

Unlikely intersections for curves in additive groups over positive characteristic

W. D. Brownawell, D. W. Masser

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2016-30
December 2016

www.math.unibas.ch

Unlikely intersections for curves in additive groups over positive characteristic

W.D. Brownawell and D.W. Masser

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. Recently the second author made a start on removing this restriction by studying multiplicative groups over positive characteristic, and here we go further for additive groups with extra Frobenius structure. We state a conjecture for curves in general dimension and we prove it in three dimensions. We also give an example where the finite set in question can be explicitly determined.*

2010 MSC codes. 11G20, 14G17, 14H99.

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 the second author (for example the early paper [BMZ1] on curves, our later paper [BMZ2] on varieties of codimension 2, and our paper [BMZ3] on planes) and the wide-ranging extension of Habegger to arbitrary varieties (see [Ha] for example). When the group variety is projectively complete there are the results of Viada about powers of a fixed elliptic curve (see [V] for example) as well as those of Rémond generalizing to abelian varieties (see [R] for example); see especially the forthcoming paper [HP] of Habegger and Pila. There are also investigations of Zannier and the second author inside varying group varieties such as elliptic and abelian schemes (see [MZ1],[MZ2] for example). All this work on “unlikely intersections” takes place over zero characteristic, and one may consult the book [Za] of Zannier for a comprehensive survey. The general conjectures are due to Zilber [Zi] and Pink [P].

Over positive characteristic it is well-known that related simpler problems, such as those associated with the names Manin-Mumford about torsion points, can become false. 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.

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

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

For much more see for example the papers [Hr] of Hrushovski and [MS] of Moosa and Scanlon.

And the torsion situation can be combined with the finitely generated situation by allowing finite rank; under this heading see for example the papers [GM] of Ghioca and Moosa and [G] of Ghioca.

The second author [Mas] recently made a start on Zilber-Pink problems over positive characteristic, formulating a conjecture for curves in \mathbf{G}_m^n and proving it for \mathbf{G}_m^3 .

The object of the present paper is to continue the study of such problems, but now for the additive group \mathbf{G}_a^n . In zero characteristic the naive conjectures for \mathbf{G}_a^n become false, because they implicitly involve group subvarieties (of codimension 2), and there are simply far too many of these. For example the union of all of codimension 1 (and even of codimension $n - 1$) is the whole \mathbf{G}_a^n .

In positive characteristic it is well-known that problems of Manin-Mumford or Mordell-Lang type can be formulated for \mathbf{G}_a^n by imposing some extra structure. One immediately thinks of Drinfeld modules (on which the literature is already substantial); but there is an easier way using Frobenius (also see [G], in particular Theorem 2.6 p.3841). It is these “Frobenius modules” or “ F -modules” that we will study here. In a later paper we will advance to Carlitz modules.

To fix ideas, let us first review the situation for the multiplicative \mathbf{G}_m^n over zero characteristic. The decisive result was obtained by Maurin [Mau] (see also [BHMZ]), and, taking into account [BMZ4], we now know the following best possible result.

Theorem A. *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 for any non-zero (r_1, \dots, r_n) in \mathbf{Z}^n that the monomial $x_1^{r_1} \cdots x_n^{r_n}$ is not identically 1 on C . Then there are at most finitely many (ξ_1, \dots, ξ_n) in $C(K)$ for which there exist linearly independent $(a_1, \dots, a_n), (b_1, \dots, b_n)$ in \mathbf{Z}^n such that*

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

It was already pointed out in [Mas] (p.506) that the naive analogue of this in positive characteristic is false, in that a (stronger) hypothesis about two monomials, not one, is needed. Namely, we proved

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

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

In the case of F -modules, the p -Frobenius F acts on \mathbf{G}_a , and so does the (non-twisted) polynomial ring $R = \mathbf{F}_p[F]$ by

$$\varphi z = f_0 z + f_1 z^p + f_2 z^{p^2} + \cdots$$

for $\varphi = f_0 + f_1 F + f_2 F^2 + \cdots$.

From this we see that every “root of unity”, or better torsion element, is in $\overline{\mathbf{F}_p}$; but conversely any ζ in $\overline{\mathbf{F}_p}$ (including $\zeta = 0$) is in some finite extension of \mathbf{F}_p and so $\zeta, \zeta^p, \zeta^{p^2}, \dots$ are linearly dependent over \mathbf{F}_p showing that ζ is torsion.

Our analogue of the conjecture in [Mas] (p.506) is then

Conjecture. *Let K be an algebraically closed field of characteristic $p > 0$, and let C in \mathbf{G}_a^n be an irreducible curve defined over K .*

(*) Assume for any linearly independent $(\rho_1, \dots, \rho_n), (\sigma_1, \dots, \sigma_n)$ in R^n that the forms

$$\rho_1 x_1 + \dots + \rho_n x_n, \quad \sigma_1 x_1 + \dots + \sigma_n x_n$$

are algebraically independent over \mathbf{F}_p on C . Then there are at most finitely many (ξ_1, \dots, ξ_n) in $C(K)$ for which there exist linearly independent $(\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n)$ in R^n such that

$$\alpha_1 \xi_1 + \dots + \alpha_n \xi_n = \beta_1 \xi_1 + \dots + \beta_n \xi_n = 0. \quad (1.2)$$

Again a hypothesis about a single form $\rho_1 x_1 + \dots + \rho_n x_n$, not being zero or even constant, does not suffice for finiteness, as the example $x_1 x_2 = 1$ for $n = 2$ shows, because the condition on (ξ_1, ξ_2) means that ξ_1, ξ_2 are both torsion.

