J. reine angew. Math., Ahead of Print
DOI 10.1515/CRELLE.2011.139

Journal für die reine und
angewandte Mathematik

Explicit uniform estimation of rational points II. Hypersurface coverings

By *Huayi Chen* at Paris

Abstract. We obtain an explicit uniform estimate for the number of rational points in a projective plane curve whose heights do not exceed the degree of the curve.

1. Introduction

This article is a continuation of [12]. Let K be a number field and X be a sub-variety of $\mathbb{P}^n_K$ of dimension d and of degree δ. The purpose of this article is to establish the following explicit estimate (see Theorem 4.2):

Theorem A. *Let $\varepsilon > 0$ and D be an integer such that*

$$D > \max\{(\varepsilon^{-1}+1)(2\delta^{-\frac{1}{d}}(d+1)+\delta-2), 2(n-d)(\delta-1)+d+2\}.$$

There is an explicitly computable constant $C = C(\varepsilon, \delta, n, d, K)$ such that, for any $B \geqq e^{\varepsilon}$, the set $S_1(X; B)$ of regular rational points of X with exponential height $\leqq B$ is covered by not more than $CB^{(1+\varepsilon)\delta^{-\frac{1}{d}}(d+1)}$ hypersurfaces of degree $\leqq D$ not containing X.

This theorem generalizes some results of Heath-Brown [16], Theorem 14, and Broberg [6], Theorem 1, in the sense that we estimate explicitly the degree and the number of the auxiliary hypersurfaces needed to cover the set of rational points with bounded height.

The strategy of Heath-Brown in the proof of [16], Theorem 14, consists of establishing that a family of rational points having the same reduction modulo a "large" prime number are contained in one hypersurface (not containing X) with "low" degree. This idea is inspired by results of Bombieri–Pila [1] and Pila [22], and has been developed later in [6], [7], [8], [9], [10], [14], [17], [18], [23], [24].

Suggested by Bost, we adapt the above idea into the framework of his slope method [2], [3], [4]. Note that Bogomolov has asked a similar question on the possibility of replacing the method of Heath-Brown by arguments in Arakelov geometry (see [13], Question 34). We consider the evaluation map from the space of homogeneous polynomials to the space of values of these polynomials on a family of rational points. If the rational points in the family have the same reduction modulo some finite place $\mathfrak{p}$ of K such that the norm of $\mathfrak{p}$ is big, then the (logarithmic) height of this evaluation map is very negative. Hence by the slope inequality, the evaluation map cannot be injective and thus we obtain a non-zero homogeneous polynomial whose image by the evaluation map vanishes. The desired hypersurface is obtained as the zero locus of the homogeneous polynomial.

The flexibility of the geometric framework (see Theorem 3.1) permits us to develop several interesting variants. For example, instead of considering the reduction modulo a finite place $\mathfrak{p}$, we treat the case where the family of rational points has the same reduction modulo some power of $\mathfrak{p}$. In other words, we can take a finite place $\mathfrak{p}$ with relatively lower norm and consider a family of rational points whose $\mathfrak{p}$-adic distances are very small. Such a family is contained in a hypersurface of lower degree. This argument permits us to prove that the constant C figuring in Theorem A depends on the degree of K over $\mathbb{Q}$ but not on the discriminant. Another variant consists of taking into account the local Hilbert–Samuel functions of the variety, which generalizes a result of Salberger [23], Theorem 3.2. This permits us to sharpen the constant C in Theorem A in the case where X is a plane curve and B is small. As a consequence, we obtain the following result.

Theorem B. *Assume that X is an integral plane curve of degree δ. Then, for any $\varepsilon > 0$, one has*

$$\#S(X;\delta) \ll_K \delta^{2+\varepsilon}.$$

This gives an answer to a question of Heath-Brown [13], Question 27.

To obtain an explicit upper bound for the number and the degree of the auxiliary hypersurfaces, we need several effective estimates in algebraic geometry and in Arakelov geometry, which shall be recalled in the second section. In the third section, we explain the conditions which ensure that a family of rational points lies in the same hypersurface of low degree. Finally, in the fourth section, we estimate the number of hypersurface needed to cover rational points; in the fifth section, we discuss the plane curve case.

We keep Notation 1–8 introduced in [12], §2. Remind that K denotes a number field and $\mathcal{O}_K$ denotes its integer ring. We shall also use the following notation.

Notation. 9. Denote by $n \in \mathbb{N}\setminus\{0\}$ an integer and by $\bar{\mathcal{E}}$ the *trivial* Hermitian vector bundle of rank $n+1$. In other words, $\mathcal{E} = \mathcal{O}_K^{\oplus(n+1)}$, and for any embedding $\sigma : K \to \mathbb{C}$, the canonical basis of $\mathcal{E}$ is an orthonormal basis of $\|\cdot\|_\sigma$. See Notation 4 for the notion of Hermitian vector bundles.

10. Denote by $\bar{\mathcal{L}}$ the universal quotient sheaf on $\mathbb{P}^n_{\mathcal{O}_K} = \mathbb{P}(\mathcal{E})$, equipped with the Fubini–Study metrics.

11. Any point $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$ gives rise to a unique $\mathcal{O}_K$-point $\mathcal{P} \in \mathbb{P}(\mathcal{E})$. The height of P (with respect to $\bar{\mathcal{L}}$) is by definition the slope (see Notation 6) of $\mathcal{P}^*(\bar{\mathcal{L}})$, denoted by $h(P)$. Note that one has

$$h(P) = \frac{1}{[K:\mathbb{Q}]}\left(\sum_{\mathfrak{p}\in\operatorname{Spm}\mathcal{O}_K} \log \max_{1\leqq i\leqq n} |x_i|_{\mathfrak{p}} + \frac{1}{2}\sum_{\sigma:K\to\mathbb{C}} \log\sum_{j=0}^{n}|x_j|_\sigma^2\right).$$

See Notation 2 for the definition of the absolute values $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_\sigma$. Define $H(P) := \exp\big([K:\mathbb{Q}]h(P)\big)$. Remind that here the logarithmic height function h is absolute (i.e., invariant under finite field extensions of K), while the exponential one H is relative.

12. For any integer $D \geqq 1$, let $\bar{E}_D$ be the $\mathcal{O}_K$-module $H^0\big(\mathbb{P}(\mathcal{E}), \mathcal{L}^{\otimes D}\big)$, equipped with the John metrics $\|\cdot\|_{\sigma,J}$ associated to the sup-norm $\|\cdot\|_{\sigma,\sup}$. We remind that the sup-norm is defined as follows:

$$\forall s \in E_D \otimes_{\mathcal{O}_K,\sigma} \mathbb{C}, \quad \|s\|_{\sigma,\sup} := \sup_{x \in \mathbb{P}^n_\sigma(\mathbb{C})} \|s(x)\|_\sigma.$$

The John norm $\|\cdot\|_{\sigma,J}$ is a Hermitian norm on $E_D \otimes_{\mathcal{O}_K,\sigma} \mathbb{C}$ such that

$$\|s\|_{\sigma,\sup} \leqq \|s\|_{\sigma,J} \leqq \sqrt{\mathrm{rk}(E_D)} \cdot \|s\|_{\sigma,\sup}.$$

Denote by $r(D)$ the rank of E_D. One has $r(D) = \binom{n+D}{D}$.

13. Let X be an integral closed subscheme of $\mathbb{P}^n_K = \mathbb{P}(\mathcal{E}_K)$. Let d be the dimension of X and δ be the degree of X. Recall that one has $\delta = \deg\big(c_1(\mathcal{L}_K)^d \cdot [X]\big)$. Denote by $\mathscr{X}$ the Zariski closure of X in $\mathbb{P}(\mathcal{E})$. The (relative) Arakelov height of X is denoted by $h_{\bar{\mathcal{L}}}(X)$. Recall that

$$h_{\bar{\mathcal{L}}}(X) := \frac{1}{[K:\mathbb{Q}]} \widehat{\deg}\big(\hat{c}_1(\bar{\mathcal{L}})^{d+1} \cdot [\mathscr{X}]\big).$$

14. For any integer $D \geqq 1$, let F_D be the saturation (in $H^0(\mathscr{X}, \mathcal{L}|_{\mathscr{X}}^{\otimes D})$) of the image of the restriction map

$$\eta_{X,D} : E_{D,K} = H^0\big(\mathbb{P}(\mathcal{E}_K, \mathcal{L}_K^{\otimes D})\big) \to H^0(X, \mathcal{L}|_X^{\otimes D}),$$

namely F_D is the largest sub-$\mathcal{O}_K$-module of $H^0(\mathscr{X}, \mathcal{L}|_{\mathscr{X}}^{\otimes D})$ containing $\mathrm{Im}(\eta_{X,D})$ and such that $F_{D,K} = \mathrm{Im}(\eta_{X,D})_K$. We equip F_D with the quotient metrics (from the metrics of E_D) so that $\bar{F}_D$ becomes a Hermitian vector bundle on $\mathrm{Spec}\,\mathcal{O}_K$. Denote by $r_1(D)$ the rank of F_D.

15. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ with residue field $\mathbb{F}_{\mathfrak{p}}$. For any point in $\mathscr{X}(\mathbb{F}_{\mathfrak{p}})$, denote by $\mathcal{O}_\xi$ the local ring of $\mathscr{X}$ at ξ and by $\mathfrak{m}_\xi$ the maximal ideal of $\mathcal{O}_\xi$. Note that $\mathcal{O}_\xi$ is a local algebra over $\mathcal{O}_{K,\mathfrak{p}}$. Denote by $H_\xi : \mathbb{N} \to \mathbb{N}$ the Hilbert–Samuel function of $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$ (which is the local ring of $\mathscr{X}_{\mathbb{F}_{\mathfrak{p}}}$ at ξ), namely,

$$H_\xi(k) = \mathrm{rk}_{\mathbb{F}_{\mathfrak{p}}}\big((\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^k/(\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^{k+1}\big).$$

Let $\big(q_\xi(m)\big)_{m \geqq 1}$ be the increasing sequence of non-negative integers such that the integer $k \in \mathbb{N}$ appears exactly $H_\xi(k)$ times. Let $Q_\xi(m) = q_\xi(1) + \cdots + q_\xi(m)$. Denote by μ_ξ the multiplicity of the local ring $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$. Recall that one has

$$H_\xi(k) = \frac{\mu_\xi}{(d-1)!} k^{d-1} + o(k^{d-1}).$$

16. For any real number $B > 0$, let $S(X;B)$ be the subset of $X(K)$ consisting of points P such that $H(P) \leqq B$ (see Notation 11 for the definition of $H(\cdot)$). Denote by $S_1(X;B)$ the subset of $S(X;B)$ of regular points. Define $N(X;B)$ and $N_1(X;B)$ to be the cardinality of $S(X;B)$ and $S_1(X;B)$ respectively.

17. For any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\xi \in \mathscr{X}(\mathbb{F}_\mathfrak{p})$ and $B > 0$, denote by $S(X;B,\xi)$ the set of points $P \in S(X;B)$ whose reduction modulo $\mathfrak{p}$ is ξ. Define

$$S_1(X;B,\mathfrak{p}) = \bigcup_{\substack{\xi \in \mathscr{X}(\mathbb{F}_\mathfrak{p}) \\ \xi \text{ regular}}} S(X;B,\xi),$$

where ξ regular means that ξ is a regular point of $\mathscr{X}_{\mathbb{F}_\mathfrak{p}}$, or equivalently, $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$ is a regular local ring.

18. More generally, for any maximal ideal $\mathfrak{p}$ and any $a \in \mathbb{N}\setminus\{0\}$, denote by $A_\mathfrak{p}^{(a)}$ the Artinian local ring $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^a\mathcal{O}_{K,\mathfrak{p}}$. For any point $\eta \in \mathscr{X}(A_\mathfrak{p}^{(a)})$, denote by $S(X;B,\eta)$ the set of points in $S(X;B)$ whose reduction modulo $\mathfrak{p}^a$ coincides with η. We shall use the fact that

$$\forall a \in \mathbb{N}\setminus\{0\},\ \forall \xi \in \mathscr{X}(\mathbb{F}_\mathfrak{p}),\quad S(X;B,\xi) = \bigcup_{\substack{\eta \in \mathscr{X}(A_\mathfrak{p}^{(a)}) \\ \xi = (\eta \bmod \mathfrak{p})}} S(X;B,\eta).$$

19. We introduce several constants as follows:

$$\begin{aligned} C_1 &= (d+2)\hat{\mu}_{\max}\big(S^\delta(\bar{\mathcal{E}}^\vee)\big) + \frac{1}{2}(d+2)\log \operatorname{rk}(S^\delta\mathcal{E}) \\ &\quad + \frac{\delta}{2}\log\big((d+2)(n-d)\big) + \frac{\delta}{2}(d+1)\log(n+1), \\ C_2 &= \frac{r}{2}\log\operatorname{rk}(S^\delta\mathcal{E}) + \frac{1}{2}\log\operatorname{rk}(\Lambda^{n-d}\mathcal{E}) + \log\sqrt{(n-d)!} + (n-d)\log\delta, \\ C_3 &= (n-d)C_1 + C_2. \end{aligned}$$

Recall that the constant C_1 has been defined in [12], (21).[1] With the notation of [12], Theorem 3.8, the constant C_2 is just $C_2(\bar{\mathcal{E}}, n-d, \delta)$ (see also Remark 3.9 loc. cit.). Finally, the constant C_3 appears in [12], Theorem 3.10. Recall that one has $C_3 \ll_{n,d} \delta$ (see Theorem 3.10 loc. cit.).

20. By the effective version of Chebotarev's theorem (cf. [20], see also [25], Theorem 2) there exists an explicitly computable constant $\alpha(K)$ such that, for any real number $x \geqq 1$, there exists a finite place $\mathfrak{p} \in \Sigma_f$ such that $N_\mathfrak{p} \in \big(x, \alpha(K)x\big]$. This is an analogue of Bertrand's postulate for number fields.

2. Reminders

We recall in this section several results that we shall use in the sequel. They are either well known or described in [12].

---

[1] Since $S^\delta\bar{\mathcal{E}}$ is a direct sum of Hermitian line bundles, the quantity $\varrho^{(d+2)}\big(\Gamma^\delta(\bar{E})\big)$ vanishes (see [12], §2.2). Furthermore, when $\bar{\mathcal{E}}$ is trivial, one has $\hat{\mu}_{\max}(\Lambda^{n-d}\bar{\mathcal{E}}) = 0$.

2.1. Let $(P_i)_{i\in I}$ be a collection of distinct rational points of X (see Notation 13) and $D \geqq 1$ be an integer. Assume that the evaluation map $f : F_{D,K} \to \bigoplus_{i\in I} P_i^* \mathcal{L}^{\otimes D}$ is an isomorphism (see Notation 14). Then the equality

$$\hat{\mu}(\overline{F}_D) = \frac{1}{r_1(D)} \left[\sum_{i\in I} D h(P_i) + h(\Lambda^{r_1(D)} f) \right]$$

holds. In particular, one has

$$\frac{\hat{\mu}(\overline{F}_D)}{D} \leqq \sup_{i\in I} h(P_i) + \frac{1}{D r_1(D)} h(\Lambda^{r_1(D)} f), \tag{1}$$

where $h(\Lambda^{r_1(D)} f)$ is defined as

$$h(\Lambda^{r_1(D)} f) = \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\mathfrak{p}} \log \|\Lambda^{r_1(D)} f\|_{\mathfrak{p}} + \sum_{\sigma: K\to\mathbb{Q}} \log \|\Lambda^{r_1(D)} f\|_{\sigma} \right).$$

A slight variant of this argument shows that, if $(P_i)_{i\in J}$ is a family of rational points of X such that

$$\sup_{i\in J} h(P_i) < \frac{\hat{\mu}_{\max}(\overline{F}_D)}{D} - \frac{1}{2}\log(n+1), \tag{2}$$

then there exists a hypersurface of degree D in $\mathbb{P}^n_K$ not containing X which contains all rational points P_i. See [12], Proposition 2.12, for details.

2.2. For any integer $D \geqq 1$, one has the following estimates:

$$\binom{D+d+1}{d+1} - \binom{D-\delta+d+1}{d+1} \leqq r_1(D) := \mathrm{rk}(F_D) \leqq \delta \binom{D+d}{d}. \tag{3}$$

See [11] for the upper bound and [26] for the lower bound.

2.3. For any integer $D \geqq 2(n-d)(\delta-1)+d+2$, one has

$$\frac{\hat{\mu}(\overline{F}_D)}{D} \geqq \frac{d!}{\delta(2d+2)^{d+1}} h_{\bar{\mathcal{L}}}(X) - \log(n+1) - 2^d, \tag{4}$$

where $h_{\bar{\mathcal{L}}}(X)$ is the Arakelov height of X. See [12], Theorem 4.8 and Remark 4.9, for details.

2.4. Since $\overline{F}_D$ is a quotient of $\overline{E}_D$, one has (see Notation 12)

$$\hat{\mu}(\overline{F}_D) \geqq \hat{\mu}_{\min}(\overline{E}_D) \geqq -\frac{1}{2} D \log(n+1). \tag{5}$$

We refer to [12], Corollary 2.9, for the proof. Note that this bound is much less precise than (4). However, it works for any integer $D \geqq 1$.

