Computation of Mordell–Weil bases for ordinary elliptic curves in characteristic two

G. Moehlmann

Abstract

In this paper we consider ordinary elliptic curves over global function fields of characteristic 2. We present a method for performing a descent by using powers of the Frobenius and the Verschiebung. An examination of the local images of the descent maps together with a duality theorem yields information about the global Selmer groups. Explicit models for the homogeneous spaces representing the elements of the Selmer groups are given and used to construct independent points on the elliptic curve. As an application we use descent maps to prove an upper bound for the naive height of an $S$-integral point on $A$. To illustrate our methods, a detailed example is presented.

1. Introduction

Let $A$ be an elliptic curve defined over a global field $K$. Then $\hat{A}(K) := A(K)/(A(K))_{\text{tor}}$ is a free abelian group of finite rank. For $K$ a number field or a rational function field of characteristic greater than or equal to 5, there are algorithms, which may not always succeed, to compute generators for $\hat{A}(K)$ by doing a two-descent. These generators are called a Mordell–Weil basis. See the documentation of [1] for references for the algorithms that are used in Magma. These algorithms make use of the separability of the multiplication by two isogeny. Our main goal in this paper is to describe how similar techniques can be applied to compute Mordell–Weil bases for ordinary elliptic curves over global function fields of characteristic 2. By using flat cohomology we first construct descent maps as described in [7, 16, 17] and utilize them to compute Selmer groups. Then we represent the elements of the Selmer groups as homogeneous spaces as in [4], utilize them to construct independent points, and enlarge the group generated by these points as in [10]. At the end we use our descent maps to compute an upper bound for the naive height of an $S$-integral point on $A$.

This paper is based on the author’s PhD thesis at Carl-von-Ossietzky University Oldenburg.

2. Descent via Frobenius and Verschiebung

Let $A$ be an ordinary elliptic curve defined over a field $K$ of characteristic 2. Then we can assume that $A$ is given by a Weierstrass equation of the form

$A : y^2 + a_1 xy + x^3 + a_2 x^2 + a_6 = 0$.

We denote the zero of $A$ by $O_A$. Let $\phi : A \to B$ be an isogeny of degree $n$ and $\phi^\vee$ its dual isogeny. As a result of the snake lemma, the sequence of kernels and cokernels

$0 \to A(K)[\phi] \to A(K)[n] \to B(K)[\phi^\vee] \to B(K)/\phi(A(K)) \to 0$

$\to A(K)/nA(K) \to A(K)/\phi^\vee(B(K)) \to 0$

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11G05 (primary), 11G07, 14G25, 14G17 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.
As we require \( \psi \) by mapping \( K \) to \( A \). The dual isogeny of \( F \) in flat cohomology. Thus we get homomorphisms of \( \mathbb{Z} \)-linear independent points on \( A(K) \): the \( i \)th power Frobenius is a purely inseparable isogeny \( F^i : A \to A^{(2^i)} \) of degree \( 2^i \) given by \( F^i(x, y) = (x^{2^i}, y^{2^i}) \). The Weierstrass equation of \( A^{(2^i)} \) is

\[
A^{(2^i)} : y^2 + a_1^{2^i}xy + x^3 + a_2^{2^i}x^2 + a_6^{2^i} = 0. \tag{2.1}
\]

The dual isogeny of \( F^i \) is called the \( i \)th power Verschiebung. We denote it by \( V^i : A^{(2^i)} \to A \). As we require \( A \) to be ordinary, the Verschiebung is separable. If the \( 2^i \)-torsion of \( A^{(2^i)} \) is \( K \)-rational, the kernel of the Verschiebung, \( \ker V^i \), is isomorphic to \( \mathbb{Z}/2^i\mathbb{Z} \) as a finite flat group scheme over \( K \). In the following, let \( T \) denote a generator of \( \ker V^i \). An isomorphism \( \Xi \) is given by mapping \( T \) to \( 1 \). For an arbitrary isogeny \( \Phi \), the kernel of the dual isogeny \( \Phi^\vee \) is isomorphic to the Cartier dual (\( \ker \Phi \))^\vee of the kernel of \( \Phi \). The Cartier dual of \( \mathbb{Z}/2^i\mathbb{Z} \) is isomorphic to the \( K \)-group scheme of \( 2^i \)th roots of unity \( \mu_{2^i} \). Hence for the Frobenius there is an isomorphism \( \psi : \ker F^i \to \mu_{2^i} \), such that the diagram

\[
\begin{array}{ccc}
\ker F^i \times \ker V^i & \xrightarrow{\psi} & \mathbb{G}_m \\
\downarrow & & \downarrow \Xi \\
\mu_{2^i} \times \mathbb{Z}/2^i\mathbb{Z} & \xrightarrow{id} & \mathbb{G}_m
\end{array}
\]

commutes. Here the rows are given by the Weil pairing \( e_i \) or the Cartier duality pairing. Let \( R \) be a finite \( K \)-algebra, then due to the commutativity of the diagram we have \( \psi(P') = e_i(P', T) \) for every Spec \( R \)-rational point \( P' \) on \( \ker F^i \). The short exact sequences

\[
0 \to \ker V^i \to A^{(2^i)} \xrightarrow{V^i} A \to 0 \\
0 \to \ker F^i \to A \xrightarrow{F^i} A^{(2^i)} \to 0
\]

induce the long exact sequences

\[
0 \to \ker V^i(K) \to A^{(2^i)}(K) \xrightarrow{V^i} A(K) \to H^1(K, \ker V^i) \\
0 \to \ker F^i(K) \to A(K) \xrightarrow{F^i} A^{(2^i)}(K) \to H^1(K, \ker F^i)
\]

