Fakultät für Elektrotechnik, Informatik und Mathematik

Diplomarbeit im Studiengang
Mathematik

Analyse von verallgemeinerten RSA Polynomen mit Hilfe der Coppersmith'schen Methode

von
Benedikt Brieden

Paderborn, den 28.02.2007

Erklärung

Ich versichere, dass ich die beiliegende Diplomarbeit ohne Hilfe Dritter und ohne anderer als der angegebenen Quellen und Hilfsmittel angefertigt und die den benutzten Quellen wörtlich oder inhaltlich entnommenden Stellen als solche kenntlich gemacht habe.

Paderborn, den 28.02.2007

Benedikt Brieden

Inhaltsverzeichnis

Kapitel 1

Einleitung

In der heutigen Zeit, da ein Großteil der Kommunikation digital erfolgt und online-Dienste eine immer größere Rolle einnehmen, gewinnen die Verschlüsselungstechniken, die eine sichere Datenübertragung gewährleisten, immer mehr an Bedeutung. So möchte man z.B. nicht, dass ein unbekannter Dritter den E-Mail- oder Banktransfer abfangen und dekodieren kann.
Rivest, Shamir und Adleman entwickelten 1977 das sogenannte RSA-Verschlüsselungsverfahren, welches auch heute noch zu den am meist verbreitetsten und benutzten „public-key“ Verfahren gehört. Dieses asymmetrische Verfahren hat einen großen Vorteil gegenüber den bis dahin größtenteils benutzten symmetrischen Verschlüsselungen wie DES (Data Encryption Standard) oder AES (Advanced Encryption Standard). Während bei den Letzteren der geheime Schlüssel über ein Treffen oder eine sichere Leitung zwischen den Kommunikationspartnern ausgetauscht werden muß, so ist dies bei den asymmetrischen Verfahren nicht mehr nötig. Es genügt, den öffentlichen Schlüssel über eine frei zugängliche Leitung zu übermitteln.

Die Sicherheit des RSA-Verfahrens beruht auf dem auch jetzt noch aktuellen Stand, dass die Multiplikation zweier Zahlen (in diesem Fall $N = pq$) einfach zu berechnen ist, wohingegen die Zerlegung einer großen Zahl in deren Primfaktoren ein extrem hoher Zeitaufwand ist.
Die genaue RSA-Verschlüsselung erfolgt, indem man zuerst zwei unterschiedliche Primzahlen p und q wählt und deren Produkt $N = pq$ bildet. Als nächstes berechnet man die Eulersche-Phi-Funktion von N, also $\Phi(N) = (p-1)(q-1)$. Danach bestimmt man eine zu $\Phi(N)$ teilerfremde Zahl e. Das Paar (N, e) nennt man den öffentlichen Schlüssel. Man berechnet jetzt den geheimen oder auch privaten Schlüssel d als multiplikativ Inverses zu e modulo $\Phi(N)$. Damit gilt

$$ed \equiv 1 \mod \Phi(N). \tag{1.1}$$

Mit Hilfe des öffentlichen Schlüssels (N, e) wird durch $y \equiv x^e \mod N$ der Plaintext x kodiert und man erhält den Chiffretext y. Durch $y^d \equiv (x^e)^d \equiv x \mod N$ wird der Chiffretext wieder zurück dekodiert.

Das Ziel vieler Angriffe auf RSA ist die Zerlegung von N in deren Primfaktoren p und q. Gelingt es, diese beiden Primzahlen einmal zu bestimmen, so

kann man $\Phi(N)$ und damit den geheimen Schlüssel d berechnen. Die Verschlüsselung wäre somit nicht mehr sicher. Ein wichtiges Utensil, um dies zu erreichen, ist das Finden von kleinen Nullstellen modularer Polynome.
Mit dieser Aufgabe befasst sich Coppersmith in seiner Veröffentlichung [Cop01]. Er gibt eine Methode an, um kleine Nullstellen $x_0 < X$ und $y_0 < Y$ bivariater Polynome $p(x, y)$ modulo e mit ganzzahligen Koeffizienten zu bestimmen und dabei X und Y zu maximieren. Seine Idee ist, eine Gruppe von Polynomen $p_1(x, y), p_2(x, y), \ldots, p_n(x, y)$ zu konstruieren, die alle die gleiche Nullstelle modulo e^m für ein geeignetes $m \in \mathbb{N}$ haben. Hat man solche Polynome gefunden, so muß auch eine ganzzahlige Linearkombination darüber dieselbe Nullstelle modulo e^m haben. Mit Hilfe des Lemmas von Howgrave-Graham ist es dann möglich, die Berechnung von Nullstellen modularer Polynome zu einer Berechnung von Nullstellen über den ganzen Zahlen zu vereinfachen. Hierfür gibt es Verfahren (z.B. Newton-Iteration, Sturm'sche Ketten), die in polynomieller Zeit arbeiten.

Mit Hilfe der Methode von Coppersmith zeigen Boneh und Durfee, dass es nicht ganz so einfach ist einen Nachteil des RSA-Verfahrens zu beheben. Da die Zeit zum Ver-/Entschlüsseln mit RSA um etwa einen Faktor 1000 größer als bei DES oder AES ist, könnte man dazu neigen, kleine Parameter d oder e zu wählen, um die Zeit zur Ver/-Entschlüsselung mit der RSA-Methode zu verringern. In der Veröffentlichung [BD00] zeigen Boneh und Durfee mit der Coppersmith'schen Methode allerdings, dass es für $d < N^{1-\frac{1}{2}\sqrt{2}} \approx N^{0.293}$ möglich ist in polynomieller Zeit auf die Faktorisierung von N zu schließen. Sie verbesserten hiermit die bis dahin beste Grenze $d < N^{0.25}$, aufgestellt von Wiener [Wie90]. Boneh und Durfee bekamen dieses Resultat, indem sie Funktionen der Form $f(x, y) = x(A + y) - 1$ mit $A \in \mathbb{Z}$ untersuchen. Diese Art von Funktionen leiten sie aus der Gleichung (1.1) ab und benutzen die Methode von Coppersmith, um die Nullstelle (x_0, y_0) zu berechnen. Durch $y_0 = \frac{p+q}{2}$ und $N = pq$ erhalten sie dann die Primfaktoren p und q.
In den darauf folgenden Jahren gab es viele unterschiedliche Ansätze, um zu zeigen, dass das RSA-Verschlüsselungsverfahren unter bestimmten Voraussetzungen nicht sicher ist. So zeigen Bleichenbacher und May in [BM06], dass man RSA für $q < N^{0.468}$ erfolgreich angreifen kann. Ebenfalls mit der Coppersmith Methode arbeiteten Ernst, Jochemsz, May und de Weger [EJMdW05]. Dabei durchspielten sie drei mögliche Szenarien:

- Kennen der MSB (most significant bits, d.h. höchstwertigste Bits) von kleinem d
- Kennen der MSB von kleinem e
- Kennen der LSB (least significant bits, d.h. geringwertigste Bits) von kleinem d

In [BDF98] arbeiten Boneh, Durfee und Frankel mit einem ähnlichem Szenario. Sie zeigen, dass man bei einem kleinen öffentlichen Schlüssel e und Kenntnis von einem Viertel des geheimen Schlüssels d den gesamten geheimen Schlüssel bekommen kann.

Diese Diplomarbeit baut auf der Veröffentlichung von Boneh und Durfee [BD00]

auf. Aber anstatt Funktionen der Art $f(x, y) = x(A + y) - 1$ mit $A \in \mathbb{Z}$ zu untersuchen, betrachten wir, ebenfalls mit Hilfe der Coppersmith'schen Methode, verallgemeinerte Polynomgleichungen der Form

$$f(x, y) = \sum_{i=0}^{d_x} \sum_{j=0}^{d_y} a_{ij} x^i y^j$$

und

$$f(x, y) = \sum_{0 \leq i+j \leq d} a_{ij} x^i y^j.$$

Dafür stellen wir Bedingungen auf, unter denen man in polynomieller Zeit eine kleine Nullstelle (x_0, y_0) mit $x_0 < X$ und $y_0 < Y$ modulo e bestimmen kann. Die Werte X und Y werden anschließend maximiert, um eine Bewertung der Methode zu erlangen. Dabei unterscheiden wir den Fall, bei dem X und Y ungefähr von derselben Größenordnung sind und den Fall, bei dem $X < Y^\eta$ für $0 < \eta \leq 1$.

Eine kurze Übersicht über die einzelnen Kapitel:

Kapitel 2 dient der Festlegung von Bezeichnungen und Definitionen. Ausserdem werden die für diese Arbeit wichtigen Theoreme (z.B. das 1.Theorem von Minkowski) oder auch Verfahren (LLL-Reduktionsalgorithmus) beschrieben.

Kapitel 3 befasst sich mit einer ersten einfachen Funktion der Form $f(x, y) = (x - a_0)y + a_1 x + a_2,\ a_i \in \mathbb{Z}$, um ein Gefühl für die in dieser Arbeit behandelten Vorgehensweise zu bekommen.

Kapitel 4 verallgemeinert die im vorherigen Kapitel 3 gegebene Polynomgleichung für den balancierten Fall, d.h. dass die Schranken X und Y ungefähr gleich groß sind.

Kapitel 5 behandelt die gleichen Polynomgleichungen wie Kapitel 4. Der Unterschied besteht darin, dass X und Y nicht mehr von derselben Größenordnung sein müssen, sondern dass $X < Y^\eta$ mit $0 < \eta \leq 1$ gilt.

Kapitel 2

Grundlagen

Der erste Abschnitt dieses Kapitels dient der Einführung in die Gittertheorie. Dazu müssen Begriffe wie Gitter, Basismatrix, Determinante eines Gitters und damit in Zusammenhang stehende Notationen geklärt werden. Der zweite Abschnitt befasst sich mit dem 1. Theorem von Minkowski, das eine obere Abschätzung für den kürzesten, nichttrivialen Vektor eines Gitters liefert.
Bei vielen Problemen in der Kryptoanalysis beschäftigt man sich mit der Suche nach kleinen Nullstellen von modularen Polynomen. Mit Hilfe des LLL-Reduktionsalgorithmus', oder auch einfach LLL-Algorithmus, benannt nach seinen drei Entwicklern H.W. Lenstra, A.K. Lenstra, L.Lovász [LJL82], und dem Lemma von Howgrave-Graham werden im weiteren Verlauf dieser Arbeit Bedingungen aufgestellt, unter denen es möglich ist, kleine Nullstellen von modularen Polynomen in polynomieller Zeit zu bestimmen. Daher bildet der LLL-Algorithmus das Thema des dritten und das Lemma von Howgrave-Graham des vierten Abschnitts.

2.1 Gitter

Definition 2.1 *Seien $b_1, \ldots, b_n$ beliebige linear unabhängige Vektoren im $\mathbb{R}^m$. Dann bezeichne*

$$L := L(b_1, \ldots, b_n) := \sum_{i=1}^{n} \mathbb{Z} b_i$$

das durch die Vektoren $b_1, \ldots, b_n$ aufgespannte Gitter der Dimension $\dim(L) = n$. Die Matrix $B = (b_1, \ldots, b_n)$ nennt man Basismatrix von L. Ist andererseits $B = (b_1, ..., b_n) \in \mathbb{R}^{m \times n}$ eine Matrix, deren Spaltenvektoren linear unabhängig sind, so heißt $L(B)$ das durch die Matrix B erzeugte oder aufgespannte Gitter.

Im ersten Abschnitt des Kapitels befassen wir uns mit der allgemeinen Definition eines Gitters, d.h. $b_1, \ldots, b_n \in \mathbb{R}^m$. Im weiteren Verlauf dieser Arbeit werden allerdings nur Vektoren im $\mathbb{Z}^m$ betrachtet.
Abbildung 2.1 zeigt ein Beispiel eines einfachen Gitters. Dieses wurde durch die Matrix

$$B_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

erzeugt. Allerdings ist die Basismatrix B_1 nicht eindeutig durch das Gitter bestimmt. Es gibt sogar unendlich viele Basismatrizen ein und desselben Gitters. In diesem Fall spannt z.B. auch

$$B_2 = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}$$

das Gitter aus Abbildung 2.1 auf. Durch Multiplikation mit einer Transformationsmatrix T kann man eine Basismatrix in eine andere transformieren. Diese Matrizen T haben die Eigenschaft, dass ihre Determinante $\det(T) = \pm 1$ ist, was zu folgender Definition führt.

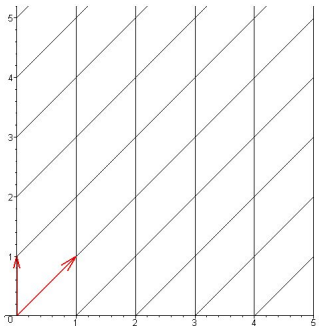

Abbildung 2.1: *Beispiel für ein 2-dimensionales Gitter*

Definition 2.2 *Sei B eine $(m \times n)$-Basismatrix eines Gitters L. Die Determinante von L ist dann definiert als*

$$\det(L) := (|\det(B^t B)|)^{\frac{1}{2}}.$$

Im Folgenden werden $(n \times n)$-Basismatrizen konstruiert. Definition 2.2 läßt sich dann vereinfachen zu $\det(L) = |\det(B)|$. In dieser Arbeit werden wir nicht nur quadratische Matrizen erzeugen, sondern auch noch solche, die eine obere oder untere Dreiecksgestalt haben. Dadurch lassen sich die Determinanten der durch diese Basismatrizen aufgespannten Gitter durch die Multiplikation der einzelnen Diagonalelemente von B berechnen.

Bemerkung 2.1 *Sei $B = (b_1, ..., b_n)$ eine $(n \times n)$-Basismatrix eines Gitters L. Außerdem sei B eine untere oder obere Dreiecksmatrix. Dann lässt sich die Determinante von L berechnen durch*

$$\det(L) := \prod_{i=1}^{n} |b_{ii}|.$$

2.2 1. Theorem von Minkowski

In dieser Arbeit befassen wir uns nun mit der Länge des kürzesten von 0 verschiedenen Vektors eines Gitters. Das 1.Theorem von Minkowski liefert dafür eine obere Schranke. Um dieses Theorem beweisen zu können, werden zwei Sätze von Blichfeldt und von Minkowski benötigt. Bei dem Satz von Minkowski handelt es sich um das sogenannte „convex body theorem“.
Da im Folgenden hauptsächlich die euklidische Norm $\|.\|_2$ gebraucht wird, wird sie der Einfachheit halber mit $\|.\|$ bezeichnet. Desweiteren gebe $\mathrm{vol}(S)$ das Volumen einer messbaren Menge S an.

Definition 2.3 *Sei $B = (b_1, \ldots, b_n)$ eine Basismatrix des Gitters L. Dann ist die Fundamentalregion der Basis B definiert als*

$$P(B) = \left\{ \sum_{i=1}^{n} r_i b_i | 0 \leq r_i < 1 \right\}$$

Die Menge $P(B)$ bezeichnet man auch als ein halboffenes Parallelepiped.

Das Volumen der Fundamentalregion $P(B)$ ist gleich dem Absolutbetrag der Determinante von B, d.h. $\mathrm{vol}(P(B)) = |\det(B)| = \det(L)$.

Satz 2.1 (Blichfeldt) *Sei L ein beliebiges Gitter im $\mathbb{R}^n$ und S eine messbare Teilmenge des durch L aufgespannten Vektorraums. Falls vol(S) > det(L), so existieren zwei Punkte $z_1, z_2 \in S$ mit $z_1 \neq z_2$ und $z_1 - z_2 \in L$.*

Beweis: Sei B eine Basis des Gitters L. Wenn x alle Punkte von L durchläuft, so bilden die Mengen $x + P(B) = \{x + y | y \in P(B)\}$ eine Partition von $\mathbb{R}^n$. Mit $S_x = S \cap (x + P(B))$ erhält man $S = \bigcup_{x \in L} S_x$ und damit

$$\mathrm{vol}(S) = \sum_{x \in L} \mathrm{vol}(S_x).$$

Nun definieren wir die Mengen $\widehat{S_x} := S_x - x$ für alle $x \in L$. Hierdurch werden die Mengen S_x alle in die Fundamentalregion verschoben, d.h. $\widehat{S_x} \in P(B)$. Wegen der Translationsinvarianz des Volumens gilt $\mathrm{vol}(S) = \sum_{x \in L} \mathrm{vol}(\widehat{S_x})$.
Da das Volumen des Parallelepipeds gleich der Determinante des Gitters ist, gilt nach Voraussetzung

$$\sum_{x \in L} \mathrm{vol}(\widehat{S_x}) = \mathrm{vol}(S) > \det(L) = \mathrm{vol}(P(B)).$$

Das bedeutet, dass zwei Punkte $x, y \in L$ mit $x \neq y$ existieren, für die $\widehat{S_x} \cap \widehat{S_y} \neq \emptyset$ gilt. Sei $z \in \widehat{S_x} \cap \widehat{S_y}$, so erhält man duch $z_1 := z + x$ und $z_2 := z + y$ zwei Punkte in S_x bzw. S_y. Die Differenz $z_1 - z_2$ liegt aber in L, denn $z_1 - z_2 = (z + x) - (z + y) = x - y \in L$. □

Satz 2.2 (convex body theorem) *Sei L ein Gitter im $\mathbb{R}^n$ und S eine konvexe, ursprungssymmetrische Menge in dem von L aufgespannten Raum. Wenn vol(S) > $2^n \det(L)$, dann enthält S einen nichttrivialen, d.h. vom Ursprung verschiedenen, Gitterpunkt.*

Beweis: Definiere $S' = \frac{1}{2}S = \{x | 2x \in S\}$. Es gilt $\text{vol}(S') = 2^{-n}\text{vol}(S) > \det(L)$. Nach dem Satz von Blichfeldt (Satz 2.1) existieren zwei Punkte $z_1, z_2 \in S'$, so dass $z_1 - z_2 \in L$ ein von 0 verschiedener Gitterpunkt ist. Durch die Definition von S' sind $2z_1, 2z_2 \in S$ und aufgrund der Symmetrie von S zum Ursprung gilt auch $-2z_2 \in S$. Wegen der Konvexität von S erhält man

$$\frac{2z_1 - 2z_2}{2} = z_1 - z_2 \in S.$$

□

Wie schon zuvor erklärt, dienen die beiden vorangegangenen Sätze in dieser Arbeit dem Beweis des 1. Theorems von Minkowski.

