Diophantine equations in positive characteristic

Koymans, P.H.

Chapter 2

On the equation $x_1 + x_2 = 1$ in finitely generated multiplicative groups in positive characteristic[1]

Joint work with Carlo Pagano

Abstract

Let K be a field of characteristic $p > 0$ and let G be a subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}}(G \otimes_{\mathbb{Z}} \mathbb{Q}) = r$ finite. Then Voloch proved that the equation $ax+by = 1$ in $(x, y) \in G$ for given $a, b \in K^*$ has at most $p^r(p^r + p - 2)/(p - 1)$ solutions $(x, y) \in G$, unless $(a, b)^n \in G$ for some $n \geq 1$. Voloch also conjectured that this upper bound can be replaced by one depending only on r. Our main theorem answers this conjecture positively. We prove that there are at most $31 \cdot 19^{r+1}$ solutions (x, y) unless $(a, b)^n \in G$ for some $n \geq 1$ with $(n, p) = 1$. During the proof of our main theorem we generalize the work of Beukers and Schlickewei to positive characteristic, which heavily relies on diophantine approximation methods. This is a surprising feat on its own, since usually these methods can not be transferred to positive characteristic.

2.1 Introduction

Let G be a subgroup of $\mathbb{C}^* \times \mathbb{C}^*$ with coordinatewise multiplication. Assume that the rank $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q} = r$ is finite. Beukers and Schlickewei [3] proved that the equation

$$x_1 + x_2 = 1$$

[1] A slightly modified version of this chapter appeared in the Quarterly Journal of Mathematics, volume 68, issue 3, pages 923-934.

in $(x_1, x_2) \in G$ has at most 2^{8r+8} solutions. A key feature of their upper bound is that it depends only on r.

In this chapter we will analyze the characteristic p case. To be more precise, let $p > 0$ be a prime number and let K be a field of characteristic p. Let G be a subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q} = r$ finite. Then Voloch proved in [78] that an equation

$$ax_1 + bx_2 = 1 \text{ in } (x_1, x_2) \in G$$

for given $a, b \in K^*$ has at most $p^r(p^r + p - 2)/(p - 1)$ solutions $(x_1, x_2) \in G$, unless $(a, b)^n \in G$ for some $n \geq 1$.

Voloch also conjectured that this upper bound can be replaced by one depending only on r. Our main theorem answers this conjecture positively.

Theorem 2.1.1. *Let K, G, r, a and b be as above. Suppose that there is no positive integer n with $gcd(n, p) = 1$ such that $(a, b)^n \in G$. Then the equation*

$$ax_1 + bx_2 = 1 \text{ in } (x_1, x_2) \in G \tag{2.1}$$

has at most $31 \cdot 19^{r+1}$ solutions.

Our main theorem will be a consequence of the following theorem.

Theorem 2.1.2. *Let K be a field of characteristic $p > 0$ and let G be a finitely generated subgroup of $K^* \times K^*$ of rank r. Then the equation*

$$x_1 + x_2 = 1 \text{ in } (x_1, x_2) \in G \tag{2.2}$$

has at most $31 \cdot 19^r$ solutions (x_1, x_2) satisfying $(x_1, x_2) \notin G^p$.

Clearly, the last condition is necessary to guarantee finiteness. Indeed if we have any solution to $x_1 + x_2 = 1$, then we get infinitely many solutions $x_1^{p^k} + x_2^{p^k} = 1$ for $k \in \mathbb{Z}_{\geq 0}$ due to the Frobenius operator.

The set-up of the chapter is as follows. We start by introducing the basic theory about valuations that is needed for our proofs. Then we derive Theorem 2.1.2 by generalizing the proof of Beukers and Schlickewei [3] to positive characteristic. We remark that their proof heavily relies on techniques from diophantine approximation. Most of the methods from diophantine approximation can not be transferred to positive characteristic, so that this is possible with the method of Beukers and Schlickewei is a surprising feat on its own. It was more convenient for us to follow [18], which is directly based on the proof of Beukers and Schlickewei. In the final section we shall prove that Theorem 2.1.1 is a simple consequence of Theorem 2.1.2.

2.2 Valuations and heights

Our goal in this section is to recall the basic theory about valuations and heights without proofs. To prove Theorem 2.1.2 we may assume without loss of generality that

$K = \mathbb{F}_p(G)$. Thus, K is finitely generated over $\mathbb{F}_p$. Note that Theorem 2.1.2 is trivial if K is algebraic over $\mathbb{F}_p$, so from now on we further assume that K has positive transcendence degree over $\mathbb{F}_p$. The algebraic closure of $\mathbb{F}_p$ in K is a finite field, which we denote by $\mathbb{F}_q$. Then there is an absolutely irreducible, normal projective variety V defined over $\mathbb{F}_q$ such that its function field $\mathbb{F}_q(V)$ is isomorphic to K.

