Diophantine equations in positive characteristic

Koymans, P.H.

Chapter 3

Unit equations and Fermat surfaces in positive characteristic

Joint work with Carlo Pagano

Abstract

In this article we study the three-variable unit equation $x + y + z = 1$ to be solved in $x, y, z \in \mathcal{O}_S^*$, where $\mathcal{O}_S^*$ is the S-unit group of some global function field. We give upper bounds for the height of solutions and the number of solutions. We also apply these techniques to study the Fermat surface $x^N + y^N + z^N = 1$.

3.1 Introduction

Let K be a finitely generated field over $\mathbb{F}_p$ of transcendence degree 1. Denote by $\mathbb{F}_q$ the algebraic closure of $\mathbb{F}_p$ inside K, which is a finite extension of $\mathbb{F}_p$. Let M_K be the set of places of K and let $S \subseteq M_K$ be a finite subset. To avoid degenerate cases, we will assume that $|S| \geq 2$ throughout the chapter. We define $\omega(S) = \sum_{v \in S} \deg(v)$ and we let H_K be the usual height. For a precise definition of $\deg(v)$ and H_K we refer the reader to Section 3.2. Mason [54] and Silverman [67] independently considered the equation

$$x + y = 1 \text{ in } x, y \in \mathcal{O}_S^*. \tag{3.1}$$

If $x, y \notin K^p$ is a solution to (3.1), they showed that

$$H_K(x) = H_K(y) \leq \omega(S) + 2g - 2, \tag{3.2}$$

where g is the genus of K. Previously, Stothers [72] proved (3.2) for polynomials $x, y \in \mathbb{C}[t]$.

It is important to note that the condition $x, y \notin K^p$ can not be removed. Indeed if we have a solution to (3.1), then we find that

$$x^{p^k} + y^{p^k} = 1$$

is also a solution to (3.1) for all integers $k \geq 0$ due to Frobenius, but the heights $H_K(x^{p^k})$ and $H_K(y^{p^k})$ become arbitrarily large. This new phenomenon is the main difficulty in dealing with two variable unit equations in positive characteristic.

The work of Mason and Silverman has been extended in various directions. Hsia and Wang [36] looked at the equation

$$x_1 + \cdots + x_n = 1 \text{ in } x_1, \ldots, x_n \in \mathcal{O}_S^*. \tag{3.3}$$

They were able to deduce a height bound similar to (3.2) under the condition that $x_1, \ldots, x_n$ are linearly independent over K^p. In particular it follows that under the same condition there are only finitely many solutions $x_1, \ldots, x_n$. Derksen and Masser [16] considered (3.3) without the restriction that $x_1, \ldots, x_n$ are linearly independent over K^p. In this case it is not a priori clear what the structure of the solution set should be, but Derksen and Masser give a completely explicit description that we repeat here in the special case that $n = 3$.

They define so-called one dimensional Frobenius families to be

$$\mathcal{F}(\mathbf{u}) := \{(u_1, u_2, u_3)^{p^e} : e \geq 0\}$$

for $\mathbf{u} = (u_1, u_2, u_3) \in (K^*)^3$ and two dimensional Frobenius families

$$\mathcal{F}_a(\mathbf{u}, \mathbf{v}) := \left\{ \left((u_1, u_2, u_3)(v_1, v_2, v_3)^{p^{af}} \right)^{p^e} : e, f \geq 0 \right\}$$

for $a \in \mathbb{Z}_{\geq 1}$, $\mathbf{u} = (u_1, u_2, u_3) \in (K^*)^3$, $\mathbf{v} = (v_1, v_2, v_3) \in (K^*)^3$, where all multiplications of tuples are taken coordinate-wise. Then Derksen and Masser prove that the solution set of

$$x + y + z = 1 \text{ in } x, y, z \in \mathcal{O}_S^* \tag{3.4}$$

is equal to a finite union of one dimensional and two dimensional Frobenius families. On top of that Derksen and Masser give effective height bounds for $\mathbf{u}$ and $\mathbf{v}$, which can be seen as another direct generalization of (3.2). In principle this also gives an upper bound on the total number of Frobenius families that one may need to describe the solution set of (3.4), but the resulting bounds are far from optimal. Leitner [49] computed the full solution set of (3.4) in the special case $S = \{0, 1, \infty\}$ and $K = \mathbb{F}_p(t)$.

In this chapter we give explicit upper bounds for the height of $\mathbf{u}$ and $\mathbf{v}$ in the case $n = 3$. Together with a "gap principle" we will use this to give an upper bound on the number of Frobenius families. For the two variable unit equation $x + y = 1$ such upper bounds have already been established by Voloch [78] and by Koymans and Pagano [44] using different methods than in this chapter. The upper bound in the latter paper has the

particularly pleasant feature that it does not depend on p. This chapter is based on the paper of Beukers and Schlickewei [3], who had previously established a finiteness result for the two variable unit equation in characteristic 0.

Let g and γ be respectively the genus and the gonality of K. Put

$$c_{K,S} := 2\omega(S) + 4g - 4 + 4\gamma,\ c'_{K,S} := 2c_{K,S} \cdot (\omega(S) + 4c_{K,S} + 2g - 2) + 3c_{K,S}.$$

Define the following three sets

$$\begin{aligned}
A := \{\mathbf{x} = (x,y,z) \in (\mathcal{O}_S^*)^3 : x+y+z = 1, x, y, z \notin \mathbb{F}_q^*, H_K(x), H_K(y), H_K(z) \leq c'_{K,S}\},\\
B_p := \{(\mathbf{u},\mathbf{v}) \in (\mathcal{O}_S^*)^3 \times (\mathcal{O}_S^*)^3 :& \mathbf{u},\mathbf{v} \notin (\mathbb{F}_q^*)^3, (u_i,v_i) \notin \mathbb{F}_q^* \times \mathbb{F}_q^* \text{ for } i = 1,2,3,\\
& H_K(u_i) \leq c_{K,S} \text{ for } i = 1,2,3,\\
& H_K(v_i) \leq \omega(S) + 2g - 2 \text{ for } i = 1,2,3,\\
& u_1 v_1^{p^f} + u_2 v_2^{p^f} + u_3 v_3^{p^f} = 1 \text{ for all } f \in \mathbb{Z}_{\geq 0}\},\\
B_q := \{(\mathbf{u},\mathbf{v}) \in (\mathcal{O}_S^*)^3 \times (\mathcal{O}_S^*)^3 :& \mathbf{u},\mathbf{v} \notin (\mathbb{F}_q^*)^3, (u_i,v_i) \notin \mathbb{F}_q^* \times \mathbb{F}_q^* \text{ for } i = 1,2,3,\\
& H_K(u_i) \leq c_{K,S}, \text{ for } i = 1,2,3,\\
& H_K(v_i) \leq \frac{q}{p}(\omega(S) + 2g - 2), \text{ for } i = 1,2,3,\\
& u_1 v_1^{q^f} + u_2 v_2^{q^f} + u_3 v_3^{q^f} = 1 \text{ for all } f \in \mathbb{Z}_{\geq 0}\}.
\end{aligned}$$

Theorem 3.1.1. *For all $x, y, z \notin \mathbb{F}_q$ we have the following equivalence: x, y, z is a solution to (3.4) if and only if (x, y, z) is an element of one of the following three sets*

$$\bigcup_{\mathbf{x} \in A} \mathcal{F}(\mathbf{x}), \quad \bigcup_{(\mathbf{u},\mathbf{v}) \in B_p} \mathcal{F}_1(\mathbf{u},\mathbf{v}), \quad \bigcup_{(\mathbf{u},\mathbf{v}) \in B_q} \mathcal{F}_{\log_p(q)}(\mathbf{u},\mathbf{v}). \tag{3.5}$$

The novel feature of Theorem 3.1.1 is the excellent quality of the height bounds appearing in the definition of A, B_p and B_q. Because we are only dealing with the three variable unit equation, the descent step of Derksen and Masser becomes completely explicit. We make full use of this to improve on the height bounds obtained by Derksen and Masser.

We have the identity

$$\mathcal{F}_1(\mathbf{u},\mathbf{v}) = \bigcup_{x=0}^{\log_p(q)-1} \mathcal{F}_{\log_p(q)}\left(\mathbf{u}, \mathbf{v}^{p^x}\right).$$

This allows us to remove the sets

$$\bigcup_{(\mathbf{u},\mathbf{v}) \in B_p} \mathcal{F}_1(\mathbf{u},\mathbf{v})$$

from Theorem 3.1.1 if desired. We have decided to state Theorem 3.1.1 in its current shape because the sets $\mathcal{F}_1(\mathbf{u},\mathbf{v})$ naturally show up in the proof. Furthermore, it enables us to be more precise in our next theorem.

