The Quarterly Journal of Mathematics Advance Access published on April 23, 2013
Quart. J. Math. 65 (2014), 505–515; doi:10.1093/qmath/hat016

UNLIKELY INTERSECTIONS FOR CURVES IN MULTIPLICATIVE GROUPS OVER POSITIVE CHARACTERISTIC

by D. MASSER[†]

(*Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland*)

[Received 14 December 2012]

Abstract

The conjectures associated with the names of Zilber–Pink greatly generalize results associated with the names of Manin–Mumford and Mordell–Lang, but unlike the latter they are at present restricted to zero characteristic. We make a start on removing this restriction by stating a conjecture for curves in multiplicative groups over positive characteristic, and we verify the conjecture in three dimensions as well as for some special lines in general dimension. We also give an example where the finite set in question can be explicitly determined.

1. Introduction

For more than a decade now much has been written on the study of what happens when a fixed algebraic variety sitting inside a fixed commutative group variety is intersected with the union of group subvarieties of suitable dimension. When the group variety is the multiplicative group $\mathbf{G}_m^n$, we may refer to the work of Bombieri, Zannier and myself (e.g. the early paper [1] on curves, our later paper [2] on varieties of codimension 2 and our paper [3] on planes) and the wide-ranging extension of Habegger to arbitrary varieties (see, e.g. [9]). When the group variety is projectively complete, there are the works of Viada about powers of a fixed elliptic curve (see, e.g. [21]) as well as the works of Rémond generalizing to abelian varieties (see, e.g. [19]). There are also the more recent versions of Zannier and myself inside varying group varieties such as elliptic and abelian schemes (see, e.g. [14, 15]). All this takes place over zero characteristic, and one may consult the recent book [22] of Zannier for a comprehensive survey. The general conjectures are due to Zilber [23] and Pink [18].

The object of the present paper is to initiate the study of such problems over positive characteristic.

This may be an exaggeration, because in fact a lot has already been done under different headings. Thus, in codimension 1 the subject usually amounts to the study of torsion points, an area often associated with the names Manin–Mumford. The lesson we learn already here is that the trail from zero to positive characteristic is not without pitfalls. For example, over zero characteristic the equation

$$x + y = 1 \tag{1.1}$$

has only two solutions in roots of unity x and y (involving primitive sixth roots). However, over characteristic p there are infinitely many; indeed we can take any $x \neq 0, 1$ in the algebraic closure $\overline{\mathbf{F}}_p$ and then y accordingly. For much more, see, e.g. the paper [20] of Scanlon.

[†]E-mail: david.masser@unibas.ch

Another special kind of unlikely intersection occurs when we intersect the variety with a finitely generated group, an area often associated with the names Mordell–Lang. For example, over zero characteristic we can ask for solutions of (1.1) with x a power of 3 and y a power of -2, amounting essentially to the equation $3^a - 2^b = 1$. This has for centuries been known to have only two solutions in integers a, b. However, over characteristic p inside the function field $\mathbf{F}_p(t)$, with x a power of t and y a power of $1 - t$, we have infinitely many solutions

$$x = t^q, \quad y = (1-t)^q = 1 - t^q \ \ (q = 1, p, p^2, \ldots).$$

For much more, see, e.g. the papers [10] of Hrushovski and [17] of Moosa and Scanlon.

And the torsion situation can be combined with the finitely generated situation by allowing finite rank; under this heading, see, e.g. the papers [8] of Ghioca and Moosa and [7] of Ghioca.

For simplicity, we will restrict ourselves in this paper to the group variety $\mathbf{G}_m^n$, and to curves sitting inside it. Over zero characteristic, the decisive result was obtained by Maurin [16] (see also [5]), and, taking into account [4], we now know the following best possible result.

THEOREM *Let K be an algebraically closed field of characteristic 0, and let C in $\mathbf{G}_m^n$ be an irreducible curve defined over K. Assume that for any non-zero $(r_1, \ldots, r_n)$ in $\mathbf{Z}^n$, the monomial $x_1^{r_1} \cdots x_n^{r_n}$ is not identically 1 on C. Then there are at most finitely many $(\xi_1, \ldots, \xi_n)$ in $C(K)$ for which there exist linearly independent $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ in $\mathbf{Z}^n$ such that*

$$\xi_1^{a_1} \cdots \xi_n^{a_n} = \xi_1^{b_1} \cdots \xi_n^{b_n} = 1. \tag{1.2}$$

Indeed, if there is non-zero $(r_1, \ldots, r_n)$ with $x_1^{r_1} \cdots x_n^{r_n}$ identically 1, then we can assume that $r_1, \ldots, r_n$ are coprime at the expense of replacing 1 by a root of unity ζ_1. Then by an automorphism of $\mathbf{G}_m^n$, we may further assume $x_1 = \zeta_1$ on C. Now we can suppose x_2 is not constant on C, and we just intersect C with $x_2 = \zeta_2$ for various roots of unity ζ_2 to get infinitely many relations (1.2).

Already the example involving (1.1) shows that this theorem cannot be true over positive characteristic, because for $n = 2$ the condition on $(\xi_1, \xi_2) = (\xi, \eta)$ means that ξ, η are roots of unity.

We propose the following version over positive characteristic.