Fix a projective embedding of V such that $V \subseteq \mathbb{P}^M_{\mathbb{F}_q}$ for some positive integer M. A prime divisor $\mathfrak{p}$ of V over $\mathbb{F}_q$ is by definition an irreducible subvariety of V of codimension one. Recall that for a prime divisor $\mathfrak{p}$ the local ring $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring, since V is non-singular in codimension one. Following [47] we will define heights on V. To do this, we start by defining a set of normalized discrete valuations

$$M_K := \{\mathrm{ord}_\mathfrak{p} : \mathfrak{p} \text{ prime divisor of } V\},$$

where $\mathrm{ord}_\mathfrak{p}$ is the normalized discrete valuation of K corresponding to $\mathcal{O}_\mathfrak{p}$. If $v = \mathrm{ord}_\mathfrak{p}$ is in M_K, we set $\deg v := \deg \mathfrak{p}$ with $\deg \mathfrak{p}$ being the projective degree in $\mathbb{P}^M_{\mathbb{F}_q}$. Then the set M_K satisfies the sum formula

$$\sum_{v \in M_K} v(x) \deg v = 0$$

for $x \in K^*$. This is indeed a well-defined sum, since for $x \in K^*$ there are only finitely many valuations v satisfying $v(x) \neq 0$. Furthermore, we have $v(x) = 0$ for all $v \in M_K$ if and only if $x \in \mathbb{F}_q^*$. If P is a point in $\mathbb{A}^{n+1}(K) \setminus \{0\}$ with coordinates $(y_0, \ldots, y_n)$ in K, then its homogeneous height is

$$H_K^{\mathrm{hom}}(P) = -\sum_{v \in M_K} \min_i \{v(y_i)\} \deg v$$

and its height

$$H_K(P) = H_K^{\mathrm{hom}}(1, y_0, \ldots, y_n).$$

We will need the following properties of the height.

Lemma 2.2.1. *Let $P \in \mathbb{A}^{n+1}(K) \setminus \{0\}$. The height defined above has the following properties:*
1) $H_K^{hom}(\lambda P) = H_K^{hom}(P)$ for $\lambda \in K^*$.
2) $H_K^{hom}(P) \geq 0$ with equality if and only if $P \in \mathbb{P}^n(\mathbb{F}_q)$.

2.3 Proof of Theorem 2.1.2

This section is devoted to the proof of Theorem 2.1.2. We will follow the proof in [18], see Section 6.4, with some crucial modifications to take care of the presence of the Frobenius map. The general strategy of the proof in characteristic 0, and how we adapt it to characteristic p, will be explained after Lemma 2.3.9. Let us start with a simple lemma.

Lemma 2.3.1. *The equation*

$$x_1 + x_2 = 1 \text{ in } (x_1, x_2) \in G \tag{2.3}$$

has at most p^r solutions (x_1, x_2) satisfying $x_1 \notin K^p$ and $x_2 \notin K^p$.

Proof. Let $x = (x_1, x_2)$ and $y = (y_1, y_2)$ be two solutions of (2.3). We claim that $x \equiv y \mod G^p$ implies $x = y$. Indeed, if $x \equiv y \mod G^p$, we can write $y_1 = x_1\gamma^p$ and $y_2 = x_2\delta^p$ with $(\gamma, \delta) \in G$. In matrix form this means that

$$\begin{pmatrix} 1 & 1 \\ \gamma^p & \delta^p \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

For convenience we define

$$A := \begin{pmatrix} 1 & 1 \\ \gamma^p & \delta^p \end{pmatrix}.$$

If A is invertible, we find that $x_1, x_2 \in K^p$ contrary to our assumptions. So A is not invertible, which implies that $\gamma = \delta = 1$. This proves the claim.

The claim implies that the number of solutions is at most $|G/G^p|$. Let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in K. It is a finite extension of $\mathbb{F}_p$, since K is finitely generated over $\mathbb{F}_p$. It follows that $G^{\text{tors}} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q^*$. Hence $|G^{\text{tors}}| \mid (q-1)^2$, which is co-prime to p. We conclude that $|G/G^p| = p^r$ as desired. □

Lemma 2.3.1 gives the following corollary.

Corollary 2.3.2. *The equation*

$$x_1 + x_2 = 1 \text{ in } (x_1, x_2) \in G \tag{2.4}$$

has at most p^r solutions (x_1, x_2) satisfying $(x_1, x_2) \notin G^p$.

Proof. Define

$$G' := \{(x_1, x_2) \in K \times K : (x_1^N, x_2^N) \in G \text{ for some } N \in \mathbb{Z}_{>0}\}.$$

It is a well known fact that G' is finitely generated if G and K are. It follows that G' is a finitely generated group of rank r. Our goal is to give an injective map from the solutions $(x_1, x_2) \in G$ of (2.4) satisfying $(x_1, x_2) \notin G^p$ to the solutions $(x_1', x_2') \in G'$ of (2.3) satisfying $(x_1', x_2') \notin K^p$ and then apply Lemma 2.3.1.

So let $(x_1, x_2) \in G$ be a solution of (2.4) satisfying $(x_1, x_2) \notin G^p$. We start by remarking that $x_1, x_2 \notin \mathbb{F}_q$. Hence we can repeatedly take p-th roots until we get $x_1', x_2' \notin K^p$. Using heights one can prove that this indeed stops after finitely many steps. Then it is easily verified that $(x_1', x_2') \in G'$ is a solution of (2.3) and that the map thus defined is injective. Now apply Lemma 2.3.1. □

By Corollary 2.3.2 we may assume that p is sufficiently large throughout, say $p > 7$. Both the proof in [18] and our proof rely on very special properties of the family of binary forms $\{W_N(X,Y)\}_{N\in\mathbb{Z}_{>0}}$ defined by the formula

$$W_N(X,Y) = \sum_{m=0}^{N} \binom{2N-m}{N-m}\binom{N+m}{m} X^{N-m}(-Y)^m.$$

We have for all positive integers N that $W_N(X,Y) \in \mathbb{Z}[X,Y]$. Furthermore, setting $Z = -X - Y$, the following statements hold in $\mathbb{Z}[X,Y]$.

