ARTICLE IN PRESS YJNTH:6073

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The rational points on certain Abelian varieties over function fields ☆

Sajad Salami

Instituto de Matemática e Estatística, Universidade Estadual do Rio de Janeiro, Brazil

ARTICLE INFO

Article history:
Received 25 July 2017
Received in revised form 16 June 2018
Accepted 27 June 2018
Available online xxxx
Communicated by A. Pal

MSC:
11G10
14H40

Keywords:
Mordell–Weil rank
Abelian variety
Function field of varieties
Prym varieties of the cyclic covers
Jacobian variety

ABSTRACT

In this paper, we consider Abelian varieties over function fields that arise as twists of Abelian varieties by cyclic covers of irreducible quasi-projective varieties. Then, in terms of Prym varieties of the cyclic covers, we prove a structure theorem on their Mordell–Weil group. Our results give an explicit method to construct elliptic curves, hyper- and super-elliptic Jacobians that have large ranks over function fields of certain varieties.

1. Introduction and main results

Let $\mathcal{A}$ be an Abelian variety defined over an arbitrary global field k. By famous Mordell–Weil Theorem, the set $\mathcal{A}(k)$ of k-rational points on A is a finitely generated abelain group [6]. In other words, one has $\mathcal{A}(k) \cong \mathcal{A}(k)_{tors} \oplus \mathbb{Z}^r$ where $\mathcal{A}(k)_{tors}$ is a

☆ This work is a part of the author's PhD thesis in IM-UFRJ, Brazil, 2017.
E-mail address: sajad.salami@ime.uerj.br.

https://doi.org/10.1016/j.jnt.2018.06.008
0022-314X/© 2018 Published by Elsevier Inc.

finite subgroup of $\mathcal{A}(k)$ called the *torsion subgroup*, and r is a non-negative number called the *(Mordell–Weil) rank* of $\mathcal{A}$ over k and denoted by $\mathrm{rk}(\mathcal{A}(k))$. It is a mysterious quantity associated to an Abelian variety. Finding Abelian varieties with large ranks is one of the most challenging problems in Arithmetic and Diophantine geometry.

For example, when $\mathcal{A}$ is an elliptic curve defined over $k = \mathbb{Q}$, it is a folklore conjecture that the rank can be arbitrary large [12]. This conjecture should now be regarded as being in serious doubt by the results of J. Park and et al., in [10]. In short, they predict that the number of elliptic curves over $\mathbb{Q}$ with rank ≥ 21 is finite. However, in 2006, Elkies presented an elliptic curve over $\mathbb{Q}$ with 28 independent generators. In the case of the quadratic number fields, Najman showed that there exists an elliptic curve of rank at least 30 over $k = \mathbb{Q}(\sqrt{-3})$. To see the equation of these curves and more information on the high rank elliptic curves over rational numbers and quadratic number fields, we refer the reader to [3].

In contrast, for any prime p, there are known explicit elliptic curves over $k = \mathbb{F}_p(t)$ with arbitrary large rank [13,14]. In the case $k = \mathbb{C}(t)$, it has been proved that for a very general elliptic curve E over k with height $d \geq 3$ and every finite rational extension k' of k the Mordell–Weil group $E(k')$ is a trivial group, see [15].

