PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 144, Number 6, June 2016, Pages 2361–2373
http://dx.doi.org/10.1090/proc/12941
Article electronically published on October 21, 2015

MULTIPLICATIVE SUBGROUPS AVOIDING LINEAR RELATIONS IN FINITE FIELDS AND A LOCAL-GLOBAL PRINCIPLE

HECTOR PASTEN AND CHIA-LIANG SUN

(Communicated by Matthew A. Papanikolas)

Abstract. We study a local-global principle for polynomial equations with coefficients in a finite field and solutions restricted in a rank-one multiplicative subgroup in a function field over this finite field. We prove such a local-global principle for all sufficiently large characteristics, and we show that the result should hold in full generality under a certain reasonable hypothesis related to the existence of large multiplicative subgroups of finite fields avoiding linear relations. We give a method for verifying the latter hypothesis in specific cases, and we show that it is a consequence of the classical Artin primitive root conjecture. In particular, this function field local-global principle is a consequence of GRH. We also discuss the relation of these problems with a finite field version of the Manin-Mumford conjecture.

1. Introduction

Let K be a global field, S a finite set of places of K containing Archimedean ones (if any), and O_S the ring of S-integral elements in K. For any ring R, let $R^\times$ be the group of units in R. Given a positive integer n, a polynomial $f \in O_S[X_1, \dots, X_n]$ and a subgroup $\Gamma \subseteq O_S^\times$, we consider the following conditions (here, Γ^n is the n-th cartesian power of Γ):

($\mathrm{L}^{f,\Gamma}$) *For every non-zero ideal* $\mathfrak{a} \subseteq O_S$ *there exists* $(x_1, \dots, x_n) \in \Gamma^n$ *such that* $f(x_1, \dots, x_n) \in \mathfrak{a}$.

($\mathrm{G}^{f,\Gamma}$) *There exists* $(x_1, \dots, x_n) \in \Gamma^n$ *such that* $f(x_1, \dots, x_n) = 0$.

The condition ($\mathrm{L}^{f,\Gamma}$) can be seen as a local vanishing condition, while ($\mathrm{G}^{f,\Gamma}$) is a global one. A natural question is whether ($\mathrm{L}^{f,\Gamma}$) implies ($\mathrm{G}^{f,\Gamma}$), and the purpose of this note is to make some progress on this matter in the positive characteristic case.

As an interpretation of an old conjecture of Skolem, the implication ($\mathrm{L}^{f,\Gamma}$) $\Rightarrow$ ($\mathrm{G}^{f,\Gamma}$) was proposed by Harari and Voloch (Remark 2.5 in [5]) in the case where f is a linear form. In the case where K is a number field and f has total degree one and involves at most two monomials, this implication is implicitly proved by Skolem [13]. When K is a global function field with constant field $\mathbb{F}_q$, the second author (immediate consequences of Theorem 1 in [14] and of Theorem 2 in [15]) proves ($\mathrm{L}^{f,\Gamma}$) $\Rightarrow$ ($\mathrm{G}^{f,\Gamma}$) under some additional hypotheses on f; those hypotheses

Received by the editors February 24, 2015 and, in revised form, July 19, 2015.
2010 *Mathematics Subject Classification.* Primary 12E20, 14G05.
The first author was supported by a Benjamin Peirce Fellowship.
The second author was supported by an Academia Sinica Postdoctoral Fellowship.

always fail when f has constant coefficients, i.e. $f \in \mathbb{F}_q[X_1, \dots, X_n]$, and involves at least three monomials. In the present work we investigate the implication $(\mathrm{L}^{f,\Gamma}) \Rightarrow (\mathrm{G}^{f,\Gamma})$, precisely in the case where f has constant coefficients and has an arbitrary number of monomials.

Remark 1. Consider the condition $({\mathrm{L}_*}^{f,H})$ (resp. $({\mathrm{G}_*}^{f,H})$) obtained from $(\mathrm{L}^{f,\Gamma})$ (resp. $(\mathrm{G}^{f,\Gamma})$) by replacing the subgroup $\Gamma^n \subseteq (O_S^\times)^n$ with a subgroup $H \subseteq (O_S^\times)^n$. Under the assumption that H is cyclic such that the subset of $O_S^\times$ consisting of those elements appearing as some component of some element in H generates a subgroup of $O_S^\times$ with rank at most one, Bartolome, Bilu and Luca (Theorem 1.2 in [2]) prove the implication $({\mathrm{L}_*}^{f,H}) \Rightarrow ({\mathrm{G}_*}^{f,H})$ in the number field case. Using an essentially different argument, the second author (Corollary 2 in [16]) generalizes this result to any global field.

Our main result on the local-global principle (Theorem 1.1 below) relies on the following condition, where m is a positive integer, q is a prime power, and r is a positive integer relatively prime to q:

Cond(m,q,r): For any $(a_1, \dots, a_m) \in \mathbb{F}_q^m$ such that $\sum_{i=1}^m a_i \neq 0$, we have $\sum_{i=1}^m a_i \xi_r^{e_i} \neq 0$ for every $(e_1, \dots, e_m) \in \mathbb{Z}^m$, where $\xi_r \in (\mathbb{F}_q^{\mathrm{alg}})^\times$ is a primitive r-th root of unity.

We need some more notation to state our main result. If K is a global function field with constant field $\mathbb{F}_q$ and $\Gamma \subseteq O_S^\times$ is a subgroup, we let $\mathbb{F}_q(\Gamma)$ be the minimal subfield of K containing both $\mathbb{F}_q$ and Γ. Also, we denote by $\mathrm{Tor}(\Gamma)$ the torsion subgroup of Γ. Consider the following condition:

$(\mathrm{L}_{\mathrm{pr}}^{f,\Gamma})$ For every prime ideal $\mathfrak{p} \subseteq O_S$, there exists $(x_1, \dots, x_n) \in \Gamma^n$ such that $f(x_1, \dots, x_n) \in \mathfrak{p}$.

Clearly we have $(\mathrm{L}^{f,\Gamma}) \Rightarrow (\mathrm{L}_{\mathrm{pr}}^{f,\Gamma})$ and $(\mathrm{G}^{f,\mathrm{Tor}(\Gamma)}) \Rightarrow (\mathrm{G}^{f,\Gamma})$. Note that in the case where Γ is finite, the implication $(\mathrm{L}_{\mathrm{pr}}^{f,\Gamma}) \Rightarrow (\mathrm{G}^{f,\Gamma}) \Leftrightarrow (\mathrm{G}^{f,\mathrm{Tor}(\Gamma)})$ is trivial since any non-zero element in K cannot lie in infinitely many prime ideals of O_S. With this trivial case excluded, the next result addresses a local-global principle which is more precise than the conjectural implication $(\mathrm{L}^{f,\Gamma}) \Rightarrow (\mathrm{G}^{f,\Gamma})$ discussed above, in the case where K is a global function field and f has constant coefficients.