2.5. For any integer $D \geqq 1$, one has

$$\frac{\hat{\mu}(\bar{F}_D)}{D} \leqq \frac{1}{\delta} h_{\bar{\mathcal{L}}}(X) + \frac{1}{2}\log(n+1). \tag{6}$$

See [12], Remark 4.11.

2.6. There exists a Hermitian vector subbundle $\overline{M}$ of $S^{(\delta-1)(n-d)}\bar{\mathcal{E}}$ such that

(i) $\hat{\mu}_{\min}(\overline{M}) \geqq -(n-d)h_{\bar{\mathcal{L}}}(X) - C_3$,

(ii) the subscheme of $\mathbb{P}(\mathcal{E})$ defined by vanishing of M contains the singular loci of fibres of $\mathscr{X}$ but not the generic point of $\mathscr{X}$,

where the constant C_3 is defined in Notation 19. This result has been proved in [12], Theorem 3.10. In particular, the singular locus of X is contained in a hypersurface of degree $(\delta-1)(n-d)$ not containing X.

2.7. Suppose that $P \in X(K)$ is a regular point and $\mathcal{P}$ is the $\mathcal{O}_K$-point of $\mathbb{P}(\mathcal{E})$ extending P. For any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, if the reduction of $\mathcal{P}$ modulo $\mathfrak{p}$ is a singular point of $\mathscr{X}_{\mathbb{F}_\mathfrak{p}}$, we write $\alpha_\mathfrak{p}(P) = 1$, else we write $\alpha_\mathfrak{p}(P) = 0$. We have shown in [12], Proposition 2.11, that, for any real number $N_0 > 0$, the following inequality holds:

$$\sum_{N_\mathfrak{p} \geqq N_0} \alpha_\mathfrak{p}(P) \leqq \frac{(n-d)(\delta-1)h(P) + (n-d)h_{\bar{\mathcal{L}}}(X) + C_3}{(\log N_0)/[K:\mathbb{Q}]}. \tag{7}$$

In fact, it suffices to apply [12], Proposition 2.11, to the special case $\bar{I} = \overline{M}$, where $\overline{M}$ is as in §2.6.

2.8. The following estimates of binomial coefficients will be used:

$$\frac{(N-k+1)^k}{k!} \leqq \binom{N}{k} \leqq \frac{(N-(k-1)/2)^k}{k!}, \quad N \geqq k \geqq 1.$$

The second inequality comes from the comparison of the arithmetic and the geometric means:

$$N(N-1)\cdots(N-k+1) \leqq \left(\frac{N+(N-1)+\cdots+(N-k+1)}{k}\right)^k.$$

3. Existence of the auxiliary hypersurface

The purpose of this section is to establish the following theorem.

Theorem 3.1. *Let $S = (\mathfrak{p}_j)_{j\in J}$ be a finite family of maximal ideals of $\mathcal{O}_K$ and $(a_j)_{j\in J} \in (\mathbb{N}\setminus\{0\})^J$. For each $\mathfrak{p}_j$, let η_j be a point in $\mathscr{X}(A_{\mathfrak{p}_j}^{(a)})$ (see Notation 18) whose reduction modulo $\mathfrak{p}$ is denoted by ξ_j. Assume that $(\xi_j)_{j\in J}$ are distinct. Consider a family $(P_i)_{i\in I}$ of* *rational points of $\mathscr{X}_K$ such that, for any $i \in I$ and any $j \in J$, the reduction of P_i modulo $\mathfrak{p}_j^{a_j}$ coincides with η_j. Assume that* (*see Notation* 11, 14 *and* 15)

$$\sup_{i \in I} h(P_i) < \frac{\hat{\mu}(\overline{F}_D)}{D} - \frac{\log r_1(D)}{2D} + \frac{1}{[K:\mathbb{Q}]} \sum_{j \in J} \frac{Q_{\xi_j}(r_1(D))}{D r_1(D)} \log N_{\mathfrak{p}_j}^{a_j}. \tag{8}$$

Then there exists a section $s \in E_{D,K}$ which does not vanish identically on $\mathscr{X}_K$ and such that $P_i \in \operatorname{div}(s)$ for any $i \in I$.

This theorem generalizes a result of Salberger [23], Theorem 3.2, in two aspects. On one hand, we treat projective varieties over a number field; on the other hand, we consider a family of thickenings of points over finite places.

The proof of Theorem 3.1 consists of adapting the idea of Bombieri–Pila and Heath-Brown in the framework of the slope method. Note that Broberg has generalized [16], Theorem 14, to the number field case, which corresponds to the case where $|J| = 1$ and $a_j = 1$ here. However, his method is different from ours. In fact, the slope method permits us to avoid using Siegel's lemma. Moreover, in (8), there appears only the degree of the number field K but not the discriminant.

The following subsections are devoted to the proof of Theorem 3.1 and to discuss several applications. We first estimate the heights of the determinants of some evaluation maps. This stage is quite similar to the determinant argument of Bombieri–Pila and Heath-Brown. Then we use the slope inequality to obtain the desired result. To apply the theorem, we need explicit estimates of the functions Q_{ξ_j} and $r_1(D)$, which we discuss in the end of this section.

3.1. Estimation of norms.

Lemma 3.2. *Let A be a ring and M be an A-module.*

(i) *If N is a sub-A-module of M such that M/N is generated by q elements, then for any integer $m \geqq q$, we have $\Lambda^m M = (\Lambda^{m-q} N) \wedge (\Lambda^q M)$.*

(ii) *If $M = M_1 \supset M_2 \supset \cdots \supset M_i \supset M_{i+1} \supset \cdots$ is a decreasing sequence of sub-A-modules of M such that, for any $i \geqq 1$, M_i/M_{i+1} is isomorphic to a principal ideal of A, then for any integer $r \geqq 1$, we have*

$$\Lambda^r M = M_1 \wedge M_2 \wedge \cdots \wedge M_r.$$

Proof. (ii) is a consequence of (i). To prove (i), by induction it suffices to establish the case where $m = r + 1$. Since M/N is generated by q elements, we have $\Lambda^{r+1}(M/N) = 0$ (see [5], Chapter III, §7, n° 3, Proposition 3). Furthermore, since the kernel of the canonical homomorphism of exterior algebras $\Lambda M \to \Lambda(M/N)$ is the ideal generated by N (loc. cit.), we obtain that $\Lambda^{r+1} M \subset N \wedge (\Lambda^r M)$. □

Lemma 3.3. *Let k be a field equipped with a non-archimedean absolute value $|\cdot|$, U and V be two k-linear ultranormed spaces of finite rank and $\varphi : U \to V$ be a k-linear* *homomorphism. Let m be the rank of U. For any integer* $1 \leqq i \leqq m$, *let*

$$\lambda_i = \inf_{\substack{W \subset U \\ \operatorname{codim} W = i-1}} \|\varphi|_W\|.$$

If $i > m$, *let* $\lambda_i = 0$. *Then for any integer* $r > 0$, *we have*

$$\|\Lambda^r \varphi\| \leqq \prod_{i=1}^{r} \lambda_i. \tag{9}$$

Proof. Let $\varepsilon > 0$ be an arbitrary positive real number. We shall construct a decreasing filtration of U,

$$U = U_1 \supsetneq U_2 \supsetneq \cdots \supsetneq U_m, \tag{10}$$

such that $\|\varphi|_{U_i}\| \leqq \lambda_i + \varepsilon$. By definition, there exists a vector $x_m \in U$ of norm 1 such that $\|\varphi(x_m)\| \leqq \lambda_m + \varepsilon$. Suppose that we have chosen $U_{i+1} \supset \cdots \supset U_m$ such that $\|\varphi|_{U_j}\| \leqq \lambda_j + \varepsilon$ for any $i+1 \leqq j \leqq m$. Since U_{i+1} has codimension i in U, the set of vectors $x \in U$ of norm 1 with $\|\varphi(x)\| \leqq \lambda_i + \varepsilon$ can not be contained in U_{i+1}. Pick an element $x_i \in U \setminus U_{i+1}$ of norm 1 with $\|\varphi(x_i)\| \leqq \lambda_i + \varepsilon$. Let U_i be the linear subspace generated by x_i and U_{i+1}. Since the norm of U is ultrametric, one obtains $\|\varphi|_{U_i}\| \leqq \lambda_i + \varepsilon$. By induction we can construct the filtration as announced. By Lemma 3.2, one obtains

