Generalization of the ABC-conjecture

29 mei, 1995

afstudeerwerk van
Nils Bruin

onder begeleiding van
prof. dr. R. Tijdeman,
dr. J.H. Evertse

aan de
Rijksuniversiteit Leiden

Contents

Introduction

The question whether there are integer solutions to the Fermat-equation

$$x^n + y^n = z^n$$

can be read as:"Can the sum of two perfect n-th powers be a perfect n-th power itself?" More generally, can three numbers both satisfy some additive relation and be of some special multiplicative type? In this way, the ABC-conjecture is a generalization of Fermat's Last Theorem. [1]

First, a measure of multiplicative simplicity of a number is defined. This measure is such that perfect n-th powers are indeed multiplicatively simple. The ABC-conjecture states that no triples A, B, C exist that are both multiplicatively simple and satisfy $A + B = C$.

One generalization that springs to mind is to conjecture the same for n variables instead of for 3 variables. This is the n-conjecture.

After a brief introduction in some special cases of the ABC-conjecture, following roughly [Lan90], this text formulates ABC in quite a general setting. This formulation is generalized to more variables. The rest of the text investigates relations between the ABC-conjecture and the n-conjecture.

Some bounds concerning the ABC-conjecture are proved in [ST86]. Although not treated in this text, it is important to know that ABC implies several important conjectures in Diophantine geometry. This line of thought is described in [Voj87], [Fre87] and in [Lan90]. Furthermore, quite some work has been done trying to challenge the ABC-conjecture, that is, finding multiplicatively simple triples A, B, C such that $A + B = C$. See [Nit93] for an approach using continued fractions and work of Herman te Riele for an approach using a lattice basis reduction algorithm.

[1] In the rest of this text, Fermat's Last Theorem is referred to as the Fermat Conjecture. This may seem inaccurate with respect to the recent result of Wiles, but the name Wiles's Theorem seems to do no justice to the work of, for example, Ribet, who displayed the connection between the Fermat Conjecture and the theorem Wiles has proved. The name Fermat's Last Theorem, although most generally used, suggests that Fermat did have a proof of his claim, for which no other indication exists but his own famous remark.

Chapter 1

ABC in Special Cases

1.1 Polynomial Case

In 1983, R.C. Mason proved a theorem for function fields. In this section we will formulate and prove this theorem for polynomials over $\mathbb{C}$.

First we recall a concept from elementary ideal theory. If R is a ring and $I \subset R$ is an ideal, then the radical ideal of I is defined by

$$\mathrm{Rad}(I) := \{r \in R : \text{there is an } e \in \{1, 2, \dots\} \text{ such that } r^e \in I\}.$$

It is easy to check that this is indeed an ideal.

Let $F(X) \in \mathbb{C}[X]$ be a polynomial. We write

$$F(X) = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_1 X + a_0,$$

where $a_i \in \mathbb{C}$ for $i = 0, \dots, k$ and $a_k \neq 0$. Since $\mathbb{C}$ is algebraically closed, we can also write

$$F(X) = a_k \prod_{j=1}^{k'} (X - \alpha_j)^{m_j}$$

where $\alpha_j \in \mathbb{C}$ for $j = 1, \dots, k'$ and $\alpha_i \neq \alpha_j$ for $i \neq j$.

Then by $\deg F = k = \sum_{j=1}^{k'} m_j$ it follows that $k' \leq k$. We define

$$r(F) := k'$$

to indicate the number of different zeros of F. We call this the radical of F, since k' is the degree of $\prod_{j=1}^{k'}(X - \alpha_j)$, which is the generator of the radical ideal belonging to the ideal generated by F.

For $F, G, H \in \mathbb{C}[X]$ not all constant polynomials with $\gcd(F, G, H) = 1$ (which is equivalent to saying that F, G, H have no zeros in common) such that $F + G = H$, we define

$$\begin{aligned} h(F, G, H) &:= \max(\deg F, \deg G, \deg H) \text{ and} \\ r(F, G, H) &:= r(FGH) = r(F) + r(G) + r(H), \end{aligned}$$

where the last equality follows by

$$\gcd(F, G, H) = 1 \iff \gcd(F, G) = \gcd(G, H) = \gcd(F, H) = 1$$

because $F + G = H$.

We compare the multiplicative structure on $\mathbb{C}[X]$, symbolized by the measures h and r, with the additive structure represented by $F + G = H$ by defining

$$L := \left\{ \frac{h(F,G,H)}{r(F,G,H)} : F, G, H \in \mathbb{C}[X],\ \gcd(F,G,H) = 1,\ F + G = H \right\}.$$

Theorem 1.1.1 *The set L is bounded, denoted by $\sup L < \infty$.*

This theorem can be proved effectively in the sense that the bound can be given explicitly.

Theorem 1.1.2 (Mason) *Let $F, G, H \in \mathbb{C}[X]$ such that $\gcd(F,G,H) = 1$, at least one is non-constant and $F + G = H$. Then*

$$h(F,G,H) \leq r(F,G,H) - 1$$

Proof: We write

$$\begin{aligned} F(X) &= c_1 \prod (X - \alpha_i)^{m_i}, \\ G(X) &= c_2 \prod (X - \beta_j)^{n_j} \text{ and} \\ H(X) &= c_3 \prod (X - \gamma_k)^{l_k}. \end{aligned}$$

Simple differentiating gives us

$$\frac{F'}{F}(X) = \sum \frac{m_i}{X - \alpha_i},\ \frac{G'}{G}(X) = \sum \frac{n_j}{X - \beta_j} \text{ and } \frac{H'}{H}(X) = \sum \frac{l_k}{X - \gamma_k}.$$

Since $(F + G)/H = 1$ we have

$$\left(\frac{F}{H}\right)' + \left(\frac{G}{H}\right)' = 0 \text{ and } \frac{(F/H)'}{(G/H)'} = -1.$$

It then follows that

$$\frac{G}{F} = \frac{G/H}{F/H} = -\frac{(\frac{F}{H})'/(\frac{F}{H})}{(\frac{G}{H})'/(\frac{G}{H})}.$$

By using that $[\log F]' = \frac{F'}{F}$ we have that

$$\frac{(F/G)'}{(F/G)} = [\log(F/G)]' = [\log F - \log G]' = F'/F - G'/G.$$

This leads to

$$\frac{G}{F} = -\frac{F'/F - H'/H}{G'/G - H'/H} = -\frac{\sum \frac{m_i}{X-\alpha_i} - \sum \frac{l_k}{X-\gamma_k}}{\sum \frac{n_j}{X-\beta_j} - \sum \frac{l_k}{X-\gamma_k}}.$$

Define the radical polynomial of FGH by

$$R(X) := \prod (X - \alpha_i) \prod (X - \beta_j) \prod (X - \gamma_k),$$

which means that $r(F,G,H) = \deg R$. It follows that

$$\deg \frac{R(X)}{X - \alpha_i} = \deg \frac{R(X)}{X - \beta_j} = \deg \frac{R(X)}{X - \gamma_k} = r(F,G,H) - 1.$$

That means that

$$\begin{aligned} S(X) &:= \left(\sum \frac{m_i}{X-\alpha_i} - \sum \frac{l_k}{X-\gamma_k}\right) R(X) \text{ and} \\ T(X) &:= \left(\sum \frac{n_j}{X-\beta_j} - \sum \frac{l_k}{X-\gamma_k}\right) R(X) \end{aligned}$$

are polynomials with $\deg S, \deg T \leq r(F,G,H) - 1$. But then

$$\frac{G}{F} = \frac{G}{F}\frac{R}{R} = \frac{S}{T}.$$

By $\gcd(F,G) = 1$, it follows that $\deg G \leq \deg S$ and that $\deg F \leq \deg T$. Since $H = F + G$ we have

$$\deg H \leq \max(\deg F, \deg G) \leq r(F,G,H) - 1.$$

This proves that

$$h(F,G,H) = \max(\deg F, \deg G, \deg H) \leq r(F,G,H) - 1.$$

□

Most striking is that this simple theorem which needs no more than elementary differentiation proves the Fermat conjecture for polynomials.

Theorem 1.1.3 *For $n \geq 3$, no polynomials $F_1, G_1, H_1 \in \mathbb{C}[X]$ exist such that*

$$F_1^n + G_1^n = H_1^n.$$

Proof: Suppose a counterexample exists. Define

$$F_2 := \frac{F_1}{\gcd(F,G,H)},\ G_2 := \frac{G_1}{\gcd(F,G,H)} \text{ and } H_2 := \frac{H_1}{\gcd(F,G,H)}.$$

We have $F_2^n + G_2^n = H_2^n$ and $\gcd(F_2, G_2, H_2) = 1$. Define

$$F := F_2^n,\ G := G_2^n \text{ and } H := H_2^n.$$

We now have $F, G, H \in \mathbb{C}[X]$ with $F + G = H$ and $\gcd(F,G,H) = 1$. The zeros of F, G and H are exactly the zeros of F_2, G_2 and H_2 respectively, so we have

$$r(F) = r(F_2) \leq \deg F_2 = \frac{1}{n} \deg F$$

and similarly $r(G) \leq \frac{1}{n} \deg G$ and $r(H) \leq \frac{1}{n} \deg H$. That means that

$$r(F,G,H) \leq \frac{1}{n} \deg F + \frac{1}{n} \deg G + \frac{1}{n} \deg H \leq \frac{3}{n} h(F,G,H).$$

This is clearly in contradiction with Theorem 1.1.2 if $n \geq 3$. □

1.2 Integer Case

In order to formulate Mason's theorem over the ring of integers, we have to translate the quantities that are used.

The important properties of the degree of polynomials are that

$$\begin{aligned} \deg F + G &\leq \max(\deg F, \deg G) + O(1) \text{ and that} \\ \deg FG &= \deg F + \deg G. \end{aligned}$$

These properties also hold for $\log|x|$ for integer x.

Due to unique factorization we have for all $n \in \mathbb{Z}$ the unique decomposition

$$n = (-1)^{e_0} p_1^{e_1} \cdots p_k^{e_k},$$

where $p_1, \ldots, p_k$ are distinct prime numbers, e_0 is either 0 or 1 and the e_i are positive integers for $i = 1, \ldots, k$. The generator of the radical ideal of the ideal generated by n can be expressed as

$$R(n) := p_1 \cdots p_k.$$

For $a, b, c \in \mathbb{Z}$ such that $a + b = c$ and that $\gcd(a, b, c) = 1$ we define

$$h(a, b, c) := \max(\log|a|, \log|b|, \log|c|)$$

and

$$r(a, b, c) := \log R(abc).$$

As in the previous section, we define

$$L := \left\{ \frac{h(a,b,c)}{r(a,b,c)} : a, b, c \in \mathbb{Z};\ a + b = c;\ \gcd(a, b, c) = 1 \right\}.$$

Conjecture 1.2.1 (weak ABC) $\sup L < \infty$

Stronger conjectures should say something about the bound on L. Simply replacing ∞ by 1 will not work, as is proved by the following example due to W. Jastrzebowski and D. Spielman.

Lemma 1.2.2 $2^n \mid 3^{2^n} - 1$

Proof: Induction with respect to n, using that $3^{2^n} - 1$ is the difference of two squares. □

Proposition 1.2.3 *There exist infinitely many* $a, b, c \in \mathbb{Z}$ *with* $a + b = c$ *and* $\gcd(a, b, c) = 1$ *such that* $\frac{h(a,b,c)}{r(a,b,c)} > 1$.

Proof: We define

$$a_n := 3^{2^n},\ b_n := -1 \text{ and } c_n := 3^{2^n} - 1.$$

Each tuple (a_n, b_n, c_n) in this sequence clearly satisfies $a_n + b_n = c_n$ and $\gcd(a_n, b_n, c_n) = 1$. We have

$$h(a_n, b_n, c_n) = \log a_n = 2^n \log 3$$

and

$$\begin{aligned} r(a_n, b_n, c_n) &= \log R(a_n, b_n, c_n) \leq \log 3 + \log R(c_n) \\ &\leq \log 3 + \log 2 + \log \frac{c_n}{2^n} \leq \log c_n - (n-3)\log 2. \end{aligned}$$

It follows that

$$\frac{r(a_n, b_n, c_n)}{h(a_n, b_n, c_n)} \leq \frac{\log c_n - (n-3)\log 2}{2^n \log 3} \leq 1 - \frac{(n-3)\log 2}{2^n \log 3}.$$

Taking $n = 4, 5, \ldots$ proves the proposition. □

Although this rules 1 out as an upper bound for L, it might be that 1 is an essential bound in the sense that $\limsup L = 1$. That means that for every $\epsilon > 0$ there are only finitely many a, b and c that satisfy the conditions in the definition of L such that $\frac{h(a,b,c)}{r(a,b,c)} > 1 + \epsilon$. Oesterlé and Masser conjectured just that.

Conjecture 1.2.4 (ineffective ABC) $\limsup L = 1$.

An effective form would be

Conjecture 1.2.5 (effective ABC) *For all $\epsilon > 0$ there exists an effectively computable constant C_ϵ such that for all $a, b, c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$ and $a + b = c$ we have*

$$h(a, b, c) \leq (1 + \epsilon) r(a, b, c) + C_\epsilon.$$

This inequality is often stated in the equivalent form

$$\max(|a|, |b|, |c|) \leq C_\epsilon R(abc)^{1+\epsilon}.$$

In all three situations we can write

$$h(a, b, c) \leq (\alpha + \epsilon) r(a, b, c) + C_\epsilon.$$

Weak ABC then conjectures $\alpha < \infty$, ineffective ABC that $\alpha = 1$ and effective ABC that C_ϵ is effectively computable for $\epsilon > 0$.

1.3 Implications

Each of the three versions of the ABC-conjecture implies a form of the Fermat-conjecture. This leads to the weak, the ineffective and the effective Fermat-conjecture.

If we have a triple $x, y, z \in \mathbb{Z}$ such that $x + y = z$, then we can divide out any common factor. We can assume $\gcd(x, y, z) = 1$. Put $a = x^n$, $b = y^n$ and $c = z^n$. These three numbers satisfy the conditions of the ABC-conjecture, with the additional information that $h(a, b, c) = n h(x, y, z)$ and that $r(a, b, c) = r(x, y, z) \leq 3h(x, y, z)$. We write in accordance with the previous section,

$$n\, h(x, y, z) \leq 3(\alpha + \epsilon) h(x, y, z) + C_\epsilon.$$

It follows that

$$h(x, y, z) \leq \frac{C_\epsilon}{n - 3(\alpha + \epsilon)}.$$

Proposition 1.3.1 *If weak ABC holds, then there exists an n_0 such that for all $n > n_0$ there are no $x, y, z \in \mathbb{Z}$ with $x, y, z \neq 0$ such that $x^n + y^n = z^n$.*

Proof: Fix ϵ and let $n \to \infty$. The bound for $h(x, y, z)$ then approaches 0. It is clear that $h(x, y, z) \geq \log 2$. That means that from some n onwards, no solution can exist. □

Proposition 1.3.2 *If ineffective ABC holds, there are only finitely many solutions to $x^n + y^n = z^n$ with $\gcd(x, y, z) = 1$ and $n \geq 3$.*

Proof: We can take $\alpha = 1$ and $\epsilon = \frac{1}{4}$. That means that

$$h(x, y, z) \leq \frac{C_{\frac{1}{4}}}{n - 3\frac{3}{4}}.$$

For any $n > 3$ this puts a bound on $h(x, y, z) = \log \max(|x|, |y|, |z|)$, thereby limiting the possibilities to a finite number. If we take $n = 4$, we get a bound for all $n > 3$. For $n = 3$ it has been proved separately that no solutions exist. □

Proposition 1.3.3 *If effective ABC holds, then there exists an effectively computable bound C such that any solution of $x^n + y^n = z^n$ with $n \geq 3$ and $\gcd(x, y, z) = 1$ satisfies*

$$\max(|x|, |y|, |z|) < C.$$

Proof: We have the same inequality as in the previous proposition, but here $C_{\frac{1}{4}}$ can be determined effectively. Put $C = \exp(4C_{\frac{1}{4}})$. □

Conjecture 1.3.4 (strong Fermat Conjecture) *The equation $x^n + y^n = z^n$ has no integer solutions for $n \geq 3$*

From the last result, we could check the strong formulation of Fermat's conjecture with only a finite amount of calculation.

The ABC-conjecture is much stronger than the Fermat Conjecture. To illustrate that, we show that the generalized Fermat Conjecture is also implied by ABC.

Consider the equation

$$Ax^r + By^s = Cz^t.$$

Putting $A = B = C = 1$ and $r = s = t$ gives the Fermat equation and putting $A = B = C = 1$ and $y = 1$ gives $x^r + 1 = z^t$, which is the Catalan equation.

Theorem 1.3.5 (Darmon and Granville) *If r, s and t are positive integers such that $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$ and A, B and C are fixed, then the generalized Fermat equation only has finitely many integer solutions such that $\gcd(Ax, By) = 1$.*

Proof: See [DG94]. In fact, they show that some associated curve has genus greater than 1. The theorem then follows by Mordell's conjecture that has been proved by Faltings. □

This theorem is implied by the ABC-conjecture.

Lemma 1.3.6 *Let r, s and t be positive integers. If*

$$\frac{1}{r}+\frac{1}{s}+\frac{1}{t}<1$$

then

$$\frac{1}{r}+\frac{1}{s}+\frac{1}{t}\leq 1-\frac{1}{42}.$$

Proof: Without loss of generality, we assume $r\leq s\leq t$. It follows that $r\geq 2$.

$r=2$**:** From $\frac{1}{s}+\frac{1}{t}<\frac{1}{2}$ it follows that $s\geq 3$.

$s=3$**:** Then $t\geq 7$. $\frac{1}{r}+\frac{1}{s}+\frac{1}{t}\leq\frac{1}{2}+\frac{1}{3}+\frac{1}{7}=\frac{41}{42}$.
$s=4$**:** Then $t\geq 5$. $\frac{1}{r}+\frac{1}{s}+\frac{1}{t}\leq\frac{1}{2}+\frac{1}{4}+\frac{1}{7}=\frac{19}{20}$.
$s\geq 5$**:** Then $t\geq 5$ because $t>s$. The sum in this case is even smaller than in the previous one.

$r=3$**:** Then $s,t<\frac{2}{3}$ and $s,t\geq 3$.

$s=3$**:** Then $t\geq 4$, where $\frac{1}{3}+\frac{1}{3}+\frac{1}{4}=\frac{11}{12}$.
$s\geq 4$**:** Then $t\geq 4$.

$r\geq 4$**:** Then $s,t\geq 4$, which implies that $\frac{1}{r}+\frac{1}{s}+\frac{1}{t}\leq\frac{3}{4}$.

Proposition 1.3.7 *Effective and ineffective ABC imply respective versions of Theorem 1.3.5.*

Proof: Let A,B,C,r,s,t,x,y,z be as in the theorem. Define $a:=Ax^r$, $b:=By^s$ and $c:=Cz^t$. By the condition $\gcd(Ax,By)=1$, it follows that $\gcd(a,b,c)=1$. We have

$$\begin{aligned}R(abc) &= R(Ax^rBy^sCz^t)\leq R(ABC)R(x)R(y)R(z)\leq R(ABC)xyz\\ &= R(ABC)(\frac{a}{A})^{\frac{1}{r}}(\frac{b}{B})^{\frac{1}{s}}(\frac{c}{C})^{\frac{1}{t}}\end{aligned}$$

It follows that

$$\begin{aligned}r(a,b,c) &\leq \left(\frac{1}{r}+\frac{1}{s}+\frac{1}{t}\right)h(a,b,c)+\log R(ABC)-\frac{\log|A|}{r}-\frac{\log|B|}{s}-\frac{\log|C|}{t}\\ &\leq \left(1-\frac{1}{42}\right)h(a,b,c)+K_{A,B,C}\end{aligned}$$

with K an effectively computable constant, dependent on A,B,C.

Using the ABC-conjecture we get for $\epsilon>0$,

$$h(a,b,c)\leq(1+\epsilon)r(a,b,c)+C_\epsilon.$$

If we substitute that, we get

$$(1-(1+\epsilon)(1-\frac{1}{42}))h(a,b,c)\leq(1+\epsilon)K+C_\epsilon.$$

If we assume that effective ABC holds, then K and C_ϵ can be computed for some $\epsilon<\frac{1}{41}$. This then gives an effective upper bound on the size of integer solutions of the generalized Fermat equation. If we only assume ineffective ABC, we still have that $h(a,b,c)$ is bounded and, since the number of $(a,b,c)\in\mathbb{Z}^3$ such that $h(a,b,c)\leq K_0$ is finite for every finite K_0, we still have that the generalized Fermat equation only has finitely many solutions. □

In fact, we prove that there are only finitely many solutions, even if r,s,t are allowed to vary. This result is stronger than the theorem that Darmon and Granville have proved.