Theorem 1.1. *Suppose that K is a global function field with constant field $\mathbb{F}_q$. Let $\Gamma \subseteq O_S^\times$ be a rank-one subgroup, n a positive integer and $f \in \mathbb{F}_q[X_1, \dots, X_n]$. Then $(\mathrm{L}_{\mathrm{pr}}^{f,\Gamma}) \Rightarrow (\mathrm{G}^{f,\mathrm{Tor}(\Gamma)})$ provided that* Cond(m,q,r) *holds, where m is the number of monomials appearing in the expansion of*

$$\prod_{(\tau_1,\dots,\tau_n) \in \mathrm{Tor}(\Gamma)^n} f(\tau_1 X_1, \dots, \tau_n X_n),$$

and r is a positive integer larger than the cardinality of the residue field of the global field $\mathbb{F}_q(\Gamma)$ at any $w \in \Sigma_{\mathbb{F}_q(\Gamma)}$ lying below some place in S.

This theorem is proved in Section 5. We may remove the hypothesis on Cond(m,q,r) if we could establish the following statement for each positive integer m and each prime power q:

Conjecture (Conj(m,q))**.** *The condition* Cond(m,q,r) *holds for infinitely many positive integers r relatively prime to q.*

Statements similar to $\mathrm{Conj}(m,q)$ have already attracted the attention of researchers, especially in the form "large multiplicative subgroups of finite fields must satisfy some additive relation"; see for instance [1] and the references therein.

It is thus natural to investigate to what extent we can establish $\mathrm{Conj}(m,q)$. Note that $\mathrm{Conj}(2,q)$ holds; indeed, for any $(a_1,a_2)\in\mathbb{F}_q^2$ with $a_1\neq -a_2$, the quotient $-\frac{a_1}{a_2}$ is a non-trivial $(q-1)$-th root of unity and thus cannot be an r-th root of unity provided that $\gcd(q-1,r)=1$; thus $\mathrm{Cond}(2,q,r)$ holds for such r. The case of $m=3$ is established unconditionally in the following result.

Theorem 1.2. *Suppose that* $m\leq 3$. *Then* $\mathrm{Cond}(m,2^t,4^{kt}+1)$ *and* $\mathrm{Cond}(m,q,\frac{q^{2k}+1}{2})$ *both hold for all natural numbers* k, t, *and odd prime powers* q. *Hence, for* $m\geq 3$ *we have that* $\mathrm{Conj}(m,q)$ *holds for all prime powers* q.

We prove Theorem 1.2 in Section 2, based on a study of Fermat curves.

Let us recall Artin's primitive root conjecture (APRC): for every non-square positive integer a, the following statement should hold:

$\mathrm{APRC}(a)$ There are infinitely many primes ℓ such that a generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$.

The relevance of APRC in our context is due to the following result.

Theorem 1.3. *Let* m *be a positive integer, let* p *be a prime and let* $q=p^t$ *with* $t\geq 1$. *If there is a prime* $\ell\geq m^t$ *satisfying that* p *generates* $(\mathbb{Z}/\ell\mathbb{Z})^\times$, *then* $\mathrm{Cond}(m,q,\ell)$ *is true. In particular,* $\mathrm{APRC}(p)$ *implies* $\mathrm{Conj}(m,q)$ *for all* m *and for all* q *a power of* p.

After the work of Gupta and Murty [4], Murty and Srinivasan [11] and finally by Heath-Brown (Corollary 2 in [6]), we know that $\mathrm{APRC}(p)$ holds for all but at most *two* prime numbers p. Moreover, Hooley [8] showed that the generalized Riemann hypothesis (GRH) for certain Dedekind zeta functions implies a sharp form of APRC, namely, that for every non-square positive integer a there is a set of primes S with positive natural density in the primes such that a generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$ for each prime $\ell\in S$. These results towards APRC, together with Theorem 1.1 and Theorem 1.3, yield the next consequence for the local-global principle.

Theorem 1.4. *For all primes* p *with at most two exceptions (hence, for all sufficiently large primes* p*), the following local-global principle holds:*

Let K *be a global function field with constant field* $\mathbb{F}_q$ *of characteristic* p. *Let* $\Gamma\subseteq O_S^\times$ *be a rank-one subgroup, let* n *be a positive integer and let* $f\in\mathbb{F}_q[X_1,\dots,X_n]$. *Then* $(\mathrm{L}_{\mathrm{pr}}^{f,\Gamma})\Rightarrow(\mathrm{G}^{f,\mathrm{Tor}(\Gamma)})$.

Moreover, GRH implies that the local-global principle holds without restrictions on the characteristic.

While there is no prime p for which it is unconditionally known that $\mathrm{APRC}(p)$ holds, the next result permits the verification of $\mathrm{Conj}(m,q)$ for any given m and q after a finite amount of computations which finds an odd prime ℓ validating the hypothesis in the following statement.

Theorem 1.5. *Let* m *be a positive integer, and let* $q=p^t$ *be a prime power with* p *prime. Suppose that there is an odd prime* $\ell>m^t$ *such that* p *generates* $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. *Then* $\mathrm{Cond}(m,q,\ell^k)$ *is true for all* $k\geq 1$, *hence* $\mathrm{Conj}(m,q)$ *holds.*

One can ask if the hypothesis in Theorem 1.5 is expected to be satisfied, so that a finite computation is enough to successfully verify $\mathrm{Conj}(m,q)$. In fact, this is the case as we now explain.

Recall that a prime number ℓ is called a Wieferich prime to the base a if $a^{\ell-1} \equiv 1 \bmod \ell^2$. In this terminology, the hypothesis in Theorem 1.5 always holds under the assumption that for any prime p, there are infinitely many non-Wieferich primes ℓ to base p such that p generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$. This assumption is implied by two well-known conjectures in analytic number theory. First, it is widely believed that the set of Wieferich primes to any given basis has natural density zero; see [10]. Moreover, the result of Hooley on APRC mentioned above shows that under GRH we have a positive proportion of primes ℓ for which p is a primitive root modulo ℓ. Therefore, assuming GRH and the sparseness of Wieferich primes, one may always verify $\mathrm{Conj}(m,q)$ by using Theorem 1.5. For the sake of concreteness, here is a simple numerical example:

Let us check that $\mathrm{Conj}(4,9)$ holds. In the notation of Theorem 1.5 we have $m=4$, $p=3$, $q=9$, $t=2$, and we need to find a prime $\ell > m^t = 16$ such that $p=3$ generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. The relevant information for the first few primes $\ell > 16$ is in the following table:

ℓ	17	19	23	29
$\#(\mathbb{Z}/\ell^2\mathbb{Z})^\times$	272	342	506	812
$\#\langle 3\rangle$	272	342	253	812

Thus, we can take $\ell = 17, 19$ or 29 to conclude that $\mathrm{Conj}(4,9)$ holds. (Instead of checking if 3 is a primitive root modulo ℓ^2 for primes $\ell > 16$, we could have checked if 3 is a primitive root modulo ℓ and then verify if it is modulo ℓ^2 – the previous heuristic suggests that this approach is more efficient in general.)

