UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Fakultät für Elekrotechnik, Informatik und Mathematik
Institut für Mathematik

Diplomarbeit

Vergleich multivariater Varianten der Methode von Coppersmith

von
Julia Borghoff

vorgelegt bei
Prof. Dr. Johannes Blömer

Paderborn
13. Februar 2007

Erklärung

Ich versichere, dass ich die vorliegende Diplomarbeit selbstständig verfasst und keine anderen als die angegeben Quellen und Hilfsmittel benutzt sowie Zitate als solche kenntlich gemacht habe.

Paderborn, den 13. Februar 2007

Julia Borghoff

Danksagung

An dieser Stelle möchte ich mich bei all denen bedanken, die mich bei dieser Arbeit unterstützt und mir so die Fertigstellung ermöglicht haben.

Als erstes möchte ich mich bei Herrn Prof. Dr. Johannes Blömer für die Überlassung des Themas und die intensive Betreuung bedanken. Seine hilfreichen Anregungen haben mir während meiner Arbeit sehr weitergeholfen.

Ein herzliches Dankeschön geht an Stefanie Naewe, die durch viele wertvolle Hinweise und konstruktive Kritik zum Gelingen dieser Arbeit begetragen hat.

Auch bedanke ich mich bei Julia Dahlhoff und Christiane Peters für das geduldige Korrekturlesen und die hilfreichen Kommentare.

Weiterhin gilt mein Dank Dominik Blattner und Ulli Wibbeke, die mir bei meinen technischen Problemen sehr geholfen haben.

Nicht zuletzt möchte ich mich ganz herzlich bei meinen Eltern, meiner ganzen Familie und meinen Freunden bedanken, die mir zu jeder Zeit zur Seite gestanden haben.

Inhaltsverzeichnis

1 Einleitung **2**

2 Grundlagen über Gitter und Polynome **5**
2.1 Der LLL-Algorithmus 5
2.2 Schranken für Polynome 11
2.3 Weitere Grundlagen 14
2.3.1 Die Resultante 14
2.3.2 Lexikographische Ordnung 15

3 Die Ergebnisse von Coron und Coppersmith **16**
3.1 Der bivariate Fall 17
3.2 Der trivariate ganzzahlige Fall 23

4 Konstruktion der Mengen S und M **28**
4.1 Konstruktionen für den bivariaten Fall 29
4.2 Konstruktionen für den bivariaten modularen Fall 35

5 Der bivariate modulare Fall als Spezialfall des trivariaten ganzzahligen Falls **40**
5.1 Die linke untere Dreiecksform 40
5.2 Die Rechteckform 43
5.3 Die rechte untere Dreiecksform 49

6 Angriff auf RSA **54**
6.1 Eine kleine Einführung in RSA 54
6.2 Angriff auf RSA bei kleinem geheimen Schlüssel 55
6.3 Angriffe auf RSA bei kleinem, teilweise bekannten geheimen Schlüssel . 57

A Der Variablenwechsel **64**
A.1 Der bivariate Fall 64
A.2 Der trivariate Fall 64

B Abschätzung für den Exponenten von 2 **66**
B.1 Abschätzung für den Exponenten von 2 für die modulare linke untere Dreiecksform 66
B.2 Abschätzung für den Exponenten von 2 für die modulare Rechtecksform ohne zusätzliche Shifts 68

C Literaturverzeichnis **70**

1 Einleitung

Es gibt viele verschiedene Möglichkeiten für die Nullstellensuche bei univariaten Polynomen. So gibt es beispielsweise numerische Verfahren zur Bestimmung univariater Nullstellen wie das Newton-Verfahren. Für univariate Polynome bis zum Grad 4 lassen sich aber auch allgemeine Lösungsformeln für die Nullstellen direkt angeben.

Weitaus schwieriger wird jedoch die effiziente Bestimmung von Nullstellen im Fall multivariater Polynome und im modularen Fall. Im modularen Fall sind die Nullstellen eines multivariaten Polynoms modulo einer zusammengesetzen Zahl N mit unbekannter Faktorisierung gesucht. Wir möchten uns in dieser Arbeit mit der Nullstellensuche bei ganzzahligen Polynomen in diesen Fällen befassen. Bisher sind nur Algorithmen bekannt, die nur dann die Nullstellen multivariater ganzzahliger beziehungsweise modularer Polynome effizient berechnen können, wenn diese genügend klein sind. Unser Ziel bei der Konstruktion solcher Algorithmen ist, diese Schranken zu maximieren.

Betrachten wir die Problemstellung für den bivariaten ganzzahligen Fall einmal genauer: Es seien X und Y obere Schranken für die gesuchten Nullstellen des ganzzahligen Polynoms $p(x, y)$. Dann suchen wir ein Paar (x_0, y_0), sodass $p(x_0, y_0) = 0$ und $|x_0| \leq X$ und $|y_0| \leq Y$ gilt. Dabei ist unser Ziel die Schranken X und Y zu maximieren.

Im Jahr 1996 stellte Coppersmith auf Gittertheorie basierende Methoden zur Bestimmung kleiner ganzzahliger Nullstellen von Polynome vor. Zum einen betrachtet er modulare univariate Polynome und zum anderen bivariate ganzzahlige Polynome [4, 3]. Die Methode von Coppersmith liefert hierbei jedoch einen umständlich und aufwendig zu implementierenden Algorithmus. Howgrave-Graham [10] gab 1997 eine Vereinfachung der univariaten modularen Methode von Coppersmith an, welche seither besonderes in der Kryptanalyse viele Anwendungen gefunden hat. Coron [7] gelang es 2004, das Ergebnis von Coppersmith für den bivariaten ganzzahligen Fall auf eine neue Weise darzulegen und zu beweisen. Dabei benutzt er ebenso wie Coppersmith die Gitterreduktion, betrachtet allerdings keine Untergitter. Dies vereinfacht seinen Beweis im Vergleich zu Coppersmith'; er büßt allerdings auch Qualität bei den erzielten Schranken ein.

Wie bereits erwähnt, betrachtet Coppersmith den univariaten modularen und den bivariaten ganzzahligen Fall. Die Beweismethoden von Coppersmith für diese beiden Fälle sind zwar in der Struktur sehr ähnlich, unterscheiden sich aber in einigen wesentlichen Details. Im Jahre 2005 zeigten Blömer und May [1], dass der univariate modulare Fall als Spezialfall des bivariaten ganzzahligen Falls aufgefasst und bewiesen werden kann.

Blömer und May geben in ihrer Arbeit [1] eine flexible Formulierung des Ergebnisses von Coppersmith an: Die Schranken der Nullstellen des betrachteten Polynoms $p(x, y)$ werden in Abhängigkeit von Monom-Mengen angeben, die bezüglich des Polynoms $p(x, y)$

gewählt werden. Die Nullstellen von $p(x, y)$, die diesen Schranken genügen, können dann in Polynomialzeit berechnet werden. Diese Formulierung hat den Vorteil, dass das Ergebnis ohne jegliche Kenntnis über Gittertheorie als eine Art "Blackbox" angewandt werden kann.

Wir werden in dieser Arbeit zunächst den bivariaten ganzzahligen Fall des Satzes von Coppersmith in der Formulierung von Blömer und May angeben. Allerdings nutzen wir im Beweis nicht die Methode von Coppersmith, sondern verwenden die Beweismethode von Coron. Damit erhalten wir zwar ein etwas schlechteres Ergebnis, gleichzeitig müssen aber die Monom-Mengen eine wesentlich schwächere Bedingung erfüllen.

Diese Methode lässt sich auf den trivariaten ganzzahligen Fall übertragen. Dabei wird die Methode allerdings heuristisch. Denn wir können nicht gewährleisten, dass die Polynome, welche wir durch Gitterreduktion erhalten, teilerfremd sind. Somit lässt sich nicht sicherstellen, dass alle im Beweis der Methode benötigten Resultanten von 0 verschieden sind.

Auch im trivariaten Fall formulieren wir das Ergebnis nur in Abhängigkeit des betrachteten Polynoms $p(x, y, z)$ und zweier Mengen von Monomen, welche bezüglich des Polynoms $p(x, y, z)$ gewählt werden. Die Formulierung unseres Ergebnisses erlaubt uns, so wie in [1] das Maximierungsproblem der Schranken als Optimierungsproblem über zwei Mengen von Monomen zu betrachten. Das bedeutet, wir können das Ergebnis als "Blackbox" für die Optimierung der Nullstellenschranken trivariater Polynomen von spezieller Form nutzen.

In dieser Arbeit werden wir die Schranken ausschließlich für bivariate modulare Polynome analysieren, welche wir als trivariate ganzzahlige Polynome auffassen. Dabei betrachten wir verschiedene Formen des Newton-Polygons der bivariaten modularen Polynome. Es stellt sich heraus, dass der bivariate modulare Fall als Spezialfall des trivariaten Falls aufgefasst werden kann.

Ein Beispiel dafür bietet das Polynom von Boneh und Durfee [2]. Wiener [15] zeigte 1990, dass das RSA-Verschüsselungssystem gebrochen werden kann, wenn ein geheimer Schlüssel d mit $d < N^{0.25}$ benutzt wird. Boneh und Durfee verbessern dieses Ergebnis, indem sie den geheimen Schlüssel d als Nullstelle eines modularen Polynoms bestimmen, welches sich aus der RSA-Schlüsselgleichung ergibt. Dabei erhalten sie, dass der geheime Schlüssel d in Polynomialzeit berechenbar ist, wenn $d < N^{0.284}$ gilt. Wir werden in dieser Arbeit das Polynom von Boneh und Durfee als trivariates ganzzahliges Polynom betrachten und so die gleichen Ergebnis erhalten. Dies ist nur ein Beispiel für die wichtige Rolle, die die Coppersmith-Methode in der Kryptanalyse von Kryptosystemen wie RSA spielt.

Die Arbeit gliedert sich in folgende Teile:

Kapitel 2 In diesem Kapitel geben wir zunächst eine kurze Einführung in die Gittertheorie, soweit wir sie in der Arbeit benötigen. Im zweiten Abschnitt des Kapitels führen wir den Begriff der Norm eines Polynoms ein. Insbesondere befassen wir uns mit dem Zusammenhang zwischen der Norm zweier Polynome und ihrer

Teilbarkeitsbeziehung. Abschließend erläutern wir weitere mathematische Grundlagen, welche wir im Verlauf der Arbeit benötigen werden.

Kapitel 3 Wir geben zunächst obere Schranken für die Nullstellen bivariater ganzzahliger Polynome an. Alle Nullstellen, die diesen Schranken genügen, können in polynomieller Zeit gefunden werden. Unser Ergebnis ist geringfügig schlechter als das entsprechende Ergebnis von Coppersmith. Der Beweis beruht auf einer Methode von Coron und liefert einen Polynomialzeit-Algorithmus zur Nullstellensuche bei bivariaten ganzzahligen Polynomen, sofern die Nullstellen den angebenen Schranken genügen. Anschließend untersuchen wir die Schranken konkret für ein Polynom $p(x, y)$ vom Grad δ in jeder Variablen. Abschließend verallgemeinern wir den bivariaten ganzzahligen Fall auf die trivariaten ganzzahigen Fall.

Kapitel 4 Die in Kapitel 3 genannten Schranken werden in Abhängigkeit von zwei Monom-Mengen S und M angeben. Diese Mengen spielen bei der Optimierung der Schranken eine entscheidende Rolle. Daher richten wir in diesem Kapitel unser Augenmerk auf mögliche Konstruktionen für die Mengen S und M sowohl für den bivariaten ganzzahligen als auch für den bivariaten modularen Fall, welchen wir als trivariaten ganzzahligen Fall auffassen.

Kapitel 5 Hier befassen wir uns mit der Optimierung der Schranken im bivariaten modularen Fall aufgefasst als trivariaten ganzzahligen Fall. Dabei hängt die Optimierung von der Form des Newton-Polygons $N(f)$ des Polynoms $f(y, z)$ ab, welches wir modulo einer ganzen Zahl N mit unbekannter Faktorisierung betrachten. Der Satz von Coron für den trivariaten Fall, welchen wir im Kapitel 3 kennengelernt haben, dient uns als "Blackbox" bei der Analyse.

Kapitel 6 In diesem Kapitel verwenden wir die Methode von Coron und Coppersmith im trivariaten ganzzahligen Fall für die Kryptanalyse des RSA-Kryptosystem. Zunächst beweisen wir das Ergebnis von Boneh und Durfee [2]. Es besagt, dass der geheime Schlüssel d im RSA-Verfahren in Polynomialzeit berechnet werden kann, sofern $d < N^{0.284}$ gilt. Hier ist N der RSA-Modul. Anschließend geben wir zwei Angriffe auf RSA an, bei denen die höchstwertigen Bits des geheimen Schlüssels bekannt sind [8].

2 Grundlagen über Gitter und Polynome

2.1 Der LLL-Algorithmus

Gitter sind diskrete, additive Untergruppen des $\mathbb{R}^n$. Sie sind als Punktmengen des Vektorraums $\mathbb{R}^n$ Gegenstand der von Minkowski entwickelten Geometrie der Zahlen.

Es seien n und k positive ganze Zahlen, für welche $n \geq k$ gilt. Eine Teilmenge L des n-dimensionalen Vektorraums $\mathbb{R}^n$ heißt *Gitter*, wenn es eine Menge E von Vektoren im $\mathbb{R}^n$ gibt, sodass

$$L = \mathcal{L}(E) := \{r_1 b_1 + \cdots + r_k b_k \mid b_i \in E, r_i \in \mathbb{Z}\}$$

gilt. Die Menge E heißt erzeugende Menge für das Gitter L. Falls E minimale Kardinalität unter allen erzeugenden Mengen für L hat, heißt E *Basis* von L. Die Kardinalität einer Basis von L wird als *Dimension* oder *Rang* $\dim L$ des Gitters bezeichnet. Es gelte $k = \dim L$ für ein Gitter $L \subset \mathbb{R}^n$. Ein Gitter hat *vollen Rang*, wenn $k = n$ ist. Die Basis $[b_1, \ldots, b_k]$ eines Gitters L kann als Matrix

$$B = [b_1, \ldots, b_k] \in \mathbb{R}^{n \times k}$$

dargestellt werden.