Theorem 3.1.2. *There are a subset C_1 of $(K^*)^3$ and subsets C_2 and C_3 of $(K^*)^3 \times (K^*)^3$ with the following properties*

- $|C_1| \leq 279 \cdot q^2 \cdot (\log_{\frac{5}{4}}(3c'_{K,S}) + 1)^2 \cdot (15 \cdot 10^6)^{|S|}$;
- $|C_2| \leq 2883 \cdot p^4 \cdot 19^{4|S|}$;
- $|C_3| \leq 2883 \cdot \log_p(q) \cdot q^4 \cdot 19^{4|S|}$;
- *for all $x, y, z \notin \mathbb{F}_q$ we have the following equivalence: x, y, z is a solution to (3.4) if and only if (x, y, z) is an element of one of the following three sets*

$$\bigcup_{\mathbf{x} \in C_1} \mathcal{F}(\mathbf{x}), \quad \bigcup_{(\mathbf{u},\mathbf{v}) \in C_2} \mathcal{F}_1(\mathbf{u}, \mathbf{v}), \quad \bigcup_{(\mathbf{u},\mathbf{v}) \in C_3} \mathcal{F}_{\log_p(q)}(\mathbf{u}, \mathbf{v}).$$

The work of Derksen and Masser quickly implies that there are finite subsets C_1, C_2 and C_3 satisfying the fourth condition in Theorem 3.1.2; indeed, Derksen and Masser show that C_1, C_2 and C_3 can be taken to be sets of bounded height. This gives effective upper bounds for $|C_1|$, $|C_2|$ and $|C_3|$, but the resulting bounds are rather poor. Our improvement comes from Theorem 3.1.1, the aforementioned "gap principle" and a reduction step to the two variable unit equation, which brings the results of [44] in play.

Let $N > 0$ be an integer. As is well known there is a strong relation between unit equations and the Fermat equation

$$x_1^N + \ldots + x_m^N = 1$$

to be solved in $x_1, \ldots, x_m \in k(t)$ for some field k. This relation has been used in characteristic 0 by for example Voloch [77] and Bombieri and Mueller [5]. However, it is not clear how these methods can be made to work in characteristic $p > 0$. For example it would be natural to try and use a height bound for (3.3), but this is only possible when $x_1^N, \ldots, x_m^N$ are linearly independent over K^p. In the special case $m = 2$ this problem has been considered by Silverman [66], but unfortunately his main theorem is false. A correct statement with proof can be found in [40]. Here we will analyze the case $m = 3$.

Definition 3.1.3. We say that an integer $N > 0$ is (x, p)-good if the congruence

$$ap^s + b \equiv 0 \mod N$$

has no solutions in integers $s \geq 0$, $0 < a, b \leq x$.

We remark that for a given tuple (x, p) a positive density of the primes is (x, p)-good. Indeed, if $N > 2$ is a prime satisfying

$$\left(\frac{-1}{N}\right) = -1, \quad \left(\frac{p}{N}\right) = 1, \quad \left(\frac{a}{N}\right) = 1 \text{ for } 0 < a \leq x,$$

then N is (x, p)-good.

Theorem 3.1.4. *Let $p > 480$ be a prime number and suppose that N is a $(480, p)$-good integer. If we further suppose that $\gcd(N, p) = 1$, then the Fermat surface*

$$x^N + y^N + z^N = 1 \tag{3.6}$$

has no solutions $x, y, z \in \mathbb{F}_p(t)$ satisfying $x, y, z \notin \mathbb{F}_p(t^p)$ and $x/y, x/z, y/z \notin \mathbb{F}_p(t^p)$.

Note that Theorem 3.1.4 is in stark contrast with the behavior of the Fermat surface in characteristic 0 [77]. Remarkably enough it turns out that Theorem 3.1.4 becomes false if we drop any of the last two conditions, see Section 3.6. We will also explain there why we need the condition that N is $(480, p)$-good. The rough reason is that if N is not $(1, p)$-good, then the Fermat surface is known to be unirational [63]. Our work shows that the unirationality of these surfaces is strongly related to the two-dimensional Frobenius families appearing in Theorem 3.1.1. For precise details, we refer the reader to Section 3.6.

3.2 Preliminaries

In this section we start by defining heights, which will play a key role throughout the chapter. Furthermore, we give two important lemmata about heights.

3.2.1 Definition of height

Recall that K is a finitely generated field over $\mathbb{F}_p$ of transcendence degree 1 and that $\mathbb{F}_q$ is the algebraic closure of $\mathbb{F}_p$ inside K. We further recall that M_K is the set of places of K. The valuation ring of a place $v \in M_K$ is given by

$$O_v := \{x \in K : v(x) \geq 0\}.$$

This is a discrete valuation ring with maximal ideal $m_v := \{x \in K : v(x) > 0\}$. The residue class field O_v/m_v naturally becomes a finite field extension of $\mathbb{F}_q$. Hence

$$\deg(v) := [O_v/m_v : \mathbb{F}_q]$$

is a well-defined integer. With these definitions it turns out that the sum formula holds for all $x \in K^*$, i.e.

$$\sum_v v(x) \deg(v) = 0,$$

where here and below $\sum_v$ denotes a summation over $v \in M_K$. This allows us to define the height for $x \notin \mathbb{F}_q$ as follows

$$H_K(x) := [K : \mathbb{F}_q(x)] = \sum_{v \in M_K} \max(v(x), 0) \deg(v) = \sum_{v \in M_K} -\min(v(x), 0) \deg(v).$$

For $x \in \mathbb{F}_q$ we set $H_K(x) := 0$. More generally, we define the projective height to be

$$H_K(x_0 : \ldots : x_n) := -\sum_{v \in M_K} \min(v(x_0), \ldots, v(x_n)) \deg(v)$$

for $(x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$, which is well-defined due to the sum formula. One can recover the usual height by the identity $H_K(x) = H_K(1 : x)$.

3.2.2 Height lemmata

Pick $t \in K^*$ such that $K/\mathbb{F}_q(t)$ is of the minimal possible degree γ, the gonality of K. Then it follows that $K/\mathbb{F}_q(t)$ is a separable extension. Let D be the extension to K of the derivation $\frac{d}{dt}$ on $\mathbb{F}_q(t)$. We will fix such a derivation D for the remainder of the chapter. The following lemma will be important throughout.

Lemma 3.2.1. *The map $f : K^* \to K$ given by*

$$f(x) = \frac{Dx}{x}$$

is a homomorphism with kernel K^p.

Proof. The Leibniz rule implies that f is a homomorphism. Furthermore, the following is a standard fact regarding derivations

$$Dx = 0 \iff x \in K^p,$$

which immediately implies that the kernel of f is K^p. □

For every place $v \in M_K$, we choose an element z_v of K satisfying $v(z_v) = 1$. Since $K/\mathbb{F}_q(z_v)$ is a separable extension, we can uniquely extend the derivation $\frac{d}{dz_v}$ to K. For $x \in K^*$ we write $\omega(x) = \sum_{v : v(x) \neq 0} \deg(v)$.

Lemma 3.2.2. *Let $f \in K^*$. Then for $f \notin K^p$*

$$H_K\left(\frac{Df}{f}\right) \leq \omega(f) + 2g - 2 + 2\gamma,$$

where g is the genus of K.

Proof. We have

$$H_K\left(\frac{Df}{f}\right) = \frac{1}{2}\sum_v \left| v\left(\frac{Df}{f}\right)\right| \deg(v).$$

We may write

$$v\left(\frac{Df}{f}\right) = \left(v\left(\frac{df}{dz_v}\right) - v(f)\right) - v\left(\frac{dt}{dz_v}\right).$$

Therefore we get that

$$H_K\left(\frac{Df}{f}\right) = \frac{1}{2}\sum_v \left|v\left(\frac{Df}{f}\right)\right| \deg(v) \leq$$
$$\frac{1}{2}\cdot\left(\sum_v \left|v\left(\frac{df}{dz_v}\right) - v(f)\right| \deg(v) + \sum_v \left|v\left(\frac{dt}{dz_v}\right)\right| \deg(v)\right).$$

We call the two inner sums respectively T_1 and T_2.