Lemma 2.3.3. *1)* $W_N(Y,X) = (-1)^N W_N(X,Y)$.
2) $X^{2N+1}W_N(Y,Z) + Y^{2N+1}W_N(Z,X) + Z^{2N+1}W_N(X,Y) = 0$.
3) There exist a non-zero integer c_N *such that*

$$det\begin{pmatrix} Z^{2N+1}W_N(X,Y) & Y^{2N+1}W_N(Z,X) \\ Z^{2N+3}W_{N+1}(X,Y) & Y^{2N+3}W_{N+1}(Z,X)\end{pmatrix} = c_N(XYZ)^{2N+1}(X^2+XY+Y^2).$$

Proof. This is Lemma 6.4.2 in [18], which is a variant of Lemma 2.3 in [3]. □

Since the formulas in the previous lemma hold in $\mathbb{Z}[X,Y]$ they hold in every field K. But if $\mathrm{char}(K) = p > 0$ and $p \mid c_N$, then part 3) of Lemma 2.3.3 tells us that

$$det\begin{pmatrix} Z^{2N+1}W_N(X,Y) & Y^{2N+1}W_N(Z,X) \\ Z^{2N+3}W_{N+1}(X,Y) & Y^{2N+3}W_{N+1}(Z,X)\end{pmatrix} = 0$$

in $K[X,Y]$. The following remarkable identity will be handy later on, when we need that c_N does not vanish modulo p.

Lemma 2.3.4. *For every positive integer* N*, one has* $W_N(2,-1) = 4^N\binom{\frac{3}{2}N}{N}$.

Proof. It is enough to evaluate $\sum_{i=0}^{N}\binom{2N-i}{N}\binom{N+i}{N}2^{-i}$. We have

$$\sum_{i=0}^{N}\binom{2N-i}{N}\binom{N+i}{N}2^{-i} = \binom{2N}{N}F\left(-N, N+1, -2N, \frac{1}{2}\right),$$

where $F(a,b,c,z)$ is the hypergeometric function defined by the power series

$$F(a,b,c,z) := \sum_{i=0}^{\infty}\frac{(a)_i(b)_i}{i!(c)_i}z^n.$$

Here we define for a real t and a non-negative integer i $(t)_i = 1$ if $i = 0$ and for i positive $(t)_i = t(t+1)\cdot\ldots\cdot(t+i-1)$. Now the desired result follows from Bailey's formulas where special values of the function F are expressed in terms of values of the Γ-function, see [48] page 297. □

We obtain the following corollary.

Corollary 2.3.5. *Let p be an odd prime number and let N be a positive integer with $N < \frac{p}{3} - 2$. Then $c_N \not\equiv 0 \bmod p$.*

Proof. Indeed one has that

$$det \begin{pmatrix} Z^{2N+1}W_N(X,Y) & Y^{2N+1}W_N(Z,X) \\ Z^{2N+3}W_{N+1}(X,Y) & Y^{2N+3}W_{N+1}(Z,X) \end{pmatrix}$$

evaluated at $(X,Y,Z) = (2,-1,-1)$ gives up to sign $2W_N(2,-1)W_{N+1}(2,-1)$. By the previous proposition, this is a power of 2 times the product of two binomial coefficients whose top terms are less than p, hence it can not be divisible by p. □

We now state and prove the analogues of Lemmata 6.4.3-6.4.5 from [18] for function fields of positive characteristic. These are variants of respectively Lemma 2.1, Corollary 2.2 and Lemma 2.3 from [3].

Lemma 2.3.6. *Let a,b,c be non-zero elements of K, and let $(\alpha_i,\beta_i,\gamma_i)$ for $i=1,2$ be two K-linearly independent vectors from K^3 such that $a\alpha_i + b\beta_i + c\gamma_i = 0$ for $i=1,2$. Then*

$$H_K^{hom}(a,b,c) \leq H_K^{hom}(\alpha_1,\beta_1,\gamma_1) + H_K^{hom}(\alpha_2,\beta_2,\gamma_2).$$

Proof. The vector (a,b,c) is K-proportional to the vector with coordinates given by $(\beta_1\gamma_2 - \gamma_1\beta_2, \gamma_1\alpha_2 - \alpha_1\gamma_2, \alpha_1\beta_2 - \beta_1\alpha_2)$. So we have

$$\begin{aligned} H_K^{\hom}(a,b,c) &= H_K^{\hom}(\beta_1\gamma_2 - \gamma_1\beta_2, \gamma_1\alpha_2 - \alpha_1\gamma_2, \alpha_1\beta_2 - \beta_1\alpha_2) \\ &= \sum_{v\in M_K} -\min(v(\beta_1\gamma_2 - \gamma_1\beta_2), v(\gamma_1\alpha_2 - \alpha_1\gamma_2), v(\alpha_1\beta_2 - \beta_1\alpha_2)) \deg v \\ &\leq \sum_{v\in M_K} (-\min(v(\beta_1), v(\gamma_1), v(\alpha_1)) - \min(v(\gamma_2), v(\alpha_2), v(\beta_2))) \deg v \\ &= H_K^{\hom}(\alpha_1,\beta_1,\gamma_1) + H_K^{\hom}(\alpha_2,\beta_2,\gamma_2), \end{aligned}$$

which was the claimed inequality. □

We apply Lemma 2.3.6 to the equation $x_1 + x_2 = 1$.