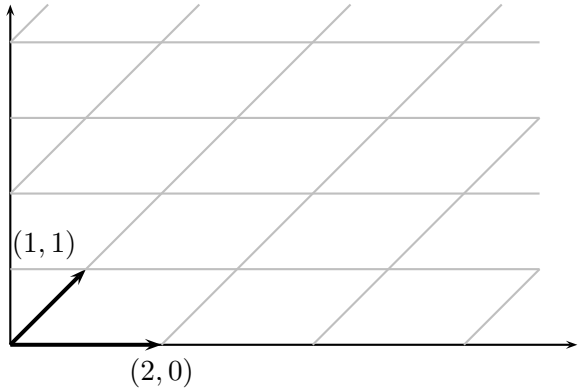

Abbildung 2.1: Gitter mit Basis $B = [(1, 1)(2, 0)]$

Eine Matrix $U \in \mathbb{Z}^{n \times n}$ heißt *unimodular*, wenn $\det(U) = \pm 1$ gilt.

Satz 2.1
Es seien $B_1, B_2 \in \mathbb{R}^{k\times n}$ zwei Basen. Dann gilt $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ genau dann, wenn eine ganzzahlige unimodulare Matrix U existiert, sodass $B_1 = B_2U$ gilt.

Der Beweis kann in [16] nachgelesen werden.

Definition 2.2
Die Determinante eines Gitters L ist gegeben durch

$$\det L := \sqrt{\det(B^T B)},$$

wobei B eine Basis von L ist. Wenn das Gitter vollen Rang hat, gilt

$$\det L = |\det B|.$$

Die Determinate eines Gitters ist eine Invariante; sie ist unabhängig von der gewählten Basis. Dies kann mit Satz 2.1 gezeigt werden: Es gelte $B_1 = B_2U$ für eine unimodulare Matrix U. Dann gilt

$$\begin{aligned}\det(B_1^T B_1) &= \det(U^T B_2^T B_2 U)\\ &= \det(U^T)\det(B_2^T B_2)\det(U)\\ &= \det(B_2^T B_2),\end{aligned}$$

da die Determinate einer unimodularen Matrix ± 1 ist.

Gram-Schmidt-Orthogonalisierung

Im Rest dieses Abschnitts bezeichnen wir mit $\langle\cdot,\cdot\rangle$ das Standard-Skalarprodukt auf dem Vektorraum $\mathbb{R}^n$ und definieren die Euklidische Norm eines Vektors $v \in \mathbb{R}^n$ als $\|v\| := \sqrt{\langle v, v\rangle}$. Die Gram-Schmidt-Orthogonalisierung berechnet zu einer gegebenen Basis $B = [b_1, \ldots, b_k] \subset \mathbb{R}^{n\times k}$ eine orthogonale Matrix B^*. Eine Matrix $B^* = [b_1^*, \ldots, b_k^*]$ heißt *orthogonal*, wenn $\left\langle b_i^*, b_j^*\right\rangle = 0$ für alle $1 \le i < j \le k$ gilt. Zu einer gegebenen Basis $B = [b_1, \ldots, b_k]$ wird die Gram-Schmidt-Orthogonalisierung folgendermaßen berechnet:

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \qquad \text{für } i = 1, \ldots, k, \tag{2.1}$$

wobei

$$\mu_{ij} = \frac{\left\langle b_i, b_j^*\right\rangle}{\left\langle b_j^*, b_j^*\right\rangle}$$

und $b_1^* = b_1$ ist.

Da die Gram-Schmidt-Orthogonalisierung B^* einer Gitterbasis B im Allgemeinen nicht

aus Gittervektoren besteht, wird eine Gitterbasis gesucht, die möglichst "nah" an der Gram-Schmidt-Orthogonalisierung liegt. Ein Maß für die Abweichung von der Gram-Schmidt-Orthogonalisierung ist der sogenannte Orthogonalitätsdefekt

$$\delta(B) = \frac{\|b_1\| \cdots \|b_k\|}{\sqrt{\det(B^T B)}},$$

wobei B eine reelle $n \times k$-Matrix ist.

Definition 2.3
Eine Gitterbasis $B = [b_1, \ldots, b_n]$ mit $b_i = \sum_{j=1}^{i} \mu_{ij} b_j^*$, wobei $\mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$ für $j < i$ und $\mu_{ii} = 1$ ist, heißt schwach-reduziert oder längenreduziert, wenn die Gram-Schmidt-Koeffizienten

$$|\mu_{ij}| \leq \frac{1}{2} \tag{2.2}$$

für $1 \leq j < i \leq m$ erfüllen.

Lenstra, Lenstra und Lovász führten 1982 den Begriff der (LLL-)reduzierten Gitterbasis ein und stellten einen Algorithmus vor, der eine solche Basis in Polynomialzeit berechnet [11]. Für diese reduzierten Basen lassen sich die folgenden Abschätzungen zeigen, die wir in Kapitel 3 für den Beweis unseres Hauptergebnisses benötigen. Im Rest des Abschnitts werden ausschließlich Gitter mit vollem Rang betrachtet. Dies stellt keine Einschränkung dar, denn alle Ergebnisse lassen sich leicht auf nicht-volldimensionale Gitter übertragen.

Definition 2.4
Eine Gitterbasis $B = [b_1, \ldots, b_n]$ des Gitters $L \subset \mathbb{R}^n$ heißt (LLL-)reduziert, falls

(i) die Basis schwach reduziert ist und

(ii) (Lovász-Bedingung)
für alle $1 \leq i \leq n$ gilt, dass

$$\frac{3}{4}\|b_i^*\|^2 \leq \|b_{i+1}(i)\|^2, \tag{2.3}$$

wobei $b_{i+1}(i) = b_{i+1}^* + \mu_{i+1,i} b_i^*$ die Projektion von b_{i+1} auf das orthogonale Komplement von $\mathbb{R}b_i + \cdots + \mathbb{R}b_{i-1}$ und $B^* = [b_1^*, \ldots, b_n^*]$ die zugehörige Gram-Schmidt-Orthogonalisierung ist.

Lemma 2.5
Für eine reduzierte Gitterbasis $B = [b_1, \ldots, b_n]$ und die zugehörige Gram-Schmidt-Orthogonalisierung $B^* = [b_1^*, \ldots, b_n^*]$ von B gilt

$$\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2 \text{ für } i = 1, \ldots, n-1.$$

Beweis: Da die Basis B reduziert ist, gilt für $1 \leq i \leq n-1$ die Bedingung (2.3):

$$\begin{aligned}
\frac{3}{4}\|b_i^*\|^2 &\leq \|b_{i+1}(i)\|^2 \\
&= \|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 \\
&= \|b_{i+1}^*\|^2 + \mu_{i+1,i}^2 \|b_i^*\|^2 \\
&\overset{(2.2)}{\leq} \|b_{i+1}^*\|^2 + \frac{1}{4}\|b_i^*\|^2.
\end{aligned}$$

Daraus folgt direkt

$$\frac{1}{2}\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2.$$

□

Mit diesem Lemma lassen sich die folgenden Abschätzungen zeigen.

Satz 2.6
Es sei $B = [b_1, \ldots, b_n]$ eine reduzierte Basis des Gitters $L \subset \mathbb{R}^n$ und $B^* = [b_1^*, \ldots, b_n^*]$ die zugehörige Gram-Schmidt-Orthogonalisierung. Dann gilt

(i)
$$\|b_j\|^2 \leq 2^{i-1}\|b_i^*\|^2 \quad \textit{für } 1 \leq j \leq i \leq n,$$

(ii)
$$\det(L) \leq \prod_{i=1}^{n} \|b_i\| < 2^{\frac{n(n-1)}{4}} \det(L),$$

(iii)
$$\|b_1\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}.$$

Beweis:

(i) Aus Lemma 2.5 ist bekannt, dass

$$\|b_{i-1}^*\|^2 \leq 2\|b_i^*\|^2 \qquad \text{für } 1 < i \leq n$$

gilt. Induktiv folgt

$$\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2 \qquad \text{für } 1 \leq j < i \leq n. \tag{2.4}$$

Weiterhin lässt sich b_i folgendermaßen abschätzen

$$\begin{aligned}
\|b_i\|^2 &= \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \|b_j^*\|^2 \\
&\leq \|b_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} \|b_j^*\|^2 \\
&\overset{(2.4)}{\leq} \|b_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} 2^{i-j} \|b_i^*\|^2 \\
&= (1 + \frac{1}{4}(2^i - 2)) \|b_i^*\|^2 \\
&\leq 2^{i-1} \|b_i^*\|^2.
\end{aligned}$$

Dies liefert insgesamt

$$\|b_j\|^2 \leq 2^{j-1} \|b_j^*\|^2 \leq 2^{j-1} 2^{i-j} \|b_i^*\|^2 \leq 2^{i-1} \|b_i^*\|^2$$

für $1 \leq j \leq i \leq n$.

(ii) Aus (2.1) folgt zunächst, dass

$$\det(L) = |\det(b_1, \ldots, b_n)| = |\det(b_1^*, \ldots, b_n^*)|$$

gilt. Mit der paarweisen Orthogonalität der Basisvektoren b_i^* gilt weiterhin:

$$\det(L) = |\det(b_1^*, \ldots, b_n^*)| = \prod_{i=1}^{n} \|b_i^*\|.$$

Zusammen mit $\|b_i^*\| \leq \|b_i\|$ und $\|b_i\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|$ liefert dies

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

(iii) Nach (i) gilt

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

Daraus ergibt sich insgesamt

$$\|b_1\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}.$$

□

Im weiteren Verlauf dieser Arbeit werden ausschließlich ganzzahlige Gitter betrachtet, da wir nur ganzzahlige Gitter benötigen und verwenden werden. Der von Lenstra, Lenstra und Lovász entwickelte LLL-Algorithmus berechnet in polynomieller Zeit zu einer gegeben ganzzahligen Gitterbasis eine reduzierte Basis:

Der LLL-Algorithmus baut auf der Definition 2.4 auf. Die Gitterbasis wird schwach-reduziert, indem die Gram-Schmidt-Koeffizienten ganzzahlig gerundet werden. Anschließend wird überprüft, ob die Lovász-Bedingung verletzt ist. Ist dies der Fall werden die entsprechenden Gittervektoren vertauscht und es wird erneut schwach-reduziert. Dieser Vertauschungsschritt wird solange wiederholt, bis die Lovász-Bedingung nicht mehr verletzt ist.

Der Algorithmus benötigt die folgende Laufzeit:

Satz 2.7
Es sei $L \subset \mathbb{Z}^n$ ein Gitter mit Basis $[b_1, \ldots, b_n]$ und $A \in \mathbb{R},\ A \geq 2,\ A = max_k \|b_k\|$. Dann berechnet der LLL-Algorithmus eine reduzierte Basis für L und benötigt dazu höchstens $\mathcal{O}(n^4 \log A)$ arithmetische Operationen beziehungsweise $\mathcal{O}(n^5 \log^2 A)$ Bit-Operationen.

Details des Algorithmus' sowie die Analyse der Laufzeit sind nachzulesen in [11].

Für die ganzzahligen Gitterbasen wird in dieser Arbeit nicht nur eine Abschätzung des Basisvektors b_1, sondern auch eine Abschätzung für den zweiten Basisvektor b_2 einer LLL-reduzierten Gitterbasis benötigt. Hier wird eine Abschätzung für einen beliebigen Basisvektor einer reduzierten ganzzahligen Gitterbasis angegeben (vgl.[12]).

Satz 2.8
Es sei $B = [b_1, \ldots, b_n]$ eine LLL-reduzierte Gitterbasis des ganzzahligen Gitters $L \subset \mathbb{Z}^n$. Dann gilt

$$\|b_i\| \leq 2^{\frac{n(n-1)}{4(n-i+1)}} \det(L)^{\frac{1}{n-i+1}} \text{ für } i = 1, \ldots, n.$$

Insbesondere liefert dies eine Abschätzung für den zweiten Basisvektor b_2:

$$\|b_2\| \leq 2^{\frac{n}{4}} \det(L)^{\frac{1}{n-1}}.$$

Beweis: Es bezeichne $B^* = [b_1^*, \ldots, b_n^*]$ die zur Gitterbasis B zugehörige Gram-Schmidt-Orthogonalisierung. Für eine LLL-reduzierte Basis $B = [b_1, \ldots, b_n]$ gilt nach Lemma 2.6 die Abschätzung

$$\|b_i\| \leq 2^{\frac{j-1}{2}} \|b_j^*\| \text{ für } 1 \leq i \leq j \leq n.$$

Diese Ungleichung wird für einen festen Basisvektor b_i einmal für alle $j,\ i \leq j \leq n$ angewendet, was Folgendes ergibt

$$\|b_i\|^{n-i+1} \leq \prod_{j=i}^{n} 2^{\frac{j-1}{2}} \|b_j^*\|.$$

Da das Gitter L und somit auch b_1 ganzzahlig ist, gilt $\|b_1^*\| = \|b_1\| \geq 1$. Die Basis ist LLL-reduziert. Daher erhalten wir zusammen mit Lemma 2.5

$$1 \leq \|b_1^*\| \leq 2^{\frac{j-1}{2}} \|b_j^*\| \text{ für } 1 \leq j \leq n.$$

Hiermit lässt sich nun folgende Abschätzung für $\|b_i\|$ angeben

$$\begin{aligned} \|b_i\|^{n-i+1} &\leq \prod_{j=i}^{n} 2^{\frac{j-1}{2}} \|b_j^*\| \\ &\leq \prod_{j=1}^{n} 2^{\frac{j-1}{2}} \|b_j^*\| \\ &= 2^{\frac{n(n-1)}{4}} \det(L). \end{aligned}$$

Es folgt

$$\|b_i\| \leq 2^{\frac{n(n-1)}{4(n-i+1)}} \det(L)^{\frac{1}{n-i+1}}.$$

□

2.2 Schranken für Polynome

In diesem Abschnitt leiten wir einige Beziehungen zwischen den Normen von Polynomen und ihrer Teilbarkeitsbeziehung her. Diese benötigen wir später, um die Teilerfremdheit zweier Polynome sicherzustellen. Des Weiteren geben wir eine Schranke für die Norm eines Polynoms an, die uns garantiert, dass die Nullstellen modulo einer ganzen Zahl n bereits Nullstellen über $\mathbb{Z}$ sind.

Es wird folgende Notation benutzt: Für ein Polynom $h(x, y, z) = \sum_{i,j,k} h_{ijk} x^i y^j z^k$ definieren wir die Euklidische Norm $\|h\|^2 := \sum_{i,j,k} |h_{ijk}|^2$ und die Maximumsnorm $\|h\|_\infty := \max_{i,j,k} |h_{ijk}|$. Die gleiche Notation wird auch für den bivariaten und univariaten Fall verwendet.

