Symmetric Diophantine approximation over function fields

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op donderdag 3 december 2015
klokke 10:00 uur

door

Weidong ZHUANG
geboren te Jiangsu, China
in 1983

Samenstelling van de promotiecommissie:

Promotor: Prof. dr. P. Stevenhagen

Copromotor: Dr. J.-H. Evertse

Overige leden:

Prof. dr. F. Beukers (Universiteit Utrecht)
Prof. dr. Y. Bugeaud (Université Strasbourg)
Prof. dr. K. Győry (University of Debrecen)
Dr. R. de Jong
Prof. dr. B. de Smit (secretaris)
Prof. dr. A.W. van der Vaart (voorzitter)
Mw. prof. dr. J. T.-Y. Wang (Academia Sinica Taiwan)

This work was funded by the NWO vrije competitie EW 2011 project "Symmetric Diophantine Approximation" and was carried out at Universiteit Leiden.

To Yana and Zhida

Contents

Introduction

Roth's theorem gives an optimal solution to the problem how well a given algebraic number can be approximated by other algebraic numbers. A natural question is to ask how well two varying algebraic numbers can approximate each other. There is only one non-trivial result, proved by Evertse, but this is far from optimal. Its proof is based on a weak version of the abc-conjecture, which is a consequence of a generalization of Roth's Theorem, hence it is non-effective.

Let k be an algebraically closed field of characteristic 0. Over algebraic function fields of transcendence degree 1 over k there is a proved analogue of the abc-conjecture, i.e., the Mason-Stothers Theorem. This suggests that it should be possible to develop much stronger symmetric Diophantine approximation results over function fields. My research focuses mainly on this interesting problem.

To tackle this problem, one considers two cases: either the two algebraic functions that approximate each other are conjugate over the field of rational functions $k(t)$ or not.

The first case is strongly connected to the following problem: over the integers, two binary forms (i.e., homogeneous polynomials) $F, G \in \mathbb{Z}[X, Y]$ are called equivalent if $G(X, Y) = F(aX + bY, cX + dY)$ for some matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$. Two equivalent binary forms have the same discriminant. A binary form F is called *reduced* if its height $H(F)$ (maximum of the absolute values of its coefficients) is minimal among the heights of the binary forms in its equivalence class.

Conjecture. *The height $H(F)$ of a reduced binary form F of degree $n \geqslant 4$ and non-zero discriminant D has an upper bound of the form $c_1(n)|D|^{c_2(n)}$, where $c_1(n)$, $c_2(n)$ are numbers depending only on n.*

An analogous estimate for $n = 2$ and $n = 3$ follows from work of Lagrange, Gauss and Hermite. However, the general case is still open. There is only the following much weaker effective result from [11]:

Theorem (Evertse, Győry)**.** *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a reduced binary form of degree $n \geqslant 2$ and discriminant $D(F) \neq 0$. Then*

$$H(F) \leqslant \exp((c_1 n)^{c_2 n^4} |D|^{8n^3}),$$

where c_1, c_2 are effectively computable, absolute constants.

More generally, we may consider the ring of integers of an algebraic number field and even the ring of S-integers instead of $\mathbb{Z}$. A weak version of Evertse [9] implies the following:

Theorem (Evertse)**.** *Let $F \in \mathbb{Z}[X, Y]$ be a reduced binary form of degree $n > 1$ with splitting field L over $\mathbb{Q}$ and non-zero discriminant. Then*

$$H(F) \leqslant C^{ineff}(n, L)|D(F)|^{\frac{21}{n-1}}.$$

The constant here depends on n, L and is ineffective in the sense that it is not effectively computable from the method of proof. We call this result a 'semi-effective' upper bound since it is effective in terms of $D(F)$, but ineffective in terms of n and L.

We proved an analogue of the above conjecture over $k[t]$. Our main tools are an analogue of the geometry of numbers over function fields (see Thunder [24]) and Mason's theorem which is an analogue of the abc-conjecture over function fields.