Lemma 2.3.7. *Suppose $x = (x_1,x_2) \in G$ and $y = (y_1,y_2) \in G$ satisfy $x_1 + x_2 = 1$ and $y_1 + y_2 = 1$. Then we have $H_K(x) \leq H_K(yx^{-1})$.*

Proof. Apply Lemma 2.3.6 with $(a,b,c) = (x_1,x_2,-1)$, $(\alpha_1,\beta_1,\gamma_1) = (1,1,1)$ and $(\alpha_2,\beta_2,\gamma_2) = (y_1x_1^{-1}, y_2x_2^{-1}, 1)$. Finally use the fact that $H_K^{\hom}(1,1,1) = 0$. □

The next Lemma takes advantage of the properties of $W_N(X,Y)$ listed in Lemma 2.3.3 and the non-vanishing of c_N modulo p obtained in Corollary 2.3.5.

Lemma 2.3.8. *Let x,y be as in Lemma 2.3.7. Let $N < \frac{p}{3} - 2$. Then there exists $M \in \{N, N+1\}$ such that $H_K(x) \leq \frac{1}{M+1} H_K(yx^{-2M-1})$.*

Proof. The proof is almost the same as in Lemma 6.4.5 in [18], with only few necessary modifications. For completeness we give the full proof.

If x_1, and thus both x_1 and x_2 are roots of unity, we have that $H_K(x) = 0$ so the lemma is trivially true. By Lemma 2.3.3 part 2) we get that

$$x_1^{2M+1} W_M(x_2, -1) + x_2^{2M+1} W_M(-1, x_1) - W_M(x_1, x_2) = 0$$

for $M \in \{N, N+1\}$ as well as

$$x_1^{2M+1}(y_1 x_1^{-2M-1}) + x_2^{2M+1}(y_2 x_2^{-2M-1}) - 1 = 0.$$

Now we claim that there is $M \in \{N, N+1\}$ such that the vectors

$$(y_1, y_2, -1) \text{ and } ({x_1}^{2M+1} W_M(x_2, -1), {x_2}^{2M+1} W_M(-1, x_1), -W_M(x_1, x_2)) \tag{2.5}$$

are linearly independent. Clearly, to prove the claim it is enough to prove that the two vectors

$$(x_1^{2M+1} W_M(x_2, -1), x_2^{2M+1} W_M(-1, x_1), -W_M(x_1, x_2)) \quad (M \in \{N, N+1\}) \tag{2.6}$$

are linearly independent. But we know that for $M \in \{N, N+1\}$ we have $c_M \not\equiv 0 \bmod p$ by Corollary 2.3.5 and the assumption that $N < \frac{p}{3} - 2$. Furthermore, x_1 and x_2 are not algebraic over $\mathbb{F}_p$. Thus the identity Lemma 2.3.3 part 3) gives us the non-vanishing of the first 2×2 minor of the vectors in 2.6, which proves the claimed independence. So by applying to (2.5) the diagonal transformation that divides the first coordinate by x_1^{2M+1} and the second by x_2^{2M+1}, we deduce that the two vectors

$$(y_1 x_1^{-2M-1}, y_2 x_2^{-2M-1}, -1)$$

and

$$(W_M(x_2, -1), W_M(-1, x_1), -W_M(x_1, x_2)) =: (w_1, w_2, w_3)$$

are linearly independent. So by Lemma 2.3.6 we get that

$$(2M+1) H_K(x) \leq H_K(y x^{-2M-1}) + H_K^{\hom}(w_1, w_2, w_3)$$

But now the inequality

$$H_K^{\hom}(w_1, w_2, w_3) \leq M \cdot H_K(x)$$

follows immediately from the non-archimedean triangle inequality. So we indeed get

$$(M+1) H_K(x) \leq H_K(y x^{-2M-1}),$$

completing the proof. □

Define

$$\mathrm{Sol}(G) := \{(x_1, x_2) \in G \setminus G^{\mathrm{tors}} : x_1 + x_2 = 1\}$$

and

$$\text{Prim-Sol}(G) := \{(x_1, x_2) \in G \setminus G^p : x_1 + x_2 = 1\}.$$

It is easily seen that Prim-Sol$(G) \subseteq$ Sol(G). Finally define

$$S := \{v \in M_K : \text{ there is } (x_1, x_2) \in G \text{ with } v(x_1) \neq 0 \text{ or } v(x_2) \neq 0\}.$$

The set S is clearly finite. Write $s := |S|$, $S = \{v_1, \ldots, v_s\}$. Then we have a homomorphism $\varphi : G \to \mathbb{Z}^s \times \mathbb{Z}^s \subseteq \mathbb{R}^s \times \mathbb{R}^s$ defined by sending $(g_1, g_2) \in G$ to

$$(v_1(g_1) \deg v_1, \ldots, v_s(g_1) \deg v_s, v_1(g_2) \deg v_1, \ldots, v_s(g_2) \deg v_s).$$

Note that $\varphi(G)$ is a subgroup of $\mathbb{Z}^s \times \mathbb{Z}^s$ of rank r.