Die nachfolgenden Lemmata benötigen wir zum Beweis der Hauptaussagen dieser Arbeit. Wir geben die Lemmata jeweils für den bivariaten und trivariaten Fall an. Die Beweise der bivariaten Versionen der Lemmata sind nachzulesen in [7]. Sie beruhen auf einem Ergebnis von Mignotte. Für den trivariaten Fall erhalten wir ähnliche Ergebnisse. Ihre Beweise verlaufen analog zu den Beweisen des bivariaten Falls. Sie beruhen ebenfalls auf dem folgenden Ergebnis von Mignotte [13].

Satz 2.9 (Mignotte)
Es seien $f(x)$ und $g(x)$ zwei von 0 verschiedene Polynome über $\mathbb{Z}$ mit $\deg f \leq k$ und f teile g in $\mathbb{Z}[x]$. Dann gilt

$$\|g\| \geq 2^{-k} \|f\|_\infty.$$

Lemma 2.10
Es seien $a(x,y)$ und $b(x,y)$ zwei von 0 verschiedene Polynome über $\mathbb{Z}$ vom maximalen Grad d_x, d_y in x und y mit der Eigenschaft, dass $b(x,y)$ eine Vielfaches von $a(x,y)$ in $\mathbb{Z}[x,y]$ ist. Dann gilt

$$||b|| \geq 2^{-(d_x+1)(d_y+1)} \cdot ||a||_\infty$$

.

Lemma 2.11
Es seien $a(x,y)$ und $b(x,y)$ wie in Lemma 2.10. Weiter sei $a(0,0) \neq 0$ und $b(x,y)$ teilbar durch eine ganze Zahl $r \neq 0$, sodass der konstante Term $a(0,0)$ des Polynoms $a(x,y)$ und r teilerfremd sind. Dann ist $b(x,y)$ teilbar durch $r \cdot a(x,y)$ und

$$||b|| \geq 2^{-(d_x+1)(d_y+1)} \cdot |r| \cdot ||a||_\infty.$$

Nun formulieren wir diese Ergebnisse für den trivariaten Fall und beweisen sie mit Hilfe des Satzes von Mignotte 2.9.

Lemma 2.12
Es seien $\tilde{a}(x,y,z)$ und $\tilde{b}(x,y,z)$ zwei von 0 verschiedene Polynome über $\mathbb{Z}$ mit maximalem Grad d_x, d_y und d_z in x, y und z, sodass $\tilde{b}(x,y,z)$ ein Vielfaches von $\tilde{a}(x,y,z)$ in $\mathbb{Z}[x,y,z]$ ist. Dann gilt

$$\|\tilde{b}\| \geq 2^{-(d_x+1)(d_y+1)(d_z+1)} \cdot \|\tilde{a}\|_\infty.$$

Beweis: Wir setzen in 2.9

$$f(x) := \tilde{a}(x, x^{d_x+1}, x^{(d_x+1)(d_y+1)}).$$

Dann gilt

$$\deg f \leq d_x + d_y(d_x+1) + d_z(d_x+1)(d_y+1) \leq (d_x+1)(d_y+1)(d_z+1)$$

und die Polynome $\tilde{a}(x,y,z)$ und $f(x)$ haben die gleiche Liste von 0 verschiedener Koeffizienten. Daher gilt $\|\tilde{a}\|_\infty = \|f\|_\infty$. Analog setzen wir

$$g(x) := \tilde{b}(x, x^{d_x+1}, x^{(d_x+1)(d_y+1)}),$$

dann gilt $\|g\| = \|\tilde{b}\|$. Außerdem ist $f(x)$ ein Teiler von $g(x)$ in $\mathbb{Z}[x]$. Mit dem Ergebnis von Mignotte (Satz 2.9) erhalten wir nun

$$\|\tilde{b}\| = \|g\| \geq 2^{-(d_x+1)(d_y+1)(d_z+1)}\|f\|_\infty = 2^{-(d_x+1)(d_y+1)(d_z+1)}\|\tilde{a}\|_\infty.$$

□

Lemma 2.13
Es seien $\tilde{a}(x,y,z)$ und $\tilde{b}(x,y,z)$ wie in Lemma 2.12. Es sei $\tilde{a}(0,0,0) \neq 0$ und $\tilde{b}(x,y,z)$ teilbar durch eine ganze Zahl $r \neq 0$ mit der Eigenschaft, dass $\mathrm{ggT}(\tilde{a}(0,0,0), r) = 1$. Dann ist $\tilde{b}(x,y,z)$ teilbar durch $r \cdot \tilde{a}(x,y,z)$ und es gelte

$$\|\tilde{b}\| \geq 2^{-(d_x+1)(d_y+1)(d_z+1)} \cdot |r| \cdot \|\tilde{a}\|_\infty.$$

Beweis: Es sei $\tilde{a}(x,y,z) = \sum a_{ijk} x^i y^j z^k$. Dann ist $a_{000} = \tilde{a}(0,0,0)$ der konstante Term des Polynoms $\tilde{a}(x,y,z)$. Es sei $\lambda(x,y,z)$ das Polynom mit

$$\tilde{a}(x,y,z) \cdot \lambda(x,y,z) = \tilde{b}(x,y,z).$$

Wir wollen zeigen, dass r ein Teiler von $\lambda(x,y,z)$ ist.
Dazu nehmen wir zunächst an, dass r das Polynom $\lambda(x,y,z)$ nicht teilt.
Es sei λ_{ijk} ein Koeffizient von $x^i y^j z^k$ in $\lambda(x,y,z)$, der nicht durch r teilbar ist. Wir wählen das bezüglich der lexikographischen Ordnung kleinste Tripel (i,j,k), sodass λ_{ijk} nicht durch r teilbar ist.
Da

$$b_{ijk} = a_{000}\lambda_{ijk} + \underbrace{a_{100}\lambda_{i-1,jk} + a_{010}\lambda_{ij-1k} + a_{001}\lambda_{ijk-1} \cdots}_{\equiv 0 \mod r}$$

ist, gilt $b_{ijk} \equiv \lambda_{ijk} \cdot \tilde{a}(0,0,0) \mod r$, wobei b_{ijk} der Koeffizient von $x^i y^j z^k$ in $\tilde{b}(x,y,z)$ ist. Da $\tilde{a}(0,0,0)$ modulo r invertierbar ist und $b_{ijk} \equiv 0 \mod r$, liefert $r \nmid \lambda_{ijk}$ einen Widerspruch. Somit teilt r das Polynom $\lambda(x,y,z)$ und $r\tilde{a}(x,y,z)$ teilt $\tilde{b}(x,y,z)$. Um die gewünschte Abschätzung zu erhalten, wird Lemma 2.12 auf $r\tilde{a}(x,y,z)$ und $\tilde{b}(x,y,z)$ angewendet. □

Auch das Lemma von Howgrave-Graham [10], welches Coron [7] für den bivariaten Fall zeigt, lässt sich auf den trivariaten Fall verallgemeinern.

Lemma 2.14 (Howgrave-Graham)
Es sei $h(x,y,z) \in \mathbb{Z}[x,y,z]$ die Summe von höchstens w Monomen. Wenn $h(x_0,y_0,z_0) \equiv 0 \mod n$ mit $|x_0| \leq X$, $|y_0| \leq Y$ und $|z_0| \leq Z$ ist und $\|h(xX,yY,zZ)\| < \frac{n}{\sqrt{w}}$ gilt, dann gilt auch $h(x_0,y_0,z_0) = 0$ über $\mathbb{Z}$.

Beweis: Es gilt:

$$\begin{aligned}
|h(x_0,y_0,z_0)| &= |\sum h_{ijk} x_0^i y_0^j z_0^k| \\
&= |\sum h_{ijk} X^i Y^j Z^k \left(\frac{x_0}{X}\right)^i \left(\frac{y_0}{Y}\right)^j \left(\frac{z_0}{Z}\right)^k| \\
&\leq \sum |h_{ijk} X^i Y^j Z^k \left(\frac{x_0}{X}\right)^i \left(\frac{y_0}{Y}\right)^j \left(\frac{z_0}{Z}\right)^k| \\
&\leq \sum |h_{ijk} X^i Y^j Z^k| \\
&\leq \sqrt{w}\|h(xX,yY,zZ)\| \\
&< n.
\end{aligned}$$

Da $h(x_0,y_0,z_0) \equiv 0 \mod n$, gilt auch $h(x_0,y_0,z_0) = 0$ über $\mathbb{Z}$. □

2.3 Weitere Grundlagen

2.3.1 Die Resultante

Es sei R ein Ring. Ferner seien $f = \sum_{0 \leq i \leq n} f_i x^i$, $g = \sum_{0 \leq i \leq m} g_i x^i$ Polynome mit Koeffizienten $f_i, g_i \in R$ vom Grad n beziehungsweise m. Für $d \in \mathbb{N}$ definieren wir

$$P_d := \{a \in R[x] | \deg a < d\}.$$

Wir betrachten für die Polynome $f, g \in R[x]$ mit $n := \deg f$ und $m := \deg g$ die folgende lineare Abbildung zwischen zwei Vektorräumen der Dimension $n + m$

$$\begin{array}{rccc} \varphi_0 & : & P_m \times P_n & \rightarrow & P_{n+m} \\ & & (s,t) & \mapsto & sf + tg. \end{array}$$

Die *Sylvestermatrix* $\mathrm{Syl}(f, g)$ ist die Darstellungsmatrix der linearen Abbildung φ_0.

$$\mathrm{Syl}(f,g) = \begin{pmatrix} f_n & & & & g_m & & & & \\ f_{n-1} & f_n & & & g_{m-1} & g_m & & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & \\ \vdots & \vdots & & f_n & g_1 & \vdots & & \ddots & \\ \vdots & \vdots & & f_{n-1} & g_0 & \vdots & & & \ddots \\ \vdots & \vdots & & \vdots & & g_0 & & & g_m \\ f_0 & \vdots & & \vdots & & & \ddots & & \vdots \\ & f_0 & & \vdots & & & & \ddots & \vdots \\ & & \ddots & \vdots & & & & & \ddots \\ & & & f_0 & & & & & g_0 \end{pmatrix}$$

Dabei enthalten die ersten m Spalten der Matrix die Koeffizienten von f und die letzten n Spalten die Koeffizienten von g.

Die *Resultante* $\mathrm{res}(f, g)$ ist definiert als Determinante der Sylvestermatrix von f und g:

$$\mathrm{res}(f,g) = \det(\mathrm{Syl}(f,g)).$$

Falls wir zwei bivariate Polynome $f(x, y)$ und $g(x, y)$ mit Koeffizienten im Ring R betrachten, berechnen wir die Resultante bezüglich x oder bezüglich y. Falls wir beispielsweise die Resultante $\mathrm{res}_y(f, g)$ von f und g bezüglich der Variablen y berechnen wollen, fassen wir $f(x, y)$ und $g(x, y)$ als Polynome in y mit Koeffizienten im Ring $R[x]$ auf. Die Resultante $\mathrm{res}_y(f, g)$ von f und g bezüglich y ist somit ein Polynom in x. Analog können wir für zwei trivariate Polynome f, g die Resultanten $\mathrm{res}_x(f, g)$ bezüglich x, $\mathrm{res}_y(f, g)$ bezüglich y und $\mathrm{res}_z(f, g)$ bezüglich z berechnen.

Wir benötigen in dieser Arbeit die folgende wichtige Eigenschaft der Resultante [9]:

Satz 2.15
Es sei R ein Euklidischer Ring und $f, g \in R[x]$ zwei Polynome. Dann gilt

$$\mathrm{ggT}(f,g) = 1 \iff \mathrm{res}(f,g) \neq 0.$$

Beweis: Es gelte $\mathrm{ggT}(f,g) > 1$. Dann existiert ein Tupel $(s,t) \in P_m \times P_n \setminus \{(0,0)\}$ mit $sf + tg = 0$ und das Paar (s,t) liegt im Kern $\ker \varphi_0$. Somit ist φ_0 nicht injektiv und folglich auch kein Isomorphismus. Daher ist auch die Darstellungsmatrix $\mathrm{Syl}(f,g)$ nicht invertierbar und ihre Determinate ist 0. Somit ist $\mathrm{res}(f,g) = \det(Syl(f,g)) = 0$.

Es gelte andererseits $\mathrm{res}(f,g) = 0$. Dann ist die Matrix $\mathrm{Syl}(f,g)$ nicht invertierbar. Daher ist φ_0 kein Isomorphismus. Da es sich um eine lineare Abbildung zwischen zwei Vektorräumen der gleichen Dimension handelt, ist φ_0 also nicht injektiv. Das heißt, es existiert ein Paar $(s,t) \in P_m \times P_n$ mit $(s,t) \neq (0,0)$ und $sf + tg = 0$. Daraus folgt nun, dass der ggT von f und g nicht trivial ist. □

2.3.2 Lexikographische Ordnung

Es seien $(a_1, \ldots, a_n)$ und $(a'_1, \ldots, a'_n)$ Elemente aus $\mathbb{Z}^n$. Dann ist $(a_1, \ldots, a_n)$ bezüglich der lexikographischen Ordnung kleiner als $(a'_1, \ldots, a'_n)$, wenn in $(a_1, \ldots, a_n) - (a'_1, \ldots, a'_n) \in \mathbb{Z}^n$ das erste von 0 verschiedene Element negativ ist. Dies bedeutet, es gilt $a_k < a'_k$ für ein $k \leq n$ und $a_i = a'_i$ für alle $i < k$.

Es seien $M = x_1^{e_1} \cdots x_n^{e_n}$ und $M' = x_1^{e'_1} \cdots x_n^{e'_n}$ zwei Monome. Dann ist M' lexikographisch kleiner als M, wenn der Multiindex $(e'_1, \ldots, e'_n)$ von M' lexikographisch kleiner ist als der Multiindex $(e_1, \ldots, e_n)$ von M.

3 Die Ergebnisse von Coron und Coppersmith

Coppersmith stellte 1996 einen Algorithmus zur Nullstellensuche bei bivariaten ganzzahligen Polynomen vor [3]. Mit diesem Algorithmus lassen sich die Nullstellen eines Polynoms in polynomieller Zeit berechnen unter der Voraussetzung, dass die Lösungen hinreichend klein sind.

Der Beweis von Coppersmith beruht auf Gitterredukion. Allerdings ist der Beweis sehr aufwendig. Coron stellt in [7] einen vereinfachten Zugang zu diesem Problem vor. Das führt jedoch zu einer etwas schlechteren Schranke als bei der Methode von Coppersmith. Außerdem betrachtet er nur zwei Spezialfälle in Bezug auf die Form des zu untersuchenden Polynoms.