Bound for T_1
By the Riemann-Roch Theorem, see e.g. equation (5) of page 96, chapter 6 in [54], we have for $f \notin K^p$ that

$$\sum_v v\left(\frac{df}{dz_v}\right) \deg(v) = 2g - 2 \tag{3.7}$$

and hence by the sum formula

$$\sum_v \left(v\left(\frac{df}{dz_v}\right) - v(f)\right) \deg(v) = 2g - 2.$$

Furthermore $v\left(\frac{df}{dz_v}\right) - v(f) < 0$ implies $v\left(\frac{df}{dz_v}\right) - v(f) = -1$. Therefore

$$\sum_{v: v\left(\frac{df}{dz_v}\right) < v(f)} \left|v\left(\frac{df}{dz_v}\right) - v(f)\right| \deg(v) \leq \omega(f)$$

and thus

$$\sum_{v: v\left(\frac{df}{dz_v}\right) \geq v(f)} \left(v\left(\frac{df}{dz_v}\right) - v(f)\right) \deg(v) \leq 2g - 2 + \omega(f).$$

In total we get that

$$T_1 \leq 2\omega(f) + 2g - 2.$$

Bound for T_2
We use equation (3.7) with $f = t$ to obtain

$$\sum_v v\left(\frac{dt}{dz_v}\right) \deg(v) = 2g - 2. \tag{3.8}$$

If $v(t) \geq 0$, then we clearly have $v\left(\frac{dt}{dz_v}\right) \geq 0$. On the other hand if $v(t) < 0$, we have

$$v\left(\frac{dt}{dz_v}\right) = v(t) - 1.$$

Hence

$$\sum_{v:v\left(\frac{dt}{dz_v}\right)<0} \left| v\left(\frac{dt}{dz_v}\right)\right| \deg(v) = \sum_{v:v(t)<0} (1-v(t))\deg(v) \leq -2 \sum_{v:v(t)<0} v(t)\deg(v) = 2\gamma, \tag{3.9}$$

which we can combine with equation (3.8) to deduce

$$\sum_{v:v\left(\frac{dt}{dz_v}\right)\geq 0} v\left(\frac{dt}{dz_v}\right)\deg(v) \leq 2g-2+2\gamma \tag{3.10}$$

After adding equation (3.9) and equation (3.10), we conclude that

$$T_2 \leq 2g-2+4\gamma.$$

Conclusion of proof
In total we get

$$H_K\left(\frac{Df}{f}\right) \leq \frac{1}{2}(T_1+T_2) \leq \omega(f)+2g-2+2\gamma,$$

which is the desired inequality. □

We will repeatedly use the following two theorems.

Theorem 3.2.3. *Let $x, y \in \mathcal{O}_S^*$. If $x, y \notin K^p$ and*

$$x+y=1,$$

then we have

$$H_K(x) = H_K(y) \leq \omega(S)+2g-2.$$

Proof. See [54] and [67]. □

Theorem 3.2.4. *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*

$$x+y=1 \text{ in } (x,y) \in G$$

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

Proof. This is Theorem 1.2 of [44]. □

3.3 Proof of Theorem 3.1.1

Proof. By construction $\mathcal{F}(\mathbf{x})$ is a solution to (3.4) for $\mathbf{x} \in A$ and likewise all elements of $\mathcal{F}_a(\mathbf{u}, \mathbf{v})$ are solutions to (3.4). Hence it suffices to prove the only if part of Theorem 3.1.1. Let x, y, z be a solution of (3.4) with $x, y, z \notin \mathbb{F}_q$. Note that the sets as given in equation (3.5) are all invariant under taking p-th roots. Since $x, y, z \notin \mathbb{F}_q$, we can keep taking p-th roots of the tuple (x, y, z) until x, y or z is not in K^p. For ease of notation we will keep using the same letters for the new x, y and z. By symmetry we may assume that $z \notin K^p$. Then also $x \notin K^p$ or $y \notin K^p$. Again we may assume by symmetry that $y \notin K^p$. Now we distinguish two cases.

Case I: First suppose that $x \in K^p$. Then using

$$x + y + z = 1$$

we find after differentiating with respect to D

$$\frac{Dy}{y} y + \frac{Dz}{z} z = 0.$$

We can rewrite this as follows

$$x + y\left(1 - \frac{z}{Dz}\frac{Dy}{y}\right) = 1$$
$$x + z\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) = 1.$$

Define $a_2 := 1 - \frac{z}{Dz}\frac{Dy}{y}$ and $b_3 := 1 - \frac{y}{Dy}\frac{Dz}{z}$. Note that $a_2 = 0$ implies $x = 1$, contrary to our assumption $x \notin \mathbb{F}_q$. Similarly $b_3 \neq 0$. The above system of equations implies that either $b_3, a_2 \notin \mathcal{O}_S^*$ or $b_3, a_2 \in \mathcal{O}_S^*$. Consider first the case $b_3, a_2 \notin \mathcal{O}_S^*$. By Lemma 3.2.2 we have

$$H_K(b_3) \leq c_{K,S}. \tag{3.11}$$

We set $l := \lfloor \log_p c_{K,S} \rfloor + 1$ and claim that $b_3 z \notin K^{p^l}$. Take $v \notin S$ such that $v(b_3) \neq 0$; such a valuation exists by our assumption that $b_3 \notin \mathcal{O}_S^*$. From the height bound in equation (3.11) we deduce that

$$|v(b_3)| \leq H_K(b_3) \leq c_{K,S}.$$

Since $z \in \mathcal{O}_S^*$, we conclude that

$$0 \neq |v(b_3 z)| \leq c_{K,S}.$$

This immediately implies that $b_3 z \notin K^{p^l}$, which establishes our claim.

Write $x = \delta^{p^s}$ and $b_3 z = \epsilon^{p^s}$, with $\delta, \epsilon \notin K^p$. Note that $\delta + \epsilon = 1$, so an application of Theorem 3.2.3 gives

$$H_K(\delta) = H_K(\epsilon) \leq \omega(S) + 2c_{K,S} + 2g - 2,$$

where we used that $\omega(b_3) \leq 2H_K(b_3) \leq 2c_{K,S}$. We conclude that

$$H_K(x) = H_K(b_3 z) = p^s H_K(\delta) = p^s H_K(\epsilon) \leq c_{K,S} \cdot (\omega(S) + 2c_{K,S} + 2g - 2),$$

since $p^s \leq p^{l-1} \leq c_{K,S}$.

We now consider the case that $a_2, b_3 \in \mathcal{O}_S^*$. Since $x \notin \mathbb{F}_q$ there is $x' \notin K^p$ such that $x = x'^{p^s}$ for some $s > 0$. There are also $y', z' \in \mathcal{O}_S^*$ such that

$$x' + a_2 y' = 1 \tag{3.12}$$
$$x' + b_3 z' = 1. \tag{3.13}$$

Applying Theorem 3.2.3 again yields

$$H_K(x') = H_K(a_2 y') \leq \omega(S) + 2g - 2.$$

We conclude that

$$(x, y, z) \in \mathcal{F}_1((1, a_2^{-1}, b_3^{-1}), (x', a_2 y', b_3 z')),$$

with $a_2, b_3 \notin \mathbb{F}_q$, since otherwise $y, z \in K^p$, which would be a contradiction. Using the identity $a_2^{-1} + b_3^{-1} = 1$ and equations (3.12), (3.13), we quickly verify the identity

$$x'^{p^f} + a_2^{-1}(a_2 y')^{p^f} + b_3^{-1}(b_3 z')^{p^f} = 1$$

for all integers $f \geq 0$, so that indeed $((1, a_2^{-1}, b_3^{-1}), (x', a_2 y', b_3 z')) \in B_1$.

Case II: Now suppose $x \notin K^p$. We start by dealing with the case $\frac{x}{Dx} \neq \frac{y}{Dy}$, $\frac{x}{Dx} \neq \frac{z}{Dz}$, $\frac{y}{Dy} \neq \frac{z}{Dz}$. Then we find that

$$x + y + z = 1$$

and after differentiating with respect to D

$$\frac{Dx}{x}x + \frac{Dy}{y}y + \frac{Dz}{z}z = 0.$$

This is equivalent to

$$x\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) + y\left(1 - \frac{z}{Dz}\frac{Dy}{y}\right) = 1$$
$$x\left(1 - \frac{y}{Dy}\frac{Dx}{x}\right) + z\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) = 1.$$

For convenience we define

$$a_1 := 1 - \frac{z}{Dz}\frac{Dx}{x}, a_2 := 1 - \frac{z}{Dz}\frac{Dy}{y}, b_1 := 1 - \frac{y}{Dy}\frac{Dx}{x}, b_3 := 1 - \frac{y}{Dy}\frac{Dz}{z}.$$

By our assumption we know that the coefficients a_1, a_2, b_1 and b_3 are not zero. If one of the coefficients, say a_1, does not lie in $\mathcal{O}_S^*$, we can proceed exactly as before obtaining the bound

$$H_K(a_1 x) = H_K(a_2 y) \leq c_{K,S} \cdot (\omega(S) + 4c_{K,S} + 2g - 2).$$

So now suppose that $a_1, a_2, b_1, b_3 \in \mathcal{O}_S^*$, but also suppose that $d := \frac{a_1}{b_1} \notin \mathbb{F}_q^*$. In this case we have

$$H_K(d) \leq 2c_{K,S}$$

and therefore $a_1 x \notin K^{p^l}$ or $b_1 x \notin K^{p^l}$ with $l := \lfloor \log_p 2c_{K,S} \rfloor + 1$. Suppose that $a_1 x \notin K^{p^l}$. Then Theorem 3.2.3 gives

$$H_K(a_1 x) = H_K(a_2 y) \leq 2c_{K,S} \cdot (\omega(S) + 4c_{K,S} + 2g - 2)$$

and the other case can be dealt with in exactly the same way.