in flat cohomology. Thus we get homomorphisms

\[
\alpha_i : A(K) \to H^1(K, \ker V^i) \\
\beta_i : A^{(2^i)}(K) \to H^1(K, \ker F^i)
\]

for which \( \ker \alpha_i = V^i(A^{(2^i)}(K)) \) and \( \ker \beta_i = F^i(A(K)) \). As a result of the Kummer sequence or the Artin–Schreier–Witt sequence together with Hilbert 90, which states that \( H^1(K, \mathbb{G}_m) \) and \( H^1(K, W_i) \) are trivial, we have \( H^1(K, \mathbb{Z}/2^i\mathbb{Z}) \simeq W_i(K)/\varphi(W_i(K)) \) and \( H^1(K, \mu_{2^i}) \simeq (K^\times/(K^\times)^2)^i \). Here \( W_i \) denotes the truncated Witt vectors of length \( i \), and \( \varphi \) is the Artin–Schreier map given by mapping a truncated Witt vector \( v \) to \( Fv - v \). The composition of \( \alpha_i \) or \( \beta_i \) and both the isomorphisms induced by \( \Xi \) or \( \psi \) and by the Artin–Schreier–Witt or Kummer sequence yields homomorphisms

\[
\alpha_i : A(K) \to W_i(K)/\varphi(W_i(K)) \\
\beta_i : A^{(2^i)}(K) \to (K^\times/(K^\times)^2)^i
\]

under the assumption that the \( 2^i \)-torsion of \( A^{(2^i)} \) is defined over \( K \). The following propositions demonstrate how \( \alpha_i \) and \( \beta_i \) can be evaluated in this situation.
Proposition 2.1. Let $Q$ be in $A^{(2)}$ with $V^i(Q) = P$, and let $\sigma$ be a generator of the cyclic Galois group of $K(Q)/K$. Then $\alpha_i(P) = v + \varphi(W_i(K))$ where $v \in W_i(K)$ is determined by the equation $\Xi(Q - \sigma(Q)) = w - \sigma(w)$ for $w \in W_i(K)$ with $K(w) = K(Q)$ and $\varphi(w) = v$.

Proof. This proposition follows from tracing through the various morphisms. As $V^i$ is separable, $\ker V^i$ is an étale group scheme. Hence Galois cohomology can be used for computations in $H^1(K, \ker V^i)$. Consequently $\hat{\alpha}_i$ maps a point $P$ to the cocycle $\sigma \mapsto Q - \sigma(Q)$, and, on the other hand, when we identify $\mathbb{Z}/2\mathbb{Z}$ and $W_i(F_2)$ via $1 \mapsto (1, \ldots, 1)$, the isomorphism $W_i(K)/\varphi(W_i(K)) \rightarrow H^1(K, \mathbb{Z}/2\mathbb{Z})$ is given by mapping $v$ to $\sigma \mapsto w - \sigma(w)$. Patching things together proves the statement.

Proposition 2.2. Let $f$ be a function in the function field of $A^{(2)}$ with principal divisor $(f) = (2^iT - 2^jO_{A^{(2)}})$ such that $f \circ F^i = g^{2^j}$ holds for a function $g$ on $A$. Then for $P$ in $A^{(2)}(K)$ we have

$$\beta_i(P) = \begin{cases} 1 & \text{if } P = O_{A^{(2)}}, \\ f(-P)^{-1} & \text{if } P = T, \\ f(P) & \text{otherwise}. \end{cases}$$

Proof. If we use Čech cocycles to represent elements in the cohomology groups, the isomorphism $K^\times/(K^\times)^{2^j} \rightarrow H^1(K, \mu_{2^j})$ is given by $a \mapsto (1 \otimes b)/(b \otimes 1)$ with $b^{2^j} = a$. We denote it by $\delta_K$. Moreover, $\hat{\beta}_i$ maps a point $P \in A^{(2)}(K)$ to the cocycle $(1 \otimes x_Q, 1 \otimes y_Q) \mapsto (x_Q \otimes 1, y_Q \otimes 1)$ representing an element in $H^1(K, \ker F^i)$. Here $F^i(x_Q, y_Q) = P$ holds. Composing $\hat{\beta}_i$ and the isomorphism that is induced by $\psi$, we get

$$e_i(\delta_F(P), T) = e_i((1 \otimes x_Q, 1 \otimes y_Q) - (x_Q \otimes 1, y_Q \otimes 1), T) = \frac{g((x_Q \otimes 1, y_Q \otimes 1))}{g(1 \otimes (x_Q, y_Q))}.$$}

This follows from the formula for the Weil pairing given in [11, p. 313]. On the other hand, we have

$$\delta_K(\varphi(Q)) = \delta_K(g(x_Q, y_Q)^{2^j}) = \frac{1 \otimes g((x_Q, y_Q))}{g((x_Q, y_Q)) \otimes 1}.$$}

For $i = 1$ this construction yields

$$\alpha_1 : A(K) \rightarrow W_1(K)/\varphi(W_1(K)), (x, y) \mapsto \frac{x + a_2}{a_1^2} \equiv \frac{a_6}{a_1^2} x^2$$

and

$$\beta_1 : A^{(2)}(K) \rightarrow K^\times/(K^\times)^2, (x, y) \mapsto \begin{cases} x & \text{for } x \neq 0, \\ a_6 & \text{for } x = 0, \\ 1 & \text{for } (x, y) = O_{A^{(i)}}. \end{cases}$$