Let $u, v \in$ Sol(G) be such that $\varphi(u) = \varphi(v)$. Suppose that $u \neq v$. Then Lemma 2.3.7 implies that $H_K(u) \leq 0$. Hence by Lemma 2.2.1 part 2) it follows that u and thus v are in G^{tors}. This implies that the restriction of φ to Sol(G) is injective. In particular the restriction of φ to Prim-Sol(G) is injective. We now call $\mathcal{S} := \varphi(\text{Sol}(G))$ and $\mathcal{PS} := \varphi(\text{Prim-Sol}(G))$. To prove Theorem 2.1.2 it suffices to bound the cardinality of $\mathcal{PS}$.

Let $||\cdot||$ be the norm on $\mathbb{R}^s \times \mathbb{R}^s$ that is the average of the $||\cdot||_1$ norms on $\mathbb{R}^s$. More precisely, we define for $u = (u_1, u_2) \in \mathbb{R}^s \times \mathbb{R}^s$

$$||u|| = \frac{1}{2}(||u_1|| + ||u_2||).$$

We now state the most important properties of $\mathcal{S}$.

Lemma 2.3.9. *The set $\mathcal{S} \subseteq \mathbb{Z}^s \times \mathbb{Z}^s$ has the following properties:*
1) For any two distinct $u, v \in \mathcal{S}$, we have that $||u|| \leq 2||v - u||$.
2) For any two distinct $u, v \in \mathcal{S}$ and any positive integer N such that $N < \frac{p}{3} - 2$, there is $M \in \{N, N+1\}$ such that $||u|| \leq \frac{2}{M+1}||v - (2M+1)u||$.
3) $p\mathcal{S} \subseteq \mathcal{S}$.

Proof. Let $x = (x_1, x_2) \in G$. By construction we have

$$||\varphi(x)|| = H_K^{\text{hom}}(1, x_1) + H_K^{\text{hom}}(1, x_2).$$

Note the basic inequalities

$$H_K^{\text{hom}}(x_1, x_2) \leq H_K^{\text{hom}}(1, x_1) + H_K^{\text{hom}}(1, x_2) \leq 2H_K^{\text{hom}}(x_1, x_2).$$

It is now clear that Lemma 2.3.7 implies part 1) and Lemma 2.3.8 implies part 2). Finally, part 3) is due to the action of the Frobenius operator. □

Denote by V the real span of $\varphi(G)$. Then V is an r-dimensional vector space over $\mathbb{R}$. We will keep writing $||\cdot||$ for the restriction of $||\cdot||$ to V.

Recall that our goal is to bound $|\mathcal{PS}|$. We sketch the ideas behind our strategy here. Let us first describe the strategy in characteristic 0 as used in [3] and [18]. In their work the set $\mathcal{S}$ satisfies part 1) of Lemma 2.3.9 and part 2) of Lemma 2.3.9 without the condition $N < \frac{p}{3} - 2$.

To finish the proof, they subdivide the vector space V in B^r cones for some absolute constant B. In each cone one can use part 1) of Lemma 2.3.9 to show that two distinct points $u, v \in \mathcal{S}$ are not too close. But part 2) of Lemma 2.3.9 shows that inside the same cone two points $u, v \in \mathcal{S}$ can not be too far apart. Together with a lower bound for the height of $u, v \in \mathcal{S}$, this proves that there are at most finitely many points $u \in \mathcal{S}$, say A, in each cone. Hence we get an upper bound of the shape $A \cdot B^r$.

Now we describe how to modify this to characteristic p. Again we subdivide V in B^r cones for some absolute constant B. From now on we only consider points $u \in \mathcal{PS}$ inside a fixed cone C. Our goal is to show that there are at most A points $u \in \mathcal{PS} \cap C$, where A is an absolute constant. It follows that then all points $v \in \mathcal{S} \cap C$ are of the shape $v = p^k u$ for $u \in \mathcal{PS}$ and $k \in \mathbb{Z}_{\geq 0}$.

Part 1) of Lemma 2.3.9 tells us that two distinct points $u, v \in \mathcal{PS}$ are not too close. Using part 3) of Lemma 2.3.9 we can multiply two points $u, v \in \mathcal{PS}$ with a power of p in such a way that the then obtained $u', v' \in \mathcal{S}$ satisfy $1 \leq \frac{||u'||}{||v'||} \leq \sqrt{p}$. Then we are in the position to apply part 2) of Lemma 2.3.9, which shows that $||u'||$ and $||v'||$ are not too far apart. This allows us to deduce that $\mathcal{PS} \cap C$ contains at most A points.

The following lemma subdivides the vector space V in B^r cones for some absolute constant B.

Lemma 2.3.10. *Given a real number $\theta > 0$, one can find a set $\mathcal{E} \subseteq \{u \in V : ||u|| = 1\}$ satisfying*
1) $|\mathcal{E}| \leq (1 + \frac{2}{\theta})^r$,
2) for all $0 \neq u \in V$ there exists $e \in \mathcal{E}$ satisfying $||\frac{u}{||u||} - e|| \leq \theta$.