1.4 Limit Points

Apart from looking at the lim sup of $L_{\mathbb{Z}}$ and $L_{\mathbb{C}[X]}$, we can also look at other limit points of these sets. This section describes work of Jerzy Browkin [Bro].

Proposition 1.4.1 *Every limit point of $L_{\mathbb{Z}}$ and $L_{\mathbb{C}[X]}$ is greater than or equal to $\frac{1}{3}$.*

Proof: Suppose $A, B, C \in \mathbb{C}[X]$ or $\mathbb{Z}$ such that $A + B = C$ and $\gcd(A, B, C) = 1$. Furthermore, suppose that $h(C)$ (that is, $\log|C|$ or $\deg C$) equals

$$\max(h(A), h(B), h(C)) = h(A, B, C).$$

Then

$$\frac{h(C)}{r(A,B,C)} = \frac{h(C)}{r(A) + r(B) + r(C)} \geq \frac{h(C)}{3h(C)} = \frac{1}{3}.$$

□

Lemma 1.4.2 *For every $\alpha \in (0, 1)$ there exists an n_0 such that for every $n > n_0$ there exists a square-free $a \in \{n, \ldots, 2n\}$ and a prime p with $n^\alpha < p < 2n^\alpha$ such that $a + p$ is square-free.*

Proof: For any n large enough, fix a prime $p \in (n^\alpha, 2n^\alpha)$. Consider

$$V_0 := \{a \in [n, 2n] : R(a) = a\},$$

which is the set of square-free numbers in the interval $[n, 2n]$. That means we have

$$\#V_0 = \frac{6}{\pi^2} n + O(\sqrt{n}).$$

We leave out the numbers that are divisible by p, which are at most $n/p \leq n/n^\alpha$ numbers. That gives us

$$V := \{a \in [n, 2n] : R(a) = a;\ p \nmid a\}$$

with

$$\#V \geq \left(\frac{6}{\pi^2} - \frac{1}{n^\alpha}\right) n + O(\sqrt{n}).$$

Now consider $I := \{a \in \{n + n^\alpha, \ldots, 2n + 2n^\alpha\} : R(a) = a\}$. Then

$$\#I = \frac{6}{\pi^2}(n + n^\alpha) + O(\sqrt{n}).$$

Denote $V + p := \{a + p : a \in V\}$. Then $\#(V + p) = \#V$ and $V + p \subset (n + n^\alpha, 2n + 2n^\alpha)$. If there are no square-free numbers in $V + p$ then I and $V + p$ are disjoint subsets of $\{n + n^\alpha, \ldots, 2n + 2n^\alpha\}$, which implies that

$$\begin{aligned} n + n^\alpha &\geq \#I + \#(V + p) \\ &= \frac{12}{\pi^2} n + \frac{6}{\pi^2} n^\alpha - \frac{n}{n^\alpha} + O(\sqrt{n}) \\ &= \frac{12}{\pi^2} n + O(n^\beta) \end{aligned}$$

where $\beta = \max(\alpha, 1 - \alpha, \frac{1}{2}) < 1$. Since $12 > \pi^2$, there exists a n_0 such that this is a contradiction for $n > n_0$. That means that for $n > n_0$, we can choose $a \in V$ such that $a + p$ is square-free. □

Theorem 1.4.3 *For every $\lambda \in [\frac{1}{3}, \frac{1}{2}]$ there are sequences $\{A_n\}$ and $\{B_n\}$ such that A_n and B_n are coprime and*

$$\lim_{n\to\infty} \frac{h(A_n, B_n, A_n + B_n)}{r(A_n, B_n, A_n + B_n)} = \lambda.$$

Proof: First suppose $\frac{1}{3} < \lambda < \frac{1}{2}$. Define $\alpha := \frac{1}{\lambda} - 2$. Since $\alpha \in (0, 1)$, we can use the lemma to get an n_0 such that for $n > n_o$ we have a square-free $a_n \in [n, 2n]$ and a prime $p_n \in (n^\alpha, 2n^\alpha)$ that are coprime such that $a_n + p_n \in (n + n^\alpha, 2(n + n^\alpha))$ is square-free. Put $A_n = a_n$ and $B_n = p_n$. We have

$$\lim_{n\to\infty} \frac{h(A_n, B_n, A_n + B_n)}{r(A_n, B_n, A_n + B_n)} = \lim_{n\to\infty} \frac{\log(a_n + p_n)}{\log a_n + \log p_n + \log(a_n + p_n)},$$

which is easily verified to equal λ using the inequalities that a_n and p_n satisfy. If every $\lambda \in (\frac{1}{2}, \frac{1}{3})$ is a limit point of $L_{\mathbb{Z}}$, then so are $\frac{1}{2}$ and $\frac{1}{3}$. □

Note that Proposition 1.2.3 shows that there is a limit point of $L_{\mathbb{Z}}$ that is greater than or equal to 1.

For polynomials we can prove a stronger result.

Lemma 1.4.4 *For $m > k > 0$, the polynomial $F(X) = X^m - X^k + 1$ has no multiple roots over $\mathbb{C}$.*

Proof: Suppose x is a multiple root. Then $F(x) = F'(x) = 0$, which leads to

$$\begin{cases} x^k(x^{m-k} - 1) &= 1 \\ x^{m-k} &= \frac{k}{m} \end{cases}.$$

Solving this, we get $x^k = \frac{m}{k-m}$ and $x^m = \frac{k}{k-m}$, leading to $m^m = k^k(m-k)^{m-k}$. Since $k \le m - 1$ and $m - k \le m - 1$, we have $m^m \le (m-1)^m$, which is a contradiction. □

Theorem 1.4.5 *Every number $\lambda \in [\frac{1}{3}, 1]$ is a limit point of $L_{\mathbb{Z}[X]} \subseteq L_{\mathbb{C}[X]}$.*

Proof: First assume $\lambda \in [\frac{1}{2}, 1]$. Then there are sequences k_n and m_n of natural numbers such that $m_n > k_n > 1$, $k_n \to \infty$ and $\frac{k_n}{m_n} \to \frac{1}{\lambda} - 1$. Put $A_n = x^{m_n}$, $B_n = -x^{k_n} + 1$ and $C_n = x^{m_n} - x^{k_n} + 1$. Then we have $h(A_n, B_n, C_n) = m_n$, $r(A_n) = 1$, $r(B_n) = k_n$ since all k_nth roots of unity are distinct and $r(C_n) = m_n$ by the lemma. Furthermore, $C_n = A_n + B_n$ and $\gcd(A_n, B_n) = 1$ because A_n and B_n have no roots in common. We have

$$\lim_{n\to\infty} \frac{h(A_n, B_n, C_n)}{r(A_n, B_n, C_n} = \lim_{n\to\infty} \frac{m_n}{1 + k_n + m_n} = \lambda,$$

which proves that λ is a limit point of $L_{\mathbb{C}[X]}$.

Now assume that $\lambda \in [\frac{1}{3}, \frac{1}{2}]$. There are sequences k_n and m_n of natural numbers such that $m_n > k_n > 1$, $k_n \to \infty$ and $\frac{k_n}{m_n} \to \frac{1}{\lambda} - 2$. Now put $A_n = x^{m_n} + 2$, $B_n = -x^{k_n} - 1$ and $C_n = x^{m_n} - x^{k_n} + 1$. We have $h(A_n, B_n, C_n) = m_n$, $r(A_n) = m_n$, $r(B_n) = k_n$, $r(C_n) = m_n$, $C_n = A_n + B_n$ and $\gcd(A_n, B_n) = 1$. It follows that

$$\lim_{n\to\infty} \frac{h(A_n, B_n, C_n)}{r(A_n, B_n, C_n)} = \lim_{n\to\infty} \frac{m_n}{2m_n + k_n} = \lambda.$$

□

Note that combining this with Proposition 1.4.1 together with Theorem 1.1.2 shows that $[\frac{1}{3}, 1]$ is the set of limit point of $L_{\mathbb{C}[X]}$. Especially, we see that Theorem 1.1.2 cannot be improved.

Chapter 2

Valuations and the Product Formula

2.1 Definitions

Let K be a field. A valuation is a real-valued function v on K denoted by

$$\begin{array}{rccc} v: & K & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & |x|_v \end{array}$$

such that

V1. $|x|_v \geq 0$ for all $x \in K$; $|x|_v = 0 \iff x = 0$,
V2. $|x|_v|y|_v = |xy|_v$ for all $x, y \in K$ and
V3. there is a $C_v \in \mathbb{R}$ such that
$|x+y|_v \leq C_v \max(|x|_v, |y|_v)$ for all $x, y \in K$.

Taking $y = 0$ in **V3** shows that $C_v \geq 1$. If we can take $C_v = 1$, we call v *nonarchimedean*, otherwise *archimedean*.

Two valuations v and w on K are called *equivalent* if there exists an $\alpha > 0$ such that $|x|_v = (|x|_w)^\alpha$ for all $x \in K$.

Lemma 2.1.1 *Let K be a field. If v and w are equivalent valuations on K, then they are both archimedean or both nonarchimedean.*

Proof: Let α be such that $|x|_v = (|x|_w)^\alpha$. Then

$$|x+y|_v = (|x+y|_w)^\alpha \leq (C_w \max(|x|_w, |y|_w))^\alpha = C_w^\alpha \max(|x|_w^\alpha, |y|_w^\alpha).$$

It follows that we can take $C_v \leq C_w^\alpha$ and by interchanging v and w that we can also take $C_w \leq C_v^{\frac{1}{\alpha}}$. We conclude that we can take $C_v = 1$ if and only if we can take $C_w = 1$. □

Thus we can speak of nonarchimedean equivalence classes. The *trivial* valuation defined by $|0|_t = 0$ and $|x|_t = 1$ for $x \in K^*$ is only equivalent to itself and will be excluded from now on. The other equivalence classes of valuations on K are called *primes* or *prime divisors* of K.

For each nonarchimedean valuation v on K we define $\nu_v(x) := -\log|x|_v$ for $x \in K^*$. It is customary to consider $\nu_v(0) = \infty$. It follows that it satisfies

EV1. $\nu_v(x) = \infty \iff x = 0$,
EV2. $\nu_v(xy) = \nu_v(x) + \nu_v(y)$ for all $x, y \in K$ and
EV3. $\nu_v(x+y) \geq \min(\nu_v(x), \nu_v(y))$ for all $x, y \in K$.

Such functions are called *exponential valuations.*

For exponential valuations and thereby for nonarchimedean valuations we define the ring of local integers $O_v := \{x \in K : \nu_v(x) \geq 0\}$ and the subring of local units $U_v := \{x \in K : \nu_v(x) = 0\}$. The local integers form a valuation ring, meaning that there is a unique maximal ideal, namely $\wp_v := \{x \in K : \nu_v(x) > 0\}$. Since the sets O_v, U_v and $\wp_v$ remain unchanged when v is replaced by an equivalent valuation, we can speak of *local integers* and *local units* at a prime.

A nonarchimedean prime P of K is called *discrete* if there is a $v \in P$ such that the image $\nu_v(K^*) \in \mathbb{R}$ is a discrete subgroup. This group is isomorphic to $\mathbb{Z}$ because all discrete subgroups of $\mathbb{R}$ are either trivial (then v would be trivial) or isomorphic to $\mathbb{Z}$. The normalized exponential valuation $\mathrm{ord}_P = \nu_P$ is the exponential valuation ν_v ($v \in P$) such that $\nu_v(K^*) = \mathbb{Z}$. Such a valuation exists for every discrete prime.

2.2 Rational fields

By a rational field, we mean either $\mathbb{Q}$ or the quotient field $k(X)$ of a polynomial ring $k[X]$ over some field k.

I. The case $K = \mathbb{Q}$

Put $M_{\mathbb{Q}} := \{\infty\} \cup \{p \in \mathbb{Z} : p > 0,\ p \text{ prime number}\}$. By the infinite prime ∞ we mean the equivalence class containing the absolute value. This implies that ∞ is archimedean. The normalized valuation in ∞ is the ordinary absolute value and is denoted by $|x|_\infty$. For every prime $p \in \mathbb{Z}$ we can write each $x \in \mathbb{Q}$ as $x = p^\epsilon \frac{r}{s}$ where $\epsilon, r, s \in \mathbb{Z}$, $s \neq 0$ and $p \nmid r, s$. The exponent ϵ is uniquely determined. We define the ordinal of x at p as $\mathrm{ord}_p x = \epsilon$. This is a normalized discrete exponential valuation. The normalized valuation at p is defined by $|x|_p = p^{-\mathrm{ord}_p x}$. The proof that all valuations on $\mathbb{Q}$ are equivalent to one of the normalized valuations mentioned here can be found in [Wei63], theorem 1-4-2.

Proposition 2.2.1 *Let $K = \mathbb{Q}$, let $M_K = \{\infty\} \cup \{p \in \mathbb{Z} : p \text{ prime number}\}$ and for $P \in M_K$ let $|x|_P$ be the normalized valuation defined as above. For each $x \in K^*$ the following properties hold:*

PF1. $|x|_P \neq 1$ *for only finitely many* $P \in M_K$
PF2. $\prod_{P \in M_K} |x|_P = 1$

Proof: **PF1** follows from the fact that for every $x \in \mathbb{Q}$ only finitely many prime numbers divide the numerator or the denominator. **PF2** follows directly from the chosen normalizations. □

II. The case $K = k(X)$

Put $M_K := \{\infty\} \cup \{P(X) \in k[X] : P(X) \text{ monic irreducible over } k\}$. If k is algebraically closed, this is equivalent with $M_K \simeq k \cup \{\infty\} \simeq \mathbb{P}^1_k$. Since $k[X]$ is a unique factorization domain, we can write every $f(X) \in k(X)$ as $\frac{R(X)}{S(X)}$ with $R(X), S(X) \in k[X]$. We define $\mathrm{ord}_\infty(f) := \deg S - \deg R$. For an irreducible polynomial $P(X)$, we can write $f(X) = (P(X))^\epsilon \frac{R(X)}{S(X)}$ with $R(X), S(X) \in k[X]$ and $P(X) \nmid R(X), S(X)$. We define $\mathrm{ord}_P f := \epsilon$. These ordinal functions are normalized discrete exponential valuations. We consider $\deg \infty := 1$. For every $P \in M_K$ we define the normalized valuation $|f|_P = (e^{\deg P})^{-\mathrm{ord}_P f}$. In [vdW67] §147 it is proved that every valuation on K that is equivalent to the trivial valuation when restricted to k, is equivalent to one of the valuations mentioned here.

Proposition 2.2.2 *Let k be a field, let $K = k(X)$ and let M_K, ord_P and $|.|_P$ ($P \in M_K$) be defined as above. For each $f \in K^*$ the following properties hold:*

PF1. $|f|_P \neq 1$ *for only finitely many* $P \in M_K$
PF2. $\prod_{P \in M_K} |f|_P = 1$

Proof: PF1 follows from the fact that every $f \in K$ has only finitely many irreducible factors in its numerator and denominator. In this case, **PF2** becomes much clearer if we write it as

$$\sum_{P \in M_K \setminus \{\infty\}} \deg(P) \mathrm{ord}_P f = -\mathrm{ord}_\infty f.$$

This follows for polynomials $f(X) \in k[X]$ from $\mathrm{ord}_\infty f = -\deg f$. It then follows for rational functions in general by multiplicativity of the ordinals. □

2.3 Extension of valuations

For our purposes, it is sufficient to look at finite extensions E of a rational field K. Such fields are called *global fields*. A valuation v on E is said to be an extension of a valuation w on K if $|a|_v = |a|_w$ for all $a \in K \subset E$. Of course, if v' is a valuation on E that is equivalent to v, then it extends some valuation w' on K that is equivalent to w. That means it is meaningful to speak of a prime Q of E that extends some prime P of K, denoted by $Q \mid P$.

The crucial and deep fact that lets us extend the product formula to these fields, is that every valuation of K can be extended to E in only finitely many inequivalent ways. This property ports to primes, meaning that we can talk of the primes $Q_1, \ldots, Q_r$ of E extending a prime P of K. If P is discrete, then $Q_1, \ldots, Q_r$ are discrete too. A proof of this can be found in [Wei63], Chapter 2.

If P is archimedean, then $K = \mathbb{Q}$ because that is the only rational field with an archimedean prime. Using the $\mathbb{Q}$-embeddings of E in $\mathbb{C}$, we can induce the ordinary absolute value on $\mathbb{C}$ to E. The valuations in Q_i are all equivalent to such absolute values and we define $\sigma_{Q_i} : E \hookrightarrow \mathbb{C}$ to be an embedding that leads to such an absolute value. If $\sigma_{Q_i}(E) \subset \mathbb{R} \subset \mathbb{C}$ then Q_i is called *real*; otherwise Q_i is called *complex*.

Furthermore, there exist normalized valuations in $Q_1, \ldots, Q_r$ such that

$$\prod_{i=1}^{r} |\alpha|_{Q_i} = |N_{E/K}\alpha|_P.$$

Again, for proofs the reader is referred to [Wei63], Chapter 2.

Proposition 2.3.1 *Let E be a finite extension of a rational field K. Then there is a set M_E of primes of E extending the primes in M_K. For each prime in that set there exists a normalized valuation such that for each $\alpha \in E^*$ the following properties hold:*

PF1. $|\alpha|_P \neq 1$ *for only finitely many* $P \in M_K$
PF2. $\prod_{P \in M_K} |\alpha|_P = 1$

Proof: Take $\alpha \in E^*$. Let

$$x^{m_0} + a_1 x^{m_1} + a_2 x^{m_2} + \cdots + a_t$$

be the monic minimum polynomial of α over K where $m_0 > m_1 > \cdots > m_{t-1} > 0$ and $a_i \neq 0$ for $i = 1, \ldots, t$. Then **PF1** for K together with the fact that K only has finitely many archimedean primes implies that all but finitely many primes $P \in M_K$ are nonarchimedean such that $a_1, \ldots, a_t$ are local units at P. If Q is an extension of P to E, then $a_1, \ldots, a_t$ are also local units at Q. It follows that

$$|\alpha^{m_0} + a_1\alpha^{m_1} + \cdots + a_{t-1}\alpha^{m_{t-1}}|_Q = |-a_t|_Q = 1.$$

On the other hand

$$\begin{aligned} |\alpha^{m_0} + a_1\alpha^{m_1} + \cdots + a_{t-1}\alpha^{m_{t-1}}|_Q &\leq \max(|\alpha^{m_0}|_Q, |a_1\alpha^{m_1}|_Q, \ldots, |a_{t-1}\alpha^{m_{t-1}}|_Q) \\ &= \max(|\alpha|_Q^{m_0}, |\alpha|_Q^{m_1}, \ldots, |\alpha|_Q^{m_{t-1}}). \end{aligned}$$

Thus $|\alpha|_Q \geq 1$. Since $\frac{a_i}{a_t}$ is a local unit at P, we can use the same argument for $\frac{1}{\alpha}$, which has the minimum polynomial

$$x^{m_0} + \frac{a_{t-1}}{a_t} x^{m_t - m_{t-1}} + \cdots + \frac{a_1}{a_t} x^{m_0 - m_1} + \frac{1}{a_t}.$$

It follows that $|\alpha|_Q = 1$ for every Q extending P to E. This proves **PF1** since the finite number of primes of K at which $a_1, \ldots, a_t$ are not local units, gives rise to only a finite number of primes of E.

The second part **PF2** follows from

$$\prod_{Q \in M_E} |\alpha|_Q = \prod_{P \in M_K} \left(\prod_{Q|P} |\alpha|_Q \right) = \prod_{P \in M_K} |N_{E/K}\alpha|_P = 1,$$

since **PF2** holds in K. □

The normalized valuations can be given quite explicitly. For number fields, the residue class field at a nonarchimedean prime Q, defined by $O_Q/\wp_Q$, is finite. The norm of such a prime is defined by $\mathfrak{N}Q = \#(O_Q/\wp_Q)$.