These are the same maps as constructed in [7]. An easy computation shows that, for an ordinary elliptic curve $A$ given by $A : y^2 + a_1 xy + x^3 + a_2 x^2 + a_6 = 0$, the curve $A^{(4)}$ has $K$-rational 4-torsion if and only if $a_2$ is of the form $a_2 = a_1^2 (s^2 + s)$ for an element $s \in K$. The
point \( T = (a_2^2a_6, a_1^6s^4a_6 + a_0^2) \) on \( A^{(4)}(K) \) is of order 4. An examination of the Galois group operation on the preimages of the Witt vector

\[
\left( \frac{a_6}{a_1^2x^2}, \frac{a_6y}{a_1^3x^3} + \frac{a_6}{a_1^2x} + \frac{sa_6 + a_6}{a_1^2x^2} + \frac{a_0^2}{a_1^4x^4} \right)
\]

and the computation of the principal divisor of \( (y + (1/a_1^4)x^2 + a_1^4s^4x) \) demonstrates that \( \alpha_2 \) and \( \beta_2 \) are given by

\[
\alpha_2 : A(K) \to W_2(K)/\varphi(W_2(K)), \quad (x, y) \mapsto \left( \frac{a_6}{a_1^2x^2}, \frac{a_6y}{a_1^3x^3} + \frac{a_6}{a_1^2x} + \frac{sa_6 + a_6}{a_1^2x^2} + \frac{a_0^2}{a_1^4x^4} \right)
\]

and

\[
\beta_2 : A^{(4)}(K) \to K^\times/(K^\times)^4, \quad (x, y) \mapsto \begin{cases} a_1^2a_0^3 & \text{if } (x, y) = T, \\ 1 & \text{if } (x, y) = \mathcal{O}', \\ y + \frac{1}{a_1^4}x^2 + a_1^4s^4x & \text{otherwise.} \end{cases}
\]

**Remark.** Similar techniques can be used to construct descent maps for supersingular elliptic curves in characteristic 2. These will be presented in a subsequent publication.

**Remark.** Let \( A^{(2^i)} \) be given by a Weierstrass equation of the form (2.1). Then for \( i = 1 \) the \( 2^i \)-torsion is always \( K \)-rational. But for \( i \geq 2 \) this is not the case. By working over \( L \), the field of definition of \( A^{(2^i)}[2^i] \), we can still construct descent maps. This time they are mapping points on \( A(K) \) or \( A^{(2^i)}(K) \) to subsets of \( W_i(L)/\varphi(W_i(L)) \) or \( L^\times/(L^\times)^{2^i} \), respectively. With an inflation-restriction argument we can describe these subsets. When it comes to calculating the global image of these descent maps for \( i = 1, 2 \) as described in \( \S \, 5 \), it is possible to construct models for the relevant homogeneous spaces that are defined over \( K \). The techniques to complete this task are basically the same as in \( \S \, 5 \).

3. **Local duality**

Throughout this section let \( K_v \) be the completion of \( K \) with respect to a valuation \( v \). For an arbitrary isogeny \( \phi : A \to B \) of elliptic curves over \( K_v \) and dual isogeny \( \phi^\vee \) we denote the connection homomorphisms in cohomology by

\[
\alpha : A(K_v) \to H^1(K_v, \ker \phi^\vee) \quad \text{and} \quad \beta : B(K_v) \to H^1(K_v, \ker \phi).
\]

The Weil pairing induces a cup product pairing

\[
\cup : H^1(K_v, \ker \phi) \times H^1(K_v, \ker \phi^\vee) \to H^2(K_v, \mathbb{G}_m).
\]

**Theorem 3.1.** The images \( \alpha(A(K_v)) \) and \( \beta(B(K_v)) \) are exact orthogonal complements under the cup product pairing.

**Proof.** The diagram

\[
\begin{array}{ccc}
H^0(K_v, A^\vee) \times H^1(K_v, A) & \to & H^2(K_v, \mathbb{G}_m) \\
\downarrow \alpha & & \\
H^1(K_v, \ker \phi^\vee) \times H^1(K_v, \ker \phi)
\end{array}
\]

\[
\begin{array}{ccc}
H^0(K_v, A^\vee) \times H^1(K_v, A) & \to & H^2(K_v, \mathbb{G}_m) \\
\downarrow \alpha & & \\
H^1(K_v, \ker \phi^\vee) \times H^1(K_v, \ker \phi)
\end{array}
\]

Downloaded from https://www.cambridge.org/core. IP address: 54.70.40.11, on 03 Dec 2019 at 05:44:18, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1112/S1461157014000175
commutes (compare [8, C.5]). The upper pairing is given by [8, Theorem 7.8], and the vertical morphisms are the suitable homomorphisms in the long exact cohomology sequences of
\[ 0 \rightarrow \ker \phi \rightarrow A \rightarrow B \rightarrow 0 \]
and its dual sequence. Let \( b \in \text{Im} \beta \subseteq H^1(K_v, \ker \phi) \) and \( a \in \text{Im} \alpha \subseteq H^1(K_v, \ker \phi^\vee) \) be elements in the images. This means there are \( K_v \)-rational points \( P \in H^0(K_v, B) = B(K_v) \) and \( Q \in H^0(K_v, A^\vee) \cong H^0(K_v, A) = A(K_v) \) such that \( \alpha(Q) = a \) and \( \beta(P) = b \). If we denote the upper pairing by \((.,.)_1\), the lower by \((.,.)_2\), and by \( \iota \) the induced homomorphism \( \iota : H^1(K_v, \ker \phi) \rightarrow H^1(K_v, A) \), then we have \((a, b)_2 = (Q, \iota(b))_1 = (Q, 0)_1 = 0 \) due to the exactness of the cohomology sequence. Hence the images are orthogonal. For the previously mentioned isogenies \( F^i \) and \( V^i \) and descent maps \( \alpha_i^v : A(K_v) \rightarrow W_i(K_v)/\varphi(W_i(K_v)) \) and \( \beta_i^v : A^{(2i)}(K_v) \rightarrow K_v^\times/(K_v^\times)^{2i} \), the cup product pairing
\[ (.,.) : W_i(K_v)/\varphi W_i(K_v) \times K_v^\times/(K_v^\times)^{2i} \rightarrow \mathbb{Q}/\mathbb{Z}. \]
is nothing other than the Artin–Schreier–Witt pairing
\[ (.,.) : W_i(K_v)/\varphi W_i(K_v) \times K_v^\times/(K_v^\times)^{2i} \rightarrow \mathbb{Q}/\mathbb{Z}. \]

