Universidade Federal do Rio de Janeiro
Instituto de Matemática

Sajad Salami

On some related conjectures in Diophantine geometry

Doctoral Thesis
Advisor: Amilcar Pacheco

Rio de Janeiro
February, 2017

On some related conjectures in Diophantine geometry

Sajad Salami

Tese de Doutorado apresentada ao Programa de Pós-graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do grau de Doutor em Matemática.

Orientador: Amilcar Pacheco

Rio de Janeiro
Fevereiro de 2017

CIP - Catalogação na Publicação

```
        Salami, Sajad
S159o      On some related conjectures in  Diophantine
        geometry / Sajad Salami. -- Rio de Janeiro, 2017.
           53 f.

           Orientador: Amilcar  Pacheco.
           Tese (doutorado) - Universidade Federal do Rio
        de Janeiro, Instituto de Matemática, Programa de Pós
        Graduação em Matemática, 2017.

           1. The Vojta's conjecture on bounded degree
        algebraic numbers. 2. The Bombieri-Lang conjecture
        on varieties of general type. 3.  Twists of Abelian
        varieties. 4. Jacobian varieties of supper-elliptic
        curves. 5. Cyclic covers of function fields of
        quasi-projective varieties. I. Pacheco, Amilcar ,
        orient. II. Título.
```

Elaborado pelo Sistema de Geração Automática da UFRJ com os
dados fornecidos pelo(a) autor(a).

On some related conjectures in Diophantine geometry

Sajad Salami

Tese de Doutorado apresentada ao Programa de Pós-graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do grau de Doutor em Matemática.

Aprovada em 08 de fevereiro de 2017 por:

Presidente, Amilcar Pacheco (Doutor - IM/UFRJ)

Douglas Ulmer (Doutor - Georgia I. T. - USA)

Fabien Mehdi Pazuki (Doutor - U. Copenhagen - DIN)

Hossein Movasati (Doutor - IMPA)

Cecília Salgado Guimarães da Silva (Doutor - IM/UFRJ)

Rio de Janeiro
Fevereiro de 2017

Dedicated to all of my family members, especially my PARENTS, to my wife VAHIDEH, and to my son DANIEL.

Acknowledgements

I would like to express my deepest gratitude to my supervisor Professor Amilcar Pacheco for for the patient guidance, encouragement and a lot of mathematical comments along preparation of my thesis.

I am grateful to all members of the defense committee, especially to Hossein Movasati (IMPA) and Cecilia Salgado (IM-UFRJ) for giving several suggestions to improve my thesis.

I would like to thank my family, especially my parents, and my wife. Without their love, I would not have been able to complete this thesis. Thank you so much for your love and care!

Resumo

Ao longo desta tese, assumimos uma versão da conjectura de Vojta sobre os números algébricas com graus limitadas em uma linha projetiva. Primeiramente, para inteiros $2 \leq s \leq r < n$, estimamos o número de polinômios de grau $r \geq 2$, cujos fatores têm multiplicidade $< s$ e têm s-valores poderosos em um dado conjunto de n elementos distintos em pares em um corpo de numérico. Em segundo lugar, estudamos os pontos racionais sobre a torção de uma variedade Abeliana arbitrária por Extensões cíclicas do corpos de funções de variedades irredutíveis quase-projetivas, estendendo um resultado de Hazama. Em terceiro lugar, aplicando o nosso resultado para certas variedades, mostramos a finitude do número de curvas super-elíptica tendo pontos racionais com coordenadas x em um determinado conjunto finito de n elementos distintos por pares em um corpo de números contendo a raiz s da unidade. Finalmente, sujeito à conjectura de Vojta, provamos a existência de variedades de interseção completas e lisas de qualquer dimensão que satisfaça a conjectura de Bombieri-Lang sobre os pontos racionais sobre variedades de tipo geral.

Palavras chaves: A conjectura de Vojta em números algébricos de grau limitado, A conjectura de Bombieri-Lang sobre variedades de tipo geral, Torções de variedades Abelianas, As variedades Jacobianas de curvas supper-elliptic, As coberturas cíclicas de corpos de funções de variedades quase-projetivas.

Abstract

Throughout this thesis, we assume a version of Vojta's conjecture on the bounded degree algebraic numbers on a projective line. First, for integers $2 \leq s \leq r < n$, we estimate the number polynomials of degree $r \geq 2$, whose factors have multiplicity $< s$ and have s-powerful values at a given set of n pairwise elements in a number field. Second, we study the rational points on the twist of an arbitrary Abelian variety by cyclic extensions of function field of irreducible quasi-projective varieties, by extending a result of Hazama. Third, by applying our result for certain varieties, we showed the finiteness of the number of supper-elliptic curve having rational points with x-coordinates in a given finite set of n pairwise distinct elements in a number field containing a s-root of unity. Finally, subject to the Vojta's conjecture, we prove the existence of smooth complete intersection varieties of any dimension that satisfied the Bombieri-Lang's conjecture on the rational points on varieties of general type.

Keywords: The Vojta's conjecture on bounded degree algebraic numbers, The Bombieri-Lang conjecture on varieties of general type, Twists of Abelian varieties, Jacobian varieties of supper-elliptic curves, Cyclic covers of function fields of quasi-projective varieties.

Contents

Chapter 1

Introduction

A large part of Diophantine geometry is motivated by the study of rational points on algebraic varieties. More precisely, study on the set $X(k)$ for an algebraic variety over a field k (which is usually a number field or a function field of an algebraic variety) is the major objective of the Diophantine geometry. In the case that X is a dimension one variety, i.e., when $X = \mathcal{C}$ is a projective curve of $\mathfrak{g} \geq 0$, the structure of the set $\mathcal{C}(k)$ for number fields is well known. In fact, if $\mathfrak{g} = 0$, then $\mathcal{C}(k) = \emptyset$ or $\mathcal{C}(k) \cong \mathbb{P}^1_k$. When $\mathfrak{g} \geq 2$, it is conjectured by Mordell and proved by Faltings that the set $\mathcal{C}(k)$ is finite for all number fields. In the case that $\mathfrak{g} = 1$, when $X = E$ is an elliptic curves, the set $E(k)$ is a finitely generated group by the famous Mordell-Weil theorem. In other words, one has $E(k) \cong T \oplus \mathbb{Z}^r$ for some positive integer r, and a finite group T, that are called the rank of E and the torsion group of E, respectively. Determining the rank is more complicated than the characterization of the torsion group. For more details on these results, one can see the [**?**], [**?**] and [**?**].

In the case that X has dimension $dim(X) = 2$, i.e, when $X = S$ is an algebraic surface, there is a classification of the surfaces due to Kodaira using the notion of Kodaira dimension $\kappa(S)$ of an algebraic variety: if $\kappa(S) = -1$, then S is either a Rational or a Ruled surface; if $\kappa(S) = 0$, then S belongs to one of the following four classes: Abelian, Hyperelliptic (or bi-elliptic), $K3$ or Enriques surfaces; if $\kappa(S) = 1$, then S is an Elliptic Surface; if $\kappa(S) = 2$, then S is a surface of General type, in this case $dim(S) = \kappa(S)$.

The first three cases have been studied extensively throughout the literature in both geometric and arithmetic approaches. In the last case, indeed more generally when $\kappa(X) = dim(X) \geq 2$ that means X is a variety of general type, one has the following conjecture [**?**]:

Conjecture 1.0.1. *(***Bombieri-Lang***) Let X be a smooth projective algebraic variety of general type, defined over a number field k_0. Then there exists a proper Zariski-closed subset Z of X such that for all number fields k containing k_0, the set $(X\backslash Z)(k)$ is finite.*

As far as the knowledge of the author, there does not exist more examples of surface or higher dimension varieties of general type in the literature such that the Bombieri-Lang conjecture to be proved for them. The main aim of this thesis is that assuming a version of the Vojta's conjecture on the bounded degree algebraic numbers, we provide a certain complete intersection varieties of general type with dimension ≥ 2 satisfying the Bombieri-Lang conjecture.

The organization of this thesis is as follows. The Chapter **??**, in other words this chapter, is an introduction to the thesis. In Chapter **??**, we have studied the powerful values of polynomials over number fields by assuming the following version of the Vojta's conjecture on the algebraic number of bounded degree on a projective line. In order to state this conjecture, let k be a number field, $\bar{k}$ its algebraic closure, and h the absolute Weil height on $\mathbb{P}^1_{\bar{k}}$. Given $\alpha \in \bar{k}$, denote by $d_k(\alpha)$ its logarithmic discriminant with respect to k. Let S be a finite subset of $\mathcal{P}_k$, the set of places of k, containing infinite places $\mathcal{P}_k^\infty$ of k, and let $N_S^{(1)}$ be the counting function respect to S. See the section **??** for more details.

Conjecture 1.0.2. *Let $b_1, \cdots, b_q$ be fixed pairwise distinct elements of k and $d \geq 2$ be an integer. Then for any $\epsilon > 0$ and $c \in \mathbb{R}$, the inequality*

$$(q - 2 - \epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{q} N_S^{(1)}(b_i, \alpha) + c + c',$$

holds for almost all $\alpha \in \bar{k}$ with $[k(\alpha) : k] \leq d$ and different from b_i's, where

$$c' := q(B + d \log 2), \;\; B := \max\{h(b_i)\}_{i=1}^{q}.$$

Let $\mathcal{B} = \{b_i\}_{i=1}^{\infty}$ be a fixed sequence of pairwise distinct elements in k. For each $n \geq 1$, we assume that $\mathcal{B}_n \subset \mathcal{B}$ contains the first n terms $b_1, \cdots, b_n$. Given integers $2 \leq s \leq r < n$, let $\mathbf{F}_{r,s}^{\mathcal{B}_n}$ be the set of all polynomials $f \in k[x]$ of degree r such that $f(b_i)$ is a s-powerful element in K for each $b_i \in \mathcal{B}_n$. For the subset of this set in which all irreducible factors have multiplicity strictly smaller than s, the notation should be $\mathbf{G}_{r,s}^{\mathcal{B}_n}$. The following theorem, which extend the theorem 2.1 in [?], is the main result of the Chapter **??**, in fact the essential result of the thesis.

Theorem 1.0.3. *Assume the Vojta's Conjecture on number fields. Given any integers $2 \leq s \leq r$, let $M := 2r^2 + 6r + 1$ if $r = s$, and $2sr^2 + sr + 1$ otherwise. Then there exist positive constants C_0 and C_1 (depending on $b_1, \cdots, b_M$, the number field k and the integer r) such that $C_0 \leq \#\mathbf{G}_{r,s}^{\mathcal{B}_M} \leq C_1$. Moreover, for each $n \geq M$ we have $\#\mathbf{G}_{r,s}^{\mathcal{B}_n} \leq C_1$.*

In Chapter **??**, after reviewing the basic facts on the twist theory in section **??** and some results of F. Hazama [?, ?, ?], on the structure of the set rational points on certain Abelian varieties over function fields in section **??**, we extend the main result of Hazama in [?] on the rational points on certain Abelian varieties over function fields as follows. Let A/k be an Abelian variety, $s \geq 2$ be an integer and $\pi : V' \to V$ be a cyclic s-cover of irreducible quasi-projective varieties, both as well as π defined over a field k such that $(char(k), s) = 1$. Let $K := k(V)$, $L := k(V')$ and G be the cyclic Galois group of the extension $L|K$ of order s. The following theorem gives a structure theorem on the set of K-rational points on A_b, the twist of A with a certain 1-cocycle $b \in Z^1(G, \mathrm{Aut}(A))$. See the section **??** for more details.

Theorem 1.0.4. *Assume that there exist a k-rational point $v_0' \in V'(k)$. Then we have an isomorphism of Abelian groups:*

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

where $A[s](k)$ denotes the Abelian group of k-rational s-division points, and $Prym_{V'/V}$ is the Prym variety associated to the cyclic cover $\pi : V' \to V$.

In particular, we have the following corollary.

Corollary 1.0.5. *Assume that $Prym_{V'/V}$ is k-isogenous with $A^n \times B$ for some positive integer n, where A and B are Abelian varieties defined over k such that $\dim(B) = 0$ or $\dim(B) > \dim(A)$ and none of irreducible components of B is k-isogenous to A. Supposing, furthermore, that $A[s](k) = \{\mathcal{O}\}$, then $rk(A_b(K)) \geq n \cdot rk(End_k(A))$.*

In section **??**, we applied the above theorem and corollary to a certain cyclic s-cover $\pi : \mathbf{C}_m \to \mathbf{V}_m$ with $m \geq 1$, where $\mathbf{C}_m$ denotes the product of m copies of a supper-elliptic curve $\mathcal{C}_{s,f}$ given by affine equations $y_i^s = f(x_i)$ for $i = 1 \cdots \leq m$, with $f(x) \in k^*[x]$ of degree $r \geq s$, where k is a field such that $(char(k), s) = 1$, and $\mathbf{V}_m$ is a quotient of $\mathbf{C}_m$ by a certain cyclic group of order $s \geq 2$. Letting $z_i := y_1^{s-1} y_{i+1}$, the variety $\mathbf{V}_m$ is given by the equations $z_i^s = f(x_1)^{s-1} f(x_{i+1})$ for $i = 1, \cdots, m-1$. Let $\mathcal{C}_{s,f}^{\xi}$ denotes the twist of $\mathcal{C}_{s,f}$ by the extension $L|K$, where $K = k(\mathbf{V}_m)$ and $L = k(\mathbf{C}_m)$, which is defined by the affine equation $f(x_1)^{s-1} y^s = f(x)$ and contains K-rational points $P_1 := (x_1, 1/y_1^{s-2})$ and $P_i := (x_{i+1}, y_{i+1}/y_1^{s-1})$ for $i = 1, \cdots m-1$. Denote by $Q_1, \cdots, Q_m$, the image of the points $P_1, \cdots, P_m$ given by (**??**) under the canonical embedding of $\mathcal{C}_{s,f}^{\xi}$ into $J(\mathcal{C}_{s,f}^{\xi})$. Using the above results, we obtain the following theorem on the Mordell-Weil group of K-rational points on the Jacobian variety of the supper-elliptic curve $\mathcal{C}_{s,f}$.