In this paper, we generalize the main result of Hazama in [5] to arbitrary cyclic s-covers of irreducible quasi-projective varieties for any integer $s \geq 2$. We fix a global field k of characteristic 0 or a prime number $p \geq 2$ not dividing s that contains an s-th root of unity denoted by ζ. Let us denote by $\mathcal{A}[s](k)$ the subgroup of k-rational s-division points of $\mathcal{A}$. Assume that there exists an automorphism $\sigma \in \mathrm{Aut}(\mathcal{A})$ of order s. Given the irreducible quasi-projective varieties $\mathcal{V}$ and $\mathcal{V}'$ with function fields $\mathcal{K}$ and $\mathcal{K}'$, respectively, we denote Prym variety of the cyclic s-cover $\pi : \mathcal{V}' \to \mathcal{V}$ by $\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}}$, all defined over k. See Section 2 for the definition and some of the properties of $\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}}$. Let $G = \langle\gamma\rangle$ be the order s cyclic Galois group of the extension $\mathcal{K}'|\mathcal{K}$. Denote by $\mathcal{A}_a$ the twist of $\mathcal{A}$ with the extension $\mathcal{K}'|\mathcal{K}$, equivalently by the 1-cocycle $a = (a_u) \in Z^1(G, \mathrm{Aut}(\mathcal{A}))$ given by $a_{id} = id$ and $a_{\gamma^j} = \sigma^j$ for each $\gamma^j \in G$, see [2,4] for more on Twist Theory. Then, we have the following theorem which is the main result of this article.

Theorem 1.1. *Notation being as above, assume that there exists a k-rational point $v'_0 \in \mathcal{V}'(k)$. Then, as an isomorphism of Abelian groups, we have:*

$$\mathcal{A}_a(\mathcal{K}) \cong Hom_k(Prym_{\mathcal{V}'/\mathcal{V}}, \mathcal{A}) \oplus \mathcal{A}[s](k).$$

Moreover, if $Prym_{\mathcal{V}'/\mathcal{V}}$ is k-isogenous to $\mathcal{A}^n \times \mathcal{B}$ for some positive integer n and an Abelian variety $\mathcal{B}$ over k, where $\dim(\mathcal{B}) = 0$ or $\dim(\mathcal{B}) > \dim(\mathcal{A})$ with no irreducible component k-isogenous to $\mathcal{A}$, then $rk(\mathcal{A}_a(\mathcal{K})) \geq n \cdot rk(End_k(\mathcal{A}))$.

For any curve $\mathcal{C}$, let $J(\mathcal{C})$ be the Jacobian variety of $\mathcal{C}$ and denote by $J(\mathcal{C})[s](k)$ its subgroup of k-rational and s-division points. As an application of the above Theorem, for given integers $s \geq 2$ and $1 \leq r \leq n$, we consider the cyclic s-cover $\pi : \mathbf{C}_n \to \mathbf{V}_n$ where

Please cite this article in press as: S. Salami, The rational points on certain Abelian varieties over function fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.008

$\mathbf{C}_n$ is the product of n copies of the curve $\mathcal{C}_{s,f}$ given by the affine equation $y^s = f(x)$, where $f(x) \in k[x]$ of degree r and non-zero discriminate, and $\mathbf{V}_n$ is the quotient of $\mathbf{C}_n$ by a certain cyclic subgroup of $\mathrm{Aut}(\mathbf{C}_n)$ of order s, see Section 5. Let $\mathcal{C}^{\xi}_{s,f}$ be the twist of $\mathcal{C}_{s,f}$ by the cyclic extension $L|K$, where $K = k(\mathbf{V}_n)$ and $L = k(\mathbf{C}_n)$. We have the following result.

Theorem 1.2. *With the above notations and assuming that there exists some k-rational point $c \in \mathcal{C}_{s,f}(k)$, we have*

$$J(\mathcal{C}^{\xi}_{s,f})(K) \cong \big(End_k(J(\mathcal{C}_{s,f}))\big)^n \oplus J(\mathcal{C}_{s,f})[s](k),$$

as an isomorphism of Abelian groups; and hence,

$$rk(J(\mathcal{C}^{\xi}_{s,f})(K)) \geq n \cdot rk(End_k(J(\mathcal{C}_{s,f}))).$$

The structure of this paper is as follows. In Section 2, we investigate some of the properties of Prym varieties of the cyclic covers of quasi-projective varieties. In Section 3, we recall the main result of Hazama from [5] that we are going to extend in this paper. Finally, we prove Theorems 1.1 and 1.2 in Sections 4 and 5, respectively.