Theorem 2.1 (1. Theorem von Minkowski) *Sei L ein Gitter der Dimension $\dim(L) = n$. Dann gilt für die Länge λ_1 des kürzesten von 0 verschiedenen Vektors des Gitters folgende obere Abschätzung.*

$$\lambda_1 \leq \sqrt{n}\det(L)^{\frac{1}{n}}$$

Beweis: Wir betrachten eine n-dimensionale Kugel $B(0, r)$ mit Radius r um den Ursprung in dem von L erzeugten Vektorraum. Die Kugel enthält einen n-dimensionalen Würfel C, dessen Diagonale die Länge $2r$ hat. Damit ergibt sich für die Kantenlänge des Würfels $\frac{2r}{\sqrt{n}}$ und man erhält für das n-dimensionale Volumen:

$$\text{vol}(B(0, r)) \geq \text{vol}(C) = (\frac{2r}{\sqrt{n}})^n \tag{2.1}$$

Sei $S = B(0, \lambda_1)$ eine offene Kugel, so ist S konvex und symmetrisch zum Ursprung. Da S nach der Definition von λ_1 keinen von 0 verschiedenen Gitterpunkt enthält, folgt nach dem convex body theorem (Satz 2.2) und Formel (2.1), dass

$$(\frac{2\lambda_1}{\sqrt{n}})^n \leq \text{vol}(S) \leq 2^n \det(L)$$

und somit

$$\lambda_1 \leq \sqrt{n}\det(L)^{\frac{1}{n}}.$$

□

2.3 Der LLL-Reduktionsalgorithmus

Oft wünscht man sich, dass man mit einer Basismatrix eines Gitters arbeitet, die eine einfache Struktur hat, d.h., dass die Basisvektoren paarweise orthogonal aufeinanderstehen und eine möglichst kurze Norm haben. Bei Eingabe von n Vektoren $u_1, \ldots, u_n$ liefert uns das Gram-Schmidt-Orthogonalisierungsverfahren Vektoren $u_1^*, \ldots, u_n^*$, die die Eigenschaft der paarweisen Orthogonalität aufweisen. Der Nachteil dieses Verfahrens ist allerdings, dass die Ausgabevektoren

$u_1^*, \ldots, u_n^*$ zwar denselben Untervektorraum erzeugen wie die Eingabevektoren $u_1, \ldots, u_n$, aber nicht unbedingt dasselbe Gitter aufspannen. Beim Gram-Schmidt-Verfahren werden die b_i^* für $i = 1, \ldots, n$ rekursiv definiert durch

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*, \quad \text{für} \quad i = 2, \ldots, n \quad \text{mit} \quad \mu_{ij} := \frac{b_i b_j^*}{\|b_j^*\|^2}. \tag{2.2}$$

Mit $B = (b_1, \ldots, b_n)$ und $B^* = (b_1^*, \ldots, b_n^*)$ können wir die letzte Gleichung umschreiben zu

$$B = B^* \cdot \begin{pmatrix} 1 & & & & \\ \mu_{21} & 1 & & & \\ \mu_{31} & \mu_{32} & 1 & & \\ \vdots & & & \ddots & \\ \mu_{n1} & \mu_{n2} & \mu_{n3} & \cdots & 1 \end{pmatrix}$$

und somit ergibt sich für die Determinante des Gitters $L(B)$

$$\det(L) = |\det(B)| = |\det(B^*)|.$$

Hat das Gitter $L(B) \in \mathbb{R}^m$ vollen Rang, d.h. $\dim(L) = n = m$, dann gilt aufgrund der Orthogonalität der Spaltenvektoren von B^*

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\|. \tag{2.3}$$

Als nächstes werden wir uns mit dem Begriff der LLL-reduzierten Basis beschäftigen. Dazu folgende Definitionen:

Definition 2.4 *Eine Basis $B = (b_1, \ldots, b_n)$ des Gitters L heißt* längenreduziert*, falls für die μ_{ij} aus dem Gram-Schmidt-Verfahren gilt:*

$$|\mu_{ij}| \leq \frac{1}{2} \quad \textit{für} \quad i = 2, \ldots, n;\ j < i$$

B heißt LLL-reduziert, falls

(i) B längenreduziert ist und

(ii) $\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2$ für $1 \leq i < n$.

Bei einer Eingabe von n linear unabhängigen Basisvektoren $u_1, \ldots, u_n$ der Dimension m, deren Normen alle kleiner als γ sind, liefert der LLL-Algorithmus in $\mathcal{O}(n^5 m \log(\gamma)^3)$, d.h. in polynomieller Zeit, längenreduzierte Basisvektoren $b_1, \ldots, b_n$ desselben Gitters. Für eine präzisere Beschreibung des LLL-Algorithmus' verweise ich auf die original Publikation von Lenstra, Lenstra und Lovàsz [LJL82].

Die Länge des kürzesten Basisvektors muss nicht unbedingt der Länge λ_1 des kürzesten Gittervektors entsprechen. Jedoch kann die Länge des kürzesten Basisvektors nicht kleiner als die des kürzesten Gittervektors sein. Das folgende Lemma sagt etwas über das Verhältnis der beiden Längen zueinander aus.

Lemma 2.1 *Sei $B = (b_1, \ldots, b_n)$ eine LLL-reduzierte Gitterbasis des Gitters L. Dann gilt folgende obere Abschätzung für die Norm des kürzesten Basisvektors b_1:*

$$\|b_1\| \leq 2^{\frac{n-1}{2}} \lambda_1$$

Somit liefert der LLL-Algorithmus eine Gitterbasis, deren Basisvektoren „relativ orthogonal“ aufeinanderstehen und zusätzlich auch noch „relativ kurz“ sind.

Für den weiteren Verlauf werden obere Abschätzungen für die zwei kürzesten Vektoren einer LLL-reduzierten Gitterbasis benötigt.

Satz 2.3 *Sei $B = (b_1, \ldots, b_n)$ eine LLL-reduzierte Gitterbasis des Gitters $L \in \mathbb{Z}^n$. Dann gilt*

(i) $\|b_1\| \leq 2^{\frac{n}{2}} \det(L)^{\frac{1}{n}}$

(ii) $\|b_2\| \leq 2^{\frac{n}{2}} \det(L)^{\frac{1}{n-1}}$

Beweis: (i): Da $b_1 = b_1^*$ und nach (2.3) gilt

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\| = \|b_1^*\|^n 2^{-\frac{1}{2}\sum_{i=1}^{n-1} i} = \|b_1\|^n 2^{-\frac{(n-1)n}{4}} \geq \|b_1\|^n 2^{-\frac{n^2}{2}}$$

und somit

$$\|b_1\| \leq 2^{\frac{n}{2}} \det(L)^{\frac{1}{n}}$$

(ii): Nach demselben Muster geht man auch hier vor. Zusätzlich beachte man, dass $\|b_1\| \geq 1$ gilt, wegen $b_1 \in \mathbb{Z}^n$. Dadurch erhält man

$$\det(L) \geq \|b_1\| \|b_2^*\|^{n-1} 2^{-\frac{1}{2}\sum_{i=1}^{n-2} i} \geq \|b_1\| \|b_2^*\|^{n-1} 2^{-\frac{(n-1)^2}{2}}$$

und somit

$$\|b_2^*\| \leq 2^{\frac{n-1}{2}} \left(\frac{\det(L)}{\|b_1\|}\right)^{\frac{1}{n-1}} \leq 2^{\frac{n-1}{2}} \det(L)^{\frac{1}{n-1}}$$

Diese Ungleichung wird jetzt noch in Formel (2.2) eingesetzt und man bekommt

$$\begin{aligned} \|b_2\|^2 &= \|b_2^* + \mu_{21} b_1\|^2 \leq \|b_2^*\|^2 + \mu_{21}^2 \|b_1\|^2 \\ &\leq \det(L)^{\frac{2}{n-1}} 2^{n-1} + 2^{n-2} \det(L)^{\frac{2}{n}} \\ &\leq 2^n \det(L)^{\frac{2}{n-1}} (2^{-1} + 2^{-2} \det(L)^{\frac{n-1}{n}}) \\ &\leq 2^n \det(L)^{\frac{2}{n-1}} \end{aligned}$$

Durch ziehen der Wurzel erzielt man das gewünschte Ergebnis. □

2.4 Lemma von Howgrave-Graham

Damit kommen wir nun zu einem weiteren wichtigen Lemma dieses Kapitels. Dieses Lemma von Howgrave-Graham beschäftigt sich mit den Nullstellen von modularen Polynomen. Sei $p(x,y) = \sum_{i,j} a_{ij} x^i y^j$ ein Polynom in den zwei Unbestimmten x und y. Die Norm von p ist definiert als die euklidische Norm des Koeffizientenvektors, d.h. $\|p(x,y)\|^2 := \sum_{i,j} |a_{ij}|^2$.

Lemma 2.2 (Howgrave-Graham) *Sei $p(x,y) \in \mathbb{Z}[x,y]$ ein Polynom mit höchstens n Monomen. Angenommen es gebe $x_0 < X$ und $y_0 < Y$, so dass gilt*

(i) $p(x_0, y_0) \equiv 0 \; mod \; e^m$, $m \in \mathbb{N}$ *und*

(ii) $\|p(xX, yY)\| < \frac{e^m}{\sqrt{n}}$.

Dann gilt $p(x_0, y_0) = 0$ über $\mathbb{Z}$.

Beweis: Sei $p(x,y) = \sum_{i,j} a_{ij} x^i y^j$, so gilt

$$\begin{aligned} |p(x_0,y_0)| &= |\sum_{i,j} a_{ij} x_0^i y_0^j| = |\sum_{i,j} a_{ij} X^i Y^j \left(\frac{x_0}{X}\right)^i \left(\frac{y_0}{Y}\right)^j| \\ &\leq \sum_{i,j} |a_{ij} X^i Y^j \left(\frac{x_0}{X}\right)^i \left(\frac{y_0}{Y}\right)^j| \leq \sum_{i,j} |a_{ij} X^i Y^j| \\ &\overset{(\star)}{\leq} \sqrt{n}\|p(xX, yY)\| \overset{(ii)}{<} e^m \end{aligned}$$

Bei dem Schritt $(\star)$ wurde die Cauchy-Schwarzsche-Ungleichung benutzt. Unter Berücksichtigung von Bedingung (i) ist klar, dass $p(x_0, y_0) = 0$ über $\mathbb{Z}$. □

Im Folgenden wird beabsichtigt das Lemma von Howgrave-Graham auf die zwei kürzesten Vektoren einer LLL-reduzierten Gitterbasis anzuwenden. Angenommen man hat zwei Polynome $p_1(x,y) = \sum_{i,j} a_{ij} x^i y^j$ und $p_2(x,y) = \sum_{i,j} b_{ij} x^i y^j$ und (x_0, y_0) sei eine Nullstelle beider Polynome modulo e^m. Weiter sei a der Koeffizientenvektor von p_1 und b von p_2 mit $\|a\| \leq \|b\|$, so gilt nach obiger Definition von der Norm eines Polynoms: $\|p_1(x,y)\| = \|a\|$ und $\|p_2(x,y)\| = \|b\|$. Um das Lemma von Howgrave-Graham anwenden zu können, muß gezeigt werden, dass $\|a\| < \frac{e^m}{\sqrt{n}}$ bzw. $\|b\| < \frac{e^m}{\sqrt{n}}$. Kombiniert man dies mit Satz 2.3, so erhält man

$$2^{\frac{n}{2}} \det(L)^{\frac{1}{n}} < \frac{e^m}{\sqrt{n}},$$

für a und

$$2^{\frac{n}{2}} \det(L)^{\frac{1}{n-1}} < \frac{e^m}{\sqrt{n}},$$

für b, was sich umformen lässt zu

$$\det(L)^{\frac{1}{n}} < \frac{e^m}{\sqrt{n} 2^{\frac{n}{2}}} \quad \text{bzw.} \tag{2.4}$$

$$\det(L)^{\frac{1}{n-1}} < \frac{e^m}{\sqrt{n} 2^{\frac{n}{2}}} \tag{2.5}$$

In den weiteren Kapiteln werden zwei bivariate, linear unabhängige Polynome $f_1(x,y)$ und $f_2(x,y)$ konstruiert, auf die das Lemma von Howgrave-Graham (Lemma 2.2) angewendet wird, d.h. diese Polynome haben beide (x_0, y_0) als Nullstelle über den ganzen Zahlen. Berechnet man als nächstes die Resultanten $Res_x(f_1, f_2) = h_1(y)$ bzw. $Res_y(f_1, f_2) = h_2(x)$, so bekommt man zwei Funktionen $h_1(y)$ bzw. $h_2(x)$, die jeweils nur noch von einer Variablen abhängen und genauso wie f_1 und f_2 die Nullstellen y_0 bzw. x_0 über $\mathbb{Z}$ haben.
An dem Beispiel von Boneh und Durfee [BD00] wird gezeigt, dass sich diese Nullstellen leicht berechnen lassen und man somit auf die Faktorisierung von N schließen kann, wobei $N = pq$ Teil des öffentlichen Schlüssels beim RSA-Verschlüsselungsverfahren ist. Leider ist dieses Verfahren zur Berechnung der Nullstellen nur heuristisch. Die beiden Polynome f_1 und f_2 können in der Form, wie sie in dieser Arbeit erstellt werden, linear abhängig sein. Dadurch hätten sie einen gemeinsamen Faktor und die Resultanten würden 0 ergeben, womit keine Aussagen über die Nullstellen gemacht werden können.

Beispiel 2.1 *In dem Paper von Boneh und Durfee [BD00] werden Bedingungen aufgestellt, unter denen das RSA-Verschlüsselungsverfahren nicht mehr sicher ist, da man auf die Faktorisierung von N schließen kann. Der öffentliche Schlüssel ist gegeben durch (N, e), wobei die Faktorisierung von $N = pq$ nicht bekannt ist. Der zugehörige private Schlüssel ist d, mit $ed \equiv 1 \mod \frac{\Phi(N)}{2}$. Die Euler-Funktion Φ ist definiert durch $\Phi(N) = (p-1)(q-1) = N - p - q + 1$. Daraus können wir schließen, dass ein $x_0 \in \mathbb{Z}$ existiert mit*

$$ed + x_0 \left(\frac{N+1}{2} - \frac{p+q}{2} \right) = 1.$$

Mit $A := \frac{N+1}{2}$ und $y_0 := -\frac{p+q}{2}$ läßt sich die Gleichung umschreiben zu

$$x_0(A + y_0) \equiv 1 \mod e.$$

Definieren wir jetzt $f(x,y) := x(A+y) - 1$, so muss das Problem gelöst werden, x_0, y_0 zu finden, die der modularen Gleichung $f(x_0, y_0) \equiv 0 \mod e$ genügen. Boneh und Durfee geben noch die zusätzlichen Bedingungen $|x_0| < e^{\delta}$ und $|y_0| < e^{0,5}$ an. Man bezeichnet dieses Problem auch als das „small inverse problem“.
Boneh und Durfee zeigen nun, dass man für $\delta < 0.284$ (später auch für $\delta < 0.292$) die kleinen Nullstellen in polynomieller Zeit finden kann. Dazu konstruieren sie zwei Gruppen von Polynomen, $g_{i,k}(x,y) := x^i f^k(x,y) e^{m-k}$ und $h_{j,k}(x,y) := y^j f^k(x,y) e^{m-k}$, die alle (x_0, y_0) als Nullstelle modulo e^m haben und deren Koeffizientenvektoren die Zeilen einer Matrix M bilden. Sei f_1 eine Linearkombination der g-Polynome und f_2 der h-Polynome, so haben sie dieselbe Nullstelle modulo e^m. Als nächstes berechnen sie unter Berücksichtigung der Gleichungen (2.4) und (2.5) die Schranke $\delta < 0.284$ (später $\delta < 0.292$). Danach schließen sie mit Hilfe der Resultanten von f_1 und f_2 auf das y_0. Damit hat man die beiden Gleichungen $y_0 = \frac{p+q}{2}$ und $pq = N$, wobei N und y_0 jetzt bekannt sind. Die Berechnungen von p und q sind nun trivial. Das bedeutet, dass man die Faktorisierung von N hat und somit das Verschlüsselungsverfahren unter den gegebenen Bedingungen nicht mehr sicher ist.

Kapitel 3

Eine erste einfache Funktion

Dieses Kapitel beschäftigt sich mit einer ersten einfachen Funktion $f = f(x, y) \in \mathbb{Z}[x, y]$, welche die Nullstelle (x_0, y_0) modulo e haben soll. Wir werden zwei Gruppen von Shifts definieren, die dieselbe Nullstelle haben, allerdings diesmal modulo e^m. Eine Linearkombinationen der Shifts hat dann ebenfalls die Nullstelle (x_0, y_0) modulo e^m. Auf diese Linearkombinationen werden wir dann das Lemma 2.2 von Howgrave-Graham anwenden.

3.1 Konstruktion

Die Funktion, mit der sich dieses Kapitel beschäftigt, hat die Form $f(x, y) = (x - a_0)y + a_1x + a_2,\ a_i \in \mathbb{Z}$ und soll die Nullstelle (x_0, y_0) modulo e haben. Als nächstes konstruieren wir uns für $l = 0, ..., m$ zwei Gruppen von Shifts, welche wir im Folgenden x-Shifts und y-Shifts nennen werden. Sei $m \in \mathbb{N}$ beliebig, dann definieren wir

$$
\begin{aligned}
l = 0, ..., m: \qquad & \text{x-Shifts:} \quad g_{i,k}(x, y) := x^i f^k(x, y) e^{m-k} && (3.1)\\
& \quad i = l - k; \quad k = 0, ..., l \\
& \text{y-Shifts:} \quad h_{j,k}(x, y) := y^j f^k(x, y) e^{m-k} && (3.2)\\
& \quad j = l - k; \quad k = 0, ..., l - 1
\end{aligned}
$$

Da $f(x_0, y_0) \equiv 0 \mod e$, ist einzusehen, dass sowohl die $g_{i,k}$'s, als auch die $h_{j,k}$'s die gleiche Nullstelle haben, nur diesmal nicht modulo e, sondern modulo e^m. Als nächstes müssen die Ungleichungen (2.4) und (2.5) aus dem vorherigen Kapitel erfüllt werden. Dafür benötigen wir die Determinante der durch die Koeffizientenvektoren der Shifts erzeugten Matrix, welche wir von nun an mit B bezeichnen werden. Die Koeffizientenvektoren der Shifts $g_{i,k}(xX, yY)$ und $h_{j,k}(xX, yY)$ bilden die Zeilen von B. Um uns die Berechnung der Determinanten etwas zu vereinfachen, werden wir zeigen, dass wir B zu einer unteren Dreiecksmatrix umwandeln können, indem wir eine spezielle Reihenfolge bei den Shifts wählen.
Hierfür betrachten wir zuerst die Anordnung der Zeilen der Matrix. Die letzte

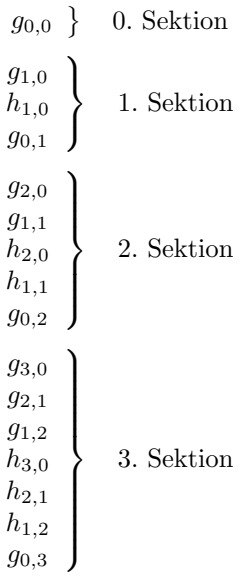

Abbildung 3.1: *Einteilung des Gitters in Sektionen für $m = 3$*

Zeile der Matrix zeigt die Koeffizienten von $g_{0,m}$. Nun unterteilen wir die Zeilen in Sektionen. Jede Sektion endet mit den Koeffizienten von $g_{0,l}$, $0 \leq l \leq m$. Damit gibt es insgesamt $m+1$ Sektionen. Die Anordnung innerhalb der l-ten Sektion ist folgende. Zuerst kommen die Koeffizienten der x-shifts $g_{i,k}$, mit $i = l-k$ und $k = 0, ..., l-1$, darauf folgen die der y-Shifts $h_{j,k}$ mit $j = l-k$ und $k = 0, .., l-1$. Als letztes in jeder Sektion erscheinen dann die Koeffizienten von $g_{0,l}$.
Abbildung 3.1 zeigt die Aufteilung der Zeilen in Sektionen für $m = 3$.
Als nächstes muss gezeigt werden, dass wir hierdurch eine untere Dreiecksgestalt bekommen, d.h., dass in jeder Zeile genau ein neues Element hinzukommt.

