TWISTS OF ELLIPTIC CURVES OVER FUNCTION FIELDS WITH A LARGE SET OF INTEGRAL POINTS

RICARDO P. CONCEIÇÃO

Abstract. For $q \equiv 3 \mod 4$, we show that there are quadratic twists of supersingular elliptic curves with an arbitrarily large set of separable $\infty$-integral points over $\mathbb{F}_q(t)$. We also show that the same holds true if we consider cubic twists of $y^2 = x^3 + 1$ in the supersingular case, i.e., $q \equiv 2 \mod 3$.

These examples allow us to show that the conjecture of Lang-Vojta concerning the behavior of integral points in varieties of log-general type cannot be readily transported to the function field case. Also for $q \equiv 2 \mod 3$ and $q \equiv 3 \mod 4$ they provide examples of elliptic curves over $\mathbb{F}_q(t)$ with an explicit set of linearly independent points with an arbitrarily large size. Finally, we will use them to construct quadratic and cubic function fields with arbitrarily large $m$-class rank, for $m$ dividing $q + 1$.

Contents

1. Introduction 2
   1.1. Uniformity of Integral Points 2
   1.2. The case of function fields 3
   1.3. Main Results 4
2. Twists with a large set of integral points 6
   2.1. Obtaining multisections on Elliptic surfaces 6
   2.2. Proof of the Main Theorem 10
   2.3. Quadratic Twists 13
   2.4. Cubic and Quartic Twists 16
3. Lang-Vojta conjecture 18
4. Explicit sets of linearly independent 20
5. Function fields with large $m$-class rank 22
Acknowledgments 22
References 23

Date: May 2009.
1. Introduction

1.1. Uniformity of Integral Points. Throughout this section we will let \( K \) be a number field and let \( \mathcal{O}_{K,S} \) be the ring of \( S \)-integers, where \( S \) is a finite set of places of \( K \) containing the archimedian places.

A famous finitude result in Arithmetic geometry is the following theorem from 1928:

**Theorem 1.1** (Siegel). Suppose \( E : y^2 = x^3 + ax + b \) is an elliptic curve, \( a, b \in \mathcal{O}_S \). Then the set of \( S \)-integral points of \( E \) is finite.

Inspired by the work of L. Caporaso, J. Harry and B. Mazur [CHM97], D. Abramovich [Abr97] asked if there could exist a universal constant that could bound the number of \( S \)-integral points of an elliptic curve \( E \), independent of the elliptic curve. As he pointed out, this cannot be a true statement: pick any elliptic curve with an arbitrary number of rational points, make a change of coordinates that will “clean denominators” of the rational points and obtain an arbitrary number of \( S \)-integral points. By doing so, you are changing the integral model, and it is natural to ask whether some kind of uniformity on the number of integral point is true if we restrict the model in some way. In [Abr97], D. Abramovich proves that, under the assumption of a conjecture of Lang and Vojta, the following uniformity result holds:

**Theorem 1.2** (Uniformity of \( S \)-integral points on quadratic twists). Let \( y^2 = x^3 + Ax + B \) be an elliptic curve where \( A \) and \( B \) are \( S \)-integers in a number field \( K \). Suppose the Lang-Vojta conjecture is true over \( K \). Then for any square-free \( S \)-integer \( d \), the number of \( S \)-integral points in the quadratic twist \( dy^2 = x^3 + Ax + B \) can be bounded independently of \( d \).

The Lang-Vojta conjecture is a generalization of Siegel’s theorem for varieties of dimension greater than 1 and, if true, it imposes some restriction on the set of integral points on varieties of “complicated geometry”. More precisely, let \( X \) be a variety of log-general type (see Section 3 for a definition) defined over a number field \( K \) and let \( X \) be any model of \( X \) over \( \mathcal{O}_{K,S} \), then:

**Conjecture 1.3** (Lang-Vojta). The set \( X(\mathcal{O}_{K,S}) \) of \( S \)-integral points is not Zariski dense in \( X \).

In this paper we will show that a statement analogous to Theorem 1.2 holds if one replace a number field \( K \) by \( \mathbb{F}_q(t) \) and \( S \)-integral points by points with coordinates in \( \mathbb{F}_q[t] \). Ultimately, see Section 1.3, we will construct an example to prove that uniformity of integral points on twists of elliptic curves cannot hold. This contradiction lead us to conclude that one needs to be careful when considering the Lang-Vojta conjecture for function fields. But before doing so, we need to address some subtleties that are intrinsic to function fields of positive characteristic. This will be done in the next subsection.
1.2. The case of function fields. Let us start with a definition:

**Definition 1.4.** Let $E$ be an elliptic curve defined over $\mathbb{F}_q(t)$ by a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. We will say that a point $(F(t), G(t))$ in $E(\mathbb{F}_q(t))$ is an \(\infty\)-integral point of $E$ if $F = F(t)$ and $G = G(t)$ are polynomials over $\mathbb{F}_q$.

In this situation a literal translation of Siegel’s theorem does not hold: it is no longer true that for each $d \in \mathbb{F}_q[t]$ the elliptic curve $E_d : dy^2 = f(x)$ has a finite set of $\infty$-integral points, with $f(x)$ a cubic polynomial over $\mathbb{F}_q$. Indeed, if $(x, y)$ is a point in $E_d$ with $x, y \in \mathbb{F}_q[t]$ then $\{(x^{q^i}, d^{\frac{q^{2i}+1}{2}}y^{q^i}) : i \in \mathbb{N}\}$ is an infinite set of points in $E_d$ such that the coordinates are polynomials over $\mathbb{F}_q$.

As we will show below, this is the set of orbits of an endomorphism of $E_d$ of infinite order. Such an endomorphism is not inherent to the elliptic curves $E_d$ – we will show that any isotrivial elliptic curve over $\mathbb{F}_q(C)$, the function field of a curve $C/\mathbb{F}_q$, also possesses an endomorphism of infinite order.

**Definition 1.5.** An elliptic curve $E$ defined over $\mathbb{F}_q(C)$ is isotrivial, if it is isomorphic to an elliptic curve $E_1$ defined over $\mathbb{F}_q$ after some finite extension of $\mathbb{F}_q(C)$.

Let $E_1/\mathbb{F}_q$ and $\phi : E \rightarrow E_1$ be an elliptic curve and an isomorphism given by the isotriviality of $E$. The elliptic curve $E_1$ possesses the Frobenius endomorphism $\Phi$ defined by:

$$(x, y) \mapsto (x^q, y^q).$$

This endomorphism will induce an endomorphism $\phi^{-1} \circ \Phi \circ \phi : E \rightarrow E$ which we will also denote by $\Phi$ and call it the Frobenius endomorphism of $E$. The set $\{\Phi^i(P) : i \in \mathbb{N}\}$ will be called the Frobenius orbit of the point $P \in E$. It is not hard to see that this is always an infinite set.

In the particular case that $E = E_d$ and $E_1 : y^2 = f(x)$, we have the isomorphism $\phi(x, y) = (x, yd^{1/2})$ defined over $\mathbb{F}_q(s, t)$ with $s^2 = d(t)$. The Frobenius endomorphism of $E_d$ is $\Phi(x, y) = (x^q, y^q d^{\frac{q^2+1}{2}})$ and the set

$$\{(x^{q^i}, d^{\frac{q^{2i}+1}{2}}y^{q^i}) : i \in \mathbb{N}\}$$

is indeed the orbit set of an endomorphism.

We should also notice that if $P$ is an $\infty$-integral point in an isotrivial elliptic curve $E$, then $\Phi(P)$ does not need to be a point with polynomial coordinates. In fact, let $d \in \mathbb{F}_q[t]$ and consider the elliptic curve $E' : y^2 = x^3 + d$. Then $\phi(x, y) = (xd^{-1/3}, yd^{-1/2})$ is an isomorphism between $E'$ and $y^2 = x^3 + 1$. The Frobenius endomorphism is then given by $\Phi(x, y) = (x^{q^i}d^{-\frac{q^i+1}{3}}, y^q d^{-\frac{q^i+1}{2}})$.

Therefore the Frobenius orbit of an $\infty$-integral point may or may not contain an infinite number of $\infty$-integral points. In any case, one can always salvage Siegel’s theorem by considering Frobenius orbits instead of just integral points; that is, in any isotrivial elliptic curve the number of Frobenius
orbits of an infinite integral point is finite. This can be made more precise by the following definition:

**Definition 1.6.** A non-constant point $P$ in an isotrivial elliptic curve $E/\mathbb{F}_q(C)$ is said to be *separable* if it is not contained in the Frobenius orbit of any other point of $E$.

**Remark 1.7.** Let $d, f \in \mathbb{F}_q[t]$. Suppose $P = (x_0, y_0)$ is a point in the quadratic twist $dy^2 = f(x)$. Then $P$ is separable if, and only if, $x_0' \neq 0$ (the prime will generally denote the formal derivative of an element in $\mathbb{F}_q(t)$).

**Theorem 1.8.** (Isotrivial Siegel’s Theorem) For any isotrivial elliptic curve, the set of separable infinite integral points is finite.

**Proof.** See for instance section 7.3 of [Mas84], or Lemma 2.15, for the special case of quadratic twists. □

In this setting, the Lang-Vojta conjecture should read:

**Conjecture 1.9** (Lang-Vojta Conjecture over $\mathbb{F}_q(t)$). Let $X$ be a variety of log-general type defined over $\mathbb{F}_q(t)$ and $X$ be any model of $X$ over $\mathbb{F}_q[t]$. The set of separable infinite integral points in $X$ is not Zariski dense.