Proposition 2.3.2 *Let K be a finite extension of $\mathbb{Q}$ and let M_K denote the set of primes extending the primes in $M_\mathbb{Q}$ to K. The normalized valuations as in Proposition 2.3.1 can be written as*

$$\begin{aligned} |\alpha|_Q &= |\sigma_Q \alpha| \text{ if } Q \text{ is real archimedean,} \\ |\alpha|_Q &= |\sigma_Q \alpha|^2 \text{ if } Q \text{ is complex archimedean and} \\ |\alpha|_Q &= (\mathfrak{N}Q)^{-\mathrm{ord}_Q \alpha} \text{ if } Q \text{ is discrete.} \end{aligned}$$

Proof: See [Wei63], proposition 5-1-2. □

In a number field K we have the concept of global integer, which is usually called a K-integer. An element $x \in K$ is called a K-integer if it is a local integer at all finite, that is discrete in this case, primes. The K-integers form a ring $\mathcal{O}_K$ such that K is the quotient field.

The same proposition holds if K is a function field. However, the definition of $\mathfrak{N}Q$ needs refinement in this case since the residue class field need not necessarily be finite. It will be a finite extension of the constant field k, however. We can define the degree of a prime by $\deg Q = [O_Q/\wp_Q : k]$. The norm of a prime can then be defined as $\mathfrak{N}Q = e^{\deg Q}$. In the next section we will see a more elegant way to define the concept of degree for primes in the function field case.

Chapter 3

Divisors on Algebraic Curves

The concept *divisor* can be defined on any algebraic variety. We will limit ourselves to one dimensional projective varieties. For a more general approach, see [Lan83] or [Har77].

3.1 Definitions

Let k be a field and let Ω be its algebraic closure. A hypersurface in $\mathbb{P}^n_\Omega$ is the locus of an irreducible homogeneous polynomial in $n+1$ variables. A hypersurface is said to be defined over k if the homogeneous polynomial is a polynomial over k.

A projective curve, or curve, is a one dimensional subvariety of some $\mathbb{P}^n_\Omega$. It is characterized by the fact that the intersection with any hypersurface is either the entire curve or a finite set of points. Every curve can be described as the intersection of finitely many hypersurfaces.

A curve is said to be defined over k if it can be described as the intersection of hypersurfaces that are defined over k. From now on, we will assume that V is a curve that is defined over k.

Let k' be a finite extension of the base field k that is embedded in Ω. A point $(x_0 : \ldots : x_n) \in \mathbb{P}^n_\Omega$ is said to be k'-rational if $(x_0 : \ldots : x_n) \in \mathbb{P}^n_{k'}$. That means the set of k'-rational points on V is

$$V_{k'} = V \cap \mathbb{P}^2_{k'}.$$

If $P \in \mathbb{P}^n_\Omega$ then $k(P)$ is the minimal field extension k' of k in Ω such that P is k'-rational. Since Ω is algebraic over k, it follows that $[k(P) : k]$ is finite.

Let $G(k(P) : k)$ denote the group of isomorphisms of $k(P)$ into Ω that leave k pointwise unchanged. We extend $\sigma \in G(k(P) : k)$ to $\mathbb{P}^n_{k(P)}$ by applying σ to the coordinates of P. We say σP is a *conjugate point* of P over k. Because V is defined over k, we have that $\sigma P \in V$ if and only if $P \in V$.

In our case, k will be a finite extension of $\mathbb{Q}$. That means that every $k(P)$ will be a separable extension of k. In general, that need not be the case. Therefore, take k_1 a maximal separable extension of k in $k(P)$. We define the order of inseparability of $k(P)$ over k by $[k(P) : k]_i := \frac{[k(P):k]}{[k_1:k]}$.

The group of divisors of V is the free Abelian group generated by the points on V. That means divisors are finite sums of integer multiples of points on V. This group is denoted by

$$\mathrm{Div}(V) := \left\{ \sum_{i=1}^{r} a_i p_i : r = 1, 2, \ldots ; a_i \in \mathbb{Z}; p_i \in V \right\}.$$

For a divisor $\mathfrak{d} = \sum_{i=1}^{r} a_i p_i \in \mathrm{Div}(V)$ we define the degree $\deg \mathfrak{d} := \sum_{i=1}^{r} a_i$. A divisor is called positive, or effective, if all $a_i \geq 0$. This is denoted by $\mathfrak{d} \geq 0$.

The prime rational divisors or prime divisors of V over k are defined by

$$\mathfrak{p}_P := [k(P) : k]_i \sum_{\sigma \in G(k(P):k)} \sigma P \text{ where } P \in V_\Omega.$$

The group of divisors over k is defined as the subgroup generated by the prime divisors over k and is denoted by $\mathrm{Div}_k(V)$.

3.2 Valuations on function fields

Let V be a nonsingular curve that is defined over k. The Noether normalization Lemma tells us that V is birationally equivalent to a plane curve over k. That means that

$$V \sim \tilde{V} = \{(x : y : z) \in \mathbb{P}^2_\Omega : P_V(x, y, z) = 0\}$$

where $P_V \in k[X, Y, Z]$ is a homogeneous polynomial, irreducible over Ω. The fields of rational functions on these curves, denoted by $k(V)$ and $k(\tilde{V})$ respectively, are isomorphic.

Since $\tilde{V}$ is explicitly embedded in a projective plane, we can obtain an affine curve $\tilde{V}^a$ that is dense in $\tilde{V}$ (with respect to the Zariski topology) by intersecting $\tilde{V}$ with a standard affine piece of $\mathbb{P}^2$. The function field $k(\tilde{V}^a)$ is isomorphic to the quotient field of $k[X, Y]/(P_V(X, Y, 1))$ and so is $k(\tilde{V})$, since $\tilde{V}$ is the projective closure of V^a.

For each $P \in V$ and every $f \in k(V)$ we define the ordinal of f at P as

$$\begin{aligned} \mathrm{ord}_P(f) &:= 0 \text{ if } f(P) \text{ is defined and } f(P) \neq 0, \\ \mathrm{ord}_P(f) &:= \text{order of zero if } f(P) = 0 \text{ and} \\ \mathrm{ord}_P(f) &:= \mathrm{ord}_P\left(\frac{1}{f}\right) \text{ if } f \text{ has a pole at } P. \end{aligned}$$

We extend this definition to prime divisors by putting

$$\mathrm{ord}_{\mathfrak{p}_P}(f) := \frac{[k(P) : k]_i}{\deg \mathfrak{p}_P} \sum_{\sigma \in G(k(P):k)} \mathrm{ord}_{\sigma P}(f).$$

The divisor of zeros of a function $f \in k(V)$ is defined by

$$(f)_0 := \sum_{P \in \Omega : \mathrm{ord}_P(f) > 0} \mathrm{ord}_P(f) P.$$

The divisor of poles is defined similarly by $(f)_\infty = \left(\frac{1}{f}\right)_0$. Because f is defined over k, we have that $(f)_0 \in \mathrm{Div}_k(V)$. The degree of a rational function on a curve is defined by

$$\deg f := \deg(f)_0 = \deg(f)_\infty,$$

where the last equality follows because rational functions have as many poles as they have zeros. The divisor of a function f is the divisor defined by $(f) := (f)_0 - (f)_\infty$.

With these definitions it follows that if $V \simeq \mathbb{P}^1_\Omega = \Omega \cup \{\infty\}$, then the primitive divisors of V over k without the infinite divisor ∞ correspond to the zero divisors of the irreducible

polynomials over k. Then $k(V) = k(X)$ and the definitions of the ordinal functions here and in Section 2.2, coincide. We define the norm of a prime divisor by $\mathfrak{N}\mathfrak{p} := e^{\deg \mathfrak{p}}$.

Now we are able to formulate a proposition regarding normalized valuations on function fields, similar to Proposition 2.3.2.

Proposition 3.2.1 *Let K be a finite extension of a rational field $k(X)$ and let V be a non-singular curve over k such that K is isomorphic to the function field $k(V)$. Define for every prime divisor $\mathfrak{p}$ over k the valuation*

$$|f|_{\mathfrak{p}} := \mathfrak{N}\mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(f)}.$$

These valuations can be taken as normalized valuations in Proposition 2.3.1 if M_K is identified with the set of prime divisors on V over k.

Proof: Since $k(X)$ is a subfield of K, these valuations extend valuations on $k(X)$. The finiteness condition **PF1** is satisfied because functions only have a finite number of poles and zeros. The product formula **PF2** holds because the number of poles equals the number of zeros. For a more detailed proof, see [Lan83], Chapter 2, §3. □

It is worth noting that, if k is a finite field, we can replace e by $\#k$ to obtain $\mathfrak{N}\mathfrak{p} = \#O_{\mathfrak{p}}/\wp_{\mathfrak{p}}$ again, provided that the notion of log is changed accordingly.

3.3 Rational maps

Let V either be a curve or a projective space over k. Let $f_0, \ldots, f_n \in k(V)$. Then

$$\begin{array}{rccc} f: & V & - \to & \mathbb{P}^n \\ & x & \longmapsto & (f_0(x) : \ldots : f_n(x)) \end{array}$$

is called a rational map from V into $\mathbb{P}^n$. This is not the most general definition for a rational map, but it suits our purposes well enough.

Note that a rational map is not necessarily defined for every $x \in V$. It is only defined for $x \in V$ if not all $f_i(x) = 0$ and no f_i has a pole in x. However, if we multiply all f_i with some fixed $g \in k(V)$ then this does not change the value of f where it remains defined. Thus, by multiplying with an appropriate function, we can assume that all gf_i are defined in x without changing the value of f in x. We therefore say that f is *regular at x* if there exists a representative $(gf_0 : \ldots : gf_n)$ that is defined in x. If f is regular for all $x \in V$ then we call f a *morphism*.

If V is a curve then we can construct for each $x \in V$ a function g with a pole or a zero at x of arbitrary order. That means that if f is regular at some point, that is $f \neq (0 : \ldots : 0)$, then f is a morphism.

If V is a projective space, then each f_i is a quotient of two homogeneous polynomials of equal degree. We can multiply with the denominators and divide out any common factors to obtain a representation $f = (F_0 : \ldots : F_n)$, where the F_i are all homogeneous polynomials of the same degree with no factors in common. In this case, we define

$$\deg f := \deg F_i.$$

One should be aware that this is not a standard definition. In the case of nonconstant maps from curves to curves, the degree of a map $f : V \to W$ is normally defined as

$$\deg f := [k(V) : f^*k(W)],$$

where $f^*k(W)$ denotes the subfield of $k(V)$ of functions that factor through f. The only overlap of the domains of these definitions is the case where $f : \mathbb{P}^1 - \to \mathbb{P}^1$. In this case, the definitions coincide.

In general, defining the degree of $f : V - \to \mathbb{P}^1$ as $[k(V) : f^*k(\mathbb{P}^n)]$ need not make sense, since $f^*k(\mathbb{P}^n)$ can be of lower transcendence degree than $k(V)$ over k, or, if f is injective, $f^*k(\mathbb{P}^n)$ is the entire $k(V)$. Therefore, we take the liberty to use the term degree in the sense stated, bearing in mind that this concept need not relate to the degree of some appropriate field extension.

Let V be a nonsingular projective curve, not necessarily embedded in $\mathbb{P}^2_\Omega$. Define the subgroup of divisors linearly equivalent to 0 by

$$\mathrm{Div}_{\mathrm{lin}}(V) := \{(f) : f \in \Omega(V)\}$$

and the Picard group by

$$\mathrm{Pic}(V) := \mathrm{Div}(V)/\mathrm{Div}_{\mathrm{lin}}(V).$$

Two divisors are called linearly equivalent if their difference is the divisor of a function. In that case, they represent the same element in the Picard group.

With a divisor $\mathfrak{d} \in \mathrm{Div}(V)$ we associate a vector space of functions

$$L(\mathfrak{d}) := \{f \in \Omega(V) : (f) + \mathfrak{d} \geq 0\}$$

which we call the linear system associated with $\mathfrak{d}$. It is easy to see that $L(\mathfrak{d})$ is finite dimensional, since the degree of the functions f, that is the degree of $(f)_\infty$, is bounded by the degree of $\mathfrak{d}$.

Let $F = \{f_0, \ldots, f_r\}$ be a basis for $L(\mathfrak{d})$. Then

$$\begin{array}{rccc} \phi_{\mathfrak{d},F} : & V & - \to & \mathbb{P}^r \\ & x & \longmapsto & (f_0(x) : \ldots : f_r(x)) \end{array}$$

is a rational map. If this map is a nonconstant morphism, then $L(\mathfrak{d})$ is said to be *without base point*. For curves, we have that $L(\mathfrak{d})$ is without base point as soon as $\dim L(\mathfrak{d}) \geq 2$, since the associated map must be nonconstant and must be regular somewhere.

Unfortunately, there is no canonical basis for $L(\mathfrak{d})$. If we take another basis $G = \{g_0, \ldots, g_r\}$ for $L(\mathfrak{d})$, then

$$g_i = \sum_{j=0}^{r} a_{i,j} f_j \text{ for } i = 0, \ldots, r.$$

That means $\phi_{\mathfrak{d},G} = A \circ \phi_{\mathfrak{d},F}$, where A is the linear transformation of $\mathbb{P}^r$ determined by the coefficients $a_{i,j}$. Thus, we can associate a rational map $\phi_{\mathfrak{d}}$ with a divisor $\mathfrak{d}$ only defined up to linear transformation.

If $\mathfrak{d}'$ is linearly equivalent to $\mathfrak{d}$, then there exists a function $g \in \Omega(V)$ such that $\mathfrak{d}' = \mathfrak{d} + (g)$. That means that

$$L(\mathfrak{d}') = \{f \in \Omega(V) : (f) - \mathfrak{d} - (g) \geq 0\}.$$

Since $(f)+(g)=(fg)$, it follows that $L(\mathfrak{d})=gL(\mathfrak{d}')$. If $\{f_0,\ldots,f_r\}$ is a basis for $L(\mathfrak{d}')$, then so is $\{gf_0,\ldots,gf_r\}$ for $L(\mathfrak{d})$. Because we map into projective space, it follows that $\phi_{\mathfrak{d}}=\phi_{\mathfrak{d}'}$.

Therefore, if $\overline{\mathfrak{d}}\in \mathrm{Pic}(V)$, we can define

$$\phi_{\overline{\mathfrak{d}}}: V- \to \mathbb{P}^r$$

up to linear transformation.

If $\phi_{\mathfrak{d}}$ is an immersion, that is, regular and injective, then $\mathfrak{d}$ is said to be *very ample*. If some multiple of $\mathfrak{d}$ is very ample, $\mathfrak{d}$ itself is called *ample*. In [Har77] Chapter 4, Corollary 3.2, it is proved that every divisor on a curve of sufficiently high degree is very ample.

Although $L(\mathfrak{d})$ is defined as an Ω-vector space, we can view it as a k'-vector space, where k' is a finite extension of k such that there is a basis that is defined over k'. In that situation we write $L_{k'}(\mathfrak{d})$ for the k'-linear combinations of these basis elements. For convenience, we will often suppress the reference to k' in the notation.

As Lang notes in [Lan83], if $L(\mathfrak{d})$ and $L(\mathfrak{d}')$ are two spaces without base point with bases $\{f_i\}_{i=1}^n$ and $\{g_j\}_{j=1}^m$, then $L(\mathfrak{d}+\mathfrak{d}')$ is spanned by $\{f_ig_j\}$, where $i=1,\ldots,n$ and $j=1,\ldots,m$. In particular, we do not need a further field extension for $L(\mathfrak{d}+\mathfrak{d}')$.

3.4 Ramification and Genus

Let V be a curve over the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Then V is a curve over some number field K. Let $f\in\bar{\mathbb{Q}}(V)$ be a rational function. We define the *branch number* of f in $x\in V$ by

$$\begin{aligned} b_f(x) &= \mathrm{ord}_x(f-f(x))-1 && \text{if } f(x) \text{ is finite, and}\\ b_f(x) &= \mathrm{ord}_x(\tfrac{1}{f})-1 && \text{if } f \text{ has a pole at } x.\end{aligned}$$

For $\alpha\in K\cup\{\infty\}$ we define the *ramification* of f above α by

$$b_f(\alpha)=\sum_{x:f(x)=\alpha} b_f(x).$$

We have

$$\deg f = \#f^{-1}(\{\alpha\})+b_f(\alpha).$$

Thus, the branch number of a point x on the curve is one less than the multiplicity with which it must be taken in the fiber $f^{-1}(\{f(x)\})$ such that the cardinality of the fiber is exactly the degree of the function.

A curve over a number field can be viewed as a Riemannian surface. The *genus* of a curve is the number of holes in it. This invariant plays an important role in algebraic and arithmetic properties of the curve. For instance, the genus is invariant under birational equivalence. That means we can speak of the genus of a function field. Especially, it means that all rational curves have genus 0, since $\mathbb{P}^1_{\mathbb{C}}$ is a sphere. Conversely, it can be proved that every curve of genus 0 is rational.

The total ramification of a rational function on a curve turns out to be closely connected to the genus of that curve.

Theorem 3.4.1 (Hurwitz) *Let V be a curve of genus g over an algebraically closed field K and let f be a nonconstant rational function on that curve. Then*

$$2\deg f=\sum_{\alpha\in K} b_f(\alpha)+2-2g.$$

Proof: See [Har77] Chapter 4, Corollary 2.4. □

If V is a curve over a number field K, then the theorem above need not be true. However, only finitely many $b_f(\alpha)$ are nonzero for $\alpha \in \bar{\mathbb{Q}}$, so the theorem is true for some finite extension of K, dependent on f.

To avoid any reference to the topology of Riemannian surfaces, we can also read the theorem as: "The total ramification of a rational function on a curve is linearly dependent on the degree of the function", and define the genus as the number that satisfies the stated equation.

For curves over number fields, we have one extra result that shows that we can control where a function is ramified.

Theorem 3.4.2 (Belyi) *Let V be a curve over $\bar{\mathbb{Q}}$. Then there exists a rational function on V that is unramified outside $\{0, 1, \infty\}$. This function can be constructed explicitly.*

Proof: See [Ser90], pages 71–73. □

Chapter 4

Heights and Norms

Fix a field K with a set of primes M_K together with a normalized valuation for each prime such that **PF1** and the product formula **PF2**, are satisfied.

4.1 Heights on Projective Spaces

For the K-rational points in projective space we define the height function

$$\begin{array}{rccc} H: & \mathbb{P}^n_K & \longrightarrow & \mathbb{R} \\ & (x_0 : \ldots : x_n) & \longmapsto & \prod_{P \in M_K} \max_i |x_i|_P. \end{array}$$

This function is well defined since

$$H(\lambda x_0 : \ldots : \lambda x_n) = \prod_{P \in M_K} |\lambda|_P \max_i |x_i|_P = H(x_0 : \ldots : x_n)$$

due to **PF2**. It is often desirable to work with the logarithmic height $h = \log H$.

Let $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n_K$ and $y = (y_0 : \ldots : y_m) \in \mathbb{P}^m_K$. We write

$$x \otimes y := (x_0 y_0 : \ldots : x_0 y_m : \cdots : x_n y_0 : \ldots : x_n y_m) \in \mathbb{P}^{(n+1)(m+1)-1}_K,$$

$x^r := (x_0^r : \ldots : x_n^r)$ and $x^{(r)} := x \otimes \cdots \otimes x$, where the product is taken over r times x.

Proposition 4.1.1 *Let K be a global field and let $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n_K$ and $y = (y_0 : \ldots : y_m) \in \mathbb{P}^m_K$ be projective points. Then we have the following properties:*

i. $H(x \otimes y) = H(x)\, H(y)$,

ii. $H(x^r) = H(x^{(r)}) = H(x)^r$ *and*

iii. *Let $\phi : \mathbb{P}^n_K - \to \mathbb{P}^m_K$ be a rational map of degree d. Then there exists an effectively computable constant $C = C_\phi$ such that for all $x \in \mathbb{P}^n_K$ where ϕ is regular, we have*

$$H(\phi(x)) \leq C\, H(x).$$

Proof:

i.

$$\begin{aligned} H(x \otimes y) &= \prod_{P \in M_K} \max_{i,j} |x_i y_j|_P = \prod_{P \in M_K} \max_{i,j} |x_i|_P |y_j|_P \\ &= \prod_{P \in M_K} \max_{i} |x_i|_P \prod_{P \in M_K} \max_{j} |y_j|_P = H(x)\, H(y). \end{aligned}$$

ii. If $|x_{i_0}|_P = \max_i |x_i|_P$, then $|x_{i_0}|_P^r = \max_{i_1,\ldots,i_r} |x_{i_1} \cdots x_{i_r}|_P$. Therefore it follows that

$$H(x^r) = H(x^{(r)}) = H(x \otimes \cdots \otimes x) = H(x)^r.$$

iii. Let $\phi = (\phi_0 : \ldots : \phi_m)$ be a representation of ϕ where the ϕ_i are homogeneous polynomials of degree d. Then for every $x \in \mathbb{P}^n_K$ where ϕ is regular, there is at least one ϕ_i nonzero at x. We can write

$$\phi_i(x) = (c_{i,1}, \ldots, c_{i,t}) \cdot x^{(d)},$$

where t is the number of entries in the vector $x^{(d)}$ and the product $\cdot$ is the standard inner product of vectors. Using **V3** for valuations, we have

$$\begin{aligned} H(\phi(x)) &= \prod_{P \in M_K} \max_{i} |c_i \cdot x^{(d)}|_P \\ &\leq \prod_{P \in M_K} C_P^{t-1} \max_{i} (\max_{j} |c_{i,j}|_P |(x^{(d)})_j|_P) \\ &\leq \left(\prod_{P \in M_K} C_P^{t-1} \right) H(c_0 : \ldots : c_m)\, H(x)^d. \end{aligned}$$

The proposition follows, since for only finitely many $P \in M_K$, we must choose $C_P > 1$.