As in [Mas] (p.506), our hypothesis (*) is a shade too strong, because we need slightly more information than its failure to get an infinite set. Namely suppose that at least one of the offending two forms is non-constant on C (as a function). We may assume that the two coefficient vectors can be extended to a basis of R^n . Then 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 (note that the conjecture is invariant under such automorphisms). Now it suffices to intersect as above with $x_2 = \zeta_2$ for various torsion ζ_2 , because the relation between x_1 and x_2 forces $x_1 = \zeta_1$ also to be torsion.

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 forms are both constant. This is equivalent to the following.

(**) Assume for any linearly independent $(\rho_1, \dots, \rho_n), (\sigma_1, \dots, \sigma_n)$ in R^n with the forms

$$\rho_1 x_1 + \dots + \rho_n x_n, \quad \sigma_1 x_1 + \dots + \sigma_n x_n$$

algebraically dependent over \mathbf{F}_p on C that these forms are constant on C .

Clearly (**) is vacuously implied by (*). It is equivalent to (*) for $n = 2$ but not for $n = 3$, as the example $x_1 = t, x_2 = 1/t$ in \mathbf{G}_a^3 over $\mathbf{F}_p(t)$ shows. Namely (**) holds, because we may assume $\sigma_3 = 0$ and then a simple calculation shows $\rho_3 = 0$ or $\sigma_1 = \sigma_2 = 0$. But (*) fails due to $(1, 0, 0), (0, 1, 0)$ and $x_1 x_2 = 1$.

Actually we see from this that if (**) holds but (*) fails in \mathbf{G}_a^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 linearly dependent. So $\gamma_1 x_1 + \gamma_2 x_2 = 0$ on C for some non-zero (γ_1, γ_2) in R^2 . Now the two forms $\gamma_1 x_1 + \gamma_2 x_2, x_3$ are algebraically dependent over \mathbf{F}_p on C ; consequently they are both constant on C , an absurdity. So one might formulate a stronger conjecture with the weaker (***) 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 two less trivial things concerning the above conjecture with (*). First we show that it holds in \mathbf{G}_a^3 (and therefore so does the (***) version). The arguments do not appear to extend immediately to \mathbf{G}_a^4 . And second we actually determine the finite set for a particular line in \mathbf{G}_a^3 ; the shape is even independent of p , at least up to constants. This kind of independence was already observed by Leitner in the context of Mordell-Lang; see for example [L1] (pp.327-329) and especially [L2].

Here are our precise results.

Theorem 1. *Let K be an algebraically closed field of characteristic $p > 0$, and let C in \mathbf{G}_a^3 be an irreducible curve defined over K . Assume for any linearly independent $(\rho_1, \rho_2, \rho_3), (\sigma_1, \sigma_2, \sigma_3)$ in R^3 that the forms*

$$\rho_1 x_1 + \rho_2 x_2 + \rho_3 x_3, \quad \sigma_1 x_1 + \sigma_2 x_2 + \sigma_3 x_3$$

are algebraically independent 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 $(\alpha_1, \alpha_2, \alpha_3), (\beta_1, \beta_2, \beta_3)$ in R^3 such that

$$\alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 = \beta_1 \xi_1 + \beta_2 \xi_2 + \beta_3 \xi_3 = 0. \quad (1.3)$$

Theorem 2. *Let C_0 be the conic over $\mathbf{F}_p(t)$ parametrized in \mathbf{G}_a^3 by (x, tx, tx^2) for t transcendental over \mathbf{F}_p . Then if (ξ_1, ξ_2, ξ_3) is in $C_0(\overline{\mathbf{F}_p(t)})$ for which there exist linearly independent $(\alpha_1, \alpha_2, \alpha_3), (\beta_1, \beta_2, \beta_3)$ in R^3 with*

$$\alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 = \beta_1 \xi_1 + \beta_2 \xi_2 + \beta_3 \xi_3 = 0 \quad (1.4)$$

we have

$$(\xi_1, \xi_2, \xi_3) = \left(\frac{a}{t}, a, \frac{a^2}{t} \right), \quad a \xi_1 - \xi_3 = \xi_2 - \xi_2^p = 0$$

or

$$(\xi_1, \xi_2, \xi_3) = (a, at, a^2t), \quad \xi_1 - \xi_1^p = a\xi_2 - \xi_3 = 0$$

for a in \mathbf{F}_p , with the further possibility

$$(\xi_1, \xi_2, \xi_3) = \left(\frac{1}{t+1}, \frac{t}{t+1}, \frac{t}{(t+1)^2} \right), \quad \xi_1 + \xi_1^2 + \xi_2 + \xi_2^2 = \xi_1 + \xi_1^2 + \xi_3 = 0$$

when $p = 2$.

The rest of this paper is arranged as follows.

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

And then in section 3 we prove Theorem 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 we use induction on the degree of a certain auxiliary polynomial, together with an iterative procedure involving various weighted degrees.

It will be apparent from the examples above, and especially the proofs below, that we are essentially working over function fields. For another interpretation of “unlikely intersections” in this context, see the work of Chatzidakis, Ghioca, Maurin and the second author [CGMM]. We thank the referee for reminding us of this and also for other valuable comments.