This conjecture also provides some sort of uniformity statement over function fields:

**Theorem 1.10** (Uniformity of separable infinite integral points on quadratic twists). Let $y^2 = x^3 + Ax + B$ be an elliptic curve where $A$ and $B$ are in $\mathbb{F}_q[t]$. Suppose the Lang-Vojta conjecture is true over $\mathbb{F}_q(t)$. Then for any square-free $d \in \mathbb{F}_q[t]$, the number of separable infinite integral points on the twists $dy^2 = x^3 + Ax + B$ can be bounded independently of $d$.

and

**Theorem 1.11** (Uniformity of separable infinite integral points on cubic twists). Let $d$ be a cube-free polynomial over $\mathbb{F}_q$ and let $X$ denote the fiber over $d$ of the surface $X$ defined by $dx^3 = y^2 - y$. If the Lang-Vojta’s conjecture is true over function fields, then there exists a positive number $N$ such that $|X_d(\mathbb{F}_q[t])| \leq N$ for $d \in \mathbb{F}_q[t]\setminus D$, where $D$ is a finite set and $X_d(\mathbb{F}_q[t])$ denotes the set of separable infinite integral points of $X_d$.

Both theorems will be proved in Section 3.

1.3. **Main Results.** As hinted in the previous section, we can find examples of quadratic and cubic twists of elliptic curves containing an arbitrarily large set of separable infinite integral points. It will be proved in Section 2 that:

**Theorem 1.12** (Main Theorem). Let $q \equiv 3 \mod 4$. Then for every odd divisor $k$ of $n$, there exists a separable infinite integral point $Q_k \in E_{t^n - t}(\mathbb{F}_q(t))$ on the curve $E_{t^n - t} : (t^n - t)y^2 = x^3 - x$. The same is true for the elliptic curve $y^2 - y = (t^n - t)x^3$, when $q \equiv 2 \mod 3$. 
An immediate consequence of Theorems 1.10 and 1.11 and this result is:

**Corollary 1.13.** The Lang-Vojta conjecture over \( \mathbb{F}_q(t) \) does not hold whenever \( q \equiv 3 \mod 4 \) or \( q \equiv 2 \mod 3 \).

The twists \((t^{q^n} - t)y^2 = x^3 - x\) considered in Theorem 1.12 are of a very special kind: up to isomorphism over \( \mathbb{F}_{q^n} \), they are the only twists of constant elliptic curves by \( t^{q^n} - t \) that can contain separable \( \infty \)-integral points of “small” height. This will be proved in Section 2.3.

**Theorem 1.14.** Let \( f(x) \) be a polynomial defined over \( \mathbb{F}_{q^n} \). The elliptic curve \((t^{q^n} - t)y^2 = f(x)\) has an \( \infty \)-integral point \((F(t), G(t))\) defined over \( \mathbb{F}_{q^n} \) satisfying \( F'(t) \neq 0 \) and \( 2 \deg F(t) \leq q^n - 1 \) if and only if \( p \equiv 3 \mod 4 \) and \( y^2 = f(x) \) is isomorphic over \( \mathbb{F}_{q^n} \) to \( ay^2 = x^3 - x \), for some \( a \in \mathbb{F}_{q^n} \).

The rest of the paper is dedicated to prove two other consequences of our main theorem: one related to the rank of elliptic curves and the other related to the \( m \)-class rank of quadratic and cubic function fields. We will prove that both numbers can be arbitrarily large.

For the rank of elliptic curves over function fields, this has been known since the late 60’s, when Shafarevic and Tate [T67] proved that there are quadratic twists of supersingular elliptic curves with arbitrarily high rank over \( \mathbb{F}_p(t) \), with \( p > 2 \). This result served as an evidence that the same should hold over number fields. Their construction had one drawback though: it relied on isotrivial elliptic curves, a notion that seems not to exist in the number field case.

For ordinary and non-isotrivial elliptic curves only recently we have seen some breakthroughs: In 2002 Ulmer [Ulm02] proved the existence of non-isotrivial elliptic curves with arbitrarily large rank over \( \mathbb{F}_p(t) \), for any prime \( p \). And in 2006, Diem & Scholten [DS07] proved the unboundedness of the rank over \( \mathbb{F}_p(x) \) for ordinary elliptic curve with constant \( j \)-invariant.

The examples constructed in Theorem 1.12 can be used to reprove the results of [T67]: the considered elliptic curves are supersingular isotrivial elliptic curves with arbitrarily large rank over function fields. One advantage of our method over theirs is that we explicitly produce a large set of linearly independent points. This advantage still holds when we compare our method with the previous methods [T67], [Elk94], [Ulm02], [BDS04], [DS07]: they do not provide explicitly the generators for the Mordell-Weil group or even a large set of linearly independent points. This will be proven in Section 4 where we prove that the points obtained in Theorem 1.12 are linearly independent.

Now let us consider the \( m \)-class rank of function fields. Recall that a global field \( K \) is a finite extension of either \( \mathbb{F}_q(t) \) or \( \mathbb{Q} \). Denote by \( \mathcal{O}_K \) the integral closure of \( \mathbb{Z} \) or \( \mathbb{F}_q[t] \) in the extension \( K/k \), \( k = \mathbb{Q} \) or \( k = \mathbb{F}_q(t) \),

\footnote{Recently, on a personal communication D. Ulmer provided me with an example of a non-isotrivial elliptic curves with an explicit and arbitrarily large set of linearly independent points. His construction is based on the method developed by L. Berger [Ber08].}
respectively. To this Dedekind ring, we can associate a finite abelian group, the ideal class group \( \text{Cl}(\mathcal{O}_K) \). The cardinality of this group is called the class number of \( K \), while the number of independent elements of order \( m \) in \( \text{Cl}(\mathcal{O}_K) \) is said to be the \( m \)-class rank of \( K \).

A lot has been written about the class number and the \( m \)-class number of a quadratic extension of a global field, and their history dates back to Gauss, as should be no surprise. One can prove that given a natural number \( n \), there are a finite number of imaginary quadratic number fields \( K \) with class number \( n \); and that this number grows as the absolute value of the discriminant \( K \) grows; see [Gol85] for more on the rich history and bibliography of this classic problem.

On the \( m \)-rank side, Peng [Pen03] shows that 2-class rank of quadratic extension of global fields can be arbitrarily large. For an odd \( m > 1 \) very little is known about the \( m \)-class rank, and recently Siman Wong considered the question of whether there are quadratic function fields \( K/\mathbb{F}_q(t) \) with arbitrarily large \( m \)-class rank. Our examples provide a positive answer to such question for \( m \) a divisor of \( q + 1 \). In fact, in Section 5 we manage to prove a little bit more:

**Theorem 1.15.** Let \( m \) be a positive integer divisor of \( q + 1 \). When \( q \equiv 3 \mod 4 \), the function field of the hyperelliptic curve \( s^2 = t^{q^m} - t \) has arbitrarily large \( m \)-class rank. When \( q \equiv 2 \mod 3 \), the function field of the curve \( s^3 = t^{q^m} - t \) has arbitrarily large \( m \)-class rank.

2. **Twists with a large set of integral points**

Recall that our objective is to construct quadratic twists of elliptic curves containing an arbitrary number of \( \infty \)-integral points. In the case of rational points on elliptic curves, the maximal number of linearly independent points is conjecturally linked to a well-known analytic function. This analytic function has been used several times to prove the unboundedness of the rank over function field. Unlike this case, the only way to obtain a large set of integral points is by exhibiting them explicitly. This is what we will be doing next.

To obtain a single point, we will use a procedure due to T. Shioda to construct a dominant rational map from a Fermat surface to the associated elliptic surface. This construction has been used by Ulmer [Ulm02, Ulm07] to show that the BSD conjecture holds for the Jacobian variety of some curves and also by Shioda [Shi91] to construct lattices with dense sphere packing in certain dimensions.

2.1. **Obtaining multisections on Elliptic surfaces.** We will consider surfaces over an arbitrary field \( k \) defined by four monomials

\[
X_A = X_A(c_0, c_1, c_2, c_3) : \sum_{i=0}^{3} c_i x_0^{a_{i0}} x_1^{a_{i1}} x_2^{a_{i2}} x_3^{a_{i3}} = 0
\]
where $A = (a_{ij})_{0 \leq i, j \leq 3}$ is a $4 \times 4$ matrix with integral coefficients. Following Shioda \cite{Shi86} we will call $X_A$ a Delsarte surface with matrix $A$, when it satisfies

- $X_A$ is irreducible;
- $\det A \neq 0$ in $k$;

Notice that the surface $F_d$ defined by

$$c_0 u_0^d + c_1 u_1^d + c_2 u_2^d + c_3 u_3^d = 0$$

is a Delsarte surface with matrix $dI_4$, where $I_4$ is the identity matrix of dimension 4. In this case we will denote $X_{dI_4}$ simply by $X_d$ and we will refer to it as a Fermat surface of degree $d$.