$$\|\Lambda^r \varphi\| \leqq \prod_{i=1}^{r} (\lambda_i + \varepsilon).$$

Since $\varepsilon > 0$ is arbitrary, the proposition is proved. □

3.2. A preliminary result on local homomorphisms. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and ξ be an $\mathbb{F}_\mathfrak{p}$-point of $\mathscr{X}$. Suppose given a family $(f_i)_{1 \leqq i \leqq m}$ of local homomorphisms of $\mathcal{O}_{K,\mathfrak{p}}$-algebras from $\mathcal{O}_\xi$ (see Notation 15) to $\mathcal{O}_{K,\mathfrak{p}}$. Let E be a free sub-$\mathcal{O}_{K,\mathfrak{p}}$-module of finite type of $\mathcal{O}_\xi$ and let f be the $\mathcal{O}_{K,\mathfrak{p}}$-linear homomorphism $(f_i|_E)_{1 \leqq i \leqq m} : E \to \mathcal{O}_{K,\mathfrak{p}}^m$. As f_1 is a homomorphism of $\mathcal{O}_{K,\mathfrak{p}}$-algebras, it is surjective. Let $\mathfrak{a}$ be the kernel of f_1. One has $\mathcal{O}_\xi/\mathfrak{a} \cong \mathcal{O}_{K,\mathfrak{p}}$. Furthermore, since $\mathcal{O}_\xi$ is a local ring of maximal ideal $\mathfrak{m}_\xi$, one has $\mathfrak{m}_\xi \supset \mathfrak{a}$. Moreover, since f_1 is a local homomorphism, the equality $\mathfrak{a} + \mathfrak{p}\mathcal{O}_\xi = \mathfrak{m}_\xi$ holds. For any integer $j \geqq 0$, $\mathfrak{a}^j/\mathfrak{a}^{j+1}$ is an $\mathcal{O}_\xi/\mathfrak{a} \cong \mathcal{O}_{K,\mathfrak{p}}$-module of finite type, and

$$\mathbb{F}_\mathfrak{p} \otimes_{\mathcal{O}_{K,\mathfrak{p}}} (\mathfrak{a}^j/\mathfrak{a}^{j+1}) \cong (\mathfrak{a}/\mathfrak{p}\mathcal{O}_\xi)^j/(\mathfrak{a}/\mathfrak{p}\mathcal{O}_\xi)^{j+1} \cong (\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^j/(\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^{j+1}.$$

By Nakayama's lemma, the rank of $\mathfrak{a}^j/\mathfrak{a}^{j+1}$ over $\mathcal{O}_{K,\mathfrak{p}}$ is equal to the rank of $(\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^j/(\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^{j+1}$ over $\mathbb{F}_\mathfrak{p}$, that is, $H_\xi(j)$ according to Notation 15. The filtration

$$\mathcal{O}_\xi = \mathfrak{a}^0 \supset \mathfrak{a}^1 \supset \cdots \supset \mathfrak{a}^j \supset \mathfrak{a}^{j+1} \supset \cdots$$

of $\mathcal{O}_\xi$ induces a filtration

$$\mathcal{F} : E = E \cap \mathfrak{a}^0 \supset E \cap \mathfrak{a}^1 \supset \cdots \supset E \cap \mathfrak{a}^j \supset E \cap \mathfrak{a}^{j+1} \supset \cdots \tag{11}$$

of E whose j-th subquotient $E \cap \mathfrak{a}^j / E \cap \mathfrak{a}^{j+1}$ is a free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank $\leqq H_\xi(j)$.

Assume that $a \in \mathbb{N}\setminus\{0\}$ is such that the reductions of f_i modulo $\mathfrak{p}^a$ are the same (in other words, the composed homomorphisms $\mathcal{O}_\xi \xrightarrow{f_i} \mathcal{O}_{K,\mathfrak{p}} \to \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^a\mathcal{O}_{K,\mathfrak{p}}$ are the same), then the restriction of f on $E \cap \mathfrak{a}^j$ has norm $\leqq N_\mathfrak{p}^{-ja}$. In fact, for any $1 \leqq i \leqq m$, one has $f_i(\mathfrak{a}) \subset \mathfrak{p}^a\mathcal{O}_{K,\mathfrak{p}}$ and hence $f_i(\mathfrak{a}^j) \subset \mathfrak{p}^{aj}\mathcal{O}_{K,\mathfrak{p}}$.

By Lemma 3.3, we obtain the following result.

Proposition 3.4. *Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and $\xi \in \mathscr{X}(\mathbb{F}_\mathfrak{p})$. Suppose that $(f_i)_{1\leqq i\leqq m}$ is a family of local $\mathcal{O}_{K,\mathfrak{p}}$-linear homomorphisms from $\mathcal{O}_\xi$ to $\mathcal{O}_{K,\mathfrak{p}}$ whose reductions modulo $\mathfrak{p}^a$ are the same, where $a \in \mathbb{N}\setminus\{0\}$. Let E be a free sub-$\mathcal{O}_{K,\mathfrak{p}}$-module of finite type of $\mathcal{O}_\xi$ and $f = (f_i|_E)_{1\leqq i\leqq m}$. Then, for any integer $r \geqq 1$, one has*

$$\|\Lambda^r f_K\| \leqq N_\mathfrak{p}^{-Q_\xi(r)a}, \tag{12}$$

where $N_\mathfrak{p}$ is the degree of $\mathbb{F}_\mathfrak{p}$ over its characteristic field. See Notation 15 *for the definition of Q_ξ.*

Proof. Consider the filtration (11) above. The restriction of f on $E \cap \mathfrak{a}^j$ has norm $\leqq N_\mathfrak{p}^{-ja}$, which implies that (see Notation 15 for the definition of q_ξ)

$$\inf_{\substack{W\subset E_K\\ \operatorname{codim} W=j-1}} \|f_K|_W\| \leqq N_\mathfrak{p}^{-q_\xi(j)a},$$

where we have used the fact that $\operatorname{rk}(E\cap\mathfrak{a}^j) - \operatorname{rk}(E\cap\mathfrak{a}^{j+1}) \leqq H_\xi(j)$. The inequality (12) then follows from Lemma 3.3. □

3.3. Proof of Theorem 3.1. Let $D \geqq 1$ be an integer. Let F_D and $r_1(D) = \operatorname{rk} F_D$ be as in Notation 14. Assume that the section predicted by the theorem does not exist. Then the evaluation map $f : F_{D,K} \to \bigoplus_{i\in I} P_i^*\mathcal{L}_K$ is injective. By possibly replacing I by a subset, we may suppose that f is an isomorphism. For any embedding $\sigma : K \to \mathbb{C}$, one has

$$\frac{1}{r_1(D)}\log\|\Lambda^{r_1(D)}f\|_\sigma \leqq \log\|f\|_\sigma \leqq \log\sqrt{r_1(D)},$$

where the second inequality comes from the definition of metrics of John (see Notation 12). Furthermore, f is induced by a homomorphism of $\mathcal{O}_K$-modules $F_D \to \bigoplus_{i\in I}\mathcal{P}_i^*\mathcal{L}^{\otimes D}$, where $\mathcal{P}_i$ denotes the $\mathcal{O}_K$-point of $\mathscr{X}$ extending P_i. Hence for any finite place $\mathfrak{p}$ of K, one has $\log\|\Lambda^{r_1(D)}f\|_\mathfrak{p} \leqq 0$.

Let $j \in J$. For each $i \in I$, the $\mathcal{O}_K$-point $\mathcal{P}_i$ defines a local homomorphism from $\mathcal{O}_{\xi_j}$ to $\mathcal{O}_{K,\mathfrak{p}_j}$ which is $\mathcal{O}_{K,\mathfrak{p}_j}$-linear. By taking a local trivialization of $\mathcal{L}$ at ξ_j, we identify F_D with a sub-$\mathcal{O}_{K,\mathfrak{p}_j}$-module of $\mathcal{O}_{\xi_j}$. Proposition 3.4 then implies that

$$\log\|\Lambda^{r_1(D)}f\|_{\mathfrak{p}_j} \leqq -Q_{\xi_j}\big(r_1(D)\big)\log N_{\mathfrak{p}_j}^{a_j}.$$

We then obtain (see §2.1)

$$\frac{\hat{\mu}(\overline{F}_D)}{D} \leqq \sup_{i\in I} h(P_i) + \frac{1}{2D}\log r_1(D) - \frac{1}{[K:\mathbb{Q}]}\sum_{j\in J}\frac{Q_{\xi_j}\big(r_1(D)\big)}{Dr_1(D)}\log N_{\mathfrak{p}_j}^{a_j},$$

which leads to a contradiction. Thus the evaluation homomorphism $F_{D,K} \to \bigoplus_{i \in I} P_i^* \mathcal{L}^{\otimes D}$ is not injective. In other words, there exists a homogeneous polynomial of degree D which is not identically zero on X but vanishes on each P_i.