We start with some notation.

Fix $K = k(t)$ where k is an algebraically closed field of characteristic 0 and t is transcendental over k. For $x \in k[t]$, define $|x|_\infty = e^{\deg(x)}$. For $f \in$

$k[t]\backslash\{0\}$, define $\nu_p(f)(p \in k)$ by $f = (t-p)^{\nu_p(f)}g$ where $g \in k[t]$ and $g(p) \neq 0$. We extend this to $k(t)$ by setting $\nu_p(0) := \infty$ and $\nu_p(\frac{f}{g}) = \nu_p(f) - \nu_p(g)$ for $f, g \in k[t], g \neq 0$. Define $|x|_\nu = e^{-\nu(x)}$ for $x \in K$. For a polynomial F with coefficients $a_0, \ldots, a_n$ in $k[t]$, define $H(F) := \max(|a_0|_\infty, \ldots, |a_n|_\infty)$. If a binary form F has a factorization $F(X,Y) = \prod_{i=1}^{m}(\alpha_i X + \beta_i Y)$ over $\overline{K}$, define its discriminant by $D(F) = \prod_{i<j}(\alpha_i\beta_j - \alpha_j\beta_i)^2$. For two binary forms

$$F(X,Y) = \prod_{i=1}^{m}(\alpha_i X + \beta_i Y),\ G(X,Y) = \prod_{j=1}^{n}(\gamma_j X + \delta_j Y),$$

we define their resultant by

$$R(F,G) = \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i\delta_j - \beta_i\gamma_j).$$

Let L be a finite extension of $K = k(t)$. We say an absolute value on $|\cdot|_\omega$ on L is an extension of $|\cdot|_\nu$ on K if $|x|_\omega = |x|_\nu^{[L_\omega:K_\nu]}$ for every $x \in K$. Here L_ω, K_ν are the completions of L, K at ω, ν respectively. Define

$$H^*(x_1, \ldots, x_n) = \Big(\prod_{\omega \in M_L} \max(1, |x_1|_\omega, \ldots, |x_n|_\omega)\Big)^{1/[L:K]} \text{ for } (x_1, \ldots, x_n) \in L^n,$$

and

$$H(F) = \max(|a_0|_\infty, \ldots, |a_m|_\infty) \text{ for } F = \sum_{i=0}^{m} a_i X^{m-i}Y^i \in k[t][X,Y].$$

For a ring R, we say that two binary forms $F, G \in R[X,Y]$ are $\mathrm{GL}\,(2,R)$-equivalent if there exists $u \in R^\times$ and $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL(2,R)$ such that $G = uF_U$, where $F_U(X,Y) = F(aX+bY, cX+dY)$. Later we will apply this definition to a polynomial ring $k[t]$ or a function field L.

We recall Mason's ABC-theorem for function fields.

Theorem (Mason)**.** *Let L be a finite extension of $K = k(t)$, g_L the genus of L and T a finite set of valuations of L. Let $\gamma_1, \gamma_2, \gamma_3$ be non-zero elements of L satisfying $\gamma_1 + \gamma_2 + \gamma_3 = 0$ and $\nu(\gamma_1) = \nu(\gamma_2) = \nu(\gamma_3)$ for every valuation $\nu \notin T$. Then either $\frac{\gamma_1}{\gamma_2} \in k$, which means $H^*(\frac{\gamma_1}{\gamma_2}) = 1$, or $H^*(\frac{\gamma_1}{\gamma_2}) \leqslant e^{(\#T+2g_L-2)/[L:K]}$.*

As a consequence we derived a non-trivial result, Theorem 5, on how well two algebraic functions that are conjugate over $k(t)$ can approximate each other. We will come back to this with more details in the next few pages.