Finally suppose that $a_1, a_2, b_1, b_3 \in \mathcal{O}_S^*$ and $d \in \mathbb{F}_q^*$. If we additionally suppose that one of the coefficients is in $\mathbb{F}_q^*$, another application of Theorem 3.2.3 yields

$$H_K(a_1 x) = H_K(a_2 y) = H_K(b_1 x) = H_K(b_3 z) \leq \omega(S) + 2g - 2.$$

Hence we will assume that $a_1, a_2, b_1, b_3 \notin \mathbb{F}_q^*$ from now on. If $a_1 x \in \mathbb{F}_q^*$, we immediately get a height bound for x. So we may further assume that $a_1 x \notin \mathbb{F}_q^*$. Then let $l \geq 0$ be the largest integer such that $a_1 x \in K^{q^l}$. Define $x' \in \mathcal{O}_S^*$ as

$$(a_1 x')^{q^l} = a_1 x$$

and then define $y', z' \in \mathcal{O}_S^*$ such that

$$a_1 x' + a_2 y' = 1 \tag{3.14}$$
$$b_1 x' + b_3 z' = 1. \tag{3.15}$$

Furthermore,

$$H_K(a_1 x') = H_K(a_2 y') \leq \frac{q}{p}(\omega(S) + 2g - 2)$$

and

$$(x, y, z) \in \mathcal{F}_{\log_p(q)}((a_1^{-1}, a_2^{-1}, b_3^{-1}), (a_1 x', a_2 y', b_3 z')).$$

Once more, a direct verification using $a_2^{-1} + b_3^{-1} = 1$, $1 - \frac{a_1}{a_2} - \frac{b_1}{b_3} = 0$ and the equations (3.14), (3.15) shows that

$$a_1^{-1}(a_1 x')^{q^f} + a_2^{-1}(a_2 y')^{q^f} + b_3^{-1}(b_3 z')^{q^f} = 1$$

for all integers $f \geq 0$. We conclude that $((a_1^{-1}, a_2^{-1}, b_3^{-1}), (a_1 x', a_2 y', b_3 z')) \in B_q$. This deals with the case $x \notin K^p$ and $\frac{x}{Dx} \neq \frac{y}{Dy}$, $\frac{x}{Dx} \neq \frac{z}{Dz}$, $\frac{y}{Dy} \neq \frac{z}{Dz}$.

We still have to deal with the case $x \notin K^p$ and $\frac{x}{Dx} = \frac{y}{Dy}$ or $\frac{x}{Dx} = \frac{z}{Dz}$ or $\frac{y}{Dy} = \frac{z}{Dz}$. Recall that $y, z \notin K^p$ as well, hence the three cases are symmetrical. So we will only deal with the case $\frac{y}{Dy} = \frac{z}{Dz}$. Then we get the equations

$$x\left(1 - \frac{y}{Dy}\frac{Dx}{x}\right) = x\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) = 1$$

and hence

$$H_K(x) \leq c_{K,S}.$$

Our equation implies that $a_1 := b_1 := 1 - \frac{y}{Dy}\frac{Dx}{x} \in \mathcal{O}_S^*$. Substitution in the original equation yields

$$\frac{1}{a_1} + y + z = 1$$

or equivalently

$$y + z = 1 - \frac{1}{a_1} = \frac{a_1 - 1}{a_1}.$$

After putting $\alpha := \frac{a_1}{a_1 - 1}$ we get

$$\alpha y + \alpha z = 1.$$

Note that

$$H_K(\alpha) = H_K(a_1) = H_K(x) \leq c_{K,S}.$$

Suppose that $\alpha \notin \mathcal{O}_S^*$. Just as before we find that $\alpha y \notin K^{p^l}$, where $l := \lfloor \log_p c_{K,S} \rfloor + 1$. Then Theorem 3.2.3 gives

$$H_K(\alpha y) = H_K(\alpha z) \leq c_{K,S} \cdot (\omega(S) + c_{K,S} + 2g - 2).$$

The last case is $\alpha \in \mathcal{O}_S^*$. Suppose that $\alpha \in \mathbb{F}_q^*$. From Theorem 3.2.3 we deduce that

$$H_K(\alpha y) = H_K(\alpha z) \leq \omega(S) + 2g - 2.$$

So from now on we further assume that $\alpha \notin \mathbb{F}_q^*$. If $\alpha y \in \mathbb{F}_q^*$ or $\alpha z \in \mathbb{F}_q^*$, we immediately get a height bound for respectively y or z. So suppose that $\alpha y \notin \mathbb{F}_q^*$ and $\alpha z \notin \mathbb{F}_q$. Then there are $y', z' \notin K^p$ and $s \in \mathbb{Z}_{\geq 0}$ such that $y'^{p^s} = \alpha y$ and $z'^{p^s} = \alpha z$ and we get an equation

$$y' + z' = 1. \tag{3.16}$$

Applying Theorem 3.2.3 once more

$$H_K(y') = H_K(z') \leq \omega(S) + 2g - 2.$$

We conclude that

$$(x, y, z) \in \mathcal{F}_1((x, \alpha^{-1}, \alpha^{-1}), (1, y', z')).$$

A simple check using $x + \alpha^{-1} = 1$ and equation (3.16) shows that

$$x + \alpha^{-1}(y')^{p^f} + \alpha^{-1}(z')^{p^f} = 1$$

for all integers $f \geq 0$ and hence $((x, \alpha^{-1}, \alpha^{-1}), (1, y', z')) \in B_1$. This completes the proof. □

3.4 Proof of Theorem 3.1.2

Define the set B'_p by

$$B'_p := \{(\mathbf{u}, \mathbf{v}) \in (\mathcal{O}_S^*)^3 \times (\mathcal{O}_S^*)^3 : \mathbf{u}, \mathbf{v} \notin (K^p)^3, (u_i, v_i) \notin \mathbb{F}_q^* \times \mathbb{F}_q^*, H_K(u_i) \leq c_{K,S},$$
$$H_K(v_i) \leq \omega(S) + 2g - 2, u_1 v_1^{p^f} + u_2 v_2^{p^f} + u_3 v_3^{p^f} = 1 \text{ for all } f \in \mathbb{Z}_{\geq 0}\}.$$

For the reader's convenience we recall that in the definition of B_p we only required that $\mathbf{u}, \mathbf{v} \notin (\mathbb{F}_q^*)^3$ instead of the stronger condition $\mathbf{u}, \mathbf{v} \notin (K^p)^3$. Nevertheless we have the equality

$$\bigcup_{(\mathbf{u},\mathbf{v})\in B_p} \mathcal{F}_1(\mathbf{u},\mathbf{v}) = \bigcup_{(\mathbf{u},\mathbf{v})\in B'_p} \mathcal{F}_1(\mathbf{u},\mathbf{v}). \tag{3.17}$$

To prove equality (3.17), we need two lemmata.

Lemma 3.4.1. *Let K be a field of characteristic $p > 0$ and let $n \geq 0$ be an integer. Suppose that $u_1, \ldots, u_n, v_1, \ldots, v_n \in K$ are such that*

$$u_1 v_1^{p^f} + \ldots + u_n v_n^{p^f} = 1$$

for all integers $f \geq 0$. Then $v_1, \ldots, v_n$ are linearly dependent over $\mathbb{F}_p$ or $u_1, \ldots, u_n \in \mathbb{F}_p$.