2. Prym varieties of the cyclic covers

The notion of Prym variety was introduced by Mumford in [9] and has been extensively studied for double covers of curves in [1]. It has been generalized to the double covers of irreducible quasi-projective varieties in [5]. Here, we generalize this notion to the case of cyclic s-covers of varieties.

Definition 2.1. For an integer $s \geq 2$, the Prym variety of the cyclic s-cover $\pi : \mathcal{V}' \to \mathcal{V}$ of irreducible quasi-projective varieties over k is defined by the quotient Abelian variety

$$\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}} := \frac{\mathrm{Alb}(\mathcal{V}')}{\mathrm{Im}(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1})},$$

where $\mathrm{Alb}(\mathcal{V}')$ is Albanese variety and $\tilde{\gamma}$ is the automorphism of $\mathrm{Alb}(\mathcal{V}')$ induced by an order s automorphism $\gamma \in \mathrm{Aut}(\mathcal{V}')$ defined over k.

We note that if both of the varieties $\mathcal{V}$ and $\mathcal{V}'$ are curves, then this definition is compatible with the one given in [8], according to the following lemma.

Lemma 2.2. *Given an integer $s \geq 2$, let $\pi : \mathcal{V}' \to \mathcal{V}$ be a cyclic s-cover of irreducible quasi-projective varieties, both as well as π defined over k. Suppose that $\gamma \in Aut(\mathcal{V}')$ is an automorphism of order s defined over k. Denote by $\tilde{\gamma}$ the automorphism of $Alb(\mathcal{V}')$ induced by γ. Then there is a k-isogeny of Abelian varieties,*

Please cite this article in press as: S. Salami, The rational points on certain Abelian varieties over function fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.008

$$Prym_{\mathcal{V}'/\mathcal{V}} \sim_k \ker(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1} : Alb(\mathcal{V}') \to Alb(\mathcal{V}'))^\circ,$$

where $(*)^\circ$ *means the connected component of its origin.*

Proof. Let $\mathcal{A} = \mathrm{Alb}(\mathcal{V}')$ and define $m = \dim \mathcal{A}$, $m_1 := \dim \ker(id - \gamma)^\circ$, and $m_2 := \dim \ker(id + \gamma + \cdots + \gamma^{s-1})^\circ$. Then, $m = m_1 + m_2$ by considering the induced action on the tangent space of $\mathcal{A}$ at the origin. We have $\gamma(P) = P$ for all $P \in \ker(id - \gamma)^\circ \cap \ker(id + \gamma + \cdots + \gamma^{s-1})^\circ$, so $0 = (id + \gamma + \cdots + \gamma^{s-1})(P) = sP$ which implies that $\ker(id - \gamma)^\circ \cap \ker(id + \gamma + \cdots + \gamma^{s-1})^\circ \subseteq \mathcal{A}[s]$. This shows the k-isogeny,

$$\mathcal{A} \sim_k \ker(id - \gamma)^\circ \times \ker(id + \gamma + \cdots + \gamma^{s-1})^\circ.$$

Moreover, we note that $\mathrm{Im}(id + \gamma + \cdots + \gamma^{s-1}) \subseteq \ker(id - \gamma)^\circ$ and

$$m - m_2 = \dim \mathrm{Im}(id + \gamma + \cdots + \gamma^{s-1}) = \dim \ker(id - \gamma)^\circ = m_1.$$

Therefore, $\mathrm{Im}(id + \gamma + \cdots + \gamma^{s-1}) = \ker(id - \gamma)^\circ$ that gives the desired result. □

Here, we describe a general method to construct new s-cover using the given ones. Then, we determine the relation between their Prym Varieties. We will use this result in the proof of Theorem 1.2.

