Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/36589 holds various files of this Leiden University dissertation.

Author: Zhuang, Weidong
Title: Symmetric diophantine approximation over function fields
Issue Date: 2015-12-03

Samenvatting

Een binaire vorm van graad n is een homogeen polynoom in twee variabelen van graad n. We bekijken voorlopig binaire vormen van graad n met geheeltallige coëfficiënten. Een belangrijke invariant van een binaire vorm is zijn *discriminant*. Dit is een homogeen polynoom van graad $2n-2$ in de coëfficiënten van F. We geven met $D(F)$ de discriminant van zo'n binaire vorm F aan, en met $H(F)$ de *hoogte*, dat wil zeggen het maximum van de absolute waarden van de coëfficiënten van F. Dan is $|D(F)| \leqslant c(n)H(F)^{2n-2}$ waarbij $c(n)$ alleen van n afhangt. We zeggen dat twee binaire vormen F en G equivalent zijn, als $G = \pm F_U$ voor zekere matrix $U \in \mathrm{GL}\,(2,\mathbb{Z})$. Hier is $F_U(X,Y) = F(aX+bY, cX+dY)$ voor $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Twee equivalante binaire vormen hebben dezelfde discriminant. We kunnen de hoogte van een binaire vorm steeds kleiner proberen te maken door hem te vervangen door een equivalente binaire vorm. Wanneer de hoogte van een binaire vorm op die manier niet meer kleiner kan worden gemaakt noemen we hem gereduceerd. Een vermoeden geformuleerd door Evertse maar waarschijnlijk al veel ouder, zegt dat van elke gereduceerde binaire vorm $F \in \mathbb{Z}[X,Y]$ van graad $n \geqslant 2$ met discriminant $\neq 0$ de hoogte $H(F)$ kan worden afgeschat als $H(F) \leqslant c_1(n)|D(F)|^{c_2(n)}$, waarbij $c_1(n)$ en $c_2(n)$ alleen van n afhangen. Dit vermoeden is voor $n=2$ en $n=3$ bewezen. Voor $n=2$ volgt het uit werk van Lagrange (1773) en Gauss (1801) en voor $n=3$ uit werk van Hermite (1851) maar voor $n \geqslant 4$ is het nog open. Evertse bewees in 1993 een zwakkere verse van bovenstaand vermoeden met in plaats van c_1 een constante die afhangt van zowel n als het splitsingslichaam van F, en die

niet effectief te berekenen is uit het gegeven bewijs. Verder bewezen Evertse en Győry in 1991 een andere zwakkere versie van bovenstaand vermoeden, met een bovengrens voor $H(F)$ van de vorm $\exp\left(c_1(n)|D(F)|^{c_2(n)}\right)$, waarbij $c_1(n), c_2(n)$ effectief uit het bewijs kunnen worden berekend.

In dit proefschrift bekijken we binaire vormen met coëfficiënten in de ring $\mathbb{C}[t]$ van polynomen met complexe coëfficiënten (of meer algemeen met coëfficiënten in een algebraïsch afgesloten lichaam van karakteristiek 0). De ring $\mathbb{C}[t]$ heeft veel eigenschappen gemeen met $\mathbb{Z}$, bijvoorbeeld eenduidige priemontbinding. Verder kunnen we op $\mathbb{C}[t]$ een absolute waarde definiëren, namelijk $|f| := e^{\text{graad}\, f}$ voor $f \in \mathbb{C}[t]$. We kunnen nu een analoge versie van Evertse's vermoeden formuleren voor binaire vormen in $\mathbb{C}[t][X, Y]$. In dit proefschrift geven we een bewijs voor die analoge versie, met expliciete waarden voor $c_1(n)$ en $c_2(n)$. Om een idee van het proefschrift te geven gaan we dieper in op twee belangrijke aspecten vsn het bewijs.

Het eerste aspect betreft de meetkunde der getallen. We geven een idee van die theorie aan de hand van twee voorbeelden. Bekijk een schoolbord met daarop twee coördinaatassen getekend, de x-as en de y-as. Teken alle roosterpunten op dit bord, dat wil zeggen met $x, y \in \mathbb{Z}$, bijvoorbeeld $(0, 1), (2, 3), (-5, 4)$, etc. Kunnen we vier roosterpunten bedekken met een stuk papier in de vorm van een cirkel met straal 1? Het is niet moeilijk te laten zien dat dit inderdaad kan. Kan dit met een driehoekig stuk papier met oppervlakte π? Of met een stuk papier van oppervlakte π van een willekeurige vorm? Blichfeldt [3] bewees in 1914 dat je met een stuk papier van oppervlakte k, na indien nodig een verschuiving, altijd $k+1$ roosterpunten kan bedekken. Bekijk nu een vierkant stuk papier met zijdelengte gelijk aan 2, maar speld het middelpunt van de vierkant vast op de oorsprong $(0, 0)$, dat wil zeggen het snijpunt van de coördinaatassen. Dus we kunnen dit stuk papier wel draaien maar niet verschuiven. Ligt er altijd een ander roosterpunt dan $(0, 0)$ onder het stuk papier, ongeacht hoe we het draaien? Wat als we in plaats van een vierkant stuk papier een rechthoekig stuk paper nemen met het middelpunt vastgespeld op $(0, 0)$? Of een ellipsvormig stuk papier