Theorem 1.0.6. *Notation being as above, we assume that there exists $c \in \mathcal{C}_{s,f}(k)$ and let $J(\mathcal{C}_{s,f})[s](k)$ be the group of k-rational s-division points in $J(\mathcal{C}_{s,f})$. Then we have an isomorphism of Abelian groups:*

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

Assuming that $J(\mathcal{C}_{s,f})[s](k)$ is trivial group, we have

$$rk(J(\mathcal{C}_{s,f}^{\xi})(K)) = m \cdot rk(End_k(J(\mathcal{C}_{s,f}))),$$

and the points $Q_1, \cdots, Q_m$, are contained in the set of independent generators of $J(\mathcal{C}_{s,f}^{\xi})(K)$. Furthermore, if $End_k(J(\mathcal{C}_{s,f})) \cong \mathbb{Z}$, then the rank of the Mordell-Weil group $J(\mathcal{C}_{s,f}^{\xi})(K)$ is exactly m with generators $Q_1, \cdots, Q_m$.

Since the varieties $\mathbf{C}_m$ and $\mathbf{V}_m$ are defined by a fixed polynomial $f \in k^*[x]$, so if we suppose that $f(x) = \sum_{j=0}^{r} a_j x^{r-j} \in k^*[x]$ is an arbitrary element, then $\mathbf{V}_m$ can be seen as a variety over the field $k(x_1, \cdots, x_m)$ and letting $x_1 = \alpha_0$ and $x_{i+1} = \alpha_i$ gives a variety $\mathbf{W}_m$ defined by $z_i^s = f(\alpha_0)^{s-1} f(\alpha_{i+1})$ for $i = 1, \cdots, m-1$, which can be regarded as a sub-variety in the projective space $\mathbb{P}_{\bar{k}}^{m+r}$ with coordinates $a_0, \cdots, a_r, z_1, \cdots, z_{m-1}$. We assume that k_0 is a number field containing a primitive s-th root of unity and we fix a sequence $\mathcal{B} = \{\alpha_i\}_{i=0}^{\infty}$ of pairwise distinct algebraic numbers over k_0. For integers $2 \leq s \leq r < n$, we suppose that k is a finite extension of k_0 containing $k_0(\alpha_0, \cdots, \alpha_n)$. Then, we showed that there is a k-birational map between $\mathbf{W}_{n+1}$ and the $(s, \cdots, s)$-complete intersection variety $\mathbf{X}_n \in \mathbb{P}_{\bar{k}}^n$ defined by certain equations. In the section **??**, we relate the results on the powerful values of polynomials with those in sections **??** to conclude the following theorem.

Theorem 1.0.7. *Assume the Vojta's Conjecture on number fields. Suppose that k_0 is sufficiently large number field so that it contains a primitive s-th root of unity. Given any integers $2 \leq s \leq r$, let $N := 2r^2 + 6r$ if $r = s$, and $2sr^2 + sr$ otherwise. Assume that k is an arbitrary finite extension of k_0 containing $k_0(\alpha_0, \cdots, \alpha_N)$. Then, there exist positive constants C_0 and C_1 such that*

$$C_0 \leq \#(\mathbf{W}_{N+1} \backslash W_{N+1})(k) = \#(\mathbf{X}_{N+1} \backslash X_{N+1})(k) \leq C_1,$$

and hence for each $n > N$, we have $\#(\mathbf{W}_{n+1} \backslash W_{n+1}) = \#(\mathbf{X}_n \backslash X_n) \leq C_1$.

The above theorem shows that the Vojta's Conjecture implies the Bombieri-Lang's conjecture for the varieties $\mathbf{W}_{n+1}$ and $\mathbf{X}_n$ for $n \geq N$, where N is as in the above theorem.

Chapter 2

Powerful values of polynomials over number fields

2.1 Introduction and main results

Let k be a number field and let $2 \leq s \leq r$ an integers. A nonzero element α of $\mathcal{O}_k$ is called *s-powerful* if for each prime ideal $\mathfrak{p} \in Spec(\mathcal{O}_k)$ we have $v_{\mathfrak{p}}(\alpha) \geq s$, where $v_{\mathfrak{p}}(\cdot)$ denotes the discrete normalized valuation associated to $\mathfrak{p}$. This definition immediately extends to elements of k. Clearly, any s-power in k is a s-powerful element. Given $f \in k[x]$ of degree r, we say that f is *s-powerful polynomial*, if each irreducible factor of f has multiplicity at least s. It is clear that any s-power in $k[x]$ is a s-powerful element.

The powerful values of polynomials have been studied by several authors in the literature, [?], [?], [?], [?] and the recent work [?], done by H. Pasten, based on a conjecture of Vojta on algebraic numbers of bounded degree on a projective line. Let us to recall the version of this conjecture, which is used in [?]. See the section **??** or [?, ?], for more details on these notations and following conjecture.

Let $\bar{k}$ be an algebraic closure of k and h the absolute Weil height of $\mathbb{P}^1_{\bar{k}}$. Given $\alpha \in \bar{k}$, denote by $d_k(\alpha)$ its logarithmic discriminant with respect to k. Let $\mathcal{P}_k$ be the set of all places of k and S is a finite subset of $\mathcal{P}_k$ containing infinite places $\mathcal{P}_k^{\infty}$ of k. Let $N_S^{(1)}$ denote the counting function respect to S on k.

Conjecture 2.1.1. *Fix $b_1, \cdots, b_q \in k$, pairwise distinct elements and let $d \geq 2$ be an integer. Then for each $\epsilon > 0$ there exists $c_\epsilon > 0$ such that the* *inequality*

$$(q-2-\epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{q} N_S^{(1)}(b_i,\alpha) + c_\epsilon,$$

holds for all $\alpha \in \bar{k}$ of degree $[k(\alpha):k] \leq d$ different from b_i's.

Assuming the above conjecture, Pasten showed the following result on s-powerful values of monic polynomials over number field, see the theorem 2.1 in [**?**].

Theorem 2.1.2. *(Pasten). Assume the Vojta's Conjecture (**??**). Let $2 \leq s \leq r$ be integers, and define $\bar{M} = 2r^2 + 9r + 1$, if $r = s$; and $\bar{M} = 2sr^2 + (2s+1)r + 1$ otherwise. Given pairwise distinct $b_1, \cdots, b_{\bar{M}} \in k$, the set of monic polynomial $f \in k[x]$ of degree r whose irreducible factors have multiplicity strictly less than s and such that $f(b_i)$ are s-powerful for each $i = 1, \cdots, \bar{M}$, is a finite set.*

In order to explain our result on the s-powerful values of polynomials, we need to fix some notations. Let $\mathcal{B} = \{b_i\}_{i=1}^{\infty}$ be a fixed sequence of pairwise distinct elements in k. For each $n \geq 1$, we assume that $\mathcal{B}_n \subset \mathcal{B}$ contains the first n terms $b_1, \cdots, b_n$. Given integers $2 \leq s \leq r < n$, let $\mathbf{F}_{r,s}^{\mathcal{B}_n}$ be the set of all polynomials $f \in k[x]$ of degree r such that $f(b_i)$ is a s-powerful element in k for each $b_i \in \mathcal{B}_n$. Denote by $\mathbf{G}_{r,s}^{\mathcal{B}_n}$ the subset of this set in which all irreducible factors have multiplicity strictly smaller than s. Given integers $n' > n$, one has the inclusions $\mathbf{F}_{r,s}^{\mathcal{B}_{n'}} \subseteq \mathbf{F}_{r,s}^{\mathcal{B}_n}$ and $\mathbf{G}_{r,s}^{\mathcal{B}_{n'}} \subseteq \mathbf{G}_{r,s}^{\mathcal{B}_n}$.

The following conjecture is an equivalent version of the Vojta's Conjecture (**??**), which is important to get the results of the thesis.

Conjecture 2.1.3. *Let k be a number field, $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^{\infty}$, $\bar{k}$ algebraic closure of k. Let $b_1, \cdots, b_q$ be fixed pairwise distinct elements of k and $d \geq 2$ be an integer. Then for any $\epsilon > 0$ and $c \in \mathbb{R}$, the inequality*

$$(q-2-\epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{q} N_S^{(1)}(b_i,\alpha) + c + c',$$

holds for almost all $\alpha \in \bar{k}$ with $[k(\alpha):k] \leq d$ and different from b_i's, where

$$c' := q(B + d\log 2),\ B := \max\{h(b_i)\}_{i=1}^{q}.$$

This conjecture is a special case the Vojta's conjecture in a more general context on the algebraic points on varieties defined over number fields. See the conjecture 25.1 in [?].

Theorem 2.1.4. *Assume the Vojta's Conjecture (??). Given any integers $2 \leq s \leq r$, let $M := 2r^2 + 6r + 1$ if $r = s$, and $2sr^2 + sr + 1$ otherwise. Then there exist positive constants C_0 and C_1 such that $C_0 \leq \#\mathbf{G}_{r,s}^{\mathcal{B}_M} \leq C_1$. Moreover, for each $n \geq M$ we have $\#\mathbf{G}_{r,s}^{\mathcal{B}_n} \leq C_1$.*

Remark 2.1.5. *The integer M in this theorem depends only on the number field k and the integers r and s, but it is independent of the fixed set $\mathcal{B}_M$. In contrast, the explicit lower and upper bounds for $\#G_{r,s}^{\mathcal{B}_M}$ depends on $b_i \in \mathcal{B}_M$.*

Remark 2.1.6. *The theorem (??) generalizes the Pasten's result (??) because it gives explicit lower and upper bounds for the cardinal of the set $\mathbf{G}_{r,s}^{\mathcal{B}_M}$.*

2.2 Height functions over number fields

In this section, we give the basic definitions and facts on height functions and bounded degree algebraic numbers, which are used in the next sections. See [?], [?], or [?] for more details.

Given a number field k, let $\mathcal{P}_k$ be the set of places of k that splits into two disjoint subsets. One, $\mathcal{P}_k^0$ the set of the finite places, *i.e.*, those extending the places corresponding to the p-adic absolute values of $\mathbb{Q}$, and another one of the infinite places, denoted $\mathcal{P}_k^\infty$, *i.e.*, those extending the infinite place of $\mathbb{Q}$. For any $v \in \mathcal{P}_k$, denote by $\|\cdot\|_v$ its associated almost absolute value. The *multiplicative height* of any $\alpha \in k$ is defined by the equality

$$H_k(\alpha) := \prod_{v \in \mathcal{P}_k} \max\{\|\alpha\|_v, 1\}.$$

This is easily extended to a point $P = [\alpha_0 : \cdots : \alpha_n] \in \mathbb{P}_k^n$, as follows

$$H_k(P) := \prod_{v \in \mathcal{P}_k} \max\{\|\alpha_0\|_v, \cdots, \|\alpha_n\|_v\}.$$

Given $x \in \mathbb{R}_{>0}$, define $\log^+ x = \max\{\log x, 0\}$. The *logarithmic height* of $\alpha \in k$ is defined by the equality

$$h_k(\alpha) := \log^+ H_k(\alpha) = \sum_{v \in \mathcal{P}_k} \log^+ \|\alpha\|_v.$$

The *logarithmic height* of $P = [\alpha_0 : \cdots : \alpha_n] \in \mathbb{P}^n_k$ is defined by equality

$$h_k(P) := \log H_k(P) = \sum_{v \in \mathcal{P}_k} \log \max\{\|\alpha_0\|_v, \cdots, \|\alpha_n\|_v\},$$

For any finite extension $K|k$, $\alpha \in k$, and $P \in \mathbb{P}^n_k$, one has

$$H_k(\alpha) = H_K(\alpha)^{1/[K:k]},\ h_k(\alpha) = \frac{1}{[K:k]} h_K(\alpha),$$

$$H_k(P) = H_K(P)^{1/[K:k]},\ h_k(P) = \frac{1}{[K:k]} h_K(P).$$

Considering these facts, one may extend the definition of height function to $\mathbb{P}^n_{\bar{k}}$, where $\bar{k}$ is an algebraic closure of k. In this case, they are called the *absolute multiplicative and additive heights* of $P \in \mathbb{P}^n_{\bar{k}}$ and denoted by $H(P)$ and $h(P)$, respectively.

Proposition 2.2.1. *The absolute heights over $\bar{k}$ satisfied in following properties:*

(i) For each $\alpha, \beta \in \bar{k}^*$ and $n \in \mathbb{Z}$, we have

$$h(\alpha^n) = |n| h(\alpha),\ h(\alpha\beta) \leq h(\alpha) + h(\beta),\ h(\alpha+\beta) \leq h(\alpha) + h(\beta) + \log 2;$$

(ii) The action of Galois group of $\mathbb{P}^n_{\bar{k}}$ leaves the absolute heights invariant.

Proof. One can see the lemma 3.3 in [**?**] for part (i), and the propositions B.2.2 in [**?**] for part (ii). □

Given any polynomial $f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d \in k[x]$, the *absolute multiplicative and additive heights* are $H(f) := H([a_0 : a_1 : \cdots : a_d])$, and $h(f) := h([a_0 : a_1 : \cdots : a_d]$, respectively.

Proposition 2.2.2. *Let $f \in k[x]$ be a polynomial of degree $d \geq 2$ with roots $\alpha_1, \cdots, \alpha_d$ in $\bar{k}$, and let $f_i \in k[x]$ be polynomials of degree $d_i \geq 2$ for $1 \leq i \leq t$. Then* *(i)* $-d\log 2 + \sum_{i=1}^{d} h(\alpha_i) \leq h(f) \leq \sum_{i=1}^{d} h(\alpha_i) + (d-1)\log 2$;

(ii) If $f = f_1 \cdots f_t$, *then* $h(f_1 f_2 \cdots f_t) \leq \sum_{i=1}^{t}(h(f_i) + (d_i+1)\log 2)$;

Proof. One can prove (i) using theorem 1.6.13 and remark 1.6.14 in [**?**]. The parts (ii) come from the proposition (B.7.2) in [**?**]. □

Without loos of generality, we may suppose that $\bar{k} = \mathbb{C}$ and

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d = a_0 \prod_{j=1}^{d} (x - \alpha_j) \in \mathbb{C}[x]. \tag{2.2.1}$$

In this case, the *Mahler measure* of any $f \in \mathbb{C}[x]$ is defined by

$$M(f) := |a_0| \cdot \prod_{j=1}^{r} \max\{1, |\alpha_j|\},$$

where $|\cdot|$ is the usual absolute value on $\mathbb{C}$. When $\alpha \in \bar{k} = \mathbb{C}$ is an algebraic number over k with minimal polynomial $f_\alpha \in k[x]$, we define its Mahler measure by $M(\alpha) = M(f_\alpha)$.