Satz 3.1 *Die durch die x- und y-Shifts (3.1) und (3.2) erzeugte Matrix hat eine untere Dreiecksgestalt.*

Beweis: Wir werden hier jetzt zeigen, dass wir in jeder Zeile der Matrix immer genau ein neues Monom erhalten, was äquivalent zu der Aussage des Satzes ist. Da uns hier nur die Monome der Shifts interessieren, werden wir die Koeffizienten vorerst vernachlässigen.
Zuerst wird bewiesen, dass das erste Polynom einer jeden Sektion genau ein neues Monom enthält. Danach zeigen wir, dass bei den aufeinanderfolgenden x- bzw. y-Shifts nur ein neues Monom auftaucht. Zuletzt wird gezeigt, dass auch das letzte Polynom einer jeden Sektion genau ein neues Monom liefert. Mit dem Ausdruck „g ist enthalten in h“ ist in diesem Beweis gemeint, dass die Monome des Polynoms g auch Monome des Polynoms h sind.
Die höchste Potenz von x für $g_{i,k}$ ist gegeben durch $i + k$. Das erste Polynom einer jeden Sektion hat die Form $g_{l,0}$ für $l = 0, \ldots, m$ und besteht somit nur

	1	x	y	xy	x^2	x^2y	y^2	xy^2	x^2y^2	x^3	x^3y	x^3y^2	y^3	xy^3	x^2y^3	x^3y^3
$g_{0,0}$	e^3															
$g_{1,0}$		e^3X														
$h_{1,0}$			e^3Y													
$g_{0,1}$	$-$	$-$	$-$	e^2XY												
$g_{2,0}$					e^3X^2											
$g_{1,1}$		$-$		$-$	$-$	e^2X^2Y										
$h_{2,0}$							e^3Y^2									
$h_{1,1}$			$-$	$-$			$-$	e^2XY^2								
$g_{0,2}$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	eX^2Y^2							
$g_{3,0}$										e^3X^3						
$g_{2,1}$					$-$	$-$				$-$	e^2X^3Y					
$g_{1,2}$		$-$		$-$	$-$	$-$		$-$	$-$	$-$	$-$	eX^3Y^2				
$h_{3,0}$													e^3Y^3			
$h_{2,1}$							$-$	$-$					$-$	e^2XY^3		
$h_{1,2}$			$-$	$-$		$-$	$-$	$-$	$-$				$-$	$-$	eX^2Y^3	
$g_{0,3}$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	X^3Y^3

Abbildung 3.2: *Matrix für* $m = 3$

aus einem einzigen Monom, nämlich x^l. Da zuvor nur kleinere Potenzen von x vorgekommen sind, muss dieses Monom neu sein und der erste Teil des Beweises wäre gezeigt.
Die Monome von f sind $\{1, x, y, xy\}$. Für den Fall der aufeinanderfolgenden x-Shifts betrachten wir den Schritt von $g_{l-n,n} = x^{l-n}f^n$ zu $g_{l-n-1,n+1} = x^{l-n-1}f^{n+1} = x^{l-n-1}f^nf = g_{l-n-1,n}f$ für $0 \leq n \leq l-2$. Jetzt wird die Multiplikation mit f für jedes Monom einzelnd untersucht. Somit bekommt man

$$\begin{aligned}
1 \cdot g_{l-n-1,n} &= g_{l-n-1,n} \\
x \cdot g_{l-n-1,n} &= x^{l-n}f^n = g_{l-n,n} \\
y \cdot g_{l-n-1,n} &= yx^{l-n-1}f^n && \text{ist enthalten in} && g_{0,l-1} \\
xy \cdot g_{l-n-1,n} &= yx^{l-n}f^n && \text{liefert ein neues Monom:} && x^ly^{n+1}
\end{aligned}$$

Analog verläuft die Beweisführung bei den y-Shifts. Damit wäre auch der zweite Teil bewiesen.
Der letzte Teil besteht daraus, dass man zeigen muss, dass das letzte Polynom einer jeden Sektion, also $g_{0,l} = f^l = ff^{l-1}$ ein neues Monom liefert. Wie zuvor unterteilen wir das Produkt ff^{l-1} wieder in die Multiplikation mit den einzelnen Monomen von f.

$$\begin{aligned}
1 \cdot f^{l-1} && \text{ist enthalten in} && g_{0,l-1} \\
x \cdot f^{l-1} && \text{ist enthalten in} && g_{1,l-1} \\
y \cdot f^{l-1} && \text{ist enthalten in} && h_{1,l-1} \\
xy \cdot f^{l-1} && \text{liefert ein neues Monom:} && x^ly^l
\end{aligned}$$

Damit wäre zum einen die Aussage des Satzes bewiesen und zum anderen wurde gezeigt, dass immer das Monom xy von f das neue Monom liefert, d.h. für $g_{i,k}$ ist das neue Monom gegeben durch $x^{i+k}y^k$ und für $h_{j,k}$ durch x^ky^{j+k}. □

3.2 Determinantenberechnung

Da wir gezeigt haben, dass es sich hierbei um eine obere Dreicksmatrix handelt, können wir zur Berechnung der Determinanten Bemerkung 2.1 benutzen und brauchen nur noch die Diagonalelemente betrachten. Wie im Beweis zu Satz 3.1 gezeigt, gibt das Monom xy von f den Eintrag auf der Hauptdiagonalen. Bildet man nun die Shifts $g_{i,k}(xX, yY)$ bzw. $h_{j,k}(xX, yY)$ und mit deren Koeffizientenvektoren eine Matrix, so bekommen wir jeweils als Hauptdiagonaleintrag $X^{i+k}Y^k e^{m-k}$ bzw. $X^k Y^{j+k} e^{m-k}$. Da die Determinante durch das Produkt dieser Diagonalwerte gegeben ist, können wir die Einträge aufspalten in diejenigen, die die x-Shifts und in diejenigen, die die y-Shifts liefern. Im Folgenden bezeichne Potenz(g_X) die Potenz von X, die wir durch die x-Shifts $g_{i,k}$ bekommen. Analog definieren wir Potenz(g_Y), Potenz(g_e), Potenz(h_X), Potenz(h_Y) und Potenz(h_e). Bevor wir zur Determinantenberechnung kommen, benötigen wir noch ein Lemma über zwei spezielle arithmetische Summen.

Lemma 3.1 *Es gelten folgende Formeln zur Berechnung arithmetischer Summen:*

(a) $$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

(b) $$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$$

Damit hätten wir alles, was wir für die Determinantenberechnung brauchen und formulieren

Satz 3.2 *Durch die Aufspaltung der Determinanten in die Anteile det(L_g), die die x-Shifts liefern, und die Anteile det(L_h), die die y-Shifts liefern, bekommen wir*

$$\det(L_g) = X^{\frac{m(m+1)(m+2)}{3}} Y^{\frac{m(m+1)(m+2)}{6}} e^{\frac{m(m+1)(m+2)}{3}} \quad (3.3)$$

$$\det(L_h) = X^{\frac{m(m+1)(m-1)}{6}} Y^{\frac{m(m+1)(2m+1)}{6}} e^{\frac{m(m+1)(2m+1)}{6}} \quad (3.4)$$

Beweis: Das die Einträge auf der Hauptdiagonalen die Form $X^{i+k}Y^k e^{m-k}$ (für die x-Shifts) bzw. $X^k Y^{j+k} e^{m-k}$ (für die y-Shifts) haben, wurde bereits vorher erklärt. Dadurch können wir die Potenzen von X, Y und e separat berechnen

durch

$$\begin{aligned}
\text{Potenz}(g_X) &= \sum_{l=0}^{m}\sum_{k=0}^{l} i+k = \sum_{l=0}^{m}\sum_{k=0}^{l} l-k+k = \sum_{l=0}^{m}\sum_{k=0}^{l} l = \sum_{l=0}^{m} l(l+1) \\
&= \sum_{l=0}^{m} l^2+l = \frac{m(m+1)(2m+1)}{6} + \frac{m(m+1)}{2} \\
&= \frac{m(m+1)(m+2)}{3} \\
\text{Potenz}(g_Y) &= \sum_{l=0}^{m}\sum_{k=0}^{l} k = \sum_{l=0}^{m} \frac{l^2+l}{2} = \frac{m(m+1)(m+2)}{6} \\
\text{Potenz}(g_e) &= \sum_{l=0}^{m}\sum_{k=0}^{l} m-k = \sum_{l=0}^{m} m(l+1) - \frac{l^2+l}{2} \\
&= \sum_{l=0}^{m} m + (m-\frac{1}{2})l - \frac{1}{2}l^2 \\
&= m(m+1) + (m-\frac{1}{2})\frac{m(m+1)}{2} - \frac{1}{2}\frac{m(m+1)(2m+1)}{6} \\
&= \frac{m(m+1)(m+2)}{3}.
\end{aligned}$$

Damit ergibt sich Behauptung (3.3). Auf die gleiche Weise berechnen wir die Potenzen bei den y-Shifts

$$\begin{aligned}
\text{Potenz}(h_X) &= \sum_{l=0}^{m}\sum_{k=0}^{l-1} k = \sum_{l=0}^{m} \frac{l^2-l}{2} = \frac{1}{2}(\frac{m(m+1)(2m+1)}{6} - \frac{m(m+1)}{2}) \\
&= \frac{m(m+1)(m-1)}{6} \\
\text{Potenz}(h_Y) &= \sum_{l=0}^{m}\sum_{k=0}^{l-1} j+k = \sum_{l=0}^{m}\sum_{k=0}^{l-1} l = \sum_{l=0}^{m} l^2 \\
&= \frac{m(m+1)(2m+1)}{6} \\
\text{Potenz}(h_e) &= \sum_{l=0}^{m}\sum_{k=0}^{l-1} m-k = \sum_{l=0}^{m} ml - \frac{l^2-l}{2} \\
&= (m+\frac{1}{2})\frac{m(m+1)}{2} - \frac{m(m+1)(2m+1)}{12} \\
&= \frac{m(m+1)(2m+1)}{6}.
\end{aligned}$$

Somit wäre dann auch Behauptung (3.4) und damit Satz 3.2 bewiesen. □

Um nun die Determinante der durch die x- und y-Shifts erzeugten Matrix zu berechnen, brauchen wir nur die beiden Behauptungen (3.3) und (3.4) zusammenzufassen und erhalten

Folgerung 3.1 *Die Determinante der durch die Shifts (3.1) und (3.2) erzeugten Matrix ist*

$$\det(L) = (XY)^{\frac{m(m+1)^2}{2}} e^{\frac{m(m+1)(4m+5)}{6}} \tag{3.5}$$

Beweis: Fassen wir die Potenzen von X,Y und e aus (3.3) und (3.4) zusammen, so erhalten wir:

$$\begin{aligned}
\text{Potenz}(X) &= \frac{m(m+1)(m+2)}{3} + \frac{m(m+1)(m-1)}{6} = \frac{m(m+1)(3m+3)}{6} \\
&= \frac{m(m+1)^2}{2} \\
\text{Potenz}(Y) &= \frac{m(m+1)(m+2)}{6} + \frac{m(m+1)(2m+1)}{6} = \frac{m(m+1)(3m+3)}{6} \\
&= \frac{m(m+1)^2}{2} \\
\text{Potenz}(e) &= \frac{m(m+1)(m+2)}{3} + \frac{m(m+1)(2m+1)}{6} = \frac{m(m+1)(4m+5)}{6}
\end{aligned}$$

□

3.3 Schrankenberechnung

Mit Hilfe der Gleichung (3.5) aus Folgerung 3.1 wollen wir eine Schranke für XY bestimmen. Hierfür benutzen wir die oben hergeleiteten Ungleichungen (2.4) und (2.5), wobei n die Dimension von L, also von dem Gitter, das durch die Matrix erzeugt wird, angibt. In diesem Fall gilt

$$\begin{aligned}
n = \dim(L) &= \sum_{l=0}^{m}\sum_{k=0}^{l} 1 + \sum_{l=0}^{m}\sum_{k=0}^{l-1} 1 \\
&= \sum_{l=0}^{m}(l+1) + \sum_{l=0}^{m} l \\
&= (m+1) + \frac{m(m+1)}{2} + \frac{m(m+1)}{2} \\
&= (m+1)^2. \qquad (3.6)
\end{aligned}$$

Jetzt haben wir alles beisammen, was wir zu Bestimmung einer oberen Schranke für XY benötigen und können somit eine Bedingung aufstellen, unter der wir kleine Nullstellen unseres Polynoms $f(x,y) = (x-a_0)y + a_1x + a_2$ bestimmen können.

Satz 3.3 *Gilt*

$$XY < e^{\frac{(m-1)(2m+5)}{3(m+1)(m+1)}\gamma - \frac{2(m+2)}{(m+1)(m+1)}}$$

mit $\gamma = (m+1)2^{\frac{(m+1)(m+1)}{2}}$*, so können wir kleine Nullstellen unseres Polynoms* $f(x,y) = (x-a_0)y + a_1x + a_2$ *bestimmen.*

Beweis: Da (2.5) eine schärfere Schranke für die Determinante ergibt als (2.4), werden wir nun unsere berechneten Formeln (3.5) und (3.6) in Ungleichung (2.5) einsetzen. Somit sind folgende Ungleichungen äquivalent

$$e^{\frac{m(m+1)(4m+5)}{6((m+1)^2-1)}}(XY)^{\frac{m(m+1)^2}{2((m+1)^2-1)}} < \frac{e^m}{\gamma}$$

$$e^{\frac{m(m+1)(4m+5)}{6}}(XY)^{\frac{m(m+1)^2}{2}} < e^{m((m+1)^2-1)_\gamma - ((m+1)^2-1)}$$

$$e^{\frac{m(m+1)(4m+5)}{6}}(XY)^{\frac{m(m+1)^2}{2}} < e^{m^2(m+2)_\gamma - m(m+2)}$$

$$(XY)^{\frac{m(m+1)^2}{2}} < e^{m^2(m+2) - \frac{m(m+1)(4m+5)}{6}_\gamma - m(m+2)}$$

$$XY < e^{\frac{2m(m+2)}{(m+1)^2} - \frac{4m+5}{3(m+1)}_\gamma - \frac{2(m+2)}{(m+1)^2}}$$

$$XY < e^{\frac{(m-1)(2m+5)}{3(m+1)^2}_\gamma - \frac{2(m+2)}{(m+1)^2}}.$$

Benutzt man nicht die Ungleichung (2.5), sondern (2.4), so erhält man die etwas überschaubarere Schranke

$$XY < \gamma^{-\frac{2}{m}} e^{\frac{2m+1}{3(m+1)}}$$

□

Zum Abschluß dieses Kapitels ziehen wir noch eine Folgerung aus dem letzten Satz.

Korollar 3.1 *Man kann in polynomieller Zeit für alle $\epsilon > 0$ und $XY < e^{\frac{2}{3}-\epsilon}$ kleine Nullstellen unseres Polynoms $f(x,y) = (x-a_0)y + a_1x + a_2$ bestimmen.*

Beweis: Der vorherige Satz lieferte uns die Schranke

$$XY < e^{\frac{(m-1)(2m+5)}{3(m+1)(m+1)}_\gamma - \frac{2(m+2)}{(m+1)(m+1)}}$$

mit $\gamma = (m+1)2^{\frac{(m+1)(m+1)}{2}}$. Betrachtet man nun den Grenzwert für $m \to \infty$, so geht die Potenz von e gegen $\frac{2}{3}$, wohingegen der γ-Term gegen 0 strebt. □

Kapitel 4

Funktionen mit balancierten X und Y

In dem vorherigen Kapitel betrachteten wir ein einfaches Polynom, dass nur aus vier Monomen bestand. Dieses Kapitel dagegen arbeitet mit Polynomen mit beliebigem Grad. Die einzige Annahme die wir hier machen ist, dass X und Y ungefähr von derselben Größenordnung sein sollen. Das erste Unterkapitel untersucht Funktionen der Form $f(x,y) = \sum_{i=0}^{d_x} \sum_{j=0}^{d_y} a_{ij} x^i y^j$, wobei die Höchstpotenzen d_x und d_y von x und y unabhängig voneinander sind. Das zweite Unterkapitel beschäftigt sich mit den Polynomen $f(x,y) = \sum_{0 \leq i+j \leq d} a_{ij} x^i y^j$. Bei diesem Fall betrachtet man nur den totalen Höchstgrad der Funktion. Die Höchstpotenzen von x und y sind nicht mehr unabhängig voneinander.

4.1 Schrankenberechnung für allgemeine Funktionen

In diesem Unterkapitel betrachten wir den Fall, dass wir eine Funktion f der Form

$$f(x,y) = \sum_{i=0}^{d_x} \sum_{j=0}^{d_y} a_{ij} x^i y^j$$

haben, die die Nullstelle (x_0, y_0) modulo e hat. Im ersten Abschnitt dieses Unterkapitels untersuchen wir die Vorgehensweise für $d_x = d_y = d = 2$. Danach verallgemeinern wir das Ganze für beliebiges $d \in \mathbb{N}$, bevor wir zu beliebigen $d_x, d_y \in \mathbb{N}$ übergehen.

4.1.1 Fall d=2

Indem wir $d_x = d_y = d = 2$ setzen, erhalten wir für f

$$\begin{aligned} f(x,y) &= \sum_{i=0}^{2}\sum_{j=0}^{2} a_{ij}x^i y^j \\ &= a_{00} + a_{10}x + a_{20}x^2 + a_{01}y + a_{11}xy + a_{21}x^2y \\ &\quad + a_{02}y^2 + a_{12}xy^2 + a_{22}x^2y^2 \end{aligned}$$

mit

$$f(x_0, y_0) \equiv 0 \mod e$$

Im weiteren Verlauf dieses Abschnitts können wir ohne Beschränkung der Allgemeinheit $a_{00} = 1$ setzen.
Der Aufbau dieses Kapitels entspricht in etwa dem vorherigen. Zuerst werden die Shifts konstruiert, danach die Determinante der von den Koeffizientenvektoren der Shifts aufgespannten Matrix bestimmt und als letztes eine obere Schranke für XY berechnet. Allerdings besteht auch ein Unterschied zum vorherigen Kapitel. Diesmal erhalten wir keine untere, sondern eine obere Dreiecksmatrix. Da wir in 4.1.3 eine Verallgemeinerung dieses Unterkapitels betrachten, werden wir auch erst dann einen Beweis für die obere Dreiecksgestalt liefern. Ebenso lassen sich die Berechnungen aus den Ergebnissen in 4.1.3 ableiten. Daher werden wir hier auf die genauen Herleitungen der Formeln verzichten.