Blömer und May stellen in [1] eine neue, flexible Formulierung der Coppersmith-Methode zur Suche kleiner Nullstellen ganzzahliger bivariater Polynome $p(x, y)$ vor. Dabei hängt das Ergebnis von zwei Monom-Mengen ab, die bezüglich des betrachteten Polynoms $p(x, y)$ gewählt werden. Diese Methode erlaubt es, die Schranken der Lösungen zu maximieren. Weiterhin werden in ihrer Arbeit [1] Konstruktionen für Monom-Mengen für verschiedenen Formen des Newton-Polygons von $p(x, y)$ angegeben.

Wir werden in diesem Kapitel zunächst allgemein den bivariaten ganzzahligen Fall des Satzes von Coppersmith mit den Bezeichnungen von Blömer und May [1] formulieren und ihn mit der Methode von Coron beweisen. Dabei benötigen wir in Bezug auf die Mengen, die wir betrachten, eine schwächere Bedingung als Coppersmith, erhalten aber ebenso wie Coron auch etwas schlechtere Schranken im Vergleich zu Coppersmith. Anschließend werden wir diese Methode auf den trivariaten ganzzahligen Fall verallgemeinern.

Zunächst benötigen wir noch einige Definitionen.

Definition 3.1
Es sei M eine Menge von Monomen in den Variablen $x_1, \ldots, x_n$. Ein Polynom $g(x_1, \ldots, x_n)$ ist definiert über M oder ein Polynom über M genau dann, wenn das Polynom $g(x_1, \ldots, x_n)$ dargestellt werden kann als

$$g(x_1, \ldots, x_n) = \sum_{\mu \in M} c_\mu \mu \text{ mit } c_\mu \in \mathbb{Z}.$$

Ein Polynom $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ ist *irreduzibel*, falls aus $p(x_1 \ldots, x_n) = f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)$ mit $f(x_1, \ldots, x_n),\ g(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ folgt, dass entweder $f(x_1, \ldots, x_n) = \pm 1$ oder $g(x_1, \ldots, x_n) = \pm 1$ gilt. Dies bedeutet insbesondere, dass der Inhalt eines irreduziblen Polynoms 1 ist, wobei der *Inhalt* eines Polynoms p als größter gemeinsamer Teiler der Koeffizienten von p definiert ist.

Weiterhin definieren wir das *Newton-Polygon* $N(f)$ eines bivariaten Polynoms $f(x, y) = \sum f_{ij} x^i y^j$ als konvexe Hülle der im Polynom f auftretenden Exponenten der Monome:

$$N(f) := \operatorname{conv}\left\{(i, j) \in \mathbb{N}^2 \mid f_{ij} \neq 0\right\}.$$

Diese Definition lässt sich auf den trivariaten Fall übertragen. So ist das *Newton-Polytop* $N(g)$ eines trivariaten Polynoms $g(x, y, z) = \sum g_{ijk} x^i y^j z^k$ definiert als

$$N(g) := \operatorname{conv}\left\{(i, j, k) \in \mathbb{N}^3 \mid g_{ijk} \neq 0\right\}.$$

3.1 Der bivariate Fall

In seiner Arbeit [7] betrachtet Coron nur bivariate ganzzahlige Polynome $p(x, y)$ mit Grad δ in jeder Variablen beziehungsweise vom totalen Grad δ. Wir beweisen in diesem Abschnitt mit der Methode von Coron eine allgemeine Bedingung für die Größe der Nullstellen irreduzibler bivariater ganzzahliger Polyome $p(x, y)$ vom Grad d_x in x und d_y in y. Anschließend geben wir für bivariate ganzzahlige Polynome vom Grad δ in jeder Variablen eine genauere Schranke für die Größe der Nullstellen an und erhalten hier das gleiche Ergebnis wie Coron [7].

Nun geben wir eine allgemeine Bedingung an, welche Nullstellen bivariater ganzzahliger Polynome erfüllen müssen, damit sie in Polynomialzeit berechnet werden können.

Satz 3.2 (Coron, bivariater Fall)
Es sei $p(x, y)$ ein irreduzibles ganzzahliges Polynom in zwei Variablen vom Grad höchstens $d_x, d_y \geq 1$ in den Variablen x und y und $W = \|p(xX, yY)\|_\infty$. Ferner seien S und M, $S \subset M$, Monom-Mengen mit der Eigenschaft, dass für alle Monome $\mu \in S$ gilt, dass $\mu \cdot p(x, y)$ über M definiert ist. Wir setzen

$$s := |S| \qquad m := |M|$$

$$s_x := \sum_{x^i y^j \in M \setminus S} i \qquad s_y := \sum_{x^i y^j \in M \setminus S} j.$$

Es seien k, γ und ω derart, dass

- $k = \max\{j \mid x^i y^j \in S\}$,
- $\gamma\, k = \max\{i \mid x^i y^j \in S\}$ *und*
- $\omega = (d_x + \gamma\, k + 1)(d_y + k + 1)$

gilt. Ferner seien X und Y natürliche Zahlen, welche

$$X^{s_x}Y^{s_y} < 2^{-\frac{m(4\omega+m+3)-4s}{4}}W^s \tag{3.1}$$

erfüllen. Dann können alle ganzzahligen Nullstellen (x_0, y_0) des Polynoms $p(x, y)$ mit $|x_0| \leq X$, $|y_0| \leq Y$ in Zeit polynomiell in $(\log W, m)$ gefunden werden.

Bevor wir den Satz beweisen, klären wir noch einige Bezeichnung. Elemente der Menge S heißen *Shiftmonome*. Entsprechend wird die Menge S selbst als *Shift-Menge* oder Menge der Shiftmonome bezeichnet. Gleichzeitig werden die Monom-Mengen S und M mit Mengen in der Eukidischen Ebene $\mathbb{R}^2$ identifiziert. Es sei S eine Menge von Monomen in x und y. Dann betrachten wir die konvexe Hülle conv $\left(\{(i, j) \in \mathbb{N}^2 \mid x^i y^j \in S\}\right) \subset \mathbb{R}^2$. Diese Menge wird zu Vereinfachung auch mit S bezeichnet.

Beweis: Es sei (x_0, y_0) eine ganzzahlige Nullstelle von $p(x, y)$. Wir setzen

- $W := \|p(xX, yY)\|_\infty$
- $\gamma k := \max\{j, x^i y^j \in S\}$ und
- $k := \max\{i, x^i y^j \in S\}$.

Dann gibt es ein $\lambda \in \mathbb{R}$, sodass $d_x = \lambda d_y$ gilt. Es wird angenommen, dass $p_{00} \neq 0$ und $\mathrm{ggT}(p_{00}, (X^\gamma Y)^k) = 1$ gilt.

Ist $p_{00} = 0$, so erhalten wir durch einen einfachen Wechsel der Variablen ein Polynom $p^*(x, y)$ mit $p^*_{00} \neq 0$. Das genaue Vorgehen wird im Anhang A.1 erläutert.

Falls $\mathrm{ggT}(p_{00}, (X^\gamma Y)^k)) \neq 1$ gilt, wählen wir Primzahlen X' und Y' mit $X \leq X' < 2X$ beziehungsweise $Y \leq Y' < 2Y$, sodass $\mathrm{ggT}(p_{00}, (X'^\gamma Y')^k) = 1$ gilt. Wir ersetzen dann im Folgenden X durch X' und Y durch Y'.

Wir setzen

$$u = W + ((1 - W) \mod |p_{00}|).$$

Dann lässt sich durch Nachrechnen leicht zeigen, dass

$$\sqrt{m} \cdot 2^{-m} W \leq u < 2W$$

und $\mathrm{ggT}(p_{00}, u) = 1$ gilt. Wir setzen $n = u \cdot (X^\gamma Y)^k$. Da sowohl u und p_{00} als auch $(X^\gamma Y)^k$ und p_{00} teilerfremd sind, gilt auch $\mathrm{ggT}(p_{00}, n) = 1$ und

$$\sqrt{m} \cdot 2^{-m} (X^\gamma Y)^k W \leq n < 2(X^\gamma Y)^k W. \tag{3.2}$$

Gesucht ist ein Polynom $h(x, y)$, für das $h(x_0, y_0) = 0$ gilt und welches kein Vielfaches von $p(x, y)$ ist. Da $p(x, y)$ irreduzibel ist, ist dann die Resultante bezüglich y von $p(x, y)$ und $h(x, y)$ von 0 verschieden und besitzt x_0 als Nullstelle. So können wir eine der Variablen eliminieren und die Nullstellensuche im univariaten Fall durchführen. Um ein Polynom $h(x, y)$ mit diesen Eigenschaften zu erhalten, konstruieren wir ein Gitter vollen Ranges aus den Koeffizientenvektoren von Polynomen $q_{ij}(xX, yY)$, die die Kongruenz $q_{ij}(x_0, y_0) \equiv 0 \mod n$ erfüllen. Wir wählen dann $h(xX, yY)$ mit Hilfe des

LLL-Algorithmus' als kurzen Gittervektor. Die Schranken für X und Y ergeben sich daraus, dass $h(x_0, y_0) = 0$ über $\mathbb{Z}$ gelten muss und $h(x, y)$ kein Vielfaches von $p(x, y)$ sein darf.

Es sei $q(x, y)$ definiert als das Polynom

$$q(x, y) = p_{00}^{-1} p(x, y) \mod n.$$

Für alle $(i, j) \in S$ definieren wir die Shift-Polynome

$$q_{ij}(x, y) = x^i y^j X^{\gamma k - i} Y^{k-j} q(x, y).$$

Für alle $(i, j) \in M \setminus S$ definieren wir die folgenden Hilfspolynome

$$q_{ij}(x, y) = x^i y^j n.$$

Für alle $(i, j) \in M$ gilt $q_{ij}(x_0, y_0) \equiv 0 \mod n$. Wir betrachten die zugehörigen Polynome $\tilde{q}_{ij}(x, y) = q_{ij}(xX, yY)$. Dann sind die Polynome $\tilde{q}_{ij}(x, y)$ für $(i, j) \in M$ durch $(X^\gamma Y)^k$ teilbar.

Wenn $h(x, y)$ eine ganzzahlige Linearkombination der Polynome $q_{ij}(x, y)$ ist, dann ist $h(xX, yY)$ eine Linearkombination der Polynome $\tilde{q}_{ij}(x, y)$ mit den gleichen ganzzahligen Koeffizienten. Das Polynom $h(x, y)$ ist die Summe von höchstens m Monomen, denn alle Polynome $q_{ij}(x, y)$ sind nach der Voraussetzung an die Mengen S und M über M definiert. Es gilt $h(x_0, y_0) \equiv 0 \mod n$ und $(X^\gamma Y)^k$ teilt $h(xX, yY)$. Außerdem hat $h(x, y)$ maximalen Grad $\lambda d_y + \gamma k$ beziehungsweise $d_y + k$ in x und y. Die Koeffizienten von $h(xX, yY)$ müssen hinreichend klein sein, sodass $h(x, y)$ die folgenden zwei Bedingungen erfüllt:

(1) Die Gleichheit $h(x_0, y_0) = 0$ gilt nicht nur modulo n, sondern auch über $\mathbb{Z}$. Die Bedingung ist nach der bivariaten Variante des Lemmas 2.14 (vgl [7, Lemma 1])

$$\|h(xX, yY)\| \leq \frac{n}{\sqrt{m}}.$$

(2) Das Polynom $h(x, y)$ ist kein Vielfaches von $p(x, y)$. Die Bedingung dafür ergibt sich aus Lemma 2.11 und lautet

$$\|h(xX, yY)\| < 2^{-\omega} \cdot (X^\gamma Y)^k W$$

mit $\omega = (d_x + \gamma k + 1)(d_y + k + 1)$. Diese Bedingung folgt aus der Anwendung von Lemma 2.11 mit $a(x, y) = p(xX, yY)$, $b(x, y) = h(xX, yY)$ und $r = (X^\gamma Y)^k$. Wenn die obige Bedingung erfüllt ist, ist $h(xX, yY)$ kein Vielfaches von $p(xX, yY)$. Daher ist auch $h(x, y)$ kein Vielfaches von $p(x, y)$.

Die erste Bedingung ist erfüllt, wenn die zweite Bedingung erfüllt ist. Denn es gilt

$$\frac{n}{\sqrt{m}} \overset{(3.2)}{\geq} \frac{\sqrt{m} \cdot 2^{-m} (X^\gamma Y)^k W}{\sqrt{m}} \geq 2^{-\omega} (X^\gamma Y)^k W,$$

da $\omega \geq m$ ist.

Wir möchten nun ein Polynom $h(x, y)$ finden, dass diese Bedingungen erfüllt. Dazu betrachten wir das Gitter L, welches durch die Koeffizientenvektoren der Polynome $\tilde{q}_{ij}(x, y)$ aufgespannt wird. Die Polynome haben m Koeffizienten und es gibt m dieser Polynome. Dies liefert ein volldimensionales Gitter mit Rang m, da die Polynome nach Konstruktion linear unabhängig sind.