Let $\mathfrak{d}_k$ be the absolute discriminant of k. The *logarithmic discriminant* of k is defined by $d_k := \log \mathfrak{d}_k / [k : \mathbb{Q}]$. For a tower of number fields $\mathbb{Q} \subseteq k \subseteq K \subset \bar{k}$ with absolute discriminants $\mathfrak{d}_k$ and $\mathfrak{d}_K$, respectively, the *relative logarithmic discriminant* of $K|k$ is

$$d_k(K) := \frac{1}{[K : k]} \log \mathfrak{d}_{K/k} - \log \mathfrak{d}_k,$$

where $\mathfrak{d}_{K/k}$ is the relative discriminant of the extension $K|k$. The *relative logarithmic discriminant* of each $\alpha \in \bar{k}$ is defined by $d_k(\alpha) := d_k(k(\alpha))$.

We will use the following theorem in the proof of the main theorem (**??**), which gives an upper bound for the logarithmic discriminant $d_k(\alpha)$ in the Vojta's conjectures.

Theorem 2.2.3. *[**?**, **?**]. Let* $f \in k[x]$ *be of the form (**??**) with degree* $d \geq 2$ *and* $A(d) = d\log d$ *if* $k = \mathbb{Q}$, *and* $A(d) = (2d-1)\log d$ *otherwise.*

(i) $D(f) = a_0^{2d-2} \prod_{i>j} (\alpha_i - \alpha_j)^2$, *and* $|D(f)| \leq d^d \cdot M(f)^{2d-2}$;

(ii) If $D(f) \neq 0$, *then* $h(D(f)) \leq 2(d-1)h(f) + A(d)$;

(iii) If $\alpha \in \bar{k}$ is of degree $d \geq 2$, then $d_k(\alpha) \leq 2(d-1)h(\alpha) + A(d)$.

Proof. See theorem 1 in [?] for part (i). The part (ii) is consequence of part (i) in the case $k = \mathbb{Q}$, and it is the lemma 3.7 in [?] when $k \neq \mathbb{Q}$. The part (iii) is the proposition 1.6.9 in [?] in the case $k = \mathbb{Q}$; and generally it comes from part (ii). □

The following theorem plays a central role in Diophantine geometry, since proving an upper bound on the heights of rational points over number fields is equivalent to proving finiteness of certain set.

Theorem 2.2.4. ***(Northcott)*** *[?]. Let k be a number field and $\bar{k}$ its algebraic closure. For any constant T and integer $d \geq 1$, the set*

$$\{P = [\alpha_0 : \alpha_1 : \cdots : \alpha_n] \in \mathbb{P}^n_{\bar{k}} | H(P) \leq T,\ [k(P) : k] \leq r\},$$

are finite, where $k(P) = k(\alpha_0/\alpha_j, \alpha_1/\alpha_j, \cdots, \alpha_n/\alpha_j)$ with $\alpha_j \neq 0$.

The problem of giving a quantitative version of Northcott's theorem started with Schanuel in [?]. Let k be of degree $m \geq 1$ and fix a parameter T. Let $h : \mathbb{P}^n_{\bar{k}} \to \mathbb{R}$ be the absolute logarithmic height. Denote by $N(\mathbb{P}^n_k; T)$ the number of points $P \in \mathbb{P}^n_k$ with $h(P) \leq T$. The following theorem approximate the $N(\mathbb{P}^n_k; T)$ using the parameter T.

Theorem 2.2.5. ***(Schanuel)*** *[?]. Under above assumption, one has*

$$N(\mathbb{P}^n_k; T) \sim cT^n + 1 \textit{ for some } \ c > 0 \textit{ as } T \to \infty.$$

Extending the Schanuel's result for bounded degree points over k is started by [?] and continued by [?], [?], [?], and so on. In this text, we will use the following quantitative version of the Northcott's theorem from [?], which extend the Schanuel's theorem in the case $\mathbb{P}^1_{\bar{k}}$ for bounded degree algebraic points. This is closely connected with the Schmidt's subspce theorem, as well as its reformulation by Masser and Valer.

In order to explain the result of *Su-Ion Ih*, we need to fix some notations. Denote by $N(\mathbb{P}^1_{\bar{k}}; r; T)$ the number of points $\alpha \in \mathbb{P}^1_{\bar{k}}$ of degree at most r and $h(\alpha) \leq T$ for every constant $T > 0$ and integer $r \geq 2$. Let h_k be the class number of k, Reg_k the regulator of $\mathcal{O}^*_k$, w_k the number of roots of unity in k, $\zeta_k(s)$ the Dedekind zeta-function of k, $\mathfrak{d}_k$ the absolute discriminant of

k, m_1 the number of real embedding of k and m_2 the number of pairs of complex embedding of k. Define the Scanuel type constant related to k as

$$a_{k,r} := \frac{h_k \cdot \mathrm{Reg}_k}{w_k \zeta_k(r+1)} \cdot \Big(\frac{2^{m_1}(2\pi)^{m_2}}{\mathfrak{d}_k^{1/2}}\Big)^{r+1} \cdot (r+1)^{m_1+m_2-1}, \tag{2.2.2}$$

and denote $b_{k,r} = r \cdot a_{k,r} \cdot T^{mr(r+1)}$ and $T_1 = T^{mr(r+1)-r}$.

Theorem 2.2.6. *[?]. For each $\varepsilon > 0$, we have the inequalities*

$$b_{k,r} \cdot 2^{-mr(r+1)} T^{mr(r+1)} - O_\varepsilon(T_1 \cdot T^\varepsilon) \leq N(\mathbb{P}^1_{\bar{k}}; r; T) \leq b_{k,r} \cdot 2^{mr(r+1)} + O(T_1).$$

In particular,

$$2^{-mr(r+1)} + o(1) \leq \frac{N(\mathbb{P}^1_{\bar{k}}; r; T)}{b_{k,r}} \leq 2^{mr(r+1)} + o(1) \quad \text{as} \quad T \to \infty.$$

2.3 The Vojta's conjecture on algebraic numbers of bounded degree

In this section, we recall the basic definitions on the value distribution theory over number fields. This theory is an analogue of the Nevanlinna theory in the context of complex numbers. We have focused to provide equivalent versions of the Vojta's conjecture on the algebraic points of bounded degree on a projective line. For more details, one can refer to [?], [?].

Let k be a number field and $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^\infty$, and $b, \alpha \in k$ are distinct elements. The *proximity functions* with respect to S are defined by

$$m_S(\alpha) := \sum_{v \in S} \log^+ \|\alpha\|_v, \;\; m_S(b, \alpha) := m_S(\frac{1}{\alpha - b}).$$

Similarly, the *counting functions* with respect to the set S are defined by equality

$$N_S(\alpha) := \sum_{v \notin S} \log^+ \|\alpha\|_v, \mathbb{N}_S(b, \alpha) := N_S(\frac{1}{\alpha - b}).$$

By the properties of the logarithm function, one has

$$m_S(\alpha) + N_S(\alpha) = \sum_{v \in \mathcal{P}_k} \log^+ \|\alpha\|_v = h(\alpha), \;\; (\alpha \in k).$$

The following theorem is an analogue to the *first main theorem* in classic value distribution theory. See theorem 6.3 in [**?**] for its proof.

Theorem 2.3.1. *Let k be a number field, $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^\infty$. Then for any $\alpha \in k$ and fixed $b \in k \backslash \{\alpha\}$, one has*

$$h(\alpha) \leq m_S(b, \alpha) + N_S(b, \alpha) + h(b) + [k : \mathbb{Q}] \cdot \log 2.$$

There is a natural way of extending the definition of the proximity and counting function to algebraic closure $\bar{k}$ of number field k. Indeed, if we assume that $S \subset \mathcal{P}_k$ is a finite set containing $\mathcal{P}_k^\infty$, $\alpha \in \bar{k}$, K and K' are finite extensions of k such that $k(\alpha) \subset K \subset K' \subset \bar{k}$, $T \subset \mathcal{P}_K$ and $T' \subset \mathcal{P}_{K'}$ are finite sets containing $\mathcal{P}_K^\infty$ and $\mathcal{P}_{K'}^\infty$, respectively, such that any element of T lies over some element of S and elements of T' lie over places of k, then

$$m_{T'}(\alpha) = [K' : K] \cdot m_T(\alpha), \; N_{T'}(\alpha) = [K' : K] \cdot N_T(\alpha).$$

Thus, one can define the proximity and counting functions for $\alpha \in \bar{k}$ by equalities

$$m_S(\alpha) := \frac{1}{[K : k]} \cdot m_T(\alpha), \; N_S(\alpha) := \frac{1}{[K : k]} \cdot N_T(\alpha).$$

These definitions are independent of the choice of the extension K containing $k(\alpha)$. If $b \in k(\alpha)$ be an element distinct from α, one can also define

$$m_S(b, \alpha) := \frac{1}{[k(\alpha) : k]} \cdot m_T(b, \alpha), \; N_S(b, \alpha) := \frac{1}{[k(\alpha) : k]} \cdot N_T(b, \alpha). \quad (2.3.1)$$

Remark 2.3.2. *It is easy to see that $h(\alpha) = m_S(\alpha) + N_S(\alpha)$ for all $\alpha \in \bar{k}$. By following the proof of the first main theorem, as in [**?**], and using equalities (**??**), one can see the inequality*

$$h(\alpha) \leq m_S(b, \alpha) + N_S(b, \alpha) + h(b) + [k(\alpha) : \mathbb{Q}] \cdot \log 2,$$

holds for any $\alpha \in \bar{k}$ and $b \in \bar{k}$ distinct from α.

The following conjecture is a special case the Vojta's conjecture on the algebraic points of bounded degree on varieties. See the section 3 of Chapter 5 in [**?**] for more details.

Conjecture 2.3.3. *Let k be a number field, $\bar{k}$ its algebraic closure and $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^\infty$. Let $b_1, \cdots, b_q$ be pairwise distinct elements of k and $d \geq 2$ an integer. For each $\epsilon > 0$ there exists $c_\epsilon > 0$ such that for every $\alpha \in \bar{k}$ of degree at most $d \geq 2$ the following inequality holds,*

$$\sum_{i=1}^{q} m_S(b_i, \alpha) \leq (2+\epsilon)h(\alpha) + d_k(\alpha) + c_\epsilon. \tag{2.3.2}$$

Using the Northcott's theorem one can see that the above conjecture is equivalent to the following one.

Conjecture 2.3.4. *Let k be a number field, $\bar{k}$ its algebraic closure and $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^\infty$. Let $b_1, \cdots, b_q$ be pairwise distinct elements of k and $d \geq 2$ an integer. Then for any $\epsilon > 0$ and $c \in \mathbb{R}$, the inequality*

$$\sum_{i=1}^{q} m_S(b_i, \alpha) \leq (2+\epsilon)h(\alpha) + d_k(\alpha) + c, \tag{2.3.3}$$

holds for almost all $\alpha \in \bar{k}$ with $[k(\alpha) : k] \leq d$ and different from b_i's.

Using the inequality in remark (**??**), for $i = 1, \cdots, q$, one has

$$h(\alpha) \leq m_S(b_i, \alpha) + N_S(b_i, \alpha) + h(b_i) + d\log 2,$$

so the inequalities of the above conjectures can be rewritten as follows:

$$(q-2-\epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{n} N_S(b_i, \alpha) + c_\epsilon,$$

and

$$(q-2-\epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{n} N_S(b_i, \alpha) + c + c',$$

where $c' := q(B + d \cdot \log 2)$ and $B := \max\{h(b_i)\}_{i=1}^{q}$.

The *truncated counting function* on $\bar{k}$ is defined by

$$N_S^{(1)}(b, \alpha) := \sum_{v \notin S} \min\{1, \operatorname{ord}_{\mathfrak{p}}{}^+(\alpha - b)\} \cdot \log(\#\frac{\mathcal{O}_K}{\mathfrak{p}_v}),$$

where $b \in k$, $\alpha \in \bar{k}^*\backslash k$, and $\mathfrak{p}_v \in Spec(\mathcal{O}_K)$ corresponds to $v \in \mathcal{P}^0_{k(\alpha)}$.

There are truncated versions of the above conjectures as follows.

Conjecture 2.3.5. *Let k be a number field, $\bar{k}$ its algebraic closure and $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^\infty$. Let $b_1, \cdots, b_q$ be pairwise distinct elements of k and $d \geq 2$ an integer. For each $\epsilon > 0$ there exists $c_\epsilon > 0$ such that for every $\alpha \in \bar{k}$ of degree at most $d \geq 2$ the following inequality holds,*

$$(q-2-\epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{q} N_S^{(1)}(b_i, \alpha) + c_\epsilon. \tag{2.3.4}$$

Conjecture 2.3.6. *Let k be a number field, $\bar{k}$ its algebraic closure and $S \subset \mathcal{P}_k$ a finite set containing $\mathcal{P}_k^\infty$. Let $b_1, \cdots, b_q$ be pairwise distinct elements of k and $d \geq 2$ an integer. Then for any $\epsilon > 0$ and $c \in \mathbb{R}$, the inequality*

$$(q-2-\epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{q} N_S^{(1)}(b_i, \alpha) + c + c' \tag{2.3.5}$$

holds for almost all $\alpha \in \bar{k}$ with $[k(\alpha) : k] \leq d$ and different from b_i's, where

$$c' := q(B + d \cdot \log 2), \ \ B := \max\{h(b_i)\}_{i=1}^{q}.$$

Remark 2.3.7. *Since $N_S^{(1)}(b, \alpha) \leq N_S(b, \alpha)$, for each b and α as above, so the truncated versions of the Vojta (I') and (II') implies the non truncated ones. The converse is the special case of theorem (3.1) in [**?**]. We note that the conjecture (**??**) implies the ABC-conjecture of the Masser and Oeserlé, see for details [**?**]. The truncated version Vojta II' is known as ABC-conjecture for bounded degree extension of number field.*

2.4 Proof of the main theorem

In this section, we will give the proof of the theorem (**??**). Let us recall some notation from the first section. Given integers $2 \leq s \leq r$, let $M = 2r^2 + 6r + 1$ if $r = s$ and $M = 2sr^2 + sr + 1$, otherwise. For a fixed sequence $\mathcal{B} = \{b_i\}_{i=1}^{\infty}$ of pairwise distinct elements of k, we assume that $\mathcal{B}_M := \{b_1, b_2, \cdots, b_M\}$ and we consider the set $\mathbf{G}_{r,s}^{\mathcal{B}_M}$, which contains the polynomials $f \in k[x]$ of degree $r \geq 2$ such that all of irreducible factors of f has multiplicity strictly less than s and $f(b_i)$ is a s-powerful element in k for each $b_i \in \mathcal{B}_M$. Here, we are going to give an explicit lower and upper bound for the cardinal of $\mathbf{G}_{r,s}^{\mathcal{B}_M}$. Without loose of generality, we may consider $f \in \mathbf{G}_{r,s}^{\mathcal{B}_M}$ with factorization $f = f_1^{s_1} \cdots f_t^{s_t}$, where $f_j \in k[x]$ are irreducible polynomial of degree $d_j := \deg(f_j)$. For each $j = 1, \cdots, t$, let $\alpha_j \in \bar{k}$ is an arbitrary root of f_j and define $k_j := k(\alpha_j)$ and $g := f_1 \cdots f_t$ of degree $d := d_1 + \cdots + d_t$.