We prove both Theorem 1.3 and Theorem 1.5 in Section 3.

There is also a connection between our $\mathrm{Conj}(m,q)$ and the Manin-Mumford conjecture. The latter conjecture does not have an obvious analogue over finite fields (note that we do *not* mean global function fields) because all algebraic points of a semi-abelian variety A defined over $\mathbb{F}_q$ are torsion. However, Poonen proposed an analogue for the Manin-Mumford conjecture over finite fields, based on the idea that for a semi-abelian variety $A/\mathbb{F}_q$ one should consider a point in $A(\mathbb{F}_q^{\mathrm{alg}})$ as non-torsion whenever its order is 'large' in a precise way. See Section 4 in [18] or Conjecture 4.2 in Section 4 below for the precise statement of Poonen's conjecture. In Section 4 we prove Theorem 4.4, which roughly says that a much weaker version of Poonen's conjecture implies the following stronger version of $\mathrm{Conj}(m,q)$, where m is a positive integer and q is a prime power.

Conjecture ($\mathrm{sConj}(m,q)$)**.** *There is a set of primes $\mathcal{L}$ (depending on m and q) with natural density 1 in the primes such that the condition $\mathrm{Cond}(m,q,\ell)$ holds for all $\ell \in \mathcal{L}$.*

Here, we recall that the (natural) density of a set of primes $\mathcal{P}$ (in the primes) is the following quantity, provided that it exists:

$$\lim_{t\to+\infty} \frac{\#\mathcal{P} \cap [1,t]}{\pi(t)}$$

where $\pi(t)$ is the number of prime numbers up to t.

2. Conj(m,q) and Fermat curves

This section is devoted to proving Theorem 1.2. Our approach using Fermat curves originates in the work of Yekhanin (cf. Lemma 5, Theorem 6 and Corollary 7 in [19]). See also the appendix in [1].

For every $i \in \mathbb{N}$, we denote by $\mu(i) \subseteq (\mathbb{F}_q^{\mathrm{alg}})^\times$ the finite subgroup generated by a primitive i-th root of unity.

Lemma 2.1. *Suppose that $n \leq 3$ and let $a_1, \ldots, a_n \in \mathbb{F}_q^*$. Then every $\mathbb{F}_{q^4}$-rational point on the Fermat hypersurface in $\mathbb{P}^{n-1}$ defined by $\sum_{i=1}^n a_i X_i^{q+1} = 0$ is actually $\mathbb{F}_{q^2}$-rational.*

Proof. We can assume that $n = 3$, for otherwise the result can be easily checked. Note that each $a_i \in \mathbb{F}_q^*$ is a $(q+1)$-th power of elements in $\mathbb{F}_{q^2}$. So we may further assume that $a_i = 1$ for each i.

Denote by $V \subseteq \mathbb{P}^2$ the Fermat curve defined by $\sum_{i=1}^3 X_i^{q+1} = 0$. Letting $[x_1 : x_2 : x_3] \in V(\mathbb{F}_{q^4})$ we note that $[x_1^{q^2} : x_2^{q^2} : x_3^{q^2}] \in V(\mathbb{F}_{q^4})$. For clarity, we assume that $x_i \in \mathbb{F}_{q^4}$ for each i.

It suffices to show that $[x_1 : x_2 : x_3] = [x_1^{q^2} : x_2^{q^2} : x_3^{q^2}]$ in $\mathbb{P}^2$. Assume that this is false. Then there is a unique line L in $\mathbb{P}^2$ passing through $[x_1 : x_2 : x_3]$ and $[x_1^{q^2} : x_2^{q^2} : x_3^{q^2}]$, and it is parameterized as $[sx_1 + tx_1^{q^2} : sx_2 + tx_2^{q^2} : sx_3 + tx_3^{q^2}]$ with $[s,t] \in \mathbb{P}^1$. The line L is contained in V as the following calculation shows:

$$\begin{aligned}\sum_{i=1}^3 (sx_i + tx_i^{q^2})^{q+1} &= \sum_{i=1}^3 (sx_i + tx_i^{q^2})(s^q x_i^q + t^q x_i^{q^3}) \\ &= s^{q+1} \sum_{i=1}^3 x_i^{q+1} + st^q \sum_{i=1}^3 x_i^{q^3+1} + s^q t \left(\sum_{i=1}^3 x_i^{q+1} \right)^q + t^{q+1} \left(\sum_{i=1}^3 x_i^{q+1} \right)^{q^2} \\ &= 0 + st^q \sum_{i=1}^3 x_i^{q^3+1} + 0 + 0 = 0,\end{aligned}$$

where the last equality holds since $\left(\sum_{i=1}^3 x_i^{q^3+1}\right)^q = \sum_{i=1}^3 x_i^{q^4+q} = \sum_{i=1}^3 x_i^{1+q} = 0$. However, V is a Fermat curve of degree $q+1$, thus it cannot contain a line, and we obtain a contradiction. □

Note that $\mathbb{F}_q^* \subseteq \mu(\frac{q^4-1}{q+1}) \subseteq \mathbb{F}_{q^4}^*$.

Proposition 2.2. *Suppose that $n \leq 3$. Let $x_1, \ldots, x_n \in \mu(\frac{q^4-1}{q+1})$ and $a_1, \ldots, a_n \in \mathbb{F}_q^*$ satisfy $\sum_{i=1}^n a_i x_i = 0$. Then $x_1, \ldots, x_n$ reduce to the same element in the quotient $\mu(\frac{q^4-1}{q+1})/\mathbb{F}_q^*$.*

Proof. Letting $y_1, \ldots, y_n \in \mathbb{F}_{q^4}^*$ such that $x_i = y_i^{q+1}$ for each i, we see that $[y_1, \ldots, y_n]$ is an $\mathbb{F}_{q^4}$-rational point on the hypersurface in $\mathbb{P}^{n-1}$ defined by $\sum_{i=0}^n a_i X_i^{q+1} = 0$. By Lemma 2.1, we have for each i that $\frac{y_i}{y_1} \in \mathbb{F}_{q^2}^*$, whence $\frac{x_i}{x_1} = (\frac{y_i}{y_1})^{q+1} \in \mathbb{F}_q^*$. □

Corollary 2.3. *Suppose that $n \leq 3$. Let $a_1, \ldots, a_n \in \mathbb{F}_q^*$ satisfy $\sum_{i=1}^n a_i \neq 0$. When q is even, we put $G = \mu(q^2+1)$; when q is odd, we put $G = \mu(\frac{q^2+1}{2})$. Then there is no $(x_1, \ldots, x_n) \in G^n$ such that $\sum_{i=1}^n a_i x_i = 0$.*