2. Proof of Theorem 2. As in [Mas] (p.508), there is a unique integer e (possibly negative) such that the coordinates of $(\eta_1, \eta_2, \eta_3) = F^e(\xi_1, \xi_2, \xi_3)$ lie in the separable completion \mathcal{F} of $\mathbf{F}_p(t)$ and not all the derivatives $\dot{\eta}_1, \dot{\eta}_2, \dot{\eta}_3$ are zero (this comes from $\bigcup_{i=0}^{\infty} \mathcal{F}^{1/p^i} = \overline{\mathbf{F}_p(t)}$ and $\bigcap_{i=0}^{\infty} \mathcal{F}^{p^i} = \overline{\mathbf{F}_p}$). Consider the R -module M of all (μ_1, μ_2, μ_3) in R^3 such that $\mu_1\eta_1 + \mu_2\eta_2 + \mu_3\eta_3 = 0$. It is clearly of rank 2. We claim that it has generators $(\gamma_1, \gamma_2, \gamma_3), (\delta_1, \delta_2, \delta_3)$ whose “constant vectors”, call them $(c_1, c_2, c_3), (d_1, d_2, d_3)$ in \mathbf{F}_p^3 , are linearly independent. For example by elementary divisors over the principal ring R there are generators u, v, w of R^3 and γ, δ in R such that $\gamma u, \delta v$ generate M . Now M is stable under F^{-1} and so we can assume that γ, δ have non-zero constant terms. As already the constant vectors of u, v, w are linearly independent the same is true of u, v and so of $\gamma u, \delta v$;

thus these provide the required generators. This is the additive analogue of the primitivity argument at the start of section 2 of [Mas].

At last we can start to differentiate. Note that $\xi_1\xi_2 = \xi_3$ so also $\eta_1\eta_2 = \eta_3$. We get

$$c_1\dot{\eta}_1 + c_2\dot{\eta}_2 + c_3\dot{\eta}_3 = 0$$

$$d_1\dot{\eta}_1 + d_2\dot{\eta}_2 + d_3\dot{\eta}_3 = 0$$

$$\eta_2\dot{\eta}_1 + \eta_1\dot{\eta}_2 - \dot{\eta}_3 = 0.$$

Remembering that not all the $\dot{\eta}_1, \dot{\eta}_2, \dot{\eta}_3$ are zero and taking the determinant, we get

$$e_1\eta_2 + e_2\eta_1 - e_3 = 0 \tag{2.1}$$

for e_1, e_2, e_3 in \mathbf{F}_p which by our choice of generators are not all zero. Thus also $e_1\xi_2 + e_2\xi_1 - e_3 = 0$ which for $(\xi_1, \xi_2, \xi_3) = (\xi, t\xi, t\xi^2)$ gives

$$e_1t\xi + e_2\xi - e_3 = 0$$

and so at most finitely many $\xi = \frac{e_3}{e_1t + e_2}$.

Now if $e_1 = 0$ or $e_3 = 0$ then $\xi = a$ is constant and we get the second point in Theorem 2. And if $e_2 = 0$ then $\xi = a/t$ and we get the first point.

Thus we can assume e_1, e_2, e_3 non-zero. In particular we can suppose $e_1 = -1$.

Now consider the relation $\alpha_1\xi_1 + \alpha_2\xi_2 + \alpha_3\xi_3 = 0$ in (1.4). If $\alpha_3 \neq 0$ then we see in $\alpha_3\xi_3$ a pole of order $2p^r$ at $t = e_2$, and when $p > 2$ this cannot be killed by anything in $\alpha_1\xi_1 + \alpha_2\xi_2$. So $\alpha_3 = 0$ when $p > 2$; and similarly $\beta_3 = 0$ in (1.4). But then ξ_1, ξ_2 would be torsion, contradicting $\xi_2 = t\xi_1$.

And when $p = 2$ then $e_1 = e_2 = e_3 = 1$ giving the third point in Theorem 2.

3. Proof of Theorem 1. The proof above worked well because the ‘‘new relation’’ (2.1) is clearly independent of the ‘‘old relation’’ $\eta_1\eta_2 = \eta_3$. Of course this old relation for a general curve C in \mathbf{G}_a^3 may not exist, but if there is a relation of the shape

$$P(\eta_1, \eta_2, \eta_3) = 0 \tag{3.1}$$

with P over \mathbf{F}_p , then we get in place of (2.1) $P'(\eta_1, \eta_2, \eta_3) = 0$ where $P' = \mathcal{L}(P)$ for the differential operator

$$\mathcal{L} = e_1\frac{\partial}{\partial X_1} + e_2\frac{\partial}{\partial X_2} + e_3\frac{\partial}{\partial X_3} \neq 0,$$

where for clarity we use X_1, X_2, X_3 for independent variables.

If $P' \neq 0$ then its total degree is strictly less than the total degree of P ; and, as we may assume P irreducible over \mathbf{F}_p , we could conclude that (η_1, η_2, η_3) lies on a curve C' defined over \mathbf{F}_p . So also (ξ_1, ξ_2, ξ_3) lies on C' . Now C itself is not defined over \mathbf{F}_p , otherwise for example x_1, x_2 would be algebraically dependent over \mathbf{F}_p on C , which is excluded by the hypothesis in Theorem 1. Thus C, C' intersect in at most a finite set and we are done.

It turns out that the main difficulty is indeed the possibility $P' = 0$; that is, $\mathcal{L}(P) = 0$.