Proof. See Lemma 6.3.4 in [18], which is an improvement of Corollary 3.8 in [3]. □

Let $\theta \in (0, \frac{1}{9})$ be a parameter and fix a corresponding choice of a set $\mathcal{E}$ satisfying the above properties. Given $e \in \mathcal{E}$, we define the cone

$$\mathcal{S}_e := \left\{ u \in \mathcal{S} : \left|\left| \frac{u}{||u||} - e \right|\right| \leq \theta \right\}, \ \mathcal{PS}_e := \mathcal{S}_e \cap \mathcal{PS}.$$

Fix $e \in \mathcal{E}$. We proceed to bound $|\mathcal{PS}_e|$. We start by deducing a so-called gap principle from part 1) of Lemma 2.3.9.

Lemma 2.3.11. *Let u_1, u_2 be distinct elements of $\mathcal{S}_e$, with $||u_2|| \geq ||u_1||$. Then $||u_2|| \geq \frac{3-\theta}{2+\theta}||u_1||$.*

Proof. Write $\lambda_i := ||u_i||$ for $i = 1, 2$. Then we have $u_i = \lambda_i e + u_i'$ where $||u_i'|| \leq \theta\lambda_i$, by definition of $\mathcal{S}_e$. Part 1) of Lemma 2.3.9 gives

$$\lambda_1 \leq 2||(\lambda_2 - \lambda_1)e + (u_2' - u_1')|| \leq 2(\lambda_2 - \lambda_1) + \theta(\lambda_2 + \lambda_1),$$

and after dividing by λ_1 we get that

$$1 \leq 2\left(\frac{\lambda_2}{\lambda_1} - 1\right) + \theta\left(\frac{\lambda_2}{\lambda_1} + 1\right).$$

This can be rewritten as $\frac{3-\theta}{2+\theta} \leq \frac{\lambda_2}{\lambda_1}$. □

From part 2) of Lemma 2.3.9 we can deduce the following crucial Lemma.

Lemma 2.3.12. *Let u_1, u_2 be distinct elements of $\mathcal{S}_e$. Suppose that $\frac{||u_2||}{||u_1||} < \frac{2}{3}p - 3$. Then $\frac{||u_2||}{||u_1||} \leq \frac{10}{\theta}$.*

Proof. We follow the proof of Lemma 6.4.9 of [18] part (ii) with a few modifications. For completeness we write out the full proof.

Again define $\lambda_i = ||u_i||$ and $u_i' = u_i - \lambda_i e$, for $i = 1, 2$. Assume that $\lambda_2 \geq \frac{10}{\theta}\lambda_1$. Let N be the positive integer with $2N + 1 \leq \frac{\lambda_2}{\lambda_1} < 2N + 3$. Then $2N + 1 < \frac{2}{3}p - 3$ and hence $N < \frac{p}{3} - 2$. Applying part 2) of Lemma 2.3.9 gives an integer $M \in \{N, N+1\}$ satisfying

$$\lambda_1 \leq \frac{2}{M+1}||(\lambda_2 - (2M+1)\lambda_1)e + u_2' - (2M+1)u_1'||.$$

Furthermore, we have that

$$|\lambda_2 - (2M+1)\lambda_1| \leq 2\lambda_1$$

and $M > \frac{4}{\theta}$ from the assumption $\lambda_2 \geq \frac{10}{\theta}\lambda_1$. Hence

$$\begin{aligned}
\lambda_1 &\leq \frac{2}{M+1}||(\lambda_2 - (2M+1)\lambda_1)e + u_2' - (2M+1)u_1'|| \\
&\leq \frac{2}{M+1}(2\lambda_1 + \lambda_2\theta + (2M+1)\lambda_1\theta) \\
&\leq \frac{2}{M+1}(2 + (4M+4)\theta)\lambda_1 = \left(\frac{4}{M+1} + 8\theta\right)\lambda_1 < 9\theta\lambda_1.
\end{aligned}$$

It follows that $\lambda_1 < \frac{1}{1-9\theta}$. Now observe that for any non-negative integer h the elements $p^h u_1, p^h u_2$ of $\mathcal{S}_e$ satisfy all the assumptions made so far. We conclude that also $p^h\lambda_1 < \frac{1}{1-9\theta}$ for every non-negative integer h, which implies that $||u_1|| = 0$. This contradicts the fact that $u_1 \in \mathcal{S}_e$, completing the proof. □

Remark 2.3.13. In characteristic 0, the analogue of Lemma 2.3.12 holds only when both u_1, u_2 have norms at least $\frac{1}{1-9\theta}$. Then one deals with the remaining points in $\mathcal{S}_e$ by using the analogue of part 1) of Lemma 2.3.9, together with a separate argument to deal with the "very small" solutions. In characteristic p, it is because of the additional tool given by the action of Frobenius that the condition that u_1, u_2 have norm at least $\frac{1}{1-9\theta}$ has disappeared.