Als erstes benötigen wir Shifts, deren Koeffizientenvektoren die Zeilen der Matrix bilden. Für $m \in \mathbb{N}$ bel. definieren wir

$$\begin{array}{lll} g_{ijk}(x,y) = x^i y^j f^{m-k}(x,y)e^k & & \\ \quad i = 0,\ldots,2; & j = 0,\ldots,1; & k = 1 \\ \quad i = 0,\ldots,2(k-1); & j = 2(k-1)+1,\ldots,2k; & k = 2,\ldots,m \\ h_{ijk}(x,y) = x^i y^j f^{m-k}(x,y)e^k & & \\ \quad i = 0,\ldots,2; & j = 2; & k = 1 \\ \quad i = 2(k-1)+1,\ldots,2k; & j = 0,\ldots,2k; & k = 2,\ldots,m \end{array} \tag{4.1}$$

Die Koeffizientenvektoren von $g_{ijk}(xX, yY)$ und $h_{ijk}(xX, yY)$ bilden die Zeilenvektoren unserer Matrix, die unser Gitter L aufspannt. Abbildung 4.1 zeigt, wie die Matrix für $m = 2$ aussieht.
Zur Berechnung der Schranke durch die Formeln (2.4) und (2.5) auf Seite 11 benötigen wir die Determinante der Matrix. Da wir hier eine obere Dreiecksmatrix erhalten, ist die Determinante einfach das Produkt aller Einträge auf der Hauptdiagonalen der Matrix (Bemerkung 2.1, Seite 6). Mit Potenz(g_X) bezeichnen wir die Potenz von X, die durch die Shifts g_{ijk} zur Determinante beiträgt. Analog werden auch Potenz(g_Y), Potenz(g_e), Potenz(h_X), Potenz(h_Y) und Potenz(h_e) definiert.

Satz 4.1 *Die Matrix L, die durch die Koeffizientenvektoren der in* (4.1) *definierten Shifts $g_{ijk}(xX, yY)$ und $h_{ijk}(xX, yY)$ gebildet wird, hat die Determinante*

$$\det(L) = (XY)^{m(2m+1)^2} e^{1 + \frac{4m(m+1)(2m+1)}{3}} \tag{4.2}$$

	1	y	x	xy	x^2	x^2y	y^2	xy^2	x^2y^2	y^3	$\cdots$	x^2y^4	x^3	$\cdots$	x^4y^4
g_{001}	e	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$						
g_{011}		Ye		$-$		$-$	$-$	$-$	$-$	$-$					
g_{101}			Xe	$-$	$-$	$-$		$-$	$-$				$-$		
g_{111}				XYe		$-$		$-$	$-$						
g_{201}					X^2e	$-$			$-$				$-$		
g_{211}						X^2Ye			$-$						
h_{021}							Y^2e	$-$	$-$	$-$		$-$			
h_{121}								XY^2e	$-$			$-$			
h_{221}									X^2Y^2e			$-$			$-$
g_{032}										Y^3e^2					
$\vdots$											$\ddots$				
g_{242}												$X^2Y^4e^2$			
h_{302}													X^3e^2		
$\vdots$														$\ddots$	
h_{442}															$X^4Y^4e^2$

Abbildung 4.1: *Matrix für* $d_x = d_y = d = 2$ *und* $m = 2$

Beweis: Die Einträge auf der Hauptdiagonalen sind für die g- und h-Shifts von der Form $X^iY^je^k$. Dadurch ergibt sich für die g-Shifts

$$\begin{aligned}
\text{Potenz}(g_X) &= \frac{4m^3 - 3m^2 - m + 18}{3} \\
\text{Potenz}(g_Y) &= \frac{m(8m^2 + 3m - 2)}{3} \\
\text{Potenz}(g_e) &= \frac{4m^3 + 4m^2 - m + 12}{3}
\end{aligned}$$

und für die h-Shifts

$$\begin{aligned}
\text{Potenz}(h_X) &= \frac{8m^3 + 15m^2 + 4m - 18}{3} \\
\text{Potenz}(h_Y) &= \frac{m(4m + 5)(m + 1)}{3} \\
\text{Potenz}(h_e) &= \frac{4m^3 + 9m^2 + 5m - 9}{3}.
\end{aligned}$$

Fasst man diese Ergebnisse nach den einzelnen Potenzen von X, Y und e zu-

sammen, so bekommen wir

$$\begin{aligned}
\det(L_X) &= X^{\frac{4m^3-3m^2-m+18+8m^3+15m^2+4m-18}{3}} \\
&= X^{\frac{12m^3+12m^2+3m}{3}} \\
&= X^{m(2m+1)^2} \\
\det(L_Y) &= Y^{\frac{m(8m^2+3m-2)+m(4m+5)(m+1)}{3}} \\
&= Y^{\frac{m(12m^2+12m+3)}{3}} \\
&= Y^{m(2m+1)^2} \\
\det(L_e) &= e^{\frac{4m^3+4m^2-m+12+4m^3+9m^2+5m-9}{3}} \\
&= e^{\frac{8m^3+13m^2+4m+3}{3}} \\
&= e^{1+\frac{4m(m+1)(2m+1)}{3}}.
\end{aligned}$$

□

Abbildung 4.2 zeigt den Zusammenhang zwischen den Shifts und den Monomen auf der Hauptdiagonalen für $m = 2$ unter Vernachlässigung der Potenzen von e. Die i's und j's laufen dabei wie in (4.1) definiert. Das Tupel $(1, 2)$ entspricht z.B. dem Monom XY^2 und steht auf der Hauptdiagonalen in der Zeile, die von einem Shift für $k = 1$ gebildet wurde.

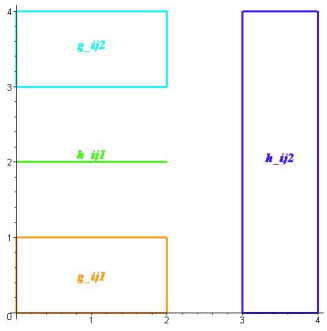

Abbildung 4.2: *Hier kann man sehen, welche Shifts welche Elemente auf der Hauptdiagonalen liefern, wobei $m = 2$ gewählt wurde.*

Um die Schranke zu berechnen, benutzen wir dieselbe Ungleichung (2.5) auf Seite 11 wie im vorherigen Kapitel

$$\det(L)^{\frac{1}{n-1}} < \frac{e^m}{\sqrt{n}2^{\frac{n}{2}}}$$

Wie schon zuvor ist $n = \dim(L)$, also hier $n = (2m+1)^2$, und damit gilt $n - 1 = 4m(m+1)$.

Satz 4.2 *Gilt*

$$XY < \gamma^{-\frac{4(m+1)}{(2m+1)^2}} e^{\frac{4m^3-4m-3)}{3m(2m+1)^2}}$$

mit $\gamma = (2m+1)2^{\frac{(2m+1)(2m+1)}{2}}$*, so können wir die kleine Nullstelle* (x_0, y_0) *unseres Polynoms* $f(x,y) = \sum_{i=0}^{2}\sum_{j=0}^{2} a_{ij}x^i y^j$ *bestimmen.*

Beweis: Setzt man (4.2) in Ungleichung (2.5) von Seite 11 ein, so sind folgende Ungleichungen äquivalent

$$\left((XY)^{m(2m+1)^2} e^{1+\frac{4m(m+1)(2m+1)}{3}}\right)^{\frac{1}{(2m+1)^2-1}} < \frac{e^m}{\gamma}$$

$$(XY)^{m(2m+1)^2} e^{1+\frac{4m(m+1)(2m+1)}{3}} < \frac{e^{m((2m+1)^2-1)}}{\gamma^{(2m+1)^2-1}}$$

$$(XY)^{m(2m+1)^2} < \frac{e^{m((2m+1)^2-1)-1-\left(\frac{4m(m+1)(2m+1)}{3}\right)}}{\gamma^{4m(m+1)}}$$

$$XY < \left(\frac{e^{3m((2m+1)^2-1)-1-\left(\frac{4m(m+1)(2m+1)}{3}\right)}}{\gamma^{4m(m+1)}}\right)^{\frac{1}{m(2m+1)^2}}$$

$$= \gamma^{-\frac{4(m+1)}{(2m+1)^2}} e^{\frac{12m^3+12m^2-3-8m^3-12m^2-4m}{3m(2m+1)^2}}$$

$$= \gamma^{-\frac{4(m+1)}{(2m+1)^2}} e^{\frac{4m^3-4m-3)}{3m(2m+1)^2}}$$

□

Korollar 4.1 *Man kann in polynomieller Zeit für alle* $\epsilon > 0$ *und* $XY < e^{\frac{1}{3}} - \epsilon$ *kleine Nullstellen unseres Polynoms* $f(x,y) = \sum_{i=0}^{2}\sum_{j=0}^{2} a_{ij}x^i y^j$ *bestimmen.*

Beweis: Der vorherige Satz lieferte uns die Schranke

$$XY < \gamma^{-\frac{4(m+1)}{(2m+1)^2}} e^{\frac{4m^3-4m-3)}{3m(2m+1)^2}}$$

mit $\gamma = (2m+1)2^{\frac{(2m+1)(2m+1)}{2}}$. Betrachtet man nun den Grenzwert für $m \to \infty$, so geht die Potenz von e gegen $\frac{1}{3}$, wohingegen der γ-Term gegen 0 strebt. □

4.1.2 Fall für beliebige d

Nachdem wir den Spezialfall $d = 2$ betrachtet haben, widmen wir uns jetzt dem allgemeinerem Fall, bei dem $d \in \mathbb{N}$ beliebig. Damit hat unsere Funktion f die Form $f(x, y) = \sum_{i=0}^{d} \sum_{j=0}^{d} a_{ij} x^i y^j$.
Der Aufbau der Shifts erfolgt nach demselben Muster wie in 4.1.1.

$$\begin{array}{lll} g_{ijk}(x,y) = x^i y^j f^{m-k}(x,y) e^k & & \\ \quad i = 0, \ldots, d; & j = 0, \ldots, d-1; & k = 1 \\ \quad i = 0, \ldots, d(k-1); & j = d(k-1)+1, \ldots, dk; & k = 2, \ldots, m \\ h_{ijk}(x,y) = x^i y^j f^{m-k}(x,y) e^k & & \\ \quad i = 0, \ldots, d; & j = d; & k = 1 \\ \quad i = d(k-1)+1, \ldots, dk; & j = 0, \ldots, dk; & k = 2, \ldots, m \end{array} \tag{4.3}$$

Die Berechnung der Determinante erfolgt ebenfalls nach demselben Prinzip wie bisher.

Satz 4.3 *Die Matrix L, die durch die Koeffizientenvektoren der in* (4.3) *definierten Shifts* $g_{ijk}(xX, yY)$ *und* $h_{ijk}(xX, yY)$ *gebildet wird, hat die Determinante*

$$\det(L) = (XY)^{\frac{dm(dm+1)^2}{2}} e^{1 + \frac{dm(m+1)(4dm+6-d)}{6}} \tag{4.4}$$

Beweis: Die Einträge auf der Hauptdiagonalen sind diesmal bei allen Shifts gegeben durch $X^{i+}Y^j e^k$. Dadurch ergibt sich für die g-Shifts

$$\begin{aligned} \text{Potenz}(g_X) &= \frac{d^2(2dm^3 - 3dm^2 + 3m^2 - 3m + dm + 6 + 6d)}{12} \\ \text{Potenz}(g_Y) &= \frac{d(4d^2m^3 + 9dm^2 - 3d^2m^2 + 6m - d^2m - 3dm - 6d - 12 + 6d^2)}{12} \\ \text{Potenz}(g_e) &= \frac{d(2dm^3 + 3m^2 + 3m - 2dm + 6d)}{6} \end{aligned}$$

und für die h-Shifts

$$\begin{aligned} \text{Potenz}(h_X) &= \frac{d(4d^2m^3 + 3d^2m^2 - d^2m - 6d^2 + 9dm^2 + 3dm + 6m - 6d)}{12} \\ \text{Potenz}(h_Y) &= \frac{d(2d^2m^3 + 3d^2m^2 + d^2m - 6d^2 + 3dm^2 + 3dm + 12 + 6d)}{12} \\ \text{Potenz}(h_e) &= 1 + \frac{d(3m^2 + 3m + 2dm^3 + 3dm^2 + dm - 6d)}{6} \end{aligned}$$

Fasst man diese Ergebnisse zusammen, so erhalten wir

$$\begin{aligned} \text{Potenz}(X) &= \frac{dm(dm+1)^2}{2} \\ \text{Potenz}(Y) &= \frac{dm(dm+1)^2}{2} \\ \text{Potenz}(e) &= 1 + \frac{dm(m+1)(4dm+6-d)}{6} \end{aligned}$$

und somit das gewünschte Ergebnis. □

Das einzige was wir zur Bestimmung einer Schranke für XY noch benötigen ist die Dimension unserer Matrix. Diese ist gegeben durch $n = (dm+1)^2$ und damit $n-1 = dm(dm+2)$. Unter Benutzung von Ungleichung (2.5) auf Seite 11 läßt sich nun eine Schranke berechnen.

Satz 4.4 *Gilt*

$$XY < \gamma^{-\frac{2(dm+2)}{(dm+1)^2}} e^{\frac{2d^2m^3+6dm^2-3d^2m^2-6dm+d^2m-6}{3dm(dm+1)^2}}$$

mit $\gamma = (dm+1)2^{\frac{(dm+1)(dm+1)}{2}}$*, so können wir die kleine Nullstelle* (x_0, y_0) *unseres Polynoms* $f(x,y) = \sum_{i=0}^{d}\sum_{j=0}^{d} a_{ij}x^iy^j$ *bestimmen.*

Beweis: Setzt man (4.4) in Ungleichung (2.5) von Seite 11 ein, so sind wieder folgende Ungleichungen äquivalent

$$\left((XY)^{\frac{dm(dm+1)^2}{2}} e^{1+\frac{dm(m+1)(4dm-d+6)}{6}}\right)^{\frac{1}{(dm+1)^2-1}} < \frac{e^m}{\gamma}$$

$$(XY)^{\frac{dm(dm+1)^2}{2}} e^{1+\frac{dm(m+1)(4dm-d+6)}{6}} < \frac{e^{m((dm+1)^2-1)}}{\gamma^{(dm+1)^2-1}}$$

Als nächstes bringen wir alle e-Terme auf die rechte Seite

$$(XY)^{\frac{dm(dm+1)^2}{2}} < \frac{e^{m((dm+1)^2-1)-1-\left(\frac{dm(m+1)(4dm-d+6)}{6}\right)}}{\gamma^{dm(dm+2)}}$$

und potenzieren alles mit dem reziproken Wert der Potenz von XY

$$\begin{aligned} XY &< \left(\frac{e^{\left(\frac{6dm^2(dm+2)-6-dm(m+1)(4dm-d+6)}{6}\right)}}{\gamma^{dm(dm+2)}}\right)^{\frac{2}{dm(dm+1)^2}} \\ &= \gamma^{-\frac{2(dm+2)}{(dm+1)^2}} e^{\frac{6dm^2(dm+2)-6-dm(m+1)(4dm-d+6)}{3dm(dm+1)^2}} \\ &= \gamma^{-\frac{2(dm+2)}{(dm+1)^2}} e^{\frac{2d^2m^3+6dm^2-3d^2m^2-6dm+d^2m-6}{3dm(dm+1)^2}}. \end{aligned}$$

□

Abschließend kommt hier noch eine Folgerung aus dem letzten Satz:

Korollar 4.2 *Man kann in polynomieller Zeit für alle $\epsilon > 0$ und $XY < e^{\frac{2}{3d}} - \epsilon$ kleine Nullstellen unseres Polynoms $f(x,y) = \sum_{i=0}^{d}\sum_{j=0}^{d} a_{ij}x^i y^j$ bestimmen.*

Beweis: Satz 4.4 lieferte uns die Schranke

$$XY < \gamma^{-\frac{2(dm+2)}{(dm+1)^2}} e^{\frac{2d^2m^3+6dm^2-3d^2m^2-6dm+d^2m-6}{3dm(dm+1)^2}}$$

mit $\gamma = (dm+1)2^{\frac{(dm+1)(dm+1)}{2}}$. Betrachtet man nun den Grenzwert für $m \to \infty$, so geht die Potenz von e gegen $\frac{2}{3d}$, wohingegen der γ-Term gegen 0 strebt. □

Setzt man $d = 2$, so erhalten wir wieder dieselbe Schranke für XY wie schon in 4.1.1.

4.1.3 Fall für beliebige und unterschiedliche d´s

Handelt es sich bei dem zu untersuchendem Polynom um eines der allgemeinsten Form, d.h.

$$f(x,y) = \sum_{i=0}^{d_x}\sum_{j=0}^{d_y} a_{ij}x^i y^j,$$

wobei $d_x, d_y \in \mathbb{N}$ bel., so genügen die Berechnungen aus 4.1.2 nicht mehr. Man kann allerdings die vorherigen Fälle aus diesem ableiten, indem man in den folgenden Gleichungen d_x und d_y durch d bzw. 2 ersetzt. Daher werden die Herleitungen der Formeln dieses Kapitels etwas ausführlicher behandelt als zuvor.

Prinzipiell bleiben die Shifts so wie bisher. Man muss sie nur an die neue Situation anpassen.

$$\begin{aligned}
g_{ijk}(x,y) &= x^i y^j f^{m-k}(x,y)e^k \\
&\quad i = 0,\dots,d_x; \quad j = 0,\dots,d_y-1; \quad k = 1 \\
&\quad i = 0,\dots,d_x(k-1); \quad j = d_y(k-1)+1,\dots,d_yk; \quad k = 2,\dots,m \\
h_{ijk}(x,y) &= x^i y^j f^{m-k}(x,y)e^k \\
&\quad i = 0,\dots,d_x; \quad j = d_y; \quad k = 1 \\
&\quad i = d_x(k-1)+1,\dots,d_xk; \quad j = 0,\dots,d_yk; \quad k = 2,\dots,m
\end{aligned} \tag{4.5}$$

Schon in 4.1.1 und 4.1.2 haben wir benutzt, dass die Matrix, die durch die jeweiligen Shifts gebildet wird, eine obere Dreiecksgestalt hat. Dies werden wir nun in diesem Abschnitt auch beweisen.