CONJECTURE *Let K be an algebraically closed field of characteristic $p > 0$, and let C in $\mathbf{G}_{\mathrm{m}}^n$ be an irreducible curve defined over K. Assume that*

$(*)$ for any linearly independent $(r_1, \ldots, r_n)$, $(s_1, \ldots, s_n)$ in $\mathbf{Z}^n$ the monomials

$$x_1^{r_1} \cdots x_n^{r_n}, \quad x_1^{s_1} \cdots x_n^{s_n}$$

are algebraically independent over $\mathbf{F}_p$ on C.

Then there are at most finitely many $(\xi_1, \ldots, \xi_n)$ in $C(K)$ for which there exist linearly independent $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ in $\mathbf{Z}^n$ such that

$$\xi_1^{a_1} \cdots \xi_n^{a_n} = \xi_1^{b_1} \cdots \xi_n^{b_n} = 1.$$

Thus, the hypothesis $(*)$ is somewhat more stringent. It is reminiscent of Habegger's condition in [9, Corollary 1.5, p. 863]. Actually, we may be being over-careful here, because we need slightly more information than the failure of $(*)$ to get an infinite set. Namely, suppose that at least one of

the offending two monomials is non-constant on C (as a function). We may assume that the exponent vectors can be extended to a basis of $\mathbf{Z}^n$. Then as above with an automorphism, we can make sure that x_1, x_2 are algebraically dependent over $\mathbf{F}_p$ and x_2 is non-constant on C. Now it suffices to intersect as above with various $x_2 = \zeta_2$, because the relation between x_1 and x_2 forces x_1 also to be a root of unity ζ_1.

Thus, we may hope to be able to prove finiteness even when $(*)$ fails for a particular C. For example, suppose that whenever $(*)$ fails the offending monomials are both constant. In other words, any two multiplicatively independent monomials algebraically dependent over $\mathbf{F}_p$ on C must be constant on C. We could call this $(**)$, a hypothesis vacuously implied by $(*)$. It is equivalent to $(*)$ for $n = 2$ but not for $n = 3$, as the example $x = t$, $y = 1 - t$ in $\mathbf{G}_{\mathrm{m}}^3$ over $\mathbf{F}_p(t)$ shows.

Actually, we see from this that if $(**)$ holds but $(*)$ fails in $\mathbf{G}_m^3$, then there are no ξ_1, ξ_2, ξ_3 at all in (1.2)! For as above, we can suppose that both $x_1 = \xi_1$, $x_2 = \xi_2$ are constant on C; then x_3 is certainly not. If there is any point at all satisfying two relations, then we deduce by eliminating ξ_3 that ξ_1, ξ_2 are multiplicatively dependent. So $x_1^{c_1} x_2^{c_2} = 1$ on C for some non-zero (c_1, c_2) in $\mathbf{Z}^2$. Now the two monomials $x_1^{c_1} x_2^{c_2}, x_3$ are algebraically dependent over $\mathbf{F}_p$ on C; consequently, they are both constant on C, an absurdity. So one might formulate a conjecture with $(**)$ instead of $(*)$; but at the moment we refrain.

At any rate, the above conjecture with $(*)$ is trivial for $n = 2$: if C contains infinitely many points over $\overline{\mathbf{F}_p}$, then it must be defined over this field, and so x_1, x_2 are algebraically dependent over this field and so over $\mathbf{F}_p$.

In the present paper, we do three less trivial things concerning the above conjecture with $(*)$. First, we show that it holds in $\mathbf{G}_m^3$ (and therefore also in $\mathbf{G}_m^2$). The arguments do not appear to extend immediately to $\mathbf{G}_m^4$. Second, we show that it holds for certain families of lines in any $\mathbf{G}_m^n$, even with a hypothesis substantially weaker than $(*)$. And finally, we actually determine the finite set for a particular line in $\mathbf{G}_m^3$; the shape is even independent of p. This kind of independence was already observed by Leitner in the context of Mordell–Lang; see, e.g. [**12**, (pp. 327–329)].

Here are our precise results.

THEOREM 1.1 *Let K be an algebraically closed field of characteristic $p > 0$, and let C in $\mathbf{G}_{\mathrm{m}}^3$ be an irreducible curve defined over K. Assume that for any linearly independent (r_1, r_2, r_3), (s_1, s_2, s_3) in $\mathbf{Z}^3$, the monomials*

$$x_1^{r_1} x_2^{r_2} x_3^{r_3}, \quad x_1^{s_1} x_2^{s_2} x_3^{s_3}$$

are algebraically dependent over $\mathbf{F}_p$ on C. Then there are at most finitely many (ξ_1, ξ_2, ξ_3) in $C(K)$ for which there exist linearly independent (a_1, a_2, a_3), (b_1, b_2, b_3) in $\mathbf{Z}^3$ such that

$$\xi_1^{a_1} \xi_2^{a_2} \xi_3^{a_3} = \xi_1^{b_1} \xi_2^{b_2} \xi_3^{b_3} = 1.$$

THEOREM 1.2 *Let K be an algebraically closed field of characteristic $p > 0$, and let L in $\mathbf{G}_m^n$ be a line parametrized by x in*

$$x_1 = \alpha_1 x + \beta_1 t + \gamma_1, \ldots, x_n = \alpha_n x + \beta_n t + \gamma_n, \tag{1.3}$$

for $\alpha_1, \beta_1, \gamma_1, \ldots, \alpha_n, \beta_n, \gamma_n$ in $\overline{\mathbf{F}_p}$ and t transcendental over $\mathbf{F}_p$. Suppose that each $1, x_i, x_j$ $(i < j)$ and each $1, x_i/x_k, x_j/x_k$ $(k < i < j)$ are linearly independent over $\overline{\mathbf{F}_p}$ on L. Then

there are at most finitely many $(\xi_1, \dots, \xi_n)$ *in* $L(K)$ *for which there exist linearly independent* $(a_1, \dots, a_n)$, $(b_1, \dots, b_n)$ *in* $\mathbf{Z}^n$ *with*

$$\xi_1^{a_1} \cdots \xi_n^{a_n} = \xi_1^{b_1} \cdots \xi_n^{b_n} = 1. \tag{1.4}$$