Assume without loss of generality that $\mathcal{PS}_e$ is not empty, and fix a choice of $u_0 \in \mathcal{PS}_e$ with $||u_0||$ minimal. For any $u \in \mathcal{PS}_e$, denote by $k(u)$ the smallest non-negative integer such that $\frac{||u||}{p^{k(u)}||u_0||} < p$ and denote $\lambda(u) := \frac{||u||}{p^{k(u)}||u_0||}$.

We define $\mathcal{PS}_e(1) := \{u \in \mathcal{PS}_e : \lambda(u) \leq \sqrt{p}\}$ and $\mathcal{PS}_e(2) := \{u \in \mathcal{PS}_e : \lambda(u) > \sqrt{p}\}$. Since we may assume $p > 7$ by Corollary 2.3.2, we have $\frac{2p}{3} - 3 > \sqrt{p}$.

Lemma 2.3.14. *1) Let $i \in \{1,2\}$ and let u_1, u_2 be distinct elements of $\mathcal{PS}_e(i)$ with $\lambda(u_2) \geq \lambda(u_1)$. Then $\lambda(u_2) \geq \frac{3-\theta}{2+\theta}\lambda(u_1)$ and $\lambda(u_2) \leq \frac{10}{\theta}\lambda(u_1)$.*
2) $\lambda(\mathcal{PS}_e(2)) \subseteq [\frac{\theta p}{10}, p)$.
3) λ is an injective map on $\mathcal{PS}_e$.

Proof. 1) If $k(u_2) \geq k(u_1)$, we put $u_1' := p^{k(u_2)-k(u_1)}u_1$, $u_2' := u_2$, and if instead $k(u_2) < k_(u_1)$, we put $u_1' := u_1$, $u_2' := p^{k(u_1)-k(u_2)}u_2$. Now apply Lemma 14 and Lemma 15 to u_1', u_2'. We stress that u_1', u_2' are distinct elements of $\mathcal{S}_e$, since u_1, u_2 are distinct elements of $\mathcal{PS}_e(i)$.
2) This follows from Lemma 2.3.12 applied to the pair $(u_1, p^{k(u_1)+1}u_0)$ for each u_1 in $\mathcal{PS}_e(2)$.
3) Use part 1) and the fact that $\frac{3-\theta}{2+\theta} > 1$ for $\theta \in (0, \frac{1}{9})$. □

Proof of Theorem 2.1.2. By part 3) of Lemma 2.3.14 it suffices to bound $|\lambda(\mathcal{PS}_e)|$. By part 1) and 2) of Lemma 2.3.14 it will follow that we can bound $|\lambda(\mathcal{PS}_e)|$ purely in terms of θ: thus collecting all the bounds for e varying in $\mathcal{E}$ we obtain a bound depending only on r. We now give all the details.

For any $\theta \in (0, \frac{1}{9})$ we have

$$\frac{3-\theta}{2+\theta} > \frac{26}{19}.$$

Then we find that $|\lambda(\mathcal{PS}_e(1))|$ is at most the biggest n such that

$$\left(\frac{26}{19}\right)^{n-1} \leq \frac{10}{\theta}$$

and similarly for $|\lambda(\mathcal{PS}_e(2))|$. We conclude that

$$|\mathcal{PS}_e| \leq 2 + 2\frac{\log(\frac{10}{\theta})}{\log(\frac{26}{19})}.$$

Multiplying by $|\mathcal{E}|$ gives that for every $\theta \in (0, \frac{1}{9})$

$$|\mathcal{PS}| \leq 2\left(1 + \frac{\log(\frac{10}{\theta})}{\log(\frac{26}{19})}\right)\left(1 + \frac{2}{\theta}\right)^r.$$

So letting θ increase to $\frac{1}{9}$ we obtain

$$|\mathcal{PS}| \leq 2\left(1 + \frac{\log(90)}{\log(\frac{26}{19})}\right)19^r < 31 \cdot 19^r.$$

This completes the proof of Theorem 2.1.2. □

2.4 Proof of Theorem 2.1.1

First suppose that G and K are finitely generated. Before we can start with the proof of Theorem 2.1.1, we will rephrase Theorem 2.1.2. Recall that we write $\mathbb{F}_q$ for the algebraic closure of $\mathbb{F}_p$ in K.

Then Theorem 2.1.2 implies that there is a finite subset T of G with $|T| \leq 31 \cdot 19^r$ such that any solution of

$$x_1 + x_2 = 1, (x_1, x_2) \in G$$

with $x_1 \notin \mathbb{F}_q$ and $x_2 \notin \mathbb{F}_q$ satisfies $(x_1, x_2) = (\gamma, \delta)^{p^t}$ for some $t \in \mathbb{Z}_{\geq 0}$ and $(\gamma, \delta) \in T$.

Now let $(x_1, x_2) \in G$ be a solution to

$$ax_1 + bx_2 = 1.$$

If $ax_1 \in \mathbb{F}_q$ or $bx_2 \in \mathbb{F}_q$, it follows that both $ax_1 \in \mathbb{F}_q$ and $bx_2 \in \mathbb{F}_q$, which implies that $(a, b)^{q-1} \in G$. This contradicts the condition on (a, b) in Theorem 2.1.1.