To study how well two algebraic functions non-conjugate over $k(t)$ can approximate each other involves a study of two binary forms, and requires one to find a non-trivial lower bound for the resultant of two binary forms in terms of their heights. To obtain such a bound, we developed a generalization of Mason's theorem to more variables, based on work of Brownawell and Masser [6], J.T.-Y. Wang [25] and Zannier [26].

This dissertation is organized as follows.

Chapter 1 introduces some very standard notation and collects some results related to discriminants, resultants, valuations, heights and twisted heights.

In Chapter 2, we introduce Mason's ABC-theorem for function fields and give a generalization, which is a solid basis to build our effective results on.

In Chapter 3 we develop some geometry of numbers over the rational function field $k(t)$. The main result concerns the successive minima of a so-called S-convex symmetric body.

With the help of the results in Chapter 3, we develop in Chapter 4 a reduction theory for binary forms over the rational function field.

In Chapter 5, we first derive some consequences of the Riemann-Hurwitz formula, and by combining these with the results from Chapter 1 to 4 we prove the following effective result, which is analogous to the conjecture mentioned above. The only earlier work in this direction is due to Gaál [13]. His results are formulated differently, but they imply a similar result, with a larger upper bound in terms of $|D(F)|_\infty$ for binary forms F with $F(1,0) = 1$.

Theorem 1. *Let $F \in k[t][X,Y]$ be a binary form of degree $n \geqslant 4$ with non-zero discriminant. Then F is* $\mathrm{GL}\,(2,k[t])$*-equivalent to a binary form F^* such that*

$$H(F^*) \leqslant e^{(n^2+5n-6)}|D(F)|_\infty^{20+\frac{1}{n}}.$$

In Chapter 5, we in fact deduce a general version of Theorem 1, which deals with binary forms over localizations of $k[t]$ away from a finite set of elements of k.

In Chapter 6, we focus on the finiteness of the number of equivalence classes of binary forms of given discriminant and show the following

Theorem 2. *Given $n \in \mathbb{Z}, n \geqslant 4$, non-zero $\delta \in k[t]$ and a finite extension L of K, there are only finitely many* $\mathrm{GL}(2, K)$*-equivalence classes of binary forms satisfying*

$$\begin{cases} F \in k[t][X, Y], D(F) \in \delta k^{\times}, \\ F \text{ has splitting field } L \text{ over } K, \\ \deg F = n, \\ F \text{ is not } \mathrm{GL}(2, L)\text{-equivalent to a binary form in } k[X, Y]. \end{cases}$$

Remark. *Theorem 2 becomes false if the last condition is replaced by F not being* $\mathrm{GL}(2, K)$*-equivalent to a binary form in $k[X, Y]$. A counterexample is given in Chapter 6.*

In Chapter 7, we effectively estimate the resultant of two binary forms from below in terms of their discriminants and heights. This is based on ideas of Evertse and Győry for number fields. They deduced the following:

Theorem (Evertse, Győry [12])**.** *Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $m \geqslant 3$ and $G \in \mathbb{Z}[X, Y]$ a binary form of degree $n \geqslant 3$ such that FG has splitting field L over $\mathbb{Q}$ and FG is square-free. Then*

$$|R(F, G)| \geqslant C^{ineff}(m, n, L)\big(|D(F)|^{n/(m-1)}|D(G)|^{m/(n-1)}\big)^{1/18}.$$

Theorem (Evertse [10])**.** *Let $m, n \geqslant 3$ and let (F, G) be a pair of binary forms with coefficients in $\mathbb{Z}$ such that $\deg F = m, \deg G = n$, FG is square-free and FG has splitting field L over $\mathbb{Q}$. Then there is an $U \in \mathrm{GL}(2, \mathbb{Z})$ such that*

$$|R(F, G)| \geqslant C^{\mathrm{ineff}}(m, n, L)\big(H(F_U)^n H(G_U)^m\big)^{1/718}.$$

The ineffectivity mainly comes from Schmidt's subspace theorem from Diophantine approximation. We apply a generalization of Mason's theorem (see Chapter 2) to obtain effective results as follows.