THEOREM 1.3 *For* $p \neq 2$, *let* K *be an algebraically closed field of characteristic* $p > 0$, *and let* L *in* $\mathbf{G}_m^3$ *be the line parametrized by* x *in*

$$x_1 = x, \quad x_2 = x - t, \quad x_3 = x + t + 1,$$

for t *transcendental over* $\mathbf{F}_p$. *Then if* $P = (\xi_1, \xi_2, \xi_3)$ *is in* $C(K)$ *for which there exist linearly independent* (a_1, a_2, a_3), (b_1, b_2, b_3) *in* $\mathbf{Z}^3$ *such that*

$$\xi_1^{a_1} \xi_2^{a_2} \xi_3^{a_3} = \xi_1^{b_1} \xi_2^{b_2} \xi_3^{b_3} = 1, \tag{1.5}$$

we have

$$P = (-\tfrac{1}{2}, -t - \tfrac{1}{2}, t + \tfrac{1}{2}), \quad (t + 1, 1, 2t + 2), \quad (-t, -2t, 1). \tag{1.6}$$

The rest of this paper is arranged as follows.

By way of warm-up, we start in Section 2 with a proof of Theorem 1.3. Compared with some similar results over zero characteristic (see, e.g. the paper [**6**, pp. 99, 100] of Cohen and Zannier) it is rather simple. Essentially, we eliminate any inseparability and then differentiate with respect to t.

Then in Section 3 we prove Theorem 1.1. Here too the argument is comparatively simple, as the zero characteristic proofs involve both upper bounds and especially lower bounds for height, whereas we use no notion of height at all. But the concept of a naive Newton polyhedron (no convex hull) is useful, and on the way we run into a modest differential equation.

Finally, in Section 4 we prove Theorem 1.2. As equations (1.3) may be considered to define a plane over $\overline{\mathbf{F}_p}$ with t as an extra parameter, it is not too surprising that the arguments here have something in common with the work [**3**] on planes in zero characteristic. But again we do not use heights.

2. Proof of Theorem 1.3

It is clear that we can assume in (1.5) that not all of a_1, a_2, a_3 are divisible by p. Similarly, for b_1, b_2, b_3; but in fact we can go a step further and assume that not all the minors

$$c_1 = a_2 b_3 - a_3 b_2, \quad c_2 = a_3 b_1 - a_1 b_3, \quad c_3 = a_1 b_2 - a_2 b_1 \tag{2.1}$$

are divisible by p. For example, we can eliminate any factor p from the elementary divisors. More precisely, the group $\Gamma = \mathbf{Z}(a_1, a_2, a_3) + \mathbf{Z}(b_1, b_2, b_3)$ sits inside a unique primitive closure Γ_0 with finite index which is the highest common factor of c_1, c_2, c_3; and if $[\Gamma_0 : \Gamma] = p^e s$ with p not dividing s, then we can increase Γ to the unique group Γ' in between with $[\Gamma_0 : \Gamma'] = s$.

From either of equations (1.5), we see with $\xi_1 = \xi, \xi_2 = \xi - t, \xi_3 = \xi + t + 1$ that ξ is algebraic over $\mathbf{F}_p(t)$. If ξ is algebraic over $\mathbf{F}_p$, then it is easy to see that $\xi - t, \xi + t + 1$ must be associate in $\overline{\mathbf{F}_p}[t]$. In that case $\xi = -\frac{1}{2}$ as in (1.6). Otherwise, we can choose a minimal

$$q = \dots, p^{-2}, p^{-1}, 1, p, p^2, \dots,$$

such that ξ^q lies in the maximal separable algebraic extension $\mathcal{F}$ of $\mathbf{F}_p(t)$. This amounts to the assertion $\bigcap_{i=0}^{\infty} \mathcal{F}^{p^i} = \overline{\mathbf{F}_p}$, for which I could not find a precise reference in the literature. But it

follows, for example, by applying hyperderivatives to the minimal equation over $\mathbf{F}_p(t)$ of something in the intersection; for details see [13, Lemma 3].

With $\eta_i = \xi_i^q$ now all in $\mathcal{F}$, we have $\eta_1^{a_1}\eta_2^{a_2}\eta_3^{a_3} = \eta_1^{b_1}\eta_2^{b_2}\eta_3^{b_3} = 1$, and we can differentiate logarithmically with respect to t to get

$$0 = a_1\frac{\dot\eta_1}{\eta_1} + a_2\frac{\dot\eta_2}{\eta_2} + a_3\frac{\dot\eta_3}{\eta_3} = b_1\frac{\dot\eta_1}{\eta_1} + b_2\frac{\dot\eta_2}{\eta_2} + b_3\frac{\dot\eta_3}{\eta_3}. \tag{2.2}$$

Now

$$x_3 = 2x_1 + 1 - x_2, \tag{2.3}$$

on L and so $\xi_3 = 2\xi_1 + 1 - \xi_2$ and therefore $\eta_3 = 2\eta_1 + 1 - \eta_2$ and thus $\dot\eta_3 = 2\dot\eta_1 - \dot\eta_2$. Substituting this into (2.2), we get

$$0 = \left(\frac{a_1}{\eta_1} + 2\frac{a_3}{\eta_3}\right)\dot\eta_1 + \left(\frac{a_2}{\eta_2} - \frac{a_3}{\eta_3}\right)\dot\eta_2,$$
$$0 = \left(\frac{b_1}{\eta_1} + 2\frac{b_3}{\eta_3}\right)\dot\eta_1 + \left(\frac{b_2}{\eta_2} - \frac{b_3}{\eta_3}\right)\dot\eta_2,$$

a linear system in $\dot\eta_1, \dot\eta_2$ with determinant say Δ.