Proof. Assume that for some $(x_1, \dots, x_n) \in G^n$ we have $\sum_{i=1}^n a_i x_i = 0$. Since $G \subseteq \mu(\frac{q^4-1}{q+1})$ for any prime power q, Proposition 2.2 implies that we may further suppose for all i that $x_i \in \mathbb{F}_q^*$. It follows that $x_i = (x_i^{q-1})^{\frac{q+1}{2}} x_i = x_i^{\frac{q^2+1}{2}} = 1$ when q is odd, and that $x_i^2 = (x_i^{q-1})^{q+1} x_i^2 = x_i^{q^2+1} = 1$, i.e. $x_i = 1$, when q is even. This contradicts the assumption $\sum_{i=1}^n a_i \neq 0$. □

Proof of Theorem 1.2. Fix a natural number k and a prime power q. If q is even, we put $G = \mu(q^{2k}+1)$; if q is odd, we put $G = \mu(\frac{q^{2k}+1}{2})$. By definition of $\mathrm{Cond}(m, q, i)$ and $\mu(i)$, Corollary 2.3 yields the desired result since $a_1, \dots, a_m \in \mathbb{F}_{q^k}^*$ satisfy $\sum_{i=1}^m a_i \neq 0$. □

3. Conj(m, q) and primitive roots

In this section we prove Theorem 1.3 and Theorem 1.5. Both are obtained from a more general result, for which it will be convenient to introduce the following hypothesis for p^t, ℓ^k prime powers and m a positive integer:

$\mathrm{Hyp}(m, p^t, \ell^k)$: p is a primitive root modulo ℓ^k, and $\ell > m^{\gcd(t, \ell^2-\ell)}$.

Theorem 3.1. *Let m, t and k be positive integers, and let p and ℓ be primes. If* $\mathrm{Hyp}(m, p^t, \ell^k)$ *holds, then* $\mathrm{Cond}(m, q, \ell^k)$ *holds.*

Before proving Theorem 3.1, let us first deduce Theorem 1.3 and Theorem 1.5 from it.

Proof of Theorem 1.3. Since p is a primitive root modulo the prime ℓ and $\ell > m^t \geq m^{\gcd(t, \ell^2-\ell)}$, the hypothesis $\mathrm{Hyp}(m, q, \ell)$ in Theorem 3.1 is satisfied, and hence $\mathrm{Cond}(m, q, \ell)$ holds. □

Recall the following elementary fact.

Lemma 3.2. *Let ℓ be an odd prime. If a is a primitive root modulo ℓ^2, then it is a primitive root modulo ℓ^k for all integers $k \geq 1$.*

Proof of Theorem 1.5. Assume, as in the statement, that there is a prime $\ell > m^t \geq m^{\gcd(t, \ell^2-\ell)}$ such that p generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. Fix a natural number $k \geq 1$. By Lemma 3.2 we get that p generates $(\mathbb{Z}/\ell^k\mathbb{Z})^\times$. Hence the hypothesis $\mathrm{Hyp}(m, q, \ell^k)$ in Theorem 3.1 is satisfied, and then $\mathrm{Cond}(m, q, \ell^k)$ holds. □

To prove Theorem 3.1, we need the next two elementary lemmas, the first of which is well known.

Lemma 3.3. *The cyclotomic polynomial $\Phi_m(x) \in \mathbb{Z}[x]$ factors in $\mathbb{F}_q[x]$ as a product of distinct irreducible polynomials all of which have degree equal to the order of q in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$, where m is a positive integer relatively prime to the prime power q.*

Lemma 3.4. *Let k be a field, $P \in k[X]$ a polynomial and N a positive integer. Let $R \in k[X]$ be the remainder of P divided by $X^N - 1$. The number of monomials in R is at most the number of monomials in P.*

Proof. By induction. Noting that $R = P$ whenever $\deg P < N$, we assume the truth of this lemma in the case where $\deg P < d$ and prove it when $\deg P = d$, where $d \geq N$. Letting $a_d \in k^\times$ be the leading coefficient of P, we note that

$P_0(X) = P(X) - a_d X^{d-N}(X^N - 1)$ is either the zero polynomial or has degree less than d. We also observe that the number of monomials in P_0 is no more than that in P. By the induction hypothesis, the number of monomials in the remainder of $P_0(X)$ divided by $X^N - 1$ is at most that in P_0, which is no more than that in P as observed. Noting that $R(X)$ is also the remainder of $P_0(X)$ divided by $X^N - 1$, we finish the proof. □

Proof of Theorem 3.1. The desired conclusion holds trivially when $m = 1$. Assume that hypothesis $\mathrm{Hyp}(m, q, \ell^k)$ is satisfied for certain positive integers $m \geq 2$, prime powers $q = p^t$ and ℓ^k. We note that ℓ cannot divide t, for otherwise one would have $\ell > m^{\gcd(t,\ell^2-\ell)} \geq m^\ell \geq 2^\ell$, a contradiction. This gives $\gcd(t, \ell^k - \ell^{k-1}) = \gcd(t, \ell - 1) = \gcd(t, \ell^2 - \ell)$.

Suppose that $\mathrm{Cond}(m, q, \ell^k)$ fails, i.e., for some $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$ with $\sum_{i=1}^m a_i \neq 0$ we have

$$\sum_{i=1}^{m} a_i \xi_{\ell^k}^{e_i} = 0 \tag{3.1}$$

for some $(e_1, \ldots, e_m) \in \mathbb{Z}^m$, where $\xi_{\ell^k} \in (\mathbb{F}_q^{\mathrm{alg}})^\times$ is a primitive ℓ^k-th root of unity. For each prime-to-ℓ integer $0 \leq e \leq \ell^k - 1$, let f_e be the unique integer such that $0 \leq f_e \leq \ell^k - 1$ and $ef_e \in 1 + \ell^k\mathbb{Z}$; we define the auxiliary polynomials

$$P_e(X) = \sum_{i=1}^{m} a_i X^{e_i f_e} \in \mathbb{F}_q[X].$$

Using (3.1) we see that $P_e(\xi_{\ell^k}^e) = 0$ for each prime-to-ℓ integer $0 \leq e \leq \ell^k - 1$.

Since p generates the finite abelian group $(\mathbb{Z}/\ell^k\mathbb{Z})^\times$ with cardinality $\ell^k - \ell^{k-1}$, the order of $q = p^t$ in $(\mathbb{Z}/\ell^k\mathbb{Z})^\times$ is $\frac{\ell^k - \ell^{k-1}}{d}$, where $d = \gcd(t, \ell^k - \ell^{k-1}) = \gcd(t, \ell^2 - \ell)$ as noted in the beginning of this proof. By Lemma 3.3, the cyclotomic polynomial Φ_{ℓ^k} factors as a product of d distinct irreducible polynomials over $\mathbb{F}_q$. As each root of Φ_{ℓ^k} in $\mathbb{F}_q^{\mathrm{alg}}$ is ξ^e for some prime-to-ℓ integer $0 \leq e \leq \ell^k - 1$, there are d prime-to-ℓ integers $0 \leq n_1 < \cdots < n_d \leq \ell^k - 1$ such that Φ_{ℓ^k} divides the product $P_{n_1} \cdots P_{n_d}$ over $\mathbb{F}_q$. Let $R \in \mathbb{F}_q[X]$ be the remainder obtained when we perform the Euclidean division of $(P_{n_1} \cdots P_{n_d})(X)$ by $X^{\ell^k} - 1$ in $\mathbb{F}_q[X]$. Since $R(1) = (P_{n_1} \cdots P_{n_d})(1) = \left(\sum_{i=1}^m a_i\right)^d \neq 0$, we note that R is not the zero polynomial. Also, by Lemma 3.4, the number of monomials appearing in R is no more than that in $P_{n_1} \cdots P_{n_d}$, and thus is at most m^d. Since $\Phi_{\ell^k}(X)$ divides both $P_{n_1} \cdots P_{n_d}$ and $X^{\ell^k} - 1$ in $\mathbb{F}_q[X]$, it follows that Φ_{ℓ^k} divides the non-zero polynomial R, i.e. there is some non-zero polynomial $Q \in \mathbb{F}_q[X]$ such that $R = Q\Phi_{\ell^k}$. Since R has degree at most $\ell^k - 1$ and Φ_{ℓ^k} has degree $\ell^{k-1}(\ell - 1)$, it implies that Q has degree at most $\ell^{k-1} - 1$. Noting that