Hence $ax_1 \notin \mathbb{F}_q$ and $bx_2 \notin \mathbb{F}_q$. Define G' to be the group generated by G and the tuple (a, b). Then the rank of G' is at most $r+1$. Let $T \subseteq G'$ be as above, so $|T| \leq 31 \cdot 19^{r+1}$. We can write

$$(ax_1, bx_2) = (\gamma, \delta)^{p^t}$$

with $t \in \mathbb{Z}_{\geq 0}$ and $(\gamma, \delta) \in T$. Since $T \subseteq G'$, we can write

$$(\gamma, \delta) = (a^k y_1, b^k y_2)$$

with $k \in \mathbb{Z}$ and $(y_1, y_2) \in G$. This means that

$$(ax_1, bx_2) = (a^k y_1, b^k y_2)^{p^t},$$

which implies $(a, b)^{kp^t - 1} \in G$. If $kp^t - 1$ is co-prime to p, we have a contradiction with the condition on (a, b) in Theorem 2.1.1. But p can only divide $kp^t - 1$ if $t = 0$. Then we find immediately that there are at most $|T| \leq 31 \cdot 19^{r+1}$ solutions as desired.

We still need to deal with the case that K is an arbitrary field of characteristic p and G is a subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q} = r$ finite. Suppose that $ax_1 + bx_2 = 1$ has more than $31 \cdot 19^{r+1}$ solutions $(x_1, x_2) \in G$. Then we can replace G by a finitely generated subgroup of G with the same property. We can also replace K by a subfield, finitely generated over its prime field, containing the coordinates of the new G and a, b. This gives the desired contradiction.

2.5 Acknowledgements

We are grateful to Julian Lyczak for explaining us how identities as in Lemma 2.3.4 follow from basic properties of hypergeometric functions. Many thanks go to Jan-Hendrik Evertse for providing us with this nice problem, his help throughout and the proofreading.

Addendum

Joint work with Carlo Pagano

On the 22nd October of 2018 Professor Felipe Voloch brought to our attention the unpublished master thesis of Yi-Chih Chiu, written under the supervision of Professor Ki-Seng Tan. In this work, Chiu establishes a special case of our main theorems [44, Theorem 1.1, Theorem 1.2]. We shall begin by explaining his result, and we will next compare it to our result.

Let p be a prime number. For a field extension K of $\mathbb{F}_p$ with transcendence degree equal to 1, we let k be the algebraic closure of $\mathbb{F}_p$ in K. Denote by Ω_K the set of valuations of K. Let S be a finite subset of Ω_K and fix $\alpha, \beta \in K^*$. The following theorem is proven in Chiu's master thesis.

Theorem 2.5.1. *The S-unit equation to be solved in $x, y \in \mathcal{O}_S^*$*

$$\alpha x + \beta y = 1,$$

has at most $3 \cdot 7^{2|S|-2}$ pairwise inequivalent non-trivial solutions if $\alpha, \beta \in \mathcal{O}_S^*$. If instead α, β are not both in $\mathcal{O}_S^*$, then it has at most $39 \cdot 7^{2|S|-2}$ non-trivial solutions.

Here a solution (x, y) is called trivial if $\frac{\alpha x}{\beta y} \in k$. Two solutions $(x_1, y_1), (x_2, y_2)$ are said to be equivalent if there exists $n \in \mathbb{Z}_{\geq 0}$ with

$$(\alpha x_1)^{p^n} = \alpha x_2, (\beta y_1)^{p^n} = \beta y_2 \quad \text{or} \quad (\alpha x_2)^{p^n} = \alpha x_1, (\beta y_2)^{p^n} = \beta y_1.$$

This result is a special case with slightly better constants of our theorems that we state now for the reader's convenience, see [44, Theorem 1.1, Theorem 1.2].

Theorem 2.5.2. *Let K be a field of characteristic $p > 0$. Take $\alpha, \beta \in K^*$ and let G be a finitely generated subgroup of $K^* \times K^*$ of rank $r := \dim_{\mathbb{Q}} G \otimes \mathbb{Q}$. Then the equation*

$$\alpha x + \beta y = 1,$$

to be solved in $(x, y) \in G$, has at most $31 \cdot 19^r$ pairwise inequivalent non-trivial solutions if $(\alpha, \beta)^n \in G$ for some $n > 0$. If instead $(\alpha, \beta)^n \notin G$ for all $n > 0$, then it has at most $31 \cdot 19^{r+1}$ non-trivial solutions.

Note that Theorem 2.5.2 applies to *any* finitely generated subgroup in *any* field of characteristic p. In contrast, Chiu's theorem applies only to the case of S-units of fields

of transcendence degree 1 (with some care Chiu's theorem can be extended to S-units of function fields of projective varieties).

The reason for this difference in generality comes from the fact that Chiu's work is an adaptation of Evertse's work [17] to characteristic p. Our work is instead an adaptation of the work of Beukers and Schlickewei [3] to characteristic p. In both works [3, 17], there is a key use of a certain set of identities coming from hypergeometric functions, see [44, Lemma 3.3, Lemma 3.4]. In characteristic p these identities can be used only in a limited range, see [9, Proposition 2] and [44, Corollary 3.5] respectively.

Correspondingly, the solutions to the unit equations need to be counted only up to equivalence. One of the most important steps is to use this equivalence relation in such a way that one is inside this limited range. It is this step that allows one to obtain an upper bound that is independent of p. The reader can find this step in the two papers respectively at [9, Lemma 4] and at [44, Lemma 3.9].