	1	x	y	xy	x^2	x^2y	y^2	xy^2	x^2y^2
$\tilde{q}_{00}$	XY	$a_{10}X^2Y$	$a_{01}XY^2$	$a_{11}(XY)^2$					
$\tilde{q}_{10}$		XY		$a_{10}X^2Y$	$a_{01}XY^2$	$a_{11}(XY)^2$			
$\tilde{q}_{01}$			XY	$a_{10}X^2Y$			$a_{01}XY^2$	$a_{11}(XY)^2$	
$\tilde{q}_{11}$				XY		$a_{10}X^2Y$		$a_{01}XY^2$	$a_{11}(XY)^2$
$\tilde{q}_{20}$					X^2n				
$\tilde{q}_{21}$						X^2Yn			
$\tilde{q}_{02}$							Y^2n		
$\tilde{q}_{12}$								XY^2n	
$\tilde{q}_{22}$									X^2Y^2n

Abbildung 3.1: Beispiel eines Gitters L für $S := \left\{x^i y^j \mid 0 \le i \le k, 0 \le j \le k\right\}$ und $M := \left\{x^i y^j \mid 0 \le i \le k+\delta, 0 \le j \le k+\delta\right\}$ mit $\delta = 1$ und $k = 1$

Die Koeffizientenvektoren der Polynome $\tilde{q}_{ij}(x, y)$ lassen sich so anordnen, dass sie eine trianguläre Basis von L bilden. Ein Beispiel für eine trianguläre Gitterbasis finden wir in Abbildung 3.1. Die Determinate ist dann das Produkt der Diagonaleinträge. Die Shift-Polynome $\tilde{q}_{ij}(x, y)$ für $(i, j) \in S$ liefern jeweils als Diagonaleintrag $(X^\gamma Y)^k$. Dies ergibt insgesamt

$$\prod_{(i,j)\in S} (X^\gamma Y)^k = ((X^\gamma Y)^k)^s.$$

Die Hilfspolynome $\tilde{q}_{ij}(x, y)$ für $(i, j) \in M \setminus S$ liefern

$$\prod_{(i,j)\in M\setminus S} X^i Y^j n = X^{s_x} Y^{s_y} n^{m-s}.$$

Also ist die Determinate von L gegeben durch

$$\det(L) = (X^\gamma Y)^{k\,s} X^{s_x} Y^{s_y} n^{m-s}.$$

Mit (3.2) folgt nun

$$\begin{aligned} \det(L) &< (X^\gamma Y)^{k\,s} X^{s_x} Y^{s_y} (2\,W (X^\gamma Y)^k)^{m-s} \\ &= 2^{m-s}\,(X^\gamma Y)^{k\,m}\, X^{s_x} Y^{s_y} W^{m-s}. \end{aligned} \tag{3.3}$$

Der LLL-Algorithmus berechnet in Zeit polynomiell in $(\log W, m)$ ein von 0 verschiedenes Polynom $h(x, y)$ mit der Eigenschaft:

$$\|h(xX, yY)\| \le 2^{\frac{m-1}{4}} \cdot \det(L)^{\frac{1}{m}}.$$

Somit sind die Bedingungen (1) und (2) erfüllt, wenn gilt

$$2^{\frac{m-1}{4}} \cdot \det(L)^{\frac{1}{m}} < 2^{-\omega} \cdot (X^\gamma Y)^k W.$$

Hieraus ergibt sich mit (3.3) die gesuchte Bedingung

$$X^{s_x} Y^{s_y} < 2^{-\frac{m\,(4\,\omega+m+3)-4\,s}{4}} W^s.$$

In diesem Fall gilt $h(x_0, y_0) = 0$ über $\mathbb{Z}$ und $h(x, y)$ ist kein Vielfaches von $p(x, y)$. Das Polynom $p(x, y)$ ist irreduzibel. Daher gilt laut Satz 2.15, dass die Resultante

$$Q(x) = \mathrm{res}_y(h(x, y), p(x, y))$$

ein von 0 verschiedenes Polynom mit $Q(x_0) = 0$ ist. Mit Standard-Algorithmen zur Nullstellensuche kann dann x_0 gefunden werden und y_0 als Nullstelle von $p(x_0, y)$.

□

Betrachten wir nun Polynome vom Grad δ in jeder Variablen. Für Polynome dieser Form können wir in Abhängigkeit vom Grad δ und einem fest gewählten $\varepsilon > 0$ konkrete Schranken für die Nullstellen angeben, welche in Polynomialzeit berechnet werden können. Bei der Methode von Coppersmith hingegen hängen diese Schranken nur vom Grad δ des Polynoms ab. Dafür benötigt Coppersmith allerdings eine deutlich stärkere Bedingung in Hinblick auf die Monom-Mengen als die Bedingung, die wir benötigen. Hierauf werden wir im Kapitel 4 näher eingehen.

Satz 3.3
Es sei $p(x, y) \in \mathbb{Z}[x, y]$ ein irreduzibles bivariates ganzzahliges Polynom mit maximalem Grad δ in jeder Variablen. Ferner seien X und Y obere Schranken für die gesuchten, ganzzahligen Nullstellen (x_0, y_0) und $W = \|p(xX, yY)\|_\infty$. Falls

$$XY < 2^{-\frac{1}{\delta\,\varepsilon^2}} - \mathcal{O}\left(\tfrac{1}{\varepsilon}\right) W^{\frac{2}{3\,\delta}} - \varepsilon$$

für ein $\varepsilon \in (0, \frac{1}{\delta})$ gilt, können alle Paare $(x_0, y_0) \in \mathbb{Z}^2$, die

$$p(x_0, y_0) = 0 \text{ mit } |x_0| \leq X, |y_0| \leq Y$$

erfüllen, in Zeit polynomiell in $(\log W, \delta)$ gefunden werden.

Beweis: Diese Schranke lässt sich aus Satz 3.2 herleiten, indem wir konkrete Monom-Mengen S und M betrachten. Da das Newton-Polygon $N(p)$ des Polynoms $p(x, y) = \sum_{i=0}^{\delta} \sum_{j=0}^{\delta} p_{ij} x^i y^j$ Rechteckform hat, wählen wir

$$S := \left\{ x^i y^j \mid 0 \leq i \leq k, 0 \leq j \leq k \right\}$$

und

$$M := \left\{ x^i y^j \mid 0 \leq i \leq k + \delta, 0 \leq j \leq k + \delta \right\}.$$

Der Parameter $k \in \mathbb{N}$ wird in Abhängigkeit von ε später passend gewählt. Für diese Mengen S und M gilt offensichtlich, dass für alle $\mu \in S$ das Polynom $\mu \cdot p(x, y)$ über

M definiert ist. Somit können wir Satz 3.2 anwenden und erhalten für s, m, s_x, s_y und ω die folgenden Formeln:

$$\begin{aligned} s &= |S| = (k+1)^2, \\ m &= |M| = (k+\delta+1)^2 \\ &= \omega \end{aligned}$$

und

$$\begin{aligned} s_x &= \sum_{i \in M \setminus S} i \\ &= \frac{(\delta+k)(\delta+k+1)^2}{2} - \frac{k\,(k+1)^2}{2} \\ &= s_y = \sum_{j \in M \setminus S} j. \end{aligned}$$

Damit erhalten wir aus (3.1) die Bedingung

$$(XY)^{\frac{(\delta+k)(\delta+k+1)^2}{2} - \frac{k\,(k+1)^2}{2}} < 2^{-\frac{5\,m^2+3\,m-4\,s}{4}} W^{(k+1)^2}.$$

Daraus folgt

$$XY < 2^{-\beta} W^{\alpha}, \tag{3.4}$$

wobei

$$\begin{aligned} \alpha &= \frac{2\,(k+1)^2}{(\delta+k)(\delta+k+1)^2 - k\,(k+1)^2} \\ &\geq \frac{2}{3\,\delta} - \frac{2\,\delta+6\,k+4}{3\,(\delta^2+3\,\delta\,k+2\,\delta+3\,k^2+4\,k+1)} \\ &\geq \frac{2}{3\,\delta} - \frac{2\,(\delta+3\,k+2)}{3\,(k+1)(3\,k+3\,\delta+1)} \\ &\geq \frac{2}{3\,\delta} - \frac{2}{3\,(k+1)} \end{aligned} \tag{3.5}$$

und

$$\begin{aligned} \beta &= \frac{10\,(k+\delta+1)^4 + 6\,(k+\delta+1)^2 - 8\,(k+1)^2}{4\,((\delta+k)(\delta+k+1)^2 - k\,(k+1)^2)} \\ &\leq \frac{k^2}{\delta} + \frac{27\,\delta k^3 + (28\,\delta^2+35+54\,\delta)\,k^2 + (20\,\delta^3+66\,\delta+34+60\,\delta^2)\,k}{2\,\delta\,(3\,k^2+3\,k\,\delta+4\,k+\delta^2+2\,\delta+1)} \\ &\quad + \frac{12+33\,\delta^2+26\,\delta+5\,\delta^4+20\,\delta^3}{2\,\delta\,(3\,k^2+3\,k\,\delta+4\,k+\delta^2+2\,\delta+1)} \\ &\overset{(*)}{\leq} \frac{k^2}{\delta} + \mathcal{O}\,(k) \end{aligned} \tag{3.6}$$

gilt.

$(*)$ An dieser Stelle geht bereits ein, dass wir später $k = \lfloor 1/\varepsilon \rfloor$ wählen. Da $\varepsilon < \frac{1}{\delta}$ gilt, folgt somit auch $\delta < k$.

Wir wählen nun $k = \lfloor 1/\varepsilon \rfloor$, wobei $\varepsilon \in (0, 1/\delta)$ gilt, und erhalten mit (3.4),(3.5) und (3.6) die folgende Bedingung für X und Y:

$$\begin{aligned} 2^{-\beta} W^{\alpha} &\geq 2^{-\left(\lfloor \frac{k^2}{\delta} + \mathcal{O}(k) \right]} W^{\frac{2}{3\delta} - \frac{2}{3(k+1)}} \\ &\geq 2^{-\left[\frac{1}{\delta \varepsilon^2} + \mathcal{O}\left(\frac{1}{\varepsilon}\right)\right]} W^{\frac{2}{3\delta} - \varepsilon} \\ &> XY. \end{aligned}$$

Für X und Y, welche der obigen Bedingung genügen, können wir laut Satz 3.2 die Nullstellen (x_0, y_0) von $p(x, y)$ mit $|x_0| \leq X$ und $|y_0| \leq Y$ in Laufzeit polynomiell in $(\log W, m)$ bestimmen. Für ein festes $\varepsilon > 0$ kann m als Polynom in δ aufgefasst werden. Somit hat der Algorithmus für ein festes $\varepsilon > 0$ eine Laufzeit, die polynomiell in $(\log W, \delta)$ ist. □

3.2 Der trivariate ganzzahlige Fall

Nun möchten wir die Methode von Coron auf den trivariaten Fall übertragen. Dabei wird die Methode allerdings heuristisch. Denn wir können nicht gewährleisten, dass alle Polynome, welche wir durch Gitterreduktion erhalten, teilerfremd zueinander sind. Das bedeutet, dass wir nicht sicherstellen können, dass alle im Beweis auftretenden Resultanten vom Nullpolynom verschieden sind. Im Folgenden wird daher angenommen, dass alle auftretenden Resultanten von 0 verschieden sind.

Unter dieser Annahme kann nun der zentrale Satz dieser Arbeit formuliert und bewiesen werden. Dieser Satz gibt für trivariate ganzzahlige Polynome eine allgemeine obere Schranke für die Nullstellen an, welche in Polynomialzeit bestimmt werden können. Der Beweis gleicht im Wesentlichen dem Beweis der bivariaten Variante dieses Satzes (Satz 3.2).

Analog zum bivariaten Fall wird die Menge S als Shift-Menge bezeichnet und die Monom-Mengen S und M werden mit Mengen im Euklidischen Raum $\mathbb{R}^3$ identifiziert. Es sei S eine Menge von Monomen in x, y und z. Dann betrachten wir analog zum bivariaten Fall die konvexe Hülle $\operatorname{conv}\left(\left\{(i, j, k) \in \mathbb{N}^3 \mid x^i y^j z^k \in S\right\}\right) \subset \mathbb{R}^3$. Diese Menge wird ebenfalls mit S bezeichnet.

Satz 3.4 (Coron, trivariater Fall)
Es sei $p(x, y, z)$ ein irreduzibles trivariates ganzzahliges Polynom vom Grad d_x, d_y und $d_z \geq 1$ in den Variablen x, y und z. Ferner seien $X, Y, Z \in \mathbb{N}$ und $W = \|p(xX, yY, zZ)\|_\infty$. Es seien S und M, $S \subset M$, Mengen für die gilt: Für jedes Monom $\mu \in S$ ist $\mu \cdot p(x, y, z)$ definiert über M. Wir setzen

$$s := |S|, \qquad m := |M|$$

$$s_x = \sum_{x^i y^j z^k \in M \setminus S} i, \quad s_y = \sum_{x^i y^j z^k \in M \setminus S} j, \quad s_z = \sum_{x^i y^j z^k \in M \setminus S} k.$$

Weiter seien ℓ, τ, γ *und* ω *derart, dass*

- $\ell = \max\{i \mid x^i y^j z^k \in S\}$,
- $\tau\ell = \max\{j \mid x^i y^j z^k \in S\}$,
- $\gamma\ell = \max\{k \mid x^i y^j z^k \in S\}$ *und*
- $\omega = (d_x + \ell + 1)(d_y + \tau\ell + 1)(d_z + \gamma\ell + 1)$

gilt. Dann können alle Tripel $(x_0, y_0, z_0) \in \mathbb{Z}^3$, *welche*

$$p(x_0, y_0, z_0) = 0 \quad \textit{mit } |x_0| \leq X, |y_0| \leq Y, |z_0| \leq Z$$

erfüllen, in Laufzeit polynomiell in $(\log W, m)$ *gefunden werden unter der Voraussetzung, dass*

$$X^{s_x+\ell} Y^{s_y+\tau\ell} Z^{s_z+\gamma\ell} < 2^{-\frac{m(4\omega+m+3)}{4}} W^{s-1} \tag{3.7}$$

gilt.

Beweis: Es sei (x_0, y_0, z_0) eine ganzzahlige Nullstelle von $p(x, y, z)$. Wir setzen

- $W = \|p(xX, yY, zZ)\|_\infty$,
- $\ell = \max\{i, x^i y^j z^k \in S\}$,
- $\tau\ell = \max\{j, x^i y^j z^k \in S\}$, wobei $\tau > 0$ ist, und
- $\gamma\ell = \max\{k, x^i y^j z^k \in S\}$, wobei $\gamma > 0$ ist.

Es wird angenommen, dass $p_{000} \neq 0$ und $\mathrm{ggT}(p_{000}, (XY^\tau Z^\gamma)^\ell) = 1$ gilt.

Im Fall $p_{000} = 0$ erhalten wir durch den im Anhang A.2 erläuterten Variablenwechsel ein Polynom $p^*(x, y, z)$ mit $p^*_{000} \neq 0$.

Gilt $\mathrm{ggT}(p_{000}, (XY^\tau Z^\gamma)^\ell) > 1$, so wählen wir Primzahlen X', Y' und Z' mit $X < X' < 2X$, $Y < Y' < 2Y$ und $Z < Z' < 2Z$, sodass $\mathrm{ggT}(p_{000}, (X'Y'^\tau Z'^\gamma)^\ell) = 1$ ist. Wir ersetzen dann im Folgenden X, Y und Z durch X', Y' und Z'.