For a general Delsarte surface $X_A = X_A(c_0, c_1, c_2, c_3)$, $A^{-1}$ is a $4 \times 4$ matrix with rational entries. If $X_C = X_C(c_0, c_1, c_2, c_3)$ is another Delsarte surface then there exists a smallest integer $d$ such that $B = dA^{-1}C = (b_{ij})_{0 \leq i, j \leq 3}$ has integer entries. This easily implies the existence of a dominant rational map $\phi : X_{dC} \rightarrow X_A$ defined by

$$(u_0, u_1, u_2, u_3) \mapsto \left( \prod_{j=0}^{3} u_j^{b_{0j}}, \prod_{j=0}^{3} u_j^{b_{1j}}, \prod_{j=0}^{3} u_j^{b_{2j}}, \prod_{j=0}^{3} u_j^{b_{3j}} \right).$$

In particular, for any Delsarte surface $X_A$, there exists an integer $d$, and a rational dominant map $X_d \rightarrow X_A$ from a Fermat surface of degree $d$.

**Definition 2.1.** Let $E$ be a smooth projective algebraic surface defined over a field $k$. An elliptic fibration is a $k$-morphism $\pi : E \rightarrow C$ onto a smooth projective irreducible curve $C/k$ with generic fiber a smooth curve $E$ of genus 1. Additionally, we require that the fibration $\pi$ contains at least one section, that is, a $k$-rational map $O : C \rightarrow E$ such that $\pi \circ O : C \rightarrow C$ is the identity map. A multisection $M$ of an elliptic fibration $\pi : E \rightarrow C$ is an irreducible subvariety $M \subset E$ such that the projection map $\pi : M \rightarrow C$ has non-zero degree.

Now let us show how the described rational map can sometimes be used to construct non-constant sections on a Delsarte surface with an elliptic fibration over $\mathbb{P}^1$. For simplicity, let us assume that $\text{char}(k) \neq 2, 3$.

**Example 2.2.** Let $E_{d-1} : (t^d - t)y^{2}z = x^{3} - xz^{2}$, with $d$ a positive integer. This is a Delsarte Surface whose associated matrix $A$ is given by

$$
\begin{pmatrix}
0 & 2 & 1 & d \\
0 & 2 & 1 & 1 \\
3 & 0 & 0 & 0 \\
1 & 0 & 2 & 0
\end{pmatrix}
$$

The procedure laid out before returns the following rational map

$$(X_0, X_1, X_2, X_3) \mapsto \left[ X_0 X_2^{d-1} X_3^{-d} : X_1^d X_2^{d-1} : X_0 X_3^{3(d-1)} \right], \frac{X_0^2}{X_1}$$
from the Fermat surface \( F_{2(d-1)} : X_0^{2(d-1)} - X_1^{2(d-1)} = X_2^{2(d-1)} - X_3^{2(d-1)} \) to \( E_{d-t} \). The image through this map of the line \((t, 1, t, 1)\) contained in \( F_{2(d-1)} \) is the multisection \([t^{d-1} : t^{d-3} : 1] \). If \( d \equiv 3 \mod 4 \), then the substitution \( u = t^2 \) will yield the section \([u^{d-2} : u^{d-3} : 1], u\).

**Example 2.3.** Let \( E_{3, d-t} \) be the surface \( y^2 z - y z^2 = (t^d - t)x^3 \). In this case, we obtain the rational map

\[
(X_0, X_1, X_2, X_3) \mapsto \left( [X_0^{d-1} X_1^{d-1} X_2^3 : X_0^{3(d-1)} X_1 X_2^3], \frac{X_3^3}{X_3^3} \right)
\]

from the Fermat surface

\[
F_{2(d-1)} : X_0^{2(d-1)} - X_1^{2(d-1)} = X_2^{2(d-1)} - X_3^{2(d-1)}
\]

to \( E_{3, d-t} \). The obvious rational curves on \( F_{2(d-1)} \) are \((1, 1, t, t), (t, t, 1, t), (t, 1, t, t)\) and \((1, t, 1, t)\). Under this rational map, the first two lines do not yield any multisection on \( E_{3, d-t} \), while the lines \((t, 1, t, t)\) and \((1, t, 1, t)\) produce the same multisection \([t^{d-2} : t^{3(d-1)} : 1] \). When \( d \equiv 2 \mod 3 \), the substitution \( u = t^3 \) transforms this multisection into the section \([u^{d-2} : u^{d-3} : 1], u\).

**Example 2.4.** Let \( d \) and \( s \) be positive even integers. Consider the Delsarte surface \( X_D(1, 1, -1, -1) : X_0^s + X_1^s - X_2^d - X_3^d = 0 \) where

\[
D = \begin{pmatrix}
  s & 0 & 0 & 0 \\
  0 & s & 0 & 0 \\
  0 & 0 & d & 0 \\
  0 & 0 & 0 & d
\end{pmatrix}.
\]

Then there exists a rational map \( X_{6D}(1, 1, -1, -1) \rightarrow E_{3, d+1} \)

\[
(X_0, X_1, X_2, X_3) \mapsto \left( [X_1^{2s} X_3^d : X_0^{3s} : X_3^{3d}], \frac{X_0^3}{X_3^3} \right)
\]

where \( E_{3, d+1} \) is the Delsarte elliptic surface defined by \( y^2 z = -x^3 + (t^d + 1)z^3 \).

Suppose \( r = d/s \) is an integer. The image of the curve \((t^r, 1, 1, t) \subset X_{6D} \) under this rational map is the multisection \([1 : t^{3d} : 1] \) \( \subset E_{3, d+1} \) and the substitution \( u = t^6 \) produces the section \([1 : u^d : 1], u\). Another trivial rational curve on \( X_{6D} \) is \((1, t^r, t, 1)\) and associated to it is the multisection \(([t^{2d} : 1 : 1], t^6) \) of \( E_{3, d+1} \) which can be made into the section \([u^{d} : 1 : 1], u\), if \( d \equiv 0 \mod 3 \). The other two trivial rational curves on \( X_{6D} \) are \((t^r, 1, 1, t)\) and \((1, t^r, t, 1)\), but they do not yield any new section.

**Example 2.5.** Let \( d, s \) and \( D \) be as in the previous example. Let \( E_{4, d+1} \) be the Delsarte elliptic surface \( y^2 z = -x^3 + (t^d + 1)x z^2 \). The map

\[
(X_0, X_1, X_2, X_3) \mapsto \left( [X_1^4 X_3^d : X_0^s X_1^4 : X_3^{4d}], \frac{X_0^2}{X_3^2} \right)
\]
is a rational map from $X_{2d} : X_0^{2d} + X_1^{2d} - X_2^{2d} - X_3^{2d} = 0$ to $E_{4t^d + 1}$. Once more, if $r = d/s$ is an integer, then $(t^r, 1, t, 1)$, $(1, t^r, t, 1)$, $(t^r, 1, 1, t)$ and $(t^r, 1, 1, t)$ are curves on $X_{2d}$. As before, from these curves we obtain the multisections $([1 : t^d : 1], t^2)$ and $([t^d : t^d : 1], t^2)$. The first multisection gives the section $([1 : t^d : 1], t)$, and if $d \equiv 0 \mod 4$, we obtain the section $([t^d : t^d : 1], t)$ from the second.

**Example 2.6.** For the elliptic surface $zy^2 = x^3 + (t^d - t)xz^2$, where $d$ is an odd positive integer, this procedure generates the rational map from the Fermat surface $X_0^{4d-1} - X_1^{4d-1} = X_2^{4d-1} - X_3^{4d-1}$

$$(X_0, X_1, X_2, X_3) \mapsto \left( \left[ X_1^{2d-1}X_2^d : X_0^{2d-1}X_1^{d-1}X_2^2 : X_3^{3d} \right], \frac{X_2}{X_3} \right)$$

and the multisections $([t^2 : t^{2d+1} : 1], t^4)$ and $([\zeta^{2d-1}t^{2d} : \zeta^{3d-1}t^{d+2} : 1], t^4)$, where $\zeta^{4d-1} = -1$. In this case, we cannot associate a section to this multisection as we did before, since the odd numbers $2d + 1$ and $d + 2$ are never divisible by 4.

**Example 2.7.** The Delsarte elliptic surface $(t^d - t)y^2 = x^3 - 1$ is similar to the previous example in the sense that the multisections $([t^{2d-1} : t^{-3} : 1], t^6)$ and $([t^{2d-1} : \zeta^{3d-1}t^{-3d-1} : 1], t^6)$, $\zeta^{6d-1} = -1$, do not produce any section. Notice also that this is the first case where the multisection is given by a rational function instead of a polynomial. For the convenience of the reader, let us record the rational map from the Fermat surface $X_0^{6d-1} - X_1^{6d-1} = X_2^{6d-1} - X_3^{6d-1}$

$$(X_0, X_1, X_2, X_3) \mapsto \left( \left[ X_0^{2d}X_2^{d-1}X_3^{-d} : X_1^{3d} : X_0X_3^{3d-1} \right], \frac{X_2}{X_3} \right).$$

Since all our theorems are stated in terms of the generic fiber of the elliptic fibration, it will be convenient to rewrite these examples in a more curve-theoretical way.

- **Example 2.2.** When $d \equiv 3 \mod 4$, $(t^{d+1}, t^{d+1})$ is a $\infty$-integral point on the elliptic curve $E_{t^d - t} : (t^d - t)y^2 = x^3 - x$

- **Example 2.3.** If $d \equiv 2 \mod 3$, then the elliptic curve $E_{3t^d - t} : y^2 - y = (t^d - t)x^3$ has at least the point $(t^{d-2}, t^{d-1})$ with polynomial coordinates.