Proof. Define A to be the matrix

$$A := \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1^p & v_2^p & \ldots & v_n^p \\ \vdots & & \vdots & \\ v_1^{p^{n-1}} & v_2^{p^{n-1}} & \ldots & v_n^{p^{n-1}} \end{pmatrix}.$$

It is a well-known fact that A is invertible if and only if $v_1, \ldots, v_n$ are linearly independent over $\mathbb{F}_p$; this can be proven by induction on n. We shall henceforth assume that A is invertible and prove that $u_1, \ldots, u_n \in \mathbb{F}_p$. But observe that

$$A \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}, \quad A \begin{pmatrix} u_1^{1/p} \\ \vdots \\ u_n^{1/p} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

This implies that $u_i = u_i^{1/p}$ for $i = 1, \ldots, n$, and the lemma follows. □

Lemma 3.4.2. *Let K be a field of characteristic $p > 0$ and let $n \geq 0$ be an integer. Suppose that $u_1, \ldots, u_n, v_1, \ldots, v_n \in K$ are such that*

$$u_1 v_1^{p^f} + \ldots + u_n v_n^{p^f} = 1$$

for all integers $f > 0$. Then we also have

$$u_1 v_1 + \ldots + u_n v_n = 1.$$

Proof. We proceed by induction on n with the base case $n = 0$ being trivial. We now apply Lemma 3.4.1. If $u_1, \ldots, u_n \in \mathbb{F}_p$, we clearly have

$$u_1 v_1 + \ldots + u_n v_n = 1$$

after taking p-th roots. So suppose that $v_1, \ldots, v_n$ are linearly dependent over $\mathbb{F}_p$. Without loss of generality we may write

$$v_n = \alpha_1 v_1 + \ldots + \alpha_{n-1} v_{n-1} \tag{3.18}$$

for some $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_p$. Now substitution yields

$$(u_1 + \alpha_1 u_n) v_1^{p^f} + \ldots + (u_{n-1} + \alpha_{n-1} u_n) v_{n-1}^{p^f} = 1$$

for all integers $f > 0$. The induction hypothesis gives

$$(u_1 + \alpha_1 u_n) v_1 + \ldots + (u_{n-1} + \alpha_{n-1} u_n) v_{n-1} = 1. \tag{3.19}$$

Upon combining equation (3.18) with equation (3.19) we obtain the lemma. □

Note that Lemma 3.4.2 with $n = 3$ readily implies the validity of equation (3.17). So our goal will be to give an upper bound for the cardinality of B'_p. Now let $(\mathbf{u}, \mathbf{v}) \in B'_p$. Then we know that

$$u_1 v_1^{p^f} + u_2 v_2^{p^f} + u_3 v_3^{p^f} = 1$$

for all $f \in \mathbb{Z}_{\geq 0}$. Since $\mathbf{u} \notin (\mathbb{F}_p^*)^3$, an application of Lemma 3.4.1 shows that v_1, v_2, v_3 are indeed linearly dependent over $\mathbb{F}_p$. At the cost of multiplying our final bounds by 3, we may assume that

$$v_3 = \alpha_1 v_1 + \alpha_2 v_2$$

with $\alpha_1, \alpha_2 \in \mathbb{F}_p$. This yields

$$(u_1 + \alpha_1 u_3)\, v_1^{p^f} + (u_2 + \alpha_2 u_3)\, v_2^{p^f} = 1 \tag{3.20}$$

for all $f \in \mathbb{Z}_{\geq 0}$. Let us now apply Lemma 3.4.1 again. First suppose that v_1 and v_2 are linearly dependent over $\mathbb{F}_p$, we will show that this leads to a contradiction. Without loss of generality we may assume that $v_2 = \beta v_1$ for some $\beta \in \mathbb{F}_p$. Then we obtain

$$(u_1 + \alpha_1 u_3 + \beta u_2 + \beta \alpha_2 u_3) v_1^{p^f} = 1$$

for all $f \in \mathbb{Z}_{\geq 0}$, which implies $v_1 \in \mathbb{F}_p$. We deduce that $v_1, v_2, v_3 \in \mathbb{F}_p$, which is the desired contradiction. Hence Lemma 3.4.1 implies that

$$\lambda_1 := u_1 + \alpha_1 u_3 \in \mathbb{F}_p, \quad \lambda_2 := u_2 + \alpha_2 u_3 \in \mathbb{F}_p$$

and therefore $\lambda_1 v_1 + \lambda_2 v_2 = 1$. We claim that at most one of $\alpha_1, \alpha_2, \lambda_1, \lambda_2$ is equal to zero.

It is clear that α_1 and α_2 can not be simultaneously equal to zero, and the same holds for λ_1 and λ_2. If $\alpha_1 = \lambda_1 = 0$, we find that $u_1 = 0$, which contradicts $u_1 \in \mathcal{O}_S^*$. Now suppose that $\alpha_1 = \lambda_2 = 0$. In this case we deduce that $u_1, v_1 \in \mathbb{F}_p^*$, again contrary to our assumption $(\mathbf{u}, \mathbf{v}) \in B'_p$. The remaining two cases can be dealt with symmetrically, establishing our claim.

Let us first suppose that $\alpha_1, \alpha_2, \lambda_1, \lambda_2$ are all fixed and non-zero. Then we view the equations

$$\lambda_1 = u_1 + \alpha_1 u_3, \quad \lambda_2 = u_2 + \alpha_2 u_3, \quad \lambda_1 v_1 + \lambda_2 v_2 = 1$$

as unit equations to be solved in u_1, u_2, u_3, v_1, v_2. If one of the u_i is in K^p, then it turns out that all the u_i are in K^p, contradicting our assumption $\mathbf{u} \notin (K^p)^3$. Henceforth we may assume that $u_1, u_2, u_3 \notin K^p$ and similarly $v_1, v_2 \notin K^p$. Theorem 3.2.4 implies that there are at most $31 \cdot 19^{2|S|}$ solutions (u_1, u_3) to $\lambda_1 = u_1 + \alpha_1 u_3$ and at most $31 \cdot 19^{2|S|}$ solutions (v_1, v_2) to $\lambda_1 v_1 + \lambda_2 v_2 = 1$. Note that u_1 and u_3 determine u_2 and similarly v_1 and v_2 determine v_3. Hence there are at most $961 \cdot 19^{4|S|}$ possibilities for $(\mathbf{u}, \mathbf{v})$.

We will now treat the case $\lambda_2 = 0$ and $\alpha_1, \alpha_2, \lambda_1$ fixed and non-zero. In this case we can treat the unit equation

$$\lambda_1 = u_1 + \alpha_1 u_3$$

exactly as before; it has at most $31 \cdot 19^{2|S|}$ solutions (u_1, u_3). From $0 = \lambda_2 = u_2 + \alpha_2 u_3$ we see that u_2 is determined by u_1 and u_3. Note that $\lambda_2 = 0$ implies $\lambda_1 v_1 = 1$, i.e. $v_1 = \frac{1}{\lambda_1}$. We recall that

$$v_3 = \alpha_1 v_1 + \alpha_2 v_2$$

and therefore

$$v_3 = \frac{\alpha_1}{\lambda_1} + \alpha_2 v_2.$$

If $v_2 \in K^p$, then also $v_3 \in K^p$ and we conclude that $(v_1, v_2, v_3) \in (K^p)^3$. This is again a contradiction, so suppose that $v_2, v_3 \notin K^p$. We are now in the position to apply Theorem 3.2.4, which shows that there are at most $31 \cdot 19^{2|S|}$ solutions (v_2, v_3). Hence there are at most $961 \cdot 19^{4|S|}$ possibilities for $(\mathbf{u}, \mathbf{v})$.

Finally we will treat the case $\alpha_2 = 0$ and $\alpha_1, \lambda_1, \lambda_2$ still fixed and non-zero. We remark that the remaining two cases $\lambda_1 = 0$ and $\alpha_1 = 0$ can be dealt with using the same argument as the case $\lambda_2 = 0$ and $\alpha_2 = 0$ respectively. Note that $u_2 = \lambda_2 \in \mathbb{F}_p^*$. Using $\lambda_1 = u_1 + \alpha_1 u_3$ and $\mathbf{u} \notin (K^p)^3$, we deduce that $u_1, u_3 \notin K^p$. Hence the unit equation

$$\lambda_1 = u_1 + \alpha_1 u_3$$

has at most $31 \cdot 19^{2|S|}$ solutions (u_1, u_3). Similarly, the unit equation

$$\lambda_1 v_1 + \lambda_2 v_2 = 1$$

has at most $31 \cdot 19^{2|S|}$ solutions (v_1, v_2). Since v_1 determines v_3, we have proven that there are also at most $961 \cdot 19^{4|S|}$ possibilities for $(\mathbf{u}, \mathbf{v})$ in this case.

So far we have treated $\alpha_1, \alpha_2, \lambda_1, \lambda_2$ as fixed. To every element of B'_p we can attach a tuple $\mathbf{t} = (\alpha_1, \alpha_2, \lambda_1, \lambda_2)$. Clearly there are at most p^4 such tuples. Furthermore, we have shown that for each fixed tuple $\mathbf{t}$ there are at most $961 \cdot 19^{4|S|}$ $(\mathbf{u}, \mathbf{v}) \in B'_p$ that correspond to $\mathbf{t}$. Altogether we have proven that $|B'_p| \leq 3 \cdot 961 \cdot p^4 \cdot 19^{4|S|} = 2883 \cdot p^4 \cdot 19^{4|S|}$.