3.4. Applications. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and ξ be a rational point of $\mathscr{X}_{\mathbb{F}_\mathfrak{p}}$. Recall (see Notation 15) that $\mathcal{O}_\xi$ denotes the local ring of $\mathscr{X}$ at ξ, $\mathfrak{m}_\xi$ denotes its maximal ideal, and the local Hilbert–Samuel function of ξ is defined as

$$H_\xi(k) := \mathrm{rk}_{\mathbb{F}_\mathfrak{p}}\big((\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^k/(\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi)^{k+1}\big).$$

In some particular cases, the local Hilbert–Samuel function of ξ can be explicitly estimated.

(i) If ξ is regular (i.e., the local ring $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$ is regular), then one has $H_\xi(k) = \binom{k+d-1}{d-1}$ for any $k \geqq 0$.

(ii) Assume that the local ring $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$ is one-dimensional and Cohen–Macaulay (that is, $\mathfrak{m}_\xi/\mathfrak{p}\mathcal{O}_\xi$ contains a non zero-divisor of $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$), then by [21], Theorem 1.9, one has $H_\xi(k) \leqq \mu_\xi$ for any integer $k \geqq 0$, where μ_ξ denotes the multiplicity of the local ring $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$. Moreover, if $k \geqq \mu_\xi - 1$, then one has $H_\xi(k) = \mu_\xi$ (see [19], Theorem 2).

Proposition 3.5. *Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$, ξ be a rational point of $\mathscr{X}_{\mathbb{F}_\mathfrak{p}}$, and r be an integer, $r \geqq 1$.*

(i) *If the $\mathbb{F}_\mathfrak{p}$-point ξ is regular, then* (*see Notation* 15 *for the definition of Q_ξ*)

$$Q_\xi(r) > (d!)^{\frac{1}{d}} \frac{d}{d+1} r^{1+\frac{1}{d}} - \frac{d+3}{2d+2} dr. \tag{13}$$

(ii) *If $d = 1$ and ξ is Cohen–Macaulay, then*

$$Q_\xi(r) \geqq \frac{r^2}{2\mu_\xi} - \frac{r}{2\mu_\xi}. \tag{14}$$

Proof. Let U_ξ be the partial sum function of H_ξ. Namely,

$$U_\xi(k) := H_\xi(0) + \cdots + H_\xi(k).$$

One has

$$Q_\xi\big(U_\xi(k)\big) = \sum_{j=0}^{k} jH_\xi(j).$$

Moreover, if $r \in \big(U_\xi(k-1), U_\xi(k)\big]$, then one has $Q_\xi\big(U_\xi(k-1)\big) \leqq Q_\xi(r) \leqq Q_\xi\big(U_\xi(k)\big)$.

(i) In the case where ξ is regular, one has

$$U_\xi(k) = \sum_{j=0}^{k} \binom{j+d-1}{d-1} = \binom{k+d}{d}. \tag{15}$$

Therefore

$$Q_\xi\big(U_\xi(k)\big) = \sum_{j=0}^{k} jH_\xi(j) = \sum_{j=0}^{k} j\binom{j+d-1}{d-1} = \sum_{j=0}^{k} d\binom{j+d-1}{d} = d\binom{k+d}{d+1}.$$

Let r be an integer in $\big(U_\xi(k-1), U_\xi(k)\big]$. One has

$$\begin{aligned} Q_\xi(r) &= Q_\xi\big(U_\xi(k-1)\big) + k\big(r - U_\xi(k-1)\big) \\ &= kr + d\binom{k+d-1}{d+1} - k\binom{k+d-1}{d} = kr - \binom{k+d}{d+1} \\ &= kr - \frac{k+d}{d+1}U_\xi(k-1) > \frac{d}{d+1}(k-1)r, \end{aligned} \tag{16}$$

where in the last inequality, we have used the estimate $U_\xi(k-1) < r$. Note that (see §2.8)

$$r \leqq U_\xi(k) = \binom{k+d}{d} \leqq \frac{\big(k + (d+1)/2\big)^d}{d!}$$

implies

$$k \geqq (rd!)^{\frac{1}{d}} - (d+1)/2. \tag{17}$$

Combining with (16), we obtain that (13) holds.

(ii) Assume that $d = 1$ and $\mathcal{O}_\xi/\mathfrak{p}\mathcal{O}_\xi$ contains a non zero-divisor, then one has $1 \leqq H_\xi(k) \leqq \mu_\xi$ for any integer $k \geqq 1$. Let $(a_k)_{k\geqq 1}$ be the increasing sequence of non-negative integers such that the integer 0 appears exactly one time, and other integers appear exactly μ_ξ times. Note that one has $q_\xi(k) \geqq a_k$ for any $k \in \mathbb{N}\setminus\{0\}$. Hence

$$\begin{aligned} Q_\xi(r) &= \sum_{k=1}^{r} q_\xi(k) \geqq \sum_{k=1}^{r} a_k = \frac{\mu_\xi}{2}A(A+1) + (A+1)(r-1-\mu_\xi A) \\ &= (A+1)(r-1) - \frac{\mu_\xi}{2}A(A+1) = (A+1)(r-1-\mu_\xi A/2), \end{aligned}$$

where $A = \left\lfloor \frac{r-1}{\mu_\xi} \right\rfloor$. Using the fact that

$$\frac{r-1}{\mu_\xi} - \frac{\mu_\xi - 1}{\mu_\xi} \leqq A \leqq \frac{r-1}{\mu_\xi},$$

we obtain

$$Q_\xi(r) \geqq \frac{r}{\mu_\xi}\left(r - 1 - \frac{r-1}{2}\right) \geqq \frac{r^2}{2\mu_\xi} - \frac{r}{2\mu_\xi}. \quad \square$$

Remark 3.6. When $d = 1$, the estimate (13) is less precise than (14). The reason is that in the last inequality of (16), we have used the estimate $U_\xi(k-1) < r$ but not the more precise one $U_\xi(k-1) \leqq r-1$.

Corollary 3.7. *Let $(\mathfrak{p}_j)_{j\in J}$ be a finite family of maximal ideals of $\mathcal{O}_K$ and $\varepsilon > 0$. For any $j \in J$, let $a_j \in \mathbb{N}\setminus\{0\}$, $\xi_j \in \mathscr{X}(\mathbb{F}_{\mathfrak{p}_j})$ be a regular rational point of $\mathscr{X}_{\mathbb{F}_{\mathfrak{p}_j}}$ and $\eta_j \in \mathscr{X}(A_{\mathfrak{p}_j}^{(a_j)})$ whose reduction modulo $\mathfrak{p}_j$ is ξ_j. If*

$$\sum_{j\in J}\log N_{\mathfrak{p}_j}^{a_j} \geqq (1+\varepsilon)\big(\log B + [K:\mathbb{Q}]\log(n+1)\big)\delta^{-\frac{1}{d}}\frac{d+1}{d}, \tag{18}$$

then, for any integer D such that

$$D > (\varepsilon^{-1}+1)\big(\delta^{-\frac{1}{d}}(d+3)/2 + \delta - 2\big), \tag{19}$$

there exists a hypersurface of degree D of $\mathbb{P}^n_K$ not containing X which contains $\bigcap_{j\in J} S(X;B,\eta_j)$.

Proof. Assume that such hypersurface does not exist. By Theorem 3.1, one has

$$\frac{\log B}{[K:\mathbb{Q}]} \geqq \frac{\hat{\mu}(\overline{F}_D)}{D} - \frac{\log r_1(D)}{2D} + \sum_{j\in J}\frac{Q_{\xi_j}\big(r_1(D)\big)}{Dr_1(D)}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}. \tag{20}$$

Moreover, since ξ_j is regular, Proposition 3.5 shows that

$$Q_{\xi_j}\big(r_1(D)\big) \geqq (d!)^{\frac{1}{d}}\frac{d}{d+1}r_1(D)^{1+\frac{1}{d}} - \frac{d+3}{2d+2}dr_1(D).$$

Hence

$$\frac{Q_{\xi_j}\big(r_1(D)\big)}{Dr_1(D)} \geqq (d!)^{\frac{1}{d}}\frac{d}{d+1}\frac{r_1(D)^{\frac{1}{d}}}{D} - \frac{(d+3)d}{(2d+2)D}.$$

By a result of Sombra recalled in §2.2, one has (for $D \geqq \delta - 2$)

$$r_1(D) \geqq \binom{D+d+1}{d+1} - \binom{D-\delta+d+1}{d+1} = \sum_{j=1}^{\delta}\binom{D-\delta+d+j}{d} \geqq \frac{\delta(D-\delta+2)^d}{d!}.$$