$$\Phi_{\ell^k}(X) = X^{\ell^{k-1}(\ell-1)} + X^{\ell^{k-1}(\ell-2)} + \cdots + X^{\ell^{k-1}} + 1,$$

we see that the expression

$$R(X) = Q(X)X^{\ell^{k-1}(\ell-1)} + Q(X)X^{\ell^{k-1}(\ell-2)} + \cdots + Q(X)X^{\ell^{k-1}} + Q(X)$$

involves no cancellation among terms. From this, we observe that R has at least ℓ monomials. Since $\ell > m^d$, this is a contradiction to the fact that at most m^d monomials appear in R. This shows that $\mathrm{Cond}(m, q, \ell^k)$ holds. □

4. Finite field analogue of the Manin-Mumford conjecture

In this section, we connect Poonen's analogue of the Manin-Mumford conjecture over finite fields with our conjecture $\mathrm{sConj}(m,q)$, which is a much stronger version of $\mathrm{Conj}(m,q)$. We begin by recalling the statement of the Manin-Mumford conjecture over number fields, which is now a theorem.

Theorem 4.1. *Let K be a number field, let A/K be a semi-abelian variety, and let X/K be a closed subvariety of A. Let Z be the union of all translates of positive-dimensional semi-abelian subvarieties of A defined over K^{alg} and contained in X. Then at most finitely many points $x \in (X \smallsetminus Z)(K^{\mathrm{alg}})$ are torsion.*

A first version of this was proved by Raynaud [12] in the case when X is a curve of genus $g > 1$ embedded in an abelian variety, and since then the result has been extended in a number of ways. The version stated here is due to Hindry (cf. Théorème 2 in [7]). See [17] for a survey on this subject.

As promised in the introduction, let us recall the following finite field analogue of the Manin-Mumford conjecture proposed by Poonen (see Section 4 in [18]).

Conjecture 4.2. *Let k be a finite field, let A/k be a semi-abelian variety, and let X/k be a closed subvariety of A. Let Z be the union of all translates of positive-dimensional semi-abelian subvarieties of A defined over k^{alg} and contained in X. Then there is a positive constant $c > 0$, depending on A and X, such that for all $x \in (X \smallsetminus Z)(k^{\mathrm{alg}})$ we have*

$$\#\langle x\rangle > (\#\kappa_x)^c,$$

where $\langle x\rangle \subset A(k^{\mathrm{alg}})$ is the cyclic subgroup generated by x, and κ_x is the smallest field extension of k such that $x \in A(\kappa_x)$.

One way to think about this conjecture is that, although all $\mathbb{F}_q^{\mathrm{alg}}$-rational points in A are torsion, one should see points of 'large' order as the finite field analogue of non-torsion points. From this point of view, Conjecture 4.2 is analogous to the Manin-Mumford conjecture over number fields. Remarkably, the Manin-Mumford conjecture over number fields is now a theorem (and there are analogous results over function fields; see for instance [9]), while Conjecture 4.2 remains open.

For our purposes, the following weaker version of Conjecture 4.2 will suffice.

Conjecture 4.3. *Let k be a finite field, let A/k be a semi-abelian variety, and let X/k be a closed subvariety of A. Let Z be the union of all translates of positive-dimensional semi-abelian subvarieties of A defined over k^{alg} and contained in X. Then, depending on A and X, there is a positive function $F(t)$ defined on $\mathbb{Z}_{\geq 1}$ satisfying for every $\epsilon > 0$ that $F(t) = O(t^{\epsilon})$ as t goes to infinity, such that for all $x \in (X \smallsetminus Z)(k^{\mathrm{alg}})$ we have*

$$\#\langle x\rangle > \frac{[\kappa_x : k]^2}{F([\kappa_x : k])}, \tag{4.1}$$

where $\langle x\rangle \subset A(k^{\mathrm{alg}})$ is the cyclic subgroup generated by x, and κ_x is the smallest field extension of k such that $x \in A(\kappa_x)$.

To derive Conjecture 4.3 from Conjecture 4.2, just note that $\#\kappa_x = (\#k)^{[\kappa_x:k]}$ and take $F(t) = t^2(\#k)^{-ct}$, which tends to zero as t goes to infinity. This exponentially decaying property is not necessary for our application, where we only have to require that $F(t)$ does not grow too fast; for instance, candidates of type

$F(t) = (\log t)^b$ (with positive constants b) make the bound (4.1) useful. To the best of our knowledge, however, even this much weaker Conjecture 4.3 remains open, although substantial progress has been achieved by Voloch in the case $A = \mathbb{G}_{\mathrm{m}}^2$; see the main Theorem in [18]. We remark that the exponent 2 in (4.1) is critical in Voloch's work.

The main result in this section is the following.

Theorem 4.4. *Let m be a positive integer, and let q be a power of a prime. Suppose that Conjecture 4.3 holds for $k = \mathbb{F}_q$ and any torus A with dimension $< m$. Then* $\mathrm{sConj}(m, q)$ *holds.*

Before proving this result, we need the following lemmas.

Lemma 4.5. *Let K be an algebraically closed field, and let S be a semi-abelian variety embedded in a torus $\mathbb{G}_m^r/K$. Then S is a torus.*

Proof. There is a maximal torus subgroup $T \subseteq S$ such that $A = S/T$ is an abelian variety. On the other hand T is also a subtorus of $\mathbb{G}_{\mathrm{m}}^r$ and the quotient $\mathbb{G}_{\mathrm{m}}^r/T$ is affine. Since A embeds into $\mathbb{G}_{\mathrm{m}}^r/T$, we conclude that A is a point. □

Lemma 4.6. *Let $r \geq 2$ be an integer. Let $a_1, \ldots, a_r \in \mathbb{F}_q$ be non-zero, and let $X/\mathbb{F}_q$ be the subvariety of $\mathbb{G}_m^r/\mathbb{F}_q$ defined by*

$$X: \quad a_1x_1 + \ldots + a_rx_r = 1.$$

Let Z be the union of all translates of positive-dimensional semi-abelian subvarieties of $\mathbb{G}_m^r$ contained in X and defined over $\mathbb{F}_q^{\mathrm{alg}}$. Let Z' be the union of subvarieties of $X \subseteq \mathbb{G}_m^r$ defined by the vanishing of a (proper, non-empty) subsum of $a_1x_1 + \ldots + a_rx_r$. Then $Z \subseteq Z'$.