Theorem 3. *Assume $F, G \in k[t][X, Y]$ are two binary forms such that $\deg F = m \geqslant 3, \deg G = n \geqslant 3$, FG is square-free and splits in $k(t)$. Then*

$$|R(F,G)|_\infty \geqslant |D(F)|_\infty^{\frac{n}{17(m-1)}} |D(G)|_\infty^{\frac{m}{17(n-1)}}.$$

As a consequence of Theorem 1 and Theorem 3, we also show that

Theorem 4. *Let $m, n > 2$ and let F, G be binary forms in $k[t][X, Y]$ such that FG is square-free and splits in $k(t)$. Then there exists $U \in \mathrm{GL}\,(2, k[t])$ such that*

$$|R(F,G)|_\infty \geqslant c_1(m,n)^{-1} H(G_U)^{\frac{m}{717}} H(F_U)^{\frac{n}{717}},$$

where

$$c_1(m,n) = \exp\Big(- \tfrac{mn(4m+4n+11)}{717} \Big).$$

We actually prove a more general result where FG splits over a given arbitrary finite extension L of $k(t)$.

As an application, in Chapter 8 we prove a root separation result and a symmetric improvement of a Liouville-type inequality.

A result of Mahler states that for a polynomial $f(X) = a(X-\gamma_1)\dots(X-\gamma_n)$ with complex coefficients we have

$$\min_{1 \leqslant i < j \leqslant n} |\gamma_i - \gamma_j| \geqslant (n+1)^{-n-1} \frac{|D(f)|^{1/2}}{H(f)^{n-1}}.$$

In case that f has integer coefficients and non-zero discriminant this implies that

$$\min_{1 \leqslant i < j \leqslant n} |\gamma_i - \gamma_j| \geqslant (n+1)^{-n-1} H(f)^{1-n}. \qquad (*)$$

This inequality is proved by an elementary argument, similar to Liouville's inequality from Diophantine approximation on the approximation of algebraic numbers by rationals. Therefore, we call $(*)$ a Liouville-type inequality.

The root separation problem is to prove a similar inequality with instead of $1-n$ a larger exponent on $H(f)$. But this is still open. The only known case is, rather surprisingly, that when $n=3$ the exponent $1-n$ is best possible. The latest result [7] of Y. Bugeaud and A. Dujella shows that for $n \geqslant 4$ the exponent cannot be bigger than $-\frac{2n-1}{3}$.

We obtain an improvement of the exponent over the rational function field as follows.

Theorem 5. *Let $K=k(t)$ and $f \in K[X]$ be a polynomial of degree $n \geqslant 4$ with splitting field L. Write $f = a\prod_{i=1}^{n}(X-\gamma_i)$ with $a \in K^*$ and $\gamma_i \in L$. Fix an extension of $|\cdot|_\infty$ to L and denote this also by $|\cdot|_\infty$. Define*

$$\Delta_\infty(f) := \min_{1\leqslant i<j\leqslant n} \frac{|\gamma_i-\gamma_j|_\infty}{\max(1,|\gamma_i|_\infty)\max(1,|\gamma_j|_\infty)}.$$

Then

$$\Delta_\infty(f) \geqslant c_3(n)^{-1} H(f)^{-n+1+\frac{n}{40n+2}},$$

where

$$c_3(n) = \exp\left(\frac{(n-1)(n+6)}{20+1/n}\right).$$

We return to number fields. If we consider two algebraic numbers α, β not conjugate to each other, the problem becomes more general. A typical result is the following generalization of $(*)$: for T a finite set of valuations of $K(\alpha,\beta)$, we have

$$\left(\prod_{\omega\in T}|\alpha-\beta|_\omega\right)^{1/[L:K]} \geqslant \frac{1}{2}H^*(\alpha)^{-1}H^*(\beta)^{-1},$$