We need two lemmas concerning differential operators \mathcal{L} as above. Given independent variables X_1, \dots, X_n we will say that $\tilde{X}_1, \dots, \tilde{X}_n$ are new variables if they are related to X_1, \dots, X_n by a transformation in $GL_n(\mathbf{F}_p)$. This defines an automorphism of \mathbf{G}_a^n , and we have already remarked that our conjecture is invariant under such automorphisms and even under $GL_n(R)$. More significantly we can check invariance under “isogenies” or surjective endomorphisms corresponding to non-singular matrices with entries in R . A particularly useful example for $n = 3$ is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & F \end{pmatrix} \quad (3.2)$$

sending (X_1, X_2, X_3) to (X_1, X_2, X_3^p) .

Lemma 1. Suppose $n = 3$.

(i) If $\mathcal{L}(X_1) \neq 0$ or $\mathcal{L}(X_2) \neq 0$ then there are new variables X_1, X_2, \tilde{X}_3 with $\mathcal{L}(\tilde{X}_3) = 0$.

(ii) If $\mathcal{L}(X_1) \neq 0$ then there are new variables $X_1, \tilde{X}_2, \tilde{X}_3$ with $\mathcal{L}(\tilde{X}_2) = \mathcal{L}(\tilde{X}_3) = 0$.

Proof. For (i) we have $e_1 \neq 0$ or $e_2 \neq 0$ and we just have to choose $\tilde{X}_3 = a_1 X_1 + a_2 X_2 + X_3$ with $a_1 e_1 + a_2 e_2 + e_3 = 0$. For (ii) we have $e_1 \neq 0$ and we choose $\tilde{X}_2 = a_2 X_1 + X_2, \tilde{X}_3 = a_3 X_1 + X_3$ with $a_2 e_1 + e_2 = a_3 e_1 + e_3 = 0$.

Next we generalize to variables X_1, \dots, X_n and

$$\mathcal{L} = e_1 \frac{\partial}{\partial X_1} + \dots + e_n \frac{\partial}{\partial X_n} \neq 0$$

for $n \geq 2$ (in fact later only $n = 3$ or $n = 2$).

Lemma 2. There are new variables $\tilde{X}_1, \dots, \tilde{X}_{n-1}, \tilde{X}_n$ with $\mathcal{L}(\tilde{X}_1) = \dots = \mathcal{L}(\tilde{X}_{n-1}) = 0$. If $\mathcal{L}(P) = 0$ for some P in $\mathbf{F}_p[X_1, \dots, X_n]$, then there is a polynomial \tilde{P} with

$$P = \tilde{P}(\tilde{X}_1, \dots, \tilde{X}_{n-1}, \tilde{X}_n^p).$$

Proof. We note that the vanishing of $\mathcal{L}(a_1X_1 + \cdots + a_nX_n) = a_1e_1 + \cdots + a_ne_n$ defines a subspace of \mathbf{F}_p^n of dimension at least $n-1$, so we can certainly find $\tilde{X}_1, \dots, \tilde{X}_{n-1}$ and then \tilde{X}_n . Now we write $P(X_1, \dots, X_n)$ as a polynomial $\tilde{P}_0(\tilde{X}_1, \dots, \tilde{X}_n)$ in the new variables, so that $\mathcal{L}(P) = (\partial\tilde{P}_0/\partial\tilde{X}_n)\mathcal{L}(\tilde{X}_n)$, and note that necessarily $\mathcal{L}(\tilde{X}_n) \neq 0$. Thus $\partial\tilde{P}_0/\partial\tilde{X}_n = 0$; and this is well-known to imply that \tilde{P}_0 involves only powers of \tilde{X}_n^p .

Now in proving Theorem 1 we may suppose that K has finite transcendence degree over \mathbf{F}_p . For C is certainly defined over such a K ; and we claim that any point (ξ_1, ξ_2, ξ_3) on it with (1.3) is automatically in K^3 . If not, then C lies in the hypersurface H_α defined by $\alpha_1X_1 + \alpha_2X_2 + \alpha_3X_3 = 0$; and similarly C lies in H_β with $\beta_1X_1 + \beta_2X_2 + \beta_3X_3 = 0$. So C lies in $H_\alpha \cap H_\beta$. However that is a curve over \mathbf{F}_p and it would follow that C is a component so defined over $\overline{\mathbf{F}_p}$. But then x_1, x_2 would be algebraically dependent over \mathbf{F}_p contradicting the hypothesis on C . This proves the claim above.

It also shows that Theorem 1 is trivial if K has transcendence degree 0 over \mathbf{F}_p .

Next we suppose that K has transcendence degree 1 over \mathbf{F}_p . It is therefore 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 . Thus there is a relation

$$P(x_1, x_2, x_3) = 0 \tag{3.3}$$

with a polynomial $P = P(X_1, X_2, X_3) \neq 0$ defined over \mathbf{F}_p . Then indeed (3.1) holds. Further this P can be assumed to be irreducible over \mathbf{F}_p . (The example in Theorem 2 corresponds to $P = X_1X_2 - X_3$.)