Satz 4.5 *Die Matrix, die durch die Koeffizientenvektoren der durch* (4.5) *definierten Shifts $g_{ijk}(xX, yY)$ und $h_{ijk}(xX, yY)$ gebildet wird, ist eine obere Dreiecksmatrix.*

Beweis: Im Beweis zu Satz 3.1 auf Seite 14 haben wir gezeigt, dass es sich um eine untere Dreiecksmatrix handelte, indem wir bewiesen, dass bei einer speziellen Anordnung der Shifts in jeder Zeile genau ein neues Monom hinzukommt. Diesmal werden wir zeigen, dass bei einer speziellen Reihenfolge der Shifts ein zu einem Diagonalelement gehöriges Monom kein Monom der nachfolgenden Shifts

sein kann.
Zunächst einmal geben wir die Reihenfolge bei den Shifts bzw. den Zeilen an. Wir beginnen mit den Shifts für $k = 1$. Zuerst kommen die g-Shifts, wobei wir mit $j = 0$ beginnen und i laufen lassen. Dies führen wir sukzessiv für $j = 0, \ldots, d_y - 1$ fort. Danach kommen die h-Shifts für $i = 0, \ldots, d_x$. Nun haben wir alle Shifts für $k = 1$ benutzt und betrachten die Fälle $k = 2, \ldots, m$. Zuerst schreiben wir wieder die g-Shifts hin und dann die h-Shifts. Für jedes k lassen wir bei sukzessiver Erhöhung von j den Index i laufen.
Damit haben wir eine spezielle Anordnung bei den Zeilen und werden nun zeigen, dass wir eine obere Dreiecksmatrix erhalten, wenn auf der Hauptdiagonalen jeweils die Koeffizienten zu den Monomen $x^i y^j$ stehen. Da das Polynom f auch das konstante Monom enthält, ist $x^i y^j$ auch sicher ein Monom der Polynome g_{ijk} bzw. h_{ijk}. Durch die Multiplikation von $x^i y^j$ mit den anderen Monomen von f werden die Potenzen von x und y höchstens größer, aber nie kleiner. Bei der Anordnung der Zeilen kamen zuerst die g-Shifts für $k = 1$. Da bei jedem Schritt entweder i oder j erhöht wird, kann kein Tupel (i, j) zweimal vorkommen, d.h. $x^i y^j$ kann kein Monom der nachfolgenden Shifts sein. Bei diesen g-Shifts galt $j = 0, \ldots, d_y - 1$. Durch unsere Zeilenanordnung folgen nun die h-Shifts für $k = 1$. Hierbei wird i bei festem $j = d_y$ erhöht, was bedeutet, dass auch diesmal nur neue Tupel (i, j) auftreten.
Auch für $2 \leq k \leq m$ erhöhen wir bei jeder Zeile entweder i oder j aufgrund unserer Definition der Shifts (4.5). Damit kann kein Monom, dass zu dem Diagonalelement gehört, bei den nachfolgenden Shifts mehr vorkommen, d.h., dass es sich um eine obere Dreiecksmatrix handelt. □

Damit kommen wir nun wieder zur Berechnung der Determinanten. Aufgrund der Dreiecksgestalt genügt es, wenn man sich die Hauptdiagonalelemente anschaut. Wie im vorherigen Beweis erklärt, sind dies die Koeffizienten der Monome $x^i y^j$.

Satz 4.6 *Die Matrix L, die durch die Koeffizientenvektoren der in* (4.5) *definierten Shifts $g_{ijk}(xX, yY)$ und $h_{ijk}(xX, yY)$ gebildet wird, hat die Determinante*

$$\det(L) = \left(X^{d_x} Y^{d_y}\right)^{\rho} e^{1 + \frac{m(m+1)(4d_x d_y m - d_x d_y + 3d_x + 3d_y)}{6}}. \quad (4.6)$$

Dabei ist $\rho := \frac{m(d_x m + 1)(d_y m + 1)}{2}$.

Beweis: Das Diagonalelement eines jeden Shifts hat die Form $X^i Y^j e^k$. Betrachtet man nun die Indizes bei den Definitionen der Shifts in den Gleichungen (4.5), so lassen sich die Potenzen von X, Y und e folgendermaßen berechnen. Dabei

gelten dieselben Bezeichnungen wie bisher.

$$
\begin{aligned}
\text{Potenz}(g_X) &= \sum_{i=0}^{d_x}\sum_{j=0}^{d_y-1} i + \sum_{k=2}^{m}\sum_{i=0}^{d_x(k-1)}\sum_{j=d_y(k-1)+1}^{d_yk} i \\
&= \sum_{i=0}^{d_x} d_y i + \sum_{k=2}^{m}\sum_{i=0}^{d_x(k-1)} d_y i \\
&= \frac{d_x d_y (d_x+1)}{2} + \sum_{k=2}^{m} \frac{d_x d_y (k-1)(d_x k - d_x + 1)}{2} \\
&= \frac{d_x d_y (d_x+1)}{2} + \frac{d_x d_y m(m-1)(2d_x m + 3 - d_x)}{12} \\
&= \frac{d_x d_y (6d_x + 6 + d_x m - 3m + 3m^2 - 3d_x m^2 + 2d_x m^3)}{12} \\
\text{Potenz}(g_Y) &= \sum_{j=0}^{d_y-1}\sum_{i=0}^{d_x} j + \sum_{k=2}^{m}\sum_{j=d_y(k-1)+1}^{d_yk}\sum_{i=0}^{d_x(k-1)} j \\
&= \sum_{j=0}^{d_y-1} j(d_x+1) + \sum_{k=2}^{m}\sum_{j=d_y(k-1)+1}^{d_yk} (d_x k - d_x + 1) j \\
&= \frac{d_y(d_y-1)(d_x+1)}{2} + \sum_{k=2}^{m} \frac{d_y(d_x k - d_x + 1)(2d_y k - d_y + 1)}{2} \\
&= \frac{d_y(d_y-1)(d_x+1)}{2} \\
&\quad + \frac{d_y(m-1)(4d_x d_y m^2 + (d_x d_y + 6d_y + 3d_x)m + 6d_y + 6)}{12} \\
&= \frac{d_y}{12}\left(4d_x d_y m^3 + (6d_y - 3d_x d_y + 3d_x)m^2\right. \\
&\quad \left. + (6 - 3d_x - d_x d_y)m + 6d_x d_y - 12 - 6d_x\right) \\
\text{Potenz}(g_e) &= \sum_{i=0}^{d_x}\sum_{j=0}^{d_y-1} 1 + \sum_{k=2}^{m}\sum_{i=0}^{d_x(k-1)}\sum_{j=d_y(k-1)+1}^{d_yk} k \\
&= \sum_{i=0}^{d_x} d_y + \sum_{k=2}^{m}\sum_{i=0}^{d_x(k-1)} d_y k \\
&= d_y(d_x+1) + \sum_{k=2}^{m} d_y k(d_x k - d_x + 1) \\
&= d_y(d_x+1) + \frac{d_y(m-1)(2d_x m^2 + 3m + 2d_x m + 6)}{6} \\
&= \frac{d_y(6d_x - 2d_x m + 3m^2 + 3m + 2d_x m^3)}{6}
\end{aligned}
$$

Genauso lassen sich auch wieder die Potenzen bei den h-Shifts bestimmen.

$$
\begin{aligned}
\text{Potenz}(h_X) &= \sum_{i=0}^{d_x} i + \sum_{k=2}^{m} \sum_{i=d_x(k-1)+1}^{d_x k} \sum_{j=0}^{d_y k} i \\
&= \frac{d_x(d_x+1)}{2} + \sum_{k=2}^{m} \sum_{i=d_x(k-1)+1}^{d_x k} (d_y k + 1) i \\
&= \frac{d_x(d_x+1)}{2} + \sum_{k=2}^{m} \frac{d_x(d_y k+1)(2d_x k - d_x + 1)}{2} \\
&= \frac{d_x(d_x+1)}{2} + \frac{d_x(m-1)}{12} \big(4 d_x d_y m^2 \\
&\quad + (6d_x + 7 d_x d_y + 3 d_y) m + 6 + 6 d_x d_y + 6 d_y + 6 d_x) \\
&= \frac{d_x}{12} (4 d_x d_y m^3 + \big(3 d_x d_y + 6 d_x + 3 d_y) m^2 \\
&\quad + (3 d_y + 6 - d_x d_y) m - 6 d_x d_y - 6 d_y) \\
\text{Potenz}(h_Y) &= \sum_{i=0}^{d_x} d_y + \sum_{k=2}^{m} \sum_{j=0}^{d_y k} \sum_{i=d_x(k-1)+1}^{d_x k} j \\
&= d_y(d_x+1) + \sum_{k=2}^{m} \sum_{j=0}^{d_y k} d_x j \\
&= d_y(d_x+1) + \sum_{k=2}^{m} \frac{d_x d_y k (d_y k + 1)}{2} \\
&= d_y(d_x+1) + \frac{d_x d_y (m-1)}{12} (2 d_y m^2 \\
&\quad + (3 + 5 d_y) m + 6 d_y + 6) \\
&= \frac{d_y}{12} (2 d_x d_y m^3 + (3 d_x d_y + 3 d_x) m^2 \\
&\quad + (d_x d_y + 3 d_x) m - 6 d_x d_y + 6 d_x + 12) \\
\text{Potenz}(h_e) &= \sum_{i=0}^{d_x} 1 + \sum_{k=2}^{m} \sum_{i=d_x(k-1)+1}^{d_x k} \sum_{j=0}^{d_y k} k \\
&= d_x + 1 + \sum_{k=2}^{m} \sum_{i=d_x(k-1)+1}^{d_x k} (d_y k + 1) k \\
&= d_x + 1 + \sum_{k=2}^{m} d_x k (d_y k + 1) \\
&= d_x + 1 + \frac{d_x(m-1)(2 d_y m^2 + (3 + 5 d_y) m + 6 d_y + 6)}{6} \\
&= 1 + \frac{d_x(2 d_y m^3 + (3 + 3 d_y) m^2 + (3 + d_y) m - 6 d_y}{6}
\end{aligned}
$$

Fasst man diese Ergebnisse zusammen, so erhalten wir

$$\begin{aligned}
\text{Potenz}(X) &= \text{Potenz}(g_X) + \text{Potenz}(h_X) \\
&= \frac{d_x m(d_y m+1)(d_x m+1)}{2} \\
\text{Potenz}(Y) &= \text{Potenz}(g_Y) + \text{Potenz}(h_Y) \\
&= \frac{d_y m(d_x m+1)(d_y m+1)}{2} \\
\text{Potenz}(e) &= \text{Potenz}(g_e) + \text{Potenz}(h_e) \\
&= 1 + \frac{m(m+1)(4d_x d_y m - d_x d_y + 3d_x + 3d_y}{6}.
\end{aligned}$$

□

Zur Berechnung einer Schranke brauchen wir die Dimension $n = \dim(L)$ unseres Gitters.

$$\begin{aligned}
n &= \sum_{i=0}^{d_x}\sum_{j=0}^{d_y-1} 1 + \sum_{k=2}^{m}\sum_{i=0}^{d_x(k-1)}\sum_{j=d_y(k-1)+1}^{d_y k} 1 + \sum_{i=0}^{d_x} 1 + \sum_{k=2}^{m}\sum_{i=d_x(k-1)+1}^{d_x k}\sum_{j=0}^{d_y k} 1 \\
&= \sum_{i=0}^{d_x} d_y + \left(\sum_{k=2}^{m}\sum_{i=0}^{d_x(k-1)} d_y\right) + d_x + 1 + \sum_{k=2}^{m}\sum_{i=d_x(k-1)+1}^{d_x k} d_y k + 1 \\
&= d_y(d_x+1) + \left(\sum_{k=2}^{m} d_y(d_x k - d_x + 1)\right) + d_x + 1 + \sum_{k=2}^{m}(d_y k+1)d_x \\
&= (d_y+1)(d_x+1) + \frac{d_y(m-1)(d_x m+2)}{2} + \frac{d_x(m-1)(d_y m+2d_y+2)}{2} \\
&= (d_x m+1)(d_y m+1)
\end{aligned}$$

Damit haben wir alles, was wir für den folgenden Satz benötigen.

Satz 4.7 *Gilt*

$$X < \frac{e^{\frac{2d_x d_y m^3 + 3m^2(d_x+d_y-d_x d_y) - m(3d_x+3d_y-d_x d_y) - 6}{3(d_x m+1)(d_y m+1)(d_x+d_y)}}}{\gamma^{\frac{2(d_x d_y m + d_x + d_y)}{(d_x m+1)(d_y m+1)(d_x+d_y)}}}$$

mit $\gamma = \sqrt{(d_x m+1)(d_y m+1)}2^{\frac{(d_x m+1)(d_y m+1)}{2}}$*, so können wir die kleine Nullstelle* (x_0, y_0) *unseres Polynoms* $f(x,y) = \sum_{i=0}^{d_x}\sum_{j=0}^{d_y} a_{ij}x^i y^j$ *bestimmen.*

Beweis: Sei $a := \frac{m(d_x m+1)(d_y m+1)}{2}$. Setzen wir Gleichung (4.6) in (2.5) ein, so

erhalten wir die Äquivalenzen

$$\left(X^{d_x}Y^{d_y}\right)^a \overset{e}{} 1 + \frac{m(m+1)(4d_xd_ym - d_xd_y + 3d_x + 3d_y)}{6} < \frac{e^{m(n-1)}}{\gamma^n - 1}$$

$$\left(X^{d_x}Y^{d_y}\right)^a < \frac{\overset{e}{} m(n-1) - 1 - \frac{m(m+1)(4d_xd_ym - d_xd_y + 3d_x + 3d_y)}{6}}{\gamma^n - 1}$$

Mit $X \approx Y$ wird die letzte Ungleichung vereinfacht zu

$$X < \left(\frac{\overset{e}{} m(n-1) - 1 - \frac{m(m+1)(4d_xd_ym - d_xd_y + 3d_x + 3d_y)}{6}}{\gamma^n - 1} \right)^{\frac{1}{a(d_x+d_y)}}$$

$$= \frac{\overset{e}{} \frac{2d_xd_ym^3 + 3m^2(d_x + d_y - d_xd_y) - m(3d_x + 3d_y - d_xd_y) - 6}{3(d_xm+1)(d_ym+1)(d_x+d_y)}}{\gamma^{-\frac{2(d_xd_ym + d_x + d_y)}{(d_xm+1)(d_ym+1)(d_x+d_y)}}}$$

□

Wie zuvor ziehen wir eine Folgerung aus dem letzten Satz.

Korollar 4.3 *Man kann in polynomieller Zeit für* $X < e^{\frac{2}{3(d_x+d_y)}} - \epsilon$ *und für alle* $\epsilon > 0$ *kleine Nullstellen unseres Polynoms* $f(x,y) = \sum_{i=0}^{d_x}\sum_{j=0}^{d_Y} a_{ij}x^iy^j$ *bestimmen. Dabei sind* X *und* Y *etwa von derselben Größenordnung.*

Beweis: Satz 4.7 lieferte uns unter der Voraussetzung $X \approx Y$ die Schranke

$$X < \frac{\overset{e}{} \frac{2d_xd_ym^3 + 3m^2(d_x + d_y - d_xd_y) - m(3d_x + 3d_y - d_xd_y) - 6}{3(d_xm+1)(d_ym+1)(d_x+d_y)}}{\gamma^{\frac{2(d_xd_ym + d_x + d_y)}{(d_xm+1)(d_ym+1)(d_x+d_y)}}}$$

mit $\gamma = \sqrt{(d_xm+1)(d_ym+1)}2^{\frac{(d_xm+1)(d_ym+1)}{2}}$. Betrachtet man nun den Grenzwert für $m \to \infty$, so geht die Potenz von e gegen $\frac{2}{3(d_x+d_y)}$, wohingegen der γ-Term gegen ∞ strebt. □

4.2 Schrankenberechnung bei Funktionen mit totalem Grad

In diesem Kapitel befassen wir uns mit einer etwas veränderten Funktion $f(x, y)$. Hing diese Funktion zuvor noch von d_x und d_y ab, so befassen wir uns diesmal mit dem totalen Grad. Dadurch hat unsere neue Funktion die Form

$$f(x,y) = \sum_{0 \le i+j \le d} a_{ij} x^i y^j.$$

Auch in diesem Kapitel werden wir $a_{00} = 1$ setzen.
Zuerst betrachten wir wieder den Fall für $d = 2$. Hierbei werden wir sehen, dass unsere Shifts diesmal eine dreieckige Form haben im Gegensatz zu der rechteckigen, die wir im vorherigen Kapitel bekamen (s. Abbildung 4.2). Danach werden wir eine eine Schranke für allgemeines $d \in \mathbb{N}$ berechnen.

4.2.1 totaler Grad d=2

Unsere Funktion f hat in diesem speziellen Fall für $d = 2$ die Form

$$\begin{aligned} f(x,y) &= \sum_{0 \le i+j \le 2} a_{ij} x^i y^j \\ &= a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2. \end{aligned}$$

Da wir hier eine andere Funktion haben, werden wir auch andere Shifts definieren müssen. Diese haben die folgende Form:

$$\begin{array}{lllll} g_{ijk}(x,y) = x^i y^j f^{m-k}(x,y) e^k & & & & \\ \quad i = 0, \ldots, l; & j = 0, \ldots, l-i; & k = 1; & l = 1 & \\ \quad i = 0, \ldots, l & j = l - i; & k = 2, \ldots, m; & l = 2k-1 & \\ h_{ijk}(x,y) = x^i y^j f^{m-k}(x,y) e^k & & & & \\ \quad i = 0, \ldots, 2; & j = 2 - i; & k = 1 & & \\ \quad i = 0, \ldots, 2k; & j = 2k - i; & k = 2, \ldots, m & & \end{array} \tag{4.7}$$

Bemerkung 4.1 *Der Hilfsparameter l bei den Definitionen der Shifts* (4.7) *ist in diesem Fall bei $d = 2$ nicht unbedingt nötig. Da er aber bei der Verallgemeinerung in 4.2.2 gebraucht wird, führen wir ihn hier schon ein.*

Zuvor haben wir schon von einer dreieckigen Form der Shifts gesprochen. Abbildung 4.3 zeigt dies für $m = 3$.

Nun folgt wieder die Berechnung der Determinanten. Die Matrix, die wir durch die Shifts erhalten, ist eine obere Dreiecksmatrix. Ein Beweis dazu werden wir in 4.2.2 liefern, da es sich hierbei nur um einen Spezialfall handelt. Somit reicht es wieder aus, sich die Hauptdiagonalelemente zu betrachten.

Satz 4.8 *Die Matrix L, die durch die Koeffizientenvektoren der durch* (4.7) *definierten Shifts, gebildet wird, hat die Determinante*

$$\det(L) = (XY)^{\frac{2m(m+1)(2m+1)}{3}} e^{1 + \frac{m(m+1)(8m+7)}{6}}. \tag{4.8}$$

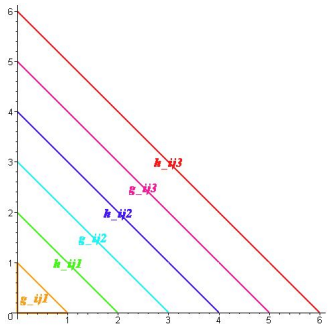

Abbildung 4.3: *Zusammenhang zwischen den Shifts und den Parametern i und j der Hauptdiagonalelemente für $m = 3$.*

Beweis: Da dieser Satz aus Satz 4.11 abgeleitet werden kann, werden wir hier nicht die genauen Herleitungen und Berechnungen liefern. Stattdessen werden wir nur die Ergebnisse angeben. Somit ergeben sich für die g-Shifts

$$\begin{aligned} \text{Potenz}(g_X) &= \frac{m(m+1)(4m-1)}{6} \\ \text{Potenz}(g_Y) &= \frac{m(m+1)(4m-1)}{6} \\ \text{Potenz}(g_e) &= 1 + \frac{m(m+1)(2m+1)}{3} \end{aligned}$$

und die h-Shifts

$$\begin{aligned} \text{Potenz}(h_X) &= \frac{m(m+1)(4m+5)}{6} \\ \text{Potenz}(h_Y) &= \frac{m(m+1)(4m+5)}{6} \\ \text{Potenz}(h_e) &= \frac{m(m+1)(4m+5)}{3}. \end{aligned}$$

Fassen wir nun wieder zusammen, so erhalten wir

$$\begin{aligned} \text{Potenz}(X) &= \frac{2m(m+1)(2m+1)}{3} \\ \text{Potenz}(Y) &= \frac{2m(m+1)(2m+1)}{3} \\ \text{Potenz}(e) &= 1 + \frac{m(m+1)(8m+7)}{6}. \end{aligned}$$

□

Um Ungleichung (2.5) von Seite 11 zur Berechnung einer Schranke benutzen zu können, benötigen wir die Dimension n des Gitters.

$$n = \dim(L) = (m+1)(2m+1)$$

Auch hier verweise ich bei der genauen Berechnung auf das nächste Unterkapitel.