Wir setzen

$$u = W + ((1 - W) \mod |p_{000}|).$$

Es ist leicht nachzurechnen, dass

$$\sqrt{m} \cdot 2^{-m} W \leq u < 2 \cdot W$$

und $\mathrm{ggT}(p_{000}, u) = 1$ gilt. Nun setzen wir $n = u \cdot (XY^\tau Z^\gamma)^\ell$. Dann gilt $\mathrm{ggT}(p_{000}, n) = 1$ und

$$\sqrt{m} \cdot 2^{-m} (XY^\tau Z^\gamma)^\ell W \leq n < 2(XY^\tau Z^\gamma)^\ell W. \tag{3.8}$$

Gesucht sind zwei Polynome $h_1(x, y, z)$ und $h_2(x, y, z)$ mit $h_1(x_0, y_0, z_0) = 0$ und $h_2(x_0, y_0, z_0) = 0$ und der Eigenschaft, dass $h_1(x, y, z)$ und $h_2(x, y, z)$ keine Vielfachen von $p(x, y, z)$ sind. Dann betrachten wir die Resultanten bezüglich z von $p(x, y, z)$ und

$h_1(x,y,z)$ beziehungsweise $p(x,y,z)$ und $h_2(x,y,z)$. Diese Resultanten sind Polynome in x und y und eine gemeinsame Nullstelle von ihnen ist (x_0,y_0). Um eine weitere Variable zu eliminieren, berechnen wir die Resultante bezüglich y der vorhergehenden beiden Resultanten. Davon ausgehend, dass diese Resultante von 0 verschieden ist, erhalten wir ein Polynom in einer Variablen x, welches x_0 als Nullstellen besitzt. So können wir nun sukzessiv x_0, y_0 und z_0 als Nullstelle eines univariaten Polynoms berechnen.

Um diese Polynome $h_1(x,y,z)$ und $h_2(x,y,z)$ zu erhalten, betrachten wir wie im Beweis des Satzes 3.2 ein Gitter L aufgespannt von den Koeffizientenvektoren von Polynomen $q_{ij}(xX,yY,zZ)$, für die $q_{ij}(x_0,y_0,z_0) \equiv 0 \mod n$ gilt. Wir wählen dann $h_1(xX,yY,zZ)$ und $h_2(xX,yY,zZ)$ mit dem LLL-Algorithmus als kurze Vektoren dieses Gitters. Da $h_i(x,y,z) = 0$ über $\mathbb{Z}$ gelten muss und $h_i(x,y,z)$ kein Vielfaches von $p(x,y,z)$ sein soll, $i = 1,2$, ergeben sich Bedingungen für die Größe der Koeffizienten und somit Schranken für die Größe der Nullstellen (x_0,y_0,z_0), die in Polynomialzeit gefunden werden können.

Zunächst definieren wir das folgende Gitter:
Es sei $q(x,y,z)$ definiert als das Polynom

$$q(x,y,z) = p_{000}^{-1} \cdot p(x,y,z) \mod n.$$

Für alle $(i,j,k) \in S$ definieren wir die folgenden Shift-Polynome

$$q_{ijk}(x,y,z) = x^i y^j z^k X^{\ell-i} Y^{\tau\ell-j} Z^{\gamma\ell-k} q(x,y,z)$$

und für alle $(i,j,k) \in M \setminus S$ definieren wir die Hilfspolynome

$$q_{ijk}(x,y,z) = x^i y^j z^k n.$$

Für alle $(i,j,k) \in M$ gilt, dass $q_{ijk}(x_0,y_0,z_0) \equiv 0 \mod n$ ist. Wir betrachten nun für alle Polynome $q_{ijk}(x,y,z)$ die zugehörigen Polynome $\tilde{q}_{ijk}(x,y,z) = q_{ijk}(xX,yY,zZ)$. Dann sind die Polynome $\tilde{q}_{ijk}(x,y,z)$ durch $(XY^\tau Z^\gamma)^\ell$ teilbar.

Es seien $h_1(x,y,z)$ und $h_2(x,y,z)$ ganzzahlige Linearkombinationen der Polynome $q_{ijk}(x,y,z)$, dann sind $\tilde{h}_1(x,y,z) = h_1(xX,yY,zZ)$ und $\tilde{h}_2(x,y,z) = h_2(xX,yY,zZ)$ Linearkombinationen der Polynome $\tilde{q}_{ijk}(x,y,z)$ mit den gleichen ganzzahligen Koeffizienten. Es gilt $h_1(x_0,y_0,z_0) \equiv 0 \mod n$ und $h_2(x_0,y_0,z_0) \equiv 0 \mod n$ und $h_1(x,y,z)$ und $h_2(x,y,z)$ sind jeweils die Summen von höchstens m Monomen. Weiterhin sind $h_1(x,y,z)$ und $h_2(x,y,z)$ höchstens vom Grad $d_x + \ell$ in x, $d_y + \tau\ell$ in y und $d_z + \gamma\ell$ in z. Gesucht sind zwei Polynome $h_1(x,y,z)$ und $h_2(x,y,z)$ mit genügend kleinen Koeffizienten, sodass die folgenden Bedingungen gelten:

(1) Die Gleichheit $h_1(x_0,y_0,z_0) = 0$ beziehungsweise $h_2(x_0,y_0,z_0) = 0$ gilt nicht nur modulo n, sondern auch über $\mathbb{Z}$. Die Bedingungen dafür sind laut Lemma 2.14:

$$\|h_1(xX,yY,zZ)\| \leq \frac{n}{\sqrt{m}}$$

und

$$\|h_2(xX,yY,zZ)\| \leq \frac{n}{\sqrt{m}}.$$

(2) Die Polynome $h_1(xX, yY, zZ)$ und $h_2(xX, yY, zZ)$ sind keine Vielfachen von $p(x, y, z)$. Um dies zu erzielen, müssen laut Lemma 2.13 die folgenden Bedingungen erfüllt sein:

$$\|h_1(xX, yY, zZ)\| < 2^{-\omega}(XY^\tau Z^\gamma)^\ell W$$

und

$$\|h_2(xX, yY, zZ)\| < 2^{-\omega}(XY^\tau Z^\gamma)^\ell W.$$

Dabei ist $\omega = (d_x + \ell + 1)(d_y + \tau\ell + 1)(d_z + \gamma\ell + 1)$. Wenn diese Bedingungen erfüllt sind, können $h_1(xX, yY, zZ)$ und $h_2(xX, yY, zZ)$ keine Vielfachen von $p(xX, yY, zZ)$ sein und somit sind auch $h_1(x, y, z)$ und $h_2(x, y, z)$ keine Vielfachen von $p(x, y, z)$.

Es genügt die zweite Bedingung zu betrachten. Wegen

$$\frac{n}{\sqrt{m}} \overset{(3.8)}{\geq} \frac{\sqrt{m}2^{-m}(XY^\tau Z^\gamma)^\ell W}{\sqrt{m}} = 2^{-m}(XY^\tau Z^\gamma)^\ell W \geq 2^{-\omega}(XY^\tau Z^\gamma)^\ell W$$

ist Bedingung (1) bereits erfüllt, wenn die zweite Bedingung erfüllt ist. Hierbei müssen wir beachten, dass $\omega \geq m$ gilt.

Um zwei Polynome zu finden, die diese Bedingungen erfüllen, verwenden wir nun den LLL-Algorithmus. Es sei L das Gitter, das durch die Koeffizientenvektoren der Polynome $\tilde{q}_{ijk}(x, y, z)$ aufgespannt wird. Die Polynome haben m Koeffizienten und es gibt m solcher Polynome. Somit liefern die Koeffizientenvektor der Polynom $q_{ijk}(x, y, z)$ ein volles Gitter der Dimension m über $\mathbb{Z}$, da die Polynome nach Konstruktion linear unabhängig sind.

Die Koeffizientenvektoren der Polynome $\tilde{q}_{ijk}(x, y, z)$ lassen sich so anordnen, dass sie eine trianguläre Basis von L bilden. Dann ist die Determinante das Produkt der Diagonaleinträge. Die Polynome $\tilde{q}_{ijk}(x, y, z)$ liefern für $(i, j, k) \in S$ jeweils den Diagonaleintrag $(XY^\tau Z^\gamma)^l$. Damit tragen die Polynome $\tilde{q}_{ijk}(x, y, z)$ für $(i, j, k) \in S$ insgesamt

$$\prod_{(i,j,k)\in S} (XY^\tau Z^\gamma)^\ell = (XY^\tau Z^\gamma)^{\ell s}$$

zur Determinante bei und die Hilfspolynome $\tilde{q}_{ijk}(x, y, z)$ für $(i, j, k) \in M \setminus S$ liefern

$$\prod_{(i,j,k)\in M\setminus S} X^i Y^j Z^k n = X^{s_x} Y^{s_y} Z^{s_z} n^{m-s}.$$

Somit ist die Determinante von L gegeben durch

$$\det(L) = (XY^\tau Z^\gamma)^{\ell s} X^{s_x} Y^{s_y} Z^{s_z} n^{m-s}. \tag{3.9}$$

Der LLL-Algorithmus berechnet laut Lemma 2.8 in Zeit polynomiell in $(\log W, m)$ zwei von 0 verschiedene Polynome $h_1(x, y, z)$ und $h_2(x, y, z)$, sodass gilt

$$\|\tilde{h}_1(x, y, z)\| \leq \|\tilde{h}_2(x, y, z)\| \leq 2^{\frac{m}{4}} \det(L)^{\frac{1}{m-1}}.$$

Somit sind die Bedingungen (1) und (2) erfüllt, wenn

$$2^{\frac{m}{4}} \det(L)^{\frac{1}{m-1}} \quad < \quad 2^{-\omega}(XY^{\tau}Z^{\gamma})^{\ell}W \tag{3.10}$$

gilt. Mit $n \leq 2 \cdot (XY^{\tau}Z^{\gamma})^{l} \cdot W$ und (3.9) erhalten wir die Schranke

$$X^{s_x}Y^{s_y}Z^{s_z}(XY^{\tau}Z^{\gamma})^{l} < 2^{-\frac{m\,(4\,\omega+m+3)}{4}}W^{s-1}.$$

In diesem Fall gilt $h_1(x_0, y_0, z_0) = 0$ und $h_2(x_0, y_0, z_0) = 0$. Außerdem sind $h_1(x, y, z)$ und $h_2(x, y, z)$ keine Vielfachen von $p(x, y, z)$. Da $p(x, y, z)$ irreduzibel ist, sind somit laut Satz 2.15 die Resultanten

$$Q_1(x, y) = \mathrm{res}_z(h_1(x, y, z), p(x, y, z))$$

und

$$Q_2(x, y) = \mathrm{res}_z(h_2(x, y, z), p(x, y, z))$$

von 0 verschiedene Polynome mit $Q_1(x_0, y_0) = 0$ und $Q_2(x_0, y_0) = 0$. Die Polynome $h_1(x, y, z)$ und $h_2(x, y, z)$ sind nicht zwangsweise teilerfremd. Daher kann der Fall auftreten, dass die Resultante $Q(x) = \mathrm{res}_y(Q_1(x, y), Q_2(x, y))$ das Nullpolynom ist. Dies macht die Methode heuristisch. Unter der Annahme, dass $Q(x)$ von 0 verschieden ist, gilt, dass x_0 ein Nullstelle des univariaten Polynoms $Q(x)$ ist und mit Standardalgorithmen zur Nullstellensuche gefunden werden kann. Ebenso kann dann y_0 als Nullstelle von $Q_1(x_0, y)$ beziehungsweise $Q_2(x_0, y)$ und z_0 als Nullstelle von $p(x_0, y_0, z)$ gefunden werden. □

4 Konstruktion der Mengen S und M

Im Kapitel 3 haben wir die Sätze von Coron für den bivariaten Fall (Satz 3.2) und den trivariaten Fall (Satz 3.4) in Abhängigkeit der Monom-Mengen S und M formuliert. Die Mengen S und M müssen dabei die folgenden Eigenschaft haben:

E.1 *Für jedes Monom $\mu \in S$ ist $\mu \cdot p(x_1, \ldots, x_n)$ definiert über M.*

Für Polynome mit beliebigen Formen der Newton-Polytope erlaubt uns diese Formulierung eine genauere Analyse der Schranke im Vergleich zum allgemeinen Fall, bei dem uns die Form des Newton-Polytops nicht bekannt ist. Es genügt, die Mengen S und M zu betrachten, die für das zu untersuchende Polynom die obige Eigenschaft E.1 erfüllen. Die Güte der Schranken hängt dabei stark von der Konstruktion dieser Mengen ab. Daher werden wir eine Möglichkeit der Konstruktion der Mengen S und M für das Polynom p betrachten:

Die bivariate und die trivariate Variante des Satzes von Coron liefern uns im Wesentlichen eine Bedingung der Art:

$$X^{s_x} Y^{s_y} Z^{s_z} < W^s, \tag{4.1}$$

wobei $s = |S|$ sowie

$$s_x = \sum_{x^i y^j z^k \in M \setminus S} i, \quad s_y = \sum_{x^i y^j z^k \in M \setminus S} j \quad \text{und} \quad s_z = \sum_{x^i y^j z^k \in M \setminus S} k$$

gilt.

Da wir möglichst große Schranken X, Y beziehungsweise X, Y und Z für die Nullstellen erhalten wollen, sollte s möglichst groß werden und die Exponenten s_x, s_y beziehungsweise s_x, s_y und s_z sollten verhältnismäßig klein bleiben.

Um dies zu erreichen, müssen wir zunächst einmal sicherstellen, dass die Menge M nicht "zu groß" wird im Vergleich zur Menge S. Denn die Größe der Exponenten $s_x,\ s_y$ beziehungsweise $s_x,\ s_y$ und s_z hängt hauptsächlich von der Größe der Menge $M \setminus S$ ab. Ist M also nicht wesentlich größer als S, so bleiben die Exponenten verhältnismäßig klein. Die Eigenschaft, dass die Menge M nicht "zu groß" wird, erzielen wir, indem wir zulässige Mengen betrachten.

Definition 4.1
Es sei $p(x_1, \ldots, x_n)$ ein ganzzahliges Polynom in n Variablen und S und M seien endliche nichtleere Mengen von Monomen in den Variablen $x_1, \ldots, x_n$. Das Paar (S, M) heißt zulässig für $p(x_1, \ldots, x_n)$ genau dann, wenn die folgenden beiden Bedingungen gelten:

- *Für jedes Monom $\mu \in S$ ist das Polynom $\mu \cdot p(x_1, \ldots, x_n)$ über M definiert.*
- *Für jedes Polynom g über M mit $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)p(x_1, \ldots, x_n)$ für ein Polynom f, ist f über S definiert.*

Die erste Eigenschaft, welche zulässige Mengen erfüllen, ist die Eigenschaft E.1. Das heißt, es handelt sich um die Eigenschaft, die die Mengen S und M in den Sätzen von Coron (Satz 3.2, Satz 3.4) für das Polynom p erfüllen müssen. Sie stellt sicher, dass die Menge M genügend groß gewählt wird, sodass alle Polynome des Gitters über M definiert sind.

Die zweite Eigenschaft sorgt dafür, dass die Menge M nicht zu groß wird. Sie wird eben nur so groß gewählt, dass die erste Eigenschaft erfüllt ist. Dazu benötigen wir die Minkowski-Summe.