□

Note that $\deg \phi$ in iii. is in the sense of Section 3.3 and thus need not correspond to the degree of some associated field extension.

In particular, this means that linear transformations of $\mathbb{P}^n_K$ change the logarithmic height by only a bounded function. Especially, the logarithmic height is only dependent on the choice of coordinates by a bounded function.

Let F be a homogeneous polynomial over K of degree d in $X_0, \ldots, X_n$ such that the coefficient of X_n^d is nonzero. That means that the point $(0 : \ldots : 0 : 1)$ does not lie on the hyperplane determined by F. Let π be the projection from $(0 : \ldots : 0 : 1)$ defined by

$$\begin{array}{rccc} \pi : & \mathbb{P}^n & - \to & \mathbb{P}^{n-1} \\ & (x_0 : \ldots : x_n) & \longmapsto & (x_0 : \ldots : x_{n-1}). \end{array}$$

Proposition 4.1.2 *Let F and π be as above. Then there exists an effectively computable constant C dependent on F such that for any $x \in \mathbb{P}^n_K$ on the hypersurface determined by F, we have*

$$h(x) - C \leq h(\pi(x)) \leq h(x).$$

Proof: As we have $F(x) = 0$, we know that x_n^d is a linear combination of other monomials. The point $x^{(d-1)} \otimes \pi(x)$ contains all those monomials. That means that $x^{(d)}$ is the image of $x^{(d-1)} \otimes \pi(x)$ under some linear map that is determined by F. By Proposition 4.1.1 there exists an effectively computable constant such that

$$h(x^{(d)}) \leq h(x^{(d-1)} \otimes \pi(x)) + C.$$

Rewriting gives

$$d\,h(x) \leq (d-1)h(x) + h(\pi(x)) + C,$$

which proves one inequality. The other one is trivial. □

As changes of coordinates change the logarithmic height only by a bounded function, Proposition 4.1.2 holds for any projection from a point not on the hypersurface, provided that we change the statement to

$$h(x) - C_1 \leq h(\pi(x)) \leq h(x) + C_2.$$

Theorem 4.1.3 *Let $\phi : \mathbb{P}^n_K \to \mathbb{P}^m_K$ be a morphism of degree d. Then there exist effectively computable constants such that for $x \in \mathbb{P}^n_K$ we have*

$$h(\phi(x)) - C_1 \leq d\,h(x) \leq h(\phi(x)) + C_2.$$

Proof: The first inequality follows by Proposition 4.1.1. Take a representation $(\phi_0 : \ldots : \phi_m)$ of ϕ, where the ϕ_i are homogeneous polynomials of degree d. Let $i : \mathbb{P}^n \to \mathbb{P}^t$ be defined by $i : x \mapsto x^{(d)}$. Then $\phi_i(x)$ are linear combinations of the coordinates of $i(x)$. Since the ϕ_i have no zero in common, there exists a combination π of projections from points outside $\phi(\mathbb{P}^n)$ and linear transformations such that $\phi = \pi \circ i$. By Proposition 4.1.2 we have that $h(\pi(y)) \leq h(y) + C_2$ for $y \in \phi(\mathbb{P}^n_K)$. Furthermore, we have that $h(i(x)) = h(x^{(d)}) = d\,h(x)$. Combining proves the second inequality. □

The motivation for defining heights lies in the following theorem.

Theorem 4.1.4 *Let K be a finite extension of $\mathbb{Q}$. Then for any bound B, the number of points $P \in \mathbb{P}^n_K$ such that $H(P) < B$, is finite.*

This is a direct consequence of a theorem by Northcott. It says that we need not to fix an extension of $\mathbb{Q}$ since finiteness also holds if we limit the degree of P over $\mathbb{Q}$. We need a concept of height that is independent of $\mathbb{Q}(P)$ then, though. See [Lan83] Chapter 2, Theorem 2.6 for a proof.

We define height on K itself simply by identifying K with a standard affine part of $\mathbb{P}^1_K$. That means that $h(x) = h(x : 1)$ for $x \in K$.

Example: Put $K = \mathbb{Q}$. For $\frac{r}{s} \in \mathbb{Q}$ with $r, s \in \mathbb{Z}$ and $\gcd(r, s) = 1$ we have $h(\frac{r}{s}) = h(r : s) = \log \max(|r|_\infty, |s|_\infty)$ since for every prime p we have $|r|_p \leq 1$ and $|s|_p \leq 1$ and equality holds in at least one case since p cannot divide both r and s.

As we have seen in section 3.3, a morphism $\phi : \mathbb{P}^1_K \to \mathbb{P}^m_K$ is in fact a projective point over $K(X)$ by writing $\phi = (f_0 : \ldots : f_m)$. Since $K(X)$ is a global field, the height $h\phi = h(f_0 : \ldots : f_m)$ is defined. There is a connection with the degree of a morphism.

Lemma 4.1.5 *Let $\phi = (f_0 : \ldots : f_m)$ be a morphism $\mathbb{P}^1_K \to \mathbb{P}^m_K$. Then*

$$h\phi = \deg \phi.$$

Proof: We write $f_0, \ldots, f_m$ as rational functions of one variable over K. By multiplying with a suitable rational function, we can assure that $f_0, \ldots, f_m$ are polynomials. We can divide out any common factor, so we can assume $\gcd(f_0, \ldots, f_m) = 1$. By definition

$$\deg \phi = \max_i \deg f_i.$$

We write $f_i = a_i g_1^{e_{i,1}} \cdots g_t^{e_{i,t}}$ where $g_1, \ldots, g_t$ are irreducible polynomials and for all j there exist i_1, i_2 such that $e_{i_1,j} = 0$ and $e_{i_2,j} \neq 0$. Of course, $e_{i,j} \geq 0$. By Section 2.2 we know that $M_{K(X)} = \{\infty\} \cup \{$ irreducible polynomials over $K\}$ and that

$$\begin{aligned} \operatorname{ord}_\infty f_i &= -\deg f_i, \\ \operatorname{ord}_{g_j} f_i &= e_{i,j} \text{ and} \\ \operatorname{ord}_P f_i &= 0 \text{ if } P \notin \{\infty, g_1, \ldots, g_t\}. \end{aligned}$$

It follows that

$$\begin{aligned} h(f_0 : \ldots : f_m) &= -\sum_{P \in M_{K(X)}} \min_i \log \mathfrak{N}P \operatorname{ord}_P f_i \\ &= -\min_i \operatorname{ord}_\infty f_i - \sum_{j=1}^{t} \min_i \deg g_j \operatorname{ord}_{g_j} f_i \\ &= \max_i \deg f_i - \sum_{j=1}^{t} \min_i e_{i,j} \deg g_j \\ &= \max_i \deg f_i = \deg \phi. \end{aligned}$$

□

4.2 Heights on Curves

Let V be a curve over K. We can define a height on V by embedding V in some $\mathbb{P}^n$. For every morphism

$$\phi : V \longrightarrow \mathbb{P}^n$$

we have a height on V, defined by $h_\phi = h \circ \phi$, where h is the height on $\mathbb{P}^n_K$.

For every very ample divisor on V we have such a morphism, defined up to linear transformation. By combining this with Theorem 4.1.3 we therefore get a height function for every very ample divisor, defined up to a bounded function. As we have seen, changing to a linearly equivalent divisor does not change the morphism and thus does not change the associated height. Furthermore, we have for divisors without base point and in particular for very ample divisors, that $L(\mathfrak{d}_1 + \mathfrak{d}_2) = L(\mathfrak{d}_1) \otimes L(\mathfrak{d}_2)$. This implies that $\phi_{\mathfrak{d}_1+\mathfrak{d}_2} = \pi \circ (\phi_{\mathfrak{d}_1} \otimes \phi_{\mathfrak{d}_2})$ for some linear map π that is regular on the image of V, and therefore that $h_{\mathfrak{d}_1+\mathfrak{d}_2} = h_{\mathfrak{d}_1} + h_{\mathfrak{d}_2} + O(1)$.

We associate height functions modulo bounded functions first with all very ample divisors and then with all divisors by enforcing additivity. We get the group homomorphism

$$\begin{array}{ccc} \mathrm{Pic}(V) & \longrightarrow & \{\text{real valued functions on } V\}/\{\text{bounded functions on } V\} \\ \overline{\mathfrak{d}} & \longmapsto & h_{\overline{\mathfrak{d}}} + O(1) = h_{\phi_{\overline{\mathfrak{d}}}} + O(1) \end{array}$$

such that $h_{\overline{\mathfrak{d}}_1+\overline{\mathfrak{d}}_2} = h_{\overline{\mathfrak{d}}_1} + h_{\overline{\mathfrak{d}}_2} + O(1)$.

On curves, the height associated to a divisor is almost completely determined by the degree of the divisor.

Theorem 4.2.1 *Let V be a curve over K and let $\mathfrak{d}_1, \mathfrak{d}_2 \in \mathrm{Div}_K(V)$. Then for every $\epsilon > 0$ there exist constants C_1, C_2 such that for all $P \in V$ it holds that*

$$(1-\epsilon)\deg(\mathfrak{d}_2)h_{\mathfrak{d}_1}(P) + C_1 \leq \deg \mathfrak{d}_1 h_{\mathfrak{d}_2}(P) \leq (1+\epsilon)\deg(\mathfrak{d}_2)h_{\mathfrak{d}_1}(P) + C_2$$

Proof: See [Lan83] Chapter 4, Corollary 3.5. □

The height associated to a zero divisor of a rational function is essentially the same as the height the function induces itself.

Proposition 4.2.2 *Let V be a curve over K and let f be a rational function on that curve. Then*

$$h(f(x)) = h(\frac{1}{f}(x)) = h_{(f)_0}(x) + O(1).$$

Proof: The first equality is obvious. Choose an m such that $m(f)_0$ is very ample. Since $(\frac{1}{f})_\infty = (f)_0$, we have that $\frac{1}{f^m} \in L(m(f)_0)$. Since $(f)_0$ is a positive divisor, we have that $1 \in L(m(f)_0)$ as well. Take a basis $\{1, \frac{1}{f^m}, g_1, \ldots, g_r\}$ for $L(m(f)_0)$. No g_i can have a pole of higher order than $\frac{1}{f^m}$ has. Therefore $(0:0:x_1:\ldots:x_r) \notin V$ for any $(x_1:\ldots:x_r)$ if V is identified with its embedding. Proposition 4.1.2 implies that projection onto the first two coordinates changes the height function only by a bounded function. That means that

$$h(f(x)) = h(1:\frac{1}{f}(x)) = h(1:\frac{1}{f}(x):g_1(x):\ldots:g_r(x)) + O(1),$$

which is exactly what we had to prove. □

4.3 Support and Norm

Notice that the definition of norm of a discrete prime is such that $\mathfrak{N}P^{\mathrm{ord}_P(x)} = |x|_P$. Since the ordinal function is integer valued, the definition of the norm could be rewritten as

$$\mathfrak{N}P = \inf\{|x|_P : x \in K, |x|_P > 1\}$$

or, equivalently,

$$\frac{1}{\mathfrak{N}P} = \sup\{|x|_P : x \in K, |x|_P < 1\}.$$

This allows us to extend the definition of norm to all primes in M_K. For nondiscrete primes this implies that $\mathfrak{N}P = 1$. The most important property of the norm still holds. If $|x|_P \neq 1$ then $|\log|x|_P| \geq \log \mathfrak{N}P$.

The support of a projective point $x \in \mathbb{P}^n_K$ is the set

$$\mathrm{Supp}(x) = \mathrm{Supp}(x_0 : \dots x_n) := \{P \in M_K : \max_i |x_i|_P > \min_i |x_i|_P\}.$$

The norm of a projective point $x \in \mathbb{P}^n_K$ is defined by

$$N(x) := \prod_{P \in \mathrm{Supp}(x)} \mathfrak{N}P.$$

Notice that nondiscrete primes never contribute to the norm of a projective point, since their own norm equals 1. It turns out that this is no problem because the fields of our interest either have no nondiscrete valuation (function fields) or have only finitely many (number fields).

Example: Put $K = \mathbb{Q}$. For $\frac{r}{s} \in \mathbb{Q}^*$ with $\gcd(r, s) = 1$ we have

$$N(\frac{r}{s}) = N(r : s) = \prod_p p$$

where p runs over the prime divisors of r and s. If $s = 1$, this means that $N(r)$ is the generator of the radical ideal associated with $r \in \mathbb{Z}$.

Example: If $K = k(X)$, then $\log N(f)$ is the sum of the degrees of the different irreducible polynomials that occur in the factorization of f. If K is algebraically closed and f is a polynomial, then $\log N(f)$ is the number of different zeros of f.

4.4 Weil Functions

In order to examine how a prime contributes to the height of a point on a curve, we need a slight reformulation of height on curves. Weil functions as treated in [Lan83] are the appropriate language for this.

We define an M_K-*constant* to be a function $\gamma : M_K \to \mathbb{R}$ such that $\gamma(P) \neq 0$ for only finitely many $P \in M_K$.

Let V be a nonsingular curve over K and let $\mathfrak{d}$ be a divisor without base point. Let $\{f_0, \dots f_r\}$ be a basis of $L(\mathfrak{d})$. We associate a function with $\mathfrak{d}$ by defining

$$\begin{array}{rccc} \lambda_{\mathfrak{d}} : & V \times M_K & \longrightarrow & \mathbb{R} \\ & (x, P) & \longmapsto & \log \max(|f_0(x)|_P, \dots, |f_r(x)|_P). \end{array}$$

We call $\lambda_{\mathfrak{d}}$ the *Weil function* associated to $\mathfrak{d}$. The definition is clearly dependent on the choice of the basis $\{f_0, \dots, f_r\}$. Let $\lambda'_{\mathfrak{d}}$ be defined using another basis $\{g_0, \dots, g_r\}$ of $L(\mathfrak{d})$. Write

$$f_i = \sum_{j=0}^{r} c_{i,j} g_j.$$

Then

$$\begin{aligned} \lambda_{\mathfrak{d}}(x, P) &= \log \max_i (|\sum c_{i,j} g_j(x)|_P) \\ &\leq \log \max_i (C_P^{r-1} \max_{i,j} (|c_{i,j} g_j(x)|_P) \\ &\leq (r-1) \log C_P + \log \max_{i,j} (|c_{i,j}|_P) + \lambda'_{\mathfrak{d}}(x, P). \end{aligned}$$

Since $\log \max_{i,j}(|c_{i,j}|_P) \neq 0$ for only finitely many P and we can choose C_P such that $\log C_P \neq 0$ for only finitely many P as well, we have that

$$\lambda_{\mathfrak{d}}(x,P) - \gamma_1(P) \leq \lambda'_{\mathfrak{d}}(x,P) \leq \lambda_{\mathfrak{d}}(x,P) + \gamma_2(P),$$

where γ_1 and γ_2 are M_K-constants. In this sense, Weil functions are defined up to M_K-constants.

It is easily checked that for base point free divisors $\mathfrak{d}_1, \mathfrak{d}_2$ it holds that

$$\lambda_{\mathfrak{d}_1+\mathfrak{d}_2}(x,P) = \lambda_{\mathfrak{d}_1}(x,P) + \lambda_{\mathfrak{d}_2}(x,P) + \gamma(P),$$

where $\gamma(P)$ is more or less formal to denote that the quantities involved are only defined up to M_K-constants. Furthermore, it is clear that

$$h_{\mathfrak{d}}(x) = \sum_{P \in M_K} \lambda_{\mathfrak{d}}(x,P) + \sum_{P \in M_K} \gamma(P) = \sum_{P \in M_K} \lambda_{\mathfrak{d}}(x,P) + O(1)$$

and that either $\lambda_{\mathfrak{d}}(x,P) = 0$ or $|\lambda_{\mathfrak{d}}(x,P)| \geq \log \mathfrak{N}P$.

Since divisors of sufficiently high degree are very ample, we have in particular that every divisor can be written as the difference of two base point free divisors. It may be necessary to make a finite field extension for this. We use this to associate a Weil function with any divisor. We still have that $\lambda_{\mathfrak{d}}(x,P)$ does not take nonzero values between $-\log \mathfrak{N}P$ and $\log \mathfrak{N}P$.

If $\mathfrak{d}$ is positive and $\mathfrak{d}_1$ and $\mathfrak{d}_2$ are divisors without base point such that $\mathfrak{d} = \mathfrak{d}_1 - \mathfrak{d}_2$, then we know that $\mathfrak{d}_2 \leq \mathfrak{d}_1$ and thus $L(\mathfrak{d}_1) \subseteq L(\mathfrak{d}_2)$. It follows that

$$\lambda_{\mathfrak{d}}(x,P) = \lambda_{\mathfrak{d}_1}(x,P) - \lambda_{\mathfrak{d}_2}(x,P) + \gamma(P) \geq 0 + \gamma(P)$$

by choosing a basis for $L(\mathfrak{d}_2)$ and extending it to a basis for $L(\mathfrak{d}_1)$.

Chapter 5

ABC over Global Fields

Let K be a global field and let M_K be the usual set of primes. Assume that K has characteristic zero.

5.1 Formulation

We define

$$L_K := \left\{ \frac{h(a:b:c)}{\log N(a:b:c)} : a,b,c \in K^*;\ A+B+C=0 \right\}.$$

Note: If K is of characteristic p, then $a^p+b^p+c^p = (a+b+c)^p = 0$. We have $h(a^p : b^p : c^p) = p\,h(a:b:c)$ and $\log N(a^p : b^p : c^p) = \log N(a:b:c)$. In this case, we cannot hope that L_K is bounded. The only global fields of positive characteristic are function fields. The problem above can be remedied by demanding that the derivatives of a, b and c are nonzero. Then the definition for L_K would be different for function fields and number fields. Therefore, we choose to exclude fields of positive characteristic in favor of uniformity for zero characteristic.

Conjecture 5.1.1 (weak ABC) *It holds that* $\limsup L_K < \infty$.

Conjecture 5.1.2 (ABC ineffective) *It holds that* $\limsup L_K = 1$.

Lemma 5.1.3 *The following statements are equivalent.*

i. For all $\epsilon > 0$ there exists an effectively computable constant $D = D_{\epsilon,K}$ such that $a,b,c \in K^*$, $a+b+c=0$ and

$$\frac{h(a:b:c)}{\log N(a:b:c)} > 1+\epsilon$$

implies that $h(a:b:c) \le D$.

ii. For all $\epsilon > 0$ there exists an effectively computable constant $C = C_{\epsilon,K}$ such that for all $a,b,c \in K^*$ such that $a+b+c=0$ we have

$$h(a:b:c) \le (1+\epsilon)\log N(a:b:c) + C.$$

Proof:

i. $\Rightarrow$ *ii.* If $h(a:b:c) > D$, then the implication is obvious. In the other case, we have $D \geq h(a:b:c)$. Since $\log N(a:b:c)$ is effectively bounded below for $(a:b:c)$ that have a discrete prime in their support, the implication follows.

i. $\Leftarrow$ *ii.* Take C such that $h(a:b:c) \leq (1+\frac{1}{2}\epsilon)\log N(a:b:c) + C$. If $\frac{h(a:b:c)}{\log N(a:b:c)} > 1+\epsilon$, then $1+\frac{1}{2}\epsilon \leq (1+\frac{1}{2}\epsilon)\log N + C$. Then we have $\log N(a:b:c) \leq 2\frac{C}{\epsilon}$. This puts an effective bound on $h(a:b:c) \leq (1+\frac{1}{2}\epsilon)N + C$. □

Conjecture 5.1.4 (ABC effective) *The statements in Lemma 5.1.3 are true.*

R.C. Mason has proved in [Mas84] that conjecture 5.1.4 holds if K is a function field. He even proved it under appropriate restrictions if K is of positive characteristic.