Satz 4.9 *Gilt*

$$XY < \gamma^{-\frac{3(2m+3)}{2(m+1)(2m+1)}} e^{\frac{4m^2-m-6}{4m(2m+1)}}$$

mit $\gamma = \sqrt{(m+1)(2m+1)}2^{\frac{(m+1)(2m+1)}{2}}$*, so können wir die kleine Nullstelle* (x_0, y_0) *unseres Polynoms* $f(x,y) = \sum_{0\leq i+j\leq 2} a_{ij}x^i y^j$ *bestimmen.*

Beweis: Setzt man Gleichung(4.8) in (2.5) ein, so erhalten wir die folgenden Äquivalenzen

$$\begin{aligned}
(XY)^{\frac{2m(m+1)(2m+1)}{3}} e^{1+\frac{m(m+1)(8m+7)}{6}} &< \frac{e^{m(n-1)}}{\gamma^{n-1}} \\
(XY)^{\frac{2m(m+1)(2m+1)}{3}} &< \frac{e^{m(n-1)-1-\frac{m(m+1)(8m+7)}{6}}}{\gamma^{n-1}} \\
XY &< \gamma^{-\frac{3(n-1)}{2m(m+1)(2m+1)}} e^{\frac{3(6m(n-1)-6-m(m+1)(8m+7))}{12m(m+1)(2m+1)}} \\
&= \gamma^{-\frac{3(2m+3)}{2(m+1)(2m+1)}} e^{\frac{4m^2-m-6}{4m(2m+1)}}
\end{aligned}$$

□

Aus diesem Satz leiten wir folgendes Korollar ab.

Korollar 4.4 *Man kann in polynomieller Zeit für alle* $\epsilon > 0$ *und* $XY < e^{\frac{1}{2}} - \epsilon$ *kleine Nullstellen unseres Polynoms* $f(x,y) = \sum_{0\leq i+j\leq 2} a_{ij}x^i y^j$ *bestimmen.*

Beweis: Satz 4.9 lieferte uns die Schranke

$$XY < \gamma^{-\frac{3(2m+3)}{2(m+1)(2m+1)}} e^{\frac{4m^2-m-6}{4m(2m+1)}}$$

mit $\gamma = \sqrt{(m+1)(2m+1)}2^{\frac{(m+1)(2m+1)}{2}}$. Betrachtet man nun den Grenzwert für $m \to \infty$, so geht die Potenz von e gegen $\frac{1}{2}$, wohingegen der γ-Term gegen ∞ strebt. □

4.2.2 totaler Grad für beliebiges d

Hier befassen wir uns nun mit dem ganz allgemeinen Fall, bei dem $d \in \mathbb{N}$ ist. Somit handelt es sich um Funktionen der Form

$$f(x,y) = \sum_{0\leq i+j\leq d} a_{ij}x^i y^j.$$

In 4.2.1 haben wir bereits erwähnt, dass es sich nur um einen Spezialfall dieses Abschnittes handelte. Daher werden die Berechnungen und Beweise auch wieder ausführlicher formuliert. Zuerst definieren wir uns die verallgemeinerten Shifts.

$$
\begin{aligned}
&g_{ijk}(x,y) = x^i y^j f^{m-k}(x,y) e^k \\
&\quad i = 0,\ldots,l;\ j = 0,\ldots,l-i;\ k = 1; \qquad\quad l = d-1 \\
&\quad i = 0,\ldots,l;\ j = l-i; \qquad\quad k = 2,\ldots,m;\ l = d(k-1)+1,\ldots,dk-1 \\
&h_{ijk}(x,y) = x^i y^j f^{m-k}(x,y) e^k \\
&\quad i = 0,\ldots,d;\ \ j = d-i;\ \ k = 1 \\
&\quad i = 0,\ldots,dk;\ j = dk-i;\ k = 2,\ldots,m
\end{aligned}
\tag{4.9}
$$

Satz 4.10 *Bei der Matrix, die durch die Koeffizientenvektoren der durch* (4.9) *definierten Shifts gebildet wird, handelt es sich um eine obere Dreiecksmatrix.*

Beweis: Die Argumentation ist in diesem Fall dieselbe, wie in Satz 4.5. Zuerst ordnen wir die Zeilen der Matrix auf eine ganz bestimmte Weise an. Danach befassen wir uns mit den Spalten. Hierbei wird darauf geachtet, dass auf der Hauptdiagonalen immer der Koeffizient des Monoms steht, dass den geringsten totalen Grad hat. Wir werden dann sehen, dass durch diese Anordnung kein Monom, dessen Koeffizient einmal auf der Hauptdiagonalen gestanden hat, Bestandteil der danach kommenden Shifts sein kann.
Bei den Zeilen beginnen wir mit den Koeffizienten der Shifts für $k = 1$. Zuerst kommen die g-Shifts, wobei wir mit $i = 0$ beginnen und j laufen lassen. Dann erhöhen wir i um eins und lassen j wieder laufen, usw. Darauf folgen die h-Shifts. Hierbei genügt es, alle Werte von i durchzugehen, da j für jedes i aufgrund der Definition der Shifts nur einen Wert annimmt. Diesen Vorgang wiederholen wir für alle $k = 2,\ldots,m$, wobei berücksichtigt werden muß, dass bei den g-Shifts nun das i für alle l laufen gelassen wird (j ist durch die Wahl des Index l bereits eindeutig bestimmt).
Um nun die Spalten anordnen zu können, müssen wir wissen, welches Monom bei den Shifts den kleinsten totalen Grad hat. Da f das konstante Monom besitzt, ist $x^i y^j$ Bestandteil eines jeden Shifts. Bei jeder Multiplikation von $x^i y^j$ mit den anderen Monomen von f erhöht sich der totale Grad, da sich mindestens eine der Potenzen von x oder y erhöht und die andere nicht kleiner werden kann. Damit steht in jeder Zeile auf der Hauptdiagonalen der Koeffizient des Shifts $x^i y^j$, welches wir ab jetzt als das kleinste Monom des Shifts bezeichenen werden. Es bleibt jetzt nur noch zu beweisen, dass wir hierdurch eine obere Dreiecksmatrix erhalten. Wenn wir zeigen können, dass die Monome, dessen Koeffizienten einmal auf der Hauptdiagonalen standen (wir bezeichnen sie im folgenden mit Diagonalmonome), keine Monome der darauffolgenden Shifts sind, so wäre die Aussage des Satzes bewiesen.
Betrachten wir zuerst die g-Shifts für $k = 1$. Hierbei wird ständig entweder das i konstant gehalten und das j erhöht, oder man vergrößert das i, wobei immer $i + j \leq d - 1$ gilt. Das ist gleichbedeutend damit, dass kein Diagonalmonom bei den nachfolgenden g-Shifts mehr auftreten kann, da diese nur aus Monomen der Form $x^{i+i'} y^{j+j'}$ bestehen, wobei mindestens einer der Parameter i' oder j' größer als 0 ist. Die Diagonalmonome können auch keine Bestandteile der nachfolgenden h-Shifts für $k = 1$ oder der weiteren Shifts für größere k sein, da bei denen der totale Grad aufgrund der Definition immer größer als $d - 1$ ist.
Genauso verhält es sich bei den h-Shifts für $k = 1$ und allen anderen Shifts bei größerem k, womit die Behauptung des Satzes bewiesen wäre. □

Damit genügt es wieder für die Berechnung der Determinanten im Beweis des folgenden Satzes nur die Diagonalelemente zu betrachten.

Satz 4.11 *Die Matrix, die durch die Koeffizientenvektoren der durch* (4.9) *definierten Shifts gebildet wird, hat die Determinante*

$$\det(L) = (XY)^{\frac{dm(dm+2)(dm+1)}{6}} e^{1+\frac{dm(m+1)(4dm-d+9)}{12}} \tag{4.10}$$

Beweis: Zuerst berechnen wir die Potenz von X, die wir aus Gründen der Übersucht aufteilen in den Anteil Potenz(g_X), den die g-Shifts liefern,

$$\begin{aligned}
\text{Potenz}(g_X) &= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1-i} i + \sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1}\sum_{i=0}^{l} i \\
&= \sum_{i=0}^{d-1} i(d-i) + \sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1} \frac{l(l+1)}{2} \\
&= \frac{d(d-1)(d+1)}{6} + \sum_{k=2}^{m} \frac{d(d-1)(3dk^2-3dk+d+3k-2)}{6} \\
&= \frac{d(d-1)(d+1)}{6} + \frac{d(m-1)(d-1)(2dm^2+2dm+2d+3m+2)}{12} \\
&= \frac{dm(d-1)(2dm^2+3m-1)}{12}
\end{aligned}$$

und in den Anteil Potenz(h_X), der von den h-Shifts hinzukommt

$$\begin{aligned}
\text{Potenz}(h_X) &= \sum_{i=0}^{d} i + \sum_{k=2}^{m}\sum_{i=0}^{dk} i = \frac{d(d+1)}{2} + \sum_{k=2}^{m} \frac{dk(dk+1)}{2} \\
&= \frac{d(d+1)}{2} + \frac{d(m-1)(2dm^2+3m+5dm+6+6d)}{12} \\
&= \frac{dm(m+1)(2dm+3+d)}{12}
\end{aligned}$$

Somit ergibt sich für die Potenz von X bei der Determinanten

$$\begin{aligned}
\text{Potenz}(X) &= \text{Potenz}(g_X) + \text{Potenz}(h_X) \\
&= \frac{dm(d-1)(2dm^2+3m-1)}{12} + \frac{dm(m+1)(2dm+3+d)}{12} \\
&= \frac{dm(dm+2)(dm+1)}{6}.
\end{aligned}$$

Genauso gehen wir jetzt für die Potenz von Y vor. Zuerst berechnen wir den Anteil der g-Shifts

$$\begin{aligned}
\text{Potenz}(g_Y) &= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1-i} j + \sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1}\sum_{i=0}^{l} l - i \\
&= \sum_{i=0}^{d-1}\frac{(d-1-i)(d-i)}{2} + \sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1}\frac{l(l+1)}{2} \\
&= \frac{d(d-1)(d+1)}{6} + \sum_{k=2}^{m}\frac{d(d-1)(3dk^2-3dk+d+3k-2)}{6} \\
&\overset{(\star)}{=} \frac{dm(d-1)(2dm^2+3m-1)}{12}
\end{aligned}$$

und dann der h-Shifts

$$\begin{aligned}
\text{Potenz}(h_Y) &= \sum_{i=0}^{d} d - i + \sum_{k=2}^{m}\sum_{i=0}^{dk} dk - i = \frac{d(d+1)}{2} + \sum_{k=2}^{m}\frac{dk(dk+1)}{2} \\
&\overset{(\star)}{=} \frac{dm(dm+2)(dm+1)}{6}.
\end{aligned}$$

Das $(\star)$ zeigt an, dass wir die Berechnung an dieser Stelle abgekürtzt haben, da wir sie schon bei Potenz(g_X) bzw. Potenz(h_X) ausgeführt haben. Bei einer Zusammenfassung der letzten beiden Ergebnisse bekommen wir die Potenz von Y.

$$\begin{aligned}
\text{Potenz}(Y) &= \text{Potenz}(g_Y) + \text{Potenz}(h_Y) \\
&= \frac{dm(d-1)(2dm^2+3m-1)}{12} + \frac{dm(dm+2)(dm+1)}{6} \\
&= \frac{dm(dm+2)(dm+1)}{6}
\end{aligned}$$

Damit sehen wir, dass X und Y bei der Bestimmung der Determinanten dieselbe Potenz haben. Als letztes muß in diesem Beweis noch die Potenz von e berechnet werden. Wie zuvor unterscheiden wir wieder zwischen den g-Shifts

$$\begin{aligned}
\text{Potenz}(g_e) &= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1-i} 1 + \sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1}\sum_{i=0}^{l} k \\
&= \sum_{i=0}^{d-1} d - i + \sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1} k(l+1) \\
&= \frac{d(d+1)}{2} + \sum_{k=2}^{m}\frac{k(d-1)(2dk-d+2)}{2} \\
&= \frac{d(d+1)}{2} + \frac{(m-1)(d-1)(4dm^2+7dm+6d+6m+12)}{12} \\
&= 1 + \frac{m(m+1)(d-1)(4dm-d+6)}{12}
\end{aligned}$$

und den h-Shifts

$$\begin{aligned}\text{Potenz}(h_e) &= \sum_{i=0}^{d} 1 + \sum_{k=2}^{m}\sum_{i=0}^{dk} k = d+1+\sum_{k=2}^{m} k(dk+1)\\ &= d+1+\frac{(m-1)(2dm^2+3m+5dm+6+6d)}{6}\\ &= \frac{m(m+1)(2dm+3+d)}{6}.\end{aligned}$$

Eine erneute Zusammenfassung liefert

$$\begin{aligned}\text{Potenz}(e) &= \text{Potenz}(g_e)+\text{Potenz}(h_e)\\ &= 1+\frac{m(m+1)(d-1)(4dm-d+6)}{12}+\frac{m(m+1)(2dm+3+d)}{6}\\ &= 1+\frac{dm(m+1)(4dm-d+9)}{12}.\end{aligned}$$

□

Bemerkung 4.2 *Die Dimension der Matrix (und damit auch des Gitters L), welches durch die Shifts* (4.9) *erzeugt wird, hat die Dimension*

$$n = \dim(L) = \frac{(dm+2)(dm+1)}{2} \tag{4.11}$$

Beweis: Ähnlich wie bei der Berechnung der Determinanten kann man auch die Dimension bestimmen.

$$\begin{aligned}n &= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1-i} 1+\sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1}\sum_{i=0}^{l} 1+\sum_{i=0}^{d} 1+\sum_{k=2}^{m}\sum_{i=0}^{dk} 1\\ &= \sum_{i=0}^{d-1} d-i+\sum_{k=2}^{m}\sum_{l=d(k-1)+1}^{dk-1} l+1+d+1+\sum_{k=2}^{m} dk+1\\ &= \frac{d(d+1)}{2}+\sum_{k=2}^{m}\frac{(d-1)(2dk-d+2)}{2}+d+1+\frac{(m-1)(dm+2d+2}{2}\\ &= \frac{d(d+1)}{2}+\frac{(m-1)(d-1)(dm+d+2)}{2}+d+1+\frac{(m-1)(dm+2d+2}{2}\\ &= \frac{(dm+2)(dm+1)}{2}\end{aligned}$$

□

Damit kommen wir jetzt wieder zur Bestimmung einer oberen Schranke für XY.

Satz 4.12 *Gilt*

$$XY < \gamma^{-\frac{3(dm+3)}{(dm+2)(dm+1)}} e^{\frac{2d^2m^3+(9d-3d^2)m^2+(d^2-9d)m-12}{2dm(dm+2)(dm+1)}}$$

mit $\gamma = \sqrt{\frac{(dm+2)(dm+1)}{2}}^{\frac{(dm+2)(dm+1)}{4}}$*, so können wir die kleine Nullstelle (x_0, y_0) unseres Polynoms $f(x,y) = \sum_{0\le i+j\le d} a_{ij}x^iy^j$ bestimmen.*

Beweis: Setzen wir (4.10) und (4.11) in Ungleichung (2.5) von Seite 11 ein, so erhalten wir folgende Äquivalenzen.

$$(XY)\ e^{\frac{dm(dm+2)(dm+1)}{6}1+\frac{dm(m+1)(4dm-d+9)}{12}} < \frac{e^{m(n-1)}}{\gamma^n-1}$$

$$(XY)\ e^{\frac{dm(dm+2)(dm+1)}{6}} < \frac{e^{m(n-1)-1-\frac{dm(m+1)(4dm-d+9)}{12}}}{\gamma^n-1}$$

$$XY < \left(\frac{e^{m(n-1)-1-\frac{dm(m+1)(4dm-d+9)}{12}}}{\gamma^n-1}\right)^{\frac{2}{(dm+2)(dm+1)}}$$

$$= \gamma^{-\frac{3(dm+3)}{(dm+2)(dm+1)}} e^{\frac{2d^2m^3+(9d-3d^2)m^2+(d^2-9d)m-12}{2dm(dm+2)(dm+1)}}$$

□

Korollar 4.5 *Man kann in polynomieller Zeit für alle $\epsilon > 0$ und $XY < e^{\frac{1}{d}} - \epsilon$ kleine Nullstellen unseres Polynoms $f(x,y) = \sum_{0\le i+j\le d} a_{ij}x^iy^j$ bestimmen.*

Beweis: Satz 4.12 lieferte uns die Schranke

$$XY < \gamma^{-\frac{3(dm+3)}{(dm+2)(dm+1)}} e^{\frac{2d^2m^3+(9d-3d^2)m^2+(d^2-9d)m-12}{2dm(dm+2)(dm+1)}}$$

mit $\gamma = \sqrt{\frac{(dm+2)(dm+1)}{2}} 2^{\frac{(dm+2)(dm+1)}{4}}$. Betrachtet man nun den Grenzwert für $m \to \infty$, so geht die Potenz von e gegen $\frac{1}{d}$, wohingegen der γ-Term gegen ∞ strebt. □

Es sei hier noch einmal angemerkt, dass man für das Einsetzen von $d = 2$ in die Ergebnisse dieses Abschnittes genau die Resultate aus 4.2.1 erhält.

Kapitel 5

Funktionen mit unbalancierten X und Y

In diesem Kapitel beschäftigen wir uns mit dem Fall, bei dem X kleiner als Y^η ist, wobei $0 < \eta \leq 1$. Zuvor sind wir davon ausgegangen, dass die beiden Parameter in etwa die gleiche Größenordnung haben. Dadurch hatten wir bei der Bildung der Matrizen (z.B. Abbildung 4.1) versucht X und Y durch eine spezielle Wahl von Shifts ungefähr gleich oft auftreten zu lassen. Im Folgenden werden wir nun einen neuen Parameter t einführen, der von η abhängen wird. Dadurch ergeben sich sowohl für den rechteckigen Fall (s. Kapitel 4.1), als auch für den dreieckigen Fall (s. Kapitel 4.2) neue Schranken. Diese werden wir nun in den folgenden Unterkapiteln berechnen.