- **Example 2.4.** When $d$ is even, $(-1, t^{d/2})$ and $(t^{d/2}, 1)$ are $\infty$-integral points on the elliptic curve $y^2 = x^3 + (t^d + 1)$, the latter only when $d \equiv 0 \mod 3$.

- **Example 2.5.** $(-t^{d/2}, t^{d/4})$ belongs to the elliptic curve $y^2 = x^3 - (t^d + 1)x$, whenever $d \equiv 0 \mod 4$.

These are the curves we will show to have arbitrarily many separable $\infty$-integral points in distinct Frobenius orbits over $F_q(t)$. We achieve this in two different ways: for elliptic curves twisted by $t^q - t$, we will use the fact
that additive polynomials defined over $\mathbb{F}_q$ form a ring under composition isomorphic to $\mathbb{F}_q[t]$. The elliptic curves twisted by $t^{q+1} + 1$ are covered by the Hermitian Fermat surface, which possesses a large automorphism group $PU(4, q)$, the projective unitary group of dimension four.

**Remark 2.8.** Multisections in a fibered surface $S \to C$ becomes sections of $S \otimes_C C' \to C'$ after a suitable finite base extension $C' \to C$. In the case of an elliptic fibered surface $E \to C$, one could try to obtain sections from multisections by using the following procedure: If $E/k(C)$ is the generic fiber of $E \to C$, then $E/k(C')$ will be the generic fiber of $E \otimes_C C' \to C'$. The group $E(k(C'))$ is isomorphic to the group of sections $E(C')$. Therefore for any multisection of $E \to C$, or equivalently, for any point $P \in E(k(C'))$, the trace $\sum_{\sigma \in \text{Gal}(k(C')/k)} P^\sigma$ produces a section of $E \to C$. In the above examples, the trace of the multisection does not yield any new information: a multisection will either be traced down to the zero section or to an integer multiple of the original section.

**Remark 2.9.** In Examples 2.2 - 2.7 the generic fiber of the elliptic surface is a constant elliptic curve of $j$-invariant equals to 0 or 1728 twisted by a polynomial with two monomials. These should explain our choice of notation: $E_{3,t^d-t}$ is a cubic twist by the polynomial $t^d - t$. These examples essentially represent all the isotrivial elliptic curves defined over $k(t)$ that can be written with just four monomials. Indeed, if $E$ is an isotrivial elliptic curve with $j$-invariant different from 0 and 1728, and $\text{char}(k) \neq 2, 3$, then necessarily $E$ is a quadratic twist of a constant elliptic curve by a rational function, so it can be written as $A(t)y^2 = x^3 + ax + b$, where $a, b \in k \setminus \{0\}$ and $A(t)$ is a squarefree polynomial. In order for the later to be written with just four monomials, it would be necessary that $A(t) = t$. For us this is not an interesting case, since this elliptic curve has rank 0 over $k(t)$.

2.2. **Proof of the Main Theorem.** From now on $p$ will denote a rational prime and $q = p^l$, for some natural number $l$.

**Definition 2.10.** An $(\mathbb{F}_q)$-additive polynomial $A(t)$ is a polynomial in $\mathbb{F}_q[t]$ of the form

$$A(t) = \sum_{i=0}^n a_i t^{q^i}.$$  

We will denote the set of all $\mathbb{F}_q$-additive polynomials by $\mathbb{F}_q[F]$.

The reason to denote the set of additive polynomials by $\mathbb{F}_q[F]$ is that an additive polynomial can be seen as an $\mathbb{F}_q$-polynomial in the indeterminate $F$, the $q$-Frobenius map $t \mapsto t^q$. Indeed, start by defining $F^0(t) = t$. We have that the $i$-th self composition of $F$ is the polynomial $F^i(t) = t^{q^i}$, and so an additive polynomial $A(t)$ is the same as a linear combination of powers of Frobenius, $A_0(F) = \sum_{i=0}^n a_i F^i$. Let us recall some trivial facts about rings of prime characteristic $p$ and the Frobenius map.
Lemma 2.11. Let $\alpha, \beta \in \mathbb{F}_q$ and $i, j$ be nonnegative integers. Then

1. $\mathbb{F}^i(\alpha \mathbb{F}^j) = \alpha \mathbb{F}^{i+j}$
2. Let $R$ be a commutative ring of characteristic $p$. Then for any $x, y \in R$, we have $\mathbb{F}^i(x + y) = \mathbb{F}^i(x) + \mathbb{F}^i(y)$.

Proof. This follows easily from the identity $(x + y)^p = x^p + y^p$, true in any commutative ring of characteristic $p$. \hfill $\square$

Corollary 2.12. Let $A(t), B(t) \in \mathbb{F}_q[\mathbb{F}]$ and $\alpha \in \mathbb{F}_q$. Then:

1. $A(t) + B(t) \in \mathbb{F}_q[\mathbb{F}]$;
2. $\alpha A(t) \in \mathbb{F}_q[\mathbb{F}]$;
3. $A(B(t)) \in \mathbb{F}_q[\mathbb{F}]$.

Furthermore, $\mathbb{F}_q[\mathbb{F}]$ can be endowed with a ring structure with multiplication defined by $A(t) \circ B(t) := A(B(t))$ and the association

$$P(t) = \sum_{i=0}^{n} a_i t^i \mapsto P(\mathbb{F}) = \sum_{i=0}^{n} a_i \mathbb{F}^i$$

is an isomorphism between $\mathbb{F}_q[t]$ and $\mathbb{F}_q[\mathbb{F}]$.

Proof. (1) and (2) are trivial. To prove (3), write

$$A(t) = \sum_{i=0}^{n} a_i \mathbb{F}^i = A_0(\mathbb{F})$$

and

$$B(t) = \sum_{j=0}^{m} b_j \mathbb{F}^j = B_0(\mathbb{F})$$

Hence, by the previous lemma

$$A(B(t)) = \sum_{i=0}^{n} a_i \mathbb{F}^i \left( \sum_{j=0}^{m} b_j \mathbb{F}^j \right) = \sum_{i=0}^{n} a_i \left( \sum_{j=0}^{m} \mathbb{F}^i(b_j \mathbb{F}^j) \right)$$

Thus (3) is proved. Associativity is inherited from $\mathbb{F}_q[t]$ and the distribution laws follow from the previous lemma. So $\mathbb{F}_q[\mathbb{F}]$ is a ring. Notice that this equation also proves that $A_0(\mathbb{F}) \circ B_0(\mathbb{F}) = (A_0B_0)(\mathbb{F})$, and so the map $P(t) \mapsto P(\mathbb{F})$ is multiplicative. Hence it is an isomorphism, since it is clearly an additive bijective map. \hfill $\square$

We are ready to prove one of our main results:

Theorem 2.13. Let $q \equiv 3 \mod 4$ and $k_i, i = 1, \ldots, n$, be distinct odd numbers. Suppose $A(t) = A_0(\mathbb{F})$ is an $\mathbb{F}_q$-additive polynomial such that for all $i$, $t^{k_i} - 1$ divides $A_0(t)$. Then the curve $A(t)y^2 = x^3 - x$ contains at least $n$ separable $\infty$-integral. The same is true for the elliptic curve $y^2 - y = A(t)x^3$, when $q \equiv 2 \mod 3$. 
Proof. Under these assumptions we may conclude that \( q^{k_i} \equiv 3 \mod 4 \). Therefore we may use Example 2.2 with \( d = q^{k_i} \) to obtain a point on the twist \((u^{q^{k_i}} - u)y^2 = x^3 - x\), namely \( P_i = (u^{q^{k_i}-1}, u^{q^{k_i}-3}) \).

By assumption for each \( 1 \leq i \leq n \), there exists a polynomial \( B_i(t) \in \mathbb{F}_q[t] \) such that \( A_0(t) = (t^{k_i} - 1)B_i(t) \), and, by Corollary 2.12 this implies the identity:

\[
(2.2) \quad A(t) = B_i(F)^{q^{k_i}} - B_i(F).
\]

Then if we make the substitution \( u = B_i(F) \), we obtain a point \( Q_i = (B_i(F)^{q^{k_i}-1}, B_i(F)^{q^{k_i}-3}) \) on the twist

\[
(B_i(F)^{q^{k_i}} - B_i(F))y^2 = x^3 - x
\]

which is the same as

\[
A(t)y^2 = x^3 - x.
\]

The degree of the first coordinate of \( Q_i \) is \( \frac{q^n-q^{n-k_i}}{2} \), so that \( Q_i \) and \( Q_j \) are distinct points for different indices \( i, j \). Also the derivative of \( B_i(F)^{q^{k_i}-1} \) is clearly different from zero, so we can conclude that these points are in distinct Frobenius orbits.

The second part is proved in the same way. The hypothesis and Example 2.3 give us the polynomial point \((u^{\frac{d-2}{3}}, u^{d-1})\) on the elliptic curve \( y^2 - y = (u^{q^k} - u)x^3 \). Using Equation 2.2 and the substitution \( u = B_i(F) \), we obtain the \( \infty \)-integral point \( S_i = (B_i(F)^{q^{k_i}-2}, B_i(F)^{q^{k_i}-1}) \) on the curve \( y^2 - y = A(t)x^3 \). Observe that for distinct values of \( i \), one would obtain polynomials with different degrees; for instance, the degree of the second coordinate of \( S_i \) is \( q^n - q^{n-k_i} \).