where $|\cdot|_\omega := |\cdot|_p^{[L_\omega:\mathbb{Q}_p]}$ if ω lies above $p \in \{\infty\}\cup\{\text{primes}\}$. The exponents of $H^*(\alpha)$ and $H^*(\beta)$ can be improved. A generalization of Roth's theorem by S. Lang implies that there is a constant $C>0$ depending on α and $K(\beta)$ such that

$$\left(\prod_{\omega\in T}|\alpha-\beta|_\omega\right)^{1/[L:K]} \geqslant CH^*(\beta)^{-(2/r)-\delta},$$

where $r = [K(\alpha, \beta) : K(\beta)] \geqslant 3$.

On the other hand, if we allow both α and β to vary, the problem gets more difficult. Evertse obtained the following improvement of Liouville-type inequality.

Theorem (Evertse)**.** *Let K be an algebraic number field and α, β distinct numbers algebraic over K. Let $L = K(\alpha, \beta)$. Suppose that*

$$[L : K] = [K(\alpha) : K][K(\beta) : K],\ [K(\alpha) : K] \geqslant 3,\ [K(\beta) : K] \geqslant 3.$$

Let T be a finite set of valuations of L above $\nu \in M_K$ such that

$$\varpi := \frac{1}{[L : K]} \sum_{\omega \in T} [L_\omega : K_\nu] < \frac{1}{3}.$$

Then

$$\prod_{\omega \in T} \frac{|\alpha - \beta|_\omega}{\max(1, |\alpha|_\omega) \max(1, |\beta|_\omega)} \geqslant C^{ineff}(L, T) \big(H^*(\alpha) H^*(\beta)\big)^{-1+\delta},$$

where $\delta = \frac{1-3\varpi}{718(1+3\varpi)}$.

Following the same idea, we give an analogous improvement of Liouville-type inequality over the rational function field, which is effective.

Let $K = k(t)$ and ξ, η be distinct and algebraic over K. Let $L = K(\xi, \eta)$ and T a finite set of valuations on L. Define

$$\Delta_T(\xi, \eta) := \left(\prod_{\omega \in T} \frac{|\xi - \eta|_\omega}{\max(1, |\xi|_\omega) \max(1, |\eta|_\omega)} \right)^{1/[L:K]}.$$

Then we have the following Liouville-type inequality

$$\Delta_T(\xi, \eta) \geqslant H^*(\xi)^{-1} H^*(\eta)^{-1}.$$

and the following effective improvement

Theorem 6. *Suppose ξ, η are algebraic over $K = k(t)$ with $[K(\xi) : K] \geqslant 3$ and $[K(\eta) : K] \geqslant 3$. Let $L = K(\xi, \eta)$ and assume*

$$[L : K] = [K(\xi) : K][K(\eta) : K].$$

Suppose that

$$\varpi := \frac{1}{[L:K]} \sum_{\substack{\omega|\infty \\ \omega\in T}} [L_\omega : K_\nu] < \frac{1}{3}.$$

Let g_1, g_2 be the genera of $K(\xi)$ and $K(\eta)$ respectively. Then

$$\Delta_T(\xi,\eta) \geqslant c_4(m,n,g_1,g_2,\varpi)^{-1}\big(H^*(\xi)H^*(\eta)\big)^{-1+\vartheta},$$

where $\vartheta = \frac{1-3\varpi}{717(1+3\varpi)}$ and

$$c_4(m,n,g_1,g_2,\varpi) = \exp\Big(\tfrac{426m+426n-1677+844g_1+844g_2}{717} + (m+n)(m+n-5)(1-\vartheta)\Big).$$

Last but not least, we remark that in this dissertation we prove more general versions of Theorem 3, 4, 5, 6 with multiple valuations, whilst Theorem 3 holds in a general function field of transcendent degree 1.