Theorem 5.1.5 (Mason) *Let K be a function field of genus g and let $f_1, f_2, f_3 \in K$ be functions, not all constant, such that $f_1 + f_2 = f_3$. Then*

$$h(f_1 : f_2) \leq \#\mathrm{Supp}(f_1 : f_2 : f_3) + 2g - 2$$

Proof: See [Mas84] Chapter 1, §3, Lemma 2. □

Since in case of function fields we can assume $\log \mathfrak{N}P \geq 1$ for all $P \in M_K$, it follows that $\log N(f_1 : f_2 : f_3) \geq \#\mathrm{Supp}(f_1 : f_2 : f_3)$. Since $(f_1 : f_2) \mapsto (f_1 : f_2 : f_1 + f_2)$ is a linear morphism, we have by 4.1.3 that $h(f_1 : f_2 : f_3) = h(f_1 : f_2) + C_2$ for some explicit constant C_2. Thus, statement *ii.* of Lemma 5.1.3 follows.

5.2 ABC implies Mordell

Mordell conjectured the following theorem, that was proved by Faltings.

Theorem 5.2.1 (Faltings) *Let V be a curve of genus g over a number field K. If $g \geq 2$ then V only has finitely many K-rational points.*

This is a very important result. For example, it proves ineffective Fermat, since it can be proved that the genus of the curve described by $X^n + Y^n = Z^n$ is at least 2 for $n \geq 4$. This section shows that it is not a coincidence that also the ABC-conjecture implies Fermat by showing that ABC implies Theorem 5.2.1. The proof described here is a more detailed version of the one N.D. Elkies wrote in [Elk91].

Let $\phi_0 = (-X : 1 : X - 1)$ be the linear map that maps every $\alpha \in K \setminus \{0, 1\}$ onto an ABC-example.

Let V be a curve of genus g over a number field K. If we can find a function f on V such that $\#f^{-1}(\{0, 1, \infty\}) < \deg f$ for curves with $g \geq 2$ and if we can prove the inequality

$$\log N(\phi_0(f(x))) \leq (1+\epsilon)\frac{\#f^{-1}(\{0\}) + \#f^{-1}(\{1\}) + \#f^{-1}(\{\infty\})}{\deg f} h(\phi_0(f(x))) + C_\epsilon$$

for every $\epsilon > 0$ then it would follow that ABC implies Theorem 5.2.1.

We factor $N(\phi_0(\alpha))$ into

$$N(\phi_0(\alpha)) = N_0(\alpha)N_1(\alpha)N_\infty(\alpha),$$

where

$$\begin{aligned} N_0(\alpha) &= \prod_{P \in M_K : |\alpha|_P < 1} \mathfrak{N}P, \\ N_1(\alpha) &= N_0(\alpha - 1) \text{ and} \\ N_\infty(\alpha) &= N_0(\frac{1}{\alpha}). \end{aligned}$$

Proposition 5.2.2 (Elkies) *Let V be a curve over K and let $f \in K(V)$ be a rational function on V. Then for every $\epsilon > 0$ there exists an effectively computable constant C_ϵ such that for all $x \in V_K \setminus f^{-1}(\{0\})$ we have*

$$\log N_0(f(x)) \leq (1+\epsilon)\frac{\deg f - b_f(0)}{\deg f} h(f(x)) + C_\epsilon.$$

Proof: Although we only need the proposition for curves of high genus, it is instructive to see the proof for rational curves. Therefore, first assume V has genus 0. Then $h(f(x)) = \deg(f)h(x) + C_1$. Write $f(\frac{x}{y})$ as $\frac{F(x,y)}{G(x,y)}$ and factor F over K as $F = w\prod_k F_k$ with $w \in K^*$ and F_k irreducible polynomials over K of degrees d_k. Without loss of generality, we can assume that the coefficients of G are K-integers.

Take $z \in K$. We can write $z = \frac{x}{y}$ with x, y K-integers. Therefore, the primes where $\frac{F(x,y)}{G(x,y)}$ is a local integer and not a local unit form a subset of the places where $F(x,y)$ is. It follows that

$$\begin{aligned} \log N_0(f(\frac{x}{y})) &= \log N_0(\frac{F(x,y)}{G(x,y)}) \leq \log N_0(F(x,y)) = \sum_k \log N_0(F_k(x,y)) \\ &\leq \sum_k h(F_k(x,y)) + C_1 \leq \sum_k d_k h(x:y) + C_1. \end{aligned}$$

Since we have that $\deg f = \sum_k m_k d_k$, $b_f(0) = \sum_k (m_k - 1)$ and $h(x:y) = \frac{1}{\deg f} h(f(\frac{x}{y})) + C_2$, the proposition follows with C_ϵ independent of ϵ.

Now assume V has genus g. Define $\mathfrak{d} := (f)_0$ and write $\mathfrak{d} = \sum_k m_k \mathfrak{p}_k$, where the $\mathfrak{p}_k$ are prime rational divisors over K of degrees d_k. We have $\deg f = \sum_k m_k d_k = \deg \mathfrak{d}$. Since we are working over a number field, field extensions are separable and thus no points in $\mathfrak{p}_k$ occur with higher multiplicity than one. Therefore, any multiple zeros of f must be due to repeated irreducible factors. That means we have $b_f(0) = \deg f - \sum_k d_k$. By Proposition 4.2.2 we have

$$h(f(x)) = h_{\mathfrak{d}}(x) + C_1 = \sum_k m_k h_{\mathfrak{p}_k}(x) + C_1,$$

where C_1 is effective after explicit choice of the morphism that defines $h_{\mathfrak{d}}$. Write $\mathfrak{d}' = \sum_k \mathfrak{p}_k$. We can express the ramification above 0 as $b_f(0) = \deg \mathfrak{d} - \deg \mathfrak{d}'$.

We assume that we are working over a large enough field K such that all $\mathfrak{p}_k$ can be written as the difference of divisors $\mathfrak{d}_{k,1}, \mathfrak{d}_{k,2}$ for which the vector spaces $L(\mathfrak{d}_{k,1})$ and $L(\mathfrak{d}_{k,2})$ have bases that are defined over K.

The following argument was pointed out by J.H. Evertse. If P contributes to $\log N_0(f(x))$, then $|f(x)|_P < 1$, or equivalently $|\frac{1}{f}(x)|_P > 1$. Since $\frac{1}{f} \in L(\mathfrak{d})$, we have that $\lambda_{\mathfrak{d}}(x,P) \geq \log \mathfrak{N}P$. Since

$$\lambda_{\mathfrak{d}}(x,P) = \sum_k m_k \lambda_{\mathfrak{p}_k}(x,P) + \gamma(P),$$

there exists a k such that $\lambda_{\mathfrak{p}_k}(x,P) \geq \log \mathfrak{N}P$. We have that $\lambda_{\mathfrak{p}_k}(x,P) \geq -\gamma_k(P)$ because $\mathfrak{p}_k$ is a positive divisor. Therefore, we have

$$\begin{aligned}
\sum_k \lambda_{\mathfrak{p}_k}(x,P) \geq & \quad \log \mathfrak{N}P - \textstyle\sum_k \gamma_k(P) \qquad \text{for } P : |f(x)|_P < 1 \text{ and} \\
\sum_k \lambda_{\mathfrak{p}_k}(x,P) \geq & \qquad - \textstyle\sum_k \gamma_k(P) \qquad\quad \text{for } P : |f(x)|_P \geq 1.
\end{aligned}$$

If we sum over all $P \in M_K$, we get

$$h_{\mathfrak{d}'}(x) = \sum_{p \in M_K} \lambda_{\mathfrak{d}'}(x,P) \geq \sum_{P:|f(x)|_P<1} \log \mathfrak{N}P - \sum_{P \in M_K} \gamma_k(P) = N_0(f(x)) - C_2.$$

By Theorem 4.2.1 we have

$$h_{\mathfrak{d}'} \leq \frac{\deg \mathfrak{d}'}{\deg \mathfrak{d}}(1+\epsilon)h_{\mathfrak{d}}(x) + C_{3,\epsilon}.$$

Combining these results then gives

$$\log N_0(f(x)) \leq (1+\epsilon)\frac{\deg f - b_f(0)}{\deg f} h(f(x)) + C_\epsilon.$$

□

Theorem 5.2.3 (Elkies) *Effective and ineffective versions of the ABC-conjecture imply respective versions of Theorem 5.2.1.*

Proof: Suppose we have a curve V over a number field K of genus $g \geq 2$ with infinitely many K-rational points. Theorem 3.4.2 ensures the existence of a rational function f on that curve that is unramified outside $\{0,1,\infty\}$. Since extending K would only increase the number of K-rational points on V, we can safely assume that $f \in K(V)$. By Theorem 3.4.1 we have

$$b_f(0) + b_f(1) + b_f(\infty) = 2\deg f + 2g - 2.$$

By Proposition 5.2.2 and the fact that $h(f(x)) = h(\frac{1}{f}(x)) = h(f(x)+1)+O(1) = h(\phi_0(f(x)))+O(1)$ with the $O(1)$ functions effectively bounded, we have

$$\begin{aligned}
\log N(\phi_0(f(x))) &= \log N_0(f(x)) + \log N_1(f(x)) + \log N_\infty(f(x)) \\
&\leq (1+\epsilon)\frac{3\deg f - b_f(0) - b_f(1) - b_f(\infty)}{\deg f} h(\phi_0(f(x))) + C_\epsilon.
\end{aligned}$$

For brevity, write $h := h(\phi_0(f(x)))$ and $lN := \log N(\phi_0(f(x)))$. We have

$$\frac{h}{lN} \geq \frac{1}{1+\epsilon}\frac{\deg f}{\deg f - 2g + 2}\left(1 - \frac{C_\epsilon}{lN}\right).$$

Pick a $\delta > 0$. Choose ϵ such that we have

$$\frac{h}{lN} > (1+\delta)\left(1 - \frac{C_\epsilon}{lN}\right).$$

By the ABC-conjecture, we have a D (effective or ineffective) such that if $h > D$, then $\frac{h}{lN} \leq 1 + \frac{1}{2}\delta$. Then

$$1 + \frac{1}{2}\delta > (1+\delta)\left(1 - \frac{C_\epsilon}{lN}\right),$$

which puts an effective bound on lN and thereby on $h > D$. If D is ineffective, then we do not get an effective bound on h.

We see that for $x \in V_K$ we have that $h(\phi_0(f(x)))$ is bounded. By 4.1.4, we have that $\phi_0(f(V_K))$ is finite. Since $\phi_0 \circ f$ is a nonconstant rational map from a curve, this implies that V_K itself is finite. □

No effective version of Theorem 5.2.1 exists yet.

Chapter 6

N-conjecture

In this section we will generalize the ABC-conjecture to more variables. Let K be a global field of characteristic 0 and let M_K be the usual set of primes.

6.1 Divisibility

We return to the ABC-conjecture over $\mathbb{Z}$ for now. There we demand that $\gcd(A, B, C) = 1$ for obvious reasons. We then conjecture that

$$\frac{\log \max(|A|, |B|, |C|)}{\log R(ABC)}$$

is bounded for $A + B = C$. The divisibility demand in this case is equivalent with demanding that A, B and C are pairwise coprime. This is not so for more than three variables.

We could assume that all terms are pairwise coprime, but that would exclude examples like $125 - 90 - 27 - 8 = 0$, which seem perfectly valid. On the other hand we could just assume that there is no factor in common to all terms. Then we wouldn't exclude examples like

$$11^{\lambda}(2 + 3 - 5) + 13^{\mu}(7 + 2 - 9) = 0 \ (\lambda, \mu \in \mathbb{N})$$

which would be counterexamples to all conceivable generalizations of the ABC-conjecture.

The minimal demand to exclude that type of example is that vanishing subsums may not have terms that have any factor in common. That means that if $x_1, \ldots, x_n \in \mathbb{Z}$ is a good example for the n-conjecture over $\mathbb{Z}$, then $\sum_{i=1}^{n} x_i = 0$ and for every subset $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} x_i = 0$, it holds that $\gcd_{i \in I}(x_i) = 1$.

If a proper subsum for $x_1, \ldots x_n$ does vanish, then so does the complementary sum, consisting of all terms not included in the subsum. That means that that particular example is in fact the sum of an m-example and an $(n-m)$-example. We can then use the m-conjecture and the $(n-m)$-conjecture to get information about the structure of this example.

Therefore, we will consider such examples degenerate and we formulate the n-conjecture for nondegenerate examples. That means that we will assume that no proper subsum vanishes. Divisibility demands then become simply that no factors divide all terms. Put more generally, it means that examples can be considered to be projective points, meaning that scalar multiplication doesn't really change the example. The next section will make all of this precise.

6.2 Formulation

It is most convenient to formulate the n-conjecture in terms of height and norm of projective points. The set of nondegenerate examples is then naturally described in terms of hyperplanes.

Let K be a global field of characteristic zero. We define

$$W^n_{K,I} := \left\{ (x_1 : \ldots : x_n) \in \mathbb{P}^{n-1}_K : \sum_{i \in I} x_i = 0 \right\} \text{ for } I \subset \{1, \ldots, n\}.$$

For convenience we write

$$V^n_K := W^n_{K,\{1,\ldots,n\}}\ ,\ W^n_K := \bigcup_{\emptyset \subsetneq I \subsetneq \{1,\ldots,n\}} W^n_{K,I}$$

The set $V^n_K \setminus W^n_K$ is called the set of nondegenerate n-examples. Note that if K is a number field, every nondegenerate n-example has a representative $(x_1, \ldots, x_n)$ with $\sum_{i=1}^n x_i = 0$, no proper subsum vanishes, all x_i are K-integers and $\gcd((x_1), \ldots, (x_n)) = (1)$.

We define

$$L_{n,K} := \left\{ \frac{h(x_1 : \ldots : x_n)}{\log N(x_1 : \ldots : x_n)} : (x_1 : \ldots : x_n) \in V^n_K \setminus W^n_K \right\}.$$

Note that the above quotient is not defined if $|x_1|_P = \ldots = |x_n|_P$ at all primes $P \in M_K$. The logarithmic height of such points equals zero as well. We tacitly exclude these points.

Conjecture 6.2.1 (weak n-conjecture) *It holds that* $\limsup L_{n,K} < \infty$.

If $n = 3$ this is the weak ABC-conjecture over K. In this case it is convenient to note that

$$V^3_K = \mathbb{P}^1_K = K \cup \{\infty\}.$$

It follows that

$$V^3_K \setminus W^3_K = \mathbb{P}^1_K \setminus \{0, 1, \infty\} = K \setminus \{0, 1\}$$

by the parametrization $x \mapsto (-x : -1 : x + 1)$.

Similar to the ABC-conjecture, if K is a function field, this is not a conjecture anymore. Brownawell and Masser have proved it in [BM86].

Theorem 6.2.2 (Brownawell, Masser) *Let K be a function field. Then*

$$h(x_1 : \ldots : x_n) \leq \frac{1}{2}(n-1)(n-2)\left(\#\mathrm{Supp}(x_1 : \ldots : x_n) + \max(2g - 2, 0)\right)$$

6.3 Nondegenerate Embeddings

Let K be a number field. We shall show a connection between the n-conjecture over K and the n-conjecture over $K(X)$. In fact, it turns out that the first implies the latter. Technically this is of little value since the latter is proved while the first is not. However, the connection is a quantitative one, so any lower bound in the function field case gives rise to a similar one for K.

Let $(f_1 : \ldots : f_n)$ be a nondegenerate n-example over $K(X)$. Since the n-conjecture is trivial if all f_i are constant or equal, we assume this is not the case. That means

$$\begin{array}{rccc} \phi = (f_1 : \ldots : f_n) : & \mathbb{P}^1_K & \longrightarrow & \mathbb{P}^{n-1}_K \\ & x & \longmapsto & (f_1(x) : \ldots : f_n(x)) \end{array}$$

is nonconstant and, in particular, $\phi \neq (0 : \ldots : 0)$. Thus ϕ is a morphism. Since $\phi \in V^n_{K(X)}$, it follows that $\phi(x) \in V^n_K$ for all $x \in \mathbb{P}^1_K$. Similarly, $\phi \notin W^n_{K(X)}$ implies that there are $x \in \mathbb{P}^1_K$ such that $\phi(x) \notin W^n_K$. Because $\phi(\mathbb{P}^1_K)$ is a curve, we can conclude that $\phi(\mathbb{P}^1_K) \cap W^n_K$ is a finite set. We call ϕ a nondegenerate embedding of $\mathbb{P}^1_K$ into the set of n-examples, since all but finitely many points are mapped to nondegenerate n-examples. Every nondegenerate n-example over $K(X)$ thus gives rise to a nondegenerate embedding.

We choose coordinates such that $\mathbb{P}^1_K = K \cup \{\infty\}$. Without loss of generality we can assume that all f_i are polynomials. We write f_i with K-integer coefficients. Since any common factors can be divided out, we can assume that $\gcd(f_1, \ldots, f_n) = 1$ and thus we can write

$$f_i = a_i \, g_1^{e_{i,1}} \cdots g_t^{e_{i,t}}$$

where $g_1, \ldots, g_t$ are distinct irreducible polynomials over K with K-integer coefficients such that for every j there are i_1, i_2 such that $e_{i_1,j} = 0$ and $e_{i_2,j} \neq 0$. Naturally, all $e_{i,j} \geq 0$. We define

$$\psi := \prod_{j=1}^{t} g_j.$$

Lemma 6.3.1 *Let ψ and ϕ be defined as above. Then*

$$\log N\phi = \deg \psi \text{ or } \log N\phi = \deg \psi + 1.$$

Proof: We have

$$\mathrm{Supp}(\psi : 1) = \{\infty\} \cup \{g_j\}_{j=1}^t.$$

and

$$\mathrm{Supp}\phi = \{g_j\}_{j=1}^t \text{ or } \mathrm{Supp}\phi = \{\infty\} \cup \{g_j\}_{j=1}^t$$

according to whether the f_i are of equal degree or not. Since $\log \mathfrak{N}\infty = 1$ it follows that $\log N\phi = \log N(\psi : 1)$ or $\log N\phi = \log N(\psi : 1) - 1$. The lemma follows by noting that $\log N(\psi : 1) = 1 + \sum_{i=1}^t \deg g_i = \deg \psi + 1$. □

In the following lemmas the norm and height are the ones defined on K, not on $K(X)$.

Lemma 6.3.2 *Let ψ and ϕ be defined as above. Then*

$$\log N\phi(x) \leq \log N\psi(x) + O(1)$$

for all $x \in K$.

Proof: We claim that there is a finite subset E of M_K such that for all $P \in M_K \setminus E$, we have that $|f_i(x)|_P = |a_i \, g_1^{e_{i,1}}(x) \cdots g_t^{e_{i,t}}(x)|_P \neq 1$ implies that $|\psi(x)|_P \neq 1$. It then follows that $\mathrm{Supp}\phi(x) \subseteq \mathrm{Supp}\psi(x) \cup E$, because if $P \in \mathrm{Supp}\phi(x)$ then there exist i_1, i_2 such that $|f_{i_1}(x)|_P \neq |f_{i_2}(x)|_P$, thus there is an i such that $|f_i(x)|_P \neq 1$. Using the claim it follows that

$$\log N\phi(x) \leq \log N\psi(x) + \sum_{P \in E} \log \mathfrak{N}P$$

where the last term is a fixed, and in fact effectively computable, constant.

It remains to prove the claim. Define $P \in E$ if $|a_i|_P \neq 1$ for some $i \in \{1, \ldots, n\}$ or if $|p|_P \neq 1$ for p the coefficient of the leading term of $\prod_{j \in J} g_j$ where J is some subset of $\{1, \ldots, n\}$ or if P is archimedean. Fix any $P \in M_K \setminus E$ and assume that $|f_i(x)|_P \neq 1$. Then $|g_j(x)|_P \neq 1$ for some j, because $|a_j|_P \neq 1$ is excluded.

If the claim were not true for P, we would have $|\psi(x)|_P = |\prod_{j=1}^{t} g_j(x)|_P = 1$. It then follows that there exist j_1, j_2 such that $|g_{j_1}(x)|_P < 1$ and $|g_{j_2}(x)|_P > 1$. We split the product into

$$Q_1(X) = \prod_{j:|g_j(x)|_P<1} g_j(X) = p_k X^k + \cdots + p_0$$

and

$$Q_2(X) = \prod_{j:|g_j(x)|_P>1} g_j(X) = q_l X^l + \cdots + q_0$$

which are nonconstant polynomials of degree k and l. Write $x = \frac{r}{s}$ with $r, s \in K$ integers such that $|r|_P = 1$ or $|s|_P = 1$.