Let $S \subset \mathcal{P}_k$ be a finite subset $\mathcal{P}_k$, which consists of the union of the sets $\mathcal{P}_k^\infty$, poles of the elements $b_i \in \mathcal{B}_M$ with the set of zeros of $b_i - b_j$ for $b_i \neq b_j \in \mathcal{B}_M$. Applying the Vojta's Conjecture (**??**) to this set S, elements $b_i \in \mathcal{B}_M$ and integer $r \geq 2$, we conclude that for any $\epsilon > 0$ and $c \in \mathbb{R}$, the following inequality

$$(M - 2 - \epsilon)h(\alpha) \leq d_k(\alpha) + \sum_{i=1}^{M} N_S^{(1)}(b_i, \alpha_j) + c + c', \tag{2.4.1}$$

holds for almost all $\alpha \in \bar{k}$ with $[k(\alpha) : k] \leq r$ and $\alpha_j \neq b_i$'s, where

$$c' := M(B + r \cdot \log 2), \text{ and } B := \max\{h(b_i) : \ 1 \leq i \leq M\}.$$

There are a finite number of elements in $\bar{k}$ of degree at most r for which the inequality (**??**) does not hold. Let us to denote by N_r the number of such elements in $\bar{k}$, which depends on $b_i \in \mathcal{B}_M$ and other data. We note that it is unknown that how the positive integer N_r is related to $b_1, \cdots, b_M$, yet. This is one of the hard problems in Diophantine approximation, which is analogue to the ineffectiveness of the Roth's theorem.

Since we are going to estimate $\#\mathbf{G}_{r,s}^{\mathcal{B}_M}$, so for a while we ignore the polynomials $f \in \mathbf{G}_{r,s}^{\mathcal{B}_M}$ that have some roots, not satisfying in inequality (**??**), and we recall them in the moment of estimating the $\#\mathbf{G}_{r,s}^{\mathcal{B}_M}$. Thus, we assume that the inequality (**??**) holds for all of the α_i's. It is clear that α_j's and b_i's are distinct elements for each $1 \leq i \leq M$ and $1 \leq j \leq t$, because $f(b_i) \neq 0$. Therefore, for each $j = 1, \cdots, t$ we have

$$(M - 2 - \epsilon)h(\alpha_j) \leq d_k(\alpha_j) + \sum_{i=1}^{M} N_S^{(1)}(b_i, \alpha_j) + c + c', \tag{2.4.2}$$

Applying the part (iii) of the theorem (**??**) to each of α_j's and using $d_j \leq d$, we obtain an upper bound for $d_k(\alpha_j)$ as follows,

$$d_k(\alpha_j) \leq 2(d_j - 1)h(\alpha_j) + A(d_j) \leq 2(d - 1)h(\alpha_j) + A(d).$$

Putting this into the inequality (**??**) and using the fact that $A(d) \leq A(r) \leq 2r \log r$, gives that

$$(M - 2d - \epsilon)h(\alpha_j) \leq \sum_{i=1}^{M} N_S^{(1)}(b_i, \alpha_j) + c + c_1, \qquad (2.4.3)$$

where $c_1 := M(B + r \cdot \log 2) + 2r \log r$. By multiplying the both side of the inequality (**??**) by d_j, using the fact that $t \leq r$ and then summing-up, we obtain that

$$\sum_{j=1}^{t}(M - 2d - \epsilon)h_{k_j}(\alpha_j) \leq \sum_{j=1}^{t}\sum_{i=1}^{M} d_j N_S^{(1)}(b_i, \alpha_j) + r(c + c_1). \qquad (2.4.4)$$

In order to give an upper bound for the term involving the truncated function in the inequality (**??**), we need the following lemma.

Lemma 2.4.1. *Let $D(g)$ be the discriminant the polynomial $g = f_1 \cdots f_t$ of degree $d \geq 2$, which is defined in initial part of the proof. Let $A(d) = d \log d$ if $k = \mathbb{Q}$, and $A(d) = (2d - 1) \log d$ otherwise. Then*

$$h(D(g)) \leq 2(d - 1) \sum_{j=1}^{t} h_{k_j}(\alpha_j) + 4d(d - 1) + A(d). \qquad (2.4.5)$$

Proof. Assume that α_{ji} are the roots of f_j for $1 \leq i \leq d_j$. Then using the proposition (**??**), we have

$$\begin{aligned}\sum_{j=1}^{t} h(f_j) &\leq \sum_{j=1}^{t}(\sum_{i=1}^{d_j} h(\alpha_{ji}) + (d_j - 1)\log(2)) \\ &\leq \sum_{j=1}^{t} d_j h(\alpha_j) + \sum_{j=1}^{t}(d_j - 1)\log(2) \\ &\leq \sum_{j=1}^{t} h_{k_j}(\alpha_j) + d - t\log(2).\end{aligned}$$

Using this inequality and applying the part (ii) of the proposition (**??**), gives that

$$\begin{aligned} h(g) = h(f_1 \cdots f_t) &\leq \sum_{j=1}^{t} [h(f_j) + (d_j + 1)\log(2)] \\ &= \sum_{i=1}^{t} h(f_j) + d + t\log(2) \leq \sum_{j=1}^{t} h_{k_j}(\alpha_j) + 2d \end{aligned}$$

Applying the part (ii) of the theorem (**??**), we obtain the desired inequality

$$h(D(g)) \leq 2(d-1)h(g) + A(d) \leq 2(d-1)\sum_{j=1}^{t} h_{k_j}(\alpha_j) + 4d(d-1) + A(d).$$

□

Let D be the reduced divisor on $Spec(\mathcal{O}_k)$ whose support consists of the union of the sets S with the zeros of $D(g)$ and the poles of the α_j's. Denote $A(S) := \sum_{\mathfrak{p}\in S} \deg(\mathfrak{p})$, where $\deg(\mathfrak{p}) := \log \#(\mathcal{O}_k/\mathfrak{p})$ for any prime $\mathfrak{p} \in Spec(\mathcal{O}_k)$. The following lemma gives an upper bound for the term containing the truncated function in (**??**).

Lemma 2.4.2. *With notation as above, we have:*

$$\sum_{j=1}^{t}\sum_{i=1}^{M} d_j N_S^{(1)}(b_i, \alpha_j) \leq \Big[\frac{Ms^+}{s} + d(2d-1)\Big] \sum_{j=1}^{t} h_{k_j}(\alpha_j) + rc_2,$$

where $s^+ := \max\{s_1, \cdots, s_t\}$, $d = d_1 + \cdots + d_t$ *and*

$$c_2 := \frac{M(B + \log 2)}{s} + A(s) + A(r) + 4r(r-1).$$

Proof. By changing the order of sums in the left hand side of the inequality (**??**) and following the last part of the proof of the lemma 4.9 in [**?**], we have

$$\begin{aligned} \sum_{i=1}^{M}\sum_{j=1}^{t} d_j N_S^{(1)}(b_i, \alpha_j) &\leq \frac{1}{s}\sum_{i=1}^{M}\sum_{j=1}^{t} s_j d_j h(b_i - \alpha_j) + d\deg(D) \\ &\leq \frac{1}{s}\sum_{i=1}^{M}\Big(\sum_{j=1}^{t} s_j d_j [h(b_i) + h(\alpha_j) + \log 2]\Big) + d\deg(D). \end{aligned}$$

Since $t \leq r = \sum_{j=1}^{t} s_j d_j$, and $s_j \leq s^+$, so we have

$$\begin{aligned}\sum_{i=1}^{M}\sum_{j=1}^{t} d_j N_S^{(1)}(b_i,\alpha_j) &\leq \frac{1}{s}\sum_{i=1}^{M}[\sum_{j=1}^{t} s_j d_j h(\alpha_j)+ \\ &\qquad \sum_{j=1}^{t} s_j d_j h_k(b_i) + t\log 2] + d\deg(D) \\ &\leq \frac{1}{s}\sum_{i=1}^{M}[\sum_{j=1}^{t} s_j h_{k_j}(\alpha_j) + r(h_k(b_i)+\log 2)] + d\deg(D) \\ &\leq \frac{M}{s}\sum_{j=1}^{t} s_j h_{k_j}(\alpha_j) + \frac{Mr(B+\log 2)}{s} + d\deg(D) \\ &\leq \frac{Ms^+}{s}\sum_{j=1}^{t} h_{k_j}(\alpha_j) + \frac{Mr(B+\log 2)}{s} + d\deg(D).\end{aligned}$$

In order to give an upper bound on the $\deg(D)$ in terms of $h(\alpha_j)$'s, let S' and S_j be subsets of $\mathcal{P}_k^0$ such that $D(g)$ vanished at $\mathfrak{p}$, α_j has a pole above $\mathfrak{p}$, respectively, and let S'' be the union of S_j's. Then

$$\begin{aligned}\deg(D) &= \sum_{\mathfrak{p}\in S''}\deg(\mathfrak{p}) + \sum_{\mathfrak{p}\in S'}\deg(\mathfrak{p}) + \sum_{\mathfrak{p}\in S}\deg(\mathfrak{p}) \\ &= \sum_{j=1}^{t}\sum_{\mathfrak{p}\in S_j}\deg(\mathfrak{p}) + \#S' + A(S) \\ &= \sum_{j=1}^{t} h_{k_j}(\alpha_j) + h(D(g)) + A(S).\end{aligned}$$

Using the inequality (**??**) in the lemma, which gives an upper bound for $h(D)$, and the facts that $d \leq r$ and $A(d) \leq A(r)$, we get that

$$\begin{aligned}\deg(D) &\leq \sum_{j=1}^{t} h_{k_j}(\alpha_j) + 2(d-1)\sum_{j=1}^{t} h_{k_j}(\alpha_j) + A(S) + A(r) + 4r(r-1) \\ &\leq (2d-1)\sum_{j=1}^{t} h_{k_j}(\alpha_j) + A(S) + A(r) + 4r(r-1).\end{aligned}$$

Multiplying the last inequality by d, gives that

$$d\deg(D) \leq d(2d-1)\sum_{j=1}^{t} h_{k_j}(\alpha_j) + r[A(S) + A(r) + 4r(r-1)]$$

Gathering all of the above inequalities together gives the desired one. □

Using the above lemma, one can rewrite the inequality (**??**) as follows,

$$\begin{aligned}\sum_{j=1}^{t}(M-2d-\epsilon)h_{k_j}(\alpha_j) &\le \sum_{j=1}^{t}\sum_{i=1}^{M} d_j N_S^{(1)}(b_i,\alpha_j)+r(c+c_1)\\ &\le \big[\frac{Ms^+}{s}+d(2d-1)\big]\sum_{j=1}^{t}h_{k_j}(\alpha_j)+r(c+c_1+c_2).\end{aligned}$$

In other words, we have the following inequality

$$\sum_{j=1}^{t}[M(1-\frac{s^+}{s})-2d^2-d-\epsilon]h_{k_j}(\alpha_j)\le r\cdot(c+c_1+c_2). \qquad (2.4.6)$$

Lemma 2.4.3. *For integers $2 \le s \le r$ and $1 \le d \le r$, we have*

$$M(1-\frac{s^+}{s})-2d^2-d\ge\frac{1}{r}. \qquad (2.4.7)$$

Proof. For each $f \in \mathbf{G}_{r,s}^{\mathcal{B}_M}$ with irreducible factorization $f = f_1^{s_1}\cdots f_t^{s_t}$, we have

$$s^+ := \max\{s_1,\cdots,s_t\}\le s-1,$$

which implies that $r - s^+ \ge d-1$. Indeed, if j_0 is an index such that $s_{j_0} = s^+$, then

$$r=\sum_{j=1}^{t}s_jd_j\ge s^+d_{j_0}+\sum_{j\ne j_0}d_j\ge s^++d_{j_0}-1+\sum_{j\ne j_0}d_j=s^++d-1.$$

Thus $r - s^+ \ge d-1$, which implies that

$$1-\frac{s^+}{s}=\frac{s-s^+}{s}\ge\frac{r-s^+}{s}\ge\begin{cases}\frac{d-1}{r} & \text{if } s=r\\ \frac{1}{s} & \text{otherwise.}\end{cases} \qquad (2.4.8)$$

In the case $s = r$, we have $d-1 \ge 1$, because if $d = 1$ then $s > s^+ = r > s$, which is a contradiction. Since $M = 2r^2 + 6r + 1$, so using $1 - s^+/s \ge d-1 \ge 1$, we have

$$\begin{aligned}M(1-\frac{s^+}{s})-2d^2-d &\ge M(\frac{d-1}{r})-2d^2-d\\ &\ge\frac{d-1}{r}(M-\frac{2rd^2+rd}{d-1})\\ &\ge\frac{d-1}{r}(M-2rd-3r-\frac{3r}{d-1}).\end{aligned}$$

Since $3r/(d-1) \leq 3r$ and $(d-1)/r \geq 1/r$ for $d-1 \geq 1$, and $d \leq r$, so we have

$$\begin{aligned} M(1-\frac{s^+}{s}) - 2d^2 - d &\geq \frac{d-1}{r}(M - 2rd - 6r) \\ &\geq \frac{1}{r}(M - 2r^2 - 6r) \geq \frac{1}{r}, \end{aligned}$$

where $M - 2r^2 - 6r \geq 1$ implies the last inequality.