Now $\dot\eta_1$ cannot be zero, otherwise $\eta_1 = \xi^q$ would be in the field of constants $\mathcal{F}^p$ of $\mathcal{F}$ (see, e.g. [11, Proposition 1, p. 185]) and then $\xi^{q/p}$ would be in $\mathcal{F}$, contradicting the minimality of q. Thus $\Delta = 0$. After a short calculation, this emerges as $2c_1\eta_1 - c_2\eta_2 - c_3\eta_3 = 0$ (for comparison, see [3, p. 74]—the connexion is not mysterious because $(x, x - t, x + t + 1)$ parametrizes a plane when t is also allowed to vary). By our remark above, this is a non-trivial relation, especially as $p \neq 2$. It holds also for ξ_1, ξ_2, ξ_3 and thus

$$0 = 2c_1\xi - c_2(\xi - t) - c_3(\xi + t + 1) = (2c_1 - c_2 - c_3)\xi + (c_2 - c_3)t - c_3.$$

It follows easily that $\xi = \alpha t + \beta$ for α, β in $\mathbf{F}_p$. Now it is also easy to see that the multiplicative dependencies (1.5) lead to linear dependencies among

$$\xi_1 = \alpha t + \beta, \quad \xi_2 = (\alpha - 1)t + \beta, \quad \xi_3 = (\alpha + 1)t + \beta + 1.$$

For example, the very simple [3, Lemma 9.4, p. 76] with $n = 2$ forces the rank of the corresponding matrix $\begin{pmatrix} \alpha & \beta \\ \alpha-1 & \beta \\ \alpha+1 & \beta+1 \end{pmatrix}$ to be at most 1, at least if $\alpha, \alpha - 1, \alpha + 1 \neq 0$. But as α, β cannot both be zero this rank must be 2. Finally, we see quickly that $\alpha = 0$ implies $\beta = -\frac{1}{2}$ (a solution already encountered), and $\alpha = 1$ implies $\beta = 1$, and $\alpha = -1$ implies $\beta = 0$. These correspond to the three anomalous curves in a non-degenerate plane in three dimensions; see [3, p. 77].

Note that for $p = 2$, we have the infinite set of all $\xi = t + \tau$ ($\tau \in \bar{\mathbf{F}}_2$); of course then $(*)$ fails because x_2 and $x_3 = x_2 + 1$ are algebraically dependent over $\mathbf{F}_2$ on C.

3. Proof of Theorem 1.1

As above, we could assume that not all the minors (2.1) are divisible by p. But before doing that we perform some similar operations on C itself. We can suppose that K has finite transcendence degree over $\mathbf{F}_p$.

Note that the theorem is trivial if K has transcendence degree 0 over $\mathbf{F}_p$. For then x_1, x_2 are algebraically dependent over $\mathbf{F}_p$, and the hypothesis $(*)$ on C fails.

Next we suppose that K has transcendence degree 1 over $\mathbf{F}_p$. It thus lies in some $\overline{\mathbf{F}_p(t)}$. The key remark here is to note that x_1, x_2, x_3 are algebraically dependent over $\mathbf{F}_p$ on C. In fact, there is a relation

$$F(x_1, x_2, x_3) = 0, \tag{3.1}$$

with a polynomial $F = F(X_1, X_2, X_3) \neq 0$ defined over $\mathbf{F}_p$. This F is unique up to units if regarded as a Laurent polynomial and assumed to be irreducible over $\mathbf{F}_p$. (The example in Theorem 1.3 corresponds to (2.3) and $F = 2X_1 - X_2 - X_3 + 1$.)

Up to now, we have freely used automorphisms of $\mathbf{G}_m^n$, but now we need surjective endomorphisms. One of these applied to C gives another curve, also absolutely irreducible and defined over K, and so we get another F. We shall show that the endomorphism can be chosen so that the resulting

$$F, \quad X_1 \frac{\partial F}{\partial X_1}, \quad X_2 \frac{\partial F}{\partial X_2}, \quad X_3 \frac{\partial F}{\partial X_3}, \tag{3.2}$$

become linearly independent over $\mathbf{F}_p$.

For this, we write out (3.1) as

$$\sum \varphi(i_1, i_2, i_3) x_1^{i_1} x_2^{i_2} x_3^{i_3} = 0, \tag{3.3}$$

with coefficients $\varphi(i_1, i_2, i_3) \neq 0$ in $\mathbf{F}_p$, and we consider the matrix $M(F)$ whose rows are the $(1, i_1, i_2, i_3)$ in (3.3).

