1308, Hermann, Paris, 1964.*

[3] B. Conrad, K. Conrad, R. Gross, Irreducible specialization in genus 0, submitted.

[4] S. Gao, AIM workshop on "Future directions in algorithmic number theory", March 24-28, 2003, American Institute of Mathematics, Palo Alto, CA, Problem 6, *http://www.aimath.org/ARCC/workshops/primesinp.html*

[5] W-D. Geyer, M. Jarden, Bounded realization of l-groups over global fields, *Nagoya Math. J.* ***150*** *(1998) 13–62.*

[6] R. Hartshorne, Algebraic Geometry, *Graduate Texts in Mathematics* ***52****, Springer-Verlag, New York, NY, 1977.*

[7] A. Hurwitz, Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten, *Math. Ann.* ***39*** *(1891) 1–61 and Math. Werke, Band 1/XXI, Birkhäuser, Basel, 1932.*

[8] N. Katz, Pinceaux de Lefschetz: théorème d'existence, Exposé XVII in: *Groupes de monodromie en géométrie algébrique II, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), [P. Deligne, N. Katz, eds.] Lecture Notes in Mathematics* ***340*** *(1973) 212–253, Springer-Verlag, Berlin-New York.*

[9] S. L. Kleiman, Tangency and duality, in: *Proceedings of the 1984 Vancouver conference in algebraic geometry, [J. Carrell, A. V. Geramita, P. Russell, eds.] CMS Conf. Proc.* ***6*** *(1986) 163–225, Amer. Math. Soc., Providence, RI.*

[10] H. Kornblum, Über die Primfunktionen in einer arithmetischen Progression, *Math. Z.* ***5*** *(1919) 100–111, published from the author's manuscript by Edmund Landau.*

[11] M. Rosen, Number theory in function fields, *Springer–Verlag, New-York, NY, 2002.*

[12] A. Schinzel, W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arithmetica* ***IV*** *(1958) 185–208; corrigé ibid.* ***V*** *(1958) 259.*

[13] J-P. Serre, Topics in Galois theory, *Research Notes in Mathematics* ***1****, Jones and Bartlett Publishers, Boston, MA, 1992.*