In the case $s < r$, we have $M = 2sr^2 + sr + 1$ and $1 - s^+/s \geq 1/s$, so using $d \leq r$ and $M; -2sr^2 - sr \geq 1$, gives that

$$\begin{aligned} M(1-\frac{s^+}{s}) - 2d^2 - d &\geq M/s - 2d^2 - d \\ &\geq \frac{1}{s}(M - 2sd^2 - sd) \\ &\geq \frac{1}{r}(M - 2sr^2 - sr) \geq \frac{1}{r}. \end{aligned}$$

□

Using the inequality (**??**), in either cases, we can rewrite the inequality (**??**) as

$$(\frac{1}{r} - \epsilon) \sum_{j=1}^{t} h_{k_j}(\alpha_j) \leq r(c + c_1 + c_2). \tag{2.4.9}$$

Since the constants ϵ and c in the Vojta's Conjecture (**??**) are arbitrary, so we consider the following constants

$$\epsilon := 1/(r+1), \; c := \frac{1}{mr^3(r+1)^2} - c_1 - c_2, \; c_3 := \frac{1}{mr(r+1)}, \tag{2.4.10}$$

where m is the degree of the number field k. Then, using the equation (**??**), we obtain that

$$h(\alpha_j) \leq d_j h(\alpha_j) = h_{k_j}(\alpha_j) \leq \sum_{j=1}^{t} h_{k_j}(\alpha_j) \leq r^2(r+1)[c + c_1 + c_2] \leq c_3.$$

We note that the consonant c_3 depends only on k and r, but not on an special $f \in \mathbf{G}_{r,s}^{\mathcal{B}_M}$. Denote by $N(\mathbb{P}^1_{\bar{k}}; r; c_3)$ the number of algebraic numbers $\alpha \in \bar{k}$ of degree at most r and height at most c_3. The Northcott's theorem (**??**) implies that $N(\mathbb{P}^1_{\bar{k}}; r; c_3)$ is a positive number. Letting $c_4 := c_3^{mr(r+1)-r}$

and applying the Ih's theorem (**??**) with constants $\varepsilon := 1$, $T := c_3$ and $T_1 := c_4$, gives us two constants $c_5, c_6 > 0$ depending on the initial data such that

$$b_{k,r} \cdot 2^{-mr(r+1)} + c_5 \cdot c_4 \cdot c_3 \leq N(\mathbb{P}^1_{\bar{k}}; r; c_3) \leq b_{k,r} \cdot 2^{mr(r+1)} + c_6 \cdot c_4.$$

Let $\mathcal{A}_r$ be the set of all $\alpha \in \bar{k}$ of degree at most r and height at most c_3 together with those algebraic numbers not satisfying the inequality (**??**). Then

$$b_{k,r} \cdot 2^{-mr(r+1)} + c_5 \cdot c_4 \cdot c_3 + N_r \leq \#\mathcal{A}_r \leq b_{k,r} \cdot 2^{mr(r+1)} + c_6 \cdot c_4 + N_r.$$

Since for each $f \in \mathbf{G}^{\mathcal{B}_M}_{r,s}$ has at most r roots in $\bar{k}$, maybe some of them does not satisfy in the inequality (**??**), so we conclude that

$$b_{k,r} \cdot 2^{-mr(r+1)} + c_5 \cdot c_4 \cdot c_3 + N_r \leq \#\mathbf{G}^{\mathcal{B}_M}_{r,s} \leq r \cdot (b_{k,r} \cdot 2^{mr(r+1)} + c_6 \cdot c_4 + N_r).$$

Therefore, we obtain the desired lower and upper bounds $C_0 \leq \#\mathbf{G}^{\mathcal{B}_M}_{r,s} \leq C_1$, where

$$C_0 := b_{k,r} \cdot 2^{-mr(r+1)} + c_5 \cdot c_4 \cdot c_3 + N_r,$$
$$C_1 := r \cdot (b_{k,r} \cdot 2^{mr(r+1)} + c_6 \cdot c_4 + N_r).$$

Chapter 3

Rational points on certain Abelian varieties over function fields

3.1 Introduction

In this chapter, by extending some results of Hazama in [**?**, **?**], we are going to prove a structure theorem on the Mordell-Weil group of the rational points on Abelian varieties over function fields, which arise as twists of Abelian varieties by cyclic covers of quasi projective variety. In particular, we use the main result to find supper-elliptic curves having a given set of algebraic numbers as x-coordinates of a set of rational points such that their images under canonical maps forms a subset of the generators of the Mordell-Weil group of their Jacobian varieties. Using the result of this chapter and the first one, subject to the Vojta's conjecture, we prove the existence of certain complete intersection varieties of general type satisfying in the Bombieri-Lang conjecture.

3.2 Twisting theory

Let us to recall two equivalent definition of twist and its basic properties. Let K be a field and $L|K$ a Galois extension with Galois group $G = G_{L|K}$. A *G-set* is a discrete topological space E such that the left action of G on E is continuous. For every $x \in E$ and $u \in G$, we denote by ${}^{u}x$ the left action of u on x. A *G-group* is a G-set A equipped with a group structure invariant under action of G, i.e., ${}^{u}(x \cdot y) = {}^{u}x \cdot {}^{u}y$ for each $x, y \in A$ and $u \in G$. Any continuous application $a : u \mapsto a_u$ of G to a G-set A is called a *cochain* of G with values in A. A cochain $a = (a_u)$ is called a 1-*cocycle* of G with values in A if $a_{uv} = a_u \cdot {}^u a_v$ for each $u, v \in G$. For any 1-cocycle $a = (a_u)$, one has $a_{id} = 1$ and $a_u \cdot^u a_{u^{-1}} = 1$, where $u \in G$ and $1 \in A$ denotes the identity element. The set of 1-cocycles of G with values in a G-set A, is denoted by $Z^1(G, A)$. We say that a G-group A acts on the G-set E from left, in a compatible way with action of G, if there is an application $(a, x) \to a \cdot x$ of $A \times E$ to E satisfying the following conditions:

(i) ${}^u(a \cdot x) =^u a \cdot^u x \quad (a \in A, x \in E, u \in G)$

(ii) $a \cdot (b \cdot x) = (a \cdot b) \cdot x, \text{and } 1 \cdot x = x, \quad (a, b \in A, x \in E)$.

Let A be a G-group, E be a G-set which is compatible with the group action of G, and $a = (a_u) \in Z^1(G, A)$ be a 1-cocycle of A. For any $u \in G$ and $x \in E$, define ${}^{u'}x := a_u \cdot {}^u x$. The G-set with this action of G is denoted by E_a and is called the *twist of* E obtained by the cocycle a.

Let X be a quasi-projective scheme defined over K, $\mathrm{Aut}(X)$ be the automorphism scheme of X and $a = (a_u) \in Z^1(G, \mathrm{Aut}(X))$ be a 1-cocyle. Then there exist an unique quasi-projective K-scheme Y and an unique L-isomorphism

$$f : X \otimes_K L \to Y \otimes_K L$$

such that ${}^u f = f \circ a_u$ holds for any $u \in G$. The scheme Y is denoted by X_a and is called the *twist of* X by 1-cocycle a. One can see that these two notion of twist are compatible in the following sense: The map $f : X(L) \longrightarrow Y(L)$ gives an isomorphism of the twisted G-set $X(L)_a$ onto the G-set $Y(L) = X_a(L)$. Therefore,

$$X_a(K) \cong \{P \in X(L)_a : \ {}^{u'}P = P\} = \{P \in X(L) : a_u \cdot \ {}^u P = P\}. \quad (3.2.1)$$

For more details on above facts, one can see the propositions 2.6 and 2.7 in [?].

Let $\mathcal{C}$ be a smooth projective curve defined over K and let $\mathcal{C}_a$ denote the twist of $\mathcal{C}$ by 1-cocycle $a = (a_u) \in Z^1(G, \mathrm{Aut}(\mathcal{C}))$. Furthermore, for any morphism of curves $\alpha : \mathcal{C}_1 \to \mathcal{C}_2$, let us to denote by $J(\alpha)$ the induced homomorphism of Jacobian variety $J(\mathcal{C}_1)$ into $J(\mathcal{C}_2)$. We note that $J(a) := (J(a_u))$ satisfies the 1-cocycle condition. For $a_{uv} = a_u \circ {}^u a_v$ implies $J(a_{uv}) = J(a_u) \circ {}^u J(a_v)$, since the construction of the Jacobian variety is compatible with base change. Under above conditions, the twist $J(\mathcal{C})_{J(a)}$ of $J(\mathcal{C})$ by the 1-cocycle $J(a)$ is K-isomorphic to $J(\mathcal{C}_a)$. Indeed, if $f : \mathcal{C} \otimes_K L \to \mathcal{C}_a \otimes_K L$ denotes the isomorphism such that ${}^u f = f \circ a_u$ for each $u \in G$, then the induced isomorphism of Jacobian varieties $J(f) : J(\mathcal{C}) \otimes_K L \to J(\mathcal{C}_a) \otimes_K L$ satisfies the equality ${}^u J(f) = J(f) \circ {}^u J(a_u)$ for each $u \in G$, by functoriality. Hence, by the uniqueness of the twist, we see that $J(\mathcal{C})_{J(a)}$ is K-isomorphic to $J(\mathcal{C}_a)$.

3.3 Some results of Hazama

Let $\mathcal{C} : u^2 = f(t)$ be a hyper-elliptic curve defined over a field k of characteristic different from 2, with $f(t) \in k[t]$ of odd degree. There exists a natural projection of $\mathcal{C}$ onto the projective line $\mathbb{P}^1_k$ defined by $(t, u) \mapsto u$, through which we can consider the function field $L := k(\mathcal{C})$ of $\mathcal{C}$ as a quadratic extension of $K := k(\mathbb{P}^1_k) = k(t)$, where t denotes the coordinate of $\mathbb{P}^1_k$. Let $\iota \in \mathrm{Aut}(\mathcal{C})$ be the involution by the extension $L|K$, and let $G = \{id, \iota\}$ be the Galois group of the extension $L|K$. Now, consider an Abelian variety A defined over k, and a 1-cocycle $b = (b_u) \in Z^1(G, \mathrm{Aut}(A))$ defined by $b_{id} = 1$ and $b_\iota = -1$. Then the twist of A by b, which is denoted by A_b, exists and is defined over K. The following theorem is the main result in [**?**].

Theorem 3.3.1. *Let $J(\mathcal{C})$ be the Jacobian variety of $\mathcal{C}$, and $A[2](k)$ be the k-rational 2-division points in $A(k)$. Then, as abelian group we have*

$$A_b(K) \cong Hom_k(J(\mathcal{C}), A) \oplus A[2](k).$$

In particular, if $\mathcal{C} : y^2 = h(x)$ with $h(x) \in k[x]$ of odd degree, and $\mathcal{C}_h$ be the twist of $\mathcal{C}$ given by $h(t)y^2 = h(x)$ defined over K, then

$$J(\mathcal{C}_h)(K) \cong End_k(J(\mathcal{C})) \oplus J(\mathcal{C})[2](k),$$

where $J(\mathcal{C})$ denotes the Jacobian variety of $\mathcal{C}$ and $J(\mathcal{C})[2](k)$ is 2-division k-rational points in $J(\mathcal{C})$.

Now, let $\pi : \mathcal{C}' \to \mathcal{C}$ be a morphism of degree two defined over k between non-singular projective curves over k. Assume that there exist a k-rational point on $\mathcal{C}'$ where π ramifies. Denote $K := k(\mathcal{C})$, $L := k(\mathcal{C}')$ and $G = G_{L|K}$, the Galois group of the extension $L|K$. For any Abelian variety A over k, we define a 1-cocycle $b = (b_u) \in Z^1(G, \mathrm{Aut}(A)$ by $b_{id} = 1$, and $b_\iota = -1$, where ι is the involution associated to the double cover π. Let A_b be the twist of A by the 1-cocycle b. The following theorem is proved by Hazama in [?] which gives the theorem (??) by taking $\mathcal{C} = \mathbb{P}^1_k$ with trivial Jacobian.

Theorem 3.3.2. *Let $A[2](k)$ be the k-rational 2-division points in $A(k)$. As abelian group we have the following isomorphism:*

$$A_b(K) \cong Hom_k(J(\mathcal{C}')/\pi^*(J(\mathcal{C})), A) \oplus A[2](k).$$

In the following, we recall the main result of Hazama in [?] that generalizes the theorems (??) and (??). Let A be an Abelian variety, V and V' are absolutely irreducible quasi-projective varieties, and $\pi : V' \to V$ be a double cover, all defined over k. Let $K := k(V)$, $L := k(V')$, and $G := G_{L|K}$ be the Galois group of the extension $L|K$. Let A_b be the twist of A by the 1-cocycle b. In [?], the Prym variety associated to the double cover $\pi : V' \to V$ is defined as the quotient Abelian variety

$$\mathrm{Prym}_{V'/V} := \frac{\mathrm{Alb}(V')}{\mathrm{Im}(id + \mathrm{Alb}(\iota))},$$

where $\mathrm{Alb}(V')$ is the Albanese variety and $\mathrm{Alb}(\iota)$ is the automorphism of $\mathrm{Alb}(V')$ induced by $\iota \in \mathrm{Aut}(V')$. The following results are the theorem 2.2 and the corollary 2.3 in [?].

Theorem 3.3.3. *With the above notations, assume that there exist a k-rational simple point $v_0' \in V'$. Then we have an isomorphism of Abelian groups:*

$$A_b(K) \cong Hom_k(Prym(V'/V), A) \oplus A[2](k),$$

where $A[2](k)$ denote the abelian group of k-rational 2-division points.

Corollary 3.3.4. *Notation being as above, assume that $Prym_{V'/V}$ is k-isogenous with $E^n \times B$ for some positive integer n, where E is an elliptic curve defined over k, and B is an Abelian variety none of whose simple component k-isogenous to E. Then,*

$$rk(E_b(K)) = n \cdot rk(End_k(E)).$$

3.4 Extension of Hazama's results to cyclic covers

Let $s \geq 2$ be an integer and k a field of characteristic different from s. We are going to generalize the notion of Prym variety to the case of cyclic s-cover $\pi : V' \to V$, for every integer $s \geq 2$, where V and V' are quasi-projective irreducible varieties both as well as π defined over a field k $(char(k), s) = 1$. The *Prym variety* associated to the cyclic s-cover $\pi : V' \to V$ is defined by the quotient Abelian variety

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

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

We note that if both of the varieties V and V' are curves, then this notion of Prym variety is compatible with that one which appeared in [**?**] by applying the following lemma.