Combining with (5) and the trivial estimate $r_1(D) \leqq (n+1)^D$, (20) implies

$$\frac{\log B}{[K:\mathbb{Q}]} \geqq -\frac{1}{2}\log(n+1) - \frac{1}{2}\log(n+1) + \left(\delta^{\frac{1}{d}}\frac{d}{d+1}\frac{D-\delta+2}{D} - \frac{(d+3)d}{(2d+2)D}\right)\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}.$$

Or equivalently

$$\left(\delta^{\frac{1}{d}}\frac{d}{d+1}\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]} - \frac{\log B}{[K:\mathbb{Q}]} - \log(n+1)\right)D \leqq \sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}\left(\delta^{\frac{1}{d}}\frac{d}{d+1}(\delta-2) + \frac{d+3}{2d+2}d\right).$$

By the hypothesis (18), the left side is not less than

$$\frac{\varepsilon}{1+\varepsilon}\delta^{\frac{1}{d}}\frac{d}{d+1}\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}D,$$

which implies that

$$D \leqq (\varepsilon^{-1}+1)\big(\delta^{-\frac{1}{d}}(d+3)/2+\delta-2\big).$$

This contradicts (19). □

Corollary 3.8. *Assume that $\mathscr{X}$ is Cohen–Macaulay and $d=1$. Let $(\mathfrak{p}_j)_{j\in J}$ be a finite family of maximal ideals of $\mathcal{O}_K$ and $\varepsilon>0$. For any $j\in J$, let $a_j\in\mathbb{N}\setminus\{0\}$, $\xi_j\in\mathscr{X}(\mathbb{F}_{\mathfrak{p}_j})$ and $\eta_j\in\mathscr{X}(A_{\mathfrak{p}_j}^{(a_j)})$ whose reduction modulo $\mathfrak{p}_j$ is ξ_j. If*

$$\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{\mu_{\xi_j}} \geqq (1+\varepsilon)\frac{2}{\delta}\big(\log B+[K:\mathbb{Q}]\log(n+1)\big), \tag{21}$$

then for any integer D such that

$$D>(1+\varepsilon^{-1})(\delta-2+\delta^{-1}), \tag{22}$$

there exists a hypersurface of degree D of $\mathbb{P}^n$ not containing X which contains $\bigcap_{j\in J}S(X;B,\eta_j)$.

Proof. The proof is quite similar to that of Corollary 3.7. By Proposition 3.5, one has the estimate

$$\frac{Q_{\xi_j}(r_1(D))}{Dr_1(D)} \geqq \frac{r_1(D)}{2\mu_{\xi_j}D}-\frac{1}{2\mu_{\xi_j}D}.$$

Assume that the hypersurface does not exist. By Theorem 3.1, one has

$$\frac{\log B}{[K:\mathbb{Q}]}+\log(n+1)\geqq\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}\left(\frac{\delta}{2\mu_{\xi_j}}\cdot\frac{D-\delta+2}{D}-\frac{1}{2\mu_{\xi_j}D}\right),$$

or equivalently

$$D\left(\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}\frac{\delta}{2\mu_{\xi_j}}-\frac{\log B}{[K:\mathbb{Q}]}-\log(n+1)\right)\leqq\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]\mu_{\xi_j}}\left(\frac{\delta(\delta-2)}{2}+\frac{1}{2}\right).$$

By the assumption (21), one obtains

$$D\frac{\varepsilon}{1+\varepsilon}\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]}\frac{\delta}{2\mu_{\xi_j}}\leqq\sum_{j\in J}\frac{\log N_{\mathfrak{p}_j}^{a_j}}{[K:\mathbb{Q}]\mu_{\xi_j}}\cdot\frac{\delta^2-2\delta+1}{2},$$
$$D\leqq(1+\varepsilon^{-1})(\delta-2+\delta^{-1}).$$

The last formula leads to a contradiction. □

4. Covering rational points by hypersurfaces

In this section, we explain how to suitably cover $S_1(X;B)$ and $S(X;B)$ by hypersurfaces of low degree. If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_K$ and ξ is a singular rational point of $\mathscr{X}(\mathbb{F}_\mathfrak{p})$, there seems to be no general explicit estimate of the local Hilbert–Samuel function Q_ξ.[2)] The idea of Heath-Brown is to consider only regular points. The difficulty then comes from the fact that the reduction modulo $\mathfrak{p}$ of a regular point P in $X(K)$ is not necessarily regular. Hence we need to estimate the "smallest" maximal ideal $\mathfrak{p}$ such that P specializes to a regular point modulo $\mathfrak{p}$. This has been obtained in [16] and in [6] by using the Jacobian criterion. Here we prove that the singular loci of fibres of $\mathscr{X}$ are actually contained in a divisor whose degree and height are controlled.

Lemma 4.1. *Let $N_0 > 0$ be a real number and r the integral part of the number*

$$\frac{(n-d)(\delta-1)\log B + \big((n-d)h_{\bar{\mathcal{L}}}(X) + C_3\big)[K:\mathbb{Q}]}{\log N_0} + 1, \tag{23}$$

where the constant C_3 is defined in Notation 19. If $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are r distinct finite places of K such that $N_{\mathfrak{p}_i} \geqq N_0$ for any i, then

$$S_1(X;B) = \bigcup_{i=1}^{r} S_1(X;B,\mathfrak{p}_i).$$

Proof. With the notation of §2.7, if P is a rational point in $S_1(X;B)$ which does not lie in any $S_1(X;B,\mathfrak{p}_i)$, then one has $\alpha_{\mathfrak{p}_i}(P) \geqq 1$ for any $i = 1, \dots, r$. Hence, by §2.7, one has

$$r \leqq \sum_{N_\mathfrak{p} \geqq N_0} \alpha_\mathfrak{p}(P) \leqq \frac{(n-d)(\delta-1)h(P) + (n-d)h_{\bar{\mathcal{L}}}(X) + C_3}{(\log N_0)/[K:\mathbb{Q}]},$$

which leads to a contradiction. □

Theorem 4.2. *Let $\varepsilon > 0$ be an arbitrary positive real number. Let D be an integer such that*

$$D > \max\big\{(\varepsilon^{-1}+1)\big(\delta^{-\frac{1}{d}}(d+3)/2 + \delta - 2\big), 2(n-d)(\delta-1) + d + 4\big\}.$$

There exists an explicitly computable constant $C(\varepsilon,\delta,n,d,K)$ such that, for any $B \geqq e^\varepsilon$, the set $S_1(X;B)$ is covered by not more than $C(\varepsilon,\delta,n,d,K)B^{(1+\varepsilon)\delta^{-\frac{1}{d}}(d+1)}$ hypersurfaces of degree D not containing X.

Proof. In the first stage, we assume that

$$h_{\bar{\mathcal{L}}}(X) \leqq \frac{(2d+2)^{d+1}}{d!}\delta\left[\frac{\log B}{[K:\mathbb{Q}]} + \frac{3}{2}\log(n+1) + 2^d\right].$$

2) In the case where $\mathscr{X}$ is Cohen–Macaulay, there are explicit estimates (see for example [27]). However, they are far from optimal.

Let $M \in \mathbb{N} \setminus \{0\}$ be the least common multiple[3)] of $1, 2, \ldots, [K:\mathbb{Q}]$. Let $N_0 \in (0, +\infty)$ be such that

$$\log N_0 = (1+\varepsilon)\delta^{-\frac{1}{d}} \frac{d+1}{dM} \big(\log B + [K:\mathbb{Q}] \log(n+1)\big).$$

Let r be the natural number as in Lemma 4.1. Note that one has

$$r \leqq \frac{A_1 \log B + A_2}{\log N_0} + 1,$$

where

$$A_1 = (n-d)(\delta - 1) + \frac{(2d+2)^{d+1}}{d!}(n-d)\delta,$$

$$A_2 = [K:\mathbb{Q}]\left(C_3 + \frac{(2d+2)^{d+1}}{d!}\delta\left(\frac{3}{2}\log(n+1) + 2^d\right)\right).$$

Recall that the constant C_3 is defined in Notation 19. Since we have assumed that $\log B \geqq \varepsilon$, the value of r is bounded from above by a constant A_3 which depends only on M, ε, n, d and δ:

$$A_3 := M \frac{A_1 + \varepsilon^{-1} A_2}{(1+\varepsilon)\delta^{-\frac{1}{d}}(d+1)/d} + 1.$$

By Bertrand's postulate, there exist r distinct prime numbers $p_1, \ldots, p_r$ such that $N_0 \leqq p_i \leqq 2^i N_0$ for any $i \in \{1, \ldots, r\}$. We choose, for each i, a maximal ideal $\mathfrak{p}_i$ of $\mathcal{O}_K$ lying over p_i. By Lemma 4.1, one has $S_1(X;B) = \bigcup_{i=1}^{r} S_1(X;B,\mathfrak{p}_i)$. Note that, for any i, $N_{\mathfrak{p}_i}$ is a power of p_i whose exponent f_i divides M (since $f_i \leqq [K:\mathbb{Q}]$). Let $a_i = M/f_i$.