For $i = 1, 2$, let $\pi_i : \mathcal{V}'_i \to \mathcal{V}_i$ be s-covers of irreducible quasi-projective varieties, all defined over k. Assume that there exists some k-rational simple point $v'_i \in \mathcal{V}'_i$. Denote by G_i the cyclic Galois group of the corresponding function field extensions. Then, the covering $\pi_1 \times \pi_2 : \mathcal{V}'_1 \times \mathcal{V}'_2 \to \mathcal{V}_1 \times \mathcal{V}_2$ has Galois group $G_1 \times G_2 \cong \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. Suppose that $\mathcal{W}$ is its intermediate cover $\mathcal{V}'_1 \times \mathcal{V}'_2/G$, where G is the group generated by $\gamma = (\gamma_1, \gamma_2) \in \mathrm{Aut}(\mathcal{V}'_1 \times \mathcal{V}'_2)$. Let $\tilde{\gamma} = (\tilde{\gamma}_1, \tilde{\gamma}_2)$ be the order s automorphism in $\mathrm{Aut}(\mathrm{Alb}(\mathcal{V}'_1) \times \mathrm{Alb}(\mathcal{V}'_2))$ corresponding to γ where $\tilde{\gamma}_i$ is an automorphism of $\mathrm{Alb}(\mathcal{V}'_i)$ induced by $\gamma_i \in \mathrm{Aut}(\mathcal{V}'_i)$ of order $s \geq 2$ for $i = 1, 2$. Then there exists a k-rational isomorphism

$$\phi := \mathrm{Alb}(\mathcal{V}'_1) \times \mathrm{Alb}(\mathcal{V}'_2) \to \mathrm{Alb}(\mathcal{V}'_1 \times \mathcal{V}'_2)$$

given by $\phi = \tilde{\phi}_1 + \tilde{\phi}_2$ where $\tilde{\phi}_i : \mathrm{Alb}(\mathcal{V}'_i) \to \mathrm{Alb}(\mathcal{V}'_1) \times \mathrm{Alb}(\mathcal{V}'_2)$ is induced by the inclusion map $\phi_i : \mathcal{V}'_i \to \mathcal{V}'_1 \times \mathcal{V}'_2$ defined by $\phi_1(v) = (v, v'_2)$ and $\phi_2(v) = (v'_1, v)$. By this isomorphism, we have $\ker(\mu) \sim_k \ker(\mu_1) \times \ker(\mu_2)$, where $\mu := id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1}$ and $\mu_i := id + \tilde{\gamma}_i + \cdots + \tilde{\gamma}_i^{s-1}$ for $i = 1, 2$. This implies that $\ker(\mu)^\circ \sim_k \ker(\mu_1)^\circ \times \ker(\mu_2)^\circ$. Therefore, applying Lemma 2.2 and putting everything together, we conclude the following result.

Proposition 2.3. *As a k-rational isogeny of Abelian varieties, we have*

$$Prym_{\mathcal{V}'_1 \times \mathcal{V}'_2/\mathcal{W}} \sim_k Prym_{\mathcal{V}'_1/\mathcal{V}_1} \times Prym_{\mathcal{V}'_2/\mathcal{V}_2}.$$

3. The result of Hazama

In [4,5], using the twist theory [2,4], Hazama gives an explicit method for construction of Abelian varieties with large rank over function fields. In [16], Wang extended the result of [4] to cyclic covers of the projective line with prime degrees. Inspired by Hazama's result, in [17], Yamagishi reduced the problem of identifying the elliptic curves of rank $1 \le n \le 7$ with given x-coordinate of generators to the problem of finding rational points on certain varieties. By providing a parametrization for the rational points on those varieties, she obtained all of the elliptic curves of rank $1 \le n \le 7$ defined over a field of characteristic different from two.

Here, we briefly recall the main result of Hazama from [5]. Let $\mathcal{A}$ be an Abelian variety over k with characteristic different from two. Suppose that $\pi : \mathcal{V}' \to \mathcal{V}$ is a double cover with Prym variety $\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}}$, of irreducible quasi-projective varieties $\mathcal{V}$ and $\mathcal{V}'$ defined over k. Let $\mathcal{K}$ and $\mathcal{K}'$ be the function fields of $\mathcal{V}$ and $\mathcal{V}'$, respectively, and G be the Galois group of the extension $\mathcal{K}'|\mathcal{K}$. Denote by $\mathcal{A}_a$ the twist of $\mathcal{A}$ by the extension $\mathcal{K}'|\mathcal{K}$, equivalently by the 1-cocycle $a = (a_u) \in Z^1(G, Aut(\mathcal{A}))$ given by $a_{id} = id$ and $a_\iota = -id$.