Lemma 3.4.1. *Let $s \geq 2$ be an integer and $\pi : V' \to V$ be a cyclic s-cover of irreducible quasi-projective varieties, both as well as π defined over k. Let $\gamma \in Aut(V')$ be an automorphism defined over k of order s and let $\tilde{\gamma}$ be the automorphism of the Albanese variety $Alb(V')$ induced by γ. Then there is a k-isogeny of Abelian varieties,*

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

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

Proof. Let us to consider a more general situation. Let A be an Abelian variety over k of dimension m, and $\lambda \in \mathrm{Aut}(A)$ an order s automorphism. Define

$$a := \dim \ker(id - \lambda)^\circ, \text{ and } \ b := \dim \ker(id + \lambda + \cdots + \lambda^{s-1})^\circ.$$

Considering the induced action on the tangent space of A at origin, we have $a + b = m$. Let A_s be the set of s-division points of A. Then

$$\ker(id - \lambda)^\circ \cap \ker(id + \lambda + \cdots + \lambda^{s-1})^\circ \subseteq A_s.$$

Indeed, if $P \in \ker(id - \lambda)^\circ \cap \ker(id + \lambda + \cdots + \lambda^{s-1})^\circ$ then $\lambda(P) = P$ and hence

$$0 = (id + \lambda + \cdots + \lambda^{s-1})(P) = sP.$$

Thus A is k-isogenous to their product, i.e.,

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

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

$$m - b = \dim \mathrm{Im}(id + \lambda + \cdots + \lambda^{s-1}) = \dim \ker(id - \lambda)^\circ = a.$$

Therefore, we obtain the equality

$$\mathrm{Im}(id + \lambda + \cdots + \lambda^{s-1}) = \ker(id - \lambda)^\circ.$$

Now, applying this general result to the case $A = \mathrm{Alb}(V')$, gives that

$$\mathrm{Prym}_{X'/X} \sim_k \ker(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1} : \mathrm{Alb}(V') \to \mathrm{Alb}(V'))^\circ.$$

□

Now, we are ready to generalize the theorem (**??**) and its corollary (**??**) as follows. Let A/k be an Abelian variety, $s \geq 2$ be an integer and assume that $\sigma : A \to A$ is an automorphism of order s. Let $\pi : V' \to V$ be a cyclic s-cover of irreducible quasi-projective varieties, both as well as π defined over k such that $(char(k), s) = 1$. Denote $K := k(V)$, $L := k(V')$ and let $G := \langle \gamma \rangle$ be the cyclic Galois group of the Galois extension $L|K$ which has order s. Let $b = (b_u) \in Z^1(G, \mathrm{Aut}(A))$ defined by $b_{id} = id$ and $b_{\gamma^j} = \sigma^j$, for each $\gamma^j \in G$. Denote by A_b the twist of A with the 1-cocycle b. The following theorem describes the Mordell-Weil group of K-rational points on A_b.

Theorem 3.4.2. *Assume that there exist a simple k-rational point $v_0' \in V'(k)$. Then we have an isomorphism of Abelian groups:*

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

where $A[s](k)$ denote the Abelian group of k-rational s-division points.

Proof. First, we recall that

$$A(L) = \{k\text{-rational maps } V' \to A\ \} \cong \mathrm{Hom}_k(\mathrm{Alb}(V'), A) \oplus A(k),$$

where $P \in A(L)$ corresponds to the pair $(\lambda, c) \in \mathrm{Hom}_k(\mathrm{Alb}(V'), A) \oplus A(k)$ such that $P(v') = \lambda(i_{V'}(v')) + c$ for each $v' \in V'$. See the theorem 4 in chapter II in [?] for more details. Here we assume that $i_{V'} : V' \to \mathrm{Alb}(V')$ maps v_0' to the origin of $\mathrm{Alb}(V')$ so that $i_{V'}$ is defined over k. This implies that the action of $\gamma^j \in G$ is given by $\gamma^j(\lambda, c) = (\lambda \circ \tilde{\gamma}^j, c)$, for $j = 0, \cdots, s-1$, where $\tilde{\gamma}$ is the automorphism of the Albanese variety $\mathrm{Alb}(V')$ induced by $\gamma \in \mathrm{Aut}(V')$. Since $\gamma^s = id$ and hence $\tilde{\gamma}^s = id$, so using the equalities (**??**), we have

$$A_b(K) \cong \{P \in A(L) : b_u \cdot \ {}^u(P) = P\},$$

which implies that $(\lambda, c) \in A_b(K)$ if and only if

$$\gamma^j(\lambda, c) = (\lambda \circ \tilde{\gamma}^j, c) = (\lambda \circ \tilde{\gamma}^{s-j}, c) = \gamma^{s-j}(\lambda, c).$$

Thus, $(\lambda, c) \in A_b(K)$ if and only if α annihilates $Im(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1})$ and $c \in A[s](k)$. Therefore, we obtain the desired isomorphism

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

□

Corollary 3.4.3. *Assume that $Prym_{V'/V}$ is k-isogenous with $A^n \times B$ for some positive integer n, where A and B are Abelian varieties defined over k such that $\dim(B) = 0$ or $\dim(B) > \dim(A)$ and none of irreducible components of B is k-isogenous to A. Supposing, furthermore, that $A[s](k) = \{\mathcal{O}\}$, then*

$$rk(A_b(K)) \geq n \cdot rk(End_k(A)).$$

Proof. By the above theorem and using the assumptions, we have

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

Therefore, as $\mathbb{Z}$-modules, we have $\mathrm{rk}(A_b(K)) \geq n \cdot \mathrm{rk}(End_k(A))$. □

Given integer $s \geq 2$, let $\pi_i : V_i' \to V_i$ $(i = 1, 2)$ be s-covers of irreducible quasi-projective varieties, $\gamma_i \in \mathrm{Aut}(V_i')$ be an automorphism of order s, all defined over k such that $(char(k), s) = 1$, and let $G_i = \langle \gamma_i \rangle$

be the corresponding Galois group. Let $\tilde{\gamma}_i$ is the automorphism of the Albanese variety $\mathrm{Alb}(V_i')$ induced by $\gamma_i \in \mathrm{Aut}(V_i')$, for $i = 1, 2$. We consider the Galois cover $\pi_1 \times \pi_2 : V_1' \times V_2' \to V_1 \times V_2$ whose Galois group is $G_1 \times G_2 \cong \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$, and we assume that W is its intermediate cover $V_1' \times V_2'/G$, where G is the cyclic group generated by $\gamma = (\gamma_1, \gamma_2) \in \mathrm{Aut}(V_1' \times V_2')$. Let $\tilde{\gamma} = (\tilde{\gamma}_1, \tilde{\gamma}_2)$ be an order s automorphism in $\mathrm{Aut}(\mathrm{Alb}(V_1') \times \mathrm{Alb}(V_2'))$ corresponding to γ. With these notations, we have the following proposition.

Proposition 3.4.4. *Assume that there exist k-rational points $v_i' \in V_i'(k)$ for $i = 1, 2$. Then there is a k-rational isogeny of Abelian varieties:*

$$Prym_{V_1' \times V_2'/W} \sim_k Prym_{V_1'/V_1} \times Prym_{V_2'/V_2}.$$

Proof. For simplicity, let $\mu = id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1}$ and $\mu_i = id + \tilde{\gamma}_i + \cdots + \tilde{\gamma}_i^{s-1}$ for $i = 1, 2$. Using the lemma (**??**), it is enough to show that

$$\ker\big(\mu\big)^\circ \sim_k \ker(\mu_1)^\circ \times \ker(\mu_2)^\circ.$$

In order to show this, we recall that there exists a k-rational isomorphism

$$\phi := \mathrm{Alb}(V_1') \times \mathrm{Alb}(V_2') \to \mathrm{Alb}(V_1' \times V_2'),$$

given by $\phi = \tilde{\phi}_1 + \tilde{\phi}_2$, where $\tilde{\phi}_i : \mathrm{Alb}(V_i') \to \mathrm{Alb}(V_1') \times \mathrm{Alb}(V_2')$ is the induced by the inclusion map $\phi_i : V_i' \to V_1' \times V_2'$ given by $\phi_1(v) = (v, v_2')$ and $\phi_2(v) = (v_1', v)$. By this isomorphism, we have

$$\ker(\mu) \sim_k \ker(\mu_1) \times \ker(\mu_2),$$

which implies that

$$\ker(\mu)^\circ \sim_k \ker(\mu_1)^\circ \times \ker(\mu_2)^\circ.$$

Therefore, applying the lemma (**??**) gives the desired result

$$\begin{aligned} \mathrm{Prym}_{V_1' \times V_2'/W} &\sim_k \ker(\mu)^\circ \sim_k \ker(\mu_1)^\circ \times \ker(\mu_2)^\circ \\ &\sim_k \mathrm{Prym}_{V_1'/V_1} \times \mathrm{Prym}_{V_2'/V_2}. \end{aligned}$$

□

In the next sections, using the corollary (**??**) and the proposition (**??**), we are going to find s-cover $\pi : V' \to V$ whose Prym variety has a high power of the Jacobian of a super-elliptic curve. This will give us certain Abelian variety defined over $K = k(V)$ with large Mordell-Weil rank.

3.5 An application of the main result

Let $s \geq 2$ be an integer and assume that k is sufficiently large field with $(char(k), s) = 1$ so that it contains a primitive s-th root of unity, which is denoted by ζ. For a fixed polynomial $f(x) = \sum_{j=0}^{r} a_j x^{r-j} \in k^*[x]$ of degree $r \geq s$, let $\mathcal{C}_{s,f}$ be the super-elliptic curve defined by the affine equation $y^s = f(x)$.[*] The curve $\mathcal{C}_{s,f}$ admits an order s automorphism $\iota : (x, y) \mapsto (x, \zeta \cdot y)$. Consider m copies of $\mathcal{C}_{s,f}$ and for each of these copies write $\mathcal{C}_{s,f}^{(i)}$, the super-elliptic curve defined by the affine equation $y_i^s = f(x_i)$, for $1 \leq i \leq m$. Denote $\mathbf{C}_m := \prod_{i=1}^{m} \mathcal{C}_{s,f}^{(i)}$, which can be expressed by the equations $y_i^s = f(x_i)$, for $i = 1, \cdots, m$. For each of the curves $\mathcal{C}_{s,f}^{(i)}$, denote by ι_i the corresponding automorphism. Consider the cyclic subgroup $G = \langle \gamma \rangle$, where $\gamma := (\iota_1, \cdots, \iota_m) \in \mathrm{Aut}(\mathbf{C}_m)$, and define $\mathbf{V}_m := \mathbf{C}_m / G$. Let L be the function field of $\mathbf{C}_m$, i.e.,

$$L = k(x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_m),$$

where $x_1, x_2, \cdots, x_m$ are independent transcendentals and each y_i defines a degree s extension by the equation $y_i^s - f(x_i) = 0$. Then, $K := k(\mathbf{V}_m)$ the function field of $\mathbf{V}_m$ is the invariant elements of L by the action of G, i.e.,

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

Since $(y_1^{s-1} y_{i+1})^s = f(x_1)^{s-1} f(x_{i+1})$ holds for $i = 1, \cdots, m-1$, so by assuming $z_i := y_1^{s-1} y_{i+1}$ the variety $\mathbf{V}_m$ is given by the equations

$$z_i^s = f(x_1)^{s-1} f(x_{i+1}) \ (i = 1, \cdots, m-1). \tag{3.5.1}$$

Note that $L|K$ is a cyclic extension of degree s determined by the $y_1^s = f(x_1)$,

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

Let $\mathcal{C}_{s,f}^{\xi}$ denotes the twist of $\mathcal{C}_{s,f}$ by the extension $L|K$. In a similar way as in the corollary 3.1 in [?], one can check that $\mathcal{C}_{s,f}^{\xi}$ is defined by the affine equation

$$f(x_1)^{s-1} y^s = f(x). \tag{3.5.2}$$

[*] The reason for taking f with all coefficients in k^* will be described in the remark (??).

Moreover, the twisted curve $\mathcal{C}_{s,f}^{\xi}$ contains the K-rational points:

$$P_1 := (x_1, 1/y_1^{s-2}) \text{ and } P_i := (x_{i+1}, y_{i+1}/y_1^{s-1}) \text{ for } (1 \leq i \leq m-1). \quad (3.5.3)$$

Remark 3.5.1. *The construction of the varieties $\mathbf{C}_m$ and $\mathbf{V}_m$ generalizes the unified method of [**?**], which is used to find elliptic curves of high rank having a given set of algebraic numbers as x-coordinates of generators of their Mordell-Weil group.*

Let $b = (b_u) \in Z^1(G, \mathrm{Aut}(J(\mathcal{C}_{s,f}))$ defined by $b_{id} = id$ and $b_{\gamma^j} = \tilde{\iota}^j$, for each $\gamma^j \in G$, where $J(\mathcal{C}_{s,f})$ is the Jacobian variety of $\mathcal{C}_{s,f}$ 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 $J(\mathcal{C}_{s,f})_b$ the twist of $J(\mathcal{C}_{s,f})$ with the 1-cocycle b. By the last argument in the first section, one has $J(\mathcal{C}_{s,f})_b = J(\mathcal{C}_{s,f}^{\xi})$. The relation between $J(\mathcal{C}_{s,f})$ and the Prym variety of the covering $\mathbf{C}_m \to \mathbf{V}_m$ is given by the following proposition, which is used in the proof of the next theorem.

Proposition 3.5.2. *Assume that there exists $c \in \mathcal{C}_{s,f}(k)$. Then there exists an k-isogeny of Abelian variety:*

$$Prym_{\mathbf{C}_m/\mathbf{V}_m} \sim_k \prod_{i=1}^{m} Prym_{\mathcal{C}_{s,f}^{(i)}/\mathbb{P}^1} = \prod_{i=1}^{m} J(\mathcal{C}_{s,f}^{(i)}), \quad (3.5.4)$$

where $J(\mathcal{C}_{s,f}^{(i)}) = J(\mathcal{C}_{s,f})$ for each $i = 1, \cdots, m$.