We claim that this matrix has full rank 4 (it is easily seen that this rank is independent under multiplying F by a Laurent unit, that is, a monomial). For if not, then there is a relation $c_0 + c_1 i_1 + c_2 i_2 + c_3 i_3 = 0$ holding on all terms in (3.3), with c_0, c_1, c_2, c_3 in $\mathbf{Z}$ not all zero. (This says that the naive Newton polyhedron of F lies in a plane in $\mathbf{Q}^3$.) But that would lead to the forbidden algebraic dependence over $\mathbf{F}_p$ of some $x_1^{r_1} x_2^{r_2} x_3^{r_3}$, $x_1^{s_1} x_2^{s_2} x_3^{s_3}$ in $(*)$. For example, we can assume $c_3 \neq 0$ and then we substitute $i_3 = -(c_0 + c_1 i_1 + c_2 i_2)/c_3$ into (3.3) to get the dependence of $x_1 x_3^{-c_1/c_3}$, $x_2 x_3^{-c_2/c_3}$ and therefore of $x_1^{c_3} x_3^{-c_1}$, $x_2^{c_3} x_3^{-c_2}$.

Now if it happens that $M(F)$ has rank 4 over $\mathbf{F}_p$ as well, then this leads to the independence of (3.2). To see this, consider a possible relation

$$\gamma_0 F + \gamma_1 X_1 \frac{\partial F}{\partial X_1} + \gamma_2 X_2 \frac{\partial F}{\partial X_2} + \gamma_3 X_3 \frac{\partial F}{\partial X_3} = 0, \tag{3.4}$$

with $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ in $\mathbf{F}_p$ not all zero. Then $\gamma_1, \gamma_2, \gamma_3$ are not all zero; pull them back to c_1, c_2, c_3 in $\mathbf{Z}$, and consider the Laurent polynomial $H(T) = F(T^{c_1}, T^{c_2}, T^{c_3})$. We get for the derivative

$$H'(T) = \sum_{h=1,2,3} \gamma_h T^{c_h - 1} \frac{\partial F}{\partial X_h}(T^{c_1}, T^{c_2}, T^{c_3}) = -\gamma_0 T^{-1} F(T^{c_1}, T^{c_2}, T^{c_3}) = -\gamma_0 T^{-1} H(T),$$

using (3.4). This is a nice differential equation for H that in zero characteristic we would probably try to solve with the exponential function. Here, with $H(T) = \sum_{\psi(i) \neq 0} \psi(i) T^i$, we get the equations $i = -\gamma_0$. Of course, these mean that $H(T) = T^{-c_0} J(T^p)$ for a pullback c_0 of γ_0 and some Laurent

polynomial J. Recalling (3.3), we see that all the $c_1 i_1 + c_2 i_2 + c_3 i_3$ are congruent to $-c_0$ modulo p. But this says that $M(F)$ has rank less than 4 over $\mathbf{F}_p$.

Now $M(F)$ has rank 4 over $\mathbf{Z}$; thus, the highest common factor $d(F)$ of all its maximal subdeterminants is a non-zero integer $p^e s$ with s prime to p. We imitate the argument with (2.1) to reduce e to 0. If $e = 0$, then $M(F)$ has rank 4 over $\mathbf{F}_p$ and there is nothing to do. If $e \geq 1$, then there is a relation $\gamma_0 + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3 = 0$ holding on all terms in (3.3), with $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ in $\mathbf{F}_p$ not all zero. Pulling these back as above, we deduce that for every (i_1, i_2, i_3) there is $j = j(i_1, i_2, i_3)$ in $\mathbf{Z}$ such that $c_0 + c_1 i_1 + c_2 i_2 + c_3 i_3 = pj$. We can suppose that $\gamma_3 \neq 0$ and even that $c_3 = 1$. We substitute $i_3 = -(c_0 + c_1 i_1 + c_2 i_2) + pj$ into (3.3) to get

$$\sum \varphi(i_1, i_2, i_3) \tilde{x}_1^{i_1} \tilde{x}_2^{i_2} x_3^{pj} = 0,$$

with $\tilde{x}_1 = x_1 x_3^{-c_1}$, $\tilde{x}_2 = x_2 x_3^{-c_2}$. Now completing these with $\tilde{x}_3 = x_3^p$ gives a new $\tilde{F}$ relating $\tilde{x}_1, \tilde{x}_2, \tilde{x}_3$ with new matrix $M(\tilde{F})$ with rows

$$(1 \quad i_1 \quad i_2 \quad j) = (1 \quad i_1 \quad i_2 \quad i_3) \begin{pmatrix} 1 & 0 & 0 & c_0/p \\ 0 & 1 & 0 & c_1/p \\ 0 & 0 & 1 & c_2/p \\ 0 & 0 & 0 & 1/p \end{pmatrix}.$$

It follows that $d(\tilde{F}) = d(F)/p = p^{e-1} s$. So we have succeeded in reducing e by 1. But why is $\tilde{F}$ also irreducible over $\mathbf{F}_p$?

Well, we just check that

$$\tilde{F}(T_1 T_3^{-c_1}, T_2 T_3^{-c_2}, T_3^p) = T_3^{c_0} F(T_1, T_2, T_3).$$

So a proper factorization of $\tilde{F}$ would lead to a proper factorization of F.

This reduction of e has been via the transformation

$$\tilde{x}_1 = x_1 x_3^{-c_1}, \quad \tilde{x}_2 = x_2 x_3^{-c_2}, \quad \tilde{x}_3 = x_3^p,$$

which represents a surjective endomorphism of $\mathbf{G}_m^3$ sending the curve C into another curve $\tilde{C}$.