5.1 Schrankenberechnung für allgemeine Funktionen und unbalancierten X und Y

Wie schon in Kapitel 4.1.2 befassen wir uns hier mit einer ganz bestimmten Form von Funktionen, nämlich

$$f(x,y) = \sum_{i=0}^{d} \sum_{j=0}^{d} a_{ij} x^i y^j$$

für ein beliebiges $d \in \mathbb{N}$. Diese Funktionen haben die Nullstelle (x_0, y_0) modulo e. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $a_{dd} = 1$ gilt.
Hier werden wir nun einen neuen Parameter t einführen, welcher von η und m abhängt. Der Parameter η stellt eine Beziehung zwischen X und Y her. Während in den bisherigen Kapiteln immer $X \approx Y$ galt, haben wir nun das Verhältnis $X < Y^\eta$ mit $0 < \eta \leq 1$. Hierfür brauchen wir auch wieder neue Shifts. Diese definieren wir durch:

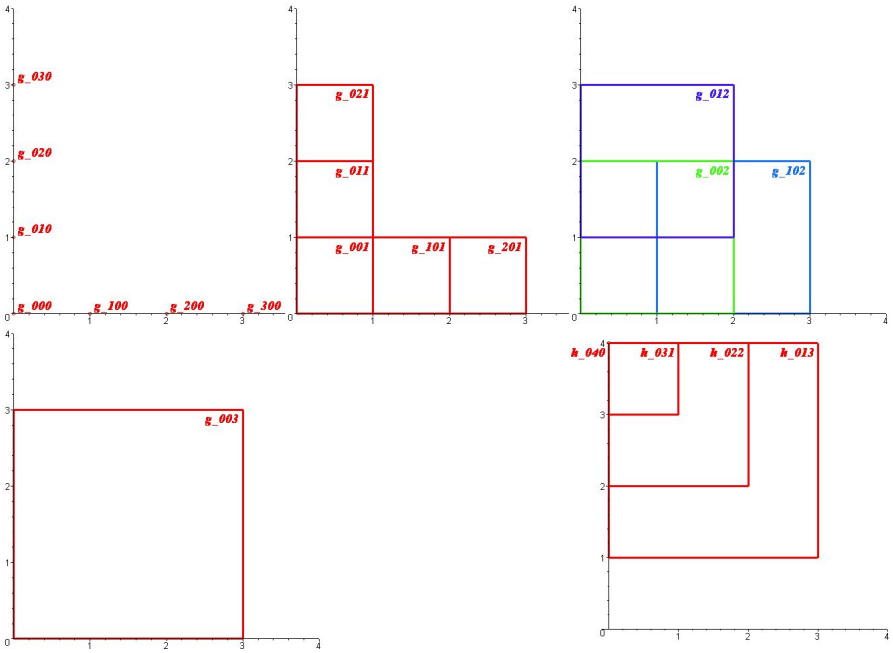

Abbildung 5.1: Hier erkennt man den Aufbau der Shifts für $m = 3$, $t = 1$ und $d = 1$. Die Abszisse stellt jeweils die Potenz der Variablen x, die Ordinate die Potenz von y dar. Die bei jedem Shift eingerahmten ganzzahligen Werte geben die Monome der jeweiligen Shifts an. So ist z.B. das Monom x^2y Bestandteil des Shifts g_{101}. Bei geeigneter Anordnung entsteht durch die Koeffizienten der Shifts eine untere Dreiecksmatrix.

$$
\begin{aligned}
&g_{ijk}(x,y) = x^i y^j f^k(x,y) e^{m-k} \\
&\qquad i = 0,\ldots,d-1; \quad j = 1+i,\ldots,d(m-k); \quad k = 0,\ldots,m-1 \\
&\qquad i = j,\ldots,d(m-k); \quad j = 0,\ldots,d-1; \quad k = 0,\ldots,m-1 \\
&\qquad i = 0; \quad j = 0; \quad k = m \\
&h_{ijk}(x,y) = x^i y^j f^k(x,y) e^{m-k} \\
&\qquad i = 0,\ldots,d-1; \quad j = d(m-k)+1,\ldots,d(m-k)+t; \quad k = 0,\ldots,m-1 \\
&\qquad i = 0; \quad j = 1,\ldots,t; \quad k = m
\end{aligned}
\tag{5.1}
$$

In Abbildung 5.1 sieht man, wie die Shifts für $d = 1$, $t = 1$ und $m = 3$ aufgebaut sind. Unsere Aufgabe ist es jetzt noch zu zeigen, dass wir bei diesen Shifts durch eine geeignete Anordnung eine untere Dreiecksmatrix erhalten. Abbildung 5.2 zeigt die Matrix, welche wir für unser Beispiel $d = 1$, $t = 1$ und $m = 3$ bekommen.

Satz 5.1 *Die Matrix, welche durch die oben genannten Shifts erzeugt wird, hat eine untere Dreiecksgestalt.*

Bew.: Wir müssen hier beweisen, dass bei jedem Shift genau ein neues Monom hinzukommt. Hierzu definieren wir uns eine spezielle Multiplikation zweier

	1	x	$\cdots$	y^2	y^3	xy	$\cdots$	xy^3	x^2y^2	x^3y^2	x^2y^3	x^3y^3	y^4	xy^4	x^2y^4	x^3y^4
g_{000}	e^3															
g_{100}		Xe^3														
$\vdots$			$\ddots$													
g_{020}				Y^2e^3												
g_{030}					Y^3e^3											
g_{001}	$-$	$-$	$-$			XYe^2										
$\vdots$							$\ddots$									
g_{021}				$-$	$-$		$-$	XY^3e^2								
g_{002}	$-$	$-$	$-$	$-$		$-$	$-$		X^2Y^2e							
g_{102}		$-$	$-$			$-$	$-$		$-$	X^3Y^2e						
g_{012}			$-$	$-$	$-$	$-$	$-$	$-$	$-$		X^2Y^3e					
g_{003}	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	X^3Y^3				
h_{040}													Y^4e^3			
h_{031}					$-$			$-$					$-$	XY^4e^2		
h_{022}				$-$	$-$		$-$	$-$	$-$		$-$		$-$	$-$	X^2Y^4e	
h_{013}			$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	X^3Y^4

Abbildung 5.2: *Matrix für* $d = 1$,$t = 1$ *und* $m = 3$

Mengen V und W:

$$V \star W := \{vw : v \in V, w \in W\}$$

Sei G_k die Menge der Monome, die bei allen g-Shifts für ein festes k mit $0 \leq k \leq m$ auftreten. Wir zeigen zuerst, dass g_{00k} mit $1 \leq k \leq m$ im Vergleich zu G_{k-1} nur ein neues Monom liefert.
Die Menge der Monome von g_{00k} und g_{00k-1} sind

$$\begin{aligned} A_k &:= \{x^i y^j : i = 0, ..., dk; j = 0, ..., dk\} \\ A_{k-1} &:= \{x^i y^j : i = 0, ..., d(k-1); j = 0, ..., d(k-1)\}. \end{aligned}$$

Desweiteren definieren wir

$$\begin{aligned} B_{k-1} &:= \{x^i y^j : i = 0, ..., d-1; j = 1+i, ..., dm - d(k-1)\} \\ C_{k-1} &:= \{x^i y^j : i = j, ..., dm - d(k-1); j = 0, ..., d-1\}. \end{aligned}$$

G_{k-1} ist dann die Mengenmultiplikation von A_{k-1} und B_{k-1} vereinigt mit der Mengenmultiplikation von A_{k-1} und C_{k-1}, also

$$G_{k-1} = (A_{k-1} \star B_{k-1}) \cup (A_{k-1} \star C_{k-1}).$$

Für die erste Produktmenge gilt:

$$\begin{aligned} A_{k-1} \star B_{k-1} &\supset \{x^0y^1, ..., x^0y^{dm-d(k-1)+d(k-1)}; x^1y^2, ..., x^1y^{dm}; \\ &\quad ...; x^{(d-1)+d(k-1)}y^{d+d(k-1)}, ..., x^{dk-1}y^{dm}\} \\ &= \{x^0y^1, ..., x^0y^{dm}; x^1y^2, ..., x^1y^{dm}; ...; x^{dk-1}y^{dk}, ..., x^{dk-1}y^{dm}\} \\ &=: D_1 \end{aligned}$$

Ähnliches erhalten wir auch bei der zweiten Produktmenge:

$$\begin{aligned} A_{k-1} \star C_{k-1} &\supset \{x^0y^0, ..., x^{dm-d(k-1)+d(k-1)}y^0; x^1y^1, ..., x^{dm}y^1; \\ &\quad ...; x^{(d-1)+d(k-1)}y^{(d-1)+d(k-1)}, ..., x^{dm-d(k-1)+d(k-1)}y^{dk-1}\} \\ &= \{x^0y^0, ..., x^{dm}y^0; x^1y^1, ..., x^{dm}y^1; ...; x^{dk-1}y^{dk-1}, ..., x^{dm}y^{dk-1}\} \\ &=: D_2 \end{aligned}$$

Bei genauerer Betrachtung stellen wir fest, dass $A_k \setminus \{x^{dk}y^{dk}\} \subseteq D_1 \cup D_2$ und $x^{dk}y^{dk} \notin G_{k-1}$. Das bedeutet, dass $x^{dk}y^{dk}$ das einzige Monom von g_{00k} ist, welches kein Element von G_{k-1} und damit aller zuvor aufgetretenden Shifts ist. Als nächstes zeigen wir, dass für ein beliebiges, aber festes k die Shifts g_{ijk} so angeordnet werden können, dass man jeweils wieder genau ein neues Monom erhält. Dazu betrachten wir A_k mal aus einem anderen Blickwinkel. Trägt man die auftretenden Potenzen von x und y in der Menge A_k in einem 2-dimensionalem Diagramm auf, so stellt man fest, dass diese ein Quadrat der Kantenlänge dk bilden. Durch g_{10k} (was nichts anderes als die Multiplikation eines jeden Elementes von A_k mit dem Monom x^1y^0 ist) wird dieses Quadrat um einen Integerwert nach rechts verschoben. Die durch diese Verschiebung neu gebildete Menge wollen wir dann mit A_{10k} bezeichnen. Allgemein definieren wir

$$A_{ijk} := \{x^i y^j\} \star A_k.$$

Für ein festes k wird A_k mit jedem Element der Menge $B_k \cup C_k$ multipliziert. Ordnen wir diese Menge in einer bestimmten Weise an, so erhalten wir

$$\begin{aligned} B_k \cup C_k \;=\; & \{x^0y^0, ..., x^{dm-dk}y^0; x^0y^1, ..., x^0y^{dm-dk}; x^1y^1, ..., x^{dm-dk}y^1; \\ & x^1y^2, ..., x^1y^{dm-dk}; ...; x^{d-1}y^{d-1}, ..., x^{dm-dk}y^{d-1}; \\ & x^{d-1}y^d, ..., x^{d-1}y^{dm-dk}\}. \end{aligned}$$

Jetzt können wir der Reihe nach jedes Element mit der Menge A_k multiplizieren, wobei wir mir x^1y^0 beginnen, da x^0y^0 ja bereits durch A_k geliefert wurde. Nach der ersten Multiplikation, also $x^1y^0 \star A_k$, vergleicht man die neu entstandene Menge mit $G_{k-1} \cup \{x^{dk}y^{dk}\}$ und sieht, dass man genau ein neues Monom erhält, nämlich $x^{dk+1}y^{dk}$. Dann multipliziert man mit dem nächsten Element und vergleicht diese neue Menge dann mit $G_{k-1} \cup \{x^{dk}y^{dk}\} \cup \{x^{dk+1}y^{dk}\}$, usw. Allgemein erhält man durch die Multiplikation $\{x^iy^j\} \star A_k$ immer genau ein neues Monom, nämlich $x^{i+dk}y^{j+dk}$.
Damit hätten wir die Behauptung für die g-Shifts bewiesen und müssen nur noch zeigen, dass die h-Shifts auch immer nur ein neues Monom liefern. Für $k = 0$ ist es klar, dass man immer ein neues Monom erhält, da die h_{ij0}'s alle nur aus einem Monom bestehen und in diesem Fall j größer ist, als bei allen bisherigen Shifts. Für $k > 0$ macht man im Prinzip das Gleiche, wie bei den g-Shifts. Bei jedem h-Shift h_{ijk} bildet man die Menge $\{x^iy^j\} \star A_k$ und vergleicht sie mit der Menge G_m vereinigt mit der Menge aller bei den h-Shifts zuvor neu aufgetretenden Monome. Dadurch erkennt man, dass man immer ein neues Monom erhält und dieses ist genau wie bei den g-Shifts $x^{i+dk}y^{j+dk}$. □

Nachdem wir bewiesen haben, dass es sich hier um eine untere Dreiecksmatrix handelt, berechnen wir nun die Determinante der durch die Shifts $g_{ijk}(xX, yY)$ und $h_{ijk}(xX, yY)$ entstandenen Matrix.

Satz 5.2 *Die Matrix L, die durch die Koeffizientenvektoren der in* (5.1) *definierten Shifts $g_{ijk}(xX, yY)$ und $h_{ijk}(xX, yY)$ gebildet wird, hat die Determinante*

$$\begin{aligned} \det(L) \;=\; & X^{\frac{dm(dm+1)(dm+t+1)}{2}} Y^{\frac{(dm+1)(dm+1+t)(dm+t)}{2}} \\ & e^{\frac{dm(m+1)(4dm-d+3t+6)}{6}}. \end{aligned} \tag{5.2}$$

Beweis: Da das Prinzip bei den folgenden Rechnungen dasselbe wie in den vorherigen Kapiteln ist, halten wir uns bei der Ausführung in diesem Fall kürzer. Im Beweis zu Satz 5.1 haben wir gezeigt, dass $X^{i+dk}Y^{j+dk}e^{m-k}$ das Element eines jeden Shifts auf der Hauptdiagonalen ist. Dadurch lassen sich die Anteile, die die g-Shifts zur Determinante beitragen, berechnen durch

$$\begin{aligned}
\text{Potenz}(g_X) &= dm + \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=1+i}^{d(m-k)}(i+dk) + \sum_{k=0}^{m-1}\sum_{j=0}^{d-1}\sum_{i=j}^{d(m-k)}(i+dk) \\
&= \frac{dm(dm+1)^2}{2} \\
\text{Potenz}(g_Y) &= dm + \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=1+i}^{d(m-k)}(j+dk) + \sum_{k=0}^{m-1}\sum_{j=0}^{d-1}\sum_{i=j}^{d(m-k)}(j+dk) \\
&= \frac{dm(dm+1)^2}{2} \\
\text{Potenz}(g_e) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=1+i}^{d(m-k)}(m-k) + \sum_{k=0}^{m-1}\sum_{j=0}^{d-1}\sum_{i=j}^{d(m-k)}(m-k) \\
&= \frac{dm(m+1)(4dm-d+6)}{6}.
\end{aligned}$$

Auf dieselbe Weise bestimmen wir die Anteile der h-Shifts.

$$\begin{aligned}
\text{Potenz}(h_X) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1}^{d(m-k)+t}(i+dk) + \sum_{j=1}^{t} dm \\
&= \frac{dtm(dm+1)}{2} \\
\text{Potenz}(h_Y) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1}^{d(m-k)+t}(j+dk) + \sum_{j=1}^{t} dm \\
&= \frac{t(dm+1)(t+1+2dm)}{2} \\
\text{Potenz}(h_e) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1}^{d(m-k)+t}(m-k) \\
&= \frac{dtm(m+1)}{2}
\end{aligned}$$

Fassen wir diese Ergebnisse zu den einzelnen Potenzen von X, Y und e zusam-

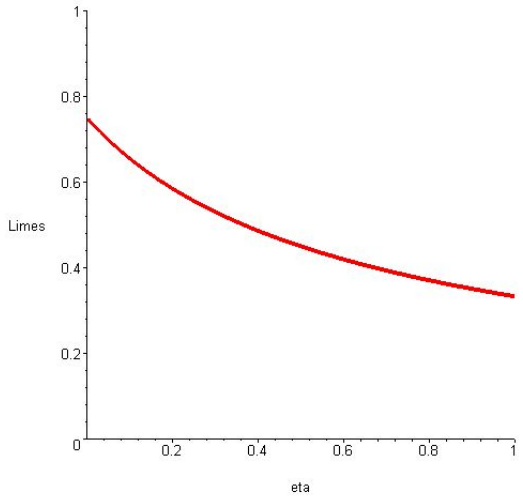

Abbildung 5.3: Man sieht hier die obere Schranke von δ in Abhängigkeit von η für $m \to \infty$ und $d = 1$.

men, so erhalten wir

$$\begin{aligned}
\text{Potenz}(X) &= \text{Potenz}(g_X) + \text{Potenz}(h_X) \\
&= \frac{dm(dm+1)^2}{2} + \frac{dtm(dm+1)}{2} \\
&= \frac{dm(dm+1)(dm+1+t)}{2} \\
\text{Potenz}(Y) &= \text{Potenz}(g_Y) + \text{Potenz}(h_Y) \\
&= \frac{dm(dm+1)^2}{2} + \frac{t(dm+1)(t+1+2dm)}{2} \\
&= \frac{(dm+1)(dm+1+t)(dm+t)}{2} \\
\text{Potenz}(e) &= \text{Potenz}(g_e) + \text{Potenz}(h_e) \\
&= \frac{dm(m+1)(4dm-d+6)}{6} + \frac{dtm(m+1)}{2} \\
&= \frac{dm(m+1)(4dm-d+6+3t)}{6}.
\end{aligned}$$

□

Für die späteren Abschätzungen werden wir noch die Dimension $n = \dim(L)$ des Gitters brauchen.

$$\begin{aligned}
n &= 1 + \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=1+i}^{d(m-k)} 1 + \sum_{k=0}^{m-1}\sum_{j=0}^{d-1}\sum_{i=j}^{d(m-k)} 1 + \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1}^{d(m-k)+t} 1 + \sum_{j=1}^{t} 1 \\
&= (dm+1)(dm+1+t)
\end{aligned}$$

Bis hierhin haben wir in diesem Kapitel alles genauso gemacht wie in den Fällen für $X \approx Y$. Jetzt lassen wir aber einfließen, dass $X < Y^\eta$ mit $0 < \eta \leq 1$

und $Y < e^{\delta}$. Unter Benutzung von Ungleichung (2.5) von Seite 11 setzen wir die Abschätzungen für X und Y in $\det(L)$ ein. Wie schon Boneh und Durfee in [BD00] beachten wir dabei nur Terme, die von e abhängen. Im Folgenden berechnen wir eine Schranke für $m \to \infty$. Man kann dies natürlich auch für jedes beliebige $m \in \mathbb{N}$ machen, allerdings wären die Gleichungen dann so lang, dass die Übersicht dieser Arbeit stark darunter leiden würde.

Satz 5.3 *Für $m \to \infty$ und*

$$Y < e^{\frac{-2\sqrt{d^6 + 3\eta d^6} + 3\eta d^3 + 2d^3}{3\eta^2 d^4}}$$

kann man in polynomieller Zeit die kleine Nullstelle unseres Polynoms $f(x,y) = \sum_{i=0}^{d}\sum_{j=0}^{d} a_{ij}x^i y^j$ bestimmen.

Beweis: Setzen wir die Abschätzungen $X < Y^{\eta}$ und $Y < e^{\delta}$ zusammen mit (5.2) in die Ungleichung (2.5) von Seite 11 ein, so ergibt sich

$$e^{m(n-1)} > e^{\frac{\eta\delta dm(dm+1)(dm+1+t)}{2}} e^{\frac{\delta(dm+1)(dm+1+t)(dm+t)}{2}} e^{\frac{dm(m+1)(4dm-d+6+3t)}{6}}.$$

Da es sich hierbei nur um Potenzen von e handelt, folgern wir aus der letzten Ungleichung

$$\begin{aligned} 0 > {} & \frac{\eta\delta dm(dm+1)(dm+1+t)}{2} + \frac{\delta(dm+1)(dm+1+t)(dm+t)}{2} \\ & + \frac{dm(m+1)(4dm-d+6+3t)}{6} - m(n-1). \end{aligned} \tag{5.3}$$

Für jedes m wird die rechte Seite minimiert für

$$t = -\frac{\delta + 3\delta dm + 2\delta d^2m^2 + dm + \eta\delta dm + \eta\delta d^2m^2 - 2m - dm^2}{2\delta(dm+1)}.$$

Setzen wir t in die Ungleichung (5.3) ein und lösen für δ, so erhalten wir einen sehr langen Ausdruck. Aus Übersichtsgründen betrachten wir den Limes für $m \to \infty$ und bekommen für δ die obere Schranke:

$$\delta < \frac{-2\sqrt{d^6 + 3\eta d^6} + 3\eta d^3 + 2d^3}{3\eta^2 d^4}$$

□

Als Folgerung aus Satz 5.3 wollen wir das letzte Ergebnis mit dem aus Kapitel 4.1.2 vergleichen, wo $X \approx Y$ galt.