Proof. It is a well known fact that the Albanese and Jacobian varieties of curves are coincided. Applying the lemma (**??**) for $V' = \mathcal{C}_{s,f}^{(i)} = \mathcal{C}_{s,f}$ and $V = \mathbb{P}^1$ gives that

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

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

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

which implies that $\mathrm{Prym}_{\mathcal{C}_{s,f}^{(i)}/\mathbb{P}^1} = J(\mathcal{C}_{s,f}^{(i)})$ and hence

$$\mathrm{Alb}(\mathbf{C}_m) = \prod_{i=1}^{m} \mathrm{Alb}(\mathcal{C}_{s,f}^{(i)}) = \prod_{i=1}^{m} J(\mathcal{C}_{s,f}^{(i)}).$$

Let $\iota_i \in \mathrm{Aut}(\mathcal{C}_{s,f}^{(i)})$ be an order s automorphism and $\tilde{\iota}_i \in \mathrm{Aut}(J(\mathcal{C}_{s,f}^{(i)}))$ be the induced automorphism by ι_i, for each $i = 1, \cdots, m$. We recall that there exists a k-rational isomorphism

$$\phi := \prod_{i=1}^{m} J(\mathcal{C}_{s,f}^{(i)}) \to \prod_{i=1}^{m} J(\mathcal{C}_{s,f}^{(i)}),$$

given by $\phi = \tilde{\phi}_1 + \cdots + \tilde{\phi}_m$, where $\tilde{\phi}_i : J(\mathcal{C}_{s,f}^{(i)}) \to \mathrm{Alb}(\mathbf{C}_m) \prod_{i=1}^{m} J(\mathcal{C}_{s,f}^{(i)})$ is the induced by the inclusion map

$$\phi_i : \mathcal{C}_{s,f}^{(i)} \to \mathbf{C}_m = \prod_{i=1}^{m} \mathcal{C}_{s,f}^{(i)}, \ P_i \mapsto \phi_i(P_i) = (c, \cdots, P_i, \cdots, c),$$

where $c \in \mathcal{C}_{s,f}^{(i)}(k)$. By this isomorphism, the automorphism $\gamma := (\iota_1, \cdots, \iota_m)$ of $\mathbf{C}_m$ corresponds to $\tilde{\gamma} = (\tilde{\iota}_1, \cdots, \tilde{\iota}_m)$ in $\prod_{i=1}^{m} \mathrm{Aut}(J(\mathcal{C}_{s,f}^{(i)}))$. Then, we have

$$\ker(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1}) \sim_k \prod_{i=1}^{m} \ker(id + \tilde{\iota}_i + \cdots + \tilde{\iota}_i^{s-1}),$$

which implies that

$$\ker(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1})^\circ \sim_k \prod_{i=1}^{m} \ker(id + \tilde{\iota}_i + \cdots + \tilde{\iota}_i^{s-1})^\circ.$$

Therefore, applying the lemma (**??**) gives that

$$\begin{aligned} \mathrm{Prym}_{\mathbf{C}_m/\mathbf{V}_m} &\sim_k \ker(id + \tilde{\gamma} + \cdots + \tilde{\gamma}^{s-1})^\circ \\ &\sim_k \prod_{i=1}^{m} \ker(id + \tilde{\gamma}_i + \cdots + \tilde{\gamma}_i^{s-1})^\circ \\ &\sim_k \prod_{i=1}^{m} \mathrm{Prym}_{\mathcal{C}_{s,f}^{(i)}/\mathbb{P}^1} = \prod_{j=1}^{m} J(\mathcal{C}_{s,f}^{(i)}). \end{aligned}$$

□

Denote by $Q_1, \cdots, Q_m$, the image of the points $P_1, \cdots, P_m$ given by (**??**) under the canonical embedding of $\mathcal{C}_{s,f}^{\xi}$ into $J(\mathcal{C}_{s,f}^{\xi})$. The following theorem describes the group of K-rational points on the Jacobian variety $J(\mathcal{C}_{s,f}^{\xi})$, and gives a lower bound for its Mordell-Weil rank. We note that the case $s = 2$ and $m = 1$ gives the theorem (**??**).

Theorem 3.5.3. *Assume that there exists $c \in \mathcal{C}_{s,f}(k)$ and let $J(\mathcal{C}_{s,f})[s](k)$ be the group of k-rational s-division points in $J(\mathcal{C}_{s,f})$. Then we have an isomorphism of Abelian groups:*

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

Assuming that $J(\mathcal{C}_{s,f})[s](k)$ is trivial group, we have

$$rk(J(\mathcal{C}^{\xi}_{s,f})(K)) = m \cdot rk(End_k(J(\mathcal{C}_{s,f}))),$$

and the points $Q_1, \cdots, Q_m$ belong to the set of independent generators of $J(\mathcal{C}^{\xi}_{s,f})(K)$.

Proof. This is consequence of the theorem (**??**) and its corollary (**??**) together with the proposition (**??**). Indeed, it is enough to consider the varieties $V' = \mathbf{C}_m$, $V = \mathbf{V}_m$, and $A = J(\mathcal{C}_{s,f})$ where $\mathcal{C}_{s,f}$ is a supper-elliptic curve given by affine equation $y^s = f(x)$. Tracing back the isomorphisms in the proof of the corollary (**??**), shows that the points $Q_1, \cdots, Q_m$ belong to the set of independent generators of $J(\mathcal{C}^{\xi}_{s,f})(K)$. □

The following corollary is an immediate consequence of the above theorem.

Corollary 3.5.4. *Assume that $End_k(J(\mathcal{C}_{s,f}))) \cong \mathbb{Z}$ and there exists a rational point $c \in \mathcal{C}_{s,f}(k)$. Then the Mordell-Weil rank of $J(\mathcal{C}^{\xi}_{s,f})(K)$ is m, where K is the function field of $\mathbf{V}_m$, and its generators are the canonical image of the points P_i's given by (**??**) in the Jacobian variety $J(\mathcal{C}^{\xi}_{s,f})$.*

Since the varieties $\mathbf{C}_m$ and $\mathbf{V}_m$ are defined by a fixed polynomial $f \in k^*[x]$, so if we suppose that $f(x) = \sum_{j=0}^{r} a_j x^{r-j} \in k^*[x]$ is an arbitrary element, then the function field of $\mathbf{C}_m$ and $\mathbf{V}_m$ are respectively

$$L' = k(x_1, \cdots, x_m)(a_0, \cdots, a_r, y_1, \cdots, y_m), \text{and}$$

$$K' = k(x_1, \cdots, x_m)(a_0, \cdots, a_r, z_1, \cdots, z_m),$$

where $L'|K'$ is a cyclic extension of degree s given by $y_1^s = f(x_1)$. Thus, intersecting $\mathbf{V}_m$ with the hyperplanes $x_1 = \alpha_0$ and $x_{i+1} = \alpha_i$ gives a new variety $\mathbf{W}_m$ defined by the following $m-1$ equations, $z_i^s = f(\alpha_0)^{s-1} f(\alpha_{i+1})$ $(i = 1, \cdots, m-1)$, regarded as a sub-variety in the projective space $\mathbb{P}_{\bar{k}}^{m+r}$ with coordinates $a_0, \cdots, a_r, z_1, \cdots, z_{m-1}$. In what follows, we will show that the variety $\mathbf{W}_m$ is k-birational to a r-dimensional complete intersection variety. Assume that k_0 is a field containing a primitive s-th root of unity, denoted by ζ, where $s \geq 2$ is an integer. Given integers $2 \leq s \leq r < n$ and a fixed sequence $\mathcal{B} = \{\alpha_i\}_{i=0}^{\infty}$ of pairwise distinct elements of k_0, let $\mathcal{B}_n := \{\alpha_0, \alpha_1, \cdots, \alpha_n\}$ and define a projective sub-variety $\mathbf{X}_n$ of $\mathbb{P}_{\bar{k}}^n$ by the equations

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & \alpha_i \\ \cdots & \cdots & \vdots & \cdots & \cdots \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & \alpha_i^r \\ Y_0^s & Y_1^s & \cdots & Y_r^s & Y_i^s \end{vmatrix} = 0, \ (r < i \leq n). \tag{3.5.5}$$

Following theorem shows a basic properties of the varieties $\mathbf{X}_n$, such as its smoothness and being varieties of general type for large enough n.

Theorem 3.5.5. *Given integers $2 \leq s \leq r < n$, we have:*

(i) The variety $\mathbf{X}_n$ is a smooth $(s, \cdots, s)$-complete intersection of dimension r;

(ii) The canonical sheaf of $\mathbf{X}_n$ is $\mathcal{O}((s-1)n - (sr+1))$. Hence $\mathbf{X}_n$ is a smooth variety of general type in $\mathbb{P}_{\bar{k}}^n$ if $n \geq N_r^s$, where

$$N_r^s := [(sr+1)/(s-1)] + 1.$$

Proof. Using the definition equations $\mathbf{X}_n$ and the Jacobian criterion one can see that $\mathbf{X}_n$ is a smooth $(s, \cdots, s)$-complete intersection varieties of dimension r. By the exercise (II.8.4.e) or applying theorem (II.8.20) in [?] repeatedly gives that the canonical sheaf of $\mathbf{X}_n$ is

$$\mathcal{O}(s(n-r) - n - 1) = \mathcal{O}((s-1)n - (sr+1)).$$

Therefore, $\mathbf{X}_n$ is a smooth variety of general type for any $n \geq N_r^s$, with N_r^s defined as above. □

We will use the following lemma in the proof of the next result.

Lemma 3.5.6. *Let m and n ($m \leq n$) be integers and $\mathbf{b}_0, \cdots, \mathbf{b}_n$ be column vectors of size m, with entries in a field of characteristic zero. Suppose that any m vector of these are linearly independent. Then the following three conditions are equivalent:*

(i) $\operatorname{rank}(\begin{bmatrix} \mathbf{b}_0 & \mathbf{b}_1 & \cdots & \mathbf{b}_{n-1} & \mathbf{b}_n \\ u_0 & u_1 & \cdots & u_{n-1} & u_n \end{bmatrix}) = m,$

(ii) For $i = m, m+1, \cdots, n,$ $\begin{vmatrix} \mathbf{b}_0 & \mathbf{b}_1 & \cdots & \mathbf{b}_{m-1} & \mathbf{b}_i \\ u_0 & u_1 & \cdots & u_{m-1} & u_i \end{vmatrix} = 0.$

(iii) For $i = 1, 2, \cdots, n-m+1,$ $\begin{vmatrix} \mathbf{b}_0 & \mathbf{b}_i & \mathbf{b}_{i+1} & \cdots & \mathbf{b}_{i+m-1} & \mathbf{b}_i \\ u_0 & u_i & u_{i+1} & \cdots & u_{i_m-1} & u_i \end{vmatrix} = 0.$

Proof. This is the lemma (3.1) in [**?**]. □

Proposition 3.5.7. *For any* $[Y_0 : Y_1 : \cdots : Y_n] \in \mathbf{X}_n$*, we have*

$$\#\{i : Y_i = 0\} \leq r.$$

Proof. Let i_0 be an index such that $Y_{i_0} \neq 0$. By definition of $\mathbf{X}_n$,

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & \alpha_i \\ \cdots & \cdots & \vdots & \cdots & \cdots \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & \alpha_i^r \\ Y_0^s & Y_1^s & \cdots & Y_r^s & Y_i^s \end{vmatrix} = 0,$$

for $i = r+1, \cdots, n$. Hence, using the lemma (**??**) with $m = r+1$, we have

$$\operatorname{rank}(\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \cdots & \cdots & \cdots & \vdots & \cdots \\ \alpha_0^r & \alpha_1^r & \alpha_2^r & \cdots & \alpha_n^r \\ Y_0^s & Y_1^s & Y_2^s & \cdots & Y_n^s \end{bmatrix}) = r+1. \quad (*)$$

Now, if we suppose that $\#\{i : Y_i = 0\} > r$, then there exist $r+1$ indexes $i_1, \cdots, i_{r+1}$ such that $Y_{i_1} = \cdots = Y_{i_{r+1}} = 0$. Thus, the $(r+2) \times (r+2)$

sub-matrix of the above matrix consisting of the $i_1-, \cdots, i_{r+1}$-th columns has the following form

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{i_0} & \alpha_{i_1} & \cdots & \alpha_{i_{r+1}} \\ \cdots & \cdots & \vdots & \cdots \\ \alpha_{i_0}^r & \alpha_{i_1}^r & \cdots & \alpha_{i_{r+1}}^r \\ Y_{i_0}^s & 0 & \cdots & 0 \end{bmatrix},$$

whose determinant does not vanish, because $Y_{i_0} \neq 0$. But, this is a contradiction to (*) by the lemma (**??**). □

The following theorem gives a relation between the varieties $\mathbf{W}_{n+1}$ and $\mathbf{X}_n$.

Theorem 3.5.8. *For every $n > r$, the variety $\mathbf{W}_{n+1}$ is k-birational to $\mathbf{X}_n$.*

Proof. For integers $n > r$, we have a rational map $\varphi : \mathbf{W}_{n+1} \to \mathbf{X}_n$ defined by

$$[a_0 : \cdots : a_r : z_1 : \cdots : z_n] \mapsto [f(\alpha_0) : z_1 : \cdots : z_n],$$

where $f(x) := \sum_{j=0}^{r} a_j x^{r-j}$. It admits an inverse $\varphi^{-1} : \mathbf{X}_n \to \mathbf{W}_{n+1}$ given by

$$[Y_0 : \cdots : Y_n] \mapsto [a_0; \cdots : a_r : Y_0^{s-1} Y_1 \cdot D : \cdots : Y_0^{s-1} Y_n \cdot D],$$

where $a_1, \cdots, a_r$ and D_r are as follows

$$a_0 := \begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & \alpha_i \\ \cdots & \cdots & \vdots & \cdots & \cdots \\ \alpha_0^{r-1} & \alpha_1^{r-1} & \cdots & \alpha_r^{r-1} & \alpha_i^{r-1} \\ Y_0^s & Y_1^s & \cdots & Y_r^s & Y_i^s \end{vmatrix}, \quad a_2 := - \begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & \alpha_i \\ \cdots & \cdots & \vdots & \cdots & \cdots \\ \alpha_0^{r-1} & \alpha_1^{r-1} & \cdots & \alpha_r^{r-1} & \alpha_i^{r-1} \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & \alpha_i^r \\ Y_0^s & Y_1^s & \cdots & Y_r^s & Y_i^s \end{vmatrix},$$

$$\cdots, a_r := (-1)^{r-1} \begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_r^2 & \alpha_i^2 \\ \cdots & \cdots & \vdots & \cdots & \cdots \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & \alpha_i^r \\ Y_0^s & Y_1^s & \cdots & Y_r^s & Y_i^s \end{vmatrix}, \quad D_r := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r \\ \cdots & \cdots & \vdots & \cdots \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r \end{vmatrix}.$$

□

Remark 3.5.9. *Let $a_0, a_1, \cdots, a_r$ and D_r be as in the proof of the theorem (**??**). Then $D_r \neq 0$, because it is the determinant of a Vondermonde matrix. Using the proposition (**??**), one can conclude that $a_j \neq 0$, for $j = 0, \cdots, r$. This is the reason for considering the polynomials $f \in k^*[x]$ in defining the varieties $\mathbf{V}_n$ and $\mathbf{W}_n$.*