**Remark.** The Artin–Schreier–Witt pairing can be evaluated efficiently as described in [9, proof of Theorem 4].

4. Local images

For \( i = 1, 2 \), statements about the images of \( \alpha_i^v \) and \( \beta_i^v \) can be proven.

**Proposition 4.1.** Let \( k \) be the residue class field of \( K_v \), \( R_v \) the valuation ring, and \( U_n \) the set \( U_n := \{ u \in R_v^\times \mid v(u - 1) \geq n \} \). Assuming that the coefficients of the Weierstrass equation for \( A \) are in \( k \), the following equations hold:

\[
\text{Im} \beta_1^v : U_{2v(a_1)}(K_v^\times)^2/(K_v^\times)^2 = [A(2)(K_v) : A_1^v(K_v)]/[A(K_v) : A_1(K_v)],
\]

\[
[K_v^\times/(K_v^\times)^2 : \text{Im} \beta_1^v] = 2(#k) v(a_1)[A(K_v) : A_1(K_v)]/[A(2)(K_v) : A_1^v(K_v)],
\]

\[
\text{Im} \beta_2^v : U_{4v(a_1)}(K_v^\times)^4/(K_v^\times)^4 = [A(4)(K_v) : A_1^v(K_v)]/[A(K_v) : A_1(K_v)],
\]

\[
[K_v^\times/(K_v^\times)^4 : \text{Im} \beta_2^v] = 4(#k) v(a_1)[A(K_v) : A_1(K_v)]/[A(4)(K_v) : A_1^v(K_v)].
\]

**Proof.** The first two equalities can be found in [7]. For the other two, we can adapt the proof. The rows of the commutative diagram
\[
\begin{array}{c}
0 \rightarrow A_1(K_v) \xrightarrow{F^2} A_1^v(K_v) \xrightarrow{\beta_1^v} U_{4v(a_1)}(K_v^\times)^4/(K_v^\times)^4 \rightarrow 0 \\
0 \rightarrow A(K_v) \xrightarrow{F^2} A_1^v(K_v) \xrightarrow{\beta_2^v} \text{Im} \beta_2 \rightarrow 0
\end{array}
\]
are exact. Here \( A_1 \) or \( A_1^{(4)} \) denotes the kernel of reduction. As in [7], the surjectivity of the upper right map is the only part that is not obvious. It can be proven by a short calculation:

\[
\left( y + \frac{x^2}{a_1} + a_1^4 s^4 x \right) \frac{a_1^4 x^4}{y^4} = \frac{x^3 a_1^3 x y + x^3 + a_1^8 s^4 x^2}{y^2} = \frac{y^2 + a_1^4 x y + a_1^6 (s^8 + s^4) x^2 + a_1^4 y^2 + a_1^8 s^8 x^2 + a_1^4}{y^2} = 1 + a_1^4 u^{-4} \left( z + a_1^4 s^4 z^2 + a_1^8 s^8 z^3 + a_6^4 \frac{z}{y^2} + a_1^4 a_6^4 s^4 z^2 \right)
\]

where \( u \) is a unit in the valuation ring and \( z := x/y \). As \((x, y)\) is in \( A_1^{(4)}(K_v) \), the valuation of \( z \) is positive. Hence the image is in \( U_{4v(a_1)} \). The map \((x, y) \mapsto x/y\) is an isomorphism between \( A_1^{(4)}(K_v) \) and the valuation ideal of \( R_v \). This proves the surjectivity.

**Corollary 4.2.** If the valuation \( v(\Delta(A)) \) of the discriminant is equal to 0 then the local images are given by

\[
\text{Im} \beta_i^v = U_0(K_v^{\times})/\left( K_v^{\times} \right)^{2i}
\]

and

\[
\text{Im} \alpha_i^v = W_i(k) + \varphi(W_i(K_v))/\varphi(W_i(K_v)).
\]

**Remark.** If \( A \) does not have good reduction at \( v \), we can still compute \( \text{Im} \alpha_i^v \). In order to do so, we calculate random points on \( A(K_v) \) and their images. To generate the points, we apply Hensel’s lemma and approximate their coordinates to a prescribed precision. Using Tate’s algorithm and the second or fourth equation of Proposition 4.1 we can determine the cardinality

\[
\# \text{Im} \alpha_i^v = \left[ K_v^{\times}/(K_v^{\times})^{2i} : \text{Im} \beta_i^v \right],
\]

and consequently we know when to stop our algorithm. For small examples this is really fast. But for increasing valuation of \( a_1 \), this step may cause trouble, as it gets more difficult to generate the random points in a way that the probability of their images generating \( \text{Im} \alpha_i^v \) is reasonable. The image of \( \beta_i^v \) is an infinite group. But it only takes finitely many computations to decide if a given element \( b \in K_v^{\times}/(K_v^{\times})^{2i} \) is in \( \text{Im} \beta_i^v \) or not. All we have to do is to test if \( b \) is orthogonal to \( \text{Im} \alpha_i^v \). Moreover, evaluating the Artin–Schreier–Witt pairing as described in [14] requires the arguments to be given only up to a finite precision.