Korollar 5.1 *Für $\eta = 1$, d.h. $X = Y$, erhalten wir mit dem in diesem Kapitel verwendeten Verfahren dieselbe Schranke wie in Kapitel 4.1.2.*

m	d	η	$\delta <$
1	1	1/2	0,144
10	1	1/2	0,370
100	1	1/2	0,445
∞	1	1/2	0,450
1	10	1/2	0,004
10	10	1/2	0,033
100	10	1/2	0,044
∞	10	1/2	0,045
1	1	1/4	0,156
10	1	1/4	0,448
100	1	1/4	0,549
∞	1	1/4	0,556
1	1	3/4	0,133
10	1	3/4	0,319
100	1	3/4	0,378
∞	1	3/4	0,382

Tabelle 5.1: *Exemplarische Werte für die Schranke von δ bei unterschiedlicher Eingabe von m, d und η.*

Beweis: In Satz 5.3 erhielten wir die Ungleichung

$$\delta < \frac{-2\sqrt{d^6 + 3\eta d^6} + 3\eta d^3 + 2d^3}{3\eta^2 d^4}.$$

Setzen wir nun $\eta = 1$, so ergibt sich

$$\begin{aligned} \delta &< \frac{-2\sqrt{d^6 + 3d^6} + 3d^3 + 2d^3}{3d^4} \\ &= \frac{d^3}{3d^4} = \frac{1}{3d}. \end{aligned}$$

Daraus folgt

$$Y < e^{\frac{1}{3d}}.$$

In 4.1.2 war das Ergebnis $XY < e^{\frac{2}{3d}}$. Setzen wir nun $X = Y$, so sehen wir, dass die beiden Ungleichungen übereinstimmen. □

Abbildung 5.3 zeigt die Schranke von δ in Abhängigkeit von η und für $m \to \infty$ bei $d = 1$. Tabelle 5.1 gibt die obere Schranke von δ bei unterschiedlichen Eingaben von d, η und diesmal auch für verschiedene Werte von m an.

5.2 Schrankenberechnung für Funktionen mit totalem Grad und unbalancierten X und Y

Zum Abschluß dieses Kapitels werden wir noch einmal Funktionen der Form

$$f(x,y) = \sum_{0 \le i+j \le d} a_{ij} x^i y^j$$

betrachten, die die Nullstelle x_0, y_0 modulo e haben sollen. Ohne Beschränkung der Allgemeinheit können wir davon ausgehen, dass es sich um monische Funktionen handelt, d.h. $a_{d0} = 0$. Als erstes werden wir uns wieder Shifts definieren, deren Koeffizientenvektoren eine untere Dreiecksmatrix bilden.

$$\begin{aligned}
&g_{ijk}(x,y) = x^i y^j f^k(x,y) e^{m-k} \\
&\quad i = 0,\ldots,d-1;\ j = 0,\ldots,d(m-k)-i;\ k = 0,\ldots,m-1 \\
&\quad i = 0; \qquad\qquad j = 0; \qquad\qquad k = m \\
&h_{ijk}(x,y) = x^i y^j f^k(x,y) e^{m-k} \qquad (5.4) \\
&\quad i = 0,\ldots,d-1;\ j = d(m-k)+1-i,\ldots,d(m-k)+t-i; \\
&\qquad\qquad\qquad\qquad k = 0,\ldots,m-1 \\
&\quad i = 0; \qquad\qquad j = 1,\ldots,t; \qquad\qquad k = m
\end{aligned}$$

Satz 5.4 *Die Matrix, die durch die Koeffizientenvektoren der durch* (5.4) *definierten Shifts erzeugt wird, hat eine untere Dreiecksgestalt.*

Beweis: Wir werden jetzt zeigen, dass wir durch die in (5.4) definierten Shifts eine untere Dreiecksmatrix erhalten, bei der die Elemente auf der Hauptdiagonalen für alle Shifts $g_{ijk}(xX, yY)$ bzw. $h_{ijk}(xX, yY)$ die Form $X^{i+dk}Y^j e^{m-k}$ haben (durch (5.4) ist klar, dass $X^{i+dk}Y^j e^{m-k}$ ein Koeffizient der Shifts ist). Wir beginnen damit, eine Reihenfolge bei den Shifts festzulegen. Danach zeigen wir, dass $x^{i+dk}y^j$ das einzige neue Monom im Vergleich zu den Monomen der zuvor aufgetretenden Shifts ist.
Zuerst geben wir die Reihenfolge bei den g-Shifts an. Wir starten mit $k = 0$. Dabei lassen wir j für $i = 0$ laufen. Als nächstes erhöhen wir i um eins und j durchläuft wieder alle Werte $0,\ldots,dm-i$. Dies machen wir für alle i und wiederholen das Gesamte dann für alle $1 \le k \le m$. Auf dieselbe Weise ordnen wir die h-Shifts an.
Sei G_k nun wieder die Menge aller Monome, die bei den g-Shifts für ein $0 \le k \le m$ auftreten.
Schritt 1: Wir zeigen, dass g_{00k} im Vergleich zu der Menge G_{k-1} nur ein neues Monom liefert. Seien A_k und A_{k-1} die Monommengen von g_k bzw. g_{k-1}. Damit gilt:

$$\begin{aligned}
A_k &= \{x^i y^j |\ 0 \le i \le dk;\ 0 \le j \le dk - i\} \\
A_{k-1} &= \{x^i y^j |\ 0 \le i \le d(k-1);\ 0 \le j \le d(k-1) - i\}
\end{aligned}$$

Nun definieren wir uns

$$B_{k-1} := \{x^i y^j |\ 0 \le i \le d-1;\ 0 \le j \le d(m-k+1) - i\}.$$

Somit erhalten wir

$$\begin{aligned} G_{k-1} &= B_{k-1} \star A_{k-1} \\ &= \{x^i y^j |\ 0 \leq i \leq d(k-1)+d-1;\ 0 \leq j \leq d(k-1)+d(m-k+1)-i\} \\ &= \{x^i y^j |\ 0 \leq i \leq dk-1;\ 0 \leq j \leq dm-i\}. \end{aligned}$$

Betrachten wir nun die Menge

$$A_k \backslash \{x^{dk}y^0\} = \{\{x^i y^j |\ 0 \leq i < dk;\ 0 \leq j \leq dk-i\},$$

so sehen wir, dass $A_k \backslash \{x^{dk}y^0\} \subseteq G_{k-1}$ und $x^{dk}y^0 \notin G_{k-1}$, aber $x^{dk}y^0 \in A_k$.
Schritt 2: Als nächstes zeigen wir, dass wir durch unsere spezielle Anordnung der Shifts für ein beliebiges, aber festes k bei jedem Schritt genau ein neues Monom erhalten. Dazu stellen wir uns die Potenzen x und y der Shifts g_{ijk} in einem 2-dimensionalen Diagramm vor. Für $k = 0$ bestehen alle Shifts g_{ij0} nur aus einem einzigen Monom. Da wir entweder i oder j bei der Anordnung immer um eins erhöhen, müssen diese Monome immer neu sein. Für $k > 0$ sehen wir, dass wir in dem Diagramm ein Dreieck erhalten. Durch die spezielle Reihenfolge bei den Shifts (zuerst gilt $i = 0$ und j wird laufen gelassen) verschieben wir dieses Dreieck bei jeder Erhöhung von j um eins nach oben. Wir sehen dann, dass bis auf $x^{dk}y^j$ alle Monome bereits bei den Shifts g_{ijl} für $l < k$ aufgetreten sind. Danach ($i = 1$ und j wird beginnend bei 0 laufen gelassen) verschieben wir das Ausgangsdreieck zuerst um einen Integerwert nach rechts und dann wieder jeweils um einen nach oben. Jedes mal erkennen wir, dass nur das Monom $x^{i+dk}y^j$ neu ist.
Schritt 3: Wir zeigen nun, dass das Monom $x^{i+dk}y^j$ auch bei den h-Shifts das einzig neue ist. Für $k = 0$ handelt es sich wieder einmal um einzelne Monome, deren totaler Grad größer ist als bei den g-Shifts und daher neu sein müssen. Bei $k > 0$ wenden wir wieder das Prinzip von Schritt 2 an. Wir verschieben unser Dreieck wieder nach oben bzw. nach rechts und sehen dadurch, dass $x^{i+dk}y^j$ bei jedem Schritt innerhalb der h-Shifts das einzige neue Monom ist. Da der totale Grad $i+dk+j$ des Monoms $x^{i+dk}y^j$ bei den h-Shifts größer als bei allen g-Shifts ist, kann $x^{i+dk}y^j$ auch nicht bei den g-Shifts vorgekommen sein, womit unsere Behauptung bewiesen wäre. □

Nachdem wir gezeigt haben, dass es sich um eine untere Dreiecksmatrix handelt, können wir auf altbewehrter Weise die Determinante berechnen.

Satz 5.5 *Die Matrix, die durch die Koeffizientenvektoren der durch* (5.4) *definierten Shifts erzeugt wird, hat die Determinante*

$$\begin{aligned} \det(L) &= e^{\frac{dm(m+1)(4dm+9-d+6t)}{12}} X^{\frac{dm(dm+1)(dm+2+3t)}{6}} \\ &\quad Y^{\frac{(dm+1)(d^2m^2+2dm+3tdm+3t^2+3t)}{6}}. \end{aligned} \tag{5.5}$$

Beweis: Das Element, das auf der Hauptdiagonalen der Matrix L steht, hat die Form $X^{i+dk}Y^j e^{m-k}$. Dadurch läßt sich die Determinante bzgl. der g-Shifts

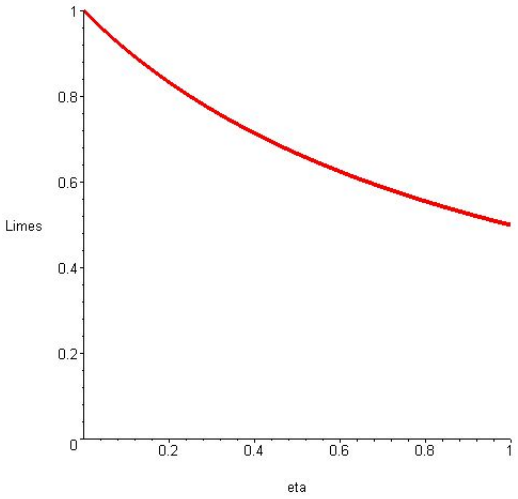

Abbildung 5.4: Man sieht hier die obere Schranke von δ in Abhängigkeit von η für $m \to \infty$ und $d = 1$.

folgendermaßen berechnen:

$$\begin{aligned}
\text{Potenz}(g_X) &= dm + \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=0}^{d(m-k)-i} i + dk = \frac{dm(dm+1)(dm+2)}{6} \\
\text{Potenz}(g_Y) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=0}^{d(m-k)-i} j = \frac{dm(dm+1)(dm+2)}{6} \\
\text{Potenz}(g_e) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=0}^{d(m-k)-i} m-k = \frac{dm(m+1)(4dm+9-d)}{12}
\end{aligned}$$

Als nächstes bestimmen wir den Determinantenanteil der $h-$Shifts.

$$\begin{aligned}
\text{Potenz}(h_X) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1-i}^{d(m-k)+t-i} i + dk + \sum_{j=1}^{t} dm = \frac{dtm(dm+1)}{2} \\
\text{Potenz}(h_y) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1-i}^{d(m-k)+t-i} j + \sum_{j=1}^{t} j = \frac{t(dm+1)(dm+1+t)}{2} \\
\text{Potenz}(h_e) &= \sum_{k=0}^{m-1}\sum_{i=0}^{d-1}\sum_{j=d(m-k)+1-i}^{d(m-k)+t-i} m-k = \frac{dtm(m+1)}{2}
\end{aligned}$$

m	d	η	$\delta <$
1	1	1/2	0,202
10	1	1/2	0,572
100	1	1/2	0,665
∞	1	1/2	0,667
1	10	1/2	0,006
10	10	1/2	0,050
100	10	1/2	0,065
∞	10	1/2	0,067
1	1	1/4	0,223
10	1	1/4	0,686
100	1	1/4	0,798
∞	1	1/4	0,800
1	1	3/4	0,185
10	1	3/4	0,491
100	1	3/4	0,570
∞	1	3/4	0,571

Tabelle 5.2: *Exemplarische Werte für die Schranke von δ bei unterschiedlicher Eingabe von m, d und η. Ausgangspunkt sind Funktionen mit totalem Grad kleiner oder gleich d.*

Fassen wir diese Ergebnisse wieder zusammen, so erhalten wir

$$\begin{aligned}
\text{Potenz}(X) &= \text{Potenz}(g_X) + \text{Potenz}(h_X) \\
&= \frac{dm(dm+1)(dm+2+3t)}{6} \\
\text{Potenz}(Y) &= \text{Potenz}(g_Y) + \text{Potenz}(h_Y) \\
&= \frac{(dm+1)(d^2m^2+2dm+3dmt+3t^2+3t)}{6} \\
\text{Potenz}(e) &= \text{Potenz}(g_e) + \text{Potenz}(h_e) \\
&= \frac{dm(m+1)(4dm+9-d+6t)}{12}.
\end{aligned}$$

□

Unter Berücksichtigung von $X < Y^\eta$ und $Y < e^\delta$ und Verwendung von (2.5) von Seite 11 können wir den nächsten Satz formulieren.

Satz 5.6 *Für $m \to \infty$ und*

$$Y < e^{\frac{-d^3+3\eta d^3}{3\eta^2 d^4 - d^4 + 2\eta d^4}}$$

kann man in polynomieller Zeit die kleine Nullstelle unseres Polynoms $f(x,y) = \sum_{0 \le i+j \le d} a_{ij} x^i y^j$ bestimmen.

Beweis: Setzen wir $X < Y^{\eta}$, $Y < e^{\delta}$ und Gleichung (5.5) in Ungleichung (2.5) von Seite 11 ein, so ergibt sich

$$\begin{aligned} m(n-1) \; > \; & \frac{dm(m+1)(4dm+9-d+6t)}{12} + \frac{\eta\delta dm(dm+1)(dm+2+3t)}{6} \\ & + \frac{\delta(dm+1)(d^2m^2+2dm+3dmt+3t^2+3t)}{6}, \end{aligned} \tag{5.6}$$

wobei wir nur Terme beachtet haben, die von e abhängen und

$$\begin{aligned} n \; &= \; 1 + \sum_{k=0}^{m-1} \sum_{i=0}^{d-1} \sum_{j=0}^{d(m-k)-i} 1 + \sum_{k=0}^{m-1} \sum_{i=0}^{d-1} \sum_{j=d(m-k)+1-i}^{d(m-k)+t-i} 1 + \sum_{j=1}^{t} 1 \\ &= \; \frac{(dm+1)(dm+2+2t)}{2} \end{aligned}$$

die Dimension der Matrix ist. Bringen wir in Gleichung (5.6) den Term $m(n-1)$ auf die rechte Seite, so hat diese für alle m ihr Minimum bei

$$t = -\frac{-dm^2 - 2m + \eta\delta d^2m^2 + \eta\delta dm + dm + \delta d^2m^2 + 2\delta dm + \delta}{2\delta(dm+1)}.$$

Um eine Abschätzung für δ zu bekommen, brauchen wir t nur noch in Gleichung (5.6) einsetzen und δ auf einer Seite isolieren. Da wir dadurch wieder einen sehr langen Ausdruck bekommen, muß hier der Grenzwert für $m \to \infty$ genügen:

$$\delta < \frac{-d^3 + 3d^3\eta}{3\eta^2d^4 - d^4 + 2\eta d^4}$$

□

Tabelle 5.2 gibt Werte für unterschiedliche m, d und η an. An Abbildung 5.4 kann man den Zusammenhang zwischen η und der oberen Schranke von δ erkennen. Je kleiner η, desto größer ist die Schranke. Bei $d = 1$ geht die Schranke für $\eta \to 0$ sogar gegen 1.
Den Abschluß dieser Arbeit bildet folgende Folgerung.

Korollar 5.2 *Für $\eta = 1$, d.h. $X = Y$, erhalten wir dasselbe Ergebnis wie beim balancierten Fall in Kapitel 4.2.2.*

Beweis: Satz 5.6 lieferte uns die Ungleichung

$$\delta < \frac{-d^3 + 3d^3\eta}{3\eta^2d^4 - d^4 + 2\eta d^4}.$$

Daraus können wir wieder mit $\eta = 1$ folgern:

$$Y < e^{\frac{1}{2d}}$$

Vergleichen wir dies mit dem Ergebnis $XY < e^{\frac{1}{d}}$ aus Kapitel 4.2.2 und setzen $X = Y$, so erkennen wir, dass auch diesmal die beiden oberen Schranken übereinstimmen.

□

Literaturverzeichnis

[BD00] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$. *IEEETIT: IEEE Transactions on Information Theory*, 46:1339–1349, 2000.

[BDF98] Dan Boneh, Glenn Durfee, and Yair Frankel. An Attack on RSA given a Small Fraction of the Private Key Bits. In *ASIACRYPT '98: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, pages 25–34, London, UK, 1998. Springer-Verlag.

[BM06] Daniel Bleichenbacher and Alexander May. New Attacks on RSA with Small Secret CRT-Exponents. In *Public Key Cryptography*, pages 1–13, 2006.

[Cop01] Don Coppersmith. Finding small solutions to small degree polynomials. In *CaLC '01: Revised Papers from the International Conference on Cryptography and Lattices*, pages 20–31, London, UK, 2001. Springer-Verlag.

[EJMdW05] Matthias Ernst, Ellen Jochemsz, Alexander May, and Benne de Weger. Partial Key Exposure Attacks on RSA up to Full Size Exponents. In *EUROCRYPT*, pages 371–386, 2005.

[LJL82] Arjen K. Lenstra, Hendrik W. Lenstra Jr., and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[May03] Alexander May. *New RSA Vulnerabilities Using Lattice Reduction Methods*. PhD thesis, University of Paderborn, 2003.

[May04] Alexander May. Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring. *In Advances in Cryptology (Crypto 2004), Lecture Notes in Computer Science Volume 3152, pages 213-219, Springer Verlag*, 2004.

[Nae06] Stefanie Naewe. Samplemethoden in der algorithmischen Geometrie der Zahlen. Master's thesis, University of Paderborn, 2006.

[Wie90] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. In *EUROCRYPT '89: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, page 372, New York, NY, USA, 1990. Springer-Verlag New York, Inc.