3.6 Relation with the results on the powerful values of polynomials

Given integers $2 \leq s \leq r < n$ and a fixed sequence $\mathcal{B} = \{\alpha_i\}_{i=0}^{\infty}$ of pairwise distinct algebraic numbers over number field k_0 containing a primitive s-th root of unity, denoted by ζ, define $\mathcal{B}_n := \{\alpha_0, \alpha_1, \cdots, \alpha_n\}$ and suppose that k is an arbitrary finite extension of k_0 containing $k_0(\alpha_0, \cdots, \alpha_n)$. Let $\mathbb{F}_{r,s}^{\mathcal{B}_n}$ denote the set of those $f \in k^*[x]$ such that $f(\alpha_i) \in (k^*)^s$ for each $0 \leq i \leq n$, i.e. there exist some $\beta_i \in k^*$ such that $f(\alpha_i) = \beta_i^s$. Let $\mathbb{G}_{r,s}^{\mathcal{B}_n}$ be the subset of $\mathbb{F}_{r,s}^{\mathcal{B}_n}$, whose irreducible factors has multiplicity strictly less than s. Let $\mathbb{D}_{r,s}^{\mathcal{B}_n}$ be the subset of $\mathbb{F}_{r,s}^{\mathcal{B}_n}$ with zero discriminant. It is clear that $\mathbb{F}_{r,s}^{\mathcal{B}_n} \backslash \mathbb{D}_{r,s}^{\mathcal{B}_n} \subseteq \mathbb{G}_{r,s}^{\mathcal{B}_n}$, with equality in the case $s = 2$. We note that $\mathbb{F}_{r,s}^{\mathcal{B}_n}$ and $\mathbb{G}_{r,s}^{\mathcal{B}_n}$ are respectively subset of $\mathbf{F}_{r,s}^{\mathcal{B}_n}$ and $\mathbf{G}_{r,s}^{\mathcal{B}_n}$, which are defined in Chapter **??**. Fix the integers r and s and for each $n > r$, denote by $\mathcal{S}_n$ and $\mathcal{D}_n$ the set of all supper-elliptic curves $\mathcal{C}_{s,f}$ with affine model $y^s = f(x)$, with $f \in \mathbb{F}_{r,s}^{\mathcal{B}_n}$ and $f \in \mathbb{D}_{r,s}^{\mathcal{B}_n}$, respectively. Therefore, each supper-elliptic curve $\mathcal{C}_{s,f} \in \mathcal{S}_n$ contains at least $n+1$ points with x-coordinates $\alpha_0, \cdots, \alpha_n$. By the main result of the Chapter **??**, one can conclude that:

Theorem 3.6.1. *Assume the Vojta's Conjecture (**??**). Given integers $2 \leq s \leq r$, let $N := 2r^2 + 6r$ if $r = s$, and $2sr^2 + sr$ otherwise. Then there exist positive constants C_0 and C_1 such that $C_0 \leq \#(\mathcal{S}_N \backslash \mathcal{D}_N) \leq C_1$; and hence for each $n \geq N$, we have $\#(\mathcal{S}_n \backslash \mathcal{D}_n) \leq C_1$.*

We note that the constants C_0 and C_1 depend on $\alpha_0, \cdots, \alpha_N$, k, r and s, but the integer M only depend on r and s

Theorem 3.6.2. *Given integers $n \geq r$, there is a one-to-one correspondence between the set $\mathcal{S}_n$ and the k-rational points on the variety $\mathbf{W}_{n+1}$.*

Proof. For $\mathcal{C}_{s,f} \in \mathcal{S}_n$ with an affine model $y^s = f(x) = \sum_{j=0}^{r} a_j x^{r-j}$, we assume that $f(\alpha_i) = \beta_i^s$ for some $\beta_i \in k^*$. Define the map $\psi : \mathcal{S}_n \to \mathbf{W}_{n+1}(k)$ by

$$\mathcal{C}_{s,f} \mapsto P_{s,f} := [a_0; \cdots ; a_r; \beta_0^{s-1}\beta_1; ...; \beta_0^{s-1}\beta_n].$$

Since $(\beta_0^{s-1}\beta_i)^s = f(\alpha_0)^{s-1}f(\beta_i)$, so the point $P_{s,f}$ belongs to $\mathbf{W}_{n+1}(k)$ and hence the map ψ is well-defined injective map. Since $\mathcal{D}_n$ contains the supper-elliptic curves $\mathcal{C}_{s,f}$ with $disc(f) = 0$, which can be described as an equation in a_j's, so its image determines a closed set in $\mathbf{W}_{n+1}$, which we denote it by W_{n+1}.

In order to show that the map ψ is surjective map, we are going to use the k-birational map $\varphi : \mathbf{W}_{n+1} \to \mathbf{X}_n$ given in the proof of the theorem (**??**). Let $X_n \subseteq \mathbf{X}_n$ be the image of W_{n+1} under the map φ. The supper-elliptic curve $\mathcal{C}_{s,f} \in \mathcal{S}_n$ corresponding to $P = [Y_0 : \cdots : Y_n] \in \mathbf{X}_n(k)$ with $Y_0 \neq 0$, is k-isomorphic to the supper-elliptic curve

$$\tilde{\mathcal{C}}_{s,f}^{\xi} : D_r^{s-1} y^s = a_0 x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + a_r,$$

which is obtained by expanding the following determinant along the last column,

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & x \\ \vdots & \vdots & \cdots & \vdots & x^2 \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & x^r \\ Y_0^s & Y_1^s & \cdots & Y_r^s & 0 \end{vmatrix} = 0.$$

Indeed, the map $\varphi^{-1} : \mathbf{X}_n(k) \to \mathbf{W}_{n+1}(k)$ in the proof of the theorem (**??**), sends a k-rational point $P = [Y_0 : \cdots : Y_n]$ on $\mathbf{X}_n$ to the point

$$[a_0 : a_1 : \cdots : a_r : Y_0^{s-1}Y_1 \cdot D_r : Y_0^{s-1}Y_2 \cdot D_r : \cdots : Y_0^{s-1}Y_n \cdot D_r] \in \mathbb{P}^{n+r},$$

where $a_0, a_1, \cdots, a_r$ and D_r are determined by expanding the above determinant, as in the proof of theorem (**??**). Thus, the twist of the supper-elliptic curve corresponding to P is $\mathcal{C}_{s,f}^{\xi} : f(\alpha_0)y^s = f(x)$, where $f(x) = a_0x^r + a_1x^{r-1} + \cdots + a_{r-1}x + a_r$. Since

$$f(\alpha_0) = -\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & \alpha_0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & \alpha_0^r \\ Y_0^s & Y_1^s & \cdots & Y_r^s & 0 \end{vmatrix} = -\begin{vmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_r & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \alpha_0^r & \alpha_1^r & \cdots & \alpha_r^r & 0 \\ Y_0^s & Y_1^s & \cdots & Y_r^s & -Y_0^s \end{vmatrix} = D_r \cdot Y_0^s,$$

so $\mathcal{C}_{s,f}^{\xi}$ is given by $(D_r \cdot Y_0^s)^{s-1}y^s = f(x)$. Hence, the map $(x', y') \mapsto (x', y'Y_0)$ provides a k-isomorphism of $\mathcal{C}_{s,f}^{\xi}$ to $\tilde{\mathcal{C}}_{s,f}^{\xi}$. Note that the points $P \in X_n$ are exceptional for creating a smooth supper-elliptic curves, because such points correspond to a polynomial with zero discriminate in $\mathcal{D}_n$. Therefore, the map ψ is a bijection map. □

Remark 3.6.3. *The point $P \in X_n$ are exceptional for creating a smooth supper-elliptic curves, because such points correspond to a polynomial with zero discriminate by the map φ defined in the proof of the theorem (**??**).*

Theorem 3.6.4. *Assume the Vojta's Conjecture (**??**). Suppose that k_0 is a number field containing a primitive s-th root of unity. Given any integers $2 \leq s \leq r$, let $N := 2r^2+6r$ if $r = s$, and $2sr^2+sr$ otherwise. Assume that k is an arbitrary finite extension of k_0 containing $k_0(\alpha_0, \cdots, \alpha_N)$. Then, there exist positive constants C_0 and C_1 such that*

$$C_0 \leq \#(\mathbf{W}_{N+1} \backslash W_{N+1})(k) = \#(\mathbf{X}_{N+1} \backslash X_{N+1})(k) \leq C_1,$$

and hence for each $n > N$, we have $\#(\mathbf{W}_{n+1} \backslash W_{n+1}) = \#(\mathbf{X}_n \backslash X_n) \leq C_1$.

Proof. By theorem (**??**), given integers $2 \leq s \leq r < n$, we know that $\mathbf{X}_n$ is a variety of general type for all $n \geq [(sr+1)/(s-1)] + 1$. Since the integer N defined as above is large than $[(sr+1)/(s-1)] + 1$, so $\mathbf{X}_n$ is a variety of general type for all $n \geq N$. By theorem (**??**)), the variety $\mathbf{X}_n$ is k-birational to $\mathbf{W}_{n+1}$, which is in one-to-one correspondence to the set $\mathcal{S}_n$ by theorem (**??**). Thus, by theorem (**??**), there exist positive constants C_0 and C_1 such that

$$C_0 \leq \#(\mathbf{W}_{N+1} \backslash W_{N+1})(k) = \#(\mathbf{X}_{N+1} \backslash X_{N+1})(k) \leq C_1,$$

and hence for each $n > N$, we have $\#(\mathbf{W}_{n+1}\backslash W_{n+1}) = \#(\mathbf{X}_n\backslash X_n) \leq C_1$, where W_n and X_n are defined as in the proof of the theorem (**??**) for each $n \geq r$. □

The above theorem shows that the Vojta's Conjecture implies the following conjecture due to Bombieri-Lang for the varieties $\mathbf{W}_{n+1}$ and $\mathbf{X}_n$ for $n \geq N$, where N is as in the above theorem.

Conjecture 3.6.5. *(***Bombieri-Lang***) Let X be a smooth projective algebraic variety of general type, defined over a number field k_0. Then there exists a proper Zariski-closed subset Z of X such that for all number fields k containing k_0, the set $(X\backslash Z)(k)$ is finite.*

References

[1] A. Bèrczes, J. H. Evertse, and L. Györy,: *Effective results for hyper- and supper-elliptic equations over number fields*. Publ. Math. Debresen, Vol. 82, N. 3-4, pp. 354-358, (2013). 609-636.

[2] E. Bombieri and W. Gubler: *Heights in Diophantine Geometry*, Cambridge University press, New york, 2006.

[3] A. Borel and J. P. Serre: *Théorèmes de finitude en cohomologie galoisienne*, J. Number Theory, Vol. 39, pp. 111-164, 1964.

[4] H. Davenport, D. J. Lewis, and A. Schinzel: *Polynomials of certain special types*, Acta Arith., Vol. 9, pp. 107-117, 1964.

[5] R. Hartshorne: *Algebraic geometry*, Graduate text in Mathematics, Vol. 52, Springer, New York, 1977.

[6] Fumio Hazama: *On the Mordell-Weil group of certain abelian varieties defined over function fields*, J. Number Theory, Vol. 37, pp. 168-172, 1991.

[7] Fumio Hazama: *The Mordell-Weil group of certain Abelian varieties defined over function fields*, Tohoku Math. J., Vol. 44, pp. 335-334, 1992.

[8] Fumio Hazama: *Rational points on certain Abelian varieties over function fields*, J. Number Theory, Vol. 50, pp. 278-285, 1995.

[9] M. Hindry and J. H. Silverman: *Algebraic geometry*, Graduate text in Mathematics, Vol. 201, Springer, New York, 2001.

[10] Su-Ion Ih:*Algebraic points on the projective line*, J. Korean Math. Soc. Vol. 45, no. 6, pp. 1635-1646, 2008.

[11] S. Lang: *Number Theory III, Survey of Diophantine Geometry*, Encyclopedia of Mathematical Sciences, Vol. 60, Springer, Berlin, 1991.

[12] S. Lang: *Abelian Varieties*, Springer, New York-Berlin, 1983.

[13] S. Lang:: *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[14] H. Lange and A. Ortega: *Prym varieties of cyclic coverings*, Geom. Dedicata, Vol. 150, pp. 391-403, 2011.

[15] K. Mahler: *An inequality for the discriminant of a polynomial*, Michigan Math. J., Vol. 11, pp. 257-262, 1964.

[16] D. Masser and J. D. Vaaler: *Counting algebraic numbers with large height. II*, Trans. Amer. Math. Soc., Vol. 359, no. 1, pp. 427-445, 2007.

[17] D. G. Northcott: *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Camb. Phil. Soc., Vol. 45, pp. 502-509, 1949.

[18] H. Pasten: *Powerful values of polynomials and a conjecture of Vojta*, J. Number Theory, Vol. 133, pp. 2964-2998, 2014.

[19] P. Ribenboim: *Polynomials whose values are powers*, Collection of articles dedicated to Helmut Hasse on his seventy- fifth birthday, J. für der reine angew. Math. II, Vol. 268/269, pp. 34-40, 1974.

[20] S. H. Schanuel: *Heights in number fields*, Bull. Soc. Math. France, Vol. 133, no. 4, pp. 433-449, 1979.

[21] W. M. Schmidt: *Northcott's theorem on heights. I*, Monatsh. Math., 115, no. 1-2, pp. 169-181, 1993.

[22] W. M. Schmidt: *Northcot's theorem on heights. II: The quadratic case*, Acta Arith., Vol. 70, no. 4, pp. 343-375, 1995.

[23] A. Shinzel and R. Tijdeman: *On the equation $y^m = P(x)$*, Acta Arith., Vol. 31, pp. 199-204, 1976.

[24] J. H. Silverman: *The Arithmetic of Elliptic Curves, second edition*, Graduate text in Mathematics, Vol. 106, Springer, New York, 2009.

[25] P. Vojta: *Diophantine Approximation and Value distribution theory*, Lecture Notes in Mathematics, Vol. 1239, Springer-Verlag, Berlin, 1987.

[26] P. Vojta: *Diophantine Approximation and Nevanlinna Theory*, in Arithmetic Geometry, (Lectures given at the C.I.M.E. Summer School held in Cetraro, Italy Sept. 10-15, 2007), pp. 111-224, 2009.

[27] P. Vojta: *A more general ABC conjecture*, Inter. Math. Res. Notices, Vol. 21, pp. 1103-1116, 1998.

[28] M. Waldschmidt: *Diophantine approximation on linear algebraic group*, Transcendence Properties of the Exponential Function in Several Variables. Grund. der Math. Wiss., Vol. 326, Springer-Verlag, Berlin-Heidelberg, 2000.

[29] P.G. Walsh: *On a conjecture of Schinzel and Tijdeman*, Zakopane-Koscielisko, de Gruyter, Vol. 1, pp. 577-582, 1997.

[30] H. Yamagishi: *A unified method of construction of elliptic curves with high Mordell-Weil rank*, Pacific J. Math, Vol. 191, pp. 507-524, 1991.

[31] H. Yamagishi: *Boundedness of Mordell-Weil ranks of certain elliptic curves and Lang's conjecture*, J. of Number Theory, Vol. 21, pp. 295-306, 2003.