The Frobenius orbit of a rational point \((x, y)\) in \( y^2 - y = A(t)x^3 \) is \( \{(A(t)^{\frac{d-1}{3}}x^{2i}, y^{2i}) : i \in \mathbb{N}\} \). So that if \((x_0, y_0)\) is another point satisfying \( y_0 \neq 0 \), then it will be in a distinct Frobenius orbit than \((x, y)\). The last statement is true for all \( S_i \).

Our Main Theorem is now an easy consequence of this result.

Proof of Main Theorem. The \( \mathbb{F}_q \)-additive polynomial \( A(t) = t^{q^n} - t \) can be written as \( A_0(F) \), where \( A_0(t) = t^n - 1 \). It is well known that \( t^k - 1 \) divides \( A_0(t) \) if and only if \( k \) divides \( n \). Therefore, in the previous theorem we can take \( k_i \) to be the odd divisors of \( n \).

In this particular case, \( B_i(F) \) is given by the trace polynomial from \( q^n \) to \( q^k \):

\[
T_k^n(t) = \sum_{i=0}^{s-1} t^{q^{ki}}.
\]
Remark 2.14. Denote by $\tau_{\text{odd}}(n)$ the number of odd divisors of $n$. Observe that the polynomial $T^n_k$ gives rise to an $\mathbb{F}_q^n$-linear function $T^n_k : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ which happens to be the trace from $\mathbb{F}_q^n$ to $\mathbb{F}_q^q$. Hence the set $\{T^n_k(t + a) : a \in \mathbb{F}_q\}$ contains $q$ distinct elements, if $p$ does not divide $n$. Since $t^{q^n} - t$ is invariant under translations $t + a$, for $a \in \mathbb{F}_q^n$, this shows that $Q_k(t + a)$ will define $q$ distinct points on $E_{\mathbb{F}_q^n}$; proving that these curves have at least $q\tau_{\text{odd}}(n)$ Frobenius orbits of points with $\mathbb{F}_q$-polynomial coordinates. Finally, let us point out that $Q_k(at)$ defines an $\mathbb{F}_q^n$-polynomial point on the curve on $a(t^{q^n} - t)y^2 = x^3 - x$, for every $a \in \mathbb{F}_q^n$.

At first it seems that the above reasoning could also be used to construct arbitrarily many $\infty$-integral points on the the quadratic twist $(t^{q^n} - t)y^2 = x^3 - 1$. Unfortunately, Example 2.7 showed that in this case, our general procedure fails to construct non-constant rational points. This fact, a computer search and Theorem 1.14 lead us to believe that this curve does not have any non-constant polynomial point. We will use the next section to prove Theorem 1.14.

2.3. Quadratic Twists. Let $A(t)$ be a square free polynomial of odd degree $d > 1$ and let $E : y^2 = f(x)$ be an elliptic curve, both defined over a finite field of order $q$. We will denote by $E_A : A(t)y^2 = f(x)$ the quadratic twist of $E$ by $A(t)$, which we view as an elliptic curve defined over $\mathbb{F}_q(t)$.

Lemma 2.15. Suppose $(F, G) = (F(t), G(t))$ is an $\infty$-integral point of $E_A$ satisfying $F'(t) \neq 0$. Then $G(t)$ divides $F(t)$ and $d/3 \leq \deg F < d - 1$.

Proof. An $\infty$-integral points $(F(t), G(t))$ induces an identity on $\mathbb{F}_q[t]$:

\begin{equation}
A(t)G(t)^2 = f(F(t)).
\end{equation}

By equating degrees in this identity we obtain the lower bound on $\deg F$, namely: $d \leq 3 \deg F$. Now by differentiating equation (2.3) we are led to

\begin{equation}
A'(t)G(t)^2 + 2A(t)G(t)G'(t) = F'(t)f'(F(t)).
\end{equation}

Let $\beta$ be a root of $G(t)$ of multiplicity $r$. By (2.3), we have that $(t - \beta)^r$ divides $f(F(t))$, and by (2.4), we conclude that $(t - \beta)^r$ divides $F'(t)f'(F(t))$. Notice that $(t - \beta, f'(F(t))) = 1$, since $f(x)$ has no repeated roots. Hence $(t - \beta)^r$ should divide $F'(t)$ and, as a consequence, $G(t)$ divides $F'(t)$. From that it follows that $\deg G \leq \deg F - 1$.

After equating the degrees in (2.3) and using the last inequality, the upper bound on $\deg F$ is obtained.

Suppose $f(x) = (x - \alpha_0)(x - \alpha_1)(x - \alpha_2)$. If we denote $F(t) - \alpha_i$ by $F_i(t)$, for $i \in \{0, 1, 2\}$, then we will have that $f(F(t)) = F_0(t)F_1(t)F_2(t)$ and $F_i$ is relatively prime to $F_j$, for any pair of distinct $i, j \in \{0, 1, 2\}$. Equating the degrees in (2.3), we obtain that $\deg F_i(t) \equiv d \mod 2$, where $d$ is the degree of $A(t)$, which is assumed to be odd. A closer look at the equation (2.3) shows that $(A(t), F_i(t)) = N_i$, for some non-constant polynomial $N_i(t).$ Therefore
we can write \( F_i(t) = N_i(t)S_i(t)^2 \), for some polynomial \( S_i(t) \). Note that 
\( G(t) = S_0(t)S_1(t)S_2(t) \) and \( A(t) = N_0(t)N_1(t)N_2(t) \).

The above considerations imply that
\[
\{ \alpha_0, \alpha_1, \alpha_2 \} = \{ F(\beta) : \beta \text{ a zero of } A(t) \}
\]
so that if \( A(t) \) is a polynomial splitting completely over \( \mathbb{F}_q \), then we may assume that \( \alpha_i \in \mathbb{F}_q \) and \( F_i \in \mathbb{F}_q[t] \).

**Theorem 2.16.** Suppose \( A(t) \) is a square-free polynomial of odd degree \( d \) that splits completely over \( \mathbb{F}_q \) such that \( A'(t) \equiv \gamma \in \mathbb{F}_q^* \). Let \( E : y^2 = f(x) \) be an elliptic curve defined over \( \mathbb{F}_q \). Suppose \( (F(t), G(t)) \) is an \( \infty \)-integral point of \( E_A \) defined over \( \mathbb{F}_q \) satisfying \( F'(t) \neq 0 \). Then the following three conditions are equivalent:

- (A) \( 2 \deg F(t) \leq d - 1 \);
- (B) \( 2 \deg G(t) \leq \deg F(t) - 1 \);
- (C) \( G(t)^2 = \beta F'(t) \), for some \( \beta \in \mathbb{F}_q^* \).

Furthermore, if one of the above equivalent conditions is true then \( E \) is isomorphic over \( \mathbb{F}_q \) to \( ay^2 = x^3 - x \), for some \( a \in \mathbb{F}_q^* \).

**Proof.** From (2.3), we know that \( d + 2 \deg G(t) = 3 \deg F(t) \), and from this it easily follows that (A) is equivalent to (B). It is also clear that (C) implies (B), so all we need to show is that (B) implies (C).

Let \( s_i = \deg S_i(t) \). Without loss of generality, let us suppose that
\[
s_0 \geq s_1 \geq s_2 \geq 0.
\]

Equation (2.4) now reads (For convenience, we will sometimes drop the \( t \) from the polynomial notation.):
\[
\gamma G^2 + 2N_0N_1N_2S_0S_1S_2(S'_0S_1S_2 + S_0S_1S'_2 + S_0S_1S'_2) = F'(F_0F_1 + F_0F_2 + F_1F_2)
\]
since \( F' = F'_i \). Equivalently,
\[
\gamma G^2 + 2N_0S_0S'_0F_1F_2 + 2N_1S_1S'_1F_0F_2 + 2N_2S_2S'_2F_0F_1 = F'(F_0F_1 + F_0F_2 + F_1F_2).
\]

Let \( \{i, j, k\} = \{0, 1, 2\} \). We have that \( F_iF_j = (\alpha_k - \alpha_i)(\alpha_k - \alpha_j) \mod F_k \),
by definition. If we let \( \beta_k = \frac{(\alpha_k - \alpha_i)(\alpha_k - \alpha_j)}{\gamma} \) then the last equation is equivalent to
\[
G^2 + 2\beta_kN_kS_kS'_k \equiv \beta_kF_k' \mod F_k
\]
and since
\[
F' = F'_i = N'_iS'_i + 2N_iS_iS'_i
\]
we finally get
\[
G^2 \equiv \beta_kN'_iS'_i \mod F_k.
\]

It is clear that \( \deg(N'_iS'_k) < \deg F_k = \deg F \). Therefore if (B) is true, we will get \( \deg G^2 < \deg F \); and ultimately, we will obtain
\[
G^2 = \beta_kN'_iS'_i
\]
for $k \in \{0, 1, 2\}$.

Now consider $\{i, k\} = \{1, 2\}$. Multiplying (2.7) by $\beta_i$ and using (2.8), we obtain

$$\beta_i F' = G^2 + 2\beta_i N_i S_i S'_i.$$

Lemma 2.15 implies that $G$ divides $2\beta_i N_i S_i S'_i$, so

$$S_0 S_k | 2\beta_i N_i S'_i$$

since $(S_0 S_k, N_i) = 1$. This in turn will imply that

$$S_0 S_k | 2\beta_i S'_i.$$

Assume that $S'_i \neq 0$ then

$$s_i \leq s_0 + s_k \leq s_i - 1$$

where the first inequality follows from (2.6). This clear contradiction shows that for $i = 1, 2$, $S'_i = 0$ and $F'_i = N'_i S'_i$. Therefore

$$G^2 = \beta_i N'_i S'_i = \beta_i F'_i = \beta_i F'$$

which proves that (A), (B) and (C) are all equivalent.