We now work with induction on the degree D of P ; thus

$$P(X_1, X_2, X_3) = \sum p(\iota_1, \iota_2, \iota_3) X_1^{\iota_1} X_2^{\iota_2} X_3^{\iota_3},$$

the sum being taken over $\iota_1 + \iota_2 + \iota_3 \leq D$. This starting situation we describe (for fixed D) as of weight (000); in general for $0 \leq m_1 \leq m_2 \leq m_3$ we will have to consider the weight $(m_1m_2m_3)$ defined by

$$p^{m_1}\iota_1 + p^{m_2}\iota_2 + p^{m_3}\iota_3 \leq D \tag{3.4}$$

in the above sum. We will prove that starting with a curve C and corresponding polynomial P of weight (000) we can eventually get to another curve and polynomial of weight $(m_1m_2m_3)$ with either $m_1 \geq 1$ or m_3 arbitrarily large. If $m_1 \geq 1$ then

$$\iota_1 + \iota_2 + \iota_3 \leq \frac{p^{m_1}\iota_1 + p^{m_2}\iota_2 + p^{m_3}\iota_3}{p} \leq \frac{D}{p} < D$$

and so induction applies. And if $p^{m_3} > D$ then (3.4) implies $\iota_3 = 0$ so the resulting polynomial is independent of X_3 ; this is ruled out by our hypothesis.

Again to warm up, we start with (000). This leads to $\mathcal{L} \neq 0$ with $\mathcal{L}(P) = 0$, so by Lemma 2 with $n = 3$ there are new variables $\tilde{X}_1, \tilde{X}_2, \tilde{X}_3$ with $P = \tilde{P}(\tilde{X}_1, \tilde{X}_2, \tilde{X}_3^p)$, and so after $GL_3(\mathbf{F}_p)$ and (3.2) to eliminate the exponent p we end up with (001). This is the first step.

Now we describe the general step. If we have not reached $m_1 \geq 1$ then there are three different weights

- (I) (00*l*) ($0 < l$),
- (II) (0*l*0) ($0 < l$),
- (III) (0*l**m*) ($0 < l < m$).

and we treat each weight in turn.

To begin with (I), where $\iota_1 + \iota_2 + p^l \iota_3 \leq D$. There are two cases.

If $(e_1, e_2) \neq (0, 0)$ for $\mathcal{L} = e_1 \frac{\partial}{\partial X_1} + e_2 \frac{\partial}{\partial X_2} + e_3 \frac{\partial}{\partial X_3}$ then by Lemma 1(i) there are new variables X_1, X_2, \tilde{X}_3 with $\mathcal{L}(\tilde{X}_3) = 0$. We write $P = \tilde{P}(X_1, X_2, \tilde{X}_3)$. Now X_3 is a linear combination of X_1, X_2, \tilde{X}_3 with coefficients in \mathbf{F}_p , and so $X_3^{\iota_3}$ involves only $X_1^{\theta_1} X_2^{\theta_2} \tilde{X}_3^{\tilde{\iota}_3}$ with $\theta_1 + \theta_2 + \tilde{\iota}_3 = \iota_3$. Thus not forgetting $X_1^{\iota_1} X_2^{\iota_2}$ we calculate

$$(\iota_1 + \theta_1) + (\iota_2 + \theta_2) + p^l \tilde{\iota}_3 \leq \iota_1 + \iota_2 + p^l(\theta_1 + \theta_2 + \tilde{\iota}_3) \leq D$$

and so \tilde{P} still has weight (00*l*). We write further $P = \sum_{\tilde{\iota}_3} Q(\tilde{\iota}_3) \tilde{X}_3^{\tilde{\iota}_3}$ with $Q(\tilde{\iota}_3) = Q(X_1, X_2; \tilde{\iota}_3)$ and note that

$$0 = \mathcal{L}(P) = \sum_{\tilde{\iota}_3} \mathcal{L}(Q(\tilde{\iota}_3)) \tilde{X}_3^{\tilde{\iota}_3}.$$

Thus each $\mathcal{L}(Q(\tilde{\iota}_3)) = 0$. By Lemma 2 with $n = 2$ (and operator $e_1 \partial / \partial X_1 + e_2 \partial / \partial X_2 \neq 0$) there are new variables \tilde{X}_1, \tilde{X}_2 related to X_1, X_2 via $GL_2(\mathbf{F}_p)$ such that $Q(X_1, X_2; \tilde{\iota}_3) = \tilde{Q}(\tilde{X}_1, \tilde{X}_2; \tilde{\iota}_3)$. So $P = \sum_{\tilde{\iota}_3} \tilde{Q}(\tilde{X}_1, \tilde{X}_2; \tilde{\iota}_3) \tilde{X}_3^{\tilde{\iota}_3}$. Here $Q(X_1, X_2; \tilde{\iota}_3)$ involves $X_1^{\iota_1} X_2^{\iota_2}$ with $\iota_1 + \iota_2 \leq D - p^l \tilde{\iota}_3$. Now if we expand the ι_1 th power of a linear combination of $Y_1, Y_2^{1/p}$ we see terms $Y_1^{\theta_1} Y_2^{\theta_2/p}$ with $\theta_1 + \theta_2 = \iota_1$; and similarly $Y_1^{\phi_1} Y_2^{\phi_2/p}$ with $\phi_1 + \phi_2 = \iota_2$ for the ι_2 th power of a second such linear combination. Multiplying, we find that $\tilde{Q}(Y_1, Y_2)$ involves $Y_1^{\tilde{\iota}_1} Y_2^{\tilde{\iota}_2}$ with

$$\tilde{\iota}_1 + p \tilde{\iota}_2 = \theta_1 + \phi_1 + p \left(\frac{\theta_2}{p} + \frac{\phi_2}{p} \right) = \iota_1 + \iota_2 \leq D - p^l \tilde{\iota}_3.$$

Then substituting $\tilde{X}_1, \tilde{X}_2^p$ for Y_1, Y_2 , changing to new variables $\tilde{X}_1, \tilde{X}_2, \tilde{X}_3$ and using a permuted form of (3.2) gives the new condition $\tilde{l}_1 + p\tilde{l}_2 + p^l\tilde{l}_3 \leq D$. This is of course (01l).