5. **Global images**

Let \( K \) be a global function field and \( v \) a valuation of \( K \). Let \( A^{(2i)} \) have \( K \)-rational \( 2^i \)-torsion. The embedding \( K \to K_v \) induces homomorphisms

\[
\text{res}^v_{V^{(i)}} : W_i(K)/\varphi W_i(K) \to W_i(K_v)/\varphi W_i(K_v) \quad \text{and} \quad \text{res}^v_{F^{(i)}} : K^{\times}/(K^{\times})^{2i} \to K_v^{\times}/(K_v^{\times})^{2i}.
\]

The \( V^{(i)} \) - and \( F^{(i)} \)-Selmer group are respectively defined as

\[
\text{Sel}(K, V^{(i)}) := \{ w \in W_i(K)/\varphi W_i(K) \mid \text{res}^v_{V^{(i)}}(w) \in \text{Im} \alpha_i^v \text{ for all valuations } v \}
\]

and

\[
\text{Sel}(K, F^{(i)}) := \{ a \in K^{\times}/(K^{\times})^{2i} \mid \text{res}^v_{F^{(i)}}(a) \in \text{Im} \beta_i^v \text{ for all valuations } v \}
\]

\[
= \{ a \in K^{\times}/(K^{\times})^{2i} \mid [\text{Im} \alpha_i^v, \text{res}^v_{F^{(i)}}(a)] = 0 \text{ for all valuations } v \}
\]
PROPOSITION 5.1. For \( i = 1, 2 \), there are effective divisors \( D_j \) of \( \text{Div}(K) \) such that every element in \( \text{Sel}(K, V^i) \) has a representative \( b = (b_0, \ldots, b_{i-1}) \in W_i(K) \) where \( b_j \) is in the Riemann–Roch space \( L(D_j) \). At most one place where \( A \) has good reduction appears in the support of the \( D_j \).

Proof. We choose one place \( v_0 \) of \( K \) and arbitrary representatives in \( W_i(K) \) for the elements in \( \text{Sel}(K, V^i) \). To deal with the places \( v \neq v_0 \) where \( A \) has good reduction, we apply Artin–Schreier–Witt reduction to get new representatives for which the valuation of the components at \( v \) is either not negative or odd. Due to Corollary 4.2 the second case does not occur. As a result of the strong approximation theorem, the components of the new representatives will not have any new poles except at \( v_0 \). Afterwards we apply the same reduction to the remaining places different from \( v_0 \). This time it is possible for the components to have an odd, negative valuation. But, as the local image is finite, the valuation is bounded below. Finally, we reduce the valuation at \( v_0 \). Again we get a lower bound, but this time it depends not only on the finite image of \( \alpha^{-v_0} \) but also on the degree of \( v_0 \) and the genus of \( K \).

\[ \Box \]

REMARK. In order to calculate the divisors \( D_j \), one only has to compute the poles and zeros of the coefficients and the genus of \( K \). As a result we get representatives for a finite subset of \( W_i(K)/\varphi(W_i(K)) \) that contains \( \text{Sel}(K, V^i) \). To compute the elements that actually are in \( \text{Sel}(K, V^i) \) we have to find those that are contained in the local images \( \text{Im} \alpha_i^v \) for the finitely many places \( v \) of bad reduction. This task requires elements in \( K \) to be represented as Laurent series in \( K_v \), to a prescribed precision and Artin–Schreier polynomials to be factorized over \( K_v \).

For \( \text{Sel}(K, F^i) \) we can proceed in a similar fashion.

PROPOSITION 5.2. For \( i = 1, 2 \), there is a finite set \( S \) of places of \( K \) such that \( \text{Sel}(K, F^i) \) is a subset of

\[ K(S, 2^i) := \{ a \in K^\times/(K^\times)^{2^i} \mid v(a) \equiv 0 \pmod{2^i} \text{ for all } v \notin S \}. \]

If \( A^{(2^i)} \) has good reduction at \( v \), then \( v \) is not in \( S \).

Proof. This is a consequence of Corollary 4.2. \[ \Box \]

REMARK. The calculation of generators for \( K(S, 2^i) \) amounts to calculating generators for the \( S \)-class and the \( S \)-unit group of \( K \) (see, for example, [13]). In order to determine if an element \( a \in K(S, 2^i) \) is in \( \text{Sel}(K, F^i) \), we examine whether it is orthogonal to \( \text{Im} \alpha_i^v \) for the places of bad reduction. This requires a finite amount of evaluations of the Artin–Schreier–Witt pairing.

Finally, we want to compute the elements \( w = (w_0, \ldots, w_{i-1}) \) that are in \( \text{Sel}(K, V^i) \) (or \( a \in \text{Sel}(K, F^i) \)) that are in the image of \( \alpha_i \) (or \( \beta_i \)). Therefore we have to decide if there is a point \( P_w \in A(K) \) (or \( P_a \in A^{(2^i)}(K) \)) for which \( \alpha_i(P_w) = w \) (or \( \beta_i(P_a) = a \)) holds or not. For \( \alpha_i \) this results in the equations

\[ i = 1 : y^2 + a_1 xy + x^3 + a_2 x^2 + a_6 = 0 \]
\[
\frac{x + a_2}{a_1^2} = w_0 + z_0^2 + z_0,
\]
\[ i = 2 : y^2 + a_1 xy + x^3 + a_2 (s^2 + s)x^2 + a_6 = 0 \]
\[
\left( \frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^2 x^3} + \frac{a_6}{a_1^3 x} + \frac{sa_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right) = (w_0, w_1) + \varphi(z_0, z_1),
\]