To show the second part, let us assume that either one of the equivalent statements (A), (B) or (C) is true. Then the above work shows that necessarily $\beta = \beta_1 = \beta_2$, since $F' \neq 0$.

By working with $F(t) + \alpha_0$, we may assume that $\alpha_0 = 0$. Therefore

$$\frac{\alpha_1 (\alpha_1 - \alpha_2)}{\gamma} = \beta_1 = \beta_2 = \frac{\alpha_2 (\alpha_2 - \alpha_1)}{\gamma}$$

and so $\alpha_1^2 = \alpha_2^2$. Hence $\alpha_1 = -\alpha_2$, since $\alpha_i$ are all distinct.

This shows that $E$ is isomorphic over $\mathbb{F}_q$ to $y^2 = x^3 - a^2 x$, for $a = \alpha_2$. \qed

Proof of Theorem 1.14. The “only if” part is essentially Theorem 2.13 and Remark 2.14.

Observe that $t^q^n - t$ together with the conditions imposed on $F(t)$ satisfy all the hypothesis of Theorem 2.16, then by applying this result we obtain the desired isomorphism. Let us prove that $p \equiv 3 \mod 4$.

Recall that a curve is said to be supersingular if its Jacobian variety is isogenous to a product of supersingular elliptic curves. The curve $s^2 = t^q^n - t$ is supersingular, since it is covered by the hermitian curve $v^{q^n+1} = u^{q^n} - u$, which can be shown to be supersingular from the work of Shioda & Katsura [SK79]. Hence $s^2 = t^q^n - t$ is a supersingular hyperelliptic curve with a map to $E$. So $E$ has to be supersingular. Now $a y^2 = x^3 - x$ is supersingular only if $p \equiv 3 \mod 4$, see [Sil92]. \qed
2.4. Cubic and Quartic Twists. Theorem [112] can be interpreted as showing that the family of quartic twists \( y^2 = x^3 - (t^{q^n} - t)x \) has at least as many separable \( \infty \)-integrals as the number of odd divisors of \( n \), whenever \( q \equiv 3 \mod 4 \). When \( q \equiv 2 \mod 3 \), the same is true for the cubic twists \( y^2 - y = (t^{q^n} - t)x^3 \). Notice that the congruence conditions on \( q \) is equivalent to the supersingularity of the considered curves.

In this section we will construct other quartic twists of \( y^2 = x^3 - x \), as well as cubic twists of \( y^2 = x^3 + 1 \), with many \( \infty \)-integral points; but only in the supersingular case: when \( q \equiv 3 \mod 4 \) and \( q \equiv 2 \mod 3 \), respectively. More precisely, we will be working with the surfaces described in Examples 2.4 and 2.6 for a suitable choice of \( s \) and \( d \).

In these examples we showed that there exists a rational map from the surface \( X_0^i + X_1^i = X_2^id + X_3^id \), where \( i = 2, 6 \) depending on whether we have a quartic or a cubic twist. When \( s \equiv d \equiv 0 \mod 4 \) (\( i = 2 \)) or \( s \equiv d \equiv 0 \mod 6 \) (\( i = 6 \)), we obtain the rational maps

\[
(2.9) \quad (X_0, X_1, X_2, X_3) \mapsto \left( \left[ \frac{X_0}{X_1}, X_2, X_3 \right], \frac{X_2}{X_3} \right)
\]

and

\[
(2.10) \quad (X_0, X_1, X_2, X_3) \mapsto \left( \left[ \frac{X_0}{X_1}^{s/3}, X_2^{d/6}, X_3^{d/2} \right], \frac{X_2}{X_3} \right)
\]

from the surface \( S : X_0^i + X_1^i = X_2^i + X_3^i \) to the surfaces \( y^2z = -x^3 + (t^d + 1)xz^2 \) and \( y^2z = -x^3 + (t^d + 1)z^3 \), respectively.

As we have noticed before, if \( s \) divides \( d \) then \( (t^{d/s}, 1, t, 1) \) is a rational curve on \( S \). What the next results will show is that when we specialize to the case \( s = q^k + 1 \), \( d = q^n + 1 \), and \( r = \frac{q^{k+1}}{q^n+1} \) integers, \( S \) will have many other non-trivial rational curves.

**Lemma 2.17.** Suppose \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_q) \) is such that \( A^tA = I_2 \). Then for any non-negative integer \( k \), the identity

\[
(aX + bY)^{q^k+1} + (cX + dY)^{q^k+1} = X^{q^k+1} + Y^{q^k+1}
\]

holds over \( \mathbb{F}_q[X,Y] \).

**Proof.** This follows from the fact that \( X^{q^k+1} + Y^{q^k+1} \) is a binary hermitian form over \( \mathbb{F}_q \).

**Remark 2.18.** Observe that the matrices satisfying the hypothesis of the previous lemma forms a group \( O(2) \), the orthogonal group. So this lemma is showing that \( O(2) \) acts on the Hermitian Fermat surface of degree \( q^{k} + 1 \). In fact, one can show a lot more [Shi88]: over \( \mathbb{F}_{q^2k} \), the group of automorphisms of such a surface is the projective unitary group, \( PU(4, q^k) = \{(a_{ij}) \in GL_4(\mathbb{F}_{q^2k}) : (a_{ij})^t(a_{ij})^k = I_4 \}/\{scalars\} \).
Corollary 2.19. Let $S$ be the surface $X_0^{q+1} + X_1^{q+1} = X_2^{q+1} + X_3^{q+1}$ defined over $\mathbb{F}_q$. Suppose $r = \frac{q^{n+1}}{q+1}$ is an integer. Then for any two orthogonal matrices $A$ and $A_0$, the curve $(at^r + b, ct^r + d, a_0t + b_0, c_0t + d_0)$ is contained in $S$.

Proof. Take $X = t^r$ and $Y = 1$ in the previous lemma to obtain
$$(at^r + b)^{q+1} + (ct^r + d)^{q+1} = (t^r)^{q+1} + 1$$
Another application of the previous lemma, with $X = t$, $Y = 1$ and $k = n$, we obtain
$$(a_0t + b_0)^{q+1} + (c_0t + d_0)^{q+1} = (t)^{q+1} + 1$$
\[\square\]

The next result is an adaptation of an example due to Shioda [Shi91], and provides results similar to the ones obtained earlier, with only one difference: the quartic twist of $y^2 = x^3 - x$ with many $\infty$-integral points cannot be obtained as a quadratic twist.

Theorem 2.20. If $q \equiv 3 \pmod{4}$ and $n$ is odd positive integer then the curve $y^2 = x^3 - (t^{q+1} + 1)x$ has at least $\tau(n) \infty$-integral points, where $\tau(n)$ is the number of divisors of $n$. If $q \equiv 2 \pmod{3}$ then the same is true for $y^2 = x^3 + t^{q+1} + 1$.

Proof. Let $k$ be a divisor of $n$. Then $r = \frac{q^{n+1}}{q+1}$ will be an integer, since $n$ is odd.

If we assume $q \equiv 3 \pmod{4}$, then $q^{k+1} \equiv q^{n+1} \equiv 0 \pmod{4}$ Consequently there exists a rational map from the surface $S$ defined in Corollary 2.19 to the surface $y^2z = -x^3 + (t^{q+1} + 1)xz^2$, see (2.9).

Now choose an orthogonal matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_q)$ with $cd \neq 0$, and let $A_0 = I_2$ be the identity matrix. From Corollary 2.19, we obtain the rational curve $(at^r + b, ct^r + d, t, 1) \subset S$, whose image under the rational map (2.9) is the section
$$\left(\left[(ct^r + d)^{\frac{q+1}{2}}, (at^r + b)^{\frac{q+1}{2}}(ct^r + d)^{\frac{q+1}{2}} : 1 \right], t\right)$$
This in turn generates the point
$$\left( -(ct^r + d)^{\frac{q+1}{2}}, (at^r + b)^{\frac{q+1}{2}}(ct^r + d)^{\frac{q+1}{2}} \right)$$
on the curve $y^2 = x^3 - (t^{q+1} + 1)x$. The binomial expansion of the first coordinate will produce the monomial $-cd\frac{q+1}{2}t^r/2$, therefore we obtain different points for distinct divisors of $n$.