To deal with B_q one can use a very similar approach, so we will only sketch the proof. In this case we define

$$B'_q := \{(\mathbf{u},\mathbf{v}) \in (\mathcal{O}_S^*)^3 \times (\mathcal{O}_S^*)^3 : \mathbf{u},\mathbf{v} \notin (K^q)^3, (u_i,v_i) \notin \mathbb{F}_q^* \times \mathbb{F}_q^*, H_K(u_i) \leq c_{K,S},$$
$$H_K(v_i) \leq \frac{q}{p}\left(\omega(S)+2g-2\right), u_1 v_1^{q^f} + u_2 v_2^{q^f} + u_3 v_3^{q^f} = 1 \text{ for all } f \in \mathbb{Z}_{\geq 0}\}.$$

Note that we now only require that $\mathbf{u},\mathbf{v} \notin (K^q)^3$ instead of $\mathbf{u},\mathbf{v} \notin (K^p)^3$. In our new setting we find that $\alpha_1,\alpha_2,\lambda_1,\lambda_2 \in \mathbb{F}_q$ instead of $\alpha_1,\alpha_2,\lambda_1,\lambda_2 \in \mathbb{F}_p$. This means that we have q^4 tuples $(\alpha_1,\alpha_2,\lambda_1,\lambda_2)$. For each fixed tuple $\mathbf{t}$ there are at most $\log_p(q)\cdot 961 \cdot 19^{4|S|}$ $(\mathbf{u},\mathbf{v}) \in B'_q$ that can map to $\mathbf{t}$. The extra factor $\log_p(q)$ comes from the fact that we merely know that $\mathbf{u},\mathbf{v} \notin (K^q)^3$ when we apply Theorem 3.2.4. We conclude that $|B'_q| \leq 2883 \cdot \log_p(q) \cdot q^4 \cdot 19^{4|S|}$.

Our only remaining task is to bound $|A|$. We start by recalling a "gap principle". Define

$$\mathcal{S} := \{(x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3(K) \setminus \mathbb{P}^3(\mathbb{F}_q) : x_0 + x_1 + x_2 = x_3,$$
$$v(x_0) = v(x_1) = v(x_2) = v(x_3) \text{ for every } v \in M_K \setminus S\}.$$

Then we have the following lemma.

Lemma 3.4.3 (Gap principle)**.** *Let B be a real number with $\frac{3}{4} < B < 1$, and let $P > 0$. Then the set of projective points $(x_0 : x_1 : x_2 : x_3)$ of $\mathcal{S}$ with*

$$P \leq H_K(x_0 : x_1 : x_2 : x_3) < \left(1 + \frac{4B-3}{2}\right) P$$

is contained in the union of at most $4^{|S|}(e/(1-B))^{3|S|-1}$ 1-dimensional projective subspaces of $x_0 + x_1 + x_2 = x_3$. Here e is the Euler constant.

Proof. This was proved in [18] for function fields in characteristic 0, but the proof works ad verbatim in characteristic p. □

Take any $P > 0$ and suppose that $(x,y,z) \in A$ is a solution to

$$x + y + z = 1$$

with $P \leq H_K(x : y : z : 1) < \left(1 + \frac{4B-3}{2}\right) P$. Then we can apply Lemma 3.4.3 to deduce that $(x : y : z : 1)$ is contained in some 1-dimensional projective subspace. This means that x, y, z satisfy an additional equation

$$ax + by + cz = d \tag{3.21}$$

for some $a,b,c,d \in K$, such that the equation is independent from the original equation $x + y + z = 1$. By adding the equation $x + y + z = 1$ to equation (3.21) if necessary, we can ensure that $a \neq 0$. We have

$$(a-b)y + (a-c)z = a - d. \tag{3.22}$$

If $a-b$, $a-c$ and $a-d$ are zero, we conclude that $a=b=c=d$. This is a contradiction, since we assumed that the equation $ax+by+cz=d$ was linearly independent from the equation $x+y+z=1$. If only one of $a-b$, $a-c$ and $a-d$ is not zero, we find that $y=0$, $z=0$ and $0=a-d\neq 0$ respectively, so we obtain a contradiction in every case. At the cost of multiplying our final bounds by 3, we may assume that $a-b\neq 0$. We will distinguish three cases.

Case I: $a-c\neq 0$, $a-d\neq 0$**.** In this case we view (3.22) as a unit equation. Since $(x,y,z)\in A$, it follows that $H_K(x), H_K(y), H_K(z)\leq c'_{K,S}$. We conclude that

$$H_K\left(\frac{a-b}{a-d}y\right)\in\left[H_K\left(\frac{a-b}{a-d}\right)-c'_{K,S}, H_K\left(\frac{a-b}{a-d}\right)+c'_{K,S}\right]. \tag{3.23}$$

If $(a-b)/(a-d)\notin\mathcal{O}_S^*$ or $(a-c)/(a-d)\notin\mathcal{O}_S^*$, we use Theorem 1.1 from [44]. In this case we see that there are at most $31\cdot 19^{2|S|-1}$ solutions. Now suppose that $(a-b)/(a-d)\in\mathcal{O}_S^*$ and $(a-c)/(a-d)\in\mathcal{O}_S^*$. Then we have

$$\frac{a-b}{a-d}y\in\mathbb{F}_q \quad\text{or}\quad y=\frac{a-d}{a-b}\cdot v^{p^z} \text{ for some } z\in\mathbb{Z}_{\geq 0}$$

with $v\notin(\mathcal{O}_S^*)^p$. The first case gives at most q^2 solutions. To treat the second case, we remark that there are at most $31\cdot 19^{2|S|-2}$ values of v due to Theorem 3.2.4. Furthermore, for fixed v, there are at most $\log_p(2c'_{K,S})+1$ choices of z by equation (3.23). Hence there are at most

$$q^2+(\log_p(2c'_{K,S})+1)\cdot 31\cdot 19^{2|S|}$$

solutions (y,z) to equation (3.22). From $x+y+z=1$ we see that y and z determine x.

We will now count the total contribution to the number of solutions from case I. Choose $B:=\frac{7}{8}$. Note that

$$H_K(x:y:z:1)\leq H_K(x)+H_K(y)+H_K(z)\leq 3c'_{K,S}.$$

Now define $l:=\log_{\frac{5}{4}}(3c'_{K,S})+1$. Then for every solution $(x,y,z)\in A$ there is i with $0\leq i<l$ such that

$$\left(\frac{5}{4}\right)^i\leq H_K(x:y:z:1)<\left(\frac{5}{4}\right)^{i+1}.$$

For fixed i every solution $(x:y:z:1)$ is contained in the union of at most $(2048e^3)^{|S|}$ 1-dimensional projective subspaces. Furthermore, we have just shown that each subspace contains at most $q^2+(\log_p(2c'_{K,S})+1)\cdot 31\cdot 19^{2|S|}$ solutions. This gives as total bound for A in case I

$$\begin{aligned}|A| &\leq (\log_{\frac{5}{4}}(3c'_{K,S})+1)\cdot(2048e^3)^{|S|}\cdot q^2\cdot(\log_p(2c'_{K,S})+1)\cdot 31\cdot 19^{2|S|}\\ &\leq 31q^2\cdot(\log_{\frac{5}{4}}(3c'_{K,S})+1)^2\cdot(15\cdot 10^6)^{|S|}.\end{aligned} \tag{3.24}$$

Case II: $a-c\neq 0$, $a-d=0$**.** In this case (3.22) gives

$$z=-\frac{a-b}{a-c}y.$$

Substitution in $x + y + z = 1$ yields

$$x + \left(1 - \frac{a-b}{a-c}\right) y = 1. \tag{3.25}$$

If $a - b = a - c$, we see that $x = 1$, contrary to our assumption $x \notin \mathbb{F}_q$. So we will assume that $a - b \neq a - c$ and treat (3.25) as a unit equation. Then, following the proof of case I, we get the bound (3.24) for A in case II.

Case III: $a - c = 0$**,** $a - d \neq 0$**.** From (3.22) we deduce that

$$y = \frac{a-d}{a-b}.$$

If $a - b = a - d$, we conclude that $y = 1$, which is again a contradiction. Substitution in $x + y + z = 1$ gives

$$x + z = 1 - \frac{a-d}{a-b}. \tag{3.26}$$

Note that (3.26) is another unit equation and, just as before, we obtain the bound (3.24) for A in case III.

3.5 Application to Fermat surfaces

The goal of this section is to prove Theorem 3.1.4. We start off with a definition.