If $|s|_P = 1$ then, by $|Q_2(\frac{r}{s})|_P > 1$, we have

$$|q_l r^l + \cdots + q_0 s^l|_P > |s|_P^l = 1$$

which contradicts the fact that $s^l Q_2(\frac{r}{s})$ is a K-integer.

If $|s|_P \neq 1$ then $|r|_P = 1$. By $|Q_1(\frac{r}{s})|_P < 1$ we have

$$|p_k r^k + s(p_{k-1} r^{k-1} + \cdots + p_0 s^{k-1})|_P < |s|_P^k < 1,$$

thus

$$\begin{aligned} |p_k r^k|_P &\leq \max(|p_k r^k + s(p_{k-1} r^{k-1} + \cdots + p_0 s^{k-1})|_P), |s(p_{k-1} r^{k-1} + \cdots + p_0 s^{k-1})|_P \\ &< 1 \end{aligned}$$

which contradicts the fact that $|p_k|_P = 1$ and $|r|_P$=1. □

Lemma 6.3.3 *Let $\psi(X) \in K[X]$ be a polynomial with K-integer coefficients. Then*

$$\log N\psi(x) \leq h(x) + h(\psi(x))$$

for all $x \in K$.

Proof: The key to this proof is the fact that if $|x|_P \neq 1$ then $|\log |x|_P| \geq \log \mathfrak{N}P$. We have

$$h\psi(x) = \sum_{P:|\psi(x)|_P>1} \log |\psi(x)|_P = \sum_{P:|\psi(x)|_P<1} -\log |\psi(x)|_P$$

because $\sum_{P \in M_K} \log |\psi(x)|_P = 0$ by **PF2**. Furthermore

$$h(x) = \sum_{P:|x|_P>1} \log |x|_P \geq \sum_{P:|\psi(x)|_P>1} \log |x|_P$$

because $|x|_P \leq 1$ implies that $|\psi(x)|_P \leq 1$ since ψ has integer coefficients. Combining this gives us

$$\begin{aligned}\log N\psi(x) &= \sum_{P:|\psi(x)|_P \neq 1} \log \mathfrak{N}P \\ &= \sum_{P:|\psi(x)|_P > 1} \log \mathfrak{N}P + \sum_{P:|\psi(x)|_P < 1} \log \mathfrak{N}P \\ &\leq h(x) + h\psi(x).\end{aligned}$$

□

Theorem 6.3.4 *Let K be a number field and let ϕ be a nondegenerate n-example over $K(X)$. Then*

$$\limsup L_{n,K} \geq \frac{h\phi}{\log N\phi + 1}.$$

Proof: By the lemmas and Theorem 4.1.3 we have for every $x \in K$

$$\begin{aligned}\frac{h\phi(x)}{\log N\phi(x)} &\geq \frac{h\phi(x)}{\log N\psi(x) + O(1)} \\ &\geq \frac{h\phi(x)}{h(x) + h\psi(x) + O(1)} \\ &= \frac{h(x)\ \deg\phi + O(1)}{(\deg\psi + 1)h(x) + O(1)} \\ &\geq \frac{h(x)\ \deg\phi + O(1)}{(\log N\phi + 1)h(x) + O(1)}.\end{aligned}$$

By taking a sequence of $x \in K$ such that $h(x) \to \infty$ it follows that

$$\limsup L_{n,K} \geq \frac{h\phi}{\log N\phi + 1}$$

because of Lemma 4.1.5. □

Corollary 6.3.5 *Let K be a number field. Then* $\limsup L_{n,K} \geq \limsup L_{n,K(X)}$.

Chapter 7

Explicit Examples over $\mathbb{Q}(X)$

In this section we construct explicit examples over the function field $\mathbb{Q}(X)$. On one hand this indicates limits to possible improvements on the bound stated in Theorem 6.2.2. On the other hand, every explicit n-example over $K(X)$ gives a lower bound on $\limsup L_{n,K}$.

7.1 Motivation and Notation

In Theorem 6.3.4 it is proved that for an explicit n-example ϕ over $K(X)$, we have $\limsup L_{n,K} \geq \frac{h\phi}{\log N\phi+1}$. In a special case, this can be improved.

Lemma 7.1.1 *Let ϕ be a nondegenerate n-example over $K(X)$, where K is a number field and* $\mathrm{Supp}\phi \subseteq \{0,-1,\infty\}$. *Then*

$$\limsup L_{n,K} \geq \deg\phi = h\phi.$$

Proof: By the notation of the previous section, $\psi(X) = X(X+1)$. We define

$$\phi_0 := (-X : X+1 : -1).$$

As proved in Proposition 1.2.3, the sequence $\{x_i\} = \{-3^{2^i}\}$ implies that

$$\limsup_{x\in K\setminus\{0,1\}} \frac{h(x)}{\log N\psi(x)} = \limsup_{x\in K\setminus\{0,1\}} \frac{h\phi_0(x)}{\log N\phi_0(x)} \geq 1.$$

Under the assumptions in the lemma we then have

$$\limsup L_{n,K} \geq \limsup \frac{h\phi(x)}{\log N\psi(x)} = \deg\phi \limsup \frac{h(x)}{\log N\psi(x)} \geq \deg\phi.$$

□

We limit ourselves to such ϕ. We write $\phi(X) = (f_1(X) : \ldots : f_n(X))$ where the f_i are polynomials satisfying

$$f_i(X) = a_i X^{k_i}(X+1)^{l_i}.$$

Since common factors can be divided out, there exist i and j such that $k_i = 0$, $l_j = 0$ and

$$d := \deg\phi = \max_i \deg f_i = \max_i (k_i + l_i).$$

Since ϕ is a nondegenerate n-example, we have that $\sum_{i=1}^{n} f_i(X) = 0$ and that no proper subsum vanishes.

With each f_i we associate a homogeneous polynomial of degree d in three variables

$$\tilde{f_i}(A,B,C) = q_{k_i,l_i} A^{k_i} B^{l_i} C^{d-k_i-l_i} \text{ where } q_{k_i,l_i} = (-1)^{d-l_i} a_i.$$

It is easy to check that $f_i = \tilde{f_i} \circ \phi_0$, where $\phi_0 = (-X : X+1 : -1)$. Therefore, we have $Q(A,B,C) := \sum \tilde{f_i}(A,B,C) = 0$ for $A+B+C = 0$ which implies that $Q(A,B,C) = (A+B+C)P(A,B,C)$. We denote

$$Q(A,B,C) = \sum_{i=0}^{d} \sum_{j=0}^{d-i} q_{i,j} A^i B^j C^{d-i-j}$$

and

$$P(A,B,C) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1-i} p_{i,j} A^i B^j C^{d-1-i-j}.$$

All other $p_{i,j}$ and $q_{i,j}$ are considered 0. That means we have

$$q_{i,j} = p_{i-1,j} + p_{i,j} + p_{i,j-1}$$

Furthermore, it follows that

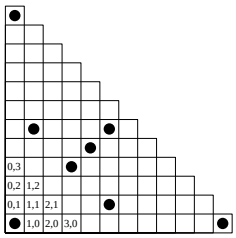
$$n = \#\{(i,j) : q_{i,j} \neq 0\}.$$

Divisibility demands translate into the existence of i, j and k such that $q_{i,0} \neq 0$, $q_{0,j} \neq 0$ and $q_{k,d-k} \neq 0$. Nondegeneracy has no simple interpretation in this context. We will check it separately.

For both degenerate and nondegenerate examples we introduce the *fingerprint* by

$$F_\phi := \{(k_i,l_i) : i = 1, \ldots, n\} = \{(i,j) : q_{i,j} \neq 0\} =: F_Q.$$

Figure 7.1: Example fingerprint: $F_{11,1}$



We will limit ourselves to studying examples with given fingerprint

$$\begin{aligned} F_{d,m} := \; & \{(0,d),(0,0),(d,0)\} \cup \\ & \bigcup_{i=0}^{m-1} \{(2i+1, \tfrac{1}{2}(d-1)-i), (\tfrac{1}{2}(d-1)-i, 2i+1)\} \cup \\ & \{(2m+1,2m+1),(2m+2,2m+2),\ldots,(\tfrac{1}{2}(d-1),\tfrac{1}{2}(d-1))\}, \end{aligned}$$

where d is odd and $m = 0, \ldots, \lceil \frac{d-1}{6} \rceil - 1$. Note that transformations like $(i,j) \mapsto (j,i)$ and $(i,j) \mapsto (d-j,i)$ do not map F_{d,m_1} onto F_{d,m_2}, meaning that these fingerprints are truly distinct in the sense that rotation and mirroring do not map one fingerprint to another.

7.2 Nondegeneracy

Assume that there exists a normalized n-example ϕ of degree d and with fingerprint $F_{d,m}$. Since the ordering of the f_i in $(f_1 : \ldots : f_n) = \phi$ is not important, we can safely assume that

$$f_1 = (X+1)^d,\ f_2 = -1 \text{ and } f_3 = -X^d.$$

For $i = 0, \ldots, m-1$ we have

$$\begin{aligned} f_{4+2i} &= a_{4+2i} X^{2i+1} (X+1)^{\frac{1}{2}(d-1)-i} \\ f_{5+2i} &= a_{5+2i} X^{\frac{1}{2}(d-1)-i} (X+1)^{2i+1} \end{aligned}$$

and for $i = 1, \ldots, \frac{1}{2}(d+5) - 3 - 2m$ we have

$$f_{3+2m+i} = a_{3+2m+i} X^{2m+i} (X+1)^{2m+i}.$$

Each f_i can be written as a coordinate vector with respect to the basis $\{1, X, X^2, \ldots, X^d\}$, leading to

$$f_i = \begin{pmatrix} f_{i,0} \\ \vdots \\ f_{i,d} \end{pmatrix} \text{ with } f_{i,j} = a_i \binom{l_i}{j - k_i}$$

where $\binom{l}{k} = 0$ if $k < 0$ or if $k > l$.

Lemma 7.2.1 *If ϕ is a normalized n-example with fingerprint $F_{d,m}$ then ϕ is nondegenerate.*

Proof: We have that $\{f_n, \ldots, f_4\}$ is a set of independent vectors, since each vector has a nonzero entry at a place where its predecessors have a zero entry. Therefore, it cannot be the case that the sum of a nonempty subset of $\{f_n, \ldots, f_4\}$ vanishes.

Suppose that $\{f_1, \ldots, f_n\}$ is a degenerate set, meaning that there exist a partition of $\{1, \ldots, n\}$ into two nonempty, disjoint sets V_1 and V_2 such that $\sum_{f \in V_1} f = \sum_{f \in V_2} f = 0$. Then one contains f_1. Since f_2 and f_3 are the only other vectors f_i with $f_{i,0} \neq 0$ or $f_{i,d} \neq 0$, they must be in the same set as f_1. The other set must then be a subset of $\{f_4, \ldots, f_n\}$, contradicting independence of that set. □

7.3 Existence and Uniqueness

In order to show that examples with given $F_{d,m}$ exist, we simply show that we can give the $p_{i,j}$ values such that $q_{i,j} \neq 0$ if and only if $(i,j) \in F_{d,m}$. For convenience we introduce a special set of indices. A *triangle border* of length e and offset f is a set

$$\begin{aligned} T_{e,f} := \ & \{(i,f) : i = f, \ldots, e+f\} \cup \\ & \{(f,j) : j = f, \ldots, e+f\} \cup \\ & \{(f+i, e+f-i : i = 0, \ldots, e\}. \end{aligned}$$

A set $\{p_{i,j}\}_{T_{e,f}}$ is called *mirror symmetric* if $p_{i,j} = p_{j,i}$ holds for all $(i,j) \in T_{e,f}$.
A set $\{p_{i,j}\}_{T_{e,f}}$ is called *rotation symmetric* if

$$\begin{aligned} p_{f+i,f} &= p_{f+e-i,f+i}, \\ p_{f+e-i,f+i} &= p_{f,f+e-i} \text{ and} \\ p_{f,f+e-i} &= p_{f+i,f} \end{aligned}$$

hold for $i = 0, \ldots, e$.

A set $\{p_{i,j}\}_{T_{e,f}}$ is called *fully symmetric* if it is both rotation and mirror symmetric. It is clear that such a set is completely determined by $p_{f,f}, \ldots, p_{f,f+\lceil \frac{1}{2}e \rceil}$.

Lemma 7.3.1 *Let $\{p_{i,j}\}_{T_{e,f}}$ be a mirror symmetric set with $e \geq 3$. Then there exist $p_{i,f+1}, p_{f+1,i}$ for $i = f+1, \ldots, e+f-2$ such that $\{p_{i,j}\}_{T_{e-2,f+1}}$ is mirror symmetric and $q_{i,f+1} = q_{f+1,i} = 0$ for $i = f+2, \ldots, e+f-1$.*

Proof: Define inductively for $i = e+f-2, \ldots, f+1$

$$\begin{aligned} p_{i,f+1} &:= -p_{i+1,f+1} - p_{i+1,f} \text{ and} \\ p_{f+1,i} &:= -p_{f+1,i+1} - p_{f,i+1}. \end{aligned}$$

Mirror symmetry is preserved and therefore there is no contradiction for $p_{f+1,f+1}$. Since

$$\begin{aligned} q_{i+1,f+1} &= p_{i,f+1} + p_{i+1,f+1} + p_{i+1,f} \text{ and} \\ q_{f+1,i+1} &= p_{f,i+1} + p_{f+1,i+1} + p_{f+1,i}, \end{aligned}$$

it follows that $q_{i+1,f+1} = q_{f+1,i+1} = 0$ for $i = f+1, \ldots, e+f-2$. □

Lemma 7.3.2 *Let $\{p_{i,j}\}_{T_{e,f}}$ be a fully symmetric set, where $e \geq 3$ is odd. Then there is a fully symmetric set $\{p_{i,j}\}_{T_{e-3,f+1}}$ such that $q_{i,j} = 0$ for $(i,j) \in T_{e-2,f+1}$.*

Proof: Define inductively for $i = 0, 1, \ldots, \frac{1}{2}(e-3)$

$$p_{f+1,f+1+i} := -p_{f,f+1+i} - p_{f+1,f+i}.$$

Other $p_{i,j}$ are defined by enforcing full symmetry. Since

$$q_{f+1,f+1+i} = p_{f,f+1+i} + p_{f+1,f+1+i} + p_{f+1,f+i}$$

it follows that these are all equal to zero for $i = 0, \ldots, \frac{1}{2}(e-3)$. It is easy to check that if $\{p_{i,j}\}_{T_{e,f}}$ and $\{p_{i,j}\}_{T_{e-3,f+1}}$ are fully symmetric sets, then $\{q_{i,j}\}_{T_{e-2,f+1}}$ is fully symmetric as well. This proves the lemma. □

Lemma 7.3.3 *Let $\{p_{i,j}\}_{T_{e,f}}$ be a fully symmetric set, where $e \geq 4$ is even. Then there is a fully symmetric set $\{p_{i,j}\}_{T_{e-3,f+1}}$ such that $q_{i,j} = 0$ for $(i,j) \in T_{e-2,f+1} \setminus \{(f+\frac{1}{2}e, f+1), (f+\frac{1}{2}e, f+\frac{1}{2}e), (f+1, f+\frac{1}{2}e)\}$.*

Proof: Same as Lemma 7.3.2, but let i run from 0 to $\frac{1}{2}e-2$. All arguments still hold, but nothing can be said of $q_{f+\frac{1}{2}e,f+1}$, $q_{f+\frac{1}{2}e,f+\frac{1}{2}e}$ and $q_{f+1,f+\frac{1}{2}e}$. □

The following algorithm produces normalized n-examples with fingerprint $F_{d,m}$ where d is odd and $m \in \{0, 1, \ldots, \lceil \frac{d-1}{6} \rceil - 1\}$.

1. For $i = 0, \ldots, d-1$ define $p_{i,0} = p_{0,i} = p_{i,d-1-i} = (-1)^i$.
2. Put $n := 3$, $f := 0$ and $e := d-1$.
3. Repeat m times:
   apply lemma 7.3.3. $n := n+3$, $f := f+1$ and $e := e-3$.
   apply lemma 7.3.2. $f := f+1$ and $e := e-3$.
4. Repeat until $e = 2$:
   apply lemma 7.3.1. $n := n+1$, $f := f+1$ and $e := e-2$.
5. $n := n+1$ and $e := e-2$.

Lemma 7.3.4 *Normalized examples with fingerprint $F_{d,m}$ with $m = 0, 1, \ldots, \lceil \frac{d-1}{6} \rceil - 1$ and d odd, exist and are unique.*

Proof: The algorithm shows a way of solving the system $\{q_{0,0} = q_{d,0} = q_{0,d} = 1\} \cup \{q_{i,j} = 0 : (i,j) \notin F_{d,m}\}$. That solution is unique, since in each step, all values assigned to the $p_{i,j}$ are completely determined by the values of earlier assigned $p_{i,j}$. □

Theorem 7.3.5 *Let $d \geq 3$ be odd. Then there exist at least $\lceil \frac{d-1}{6} \rceil$ nondegenerate $\frac{1}{2}(d+5)$-examples over $\mathbb{Q}(X)$ of degree d with* Supp$\phi = \{\infty, 0, -1\}$. *These examples are truly distinct in the sense that none is the result of combining another with a linear transformation.*

Proof: Lemma 7.3.4 proves existence and 7.2.1 proves nondegeneracy. Concerning linear transformations, we note that any such transformation should leave Suppϕ invariant. That means it permutes the set of monomials $\{-1, -x, x+1\}$. This leads to mirroring and rotation of the fingerprints involved. No $F_{d,m}$ can be mapped to another using such operations. □

7.4 Additional Solutions

The representation in Section 7.2 can be used to generate solutions as well. We write $f_1 = (X+1)^d$, $f_2 = -1$, $f_3 = -X^d$, and we regard these as column vectors with respect to the basis $\{1, X, \ldots, X^d\}$. We want to calculate a sequence of vectors $\{f_4, \ldots, f_n\}$ of the form $f_i = a_i X^s (X+1)^w$ such that $\sum_{i=1}^n f_i = 0$. We use that $f_1 + f_2 + f_3$ is symmetric in the sense that $X^d(f_1(\frac{1}{X}) + f_2(\frac{1}{X}) + f_3(\frac{1}{X})) = f_1(X) + f_2(X) + f_3(X)$ and we preserve this symmetry thoughout the algorithm. Initialize $n := 3$. Let s denote the lowest power of X that has a nonzero coefficient in $\sum_{i=1}^n f_i$ and let $s+w$ denote the highest power of X that has a nonzero coefficient in $\sum_{i=1}^n f_i$. Finally, $(\sum_{i=1}^n f_i)_t$ denotes the coefficient of X^t in $\sum_{i=1}^n f_i$.

If $w' := \frac{(\sum_{i=1}^n f_i)_{s+1}}{(\sum_{i=1}^n f_i)_s}$ is an integer, then if we substract $(\sum_{i=1}^n f_i)_s X^s (X+1)^{w'}$, this will eliminate the two lowest powers of X from $\sum_{i=1}^n f_i$. By symmetry, we have that if $w' \leq w-2$, then $(\sum_{i=1}^n f_i)_s X^{s+w-w'}(X+1)^{w'}$ will do the same for the two highest powers in $\sum_{i=1}^n f_i$, without interfering with the lowest powers of X.

Another strategy is to eliminate both the highest and the lowest powers of X from $\sum_{i=1}^n f_i$. This is done by substracting $(\sum_{i=1}^n)_s X^s (X+1)^w$ from $\sum_{i=1}^n f_i$.

By doing this iteratively and updating all quantities involved, we eventually get $\sum_{i=1}^n f_i = 0$ with n at most $\frac{1}{2}(d+5)$.

This leads to the following algorithm for d odd.

1. $f_1 := (x+1)^d$, $f_2 := -1$, $f_3 := -x^d$, $w := d-2$, $n := 3$, $s := 1$.

2. if $w' := \frac{(\sum_{i=1}^n f_i)_s}{(\sum_{i=1}^n f_i)_s}$ is an integer and $w' \leq w-2$ then choose either 2a or 2b. Otherwise go to 2b.

   (a)

$$\begin{aligned} f_{n+1} &:= -(\sum_{i=1}^n f_i)_s X^s (X+1)^{w'} \\ f_{n+2} &:= -(\sum_{i=1}^n f_i)_s X^{s+w-w'} (X+1)^{w'} \end{aligned}$$

   $n := n+2$. Update s and w such that X^s is the lowest power of X that occcurs in $\sum_{i=1}^n f_i$ and X^{s+w} is the highest power.