in the variables $x, y, z_0, \ldots, z_{i-1}$. Their homogenizations define a projective curve $C_w$ over $K$ which is a covering of $A$. Artin–Schreier–Witt theory shows that this covering is unramified, thus has genus 1 and is cyclic of exponent $2^i$. Moreover, it is flat, hence étale and smooth. The points over $O \in A(K)$ define a $K$-rational divisor of degree $2^i$ on $C_w$. For $\beta_i$ we get similar results. This time the equations are

\[
\begin{align*}
i = 1 : & \ y^2 + a_1^2 y + x^3 + a_2^2 x^2 + a_3^2 = 0 \\
& x = a z^2,
\end{align*}
\]

\[
\begin{align*}
i = 2 : & \ y^2 + a_1^4 y + x^3 + a_2^4(s^2 + s)^4 x^2 + a_3^4 = 0 \\
y + \frac{1}{a_1^2} x^2 + a_4^4 s^4 x = a z^4,
\end{align*}
\]

in the variables $x, y, z$. Their homogenizations define a projective covering $C_a$ of the elliptic curve $A^{(2)}$. This covering is defined over $K$ and purely inseparable. A short computation using Tate’s genus formula shows that $C_a$ has genus 1 and is smooth. The preimage of $O \in A^{(2)}(K)$ under $C_a \to A^{(2)}$ is a $K$-rational divisor of degree $2^i$ on $C_a$. In [4] it is shown that smooth projective curves of genus 1 having a $K$-rational divisor of a specific degree, in our case 2 or 4, possess special models. As these models are advantageous for the computation of rational points we have to compute rational transformations from the aforementioned models to those presented in [4]. For $i = 1$ this amounts to using the second equation to eliminate $x$ in the first, followed by some obvious transformations. As a result, for $i = 1$ we get the models given by

\[
C_w : y^2 + (a_1 z^2 + a_2^2 z + (a_3^2 w_0 + a_4^2 a_2)) y + a_2^4 w_0 z^4 + (a_3^2 w_0 + a_4^2 + a_5 a_2) z^3
\]

\[
+ (a_4^2 w_0^2 + a_5^2 w_0 + a_6^2) z^2 + (a_1^5 w_0^4 + a_1 a_2^2) z + a_1^6 w_0^3 + a_2^2 a_3 w_0 + a_3 = 0
\]

and

\[
C_a : y^2 + a_2^2 a x y + a_4^2 a_6 a x^4 + a_5^2 a_2^2 x^2 z^2 + a_3^3 x^4 = 0
\]

in a weighted projective space. For $i = 2$ we can represent $C_w$ and $C_a$ as the intersection of two quadrics. This time it is too hard to find a transformation to such a model by hand. We can do it by using Magma for the computation of bases for some Riemann–Roch spaces. This results in formulas for the defining equations, but as they are rather lengthy we omit them. Deciding whether an element $w \in \text{Sel}(K, V^i)$ or $a \in \text{Sel}(K, F^i)$ is in the image of $\alpha_i$ or $\beta_i$ is equivalent to deciding if $C_w$ or $C_a$ possesses a $K$-rational point, and such a $K$-rational point yields a preimage on $A(K)$ or $A^{(2)}(K)$. The element $w$ (or $a$) is by construction in the local image of $\alpha_i^p$ (or $\beta_i^p$). Consequently, there is a $K_v$-rational point on $C_w$ (or $C_a$) for every valuation $v$ of $K$. Due to the failure of the Hasse principal for curves of genus 1, this does not imply the existence of a $K$-rational point. As described in [4], when performing a search for $K$-rational points on such a curve it is advantageous if the curve is given by a model with small coefficients. In [4] techniques to minimize and reduce the coefficients of the models we are dealing with are presented. The minimization algorithms can be applied to our situation without any modifications. A straightforward algorithm based on Groebner base computations over the constant field of $K$ can be used to reduce the coefficients. Sieving techniques as described in [18] prove to be useful for the computation of points on the minimized and reduced model. For the computation of Mordell–Weil bases, this calculation of rational points on the homogeneous spaces is a major bottleneck. Here the models given by the $\alpha_2$- and $\beta_2$-descent are often advantageous. Assuming a point $P$ on $A(K)$ can be computed as a preimage of a point on a homogeneous space $C_1$ for $\alpha_1$ (or $\beta_1$) and as a preimage of a point $C_2$ for $\alpha_2$ (or $\beta_2$), and assuming the models both for $i = 1$ and for $i = 2$ are minimized and reduced, then in general $C_2(K)$ will have a point that has roughly one half of the height of the smallest
point on $C_1(K)$. The rank of the elliptic curve $A$ given by
\[y^2 + (t^4 + t^3 + t^2 + 1)xy + x^3 + (t^4 + t^3 + t^2) = 0\]
over $\mathbb{F}_2(t)$ is 1. But even though the coefficients of the Weierstrass equation are small, finding a point of infinite order on $A(K)$ using a $V$- and $F$-descent is very time-consuming. Using a $V^2$- and $F^2$-descent instead, it only takes a few minutes.

6. Heights and infinite descent
Siksek [10] presents an algorithm to compute a Mordell–Weil basis for an elliptic curve over a number field given the generators of a subgroup of finite index. With minor modifications, this algorithm can also be applied over global function fields of characteristic 2. All we need is an estimate of the difference between the naive height $h$ and the canonical height $\hat{h}$. Such an estimate can be achieved by the same means as described in [12]. As a result we get the following proposition.