Proof. Up to a multiplicative translation, we can assume that $a_i = 1$ for each i (because they are non-zero), so X is given by $x_1 + \ldots + x_r = 1$. Let G be a translate of some positive-dimensional (proper) semi-abelian subvariety $T \subset \mathbb{G}_{\mathrm{m}}^r$ contained in X and defined over $\mathbb{F}_q^{\mathrm{alg}}$. By Lemma 4.5, we have $T \simeq \mathbb{G}_{\mathrm{m}}^k$ for some $1 \leq k < r$. It suffices to show for any $b = (b_1, \ldots, b_r) \in G(\mathbb{F}_q^{\mathrm{alg}})$ that some proper non-empty subsum of the b_i vanishes. Since $G = b \cdot T$, there are rational functions $f_i \in \mathbb{F}_q^{\mathrm{alg}}(y)$, $1 \leq i \leq r$, defining a rational map $f = (f_i)_{1 \leq i \leq r} : \mathbb{P}^1 \dashrightarrow T$ which restricts to an embedding of $\mathbb{G}_{\mathrm{m}} \subseteq \mathbb{P}^1$ into T, and since T is an algebraic group and $b \cdot T = G \subset X$, we have for each positive integer n that

$$b_1 f_1^n + \ldots + b_r f_r^n = 1. \tag{4.2}$$

As f is non-constant, some f_i must have a pole at $\mathfrak{p} \in \mathbb{P}^1 \setminus \mathbb{G}_{\mathrm{m}}$. Let $I \subseteq \{1, \ldots, r\}$ be the subset of indices i such that the order of pole for f_i at $\mathfrak{p}$ is maximal over $i \in \{1, \ldots, r\}$. Noting that the right-hand side of (4.2) has no poles, we look at the Taylor expansion of both sides of (4.2) at $\mathfrak{p}$, and find

$$\sum_{i \in I} b_i \alpha_i^n = 0,$$

where $\alpha_i \in (\mathbb{F}_q^{\mathrm{alg}})^\times$ is the first non-zero coefficient of the power series expansion of f_i at $\mathfrak{p}$. Choosing a suitable positive integer n we conclude $\sum_{i \in I} b_i = 0$. Note that I is non-empty by construction, and it is a proper subset of $\{1, \ldots, r\}$ because $\sum_{i=1}^r b_i = 1$. □

We also need the following result of Erdös and Murty (Theorem 1 in [3]).

Theorem 4.7. *Let $f(t)$ be a positive function tending to 0 as t grows. Let $a > 1$ be an integer. Let $\mathcal{P}$ be the set of prime numbers ℓ satisfying that the order of a in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is greater than $\ell^{\frac{1}{2}+f(\ell)}$. Then $\mathcal{P}$ has density 1 in the primes.*

Proof of Theorem 4.4. For any positive integer n, it follows from relabeling and scaling that $\mathrm{sConj}(n, q)$ is equivalent to the following statement: There is a set of primes $\mathcal{L}$ (depending on n and q) with natural density 1 in the primes such that for any $(a_1, \dots, a_{n-1}) \in \mathbb{F}_q^{n-1}$ with $\sum_{i=1}^{n-1} a_i \neq 1$, the equation $\sum_{i=1}^{n-1} a_i x_i = 1$ has no solutions in the group $\mu(\ell)$ of ℓ-th roots of unity in $\mathbb{F}_q^{\mathrm{alg}}$.

Assume that Conjecture 4.3 holds for $k = \mathbb{F}_q$ and any torus A with dimension $< m$. We desire to show that $\mathrm{sConj}(m, q)$ holds; the case where $m = 1$ is trivial. By induction on m, we can assume that $\mathrm{sConj}(n, q)$ holds for all $n < m$.

Write $r = m - 1$ and let $(a_1, \dots, a_r) \in \mathbb{F}_q^r$ be such that $\sum_{i=1}^r a_i \neq 1$. Let X_0 be the subvariety of $\mathbb{G}_{\mathrm{m}}^r$ defined by $\sum_{i=1}^r a_i x_i = 1$; let Z_0 be the union of all translates of positive-dimensional semi-abelian subvarieties of $\mathbb{G}_{\mathrm{m}}^r$ defined over $\mathbb{F}_q^{\mathrm{alg}}$ and contained in X_0. Note that $1 \in (\mathbb{G}_{\mathrm{m}}^r \setminus X_0)(\mathbb{F}_q^{\mathrm{alg}})$.

Let $F(t)$ be the positive function on $\mathbb{Z}_{\geq 1}$ coming from Conjecture 4.3 specialized to the case where $(k, A, X) = (\mathbb{F}_q, \mathbb{G}_{\mathrm{m}}^r, X_0)$. Replacing $F(t)$ by $\max\{F(n) : 1 \leq n \leq t\}$ if necessary, we can assume without loss of generality that $F(t)$ is non-decreasing (keeping the bound (4.1) valid and the property that for every $\epsilon > 0$ we have $F(t) = O(t^\epsilon)$ as t goes to infinity).

Consider the function

$$f(t) = \frac{\log(\max\{1, F(t)\} \cdot \log t)}{\log t}$$

which tends to 0 as t goes to infinity because $F(t) = O(t^\epsilon)$ for every $\epsilon > 0$. Let $\mathcal{P}$ be the set of primes ℓ such that q has order larger than

$$\ell^{\frac{1}{2}+f(\ell)} = \ell^{\frac{1}{2}} \max\{1, F(\ell)\} \log \ell$$

in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. By Theorem 4.7 we know that $\mathcal{P}$ has density 1 in the primes.