   (b)

$$f_{n+1} := -(\sum_{i=1}^n f_i)_s x^s (x+1)^{w'}$$

   $n := n+1$. Update s and w such that X^s is the lowest power of X that occcurs in $\sum_{i=1}^n f_i$ and X^{s+w} is the highest power.

3. if $\sum_{i=1}^n f_i = 0$ then stop, else go to 2.

Existence of examples with fingerprint $F_{d,m}$ ensures that it is possible to start with choosing 2a m times to start with and then execute 2b for the rest of the algorithm. It turns out, however that sometimes it is possible to execute 2a after 2b has been executed. For instance, if $d = 27$ it is possible to execute 2b followed by 2a and then finish with executing 2b.

This gives additional examples in these special cases. They are not better or worse, but they do have other fingerprints. Below is a table of all abnormal examples for $d \leq 147$. For brevity, only the string of successively executed steps a and b is denoted. " ... " stands for enough bs to finish the algorithm.

$$\begin{aligned} 27 &: abab\ldots \\ 65 &: aabab\ldots \\ 67 &: bbbbbbbbbbab\ldots \\ 97 &: bbbbbbbbbbbbbbbbbbbbab\ldots \\ 119 &: aaabab\ldots \end{aligned}$$

7.5 Formulas

Let $Q(A,B,C)$ be a homogeneous polynomial in 3 variables of degree d that is divisible by $A+B+C$. We write

$$Q(A,B,C) = \sum_{i,j} q_{i,j} A^i B^j C^{d-i-j}.$$

We have $Q(A,B,C) = (A+B+C)P(A,B,C)$, where $P(A,B,C)$ is a homogeneous polynomial in 3 variables of degree $d-1$. We write

$$P(A,B,C) = \sum_{i,j} p_{i,j} A^i B^j C^{d-1-i-j}.$$

We have that

$$q_{i,j} = p_{i-1,j} + p_{i,j} + p_{i,j-1}.$$

This gives us enough equations to express $p_{i,j}$ in terms of $q_{k,l}$. By induction, we have

$$p_{i,j} = \sum_{k=0}^{i} \sum_{l=0}^{j} (-1)^{(i+j)-(k+l)} \binom{(i+j)-(k+l)}{i-k} q_{k,l}.$$

Since $p_{i,d-i} = 0$, it follows that

$$\sum_{k=0}^{i} \sum_{l=0}^{d-i} (-1)^{d-(k+l)} \binom{d-(k+l)}{i-k} q_{k,l} = 0 \text{ for } i = 0, \ldots, d. \tag{7.1}$$

By symmetry, we have that these equations must also hold if we apply the rotation $q_{i,j} \mapsto q_{d-i-j,i}$ or $q_{i,j} \mapsto q_{j,d-i-j}$. This leads to the equations

$$\sum_{k=0}^{i} \sum_{l=0}^{d-i} (-1)^{d-(k+l)} \binom{d-(k+l)}{i-k} q_{d-k-l,k} = 0 \text{ for } i = 0, \ldots, d; \tag{7.2}$$

$$\sum_{r=0}^{i} \sum_{l=0}^{d-i} (-1)^{d-(k+l)} \binom{d-(k+l)}{i-k} q_{l,d-k-l} = 0 \text{ for } i = 0, \ldots, d. \tag{7.3}$$

Let $G_{i,d}^{(t)}$ be the set of indices (k,l) with $k \geq 0$, $l \geq 0$ and $k+l \leq d$ such that the coefficient of $q_{k,l}$ in the corresponding equation is nonzero. That means that

$$\begin{aligned} G_{i,d}^{(1)} &= \{(k,l) : k = 0, \ldots, i,\ l = 0, \ldots, d-i\} \\ G_{i,d}^{(2)} &= \{(k,l) : l = 0, \ldots, i,\ k = i-l, \ldots, d-l\} \\ G_{i,d}^{(3)} &= \{(k,l) : k = 0, \ldots, d-i,\ l = d-i-k, \ldots, d-k\} \end{aligned}$$

Let $F_d := \{(k,l) : q_{k,l} \neq 0\}$. Since

$$\sum_{(k,l) \in G_{i,d}^{(t)}} C_{k,l,i,d}^{(t)} q_{k,l} = 0,$$

where the $C_{k,l,i,d}^{(t)}$ are nonzero, we have that

$$\#G_{i,d}^{(t)} \cap F_d = 0 \text{ or } \#G_{i,d}^{(t)} \cap F_d \geq 2.$$

Recall that if F_d is the fingerprint of a nondegenerate n-example of degree d, then we have that $\{(i_1,0),(0,j_2),(i_3,d-i_3)\} \subseteq F_d$ for certain i_1, j_2, i_3 since the monomials in Q have no factor in common. Thus, for fingerprints of nondegenerate examples we have

$$\#G_{0,d}^{(t)} \cap F_d \geq 2 \text{ for } t = 1,2,3.$$

Equation (7.1) enables us to determine closed formulas for some n-examples given in previous sections.

Proposition 7.5.1 *Let $\sum q_{k,l}A^kB^lC^{d-k-l}$ be the polynomial associated with the normalized n-example with fingerprint $F_{d,0}$. We have $q_{0,0} = q_{0,d} = q_{d,0} = 1$ and*

$$q_{i,i} = (-1)^i \frac{d}{d-i}\binom{d-i}{i} \text{ for } i = 1, 2, \ldots, \frac{1}{2}(d-1)$$

Proof: Equation (7.1) holds for $i = 1, 2, \ldots, \frac{1}{2}(d-1)$. If we simplify this using $q_{k,l} = 0$ if $(k,l) \notin F_{d,0}$, we get

$$\sum_{k=0}^{i} \binom{d-2k}{i-k} q_{k,k} = 0.$$

This leads to the recurrence relation

$$q_{i,i} = -\sum_{k=0}^{i-1} \binom{d-2k}{i-k} q_{k,k}.$$

Using induction, the formula in the proposition can be checked. □

The family of examples with fingerprint $F_d, 0$ is the family that was already constructed by Browkin and Brzezinski in [BB92]. They state the same formula. Their proof of the existence and nondegeneracy of these examples is different from the proof given here.

7.6 Optimality

Let $\phi = (f_1 : \ldots : f_n)$ be a nondegenerate n-example of degree d and such that $\mathrm{Supp}\phi \subseteq \{0, -1, \infty\}$. With such an example, we can associate an embedding $\tilde{\phi} : \mathbb{P}^2 \to \mathbb{P}^{n-1}$ by $\phi := (\tilde{f_1} : \ldots : \tilde{f_n})$, where the $\tilde{f_i}$ are monomials in the coordinates of $\mathbb{P}^2$. By nondegeneracy of ϕ we have $\tilde{\phi}(V_3) \subset V_n$ and $\tilde{\phi}(V_3) \not\subset W_n$. Lemma 7.1.1 shows how we can use this to lift 3-examples over $\mathbb{Q}$ to n-examples over $\mathbb{Q}$.

The same can be done for 3-examples over $\mathbb{Q}(X)$. Suppose $(g_1 : g_2 : g_3)$ is a nondegenerate example over $\mathbb{Q}(X)$. Then $\mathrm{Im}\,(g_1 : g_2 : g_3) \cap V_3 \setminus W_3$ is infinite. $\tilde{\phi} \circ (g_1 : g_2 : g_3)$ is a nondegenerate n-example since $\mathrm{Im}\,\tilde{\phi} \circ (g_1 : g_2 : g_3) \subset V_n$ and $\mathrm{Im}\,\tilde{\phi} \circ (g_1 : g_2 : g_3) \not\subset W_n$, because only finitely many points in V_3 are mapped into W_n by $\tilde{\phi}$. We have $\mathrm{Supp}\tilde{\phi} \circ (g_1 : g_2 : g_3) \subset \mathrm{Supp}(g_1 : g_2 : g_3)$, since $\tilde{f_i}(g_1, g_2, g_3) = q_{k_i,l_i} g_1^{k_i} g_2^{l_i} g_3^{d-k_i-l_i}$. Furthermore we have

$$\deg \tilde{\phi} \circ (g_1 : g_2 : g_3) = \deg \tilde{\phi} \deg(g_1 : g_2 : g_3).$$

That means we have

Lemma 7.6.1 *Let $\tilde{\phi} = (\tilde{f_1} : \ldots : \tilde{f_n})$ be the map belonging to a nondegenerate n-example over $\mathbb{Q}(X)$ of degree d with $\mathrm{Supp}\tilde{\phi} \subset \{-1, 0, \infty\}$. Then for any nondegenerate 3-example $(g_1 : g_2 : g_3)$ over $\mathbb{Q}(X)$ we have a nondegenerate n-example $\xi = (\tilde{f_1}(g1, g2, g3) : \ldots : \tilde{f_n}(g1, g2, g3))$ such that*

$$\frac{h\xi}{\log N\xi} = d\frac{h(g_1 : g_2 : g_3)}{\log N(g_1 : g_2 : g_3)}$$

On one hand, this gives us a lower bound for the n-conjecture over $\mathbb{Q}(X)$.

Proposition 7.6.2 $\limsup L_{\mathbb{Q}[X]} \geq 2n - 5$

Proof: Theorem 1.4.5 proves that there is a sequence of 3-examples over $\mathbb{Z}[X]$ for which $\frac{h}{\log N}$ converges to 1. Using an n-example of degree $2n-5$ with support $\{-1,0,\infty\}$, we can map this sequence to a sequence of n-examples. Applying the lemma proves the proposition. □

On the other hand, since Brownawell and Masser proved the n-conjecture for function fields, we have an upper bound on the degree of n-examples with Supp $\subset \{-1,0,\infty\}$.

Proposition 7.6.3 *If ϕ is a nondegenerate n-example over $\mathbb{Q}(X)$ of degree d with* Supp$\phi \subset \{-1,0,\infty\}$, *then*

$$d \leq \frac{1}{2}(n-1)(n-2).$$

Proof: An example with $d > \frac{1}{2}(n-1)(n-2)$ would contradict Theorem 6.2.2. □

For $n = 3, 4$, the bound by Proposition 7.6.3 is 1 and 3 respectively. This coincides with our explicitly constructed examples. For $n = 5$, it is guaranteed that $d \leq 6$. We only know of a 5-example of degree 5. Using ad hoc techniques, we can prove that no 5-example of degree 6 exists.

Theorem 7.6.4 *No 5-example ϕ over $\mathbb{Q}[X]$ of degree 6 with* Supp$\phi \subset \{0,-1,\infty\}$ *exists.*

Proof: Suppose it does. Then the associated fingerprint F has the properties that

$$\begin{aligned} \#F &= 5; \\ \#(F \cap G_{i,6}^{(t)}) &\neq 1 \text{ for } i = 0,\ldots,6 \text{ and } t = 1,2,3; \\ F \cap G_{0,6}^{(t)} &\neq \emptyset \text{ for } t = 1,2,3. \end{aligned}$$

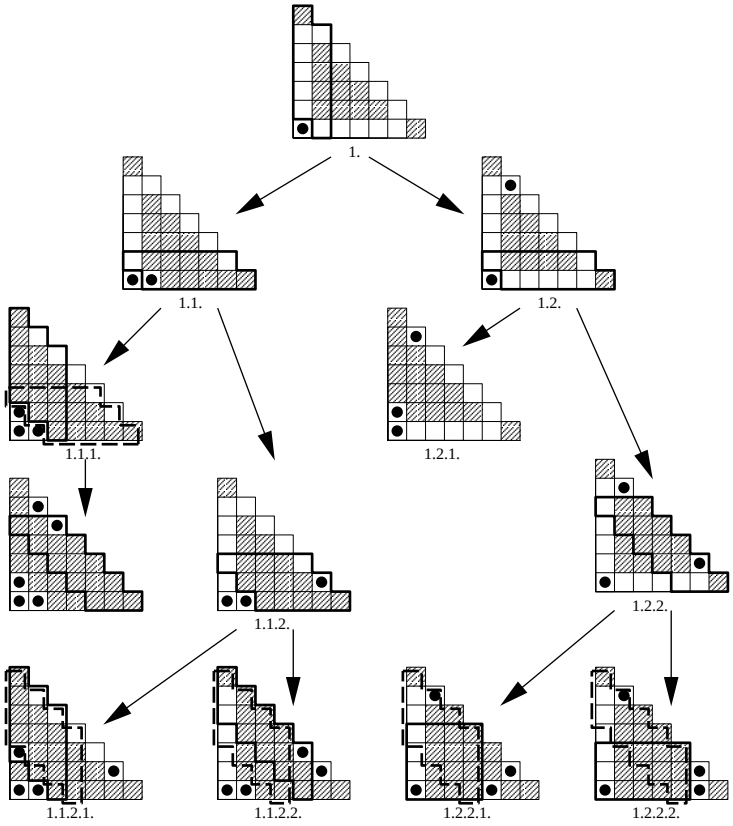
That means that $\#(F \cap G_{0,6}^{(t)}) \geq 2$ for $t = 1,2,3$, meaning that at least one of the points (0,0), (6,0) and (0,6) must be an element of F. By rotational symmetry, we only need to consider the cases:

1. $(0,0) \in F$; $(0,6), (6,0) \notin F$,
2. $(6,0), (0,6) \in F$; $(0,0) \notin F$,
3. $(0,0), (6,0), (0,6) \in F$.

By intersecting F with various $G_i^{(t)} = G_{i,6}^{(t)}$ we can exclude nearly all possible configurations. The remaining cases can be checked by trying to solve the equations (7.1) together with $q_{k,l} = 0$ for $(k,l) \notin F$.

1. (see also Figure 7.2) $F = \{(0,0), (i_1,0), (0,i_2), (i_3, 6-i_3), (i_4, 6-i_4)\}$. Since $F \cap G_5^{(3)} \neq \emptyset$, some second point must lie in the intersection. That means that $i_1 = 1$ or $i_3 = 1$.
   - 1.1. $F = \{(0,0), (1,0), (0,i_2), (i_3, 6-i_3), (i_4, 6-i_4)\}$. Since $F \cap G_1^{(2)} \neq \emptyset$, we have $i_2 = 1$ or $i_4 = 5$.
     - 1.1.1. $F = \{(0,0), (1,0), (0,1), (i_3, 6-i_3), (i_4, 6-i_4)\}$. Then $(i_3, 6-i_3)$ and $(i_4, 6-i_4)$ must both lie in either $G_2^{(2)}$ or $G_4^{(3)}$, which are mirror symmetric situations. Assume the latter. Then $i_3 = 1$ and $i_4 = 2$ (or conversely). Then $F \cap G_4^{(2)} = \{(2,4)\}$, which is in contradiction with the fact that no such intersection can contain precisely one point.

Figure 7.2: Configurations with one corner occupied.



1.1.2. $F = \{(0,0),(1,0),(0,i_2),(i_3,6-i_3),(5,1)\}$. Intersection of F with $G_2^{(2)}$ gives $i_2 = 2$ or $i_3 = 4$.

1.1.2.1. $F = \{(0,0),(1,0),(0,2),(i_3,6-i_3),(5,1)\}$. Intersection with $G_4^{(3)}$ gives $i_3 \leq 2$, which implies the impossible equality $F \cap G_3^{(3)} = \{(i_3,6-i_3)\}$.

1.1.2.2. $F = \{(0,0),(1,0),(0,i_2),(4,2),(5,1)\}$. Intersection with $G_2^{(3)}$ gives $i_2 \geq 4$, implying that $F \cap G_3^{(3)} = \{(0,i_2)\}$, which cannot be.

1.2. $F = \{(0,0),(i_1,0),(0,i_2),(1,5),(i_4,6-i_4)\}$. Intersection with $G_1^{(2)}$ gives $i_2 = 1$ or $i_4 = 5$.

1.2.1. $F = \{(0,0),(i_1,0),(0,1),(1,5),(i_4,6-i_4)\}$. This is a special case of the mirrored situation of 1.1. and is therefore impossible.

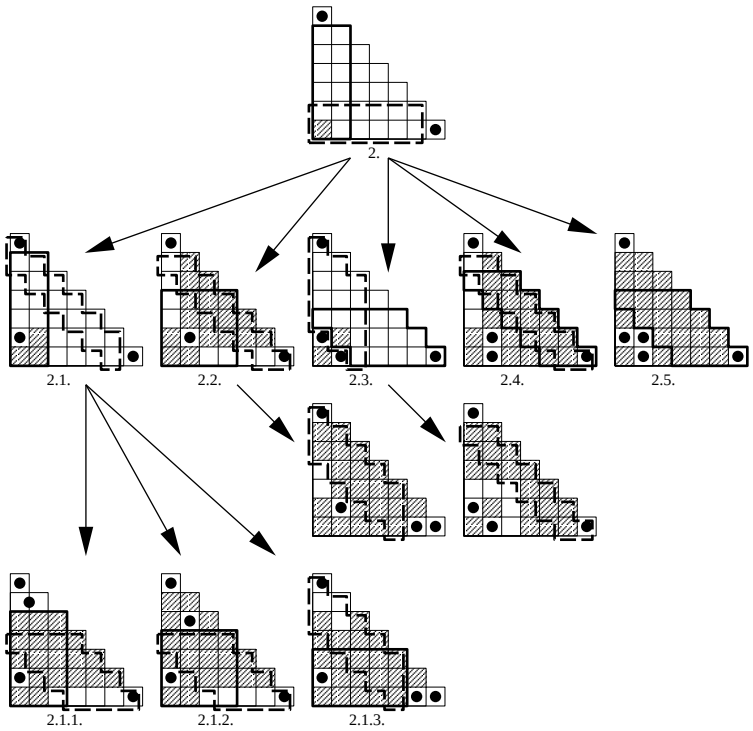
1.2.2. $F = \{(0,0),(i_1,0),(0,i_2),(1,5),(5,1)\}$. Intersection with $G_4^{(2)}$ gives that $i_2 = 4$ or $i_1 \geq 4$. By symmetry it suffices to consider $i_1 = 4$ and $i_1 = 5$.

1.2.2.1. $F = \{(0,0),(4,0),(0,i_2),(1,5),(5,1)\}$. Intersecting with $G_3^{(1)}$ and $G_3^{(3)}$ gives that $i_2 = 3$. If we solve the equations (7.1) with $q_{k,l} = 0$ for $(k,l) \notin F$, then we only get the trivial solution, which does not correspond to a nondegenerate 5-example.

1.2.2.2. $F = \{(0,0),(5,0),(0,i_2),(1,5),(5,1)\}$. Intersecting with $G_4^{(1)}$ and $G_2^{(3)}$

gives $i_2 \leq 2$ and $i_2 \geq 4$ respectively.

Figure 7.3: Configurations with two corners occupied.



2. (see also Figure 7.3) $F = \{(6,0),(0,6),(i_1,0),(0,i_2),(i_3,i_4)\}$. Since $\#G_1^{(1)} \cap F \geq 2$ as well as $\#G_5^{(1)} \cap F \geq 2$ and $(6,0),(0,6) \notin G_1^{(1)}, G_5^{(1)}$, we have that at least one point must lie in $G_1^{(1)} \cap G_5^{(1)} \cap F$. By symmetry, it suffices to consider five situations:

   2.1. $G_1^{(1)} \cap G_5^{(1)} \cap F = \{(0,1)\}$,

   2.2. $G_1^{(1)} \cap G_5^{(1)} \cap F = \{(1,1)\}$,

   2.3. $G_1^{(1)} \cap G_5^{(1)} \cap F = \{(0,1),(1,0)\}$,

   2.4. $G_1^{(1)} \cap G_5^{(1)} \cap F = \{(1,1),(1,0)\}$,

   2.5. $G_1^{(1)} \cap G_5^{(1)} \cap F = \{(0,1),(1,1),(1,0)\}$.

   2.1. $F = \{(6,0),(0,6),(i_1,0),(0,1),(i_3,i_4)\}$ with $i_1 \geq 2$ and not both i_3 and $i_4 \leq 1$. Intersection with $G_1^{(1)}$ gives $i_3 \leq 1$, which implies that $i_4 \geq 2$. Intersection with $G_1^{(3)}$ then gives $i_4 = 5$ or $(i_3,i_4) = (1,4)$ or $i_1 = 5$.

      2.1.1. $F = \{(6,0,(0,6),(i_1,0),(0,1),(i_3,5)\}$ with $i_3 = 0$ or 1. Intersecting with $G_2^{(1)}$ gives that $i_1 = 2$. Intersecting with $G_3^{(2)}$ then gives a contradiction.