Definition 3.5.1. We say that a valuation v of K is D-generic if the following two conditions are satisfied

- first of all
$$v\left(\frac{Dx}{x}\right) = -1$$
for all $x \in K^*$ satisfying $p \nmid v(x)$;
- and secondly
$$v\left(\frac{Dx}{x}\right) \geq 0$$
for all $x \in K^*$ with $p \mid v(x)$.

In $\mathbb{F}_p(t)$ and D differentiation with respect to t, every valuation is D-generic except for the infinite valuation. In general only finitely many valuations are not generic.

In this section K and D will always be equal to respectively $\mathbb{F}_p(t)$ and differentiation with respect to t. Whenever we say that v is generic, we will mean generic with respect to this

D. Let N be a $(480, p)$-good integer coprime to p. In particular we have that $N > 480$, which we shall use at several points during the proof. Suppose that $x, y, z \in \mathbb{F}_p(t)$ is a solution to

$$x^N + y^N + z^N = 1 \tag{3.27}$$

satisfying the conditions of Theorem 3.1.4, i.e. $x, y, z, x/y, x/z, y/z \notin \mathbb{F}_p(t^p)$. By Lemma 3.2.1 this is equivalent to $\frac{Dx}{x} \neq 0$, $\frac{Dy}{y} \neq 0$, $\frac{Dz}{z} \neq 0$, $\frac{Dx}{x} \neq \frac{Dy}{y}$, $\frac{Dx}{x} \neq \frac{Dz}{z}$ and $\frac{Dy}{y} \neq \frac{Dz}{z}$. Then differentiation with respect to D yields

$$x^N \cdot \frac{NDx}{x} + y^N \cdot \frac{NDy}{y} + z^N \cdot \frac{NDz}{z} = 0,$$

and using that $(N, p) = 1$

$$x^N \cdot \frac{Dx}{x} + y^N \cdot \frac{Dy}{y} + z^N \cdot \frac{Dz}{z} = 0. \tag{3.28}$$

We multiply equation (3.28) with $\frac{z}{Dz}$ and subtract it from equation (3.27) to obtain

$$x^N \left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) + y^N \left(1 - \frac{z}{Dz}\frac{Dy}{y}\right) = 1 \tag{3.29}$$

and similarly

$$x^N \left(1 - \frac{y}{Dy}\frac{Dx}{x}\right) + z^N \left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) = 1. \tag{3.30}$$

Define

$$S := \{v \in M_K : v(x) \neq 0 \text{ or } v(y) \neq 0 \text{ or } v(z) \neq 0\}.$$

We may assume that x is such that

$$\omega(x) \geq \frac{\omega(S)}{3}. \tag{3.31}$$

If $N > 12$, thanks to Lemma 3.2.2 applied with $K = \mathbb{F}_p(t)$, we have

$$H_K(x^N) = NH_K(x) > 6\omega(x) \geq 2\omega(S) \geq H_K\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right)$$

and similarly

$$H_K(x^N) > H_K\left(1 - \frac{y}{Dy}\frac{Dx}{x}\right).$$

Hence $x^N\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right), x^N\left(1 - \frac{y}{Dy}\frac{Dx}{x}\right) \notin \mathbb{F}_p$ and therefore we can write

$$x^N \left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) = \delta^{p^s} \tag{3.32}$$

$$x^N \left(1 - \frac{y}{Dy}\frac{Dx}{x}\right) = \epsilon^{p^r} \tag{3.33}$$

with $\delta, \epsilon \notin \mathbb{F}_p(t^p)$. Now we claim that for $N > 48$

$$\omega(\delta) \geq \frac{\omega(S)}{4}. \tag{3.34}$$

Indeed suppose for the sake of contradiction that $\omega(\delta) < \frac{\omega(S)}{4}$. Using equation (3.31) we find that there is a finite subset T of M_K with $\omega(T) \geq \frac{\omega(S)}{12}$ such that for all $v \in T$ we have $v(x) \neq 0$ and $v(\delta) = 0$. For such a valuation $v \in T$ we have due to equation (3.32)

$$v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) = -Nv(x) \neq 0.$$

This implies that

$$4\omega(S) \geq 2H_K\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) \geq \sum_{v \in T}\left|v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right)\right| \deg(v) \geq N\frac{\omega(S)}{12}.$$

This is impossible for $N > 48$, so we have established (3.34). For convenience we define for a valuation v and $a, b \notin \mathbb{F}_p(t^p)$

$$f_v(a,b) := \left|v\left(1 - \frac{a}{Da}\frac{Db}{b}\right)\right|,$$

$$\begin{aligned} g_v(x,y,z) := |v(\delta)| + |v(\epsilon)| + f_v(x,y) + f_v(y,x) + \\ + f_v(x,z) + f_v(z,x) + f_v(y,z) + f_v(z,y). \end{aligned}$$

Our next claim is that there is a generic place $v \in M_K$ such that $v(\delta) \neq 0$ and

$$g_v(x,y,z) \leq 480. \tag{3.35}$$

Lemma 3.2.2 with $K = \mathbb{F}_p(t)$ shows that

$$\sum_{v \in M_K} f_v(x,y)\deg v = 2H_K\left(1 - \frac{x}{Dx}\frac{Dy}{y}\right) \leq 2\left(H_K\left(\frac{Dx}{x}\right) + H_K\left(\frac{Dy}{y}\right)\right) \leq 4\omega(S) \tag{3.36}$$

and similarly for the other f_v. Equation (3.29) and equation (3.32) combined with equation (3.36) show that

$$\sum_{\substack{v \in M_K \\ v(\delta)\neq 0 \text{ or } v(1-\delta)\neq 0}} \deg v \leq \omega(S) + \omega\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) + \omega\left(1 - \frac{z}{Dz}\frac{Dy}{y}\right) \leq 9\omega(S).$$

Indeed, if $v(\delta) \neq 0$, we have $v(x) \neq 0$, so $v \in S$, or $v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) \neq 0$, while if $v(1-\delta) \neq 0$, we have $v(y) \neq 0$, hence $v \in S$, or $v\left(1 - \frac{z}{Dz}\frac{Dy}{y}\right) \neq 0$. Similarly, equation (3.30) and equation (3.33) yield

$$\sum_{\substack{v \in M_K \\ v(\epsilon)\neq 0 \text{ or } v(1-\epsilon)\neq 0}} \deg v \leq 9\omega(S).$$

Then Theorem 3.2.3 gives

$$\sum_{v\in M_K} |v(\delta)| \deg v = 2H_K(\delta) \leq 18\omega(S) \tag{3.37}$$

and the same for $|v(\epsilon)|$. Hence we have

$$\sum_{\substack{v\in M_K\\ v(\delta)\neq 0}} g_v(x,y,z)\deg(v) \leq \sum_{v\in M_K} g_v(x,y,z)\deg(v) \leq 60\omega(S)$$

by equation (3.36) and equation (3.37). Note that there are at least two places such that $v(\delta)\neq 0$, so there is at least one generic place v such that $v(\delta)\neq 0$. Hence if $\omega(S)\leq 8$, (3.35) follows immediately. So suppose that $\omega(S)>8$. Using (3.34) we conclude that

$$\begin{aligned}\frac{\omega(S)}{8} \min_{\substack{v\in M_K\\ v(\delta)\neq 0\\ v \text{ generic}}} g_v(x,y,z) &\leq \left(\frac{\omega(S)}{4}-1\right) \min_{\substack{v\in M_K\\ v(\delta)\neq 0\\ v \text{ generic}}} g_v(x,y,z)\\ &\leq (\omega(\delta)-1) \min_{\substack{v\in M_K\\ v(\delta)\neq 0\\ v \text{ generic}}} g_v(x,y,z)\\ &\leq 60\omega(S),\end{aligned}$$

thus proving our claim, i.e. equation (3.35). From now on fix a generic $v\in M_K$ satisfying $v(\delta)\neq 0$ and equation (3.35). Note that equation (3.32) yields the following equality

$$v\left(1-\frac{z}{Dz}\frac{Dx}{x}\right) + Nv(x) = p^s v(\delta). \tag{3.38}$$

We will next show that $s>0$ and $r>0$. Suppose not. Then we may assume that $s=0$ by symmetry considerations. Equation (3.31) and (3.32) give

$$\frac{N\omega(S)}{6} \leq NH_K(x) \leq H_K(\delta) + H_K\left(1-\frac{z}{Dz}\frac{Dx}{x}\right) \leq 11\omega(S),$$

where the last inequality follows from equation (3.36) and equation (3.37). If $N>480$, this gives us the desired contradiction, so henceforth we may assume that $s,r>0$.