Theorem 3.1. *With the above notations, assume that there exists a k-rational simple point $v'_0 \in \mathcal{V}'$. Then we have an isomorphism of Abelian groups,*

$$\mathcal{A}_a(\mathcal{K}) \cong Hom_k(Prym_{\mathcal{V}'/\mathcal{V}}, \mathcal{A}) \oplus \mathcal{A}[2](k).$$

Moreover, if $Prym_{\mathcal{V}'/\mathcal{V}}$ is k-isogenous with $\mathcal{E}^n \times \mathcal{B}$ for some positive integer n, where $\mathcal{E}$ is an elliptic curve over k and $\mathcal{B}$ is an Abelian variety with no simple component k-isogenous to $\mathcal{E}$, then $rk(\mathcal{A}_b(\mathcal{K})) = n \cdot rk(End_k(\mathcal{E}))$.

We refer the reader to Theorem 2.2 and Corollary 2.3 in [5] to see the proof.

4. Proof of Theorem 1.1

Suppose that the natural map $i_{\mathcal{V}'} : \mathcal{V}' \to \mathrm{Alb}(\mathcal{V}')$ sends v'_0 to the origin of $\mathrm{Alb}(\mathcal{V}')$ so that $i_{\mathcal{V}'}$ is defined over k. Then, using Theorem 4 of Chapter II in [7], we have $\mathcal{A}(\mathcal{K}') = \{k\text{-rational maps } \mathcal{V}' \to \mathcal{A}\} \cong \mathrm{Hom}_k(\mathrm{Alb}(\mathcal{V}'), \mathcal{A}) \oplus \mathcal{A}(k)$, where $P \in \mathcal{A}(\mathcal{K}')$ corresponds to the pair $(\lambda, Q) \in \mathrm{Hom}_k(\mathrm{Alb}(\mathcal{V}'), \mathcal{A}) \oplus \mathcal{A}(k)$ such that $P(v') = \lambda(i_{\mathcal{V}'}(v')) + Q$ for each $v' \in \mathcal{V}'$. This implies that the action of $\gamma^j \in G$ is given by $\gamma^j(\lambda, Q) = (\lambda \circ \tilde{\gamma}^j, Q)$ for $j = 0, \cdots, s-1$, where $\tilde{\gamma}$ is the automorphism of the Albanese variety $\mathrm{Alb}(\mathcal{V}')$ induced by $\gamma \in \mathrm{Aut}(\mathcal{V}')$. Since $\gamma^s = id$ and hence $\tilde{\gamma}^s = id$, so

$$\mathcal{A}_a(\mathcal{K}) \cong \{P \in \mathcal{A}(\mathcal{K}') : b_{\gamma^j} \cdot^{\gamma^j} (P) = P, \ \forall \gamma^j \in G\},$$

by applying Proposition 1.1 in [4]. This implies that $(\lambda, Q) \in \mathcal{A}_a(\mathcal{K})$ if and only if $\gamma^j(\lambda, Q) = (\lambda \circ \tilde{\gamma}^j, Q) = (\lambda \circ \tilde{\gamma}^{s-j}, Q) = \gamma^{s-j}(\lambda, Q)$. Thus $(\lambda, Q) \in \mathcal{A}_a(\mathcal{K})$ if and only if λ annihilates $\mathrm{Im}(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1})$ and $Q \in \mathcal{A}[s](k)$. Therefore,

Please cite this article in press as: S. Salami, The rational points on certain Abelian varieties over function fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.008

$$\mathcal{A}_a(\mathcal{K}) \cong \mathrm{Hom}_k(\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}}, \mathcal{A}) \oplus \mathcal{A}[s](k).$$