After finitely many steps, we reach $e = 0$ and so the desired independence in (3.2). The endomorphisms do not have any effect on either the hypotheses or the conclusion of Theorem 1.2 (even though they are certainly not invertible modulo p), and we now proceed to imitate the above proof of Theorem 1.3.

If $C(\overline{\mathbf{F}_p})$ is infinite, then C must be defined over $\overline{\mathbf{F}_p}$ which is ruled out by $(*)$. Thus, we can assume that not all of ξ_1, ξ_2, ξ_3 lie in $\overline{\mathbf{F}_p}$. We choose q minimal such that $\eta_1 = \xi_1^q$, $\eta_2 = \xi_2^q$, $\eta_3 = \xi_3^q$ lie in the maximal separable algebraic extension of $\mathbf{F}_p(t)$. We have $\eta_1^{a_1} \eta_2^{a_2} \eta_3^{a_3} = \eta_1^{b_1} \eta_2^{b_2} \eta_3^{b_3} = 1$, and now is the time to adjust the minors (2.1). We can then differentiate logarithmically with respect to t to get

$$0 = a_1 \frac{\dot{\eta}_1}{\eta_1} + a_2 \frac{\dot{\eta}_2}{\eta_2} + a_3 \frac{\dot{\eta}_3}{\eta_3} = b_1 \frac{\dot{\eta}_1}{\eta_1} + b_2 \frac{\dot{\eta}_2}{\eta_2} + b_3 \frac{\dot{\eta}_3}{\eta_3}.$$

We also have $F(\xi_1, \xi_2, \xi_3) = 0$ and so $F(\eta_1, \eta_2, \eta_3) = 0$. This differentiates to

$$0 = \dot{\eta}_1 \chi_1 + \dot{\eta}_2 \chi_2 + \dot{\eta}_3 \chi_3,$$

where $\chi_i = (\partial F/\partial X_i)(\eta_1, \eta_2, \eta_3)$ $(i = 1, 2, 3)$. As $\dot\eta_1, \dot\eta_2, \dot\eta_3$ are not all zero by the minimality of q, this leads to

$$\begin{vmatrix} \dfrac{a_1}{\eta_1} & \dfrac{a_2}{\eta_2} & \dfrac{a_3}{\eta_3} \\ \dfrac{b_1}{\eta_1} & \dfrac{b_2}{\eta_2} & \dfrac{b_3}{\eta_3} \\ \chi_1 & \chi_2 & \chi_3 \end{vmatrix} = 0.$$

Expanding and multiplying by $\eta_1\eta_2\eta_3$ yields

$$c_1\eta_1\chi_1 + c_2\eta_2\chi_2 + c_3\eta_3\chi_3 = 0,$$

which is just the vanishing of the polynomial

$$G = c_1X_1\frac{\partial F}{\partial X_1} + c_2X_2\frac{\partial F}{\partial X_2} + c_3X_3\frac{\partial F}{\partial X_3},$$

at (η_1, η_2, η_3). (In the proof of Theorem 1.3, the F in (2.3) leads to $G = 2c_1X_1 - c_2X_2 - c_3X_3$.) We therefore have

$$F(\xi_1, \xi_2, \xi_3) = G(\xi_1, \xi_2, \xi_3) = 0. \tag{3.5}$$

Clearly, the degree of G does not exceed the degree of F, and we specified that F was irreducible over $\mathbf{F}_p$. So by the independence in (3.2), the variety $F = G = 0$ is a curve over $\mathbf{F}_p$. If the intersection of this curve with C is an infinite set, then C is defined over $\overline{\mathbf{F}_p}$ and we are back to the case of transcendence degree 0. Thus, we can assume that the intersection is finite, and we are finished.

What if K has transcendence degree more than 1 over $\mathbf{F}_p$? Say in some $\overline{\mathbf{F}_p(t, u)}$. With our point (ξ_1, ξ_2, ξ_3), the two multiplicative relations show that $\Xi = \mathbf{F}_p(\xi_1, \xi_2, \xi_3)$ has transcendence degree at most 1 over $\mathbf{F}_p$. Thus, at least one of t, u is transcendental over Ξ, say t. On the other hand, t, x_1, x_2, x_3 are algebraically dependent over $\mathbf{F}_p$ on C, because $\mathbf{F}_p(x_1, x_2, x_3, t, u)$ has transcendence degree 1 over $\mathbf{F}_p(t, u)$. Write out a fixed polynomial relation

$$\sum G(i; x_1, x_2, x_3)t^i = 0,$$

where we can assume that all the $G(i; X_1, X_2, X_3)$ have no common factor. Specializing and recalling that t was transcendental over $\Xi = \mathbf{F}_p(\xi_1, \xi_2, \xi_3)$, we deduce that all the $G(i; \xi_1, \xi_2, \xi_3) = 0$. This is a system like (3.5), again corresponding to a curve over $\mathbf{F}_p$, and as there we get our finite set.