van oppervlakte 4 met middelpunt, dat wil zeggen het snijpunt van de korte as en de lange as vastgespeld op $(0,0)$? Minkowski bewees in 1896 dat een convexvormig stuk papier van oppervlakte minstens 4, dat spiegelsymmetrisch is ten opzichte van zijn zwaartepunt en waarvan het zwaartepunt op $(0,0)$ is vastgespeld, afgezien van $(0,0)$ altijd een ander roosterpunt bedekt. Dit is de zogenaamde eerste stelling van Minkowski over convexe gebieden. Deze stelling is in zekere zin kwalitatief. Later, in 1910, bewees Minkowski zijn tweede stelling over convexe gebieden. In termen van het stuk papier, kan deze als volgt worden geformuleerd. Neem weer een convexvormig stuk papier waarvan het zwaartepunt is vastgespeld op $(0,0)$ en dat spiegelsymmetrisch is ten opzichte van zijn zwaartepunt. We kunnen dit stuk met een factor λ "vermenigvuldigen" door het in alle richtingen ten opzichte van $(0,0)$ met een factor λ uit te rekken (waarbij een uitrekking met een factor $1/2$ op hetzelfde neerkomt als een inkrimping met een factor 2). Noem λ_1 de kleinste factor waarmee we het stuk papier moeten vermenigvuldigen opdat het naast $(0,0)$ nog een ander roosterpunt bedekt. Noem λ_2 de kleinste factor waarmee we het stuk papier moeten vermenigvuldigen opdat het naast $(0,0)$ nog twee andere roosterpunten bedekt die niet samen met $(0,0)$ op dezelfde lijn liggen. Dan zegt de stelling van Minkowski voor convexe gebieden dat $\frac{2}{S} \leqslant \lambda_1\lambda_2 \leqslant \frac{4}{S}$. Minkowski bewees bovengenoemde stellingen niet alleen voor het tweedimensionale geval dat we boven hebben beschreven, maar ook voor dimensies $3, 4, \ldots$. Deze resultaten blijken erg krachtig te zijn, zelfs in het onderzoek van vandaag in de Diophantische meetkunde. In hoofdstukken 3 en 4 van dit proefschrift passen we een analoge theorie van de meetkunde der getallen over $\mathbb{C}[t]$ toe en leiden daaruit een reductietheorie voor binaire vormen over $\mathbb{C}[t]$ af.

Het tweede aspect van ons bewijs heeft betrekking op het ABC-vermoeden voor algebraïsche getallen, en een analoge versie daarvan voor algebraïsche functies, die wel bewezen is. Het ABC-vermoeden gaat over drie positieve gehele getallen a, b, c met $a + b = c$ zodat a, b en c geen factor gemeenschappelijk hebben. Noem d het product van de verschillende priemdelers

van *abc*. Het ABC-vermoeden zegt ruwweg, dat c niet te groot kan zijn ten opzichte van d. Dus wanneer a, b deelbaar zijn door hoge machten van priemgetallen, dan kan c niet deelbaar zijn door hoge machten van priemgetallen. Het ABC-vermoeden, dat geformuleerd is door Oesterlé en later op een preciezere manier door Masser in 1986, zegt het volgende:

ABC-Vermoeden. *Voor elke $\varepsilon > 0$ zijn er maar eindig veel drietallen a, b, c van positieve gehele getallen, zodat a, b, c geen factor gemeen hebben en zodat $c > d^{1+\varepsilon}$, waarbij d het product is van de priemgetallen die abc delen.*

Dit vermoeden ziet er eenvoudig uit, maar het bleek extreem moeilijk te zijn. In 1996 beschreef de Amerikaanse wiskundige Goldfeld het als "het belangrijkste onopgeloste probleem in de Diophantische analyse." Het vermoeden is nog steeds open. De Japanse wiskundige Mochizuki beweerde in 2012 een bewijs voor het ABC-vermoeden gevonden te hebben, maar experts hebben nog niet kunnen bevestigen of zijn bewijs correct is of niet. Wanneer het ABC-vermoeden juist is, heeft dit erg veel gevolgen, bijvoorbeeld allerlei generalisaties van de laatste stelling van Fermat, verscherpingen van de Stelling van Roth over hoe goed algebraïsche getallen door rationale getallen kunnen worden benaderd, en nog veel meer.