Furthermore, if we assume that $\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}}$ is k-isogenous with $\mathcal{A}^n \times \mathcal{B}$ for some positive integer n and some Abelian variety $\mathcal{B}$ defined over k such that $\dim(\mathcal{B}) = 0$ or $\dim(\mathcal{B}) > \dim(\mathcal{A})$ with no irreducible component k-isogenous to $\mathcal{A}$, then

$$\begin{aligned}
\mathcal{A}_a(\mathcal{K}) &\cong \mathrm{Hom}_k(\mathrm{Prym}_{\mathcal{V}'/\mathcal{V}}, \mathcal{A}) \oplus \mathcal{A}[s](k) \\
&\cong \mathrm{Hom}_k(\mathcal{A}^n \times \mathcal{B}, \mathcal{A}) \oplus \mathcal{A}[s](k) \\
&\cong \mathrm{Hom}_k(\mathcal{A}^n, \mathcal{A}) \oplus \mathrm{Hom}_k(\mathcal{B}, \mathcal{A}) \oplus \mathcal{A}[s](k) \\
&\cong (End_k(\mathcal{A}))^n \oplus \mathrm{Hom}_k(\mathcal{B}, \mathcal{A}) \oplus \mathcal{A}[s](k).
\end{aligned}$$

Therefore, as $\mathbb{Z}$-modules, we have $\mathrm{rk}(\mathcal{A}_a(\mathcal{K})) \geq n \cdot \mathrm{rk}(\mathrm{End}_k(\mathcal{A}))$.

5. The proof of Theorem 1.2

Given the integers $s \geq 2$ and $1 \leq r \leq n$, fix a polynomial $f(x) \in k[x]$ of degree r and non-zero discriminant. Consider the curve $\mathcal{C}_{s,f} : y^s = f(x)$ with a rational point $c \in \mathcal{C}_{s,f}(k)$ that admits an order s automorphism $\iota : (x, y) \mapsto (x, \zeta \cdot y)$. For each $1 \leq i \leq n$, let $\mathcal{C}_{s,f}^{(i)}$ be a copy of $\mathcal{C}_{s,f}$ defined by the affine equation $y_i^s = f(x_i)$ and denote by ι_i the corresponding automorphism for each of these curves. Define $\mathbf{C}_n := \prod_{i=1}^n \mathcal{C}_{s,f}^{(i)}$ which can be expressed by the simultaneous equations $y_i^s = f(x_i)$ for $i = 1, \cdots, n$. Let $G = \langle \gamma \rangle$ be the order s cyclic subgroup of $\mathrm{Aut}(\mathbf{C}_n)$, where $\gamma := (\iota_1, \cdots, \iota_n)$, and define $\mathbf{V}_n := \mathbf{C}_n/G$. If we assume that L is the function field of $\mathbf{C}_n$, i.e., $L = k(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$ where $x_1, x_2, \cdots, x_n$ are independent transcendental variables and each y_i defines a degree s extension by the equation $y_i^s - f(x_i) = 0$, then $K = k(\mathbf{V}_n)$ the function field of $\mathbf{V}_n$ is equal to the set of all G-invariant elements of L, i.e.,

$$K = L^G = k(x_1, \cdots, x_n, y_1^{s-1} y_2, \cdots, y_1^{s-1} y_{n-1}).$$

Since $(y_1^{s-1} y_{i+1})^s = f(x_1)^{s-1} f(x_{i+1})$ holds for $i = 1, \cdots, n-1$, so by defining $z_i := y_1^{s-1} y_{i+1}$ the variety $\mathbf{V}_n$ can be expressed by $z_i^s = f(x_1)^{s-1} f(x_{i+1})$ for $i = 1, \cdots, n-1$. Hence $L|K$ is a cyclic extension of degree s determined by $y_1^s = f(x_1)$, i.e.,

$$L = K(y_1) = k(x_1, \cdots, x_n, z_1, \cdots, z_{n-1})(y_1).$$

Define $\mathcal{C}_{s,f}^{\xi}$ to be the twist of $\mathcal{C}_{s,f}$ by the extension $L|K$. In a similar way as Corollary 3.1 in [4], one can see that $\mathcal{C}_{s,f}^{\xi}$ is defined by the affine equation $f(x_1) z^s = f(x)$. It is also easy to check that $\mathcal{C}_{s,f}^{\xi}$ contains the following K-rational points:

$$P_1 := (x_1, 1) \text{ and } P_i := (x_{i+1}, z_i/f(x_1)) \;\text{ for } (1 \leq i \leq n-1). \tag{1}$$