If $p>480$, we find that $v(x)\neq 0$ due to equation (3.38) and $s>0$. We claim that

$$v\left(1-\frac{z}{Dz}\frac{Dx}{x}\right) \neq 0. \tag{3.39}$$

Assume the contrary. Then equation (3.38) implies that N divides $v(\delta)\neq 0$, but this is impossible by construction of v and the fact that $N>480$ thus establishing equation (3.39). Finally observe that

$$N \mid p^s v(\delta) - v\left(1-\frac{z}{Dz}\frac{Dx}{x}\right).$$

We now distinguish two cases. First suppose that $v(\delta) > 0$. Then clearly also $v(x) > 0$. If furthermore $v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) < 0$, we get that N divides $ap^s + b$ with $0 < a, b \leq 480$ contrary to our assumptions. Due to equation (3.39) we are left with the case

$$v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) > 0. \tag{3.40}$$

Now comes the crucial observation that $p \nmid v(x)$. Indeed, otherwise we find by equation (3.38)

$$p \mid v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right),$$

which is not possible due to $p > 480$, equation (3.35) and equation (3.40). Hence we deduce for a generic valuation v that $v\left(\frac{Dx}{x}\right) = -1$. Combining this with equation (3.40) again we get that $v(z) \neq 0$. Equation (3.33) gives the equality

$$v\left(1 - \frac{y}{Dy}\frac{Dx}{x}\right) + Nv(x) = p^r v(\epsilon).$$

Recall that $v(x) > 0$, hence $v(\epsilon) > 0$. Using equation (3.30) and equation (3.33), we get

$$z^N\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) = (1-\epsilon)^{p^r}.$$

Since $v(1-\epsilon) = 0$, this shows

$$v\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) + Nv(z) = 0,$$

which is a contradiction for $N > 480$.

We still need to treat the case $v(\delta) < 0$. In that case we find that $v(x) < 0$ and $v\left(1 - \frac{z}{Dz}\frac{Dx}{x}\right) < 0$. Similarly as before we can show that this implies $p \mid v(z)$ for a generic valuation v. We will use equation (3.30) and equation (3.33) once more to deduce that

$$z^N\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) = (1-\epsilon)^{p^r}.$$

Since $v(x) < 0$ implies that $v(\epsilon) < 0$, we find that

$$v\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) + Nv(z) = p^r v(1-\epsilon) = p^r v(\epsilon). \tag{3.41}$$

Combining (3.41) with $p \mid v(z)$ we get that

$$p \mid v\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right).$$

If $p > 480$, then (3.35) implies that $v\left(1 - \frac{y}{Dy}\frac{Dz}{z}\right) = 0$. Hence (3.41) gives $N \mid v(\epsilon)$. Using (3.35) and $N > 480$ once more we conclude that $v(\epsilon) = 0$, which is the desired contradiction.

3.6 Curves inside Fermat surfaces

The goal of this section is to show that Theorem 3.1.4 becomes false if we allow x, y, z, x/y, x/z or y/z to be in $\mathbb{F}_p(t^p)$. By symmetry it suffices to do this in the case x or y/z in $\mathbb{F}_p(t^p)$. We will do this by exhibiting explicit curves inside the Fermat surface.

Let us start by allowing $y/z \in \mathbb{F}_p(t^p)$. We can rewrite

$$x^N + y^N + z^N = 1$$

as

$$\frac{1}{1-x^N} y^N + \frac{1}{1-x^N} z^N = 1.$$

Then if N is odd, we have

$$\frac{1}{1-x^N} y^N + \frac{-x^N}{1-x^N} \frac{(-z)^N}{x^N} = 1.$$

The key point is that we can now put $\alpha := \frac{1}{1-x^N}$, $\tilde{z} = \frac{-z}{x}$, after which the last equation can be rewritten as

$$\alpha y^N + (1-\alpha)\tilde{z}^N = 1. \tag{3.42}$$

But it is rather straightforward to find solutions to this last equation. Indeed, we know that $N \mid p^k - 1$ for some $k > 0$. For such a k we put

$$y := \alpha^{\frac{p^k-1}{N}}, \tilde{z} := (1-\alpha)^{\frac{p^k-1}{N}},$$

and one easily verifies that y and $\tilde{z}$ satisfy (3.42). Going back to our original variables x, y and z we get that

$$y := \left(\frac{1}{1-x^N}\right)^{\frac{p^k-1}{N}}, z := -x\left(\frac{-x^N}{1-x^N}\right)^{\frac{p^k-1}{N}}.$$

There are two important remarks to make about the above construction. First of all, it is easily verified that $y/z \in \mathbb{F}_p(t^p)$ as we claimed. Secondly, we used that N is odd during our construction. However, we only need that -1 is an N-th power in $\mathbb{F}_p^*$.

Now suppose that $x \in \mathbb{F}_p(t^p)$. For simplicity we will again assume that N is odd. Then from the equation

$$x^N + y^N + z^N = 1$$

we find that

$$\left(\frac{1}{z}\right)^N + \left(\frac{-x}{z}\right)^N + \left(\frac{-y}{z}\right)^N = 1.$$

After putting $\tilde{x} = \frac{-y}{z}$, $\tilde{y} = \frac{-x}{z}$ and $\tilde{z} = \frac{1}{z}$ we get that

$$\tilde{x}^N + \tilde{y}^N + \tilde{z}^N = 1$$

with $\frac{\tilde{y}}{\tilde{z}} = -x \in \mathbb{F}_p(t^p)$. Hence we can apply the previous construction.

Finally we will explain why we need the condition that N is $(480, p)$-good. If $N = p^r + 1$ for some $r \geq 0$, it is possible to write down non-trivial lines on the Fermat surface, see Section 5.1-5.4 of [63]. It turns out that our method is unable to distinguish between the case $N = p^r + 1$ and $N = ap^r + b$ with $0 < a, b$ small. This may seem strange at first, but it is in fact quite natural.

Indeed, let us compare this with the situation in characteristic 0. In this case it follows from the work of Voloch [77] that for N sufficiently large the equation

$$x^N + y^N + z^N = 1$$

has no non-constant solutions $x, y, z \in \mathbb{C}(t)$. In fact, this is a rather easy consequence from his abc Theorem. However, it is a more difficult task to find the smallest N using abc Theorems, see for example [13]. Our Theorem 3.1.4 is also based on abc type arguments and for this reason it should not be surprising that we can not distinguish between the case $N = p^r + 1$, giving unirational surfaces [63], and $N = ap^r + b$ with $0 < a, b$ small.

Thus, morally, the notion of N being $(480, p)$-good in Theorem 3.6 can be interpreted as saying that N is "far enough" from an exponent that gives a unirational surface. In the proof we use this condition when we analyze the two dimensional Frobenius families. It is therefore instructive to notice here that there is a partial converse. Namely, we can use the description given at the beginning of Section 3.4 to produce non-trivial rational curves on Fermat surfaces. We will assume $p \equiv 1 \mod 4$ for simplicity: a similar computation can be carried out for the case $p \equiv 3 \mod 4$.

We will use the notation of Section 3.4. Rename $\tilde{\alpha_1} = \frac{\alpha_1}{\alpha_3}$ and $\tilde{\alpha_2} = \frac{\alpha_2}{\alpha_3}$. Choose $\tilde{\alpha_1}, \tilde{\alpha_2} \neq 0$ such that

$$\tilde{\alpha_1}^2 + \tilde{\alpha_2}^2 = -1$$

and put $\lambda_1 = i\tilde{\alpha_2}$ and $\lambda_2 = i\tilde{\alpha_1}$, where i is an element of $\mathbb{F}_p$ such that $i^2 = -1$. We further impose the conditions

$$u_1 = v_1, u_2 = v_2, u_3 = v_3.$$

With these choices, one can check that all the relevant equations in Section 3.4 are satisfied for $(v_1, v_2, v_3) = (\tilde{\alpha_1}t - i\tilde{\alpha_2}, \tilde{\alpha_2}t + i\tilde{\alpha_1}, t)$. Thus, since all the implications at the beginning of 3.4 are reversible, one deduces that the line $(\tilde{\alpha_1}t - i\tilde{\alpha_2}, \tilde{\alpha_2}t + i\tilde{\alpha_1}, t)$ is contained in *all* Fermat surfaces $x^{p^s+1} + y^{p^s+1} + z^{p^s+1} = 1$. Alternatively, one may directly verify that this yields lines on Fermat surfaces.

We conclude by remarking that the height bound in Theorem 3.1.1 *can not* be improved to a *linear* height bound in $\omega(S)$. Indeed, this follows easily by using the curves we constructed at the beginning of this section. A natural question is whether the quadratic dependency on $\omega(S)$ is sharp.

3.7 Acknowledgements

We thank Jan-Hendrik Evertse for giving us this problem, useful discussions and proof-reading. We would also like to thank Hendrik Lenstra and Ronald van Luijk for useful discussions. Finally we much appreciate the valuable remarks of the anonymous referee, which greatly improved the readability of the chapter.