Een analoge versie van het ABC-vermoeden voor polynomen en meer algemeen algebraïsche functies is onafhankelijk van elkaar bewezen door Stothers in 1981 en Mason in 1983. Het bewijs van deze ABC-stelling voor algebraïsche functies is niet zo moeilijk. Een eenvoudige versie van deze stelling is als volgt. Zijn $a(t), b(t), c(t)$ drie polynomen met complexe coëfficiënten zodat $a(t) + b(t) = c(t)$ en zodat $a(t), b(t), c(t)$ geen gemeenschappelijk nulpunt hebben. Zij S het aantal verschillende nulpunten van $a(t)b(t)c(t)$. Dan hebben $a(t), b(t), c(t)$ allemaal graad hoogstens $S-1$, tenzij $a(t), b(t), c(t)$ allemaal constant zijn. In hoofdstuk 2 van dit proefschift bewijzen we onder meer een veralgemening van de ABC-stelling voor sommen $a_1(t)+\cdots+a_n(t) = c(t)$, gebaseerd op werk van Brownawell and Masser [6], Zannier [26], en J. T-Y. Wang [25], en passen dit resultaat toe in hoofdstuk 7.

Een ander probleem dat in dit proefschrift wordt bekeken is hoever nulpunten van een polynoom van elkaar af kunnen liggen. Een elementaire ongelijkheid van Mahler (1964) zegt het volgende: zij $f \in \mathbb{Z}[X]$; dan geldt voor alle nulpunten α, β van f dat $|\alpha - \beta| \geqslant c(n)H(f)^{1-n}$, waarbij $c(n)$ een getal > 0 is dat alleen van n afhangt. Hier is $H(f)$ de hoogte van f, dat wil zeggen het maximum van de absolute waarden van de coëfficiënten van f. Het probleem is om een soortgelijke ongelijkheid te bewijzen met in plaats van $1 - n$ een grotere exponent. En wat is de grootst mogelijke exponent? Hierbij spelen de bovengenoemde afschattingen voor gereduceerde binaire vormen een belangrijke rol. Voor polynomen met coëfficiënten in $\mathbb{Z}$ is dit nog open. In dit proefschrift hebben we het analoge probleem bekeken voor polynomen met coëfficiënten in $\mathbb{C}[t]$, en bewezen dat voor polynomen $f(X) \in \mathbb{C}[t][X]$ van graad $n \geqslant 4$ in X de exponent $1 - n$ inderdaad kan worden verbeterd.

Het bovenstaande probleem ligt in het verlengde van de Stelling van Roth uit 1955 die gaat over de benadering van een vast algebraïsch getal γ door rationale getallen die we vrij laten variëren. De stelling zegt dat er voor elke $\varepsilon > 0$ een getal $c(\gamma, \varepsilon) > 0$ zodat $|\gamma - p/q| > c(\gamma, \varepsilon)q^{-2-\varepsilon}$ voor alle gehele getallen p en q met $q > 0$. Voor deze stelling kreeg Roth de Fieldsmedaille.

In het *symmetrische approximatieprobleem* kijken we naar twee algebraïsche getallen α en β die we vrij laten variëren. Neem aan dat α, β nulpunten zijn van respectievelijk de polynomen $f, g \in \mathbb{Z}[X]$. We vragen naar afschattingen $|\alpha - \beta| \geqslant cH(f)^{-\delta}H(g)^{-\eta}$ met zo klein mogelijke waarden voor δ en η in termen van de hoogtes van f en g, waarbij c alleen afhangt van het getallenlichaam dat door α en β wordt voortgebracht. In dit proefschrift bewijzen we een stelling over het analoge probleem voor algebraïsche functies in plaats van algebraïsche getallen, met effectieve constanten c, δ en η.

De opzet van dit proefschrift is als volgt. In hoofdstuk 1 introduceren we de benodigde notatie, en verzamelem we enkele hulpresultaten die later worden gebruikt. In hoofdstuk 2 noemen we de ABC-stelling voor algebraïsche functies van Mason en een generalisatie daarvan van Brownawell en Masser, en leiden een verdere generalisatie af. Vervolgens leiden we in hoofdstuk 3

een analogon voor algebraïsche functies af van een stelling van Evertse in de meetkunde der getallen die een toepassing is van de tweede stelling van Minkowski voor convexe gebieden. Dit gebruiken we in hoofdstuk 4 om een reductietheorie voor binaire vormen over $\mathbb{C}[t]$ af te leiden. In hoofdstuk 5 bewijzen we het analogon van Evertse's vermoeden voor gereduceerde binaire vormen over $\mathbb{C}[t]$ door de resultaten uit de eerdere hoofdstukken te combineren. in hoofdstuk 6 kijken we naar het aantal equivalentieklassen van binair vormen over $\mathbb{C}[t]$ van gegeven discriminant. In de laatste twee hoofdstukken bekijken we de (goed gedefinieerde) afstand tussen twee algebraïsche functies α en β en leiden hiervoor een effectieve ondergrens af, eerst in het geval dat α en β geconjugeerd zijn over $\mathbb{C}(t)$, en daarna wanneer ze niet geconjugeerd zijn over $\mathbb{C}(t)$.