Now we show for any $\ell \in \mathcal{P}$ that

$$\mu(\ell)^r \cap (X_0 \smallsetminus Z_0)(\mathbb{F}_q^{\mathrm{alg}}) = \emptyset. \tag{4.3}$$

Indeed, under Conjecture 4.3, we have for all $x \in (X_0 \smallsetminus Z_0)(\mathbb{F}_q^{\mathrm{alg}})$ that

$$\#\langle x \rangle > \frac{[\kappa_x : \mathbb{F}_q]^2}{F([\kappa_x : \mathbb{F}_q])}.$$

Suppose that for some $\ell \in \mathcal{P}$ the set $\mu(\ell)^r \cap (X_0 \smallsetminus Z_0)(\mathbb{F}_q^{\mathrm{alg}})$ is not empty and contains some element x. Then we would derive the following contradiction:

$$\begin{aligned} \ell = \#\langle x \rangle &> \frac{[\kappa_x : \mathbb{F}_q]^2}{F([\kappa_x : \mathbb{F}_q])} > \frac{\ell \max\{1, F(\ell)\}^2 (\log \ell)^2}{F(\ell)} \\ &\geq \ell \max\{F(\ell), \frac{1}{F(\ell)}\} (\log \ell)^2 \geq \ell (\log \ell)^2, \end{aligned}$$

where the first equality is due to the condition $1 \notin X_0(\mathbb{F}_q^{\mathrm{alg}})$, and the second inequality is deduced as follows: Lemma 3.3 gives that $[\kappa_x : \mathbb{F}_q]$ equals the order of q modulo ℓ, hence

$$\ell^{\frac{1}{2}} \max\{1, F(\ell)\} \log \ell < [\kappa_x : \mathbb{F}_q] < \ell$$

which, together with the fact that F is non-decreasing, yields the desired inequality. This proves (4.3).

It remains to claim that there is a set of primes $\mathcal{P}'$ of density 1 such that for all $\ell \in \mathcal{P}'$ we have

$$\mu(\ell)^r \cap Z_0(\mathbb{F}_q^{\mathrm{alg}}) = \emptyset, \tag{4.4}$$

since then for every ℓ in the set of primes $\mathcal{P} \cap \mathcal{P}'$ having density 1, we have

$$\mu(\ell)^r \cap X_0(\mathbb{F}_q^{\mathrm{alg}}) = \emptyset,$$

i.e. $\mathrm{sConj}(m, q)$ holds. By Lemma 4.6, Z_0 is contained in the union of subvarieties of $X_0 \subseteq \mathbb{G}_{\mathrm{m}}^r$ defined by the vanishing of $\sum_{i\in I} a_i x_i$ over all (finitely many) non-empty (proper) subsets $I \subsetneq \{1, \dots, r\}$. It suffices to show that for every such I there is a set of primes $\mathcal{P}'_I$ with density 1 such that for all $\ell \in \mathcal{P}'_I$ there is no common solution for $\sum_{i\in I} a_i x_i = 0$ and $\sum_{i=1}^r a_i x_i = 1$ (equivalently, for $\sum_{i\in\{1,\dots,r\}\smallsetminus I} a_i x_i = 1$ and $\sum_{i=1}^r a_i x_i = 1$) over $\mu(\ell)$, for then we can let $\mathcal{P}' = \bigcap_{I\subsetneq\{1,\dots,r\}} \mathcal{P}'_I$ since the intersection of finitely many sets of primes with density 1 also has density 1. Since $\#I \le r < m$ and $\#(\{1, \dots, r\} \smallsetminus I) \le r - 1 < m - 1$, the induction hypothesis guarantees that both $\mathrm{sConj}(\#I, q)$ and $\mathrm{sConj}(\#(\{1, \dots, r\} \smallsetminus I) + 1, q)$ holds. Note that since $\sum_{i=1}^r a_i \neq 1$, we have either $\sum_{i\in I} a_i \neq 0$ or $\sum_{i\in\{1,\dots,r\}\smallsetminus I} a_i \neq 1$. By the first sentence of this proof, we therefore conclude that the desired $\mathcal{P}'_I$ always exists. This finishes our proof. □

5. Proof of Theorem 1.1

For the purposes of this section, a *monomial* means a product of variables in a polynomial ring (the empty product gives the monomial 1 by convention), while a *term* is a monomial multiplied by a non-zero coefficient.

Lemma 5.1. *Suppose that K is a global function field with constant field $\mathbb{F}_q$. Let $\Gamma \subseteq O_S^\times$ be a finitely generated subgroup and let $\Phi \subseteq \Gamma$ be a free subgroup such that $\Gamma = \{\tau\phi : \tau \in \mathrm{Tor}(\Gamma), \phi \in \Phi\}$; note that such Φ always exists (as Γ is finitely generated abelian), and that $\mathrm{Tor}(\Gamma) \subseteq \mathbb{F}_q$. Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ and define*

$$g = \prod_{(\tau_1,\dots,\tau_n)\in\mathrm{Tor}(\Gamma)^n} f(\tau_1 X_1, \dots, \tau_n X_n) \in \mathbb{F}_q[X_1, \dots, X_n].$$

Let m be the number of terms appearing in g after expanding it, and let $h \in \mathbb{F}_q[Y_1, \dots, Y_m]$ be the linear form obtained by formally replacing the monomials in g by new variables Y_i and keeping the respective coefficients. Suppose that $(\mathrm{L}_{\mathrm{pr}}^{h,\Phi}) \Rightarrow (\mathrm{G}^{h,\{1\}})$ holds. Then $(\mathrm{L}_{\mathrm{pr}}^{f,\Gamma}) \Rightarrow (\mathrm{G}^{f,\mathrm{Tor}(\Gamma)})$ holds.

Proof. From $\Gamma = \{\tau\phi : \tau \in \mathrm{Tor}(\Gamma), \phi \in \Phi\}$, it follows that $(\mathrm{L}_{\mathrm{pr}}^{f,\Gamma})$ implies $(\mathrm{L}_{\mathrm{pr}}^{g,\Phi})$, and that $(\mathrm{G}^{g,\{1\}})$ implies $(\mathrm{G}^{f,\mathrm{Tor}(\Gamma)})$. On the other hand, by construction of h we see that $(\mathrm{L}_{\mathrm{pr}}^{g,\Phi})$ implies $(\mathrm{L}_{\mathrm{pr}}^{h,\Phi})$, and that $(\mathrm{G}^{h,\{1\}})$ implies $(\mathrm{G}^{g,\{1\}})$. This finishes the proof. □

Proposition 5.2. *Let K be a global function field of characteristic p with constant field $\mathbb{F}_q$. Let $\Phi \subseteq O_S^\times$ be an infinite cyclic subgroup, and let m be a positive integer. Then for any positive integers m and every linear form $h \in \mathbb{F}_q[X_1, \dots, X_m]$ which has m monomials, we have $(\mathrm{L}_{\mathrm{pr}}^{h,\Phi}) \Rightarrow (\mathrm{G}^{h,\{1\}})$ provided that $\mathrm{Cond}(m, q, r)$ holds, where r is a positive integer larger than the cardinality of the residue field of the global field $\mathbb{F}_q(\Phi)$ at any $w \in \Sigma_{\mathbb{F}_q(\Phi)}$ lying below some place in S.*

Proof. Let $h = \sum_{i=1}^m a_i X_i$ for certain $a_1, \dots, a_m \in \mathbb{F}_q^\times$. Suppose that $(\mathrm{G}^{h,\{1\}})$ fails, that is, $\sum_{i=1}^m a_i = h(1, \dots, 1) \neq 0$. It suffices to show that $(\mathrm{L}_{\mathrm{pr}}^{h,\Phi})$ fails. By the assumption that $\mathrm{Cond}(m, q, r)$ holds, since $\sum_{i=1}^m a_i \neq 0$, we have $\sum_{i=1}^m a_i \xi_r^{e_i} \neq 0$ for every $(e_1, \dots, e_m) \in \mathbb{Z}^m$, where $\xi_r \in (\mathbb{F}_q^{\mathrm{alg}})^\times$ is a primitive r-th root of unity.