**Proposition 6.1.** Let $A$ be an elliptic curve over a global function field $K$ given by a Weierstrass equation. Denote the $j$-invariant of $A$ by $j$. Then for every $P = (x, y) \in A(K)$ the inequality
\[h(P) - \hat{h}(P) \leq \frac{1}{12}h(j) + C\]
holds. Here $C$ is a constant that depends only on the poles of the coefficients of a Weierstrass equation of $A$. It can be calculated explicitly.

**Proof.** Silverman’s method for elliptic curves over number fields can also be applied over global function fields. The term $\frac{1}{12}h(j)$ is due to the difference of the local height function and the valuation of the $x$-coordinate for points on an elliptic curve with integral coefficients. For the poles of the coefficients of $A$ we have to transform the model. In this way the constant $C$ comes into existence.

Another way to obtain an upper bound for the difference of the naive and the canonical height is described in [10] and [5]. Their techniques can also be applied in our situation.

7. $S$-integral points
Let $S$ be a finite set of valuations of $K$, and let $A$ be an ordinary elliptic curve given by the Weierstrass equation
\[y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0,\]
where the coefficients $a_i$ do not have any poles outside of $S$. We call a point $P = (x_0, y_0) \in K^2$ that satisfies the Weierstrass equation $S$-integral if and only if $x_0$ hence also $y_0$ do not have poles outside of $S$. As shown by Voloch in [17], an ordinary elliptic curve whose $j$-invariant is transcendental over the constant field of $K$ has finitely many $S$-integral points (see also [2] and [3]). We use Voloch’s methods to compute an upper bound for their naive height. Combining $\alpha_1$ and $\beta_1$, we get a homomorphism
\[\mu : A(K) \rightarrow K, \ (x, y) \mapsto \frac{a_6}{a_1^2x^2} + \varphi \left( \frac{a_6\delta x}{x} \right).\]
Here $\delta$ is given by $\delta = d/da_6$ assuming $a_6$ is not a square in $K$ and $\varphi(z) = z^2 + z$. See [17] for details and proofs. The kernel of $\mu$ is $2A(K)$, hence its image is finite. Given generators for a subgroup of odd finite index of $A(K)$ (e.g. a Mordell–Weil basis), one can easily compute $\text{Im} \mu$ because it is generated by the images.
Due to the addition law, we have computed explicitly.

**Example 1**

In this section we apply our algorithm to different examples. The computations are carried out by our Magma implementation.

8. **Examples**

In this section we apply our algorithm to different examples. The computations are carried out by our Magma implementation.

8.1. **Example 1**

First we consider the elliptic curve $A$ given by

$$A : y^2 + x y + x^3 + t^{12} + t^{10} + t^8 + t^6 + t^4 + t^2 + t + 1 = 0$$

over the rational function field $\mathbb{F}_2(t)$. We compute the $V$- and the $F$-Selmer group. This takes less than a second. The places of bad reduction are $(t^2 + t + 1), (t^6 + t^5 + t^4 + t^2 + 1)$.
and \((1/t)\). Following Proposition 5.1, we see that the Riemann–Roch space \(\mathcal{L}(3(1/t))\) contains representatives for the image of \(\alpha_1\). The local image of \(\alpha_1\) at \((t^2 + t + 1)\) and \((t^6 + t^5 + t^3 + t^2 + 1)\) is trivial. Hence the elements in the \(V\)-Selmer group possess representatives that vanish at \((t^2 + t + 1)\) and \((t^6 + t^5 + t^3 + t^2 + 1)\). The cardinality of the local image of \(\alpha_1\) at \((1/t)\) is 4. We compute it by randomly generating sufficiently many points on \(A\) defined over \(\mathbb{F}_2((1/t))\). Combining the local information proves that the \(V\)-Selmer group is generated by the classes of 1 and \(t^3\). The \(F\)-Selmer group is generated by the class of \(t^8 + t + 1\) and \(t^2 + t + 1\). The non-trivial 2-torsion point on \(A^{(2)}\) is a preimage of \(t^8 + t + 1\) under \(\beta_1\). Therefore the rank of \(A(\mathbb{F}_2(t))\) is at most 3 and the preimages of 1 and \(t^3\) under \(\alpha_1\) plus the image of \(Q\) under the Verschiebung, where \(Q\) is a preimage of \(t^2 + t + 1\), generate a subgroup of finite index. The preimages of 1 correspond to \(\mathbb{F}_2(t)\)-rational points on the curve of genus 1 given by

\[
y^2 + (x^2 + xz + z^2)y = x^4 + xz^3 + (t^{12} + t^{10} + t^8 + t^6 + t^4 + t^2 + t + 1)z^4.
\]

We minimize it, reduce it and transform it into the intersection of two quadrics. This takes about a minute and yields the model given by the equations

\[
\begin{align*}
(t + 1)x_1^2 + tx_1x_2 + (t^3 + t + 1)x_1x_3 + (t^2 + 1)x_1x_4 + (t^2 + t)x_2x_3 + (t^4 + t^3 + t)x_2x_3 + (t^2 + 1)x_2x_4 + t^3x_2^2 + (t^3 + t)x_3x_4 + (t^2 + t + 1)x_4^2 &= 0, \\
(t^3 + t^2 + t)x_1^2 + (t^3 + t^2 + 1)x_1x_2 + (t^3 + t)x_1x_3 + (t^3 + t^2 + t + 1)x_2x_3 + (t^3 + t^2 + 1)x_2x_4 + t^2x_2^2 + (t^3 + 1)x_3x_4 + (t^3 + t^2 + t)x_4^2 &= 0.
\end{align*}
\]