In the case $q \equiv 2 \pmod{3}$, we obtain the section
$$\left(\left[(ct^r + d)^{\frac{q+1}{3}}, (at^r + b)^{\frac{q+1}{3}} : 1 \right], t\right)$$
as the image of the curve \((at^r + b, ct^r + d, t, 1) \subset \mathcal{S}\) under the rational map \(\text{[2.10]}\). So

\[
\left( -(ct^r + d)^{\frac{k+1}{3}} , (at^r + b)^{\frac{k+1}{2}} \right)
\]

is an \(\infty\)-integral point on the curve \(y^2 = x^3 + t^{q+1} + 1\). The binomial expansion of \(-(ct^r + d)^{\frac{k+1}{3}}\) shows that these points are distinct for distinct divisors of \(n\).

\[\square\]

3. Lang-Vojta conjecture

As discussed in the introduction, the work of Abramovich [AV96] shows that the Lang-Vojta conjecture over a number field \(L\) implies that the number of \(S\)-integral points on the universal family of quadratic twists of an elliptic curve is uniformly bounded. In this section we will provide a proof of the analogous implication over \(\mathbb{F}_q(t)\), but first let us recall the definition of a log-general type variety:

**Definition 3.1.** Let \(X\) be a quasi-projective variety over \(\mathbb{C}\). Let \(f : Y \to X\) be a proper, birational morphism where \(Y\) is a smooth variety (that is, \(f\) is a resolution of singularities). Suppose \(Y \subset Y_1\) is a projective compactification, such that \(Y_1\) is smooth and such that the reduced variety \(D = Y_1 \setminus Y\) is a divisor of normal crossings. Then \(X\) is said to be of \(log\)-general type if the divisor \(K_{Y_1} + D\) is big, that is, for some \(m\) the complete linear system \(|m(K_{Y_1} + D)|\) defines a birational map to the image.

**Theorem 3.2.** Suppose \(E_1 : y^2 = f(x) = x^3 + ax + b\) is an elliptic curve. Then \(K : z^2 = f(x_1)f(x_2)\) is a log-general type surface.

**Proof.** See [Con08]. \[\square\]

We will use this theorem to prove the uniformity of separable \(\infty\)-integral points on quadratic twists.

**Proof of Theorem 1.10.** Let \(K : z^2 = f(x_1)f(x_2)\) be the singular Kummer surface associated to \(E_1 \times E_1\). As stated before, \(K\) is a log-general type variety, so if Lang-Vojta’s conjecture is true, the set of separable \(\infty\)-integral points of \(K\) are not Zariski dense. In other words, there must exist a polynomial \(g(x_1, x_2, Z)\) with \(\infty\)-integral coefficients and prime to \(Z^2 - f(X_1)f(X_2)\) such that all separable \(\infty\)-integral points in \(K\) are contained in

\[
\left\{ \begin{array}{l}
z^2 = f(x_1)(f(x_2) \\
g(x_1, x_2, z) = 0
\end{array} \right.
\]

By substituting \(z^2 = f(x_1)f(x_2)\) in \(g\), we can find polynomials \(g_0 = g_0(x_1, x_2)\) and \(g_1 = g_1(x_1, x_2)\) such that the separable \(\infty\)-integral points of \(K\) satisfy

\[g_0(x_1, x_2) + g_1(x_1, x_2)z = 0\]

Notice that the polynomials \(g_0\) and \(g_1\) cannot be both zero, otherwise \(g\) would be divisible by \(Z^2 - f(X_1)f(X_2)\).
Let $\phi : E_d \times E_d \to K$ be the morphism defined by

$$(x_1, y_1, x_2, y_2) \mapsto (x_1, x_2, dy_1y_2).$$

This morphism commutes with the Frobenius endomorphism. It follows that $P$ is a separable point of $E_d \times E_d$ if, and only if, $\phi(P)$ is a separable point of $K$. In particular, the separable \(\infty\)-integral points in $E_d \times E_d$ are mapped down to separable \(\infty\)-integral points in $K$. Therefore the separable \(\infty\)-integral points in $E_d \times E_d$ satisfy

$$g_0(x_1, x_2) + g_1(x_1, x_2)dy_1y_2 = 0$$

Now fix $d \neq 0$ and a separable \(\infty\)-integral point $(x_0, y_0) \in E_d$ such that $g_0(x_0, X_1)$ and $g_1(x_0, X_1)$ are not both identically zero as polynomials in $X_1$. Assume further that $y_0 \neq 0$. Then for any other separable \(\infty\)-integral point $(x, y) \in E_d$ we can find polynomials $\overline{g}_0(X), \overline{g}_1(X)$ with $\deg \overline{g}_0, \deg \overline{g}_1 \leq \deg g$ such that

$$\overline{g}_0(x) + \overline{g}_1(x)y = 0.$$ 

Suppose $\overline{g}_1(x) = 0$, then $\overline{g}_0(x) = 0$. So there’s a polynomial $h(X)$ with $\deg h \leq \min\{\deg \overline{g}_0, \deg \overline{g}_1\} \leq \deg g$ such that $h(x) = 0$. Hence

$$|\{(x, y) \in E_d\}| \leq 2\deg g$$

and this does not depend on $d$.

If $\overline{g}_1(x) \neq 0$ then $y = -\overline{g}_0(x)/\overline{g}_1(x)$. Substituting back in the equations of $E_d$, we have

$$d \left(\frac{-\overline{g}_0(x)}{\overline{g}_1(x)}\right)^2 = f(x)$$

and this implies that

$$f(x)\overline{g}_1(x)^2 - d\overline{g}_0(x)^2 = 0$$

Therefore $x$ satisfies a polynomial equation of degree at most $2\deg g + 3$, which means that the number of integral points in $E_d$ is bounded by $4\deg g + 6$, which once more does not depend on $d$. \(\square\)

Now we will prove that a similar result holds true for the universal family of cubic twists. But this time we will follow very closely the ideas and notations on [Abr97].

Let $\pi : X \to B$ be a family of smooth irreducible curves over a field $K$. Let us denote the $n$-th fibered power of $X$ over $B$ by $\pi_n : X^n_B \to B$ and for some $P \subset X(K)$, we will denote its $n$-th fibered power by $P^n_B \subset X^n_B$, and by $P_b$ the points of $P$ on the fiber $\pi^{-1}(b)$. Under this assumptions, following [CHM97], Abramovich proved:

**Lemma 3.3.** Let $X \to B$ and $P$ be as above. Suppose that there exists an integer $n \geq 1$ such that $P^n_B \subset F$, for a Zariski-closed subset $F \subset X^n_B$. Then there exists a dense open subset $U \subset B$ and an integer $N$ such that for every $b \in U$, we have $|P_b| \leq N$. 
Proof. See [Abr97].

Remark 3.4. A subset $P \subset X(K)$ satisfying the hypothesis of the lemma is said to be $n$-correlated.

Proof of Theorem 1.11. There exists a closed subset $U_0 \subset \mathbb{A}^1$ such that for all $d \in B := \mathbb{A}^1 \setminus U_0$, $X_d$ is an elliptic curve. Therefore $X \longrightarrow B$ is a family of smooth irreducible curves.

The association $((x_1, y_1), (x_2, y_2), (x_3, y_3), t) \mapsto (y_1, y_2, y_3, tx_1x_2x_3)$, defines a dominant map from $X_B^3$ to the hypersurface $\mathcal{H} \subset \mathbb{A}^4$ defined by the equation $u^3 = (x^2 - x)(y^2 - y)(z^2 - z)$. This maps commute with the Frobenius endomorphism; therefore it will send separable $\infty$-integral points on $X_B^3$ to separable $\infty$-integral points on $\mathcal{H}$, whenever $d$ is $\infty$-integral. Assume for a moment that the set of separable $\infty$-integral points on $\mathcal{H}$ is not Zariski dense. Then this map proves that the set of separable $\infty$-integral points on $X$ is 3-correlated. From Lemma 3.3, we can find a dense open set $U \subset B$ and an integer $N_0$ such that $|X_d(\mathbb{F}_q[t])| \leq N_0$, for $d \in U$. Let $\{d_1, \ldots, d_u\} = B \setminus U$. We can apply isotrivial Siegel’s theorem to conclude that $|X_{d_i}(\mathbb{F})| = N_i < \infty$, for $i = 1, \ldots, u$. Therefore

$$|X_d(O_{K,S})| \leq N := \max\{N_0, N_1, \ldots, N_u\}$$

for all $d \in B$.

Hence, we are able to find a uniform bound for the number of separable $\infty$-integral points on the family of cubic twists of $y^2 - y = x^3$, if we can prove that separable $\infty$-integral points in $\mathcal{H}$ are not Zariski dense on $\mathcal{H}$. By assuming the Lang-Vojta conjecture the last statement will be true, if we can show that $\mathcal{H}$ is a variety of log-general type. This is the content of the next lemma.

Lemma 3.5. $u^3 = (x^2 - x)(y^2 - y)(z^2 - z)$ is a log-general type variety.

Proof. See [Con08].

4. Explicit sets of linearly independent

We will use this section to prove that the points given by Theorem 2.13 are linearly independent. But first let us recall some classic results on elliptic curves over function fields.

Let $E$ be an elliptic curve defined over a finite field $k$ and let $L = k(C)$ be the function field of a curve $C$. It is not hard to show that the Mordell-Weil group of $E(L)$ and $\text{Mor}_k(C, E)$ are isomorphic, where $\text{Mor}_k(C, E)$ is the abelian group of morphisms from $C$ to $E$. Moreover, the torsion group of $\text{Mor}_k(C, E)$ is the set $\text{Mor}_k^0(C, E)$ of constant maps, which is equal to $E(k)$ under the above isomorphism.

Let us take a look at the case where $C$ is an hyperelliptic curve defined over $k$. Suppose $C$ is given by the equation $s^2 = A(t)$. As before let
$E_A : A(t)y^2 = f(x)$ be the quadratic twist of the elliptic curve $E : y^2 = f(x)$ defined over $k$. Define a group homomorphism $\Gamma : E_A(\mathbb{F}_q(t)) \to E(L)$ by

\[
(4.1) \quad P = (F(t), G(t)) \mapsto \phi_P(s, t) := (F(t), sG(t))
\]

using the above isomorphism between $E(L)$ and $\text{Mor}_k(C, E)$. So to prove that $\{P_1, \ldots, P_n\} \subset E_A(\mathbb{F}_q(t))$ is $\mathbb{Z}$-linearly independent, it is sufficient to prove that $\{\Gamma(P_1), \ldots, \Gamma(P_n)\} \subset E(L)$ is $\mathbb{Z}$-linearly independent. This is exactly what we will be using in the proof of the next theorem.