Let ξ be an arbitrary regular $\mathbb{F}_{\mathfrak{p}_i}$-point of $\mathscr{X}_{\mathbb{F}_{\mathfrak{p}_i}}$. By Corollary 3.7, we obtain that, for any $\eta \in \mathscr{X}(A_{\mathfrak{p}_i}^{(a_i)})$ whose reduction modulo $\mathfrak{p}_i$ is ξ, $S(X;B,\eta)$ is contained in a hypersurface of degree D not containing X. Note that there exists at most $N_{\mathfrak{p}_i}^{(a_i-1)d}$ points in $\mathscr{X}(A_{\mathfrak{p}_i}^{(a_i)})$ (see Notation 15) whose reduction modulo $\mathfrak{p}_i$ equals ξ_i and the cardinal of $\mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})$ does not exceed $\delta d N_{\mathfrak{p}_i}^d$. Hence $S_1(X;B,\mathfrak{p}_i)$ is covered by at most

$$\delta d N_{\mathfrak{p}_i}^{a_i d} = \delta d p_i^{a_i f_i d} = \delta d p_i^{Md} \leqq 2^{iMd} \delta d N_0^{Md} \tag{24}$$

hypersurfaces of degree D not containing X. Therefore, $S_1(X;B)$ is covered by at most

$$\delta d N_0^{Md} \sum_{i=1}^{r} 2^{iMd} \leqq \delta d r 2^{rMd} \big((n+1)^{[K:\mathbb{Q}]} B\big)^{(1+\varepsilon)\delta^{-\frac{1}{d}}(d+1)}$$

---

3) One has $2^{[K:\mathbb{Q}]} \leqq M \leqq [K:\mathbb{Q}]^{\pi([K:\mathbb{Q}])}$. See [28], p. 30, for a proof.

such hypersurfaces. So the theorem is proved with the constant

$$C(\varepsilon,\delta,n,d,K) = \delta d A_3 2^{A_3 M d}(n+1)^{(1+\varepsilon)\delta^{-\frac{1}{d}}(d+1)[K:\mathbb{Q}]}. \tag{25}$$

Now we treat the case where

$$\frac{\log B}{[K:\mathbb{Q}]} < \frac{d!}{\delta(2d+2)^{d+1}} h_{\bar{\mathcal{L}}}(X) - \frac{3}{2}\log(n+1) - 2^d.$$

By §2.1, inequality (2) and §2.3, we obtain that the set $S(X;B)$ is contained in a hypersurface of degree D in $\mathbb{P}^n$ which does not contain X. The theorem is also true in this case. □

Corollary 4.3. *With the notation of Theorem* 4.2, *assume that* $d = 1$. *For any positive real number* $B \geqq e^{\varepsilon}$, *one has*

$$\#S(X;B) \leqq \big(C(\varepsilon,\delta,n,d,K)+1\big)\delta D B^{(1+\varepsilon)2/\delta}. \tag{26}$$

Proof. By Bézout's theorem, the intersection of each hypersurface in the conclusion of Theorem 4.2 and X contains at most δD rational points. Hence the corollary follows from Theorem 4.2 (see also §2.6). □

Remark 4.4. (i) Observe that one has $A_1 \ll_{n,d} \delta$ and $A_2 \ll_{n,d} \delta$ and hence $A_3 \ll_{n,d,\varepsilon} \delta^{1+\frac{1}{d}}$. Therefore, one has

$$\log C(\varepsilon,\delta,n,d,K) \ll_{n,d,K,\varepsilon} \delta^{1+\frac{1}{d}}.$$

Moreover, the constant $C(\varepsilon,\delta,n,d,K)$ does not depend on the discriminant of K (but on the degree of K over $\mathbb{Q}$).

(ii) The original strategy of Heath-Brown corresponds essentially to the case where $a_i = 1$ for any i. By taking a larger N_0, his strategy also allows to obtain an explicit upper bound with the same exponent. However, the choice of maximal ideals forces us to use Bertrand's postulate for the number field K where the discriminant of K is inevitable, according to a counter-example of Heath-Brown that Browning has communicated to me.

5. The case of a plane curve

In this section, we assume that X is an integral plane curve (that is, $d = 1$ and $n = 2$). Note that the model $\mathscr{X}$ of X is Cohen–Macaulay since it is a subscheme of $\mathbb{P}^2_{\mathcal{O}_K}$ defined by one homogeneous equation. We obtain, for "small" value of B, an explicit estimate of $\#S(X;B)$.

Theorem 5.1. *Assume that* $d = 1$ *and* $n = 2$. *Let* $D = \lfloor 2(\delta - 2 + \delta^{-1})\rfloor + 1$. *Then, for any real number* $B \in (e, e^{\delta^2})$, *one has*

$$\#S(X;B) \leqq C_4(K,B)\delta D, \tag{27}$$

where

$$C_4(K,B) = (\sqrt{\log B}+1)\alpha(K)^{2\sqrt{\log B}+2}\exp\left[8\frac{\log B+[K:\mathbb{Q}]\log 2}{\sqrt{\log B}}\right]$$
$$+ (\log B)^{\sqrt{\log B}+1}\left(\frac{\delta-1}{\delta-\sqrt{\log B}}\right)^{\sqrt{\log B}+1},$$

$\alpha(K)$ *being the constant introduced in Notation* 20.

Proof. Let $N_0 \in (0,+\infty)$ be such that

$$\log N_0 = 4\frac{\log B+[K:\mathbb{Q}]\log 2}{\sqrt{\log B}}.$$

Let $r = \lceil\sqrt{\log B}\rceil$. Choose a family $(\mathfrak{p}_i)_{i=1}^r$ of distinct maximal ideals of $\mathcal{O}_K$ such that $N_0 \leqq N_{\mathfrak{p}_i} \leqq \alpha(K)^i N_0$, where $\alpha(K)$ is the constant of Bertrand's postulate introduced in Notation 20. For any $(\xi_i)_{i=1}^r \in \prod_{i=1}^r \mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})$, let

$$S\big(X;B,(\xi_i)_{i=1}^r\big) := \bigcap_{i=1}^r S(X;B,\xi_i).$$

Note that one has

$$S(X;B) = \left[\bigcup_{i=1}^r \bigcup_{\substack{\xi\in\mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})\\ \mu_\xi\leqq\delta/\sqrt{\log B}}} S(X;B,\xi)\right] \cup \bigcup_{\substack{(\xi_i)_{i=1}^r\in\prod_{i=1}^r\mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})\\ \mu_{\xi_i}>\delta/\sqrt{\log B}}} S\big(X;B,(\xi_i)_{i=1}^r\big). \tag{28}$$

Let $\mathfrak{p}\in\{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$. Assume that ξ is an $\mathbb{F}_\mathfrak{p}$-point of $\mathscr{X}_{\mathbb{F}_\mathfrak{p}}$ whose multiplicity μ_ξ satisfies $\mu_\xi \leqq \delta/\sqrt{\log B}$. One has

$$\frac{\log N_\mathfrak{p}}{\mu_\xi} \geqq \frac{\log N_0}{\delta/\sqrt{\log B}} = \frac{4}{\delta}(\log B+[K:\mathbb{Q}]\log 2).$$

By Corollary 3.8 (the case where $\varepsilon = 1$ and $|J| = 1$), there exists a hypersurface of degree D not containing X which contains $S(X;B,\xi)$. Note that the cardinal of the set

$$\bigcup_{i=1}^r\{\xi\in\mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})\,|\,\mu_\xi\leqq\delta/\sqrt{\log B}\}$$

does not exceed

$$\sum_{i=1}^r \#\mathbb{P}^2(\mathbb{F}_{\mathfrak{p}_i}) \leqq \sum_{i=1}^r N_{\mathfrak{p}_i}^2 \leqq r\alpha(K)^{2r}N_0^2. \tag{29}$$

Let $i \in \{1, \dots, r\}$. By Bézout's theorem (see [15], 5–22, p. 115), one has

$$\sum_{\xi \in \mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})} \mu_\xi(\mu_\xi - 1) \leqq \delta(\delta - 1). \tag{30}$$

Hence

$$\#\{\xi \in \mathscr{X}(\mathbb{F}_{\mathfrak{p}_i}) \mid \mu_\xi > \delta/\sqrt{\log B}\} \leqq (\log B)\frac{\delta - 1}{\delta - \sqrt{\log B}},$$

which implies that the number of r-tubes $(\xi_i)_{i=1}^r \in \prod_{i=1}^r \mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})$ with $\mu_{\xi_i} \geqq \delta/\sqrt{\log B}$ does not exceed

$$(\log B)^r \left(\frac{\delta - 1}{\delta - \sqrt{\log B}}\right)^r. \tag{31}$$

Note that the inequality (30) also implies that $\mu_\xi \leqq \delta$ for any $\xi \in \mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})$. Therefore, if $(\xi_i)_{i=1}^r$ is an element in $\prod_{i=1}^r \mathscr{X}(\mathbb{F}_{\mathfrak{p}_i})$, then one has

$$\sum_{i=1}^r \frac{\log N_{\mathfrak{p}_i}}{\mu_{\xi_i}} \geqq r\frac{\log N_0}{\delta} \geqq \frac{4}{\delta}(\log B + [K : \mathbb{Q}] \log 2),$$

where the second inequality comes from the estimate $r \geqq \sqrt{\log B}$. Still by Corollary 3.8, one obtains that $S\big(X; B, (\xi_i)_{i=1}^r\big)$ is contained in a hypersurface of degree D not containing X.