There remains the possibility $(e_1, e_2) = (0, 0)$ in this situation with (I). Then $e_3 \neq 0$. Now from an analogous $P = \sum_{\iota_3} Q(\iota_3)X_3^{\iota_3}$ we deduce $0 = \mathcal{L}(P) = \sum_{\iota_3} Q(\iota_3)\iota_3 e_3 X_3^{\iota_3-1}$ and so $Q(\iota_3) = 0$ whenever p does not divide ι_3 . So $P = \tilde{P}(X_1, X_2, X_3^p)$ giving rise after (3.2) to the new $\tilde{l}_1 + \tilde{l}_2 + p^{l+1}\tilde{l}_3 \leq D$ which is (00 l + 1).

In summary the weight (00l) ($0 < l$) leads to either (01l) or (00 l + 1).

Next (II), where $\iota_1 + p^l\iota_2 + p^l\iota_3 \leq D$. There are two cases.

If $e_1 \neq 0$ then by Lemma 1(ii) there are there are new variables $X_1, \tilde{X}_2, \tilde{X}_3$ with $\mathcal{L}(\tilde{X}_2) = \mathcal{L}(\tilde{X}_3) = 0$. We write $P = \tilde{P}(X_1, \tilde{X}_2, \tilde{X}_3)$ and verify as in (I) that \tilde{P} still has weight (0ll). We write further $P = \sum_{\tilde{l}_1} Q(\tilde{l}_1)X_1^{\tilde{l}_1}$ with $Q(\tilde{l}_1) = Q(\tilde{X}_2, \tilde{X}_3; \tilde{l}_1)$ and note that $0 = \mathcal{L}(P) = \sum_{\tilde{l}_1} Q(\tilde{l}_1)\tilde{l}_1 e_1 X_1^{\tilde{l}_1-1}$. As just above this means that \tilde{P} involves X_1^p and so it is clear that we reach (1ll).

If $e_1 = 0$ we get, now with $Q(\iota_1) = Q(X_2, X_3; \iota_1)$, a similar $0 = \mathcal{L}(P) = \sum_{\iota_1} \mathcal{L}(Q(\iota_1))X_1^{\iota_1}$. Thus each $\mathcal{L}(Q(\iota_1)) = 0$. By Lemma 2 with $n = 2$ there are new variables \tilde{X}_2, \tilde{X}_3 related to X_2, X_3 via $GL_2(\mathbf{F}_p)$ such that $Q(X_2, X_3; \iota_1) = \tilde{Q}(\tilde{X}_2, \tilde{X}_3; \iota_1)$. As at the start of (I) this leads to (0l l + 1).

In summary the weight (0ll) ($0 < l$) leads to either (1ll) or (0l l + 1).

Last (III), where $\iota_1 + p^l\iota_2 + p^m\iota_3 \leq D$. This is slightly more troublesome, and there are now three cases.

If $e_1 \neq 0$ then certainly $(e_1, e_2) \neq (0, 0)$ and so there are new variables X_1, X_2, \tilde{X}_3 with $\mathcal{L}(\tilde{X}_3) = 0$. We write $P = \tilde{P}(X_1, X_2, \tilde{X}_3)$ and verify as before that \tilde{P} still has weight (0lm). We write further $P = \sum_{\tilde{l}_3} Q(\tilde{l}_3)\tilde{X}_3^{\tilde{l}_3}$ with $Q(\tilde{l}_3) = Q(X_1, X_2; \tilde{l}_3)$ and note that $0 = \mathcal{L}(P) = \sum_{\tilde{l}_3} \mathcal{L}(Q(\tilde{l}_3))\tilde{X}_3^{\tilde{l}_3}$. Thus each $\mathcal{L}(Q(\tilde{l}_3)) = 0$. By Lemma 2 there are new variables \tilde{X}_1, \tilde{X}_2 related to X_1, X_2 via $GL_2(\mathbf{F}_p)$ such that $Q(X_1, X_2; \tilde{l}_3) = \tilde{Q}(\tilde{X}_1, \tilde{X}_2; \tilde{l}_3)$; moreover this lemma shows that all we need is $\mathcal{L}(\tilde{X}_1) = 0$ and \tilde{X}_2 independent of \tilde{X}_1 . For example we can take $\tilde{X}_1 = e_2 X_1 - e_1 X_2$ and then $\tilde{X}_2 = X_1$ (because $e_1 \neq 0$). We will see that the presence of X_2 in \tilde{X}_1 leads to a new relation $p\tilde{l}_1 + \dots \leq D$ and so $m_1 = 1$.