A similar argument works for K in some $\overline{\mathbf{F}_p(t_1, \dots, t_d)}$ for $d \geq 3$. We find now that at least $d - 1$ of $t_1, \dots, t_d$ are algebraically independent over Ξ, say $t_1, \dots, t_{d-1}$. On the other hand, $t_1, \dots, t_{d-1}, x_1, x_2, x_3$ are algebraically dependent over $\mathbf{F}_p$, because $\mathbf{F}_p(x_1, x_2, x_3, t_1, \dots, t_d)$ has transcendence degree 1 over $\mathbf{F}_p(t_1, \dots, t_d)$. Write out a fixed polynomial relation

$$\sum G(i_1, \dots, i_{d-1}; x_1, x_2, x_3)t_1^{i_1} \cdots t_{d-1}^{i_{d-1}} = 0,$$

where we can assume that all the $G(i_1, \dots, i_{d-1}; X_1, X_2, X_3)$ have no common factor. Specializing and recalling that $t_1, \dots, t_{d-1}$ were algebraically independent over Ξ, we deduce that all the $G(i_1, \dots, i_{d-1}; \xi_1, \xi_2, \xi_3) = 0$. This is once more a system like (3.5), and so we get our finite set.

4. Proof of Theorem 1.2

Take $P = (\xi_1, \dots, \xi_n)$ with the two relations indicated. We can assume as in (2.1) that not all $c_{ij} = a_i b_j - a_j b_i$ $(i < j)$ are zero modulo p, and also that $\xi_1, \dots, \xi_n$ are not all in $\overline{\mathbf{F}_p}$.

We next show that $\xi_1, \dots, \xi_n$ are all in $\overline{\mathbf{F}_p(t)}$. For if just a single relation (1.4) for

$$\xi_i = \alpha_i \xi + \beta_i t + \gamma_i \quad (i = 1, \dots, n),$$

does not imply that ξ is in $\overline{\mathbf{F}_p(t)}$, then the $\alpha_i x + \beta_i t + \gamma_i$ in $\overline{\mathbf{F}_p}[x, t]$ must be multiplicatively dependent on L. By [3, Lemma 9.4, p. 76], this implies that two vectors

$$(\alpha_i, \beta_i, \gamma_i), \quad (\alpha_j, \beta_j, \gamma_j) \ \ (i < j)$$

are linearly dependent. But then x_i, x_j are linearly dependent over $\overline{\mathbf{F}_p}$ on L, against our hypothesis.

Let q be minimal with $\eta_i = \xi_i^q$ in the maximal separable algebraic extension of $\mathbf{F}_p(t)$. Then

$$0 = \frac{a_1}{\eta_1}\dot{\eta}_1 + \cdots + \frac{a_n}{\eta_n}\dot{\eta}_n = \frac{b_1}{\eta_1}\dot{\eta}_1 + \cdots + \frac{b_n}{\eta_n}\dot{\eta}_n.$$

To these, we adjoin the equations resulting from the elimination of x and t in the parametrization (1.3). These include $n - 2$ independent equations

$$\delta_1^{(m)} x_1 + \cdots + \delta_n^{(m)} x_n + \delta_0^{(m)} = 0 \quad (m = 1, \dots, n-2), \tag{4.1}$$

over $\overline{\mathbf{F}_p}$, so that $\delta_1^{(m)q}\eta_1 + \cdots + \delta_n^{(m)q}\eta_n + \delta_0^{(m)q} = 0$ and therefore

$$\delta_1^{(m)q}\dot{\eta}_1 + \cdots + \delta_n^{(m)q}\dot{\eta}_n = 0 \quad (m = 1, \dots, n-2).$$

We get the determinant $\sum_{i<j}(c_{ij}\epsilon_{ij}^q/\eta_i\eta_j) = 0$ for the maximal minors ϵ_{ij} of the matrix M with rows $(\delta_1^{(m)}, \dots, \delta_n^{(m)})$ $(m = 1, \dots, n-2)$. Thus, also $G(P) = 0$ with

$$G(X_1, \dots, X_n) = \sum_{i<j} \frac{c_{ij}\epsilon_{ij}}{X_i X_j}.$$

Now certainly not all $\epsilon_{ij} = 0$ because of the independence in (4.1). We show now that in fact all $\epsilon_{ij} \neq 0$.

The rows of M are independent because of the relations (4.1) specialized at P. They are orthogonal to the columns $(\alpha_1, \dots, \alpha_n)^t$, $(\beta_1, \dots, \beta_n)^t$. These are independent—in fact even together with $(\gamma_1, \dots, \gamma_n)^t$—due to the hypothesis of linear independence of x_k, x_i, x_j $(k < i < j)$ on L. So by duality say $\epsilon_{12} = 0$ would imply $\zeta_{12} = 0$ for $\zeta_{12} = \alpha_1\beta_2 - \alpha_2\beta_1$. However, this would lead to the forbidden linear dependence of $1, x_1, x_2$ in (1.3). And similarly all $\epsilon_{ij} \neq 0$.

We note something stronger about the matrix with columns

$$(0, \alpha_1, \dots, \alpha_n)^t, \quad (0, \beta_1, \dots, \beta_n)^t, \quad (1, \gamma_1, \dots, \gamma_n)^t. \tag{4.2}$$

Namely, all its maximal minors are non-zero. We already observed the independence of say $(0, 0, 1)$, $(\alpha_1, \beta_1, \gamma_1)$, $(\alpha_2, \beta_2, \gamma_2)$. But also the dependence of say

$$(\alpha_1, \beta_1, \gamma_1), \quad (\alpha_2, \beta_2, \gamma_2), \quad (\alpha_3, \beta_3, \gamma_3)$$

would imply the forbidden dependence of x_1, x_2, x_3. This resembles the situation for non-degenerate planes (see [**3**, p. 58]). Indeed, if we regard (1.3) as a plane $L^\sharp$ over $\overline{\mathbf{F}_p}$ with parameters x, t (and with (4.1) as its equations), then $L^\sharp$ is literally non-degenerate (of course now modulo p), because the rows $(\delta_0^{(m)}, \delta_1^{(m)}, \dots, \delta_n^{(m)})$ $(m = 1, \dots, n-2)$ are orthogonal to (4.2).