Die *Minkowski-Summe* $A + B$ zweier Mengen $A, B \subseteq \mathbb{R}^n$ ist definiert als

$$A + B := \{(a_1, \ldots, a_n) + (b_1, \ldots, b_n) \mid (a_1, \ldots, a_n) \in A, (b_1, \ldots, b_n) \in B\}.$$

Wir wählen die Menge M als Minkowski-Summe der Shift-Menge S und des Newton-Polytops $N(p)$ des Polynoms p. Dann erfüllen die Mengen S und $M{:=}S{+}N(p)$ offensichtlich für das Polynom p die oben geforderte Eigenschaft E.1. Außerdem ist M dann nach Konstruktion die kleinstmögliche Menge, welche für die Menge S und das Polynom p die Eigenschaft E.1 erfüllt.

Es bleibt die Frage zu klären, wie wir S konstruieren, um bestmögliche Schranken für die Lösungen zu erhalten. Dazu betrachten wir mehrere Mengen S, deren Form der Form des Newton-Polytops $N(p)$ gleicht. Die Menge S kann durch verschiedene Parameter beschrieben werden. Auf der Grundlage von (4.1) (beziehungsweise genauer (3.1) und (3.7)) wählen wir dann die optimalen Werte für die Parameter, sodass wir Mengen S und M erhalten, die die Bedingungen aus Satz 3.2 beziehungsweise Satz 3.4 erfüllen und möglichst große Schranken liefern.

4.1 Konstruktionen für den bivariaten Fall

Wir betrachten nun einige Beispiele für geometrische Formen, die das Newton-Polygon $N(p)$ eines bivariaten Polynoms p beschreiben.

Definition 4.2
Im Folgenden seien alle Parameter positive reelle Zahlen.

1. *Mengen der Form $R(a, b) := \{(i, j) \mid 0 \leq i \leq a, 0 \leq j \leq b\}$ heißen Rechtecke.*
2. *Mengen der Form $LD(c, a, \lambda) := \{(c + i, j) \mid 0 \leq i \leq a, 0 \leq j \leq \lambda(a - i)\}$ heißen linke untere Dreiecke.*
3. *Mengen der Form $RD(c, a, \lambda) := \{(i, c + j) \mid 0 \leq i \leq a, 0 \leq j \leq \lambda i\}$ heißen rechte untere Dreiecke.*

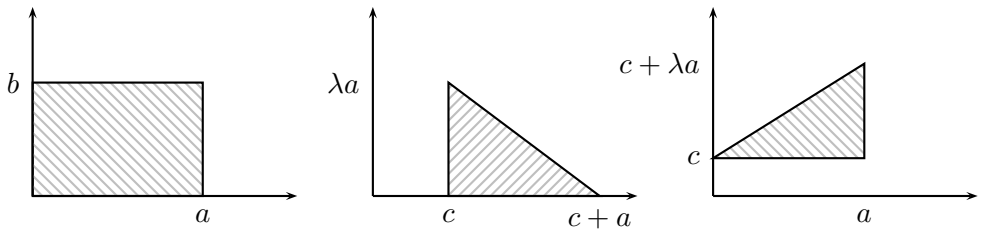

Abbildung 4.1: Rechteck, linkes und rechtes unteres Dreieck

Mit diesen Definitionen lassen sich nun wie in [1] Konstruktionen für die Mengen S und M angeben in Abhängigkeit von der Form des Newton-Polygons $N(p)$ des Polynoms $p(x, y)$.

Konstruktion 4.3 (Rechteckskonstruktion)
Das Polynom $p(x, y)$ habe Grad d in x und Grad λd in y. Dies bedeutet, dass das Newton-Polygon $N(p)$ des Polynoms $p(x, y)$ das Rechteck $R(d, \lambda d)$ mit $\lambda > 0$ ist. Dann wird die Menge S so gewählt, dass

$$x^i y^j \in S :\Leftrightarrow (i, j) \in R(\ell, \gamma\ell),$$

wobei $\ell \in \mathbb{N}$ und $\gamma > 0$ gilt. Da M als Minkowski-Summe von S und $N(p)$ gewählt wird, ist die Menge M folglich definiert durch

$$x^i y^j \in M :\Leftrightarrow (i, j) \in R(\ell + d, \gamma\ell + \lambda d).$$

Diese Konstruktion verwenden wir im Beweis des Ergebnisses von Coron (Satz 3.3) für Polynome vom Grad δ in jeder Variablen. Es kann gezeigt werden, dass für $\gamma = \sqrt{\lambda}$ maximale Schranken X und Y erzielt werden. Hierauf möchten wir aber in dieser Arbeit nicht näher eingehen.

Konstruktion 4.4 (Linke untere Dreieckskonstruktion)
Das Newton-Polygon $N(p)$ des Polynoms $p(x, y)$ sei das Dreieck $LD(0, d, \lambda)$ mit $\lambda > 0$. Dann wird die Menge S so gewählt, dass

$$x^i y^j \in S :\Leftrightarrow (i, j) \in LD(0, \ell, \lambda),$$

wobei $\ell \in \mathbb{N}$. Folglich ist die Menge M definiert durch

$$x^i y^j \in M :\Leftrightarrow (i, j) \in LD(0, \ell + d, \lambda).$$

Konstruktion 4.5 (Rechte untere Dreieckskonstruktion)
Das Newton-Polygon $N(p)$ des Polynoms $p(x,y)$ sei das Dreieck $RD(0,d,\lambda)$ mit $\lambda > 0$. Dann wird die Menge S so gewählt, dass

$$x^i y^j \in S :\Leftrightarrow (i,j) \in RD(c\ell, \ell, \lambda) \cup R(\ell, c\ell),$$

wobei $\ell \in \mathbb{N}$. Folglich ist die Menge M definiert durch

$$x^i y^j \in M :\Leftrightarrow (i,j) \in RD(c\ell, \ell + d, \lambda) \cup R(\ell + d, c\ell).$$

Für diese Konstruktionen der Mengen S und M können wir zeigen, dass sie für $p(x,y)$ zulässig sind. Dies werden wir zunächst für jede dieser hier angebenen Konstruktionen einzeln analog zum Beweis von Lemma 7 in [1] zeigen. Anschließend geben wir eine allgemeine Bedingung für $p(x,y)$, S und M an, sodass Mengen S und M, die diese Bedingung erfüllen, zulässig sind für $p(x,y)$.

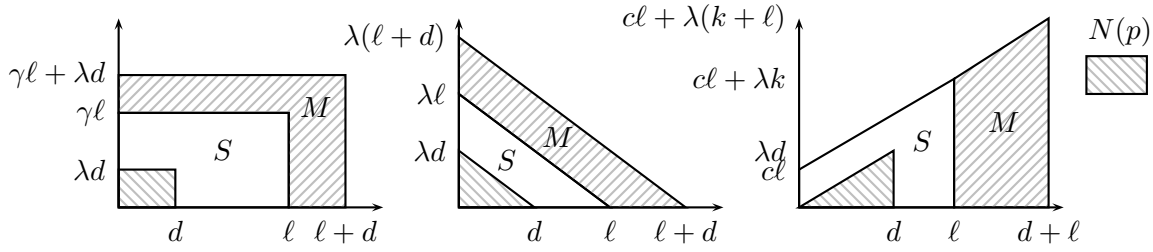

Abbildung 4.2: Rechteckkonstruktion, linke und rechte untere Dreieckskonstruktion

Lemma 4.6
Die Rechteck-, linke untere Dreiecks- und rechte untere Dreieckskonstruktion liefern zulässige Mengen S und M für die jeweiligen Polynome.

Beweis: Bei allen betrachteten Konstruktionen ist M als Minkowskisumme von $N(p)$ und S definiert. Somit erfüllen S und M für alle Konstruktionen die erste Bedingung der Definition 4.1.

Es bleibt zu zeigen, dass S und M auch die zweite Bedingung für zulässige Mengen erfüllen. Dazu betrachten wir jeweils ein Polynom $f(x,y) = \sum f_{ij} x^i y^j$, welches nicht über S definiert ist und zeigen, dass $f(x,y) \cdot p(x,y)$ dann nicht über M definiert ist.

> Rechteckskonstruktion:
> Wir bezeichnen mit l_x, l_y den Grad von $f(x,y)$ in x beziehungsweise y. Da $f(x,y)$ nicht über S definiert ist, gilt entweder $l_x > \ell$ oder $l_y > \gamma\ell$. Diese beiden Fälle sind symmetrisch. Wir betrachten daher nur den Fall $l_x > \ell$.

Es sei j_0 maximal über allen j mit $f_{l_x j} \neq 0$. Dann ist der Koeffizient von $x^{l_x+d}y^{j_0+\lambda d}$ in $p(x,y) \cdot f(x,y)$ von 0 verschieden. Da $l_x > \ell$ ist, erhalten wir $l_x + d > \ell + d$ und somit gilt $x^{l_x+d}y^{j_0+\lambda d} \notin M$. Also ist $f(x,y) \cdot p(x,y)$ nicht über M definiert.

Linke untere Dreieckskonstruktion:
Da $f(x,y)$ nicht über S definiert ist, gibt es mindestens ein Paar (i,j) mit $f_{ij} \neq 0$ und $\lambda i + j > \lambda \ell$.

Wir wählen unter allen Paaren (i,j), die $f_{ij} \neq 0$ und $\lambda i + j > \lambda \ell$ erfüllen, das bezüglich der lexikographischen Ordnung größte Paar (i_0, j_0) aus. Dann ist der Koeffizient von $x^{i_0+d}y^{j_0}$ in $p(x,y) \cdot f(x,y)$ von 0 verschieden. Da $\lambda i_0 + j_0 > \lambda k$ ist, ist $\lambda(i_0+d)+j_0 > \lambda k + \lambda d$ und somit ist $x^{i_0+d}y^{j_0} \notin M$. Folglich ist $p(x,y) \cdot f(x,y)$ nicht über M definiert.

Rechte untere Dreieckskonstruktion:
Da $f(x,y)$ nicht über S definiert ist, gilt $l_x > \ell$ oder $j > \lambda i + c\ell$. Der Beweis verläuft im ersten Fall analog zum Beweis der Rechteckform. Betrachten wir den Fall $j > \lambda i + c\ell$:

Wir wählen unter alle Paaren (i,j), für die gilt $j > \lambda i + c\ell$ und $f_{ij} \neq 0$, das bezüglich der lexikographischen Ordnung größte Paar (i_0, j_0) aus. Dann ist der Koeffizient von $x^{i_0+d}y^{j_0+d}$ von 0 verschieden. Da $j_0 > \lambda i_0 + c\ell$ ist auch $j_0 + d > i_0 + d + c\ell$, also ist $x^{i_0+d}y^{j_0+d} \notin M$. Folglich ist $p(x,y) \cdot f(x,y)$ nicht über M definiert.

Somit haben wir für alle Konstruktionen gezeigt, dass die Mengen S und M für das jeweilige Polynom $p(x,y)$ auch die zweite Bedingung erfüllen. Also sind die so konstruierten Mengen S und M zulässig für das jeweilige Polynom $p(x,y)$. □

Nun geben wir allgemein für eine größere Klasse von Polynomen eine Konstruktion für zulässige Mengen S und M an. Dazu benötigen wir den Begriff eines x-monotonen beziehungsweise y-monotonen Polynoms sowie den Begriff eines quasi-xy-monotonen Polynoms.

Definition 4.7
Ein Polynom $p(x,y)$ heißt y-monoton, wenn für $(i,j_0) \in N(p)$ gilt: $(i,j) \in N(p)$ für $0 \leq j \leq j_0$. Analog bezeichnen wir ein Polynom als x-monoton, wenn für $(i_0,j) \in N(p)$ gilt, dass $(i,j) \in N(p)$ für $0 \leq i \leq i_0$ ist.

Definition 4.8
Ein Polynom $p(x,y)$ heißt quasi-xy-monoton, wenn es

(i) ein y- und x-monotones Polynom ist oder

(ii) ein y-monotones Polynom ist, dessen Newton-Polygon dem Newton-Polygon eines x-monotonen Polynoms entspricht bis auf Spiegelung an der y-Achse und Verschiebung in den 1. Quadranten. (vgl. Abbildung 4.3)

Mit diesen Definition wollen wir nun für quasi-xy-monotone Polynome, deren konstanter Term ungleich 0 ist, ein Konstruktion für zulässige Mengen S und M angeben.

Es ist leicht nachzuprüfen, ob ein Polynom y-monoton und x-monoton ist, beziehungsweise ob das Newton-Polygon eines y-monotonen Polynoms nach Spiegelung an der y-Achse und Verschiebung in der 1. Quadranten die Eigenschaften des Newton-Polygons eines x-monotonen Polynoms erfüllt. Polynome, deren Newton-Polygon ein Rechteck oder ein linkes unteres Dreieck ist, sind sowohl x- als auch y-monoton. Polynome, der Newton-Polygon ein rechtes unteres Dreieck ist, sind hingegen nur y-monoton, aber ihr Newton-Polygon lässt sich durch Spiegelung und Verschiebung in ein Newton-Polygon eines x-monotonen Polynoms überführen. Wir bemerken dabei, dass durch die Spiegelung an der y-Achse und die Verschiebung in den 1. Quadranten, die Eigenschaft, der y-Monotonie nicht verloren geht.

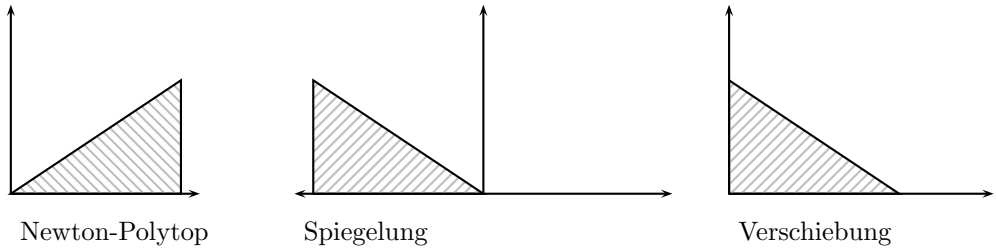

Abbildung 4.3: Newton-Polynom eines quasi-xy-monotones Polynoms

Für eine solche Klasse von Polynomen gibt uns das nachfolgende Lemma eine sehr einfach Konstruktion für zulässige Mengen S und M an.