In fact $X_1 = \tilde{X}_2$, $X_2 = -e_1^{-1}(\tilde{X}_1 - e_2\tilde{X}_2)$ so

$$\tilde{Q}(Y_1, Y_2; \tilde{l}_3) = Q(Y_2, -e_1^{-1}(Y_1 - e_2 Y_2); \tilde{l}_3).$$

This involves terms $Y_2^{\theta_1}(Y_1 - e_2 Y_2)^{\theta_2}$ with $\theta_1 + p^l\theta_2 \leq D - p^m\tilde{l}_3$ and so

$$Y_2^{\theta_1} Y_1^{\kappa_1} Y_2^{\kappa_2} = Y_1^{\kappa_1} Y_2^{\kappa_2 + \theta_1} = Y_1^{\kappa_1} (Y_2^p)^{(\kappa_2 + \theta_1)/p}$$

with $\kappa_1 + \kappa_2 = \theta_2$. So $P = \sum_{\tilde{\iota}_3} \tilde{Q}(\tilde{X}_1, \tilde{X}_2^p; \tilde{\iota}_3) \tilde{X}_3^{\tilde{\iota}_3}$ after $GL_3(\mathbf{F}_p)$ and corresponding (3.2) involves exponents $\tilde{\iota}_1, \tilde{\iota}_2, \tilde{\iota}_3$ with

$$\tilde{\iota}_1 = \kappa_1, \tilde{\iota}_2 = \frac{\kappa_2 + \theta_1}{p}.$$

For these we calculate

$$p\tilde{\iota}_1 + p\tilde{\iota}_2 + p^m\tilde{\iota}_3 = p\kappa_1 + \kappa_2 + \theta_1 + p^m\tilde{\iota}_3 \leq p\theta_2 + \theta_1 + p^m\tilde{\iota}_3 \leq \theta_1 + p^l\theta_2 + p^m\tilde{\iota}_3 \leq D.$$

So indeed we end up with $m_1 = 1$ and more precisely (11m).

Next in (III) we consider the possibility $e_1 = 0, e_2 \neq 0$. Now $\mathcal{L}(X_1) = 0$ and there is still \tilde{X}_3 with $\mathcal{L}(\tilde{X}_3) = 0$. Writing P in terms of X_1, X_2, \tilde{X}_3 we stay as before in (0lm). Now $P = \sum_{\iota_2} X_2^{\iota_2} Q(\iota_2)$ shows as above that P involves X_2^p . So we end up with (0 l + 1 m).

There remains the possibility $(e_1, e_2) = (0, 0)$. But then it should by now be clear that we get (0l m + 1).

In summary the weight (0lm) ($0 < l < m$) leads to (11m), (0 l + 1 m) or (0l m + 1).

Now examining each of the three summaries shows that at each step on $(0m_2m_3)$ we reach either $m_1 = 1$ or $(0m'_2m'_3)$ with $m'_2 + m'_3 > m_2 + m_3$. Thus if we never reach $m_1 = 1$ then $m_2 + m_3$ becomes arbitrarily large; and since $m_2 + m_3 \leq 2m_3$ the same holds for m_3 . This finishes the proof, at least for $K = \overline{\mathbf{F}_p(t)}$.

What if K has transcendence degree more than 1 over \mathbf{F}_p ? Say $K = \overline{\mathbf{F}_p(t, u)}$. With our point (ξ_1, ξ_2, ξ_3) the two additive 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 $\mathbf{F}_p(t, u)$. We can assume x_1, x_2, x_3 are algebraically independent over \mathbf{F}_p on C otherwise we get (3.3) and could proceed as before. Write out a fixed polynomial relation

$$\sum_i P(x_1, x_2, x_3; i)t^i = 0,$$

where we can assume that all the $P(X_1, X_2, X_3; i)$ 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 $P(\xi_1, \xi_2, \xi_3; i) = 0$. This defines a curve C' over \mathbf{F}_p , and as at the beginning of this section we get our finite set by intersecting C and C' .

A similar argument works for $K = \overline{\mathbf{F}_p(t_1, \dots, t_d)}$ with $d \geq 3$. 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

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

where we can assume that all the $P(X_1, X_2, X_3; i_1, \dots, i_{d-1})$ have no common factor. Specializing and recalling that t_1, \dots, t_{d-1} were algebraically independent over Ξ , we deduce that all the $P(\xi_1, \xi_2, \xi_3; i_1, \dots, i_{d-1}) = 0$. So once more we have C' and our finite set.

References

- [BHMZ] E. Bombieri, P. Habegger, D. Masser and U. Zannier, *A note on Maurin's Theorem*, Rend. Lincei Mat. Appl. **21** (2010), 251-260.
- [BMZ1] E. Bombieri, D. Masser and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Research Notices **20** (1999), 1119-1140.
- [BMZ2] E. Bombieri, D. Masser and U. Zannier, *Anomalous subvarieties - structure theorems and applications*, Int. Math. Research Notices (2007), Article ID rnm057 (33 pages), doi: 10.1093/imrn/rnm057.
- [BMZ3] E. Bombieri, D. Masser and U. Zannier, *Intersecting a plane with algebraic subgroups of multiplicative groups*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. **VII** (2008), 51-80.
- [BMZ4] E. Bombieri, D. Masser and U. Zannier, *On unlikely intersections of complex varieties with tori*, Acta Arithmetica **133** (2008), 309-323.
- [CGMM] Z. Chatzidakis, D. Ghioca, D. Masser and G. Maurin, *Unlikely, likely and impossible intersections without algebraic groups*, Rendiconti Lincei Mat. Appl. **24** (2013), 485-501.
- [CZ] 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.