Let $\gamma \in K^\times \smallsetminus \mathbb{F}_q$ generate Φ. We note that $\mathbb{F}_q(\Phi) = \mathbb{F}_q(\gamma)$ and that the extension $K/\mathbb{F}_q(\Phi)$ is finite. Consider the $\mathbb{F}_q$-isomorphism of fields $\mathbb{F}_q(T) \simeq \mathbb{F}_q(\Phi)$ given by $T \mapsto \gamma$. Let $F \in \mathbb{F}_q[T]$ be the minimal polynomial of ξ_r over $\mathbb{F}_q$. Under this isomorphism, the irreducible polynomial F corresponds to a place $w_0 \in \Sigma_{\mathbb{F}_q(\Phi)}$. Since the residue field of $\mathbb{F}_q(\Phi)$ at w_0 contains ξ_r, the cardinality of this residue field must exceed r, and hence the property of r ensures that w_0 does not lie below any place in S. Let $\mathfrak{P}$ be the maximal ideal associated to a place $v_0 \in \Sigma_K$ above $w_0 \in \Sigma_{\mathbb{F}_q(\Phi)}$. Then we have $v_0 \notin S$ and thus $\mathfrak{P} \subset O_S$ is a prime ideal.

Now we show that $(\mathrm{L}_{\mathrm{pr}}^{h,\Phi})$ fails by proving that for all $(e_1, \dots, e_m) \in \mathbb{Z}^m$ we have $\sum_{i=1}^m a_i \gamma^{e_i} \notin \mathfrak{P}$. Suppose that $\sum_{i=1}^m a_i \gamma^{e_i} \in \mathfrak{P}$ for some $(e_1, \dots, e_m) \in \mathbb{Z}^m$. Then $\sum_{i=1}^m a_i \gamma^{e_i}$ lies in $\mathfrak{P} \cap \mathbb{F}_q(\Phi)$ and hence vanishes at w_0. The $\mathbb{F}_q$-isomorphism of fields $\mathbb{F}_q(T) \simeq \mathbb{F}_q(\Phi)$ given by $T \mapsto \gamma$ shows that the rational function $\sum_{i=1}^m a_i T^{e_i}$ lies in the ideal generated by F in $\mathbb{F}_q[T, T^{-1}]$. Since $F(\xi_r) = 0$, we deduce that $\sum_{i=1}^m a_i T^{e_i}$ vanishes at ξ_r. This contradicts $\mathrm{Cond}(m, q, r)$ and finishes our proof. □

Proof of Theorem 1.1. This follows from the previous two results. □

Acknowledgments

The authors thank Ram Murty and Bjorn Poonen for several discussions and comments that greatly enhanced this work. The authors also thank the anonymous referee for carefully reading this article and for the detailed feedback provided.

This research was initiated during a visit of the first author to Academia Sinica, Taipei, Taiwan, in May of 2014. The first author heartily thanks Julie Wang for this invitation, and he gratefully acknowledges the hospitality and generosity of the Institute of Mathematics at Academia Sinica, and the National Taiwan University.

References

[1] Noga Alon and Jean Bourgain, *Additive patterns in multiplicative subgroups*, Geom. Funct. Anal. **24** (2014), no. 3, 721–739, DOI 10.1007/s00039-014-0270-y. MR3213827

[2] Boris Bartolome, Yuri Bilu, and Florian Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), no. 2, 101–111, DOI 10.4064/aa159-2-1. MR3062909

[3] Pál Erdős and M. Ram Murty, *On the order of a* (mod p), Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 87–97. MR1684594 (2000c:11152)

[4] Rajiv Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130, DOI 10.1007/BF01388719. MR762358 (86d:11003)

[5] David Harari and José Felipe Voloch, *The Brauer-Manin obstruction for integral points on curves*, Math. Proc. Cambridge Philos. Soc. **149** (2010), no. 3, 413–421, DOI 10.1017/S0305004110000381. MR2726726 (2012c:14047)

[6] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38, DOI 10.1093/qmath/37.1.27. MR830627 (88a:11004)

[7] Marc Hindry, *Autour d'une conjecture de Serge Lang* (French), Invent. Math. **94** (1988), no. 3, 575–603, DOI 10.1007/BF01394276. MR969244 (89k:11046)

[8] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR0207630 (34 #7445)

[9] Ehud Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), no. 3, 667–690, DOI 10.1090/S0894-0347-96-00202-0. MR1333294 (97h:11154)

[10] Nicholas M. Katz, *Wieferich past and future*, Topics in finite fields, Contemp. Math., vol. 632, Amer. Math. Soc., Providence, RI, 2015, pp. 253–270, DOI 10.1090/conm/632/12632. MR3329985

[11] M. Ram Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. **30** (1987), no. 1, 80–85, DOI 10.4153/CMB-1987-012-5. MR879875 (88e:11094)

[12] M. Raynaud, *Courbes sur une variété abélienne et points de torsion* (French), Invent. Math. **71** (1983), no. 1, 207–233, DOI 10.1007/BF01393342. MR688265 (84c:14021)

[13] T. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlosbarkeit gewisser diophantischer Gleichungen.* Avhandlinger Utgitt av det Norske Videnskaps-Akademi i Oslo I. Mat.-Naturv. Klasse. Ny Serie, 12: 1-16, 1937.

[14] Chia-Liang Sun, *Product of local points of subvarieties of almost isotrivial semi-abelian varieties over a global function field*, Int. Math. Res. Not. IMRN **19** (2013), 4477–4498. MR3116170

[15] Chia-Liang Sun, *Local-global principle of affine varieties over a subgroup of units in a function field*, Int. Math. Res. Not. IMRN **11** (2014), 3075–3095. MR3214315

[16] Chia-Liang Sun, *The Brauer-Manin-Scharaschkin obstruction for subvarieties of a semi-abelian variety and its dynamical analog*, J. Number Theory **147** (2015), 533–548, DOI 10.1016/j.jnt.2014.07.015. MR3276339

[17] Pavlos Tzermias, *The Manin-Mumford conjecture: a brief survey*, Bull. London Math. Soc. **32** (2000), no. 6, 641–652, DOI 10.1112/S0024609300007578. MR1781574 (2001g:11091)

[18] José Felipe Voloch, *On the order of points on curves over finite fields*, Integers **7** (2007), A49, 4. MR2373111 (2009j:14028)

[19] Sergey Yekhanin, *A note on plane pointless curves*, Finite Fields Appl. **13** (2007), no. 2, 418–422, DOI 10.1016/j.ffa.2006.11.001. MR2307138 (2008b:14032)

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, Massachusetts 02138

E-mail address: hpasten@math.harvard.edu

Institute of Mathematics, Academia Sinica, Room 626, 6F, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan

E-mail address: csun@math.sinica.edu.tw