By (28), (29) and (31), the set $S(X; B)$ is contained in a family of hypersurfaces of degree D not containing X, and the number of the hypersurfaces in the family does not exceed

$$r\alpha(K)^{2r} N_0^2 + (\log B)^r \left(\frac{\delta - 1}{\delta - \sqrt{\log B}}\right)^r \leqq C_4(K, B).$$

By Bézout's theorem the intersection of each hypersurface with X contains at most δD rational points. Therefore, we obtain

$$\#S(X; B) \leqq C_4(K, B)\delta D. \quad \square$$

Remark 5.2. The logarithmic of the first summand of $C_4(K,\delta)$ is

$$8\frac{\log\delta + [K : \mathbb{Q}] \log 2}{\sqrt{\log\delta}} + (2\sqrt{\log\delta} + 2) \log \alpha(K) + \log(\sqrt{\log\delta} + 1) \ll \sqrt{\log\delta} \quad (\delta \to \infty),$$

while the logarithmic of the second summand is

$$(\sqrt{\log\delta} + 1)\left(\log\log\delta + \log\left(\frac{\delta - 1}{\delta - \sqrt{\log\delta}}\right)\right) \ll \sqrt{\log\delta} \cdot \log\log\delta \quad (\delta \to \infty).$$

Hence there exists a constant M_K which only depends on K such that

$$C_4(K,\delta) \leqq M_K^{\sqrt{\log\delta}\cdot\log\log\delta+\sqrt{\log\delta}} \ll_K \delta^\varepsilon$$

for any $\varepsilon > 0$.

Corollary 5.2. *Assume that X is an integral plane curve of degree δ. Then, for any $\varepsilon > 0$, one has*

$$\#S(X;\delta) \ll_K \delta^{2+\varepsilon}.$$

Acknowledgment. Inspired by a talk of P. Salberger at Göttingen University, J.-B. Bost suggested me to use the slope method to study the density of rational points and shared with me his personal notes. S. David and P. Philippon kindly explained to me their work on the lower bound of arithmetic Hilbert–Samuel function. During the preparation of this work, I benefited from discussions with D. Bertrand, J.-B. Bost, R. De la Bretèche, T. Browning, A. Chambert-Loir, M. Chardin, D. R. Heath-Brown, H. A. Helfgott, H. Randriambololona, P. Salberger, C. Soulé and B. Teissier and received many helpful suggestions. I would like to express my deep gratitude to them all. Part of this work has been written during my visit to the *Institut des Hautes Études Scientifiques*. I would like to thank the institute for hospitalities. Finally I am grateful to the referees for their valuable remarks.

References

[1] *E. Bombieri* and *J. Pila*, The number of integral points on arcs and ovals, Duke Math. J. **59** (1989), no. 2, 337–357.

[2] *J.-B. Bost*, Périodes et isogénies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz), Séminaire Bourbaki, Vol. 1994/1995, Astérisque **237** (1996), Exp. No. 795, 4, 115–161.

[3] *J.-B. Bost*, Algebraic leaves of algebraic foliations over number fields, Publ. Math. Inst. Hautes Ét. Sci. **93** (2001), 161–221.

[4] *J.-B. Bost*, Evaluation maps, slopes, and algebraicity criteria, Proc. Internat. Congr. Math. (Madrid 2006) **II**, Euro. Math. Soc. (2007), 537–562.

[5] *N. Bourbaki*, Éléments de mathématique, Algèbre, Chapitres 1 à 3, Hermann, Paris 1970.

[6] *N. Broberg*, A note on a paper by R. Heath-Brown: "The density of rational points on curves and surfaces" [Ann. Math. (2) **155** (2002), no. 2, 553–595], J. reine angew. Math. **571** (2004), 159–178.

[7] *T. D. Browning* and *D. R. Heath-Brown*, Counting rational points on hypersurfaces, J. reine angew. Math. **584** (2005), 83–115.

[8] *T. D. Browning* and *D. R. Heath-Brown*, The density of rational points on non-singular hypersurfaces, I, Bull. Lond. Math. Soc. **38** (2006), no. 3, 401–410.

[9] *T. D. Browning* and *D. R. Heath-Brown*, The density of rational points on non-singular hypersurfaces, II, Proc. Lond. Math. Soc. (3) **93** (2006), no. 2, 273–303.

[10] *T. D. Browning*, *D. R. Heath-Brown* and *P. Salberger*, Counting rational points on algebraic varieties, Duke Math. J. **132** (2006), no. 3, 545–578.

[11] *M. Chardin*, Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique, Bull. Soc. Math. France **117** (1989), no. 3, 305–318.

[12] *H. Chen*, Explicit uniform estimation of rational points I, Estimation of heights, J. reine angew. Math., to appear.

[13] *Colliot-Thélène* et al., Report on the Workshop "Rational and integral points on higher dimensional varieties", 2002.

[14] *J. Ellenberg* and *A. Venkatesh*, On uniform bounds for rational points on nonrational curves, Int. Math. Res. Not. (2005), no. 35, 2163–2181.

[15] *W. Fulton*, Algebraic curves, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Math. Lect. Notes Ser., W. A. Benjamin, Inc., New York–Amsterdam 1969.
[16] *D. R. Heath-Brown*, The density of rational points on curves and surfaces, Ann. Math. (2) **155** (2002), no. 2, 553–595.
[17] *H. A. Helfgott*, Power-free values, large deviations and integer points on irrational curves, J. Th. Nombres Bordeaux **19** (2007), no. 2, 433–472.
[18] *H. A. Helfgott* and *A. Venkatesh*, Integral points on elliptic curves and 3-torsion in class groups, J. Amer. Math. Soc. **19** (2006), no. 3, 527–550.
[19] *D. Kirby*, The reduction number of a one-dimensional local ring, J. Lond. Math. Soc. (2) **10** (1975), no. 4, 471–481.
[20] *J. C. Lagarias* and *A. M. Odlyzko*, Effective versions of the Chebotarev density theorem, in: Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Durham 1975), Academic Press, London (1977), 409–464.
[21] *J. Lipman*, Stable ideals and Arf rings, Amer. J. Math. **93** (1971), 649–685.
[22] *J. Pila*, Density of integral and rational points on varieties, Columbia University Number Theory Seminar (New York 1992) Astérisque **228** (1995), 4, 183–187.
[23] *P. Salberger*, On the density of rational and integral points on algebraic varieties, J. reine angew. Math. **606** (2007), 123–147.
[24] *P. Salberger*, Rational points of bounded height on projective surfaces, Math. Z. **258** (2008), 805–826.
[25] *J.-P. Serre*, Quelques applications du théorème de densité de Chebotarev, Publ. Math. Inst. Hautes Ét. Sci. **54** (1981), 323–401.
[26] *M. Sombra*, Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz, Algorithms for algebra (Eindhoven 1996), J. Pure Appl. Algebra **117/118** (1997), 565–599.
[27] *V. Srinivas* and *V. Trivedi*, On the Hilbert function of a Cohen–Macaulay local ring, J. Alg. Geom. **6** (1997), no. 4, 733–751.
[28] *G. Tenenbaum*, Introduction à la théorie analytique et probabiliste des nombres, 3rd ed., Collection Échelles, Éditions Belin, Paris 2008.

Institut de Mathématiques de Jussieu, Université Paris Diderot—Paris 7, France
e-mail: chenhuayi@math.jussieu.fr

Eingegangen 12. November 2009, in revidierter Fassung 17. Januar 2011