- [GM] D. Ghioca and R. Moosa, *Division points on subvarieties of isotrivial semiabelian varieties*, Int. Math. Research Notices (2006), Article ID 65437 (23 pages).
- [G] D. Ghioca, *The isotrivial case in the Mordell-Lang theorem*, Trans. Amer. Math. Soc. **360** (2008), 3839-3856.
- [Ha] P. Habegger, *On the bounded height conjecture*, Int. Math. Research Notices **5** (2009), 860-886.
- [HP] P. Habegger and J. Pila, *O-minimality and certain atypical intersections*, to appear in Ann. Sci. École Norm. Sup. [arXiv:1409.0771].
- [Hr] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc **9** (1996), 667-690.
- [L1] D. Leitner, *Linear equations over multiplicative groups in positive characteristic*, Acta Arithmetica **153** (2012), 325-347.
- [L2] D. Leitner, *Linear equations over multiplicative groups in positive characteristic II*, submitted.
- [MS] R. Moosa and T. Scanlon, *F-structures and integral points on semiabelian varieties over finite fields*, Amer. J. Math. **126** (2004), 473-522.
- [MZ1] D. Masser and U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Annalen **352** (2012), 453-484.
- [MZ2] D. Masser and U. Zannier, *Torsion points on families of abelian surfaces and Pell's equation over polynomial rings (with Appendix by V. Flynn)*, J. European Math. Soc. **17** (2015), 2379-2416.
- [Mas] D. Masser, *Unlikely intersections for curves in multiplicative groups over positive characteristic*, Quarterly J. Math. **65** (2014), 505-515.
- [Mau] G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Annalen **341** (2008), 789-824.
- [P] R. Pink, *A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang*, manuscript dated 17th April 2005 (13 pages).
- [R] G. Rémond, *Intersection de sous-groupes et de sous-variétés. III*, Comment. Math. Helv. **84** (2009), 835-863.
- [V] E. Viada, *The intersection of a curve with algebraic subgroups in a product of elliptic curves*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. **5** (2003), 47-75.

[Za] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Math. Studies **181**, Princeton 2012.

[Zi] B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. **65** (2002), 27-44.

W.D. Brownawell: Department of Mathematics, The Pennsylvania State University, University Park, PA 16802 (*wdb@math.psu.edu*).

D.W. Masser: Departement Mathematik und Informatik, Universität Basel, Spiegelgasse 1, 4051 Basel, Switzerland (*David.Masser@unibas.ch*).

8th October 2016

Revised 30th November 2016

LATEST PREPRINTS

- | No. | Author: Title |
|---------|---|
| 2016-06 | M. Dambrine, I. Greff, H. Harbrecht, B. Puig
<i>Numerical solution of the homogeneous Neumann boundary value problem on domains with a thin layer of random thickness</i> |
| 2016-07 | G. Alberti, G. Crippa, A. L. Mazzucato
<i>Exponential self-similar mixing by incompressible flows</i> |
| 2016-08 | M. Bainbridge, P. Habegger, M. Möller
<i>Teichmüller curves in genus three and just likely intersections in $G_m^n \times G_a^n$</i> |
| 2016-09 | Gabriel A. Dill
<i>Effective approximation and Diophantine applications</i> |
| 2016-10 | J. Blanc, S. Zimmermann
<i>Topological simplicity of the Cremona groups</i> |
| 2016-11 | I. Hedén, S. Zimmermann
<i>The decomposition group of a line in the plane</i> |
| 2016-12 | J. Ballani, D. Kressner, M. Peters
<i>Multilevel tensor approximation of PDEs with random data</i> |
| 2016-13 | M. J. Grote, M. Kray, U. Nahum
<i>Adaptive eigenspace method for inverse scattering problems in the frequency domain</i> |
| 2016-14 | H. Harbrecht, M. Peters, M. Schmidlin
<i>Uncertainty quantification for PDEs with anisotropic random diffusion</i> |
| 2016-15 | F. Da Lio, L. Martinazzi
<i>The nonlocal Liouville-type equation in R and conformal immersions of the disk with boundary singularities</i> |
| 2016-16 | A. Hyder
<i>Conformally Euclidean metrics on R^n with arbitrary total Q-curvature</i> |
| 2016-17 | G. Mancini, L. Martinazzi
<i>The Moser-Trudinger inequality and its extremals on a disk via energy estimates</i> |
| 2016-18 | R. N. Gantner, M. D. Peters
<i>Higher order quasi-Monte Carlo for Bayesian shape inversion</i> |

LATEST PREPRINTS

No.	Author: <i>Title</i>
2016-19	C. Urech <i>Remarks on the degree growth of birational transformations</i>
2016-20	S. Dahlke, H. Harbrecht, M. Utzinger, M. Weimar <i>Adaptive wavelet BEM for boundary integral equations: Theory and numerical experiments</i>
2016-21	A. Hyder, S. Iula, L. Martinazzi <i>Large blow-up sets for the prescribed Q-curvature equation in the Euclidean space</i>
2016-22	P. Habegger <i>The norm of Gaussian periods</i>
2016-23	P. Habegger <i>Diophantine approximations on definable sets</i>
2016-24	F. Amoroso, D. Masser <i>Lower bounds for the height in Galois extensions</i>
2016-25	W. D. Brownawell, D. W. Masser <i>Zero estimates with moving targets</i>
2016-26	H. Derksen, D. Masser <i>Linear equations over multiplicative groups, recurrences, and mixing III</i>
2016-27	D. Bertrand, D. Masser, A. Pillay, U. Zannier <i>Relative Manin-Mumford for semi-abelian surfaces</i>
2016-28	L. Capuano, D. Masser, J. Pila, U. Zannier <i>Rational points on Grassmannians and unlikely intersections in tori</i>
2016-29	C. Nobili, F. Otto <i>Limitations of the background field method applied to Rayleigh-Bénard convection</i>
2016-30	W. D. Brownawell, D. W. Masser <i>Unlikely intersections for curves in additive groups over positive characteristic</i>