Please cite this article in press as: S. Salami, The rational points on certain Abelian varieties over function fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.008

Remark 5.1. The construction of $\mathbf{C}_n$ and $\mathbf{V}_n$ generalizes that given by Yamagishi in [17], which is used to characterize the elliptic curves of rank ≤ 7 with a given set of algebraic numbers as x-coordinates of the generators of their Mordell–Weil group.

By the fact that the Albanese and Jacobian varieties of curves coincide and applying Lemma 2.2 to $\mathcal{V}' = \mathcal{C}_{s,f}^{(i)} = \mathcal{C}_{s,f}$ and $\mathcal{V} = \mathbb{P}^1$, we have

$$\mathrm{Prym}_{\mathcal{C}_{s,f}^{(i)}/\mathbb{P}^1} = \frac{J(\mathcal{C}_{s,f}^{(i)})}{\mathrm{Im}(id + \tilde{\iota} + \cdots + \tilde{\iota}^{s-1})} \sim_k \ker\big(id + \tilde{\iota} + \cdots + \tilde{\iota}^{s-1}\big)^{\circ}.$$

Since $0 = id - \tilde{\iota}^s = (id - \tilde{\iota})(id + \tilde{\iota} + \cdots + \tilde{\iota}^{s-1})$ and $id \neq \tilde{\iota}$, we have

$$0 = id + \tilde{\iota} + \cdots + \tilde{\iota}^{s-1} \in \mathrm{End}(J(\mathcal{C}_{s,f}^{(i)})) = \mathrm{End}(J(\mathcal{C}_{s,f})),$$

which implies that $\mathrm{Prym}_{\mathcal{C}_{s,f}^{(i)}/\mathbb{P}^1} = J(\mathcal{C}_{s,f}^{(i)})$ for each $i = 1, \cdots, n$. Applying Proposition 2.3, one can get an k-isogeny of Abelian varieties

$$\mathrm{Prym}_{\mathbf{C}_n/\mathbf{V}_n} \sim_k \prod_{i=1}^{n} \mathrm{Prym}_{\mathcal{C}_{s,f}^{(i)}/\mathbb{P}^1} = J(\mathcal{C}_{s,f})^n. \tag{2}$$

Let us denote by Q_i the image of P_i $(i = 1, \cdots, n)$ given by (1) under the canonical embedding of $\mathcal{C}_{s,f}^{\xi}$ into $J(\mathcal{C}_{s,f}^{\xi})$. Define $a = (a_u) \in Z^1(G, \mathrm{Aut}(J(\mathcal{C}_{s,f}))$ by $a_{id} = id$ and $a_{\gamma^j} = \tilde{\iota}^j$ where $\gamma^j \in G$ and $\tilde{\iota} : J(\mathcal{C}_{s,f}) \to J(\mathcal{C}_{s,f})$ is the automorphism induced by $\iota : \mathcal{C}_{s,f} \to \mathcal{C}_{s,f}$. Denote by $J(\mathcal{C}_{s,f})_a$ the twist of $J(\mathcal{C}_{s,f})$ with the 1-cocycle $a = (a_u)$. Then $J(\mathcal{C}_{s,f})_a = J(\mathcal{C}_{s,f}^{\xi})$ by the lemma on page 172 in [4]. Applying Theorem 1.1 with $\mathcal{V}' = \mathbf{C}_n$, $\mathcal{V} = \mathbf{V}_n$, and $\mathcal{A} = J(\mathcal{C}_{s,f})$, we have