A sieving algorithm computes the point

\[(t + 1, t^4 + t^2, t^2 + 1, 1)\]

in a few seconds. This point yields the point

\[(t^2 + t + 1, t^6 + t^5 + t^3 + t + 1)\]

on \(A(\mathbb{F}_2(t))\). In the same manner we calculate

\[
\left(\frac{t^9 + t^7 + t^5 + t^4 + t^3 + t^2 + t}{t^6 + t^4 + 1}, \frac{t^{15} + t^8 + t^6 + t^5 + t^4 + 1}{t^9 + t^8 + t^7 + t^4 + t^3 + t^2 + 1}\right),
\]

which is a preimage of \(t^3\). Calculating a preimage for \(t^2 + t + 1\) yields the point

\[(t^6 + t^5 + t^4 + t^2 + t + 1, t^{12} + t^{10} + t^8 + t^6 + t^5 + t^4 + t^2 + t)\]

on \(A^{(2)}(\mathbb{F}_2(t))\). Its image under the Verschiebung is

\[
\left(\frac{t^3 + t^2 + t}{t^4 + 1}, \frac{t^{12} + t^{11} + t^9 + t^8 + t^2 + t + 1}{t^6 + t^4 + t^2 + 1}\right)
\]

on \(A(\mathbb{F}_2(t))\). These points could also be calculated using a \(V^2\)- and \(F^2\)-descent. We compute the \(V^2\)- and \(F^2\)-Selmer groups. The former is generated by the classes of the Witt vectors \((0, t^3), (1, t^5 + t^7),\) and \((t^3, t^5 + t^3 + 1),\) the latter by \(1/(t^4 + t^2 + 1)\) and \(1/(t^8 + t + 1)\). Calculating explicit models for the corresponding homogeneous spaces and \(\mathbb{F}_2(t)\)-rational points on them yields the same points on \(A(\mathbb{F}_2(t))\). These three points are \(\mathbb{Z}\)-linearly independent and generate a subgroup \(G\) of finite index of \(A(K)\). Their regulator is 30. The estimate of the difference between the naive and the canonical height together with a brute force search for small points shows that there are no points of canonical height less than \(\frac{7}{6}\). Hence the index \([A(\mathbb{F}_2(t)) : G]\)
is at most 12. See [10] for more information. A short computation reveals that the index is equal to 9, and a Mordell–Weil basis is given by

\[
\begin{pmatrix}
    t^9 + t^7 + t^5 + t^4 + t^3 + t^2 + t & t^{15} + t^8 + t^6 + t^5 + t^4 + 1 \\
    t^6 + t^4 + 1 & t^9 + t^8 + t^2 + t^3 + t^2 + 1
\end{pmatrix},
\]

\((t^2 + t + 1, t^6 + t^5 + t^3 + t + 1), \ (t^3 + t^2 + t, t^6 + t^5 + t^2 + 1).\)

Set \(S := \{1/t\}\). Then the Weierstrass equation for \(A\) has coefficients that are \(S\)-integral. With the method mentioned in §7, it can be seen that 12 is an upper bound for the naive height of an \(S\)-integral point. Iterating over the possible \(x\)-coordinates, we compute 20 different \(S\)-integral points. In [6] the authors describe a method to transform a bound for the naive height into a bound for the absolute value of the coefficients of a representation of an \(S\)-integral point as a linear combination in the Mordell–Weil basis. In our case the bound for the Mordell–Weil coefficients is 8. Iterating over the possible coefficients yields the same 20 points.

8.2. Example 2

Ulmer [15] constructs the family \(A_n\) of elliptic curves over \(\mathbb{F}_q(t)\) defined by the Weierstrass equations

\[A_n : y^2 + xy = x^3 + t^{2n+1}.\]

Without constructing any points, he proves that the rank of \(A_n(\mathbb{F}_q(t))\) is greater than or equal to \((2^n - 1)/2n\). We use our implementation to compute the rank and independent points on \(A_n(\mathbb{F}_q(t))\) for \(q = 2\) and \(n = 1, \ldots, 5\). As a result we get

\[
\begin{align*}
n & = 1 : \text{rank}(A_1(\mathbb{F}_2(t))) = 1 \\
 & \text{points: } (t, 0); \\
n & = 2 : \text{rank}(A_2(\mathbb{F}_2(t))) = 1 \\
 & \text{points: } (t^2, t^3); \\
n & = 3 : \text{rank}(A_3(\mathbb{F}_2(t))) = 2 \\
 & \text{points: } (t^3, 0), (t^4, t^6 + t^3); \\
n & = 4 : \text{rank}(A_4(\mathbb{F}_2(t))) = 2 \\
 & \text{points: } (t^6 + t^5 + t^4 + t^2, t^9 + t^5 + t^2), (t^8, t^{12} + t^{10} + t^9); \\
n & = 5 : \text{rank}(A_5(\mathbb{F}_2(t))) = 4 \\
 & \text{points: } (t^{12} + t^9, t^{18} + t^{12} + t^9), (t^{11}, 0), (t^{16}, t^{24} + t^{20} + t^{18} + t^{17}), \\
& \quad \left(\frac{t^{22} + t^{20} + t^{16} + t^{15} + t^{10} + t^6}{t^8 + t^6 + 1}, \frac{t^{33} + t^{32} + t^{31} + t^{26} + t^{24} + t^{23} + t^{16} + t^{15} + t^{12}}{t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^6 + t^4 + t^3 + 1}\right).
\end{align*}
\]

For these five curves, the rank of \(A_n(\mathbb{F}_2(t))\) is equal to \([((2^n - 1)/2n)\].

References


G. Moehlmann
*Institut für Mathematik*
*Technische Universität Berlin*
*Straße des 17. Juni 136*
*D-10623 Berlin*
*Germany*

moehlman@math.tu-berlin.de