      2.1.2. $F = \{(6,0),(0,6),(i_1,0),(0,1),(1,4)\}$. Intersecting with $G_3^{(1)}$ gives that $i_1 = 2$ or 3. If $i_1 = 2$, then intersecting with $G_3^{(2)}$ gives a contradiction. If we solve the

equations (7.1) with $q_{k,l} = 0$ for $(k,l) \notin \{(6,0),(0,6),(3,0),(4,0),(0,1),(1,4)\}$, we only get the trivial solution.

2.1.3. $F = \{(6,0),(0,6),(5,0),(0,1),(i_3,i_4)\}$. Intersecting with $G_2^{(3)}$ gives $i_4 \geq 3$ and intersecting with $G_4^{(1)}$ gives $i_4 \leq 2$.

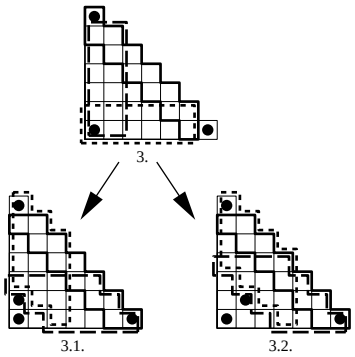
2.2. $F = \{(6,0),(0,6),(i_1,0),(0,i_2),(1,1)\}$, $i_1, i_2 \geq 2$. Intersecting with $G_3^{(1)}$ gives i_1 or $i_2 \leq 3$. Intersecting with $G_5^{(2)}$ gives $i_1 = 5$ or $i_2 = 5$. Due to mirror symmetry, it suffices to consider $F = \{(6,0),(0,6),(5,0),(0,i_2),(1,1)\}$ with $i_2 = 2,3$. $G_2^{(3)}$ gives a contradiction.

2.3. $F = \{(6,0,(0,6),(1,0),(0,1),(i_3,i_4)\}$. Intersecting with $G_4^{(3)}$ gives $i_3 \leq 2$. Intersecting with $G_2^{(3)}$ gives $i_4 \leq 2$. $G_5^{(2)}$ gives a contradiction.

2.4. $F = \{(6,0),(0,6),(1,1),(1,0),(0,i_2)\}$. Intersecting with $G_5^{(2)}$ gives $i_2 = 5$, whereas intersecting with $G_4^{(2)}$ gives that $i_2 = 4$.

2.5. $F = \{(6,0),(0,6),(1,0),(1,1),(0,1)\}$. Intersecting with $G_3^{(2)}$ gives a contradiction.

Figure 7.4: Configurations with three corners occupied.



3. (see also Figure 7.4) $F = \{(0,0),(6,0),(0,6),(i_1,i_2),(i_3,i_4)\}$. Since $G_1^{(1)}$, $G_1^{(2)}$ and $G_1^{(3)}$ each contain at least 2 points of F, we have that in at least one point must lie in an intersection of two of these Gs. Due to rotation symmetry, no generality is lost in assuming that $(i_1,i_2) \in G_1^{(1)} \cap G_1^{(2)}$, which means that $(i_1,i_2) \in \{(1,0),(1,1),(0,1)\}$. Due to mirror symmetry, we only need to study two of these cases.

3.1 $F = \{(0,0),(6,0),(0,6),(1,0),(i_3,i_4)\}$. Then we have the contradiction that

$$(i_3,i_4) \in G_2^{(2)} \cap G_4^{(3)} \cap G_5^{(2)} = \emptyset.$$

3.2 $F = \{(0,0),(6,0),(0,6),(1,1),(i_3,i_4)\}$. Then we have that $(i_3,i_4) \in G_3^{(2)} \cap G_3^{(3)} \cap G_5^{(2)} = \{(2,3),(3,3),(3,2)\}$. Solving (7.1) with $q_{k,l} = 0$ for $(k,l) \notin F$ gives only the trivial solution for each of these F.

□

Chapter 8

Explicit 4-Examples over $\mathbb{Q}$

8.1 Motivation

In [BB92] Browkin and Brzezinski formulate a stronger version of the n-conjecture.

Conjecture 8.1.1 (Browkin, Brzezinski) $\limsup L_{n,\mathbb{Q}} = 2n - 5$.

As we have seen in the previous section, if true, this conjecture is sharp. The conjecture is based on the following beliefs.

B1 The n-conjecture over $\mathbb{Q}$ is not essentially stronger than the ABC-conjecture together with the n-conjecture over $\mathbb{Q}(X)$.

B2 The bound in Theorem 6.2.2 should be linear instead of quadratic.

We have a vague indication that **B2** might be correct. For $n = 3, 4$ the bounds $2n - 5$ and $\frac{1}{2}(n-1)(n-2)$ coincide. For $n = 5$, we have seen that the bound by Theorem 6.2.2 of $\deg \phi = 6$ cannot be achieved for 5-examples ϕ with $\mathrm{Supp}\phi = \{-1, 0, \infty\}$.

Belief **B1** states that there is no interesting family of n-examples over $\mathbb{Q}$ that is not the image of some sequence of 3-examples under some n-example ϕ over $\mathbb{Q}(X)$. To get any idea as to whether this is true or not, it might be informative to look at all interesting n-examples over $\mathbb{Q}$ with height beneath some bound M_2. An example is interesting if the ratio α of the height and the log of the norm exceeds some bound α_0. We will look at 4-examples with height beneath $\log 10^{15}$ and a ratio better than $\alpha_0 = 4$.

8.2 Method

First we derive a standard form for writing 4-examples over $\mathbb{Q}$. We look at solutions of

$$A - B - C + D = 0$$

with $\gcd(A, B, C, D) = 0$ and no proper subsum equal to 0. Without loss of generality we assume $A, B, C, D \in \mathbb{Z}$ and $|A| \geq |B| \geq |C| \geq |D| > 0$ and $A > 0$.

If $B < 0$ then $A - B \geq 2|B|$ and $A - B = C - D$, which implies that $|A| = |B| = |C| = |D|$ with $C = -B$. This means that there is a proper subsum that vanishes. We conclude that

B is nonnegative and therefore $|B| < |A|$. By $|A| = |B + C - D| \leq |B| + |C| + |D| \leq 3B$ we have

$$\frac{1}{3}A \leq B < A.$$

This means that $A - B > 0$, implying that $-C + D < 0$ and hence $C > 0$. From $2C \geq |C| + |D| \geq |D - C| = |A - B|$, if follows that

$$\frac{1}{2}(A - B) \leq C \leq B.$$

This leaves us with

$$1 \leq |D| \leq C.$$

In this notation we have

$$\begin{aligned} h(A:B:C:D) &= \log A \text{ and} \\ \log N(A:B:C:D) &= r(A,B,C,D). \end{aligned}$$

If we are interested in all nondegenerate 4-examples over $\mathbb{Q}$ with

$$\begin{gathered} M_1 \leq h(A:B:C:D) \leq M_2 \text{ and} \\ \tfrac{h(A:B:C:D)}{\log N(A:B:C:D)} \geq \alpha_0, \end{gathered}$$

then it suffices to take $M_1 \leq A \leq M_2$ and

$$\log M_2 \geq h(A:B:C:D) \geq \alpha_0 \log N(A:B:C:D).$$

In other words, we only need to look at examples such that

$$r(A,B,C,D) \leq \frac{\log M_2}{\alpha_0}.$$

This limits the number of possible prime bases from which A, B, C, D are constructed. Denote the collection of possible prime bases by

$$\mathcal{B}_{M_2,\alpha_0} := \left\{ \{p_1, \ldots, p_k\} : p_i \text{ prime for } i = 1, \ldots, k;\ k \geq 2;\ \prod_{i=1}^{k} p_i \leq M_2^{\frac{1}{\alpha_0}} \right\}.$$

Let $\mathcal{P} \in \mathcal{B}_{M_2,\alpha_0}$ be such a prime basis. The norm of any example constructed from primes from this basis will be less than or equal to

$$B_{\mathcal{P}} := \prod_{p \in \mathcal{P}} p.$$

If there is another prime basis $\mathcal{Q} \in \mathcal{B}_{M_2,\alpha_0}$ such that $\mathcal{P} \subsetneq \mathcal{Q}$ then any example over $\mathcal{P}$ is also an example over $\mathcal{Q}$. Let q be the smallest prime number such that $q \notin \mathcal{P}$. Put $\mathcal{Q} = \mathcal{P} \cup \{q\}$. Define

$$T_{\mathcal{P}} := B_{\mathcal{Q}}.$$

Denote

$$V_{\mathcal{P},M_2} := \{n \in \mathbb{Z} : |n| \leq M_2;\ n = \prod_{p \in \mathcal{P}} p^{e_{p,n}}\}.$$

All 4-examples with $M_1 \leq h(A:B:C:D) \leq M_2$ and $\frac{h(A:B:C:D)}{r(A,B,C,D)} \geq \alpha_0$ can be computed as follows.

1. Construct $\mathcal{B}_{M_2,\alpha_0}$ by generating all primes smaller than $M_2^{\frac{1}{\alpha_0}}$ and selecting subsets $\mathcal{P}$ that satisfy $\prod_{p\in\mathcal{P}} p \le M_2^{\frac{1}{\alpha_0}}$.
2. For all $\mathcal{P} \in \mathcal{B}_{M_2,\alpha_0}$:
   (a) Construct $V_{\mathcal{P},M_2}$ by combining primes from $\mathcal{P}$ and store this set sorted.
   (b) Use bisection to find $A_1 := \max(B_{\mathcal{P}}^{\alpha_0}, M_1)$.
   (c) Let A run through $V_{\mathcal{P},M_2}$ from A_1 until $A > \min(M_2, T_{\mathcal{P}}^{\alpha_0})$,
   Let B run through $V_{\mathcal{P},M_2}$ from $\frac{1}{3}A$ until $B \ge A$,
   Let C run through $V_{\mathcal{P},M_2}$ from $\frac{1}{2}(A-B)$ until $C > B$:
      i. Check $\gcd(A,B,C) = 1$.
      ii. $D := B + C - A$; check $D \neq 0$. (otherwise we would have found a 3-example)
      iii. Check if $D \in V_{\mathcal{P},M_2}$.
      iv. If all checks OK, then report A, B, C, D as an example.

8.3 Results

Table 8.1: 4-examples with height$\le 10^{15}$.

A	B	C	D	$\frac{h(A:B:C:D)}{r(A,B,C,D)}$	New
$5^{12}\,7^3$	$2^3\,3^{21}$	$2\,3^8\,5^4\,7$	-1	4.703661794	no
$2^{33}\,29^3$	3^{30}	$2^{11}\,3^{11}\,7^3\,29$	-7^9	4.641225167	no
$3^{11}\,5^2$	2^{22}	$3\,5^7$	2^2	4.499477473	yes
$3^{24}\,5^3$	2^{45}	$2^{15}\,3^9\,5\,37$	-37^3	4.448730142	no
$3^2\,7^{11}$	$2^{11}\,3^{14}$	$2^{12}\,5^9$	$-5^2\,7^5$	4.414019371	yes
7^{12}	$2^{15}\,3^3\,5^6$	$2^5\,3^2\,5^2\,7^4$	-1	4.367019301	yes
$3^{12}\,5$	$2^{15}\,3^4$	5^5	2^7	4.349287536	no
$3^{24}\,13^3$	5^{21}	$2^{10}\,3^9\,5^7\,7\,13$	$-2^{30}\,7^3$	4.305017454	no
$2^2\,3^{12}$	$3^3\,5^7$	2^{14}	-5	4.283680185	yes
2^{21}	$2^{10}\,3\,5^4$	3^{11}	-5	4.279695988	no
2^{21}	5^9	$2^7\,3^2\,5^3$	-3^3	4.279695988	no
$3^{16}\,19^3$	$2\,5^5\,19^6$	5^{13}	$2^2\,3^2$	4.162090617	yes
$2^4\,3^3\,5^{16}$	$2^4\,3^{15}\,11^5$	$7^{11}\,11^4$	$5^8\,7^5$	4.108382269	yes
$3^{15}\,11^3$	$2^{11}\,3^6\,5^4\,11$	2^{33}	-5^{12}	4.082167946	no
$3^{11}\,5$	$2^{15}\,3^3$	$2^3\,5^3$	1	4.026280028	yes
$3^{11}\,5$	$2^{15}\,3^3$	2^{10}	5^2	4.026280028	yes
3^{24}	$2^{21}\,7^6$	$2^7\,3^9\,7^2\,17^2$	-17^6	4.012656302	no

The object of the systematic search for 4-examples is to see if there are any interesting 4-examples that are not parametrized by 3-examples. The best known 4-example comes from the 3-example that has been found by E. Reyssat.

$$2 + 3^{10}\,109 = 23^5;\ \frac{5\log 23}{\log(2\,3\,23\,109)} = 1.629911684.$$

If we make a 4-example of this, we get

$$23^{15} - 3^{10}\,109 - 2\,3^{11}\,23^5\,109 - 2^3 = 0;\ \alpha = 4.889735052.$$

The algorithm from the previous section has been used to determine all 4-examples with $A \leq M_2 = 10^{15}$ and $\alpha > \alpha_0 = 4$. This has taken approximately 292 CPU-days in total on mainly Silicon Graphics Indy-computers and HP9000 workstations. Note that $10^{20} < 23^{15} < 10^{21}$, which means that examples of the same magnitude as Reyssat's example are well out of reach. The results are in Table 8.1. The last column denotes if the example is new or is the image of a 3-example.

This table proves that there definitely are interesting 4-examples that are not the image of a 3-example. They are not very interesting in comparison to old examples, though. It would be interesting to see if there are any new 4-examples near the image of Reyssat's example. This cannot be done with the presented algorithm in any practical sense, however. We therefore conclude that no extra ground for belief **B1** has been found. It has become less likely in the sense that the existence of new and reasonably interesting examples is proved.

Appendix A

Computer Searches

The search done in Chapter 7 is typical for searches in number theory. The important properties are that

- they are huge in terms of needed computer time,
- searches in different areas of the space to be searched are almost completely independent,
- very few results are to be expected.

The first property compels us to use several computers simultaneously. Furthermore, it is hardly ever possible to get dedicated equipment. Therefore we have to use the computers in such a way that their performance in other tasks is affected as little as possible.

The other properties enable us to do this with virtually no penalty.

A.1 Idle Time Stealing

Workstations do nothing most of the time. That time can be used to do useful calculations. However, sometimes, the owner of the workstation has need of the processing power of the computer. Then, the background process should suspend itself to allow the primary user full access to the resources of the computer. If the primary user has no need for processing power anymore, then the background process can continue.

One way of checking whether a computer is used interactively or not, is to see if anyone is logged in. People tend not to log out when they have a coffee break, however.

Another criterion is the *system load*. This is a numerical value that is updated periodically by the operating system. It symbolizes the average number of processes that could occupy the processor completely. A system load below 1 means that the computer still has time to spare. Typically, a computer that is only used for typing in text has a system load around 0.2. By periodically checking the system load we can control a background process dynamically. If the load drops below, say 0.5, the process can be activated. Then the load will rise to at least 1, since now the processor always has work to do. If the load rises too high, however, then it is clear that there is a demanding task besides the background process. In that case, the background process should be suspended.

By adjusting the activation and suspension thresholds according to office hours, number of logged in users and whether or not the keyboard is locked for input, one can produce a

very finely tuned control scheme for background tasks. This idea has been implemented for the search described in Chapter 7 and performed satisfactorily.

A.2 Job Distribution

Using several computers for the same problem means that the problem has to be split into small chunks. For the search in Chapter 7, this is easy. There are natural splits at the changes of prime bases and, if needed, jobs can be split further by splitting the interval for A. Once all information is given to a particular computer, hardly any communication is needed. If the computer finds an example, it must report it and if it has finished the job, it has to request a new one.

First, a file is produced with on each line a job description. This can be done automatically. In the case of Chapter 7, this line consists of the prime basis and the bounds for A.

Each computer that is used, reads a line from the file. A special routine ensures that only one computer at the time can read from the file, ensuring that each line is read only once. Then, the job is executed. Results are written to another file using a similar routine. If the job is finished, a new line is read.

One big advantage of this model is the versatility. New computers can be added to the team dynamically without problem. If a computer goes down, then only the job the computer was working on, is lost. That can be diagnosed by the absence of a "job finished"-line for that job in the output file. The describing line of the lost job could even be reappended to the input file while the other computers continue with the other jobs, thus reinserting the job in the queue of jobs to do.

Furthermore, job scheduling is done completely dynamical. It is not relevant how long each job actually takes, since if a computer gets a particularly laborious job, then this is automatically compensated by the other computers continuing with the other jobs. This is especially important if the job is executed under an Idle Time Stealing scheme, since unexpected heavy use of a particular computer by other users can suspend the job for considerable time.

One big drawback is that the read and write routines have to acquire sole reading and writing rights between several computers. This is expensive (one should think of 0.1 to 5 seconds). Such penalties are only acceptable if these are very rare events, if only otherwise there would be too much conflicts in acquisition of rights. As remarked earlier, luckily most number theoretic searches satisfy this condition.

This job scheduling scheme was implemented for the search described in Chapter 7 and performed well.

Summary

Chapter 1 describes the ABC-conjecture in two typical cases where formulation is particularly easy. In the first case, the conjecture can be proved. In fact, historically, this is the motivation for the ABC-conjecture in general. As an illustration some applications are given and some associated questions are answered.

Chapter 2 through Chapter 4 describe general theory that is used in the sequel.

Chapter 5 formulates ABC in full strength and gives an application by showing that the Mordell Conjecture (Faltings's Theorem) follows from ABC.

Chapter 6 investigates problems that arise when the analogue of the ABC-conjecture is formulated for more variables. This leads to a formulation that coincides with [BM86] and [BB92]. A strong connection between the n-conjecture over number fields and the n-conjecture over rational function fields is displayed.

Chapter 7 investigates the ways in which examples for the n-conjecture for function fields can be used to parametrize examples for the n-conjecture for number fields by ABC-examples. The existence of a certain family of such parametrizations is proved. This family is a generalization of the parametrizations that Browkin and Brzezinski presented in [BB92]. In a special case, one can prove that members of this family are optimal in some sense.

Chapter 8 investigates whether there exist interesting 4-examples that are not parametrized in the sense of Chapter 7. Results are indecisive due to the lack of a reasonably efficient algorithm that does exist in the case of 3-examples (see [Nit93]).

Bibliography

[BB92] J. Browkin and J. Brzezinski. Some remarks on abc-conjecture. Technical Report No. 30, Gøteborgs Universitet, 1992.

[BM86] W. D. Brownawell and D. W. Masser. Vanishing sums in function fields. *Math. Proc. Camb. Phil. Soc.*, 100:427–434, 1986.

[Bro] Jerzy Browkin. Limit points in the abc-conjecture. unpublished.

[DG94] Henri Darmon and Andrew Granville. On the equations $z^m = f(x, y)$ and $ax^p + by^q = cz^r$. Preprint No. 28 Volume II, University of Georgia, 1994.

[Elk91] Noam D. Elkies. Abc implies mordell. *Duke Math. Journal*, 64:99–109, 1991.

[Fre87] Gerhard Frey. Links between solutions of $a + b = c$ and elliptic curves. In *Number Theory, Ulm 1987*, number 1380 in Lecture Notes in Mathematics, pages 31–62, New York, 1987. Springer Verlag.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer–Verlag, New York, 1977.

[Lan83] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer–Verlag, New York, 1983.

[Lan90] Serge Lang. Old and new conjectured diophantine inequalities. *Bulletin of the American Mathematical Society*, 23:37–75, 1990.

[Mas84] R. C. Mason. *Diophantine Equations over Function Fields*. Number 96 in London Mathematical Society Lecture Note Series. Cambridge University Press, Cambrige, 1984.

[Nit93] A. Nitaj. An algorithm for finding good abc-examples. *Comptes Rendus*, 317:811–815, 1993.

[Ser90] Jean-Pierre Serre. *Lectures on the Mordell-Weil Theorem*. Vieweg, Braunschweig, 1990.

[ST86] C. L. Stewart and R. Tijdeman. On the oesterlé-masser conjecture. *Monatshefte für Mathematik*, 102:251–257, 1986.

[vdW67] B. L. van der Waerden. *Algebra*, volume II. Springer–Verlag, Berlin, fifth edition, 1967.

[Voj87] Paul Vojta. *Diophantine Approximations and Value Distribution Theory.* Number 1239 in Lecture Notes in Mathematics. Springer Verlag, New York, 1987.

[Wei63] Edwin Weiss. *Algebraic Number Theory.* Mc Graw–Hill Book Company Inc., New York, 1963.