**Theorem 4.1.** The points $\{Q_i\}_{1 \leq i \leq n}$ given by Theorem 2.13 are linearly independent.

**Proof.** By (4.1), for every $Q_k$ we may associate a map $\phi_k : C \to E$ defined by $\phi(t, s) = (F_k(t), sG_k(t))$, where $Q_k = (F_k, G_k)$. Since $B_i(F)$ is an $\mathbb{F}_q$-additive polynomial, it follows by direct calculation that there exists $\beta \in \mathbb{F}_q$ such that $F_k^\beta = \beta G_k$. Let $\omega = dx/y$ be the invariant differential of $E$ and let $\omega'$ be the non-zero differential $dt/s$ on $C$. So

\[
\phi_k^\ast(\omega) = \frac{d\phi_k^\ast(x)}{\phi_k^\ast(y)} = \frac{F_k^\beta dt}{G_k s} = \beta G_k \omega'
\]

This shows that the set $\{\phi_k^\ast(\omega)/\omega'\}_{k \in D(n)}$ is linearly independent. Our result follows from an application of the next lemma, which roughly says that if the pullback of differentials is linearly independent, then necessarily the maps have to be linearly independent. \qed

**Lemma 4.2.** Let $C$ be a curve and $E$ be a supersingular elliptic curve, both defined over $\mathbb{F}_q$. Let $\omega$ and $\omega'$ be non-zero differentials on $E$ and $C$, respectively. For any set $\{\Phi_i\}_{i=1}^n \subset \text{Mor}_k(C, E)$ we can associate a set $\{\Phi_i\}_{i=1}^n \subset K$, where $\Phi_i = \phi_i^\ast(\omega)/\omega'$ and $K = \mathbb{F}_q(C)$ is the function field of $C$. If $\{\Phi_i\}_{i=1}^n$ is an $\mathbb{F}_q$-linearly independent set then $\{\phi_i\}_{i=1}^n$ is a set of $\mathbb{Z}$-linearly independent morphisms in $\text{Mor}_k(C, E)$.

**Proof.** Suppose, by contradiction, that there exists a non-trivial $\mathbb{Z}$-linear combination $\sum_{i=1}^n a_i \phi_i = O$ and let $p'$ be the largest power of $p$ that divides $a_i$, for all $i = 1, \ldots, n$. Hence

\[
[p'] \left( \sum_{i=1}^n \frac{a_i}{p^j} \phi_i \right) = O
\]

The $p$-torsion group of a supersingular elliptic curve is trivial, therefore we can conclude that $\sum_{i=1}^n \frac{a_i}{p^j} \phi_i = O$ is a $\mathbb{Z}$-linear combination with at least one of its coefficients prime to $p$, say $a_0/p^j$. Let us write $b_i = \frac{a_i}{p^j}$.

Since the pullback of differentials is an $\mathbb{F}_q$-linear map $\phi^\ast : \Omega_E \to \Omega_C$ between the space of differential forms of $C$ and $E$, we will have

\[
0 = \left( \sum_{i=1}^n b_i \phi_i \right)^\ast (\omega) = \sum_{i=1}^n b_i^\ast \phi_i^\ast (\omega)
\]
and so
\[ \sum_{i=1}^{n} b_i^* \Phi_i = 0 \]

By hypothesis, \( \{ \Phi_i \}_{i=1}^{n} \) is linearly independent, therefore we have \( b_i^* = 0 \), for all \( i \). This means that for all \( i \), \( p \) divides \( b_i \): a contradiction to the fact that \( p \) is prime to \( b_0 \). \( \square \)

**Remark 4.3.** Notice that the same proof holds if we work with the cubic twists \( A(t)x^3 = y^2 - y \) and \( q \equiv 2 \mod 3 \).

Our results is far from best, in the sense that our proof shows that the rank will grow very slowly, in the order of \( \tau_{\text{odd}}(n) \). In fact, the Mordell-Weil rank of the considered curves are in the same order of growth of \( q^n/2n \), as can be shown by [TS67].

5. **Function fields with large \( m \)-class rank**

Suppose that \( K = \mathbb{F}_q(C) \) is the function field of a curve \( C \) with one point at infinity. In this case we have that \( \text{Cl}(\mathcal{O}_K) \simeq (\text{Pic}^0(C)/\mathbb{F}_q) = J_C(\mathbb{F}_q) \), the Jacobian variety of \( C \).

**Proof of Theorem 1.15.** Let us consider the elliptic curves described in Theorem 2.13. As we have observed before (Theorem 4.1), the separable infinite integral points \( Q_i \in (t^{q^6} - t)y^2 = x^3 - x \) yield \( \tau_{\text{odd}}(n) \) linearly independent morphisms defined over \( \mathbb{F}_q \) from \( C : s^2 = t^{q^n} - t \) to \( E : y^2 = x^3 - x \). This, in turn, induces the following isomorphism \( J_C(\mathbb{F}_q) \simeq E_{\tau_{\text{odd}}(n)} \times A \), where \( A \) is an abelian variety over \( \mathbb{F}_q \). Since \( E(\mathbb{F}_q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(q+1) \mathbb{Z} \), for \( q \equiv 3 \mod 4 \), we have

\[ \text{Cl}(\mathcal{O}_K) \simeq J_C(\mathbb{F}_q) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/((q + 1)/2) \mathbb{Z})^{\tau_{\text{odd}}(n)} \times A. \]

Therefore for any positive divisor \( m \) of \( q+1 \), we have that \( (\mathbb{Z}/m\mathbb{Z})^{\tau_{\text{odd}}(n)} \subset \text{Cl}(\mathcal{O}_K) \), and so the \( m \)-rank of the function field of the curve \( s^2 = t^{q^n} - t \) is at least \( \tau_{\text{odd}}(n) \), which can be arbitrarily large.

When \( q \equiv 2 \mod 3 \), a similar argument works for the function field of the curve \( s^3 = (t^{q^n} - t) \). \( \square \)

**Acknowledgments**

I would like to thank Prof. José Felipe Voloch for his invaluable support and guidance during the completion of this work. I am also thankful to Prof. Douglas Ulmer and Prof. Siman Wong for discussing with me some of their unpublished results.
References

[Abr97] Dan Abramovich, Uniformity of stably integral points on elliptic curves, Invent. Math. 127 (1997), no. 2, 307–317. MR MR1427620 (98d:14033)

[AV96] Dan Abramovich and José Felipe Voloch, Lang’s conjectures, fibered powers, and uniformity, New York J. Math. 2 (1996), 20–34, electronic. MR MR1376745 (97e:14031)

[BDS04] Irene I. Bouw, Claus Diem, and Jasper Scholten, Ordinary elliptic curves of high rank over $\mathbb{F}_p(x)$ with constant $j$-invariant, Manuscripta Math. 114 (2004), no. 4, 487–501. MR MR2081948 (2005e:11069)

[Bro08] Lisa Berger, Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields, J. Number Theory 128 (2008), no. 12, 3013–3030. MR MR2464851

[CHM97] Lucia Caporaso, Joe Harris, and Barry Mazur, Uniformity of rational points, J. Amer. Math. Soc. 10 (1997), no. 1, 1–35. MR MR1325796 (97d:14033)

[Con08] R. Conceiçao, Twists of elliptic curves with many integral points over function fields, Thesis (2008), 58pgs.

[DS07] Claus Diem and Jasper Scholten, Ordinary elliptic curves of high rank over $\mathbb{F}_p(x)$ with constant $j$-invariant. II, J. Number Theory 124 (2007), no. 1, 31–41. MR MR2320989 (2008b:11063)

[Elk94] Noam D. Elkies, Mordell-Weil lattices in characteristic 2. I. Construction and first properties, Internat. Math. Res. Notices (1994), no. 8, 343 ff., approx. 18 pp. (electronic). MR MR1289579 (95f:11046)

[DS82] John Tate and I. R. Šafarevič, The rank of elliptic curves, Dokl. Akad. Nauk SSSR 175 (1967), 770–773. MR MR0237508 (38 #5790)

[Sil92] Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original. MR MR1213490 (94m:11037)

[SK79] Tetsuji Shioda and Toshiyuki Katsura, On Fermat varieties, Tôhoku Math. J. (2) 31 (1979), no. 1, 97–115. MR MR526513 (80m:14033)

[TŠ67] John Tate and I. R. Šafarevič, The rank of elliptic curves, Dokl. Akad. Nauk SSSR 175 (1967), 770–773. MR MR0237508 (38 #5790)

[Ulm02] Douglas Ulmer, Elliptic curves with large rank over function fields, Ann. of Math. (2) 155 (2002), no. 1, 295–315. MR MR1888802 (2003b:11059)

[Ulm07] L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields, Invent. Math. 167 (2007), no. 2, 379–408. MR MR2270458 (2007k:11010)
Department of Mathematics, University of Texas at Austin, Austin, Texas, 78712, USA

E-mail address: rconceic@math.utexas.edu