$$\begin{aligned} J(\mathcal{C}_{s,f}^{\xi})(K) &\cong \mathrm{Hom}_k(\mathrm{Prym}_{\mathbf{C}_n/\mathbf{V}_n}, J(\mathcal{C}_{s,f})) \oplus J(\mathcal{C}_{s,f})[s](k) \\ &\cong \mathrm{Hom}_k(J(\mathcal{C}_{s,f})^n, J(\mathcal{C}_{s,f})) \oplus J(\mathcal{C}_{s,f})[s](k) \\ &\cong (\mathrm{End}_k(J(\mathcal{C}_{s,f})))^n \oplus J(\mathcal{C}_{s,f})[s](k). \end{aligned}$$

Thus, as $\mathbb{Z}$-modules, we have

$$\mathrm{rk}(J(\mathcal{C}_{s,f}^{\xi})(K) \geq n \cdot \mathrm{rk}(\mathrm{End}_k(J(\mathcal{C}_{s,f}))).$$

Tracing back the above isomorphisms shows that the points $Q_1, \cdots, Q_n$ belong to the set of independent generators of $J(\mathcal{C}_{s,f}^{\xi})(K)$.

Please cite this article in press as: S. Salami, The rational points on certain Abelian varieties over function fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.008

Acknowledgments

The author is very grateful to Professor Amilcar Pacheco for his mathematical comments and suggestions on this work submitted as part of his PhD thesis [11]. He would also like to thank the anonymous referee for his valuable comments that helped to improve the manuscript significantly.

References

[1] A. Beauville, Variétésde prymet jacobiennes intermediares, Ann. Sci. Éc. Norm. Supér. 10 (1977) 309–391.
[2] A. Borel, J.P. Serre, Théorèmes de finitude en cohomologie galoisienne, Comment. Math. Helv. 39 (1964) 111–164.
[3] A. Dujella, High rank elliptic curves with prescribed torsion, http://www.maths.hr/~duje/tors.htl.
[4] F. Hazama, On the Mordell–Weil group of certain abelian varieties defined over function fields, J. Number Theory 37 (1991) 168–172.
[5] F. Hazama, Rational points on certain abelian varieties over function fields, J. Number Theory 50 (2) (1995) 278–285.
[6] M. Hindry, J.H. Silverman, Diophantine Geometry: An introduction, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2001.
[7] S. Lang, Abelian Varieties, Springer-Verlag, New York/Berlin, 1983.
[8] H. Lange, A. Ortega, Prym varieties of cyclic coverings, Geom. Dedicata 150 (2011) 391–403.
[9] D. Mumford, Prym Varieties (i), Contributions to Analysis (A Collection of Papers Dedicated to Lipman Bers), Academic Press, New York, 1974, pp. 325–350.
[10] J. Park, et al., A heuristic for boundedness of ranks of elliptic curves, https://arxiv.org/abs/1602.01431.
[11] S. Salami, On Some Different Related Problems in Diophantine Geometry, Ph.D. thesis, IM-UFRJ, Brazil, 2017.
[12] J.H. Silverman, The Arithmetic of Elliptic Curves, Second edition, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009.
[13] J.T. Tate, I.R. Shafarevich, The rank of elliptic curves, Akad. Nauk SSSR 175 (1967) 770–773.
[14] D. Ulmer, Elliptic curves with large rank over function fields, Ann. Math. 155 (1) (2002) 295–315.
[15] D. Ulmer, Rational curves on elliptic surfaces, J. Algebraic Geom. 26 (2017) 357–377.
[16] W.B. Wang, On the twist of abelian varieties defined by the galois extension of prime degree, J. Algebra 163 (3) (1994) 813–818.
[17] H. Yamagishi, A unified method of construction of elliptic curves with high Mordell–Weil rank, Pacific J. Math. 191 (1) (1999) 507–524.

Please cite this article in press as: S. Salami, The rational points on certain Abelian varieties over function fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.008