Now the simple argument of [**3**, Lemma 9.1, p. 73] (which is independent of the characteristic) shows that the $1/x_i x_j$ $(i < j)$ are linearly independent over $\overline{\mathbf{F}_p}$ on $L^\sharp$. So our G is not identically zero on $L^\sharp$. Thus, $G = 0$ intersects $L^\sharp$ in finitely many fixed curves over $\overline{\mathbf{F}_p}$, one of which, call it $D^\sharp$, corresponds (in the sense of [**4**, p. 311]) to our point P. It is not difficult to see that t is not constant on $D^\sharp$. For example, if $t = \tau$ on $D^\sharp$ with τ in $\overline{\mathbf{F}_p}$, then this curve would be parametrized by $x_1 = \alpha_1 x + \gamma_1', \dots, x_n = \alpha_n x + \gamma_n'$ with constants $\gamma_1' = \beta_1 \tau + \gamma_1, \dots, \gamma_n' = \beta_n \tau + \gamma_n$. Thus, we would have on the one hand

$$\alpha_2 \xi_1 - \alpha_1 \xi_2 = -\zeta_{12} \tau + \alpha_2 \gamma_1 - \alpha_1 \gamma_2,$$

arising from $D^\sharp$; and on the other hand

$$\alpha_2 \xi_1 - \alpha_1 \xi_2 = -\zeta_{12} t + \alpha_2 \gamma_1 - \alpha_1 \gamma_2,$$

arising from L. But because $\zeta_{12} \neq 0$ and t is transcendental over $\mathbf{F}_p$ this is absurd.

So t is not constant on $D^\sharp$, and belonging to $D^\sharp$ expresses $\xi_1, \dots, \xi_n$ as fixed algebraic functions of t, leading to the required finiteness of our P.

References

1. E. Bombieri, D. Masser and U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups, *Int. Math. Res. Not.* **20** (1999), 1119–1140.
2. E. Bombieri, D. Masser and U. Zannier, Anomalous subvarieties—structure theorems and applications, *Int. Math. Res. Not.* (2007), Article ID rnm057, 33 pp., doi: 10.1093/imrn/rnm057.
3. E. Bombieri, D. Masser and U. Zannier, Intersecting a plane with algebraic subgroups of multiplicative groups, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* **VII** (2008), 51–80.
4. E. Bombieri, D. Masser and U. Zannier, On unlikely intersections of complex varieties with tori, *Acta Arith.* **133** (2008), 309–323.
5. E. Bombieri, P. Habegger, D. Masser and U. Zannier, A note on Maurin's theorem, *Rend. Lincei Mat. Appl.* **21** (2010), 251–260.
6. P. B. Cohen and U. Zannier, *Multiplicative independence and bounded height, an example*, Proc. Algebraic Number Theory and Dioph. Approx. Conference, Graz 1998 (Walter de Gruyter, 2000), 93–101.

7. D. Ghioca, The isotrivial case in the Mordell–Lang theorem, *Trans. Amer. Math. Soc.* **360** (2008), 3839–3856.
8. D. Ghioca and R. Moosa, Division points on subvarieties of isotrivial semiabelian varieties, *Int. Math. Res. Not.* (2006), Article ID 65437, 23 pp.
9. P. Habegger, On the bounded height conjecture, *Int. Math. Res. Not.* **5** (2009), 860–886.
10. E. Hrushovski, The Mordell–Lang conjecture for function fields, *J. Amer. Math. Soc.* **9** (1996), 667–690.
11. S. Lang, *Introduction to Algebraic Geometry*, Addison-Wesley, Reading, MA, 1973.
12. D. Leitner, Linear equations over multiplicative groups in positive characteristic, *Acta Arith.* **153** (2012), 325–347.
13. D. Leitner, Linear equations over multiplicative groups in positive characteristic II, submitted.
14. D. Masser and U. Zannier, Torsion points on families of squares of elliptic curves, *Math. Ann.* **352** (2012), 453–484.
15. D. Masser and U. Zannier, Torsion points on families of simple abelian surfaces (with Appendix by V. Flynn), submitted, 36 pp.
16. G. Maurin, Courbes algébriques et équations multiplicatives, *Math. Ann.* **341** (2008), 789–824.
17. R. Moosa and T. Scanlon, F-structures and integral points on semiabelian varieties over finite fields, *Amer. J. Math.* **126** (2004), 473–522.
18. R. Pink, A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang, manuscript dated 17 April 2005, 13 pp.
19. G. Rémond, Intersection de sous-groupes et de sous-variétés. III, *Comment. Math. Helv.* **84** (2009), 835–863.
20. T. Scanlon, Positive characteristic Manin–Mumford theorem, *Compos. Math.* **141** (2005), 1351–1364.
21. E. Viada, The intersection of a curve with algebraic subgroups in a product of elliptic curves, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* **5** (2003), 47–75.
22. U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematics Studies 181, Princeton University Press, Princeton, NJ, 2012.
23. B. Zilber, Exponential sums equations and the Schanuel conjecture, *J. London Math. Soc.* **65** (2002), 27–44.