Lemma 4.9
Es sei $p(x, y)$ ein quasi-xy-monotones Polynom. Weiterhin sei $(0, 0) \in N(p)$. Die Menge S sei die Menge der Shiftmonome und M wird definiert als Minkowski-Summe von S und $N(p)$. Wenn wir S als geometrisches Objekt in der Euklidischen Ebene auffassen, ist der Rand von S parallel zum Rand des Newton-Polygons $N(p)$. Dann sind die Mengen S und M zulässig für $p(x, y)$ und $S \subset M$ gilt.

Wir verallgemeinern hier das Prinzip unserer vorherigen Zulässigkeitsbeweise. Die Vorgehensweise des Beweises wird in Abbildung 4.4 erläutert.

Beweis: Die erste Bedingung für zulässige Mengen ist erfüllt, da die Menge M als Minkowski-Summe von S und $N(p)$ definiert ist.

Um zu zeigen, dass die Menge S und M auch die zweite Bedingung für zulässige Mengen erfüllen, betrachten wir ein Polynom $f(x, y) = \sum f_{ij} x^i y^j$, welches nicht über S definiert ist. Wir zeigen, dass dann $p(x, y) \cdot f(x, y)$ nicht über M definiert ist.

Wir wählen das bezüglich der lexikographischen Ordnung größte Paar (i_0, j_0) unter allen Paaren (i, j), für die $x^i y^j \notin S$ und $f_{ij} \neq 0$ gilt. Weiterhin sei (i_p, j_p) das bezüglich der lexikographischen Ordnung größte Paar in $N(p)$.

Dann ist der Koeffizient von $x^{i_0+i_p} y^{j_0+j_p}$ des Polynoms $p(x, y) \cdot f(x, y)$ von 0 verschieden. Denn es gibt keine weiteres Monom in f, welches multipiliziert mit einen Monom aus p das Monom $x^{i_0+i_p} y^{j_0+j_p}$ ergibt. Dies folgt aus der Parallelität des Randes der Menge S und des Randes des Newton-Polygons $N(p)$ sowie aus der quasi-xy-Monotonie des Polynoms $p(x, y)$. Somit tritt der Fall der Annihilation des Koeffizienten von $x^{i_0+i_p} y^{j_0+j_p}$ im Polynom $f(x, y) \cdot p(x, y)$ nicht ein.

Wir wollen nun zeigen, dass $x^{i_0+i_p} y^{j_0+j_p} \notin M$ gilt, da $x^{i_0} y^{j_0} \notin S$ ist. Im Fall, dass das Polynom $p(x, y)$ bereits x- und y-monoton ist, ist offensichtlich, dass $x^{i_0+i_p} y^{j_0+j_p} \notin M$ ist. Denn der Abstand des Punktes (i_0, j_0) zur Menge S, wobei wir S als geometrisches Objekt in der Euklidischen Ebene auffassen, ist gleich dem Abstand des Punktes (i_0+i_p, j_0+j_p) zur Menge M. Dies ergibt sich aus der Parallelität des Randes der Menge S und M sowie des Randes des Newton-Polygons $N(p)$ und der Wahl von (i_p, j_p). Dies ist im zweiten Teil der Abbildung 4.4 illustiert.

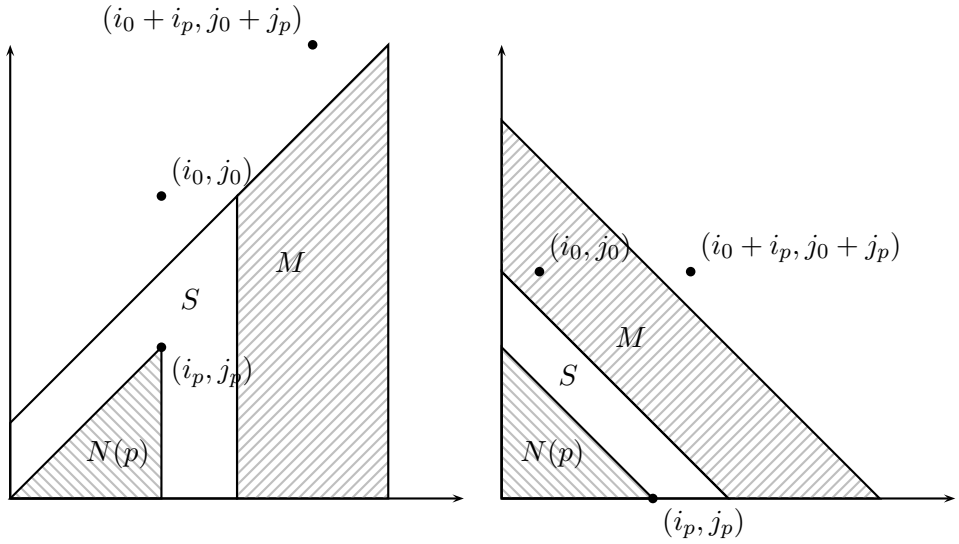

Abbildung 4.4: Illustration der Vorgehensweise im Beweis des Lemmas 4.9

Betrachten wir den Fall, dass das Polynom $p(x, y)$ quasi-xy-monoton mit den Eigenschaften (ii) der Definition 4.8 ist. Dann stellt diese Bedingung (ii) sicher, dass (i_p, j_p) genügend groß ist, sodass $x^{i_0+i_p} y^{j_0+j_p} \notin M$ gilt. Die Bedingung (ii) gewährleistet, dass wir ebenso wie im ersten Fall den gleichen Abstand zwischen (i_0, j_0) und S sowie zwischen $(i_0 + i_p, j_0 + j_p)$ und M erhalten. Dies ist im ersten Teil der Abbildung 4.4 illustiert.

Somit ist $p(x, y) \cdot f(x, y)$ nicht über M definiert.

Aus der Definition von M und aus $(0, 0) \in N(p)$ folgt, dass $S \subset M$ gilt. □

4.2 Konstruktionen für den bivariaten modularen Fall

Das Ziel dieser Arbeit ist, den bivariaten modularen Fall als Spezialfall des trivariaten ganzzahligen Falls darzustellen. Daher befassen wir uns im Rest dieses Abschnitts ausschließlich mit diesen Fällen. Wir betrachten $f(y,z) \equiv 0$ modulo einer zusammengesetzten ganzen Zahl N als trivariaten ganzzahligen Fall $p(x,y,z) := f_N(y,z) - Nx = 0$, wobei $f_N(y,z) := f(y,z) \mod N$ ist. Offensichtlich ist, dass die Form des Newton-Polytops $N(p)$ von $p(x,y,z)$ im wesentlichen von der Form des Newton-Polygons $N(f)$ von $f(y,z)$ abhängt. Dabei gehen wir davon aus, dass N die Koeffizienten von $f(y,z)$ nicht teilt.

Wir betrachten Mengen S und M, von denen gezeigt werden kann, dass sie zulässig für $p(x,y,z)$ sind. Die Konstruktion dieser Mengen hängt dabei von der jeweiligen Form des Newton-Polygons des bivariaten Polynoms $f(y,z)$ ab. In den Zulässigkeitsbeweise betrachten wir stets ein Polynom g, welches nicht über S definiert ist, und zeigen, dass dann $g(x,y,z) \cdot p(x,y,z)$ nicht über M definiert ist. Dies beweist, dass die Mengen S und M die zweite Zulässigkeitsbedingung für $p(x,y,z)$ erfüllen. Die erste Bedingung ergibt sich aus der Definition der Menge M als Minkowski-Summe von S und $N(p)$.

Konstruktion 4.10 (Modulare Reckteckform)
Angenommen das Newton-Polygon $N(f)$ des Polynoms $f(y,z)$ ist das Rechteck $R(\delta, \lambda\delta)$ mit $\lambda > 0$. Dann ist das Newton-Polytop $N(p)$ von $p(x,y,z) = f_N(y,z) - Nx$, wobei $f_N(y,z) := f(y,z) \mod N$ ist, von der Form

$$N(p) := \operatorname{conv}\left\{(i,j,k) \in \mathbb{N}^3 \mid 0 \le i \le 1, 0 \le j \le \delta(1-i), 0 \le k \le \lambda\delta(1-i)\right\}.$$

Dann definieren wir die Menge S wie folgt

$$S := \left\{x^i y^j z^k \mid 0 \le i \le \ell, 0 \le j \le \delta(\ell - i), 0 \le k \le \lambda\delta(\ell - i) + \eta\ell\right\}.$$

Dabei ist $\ell \in \mathbb{N}$ und $\eta \ge 0$ mit $\ell\eta \in \mathbb{N}$. Entsprechend ist dann die Menge M definiert als Minkowski-Summe von S und $N(p)$:

$$M := \left\{x^i y^j z^k \mid 0 \le i \le \ell + 1, 0 \le j \le \delta((\ell+1) - i), 0 \le k \le \lambda\delta((\ell+1) - i) + \eta\ell\right\}.$$

Die Parameter ℓ und η werden später zur Optimierung der Schranken verwendet.

Lemma 4.11
Die Mengen S und M, die mit Hilfe der modularen Rechteckskonstruktion bestimmt werden, sind zulässig für ein Polynom $p(x,y,z) = f_N(y,z) - Nx$, wenn das Newton-Polygon $N(f_N)$ Rechteckform hat.

Beweis: Die Menge M ist die Minkowski-Summe von S und $N(p)$. Daher erfüllen S und M die erste Bedingung der Definition 4.1 für zulässige Mengen.

Um zu zeigen, dass S und M auch die zweite Bedingung erfüllen, wird ein Polynom $g(x,y,z) = \sum g_{ijk} x^i y^j z^k$ betrachtet, welches nicht über S definiert ist, und es wird

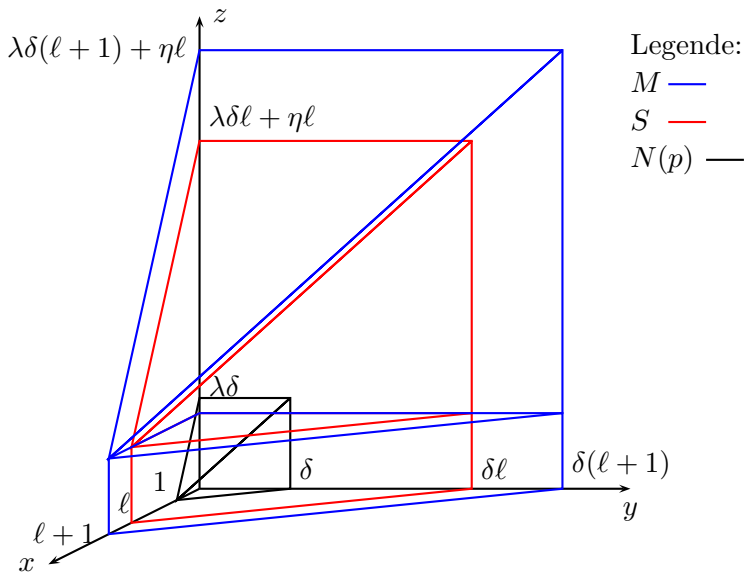

Abbildung 4.5: Modulare Rechteckkonstruktion

gezeigt, dass $p(x,y,z) \cdot g(x,y,z)$ nicht über M definiert ist. Wir bezeichnen mit l_x, l_y und l_z den Grad von g in x, y und z. Da g nicht über S definiert ist, gilt

1. $l_x > \ell$ oder $l_y > \delta\ell$ oder $l_z > \lambda\delta\ell + \eta\ell$

   oder

2. $\delta i + j > \delta\ell$ oder $\delta i + k > \lambda\delta\ell + \eta\ell$.

Da die Fälle in 1. und 2. jeweils symmetrisch sind, genügt es jeweils einen dieser Fälle zu betrachten.

1. Es sei $l_z > \lambda\delta\ell + \eta\ell$.
   Es sei (i_0, j_0) das Paar, für das j_0 maximal ist unter allen j mit $g_{ijl_z} \neq 0$. Dann ist der Koeffizient von $x^{i_0}y^{j_0+\delta}z^{l_z+\lambda\delta}$ in $g(x,y,z) \cdot p(x,y,z)$ von 0 verschieden. Da $l_z > \lambda\delta\ell + \eta\ell$ ist, ist $l_z + \lambda\delta > \lambda\delta(\ell+1) + \eta\ell$ und $x^{i_0}y^{j_0+\delta}z^{l_z+\lambda\delta} \notin M$.
2. Es sei $\delta i + k > \lambda\delta\ell + \eta\ell$, wobei $i \leq \ell$ und $k \leq \lambda\delta\ell + \eta\ell$ gilt.
   Es sei $m := \max\{\delta i + k \mid \delta i + k > \lambda\delta\ell + \eta\ell \wedge g_{ijk} \neq 0\}$. Wir wählen unter allen Tripeln (i,j,k), die $\delta i + k = m$ und $g_{ijk} \neq 0$ erfüllen, denjenigen mit maximalem j aus. Dann ist der Koeffizient von $x^i y^{j+\delta} z^{k+\lambda\delta}$ in $g(x,y,z) \cdot p(x,y,z)$ von 0 verschieden. Da $\delta i + k > \lambda\delta\ell + \eta\ell$ ist, ist $\delta i + k + \lambda\delta > \delta(\ell+1) + \eta\ell$. Daher ist $x^i y^{j+\delta} z^{k+\lambda\delta} \notin M$.

Also ist $g(x,y,z)p(x,y,z)$ nicht über M definiert.

□

Konstruktion 4.12 (Modulare linke untere Dreiecksform)
Das Newton-Polygon $N(f)$ des Polynoms $f(y,z)$ sei das linke untere Dreieck $LD(0,\delta,\lambda)$ mit $\lambda > 0$. Dann ist das Newton-Polytop $N(p)$ von $p(x,y,z) = f_N(y,z) - Nx$, wobei $f_N(y,z) := f(y,z) \mod N$ ist, von der Form

$$N(p) := \operatorname{conv}\left\{(i,j,k) \in \mathbb{N}^3 \mid 0 \le i \le 1, 0 \le j \le \delta(1-i), 0 \le k \le \lambda\delta(1-i) - \lambda j\right\}.$$

Dann definieren wir die Menge S wie folgt

$$S := \left\{x^i y^j z^k \mid 0 \le i \le \ell, 0 \le j \le \delta(\ell - i), 0 \le k \le \lambda(\delta(\ell - i) - j)\right\}.$$

Dabei ist $\ell \in \mathbb{N}$. Entsprechend ist dann die Menge M definiert durch

$$M := \left\{x^i y^j z^k \mid 0 \le i \le \ell + 1, 0 \le j \le \delta((\ell+1) - i), 0 \le k \le \lambda(\delta((\ell+1) - i) - j)\right\}.$$

Der Parameter ℓ wird später zur Optimierung der Schranken verwendet.

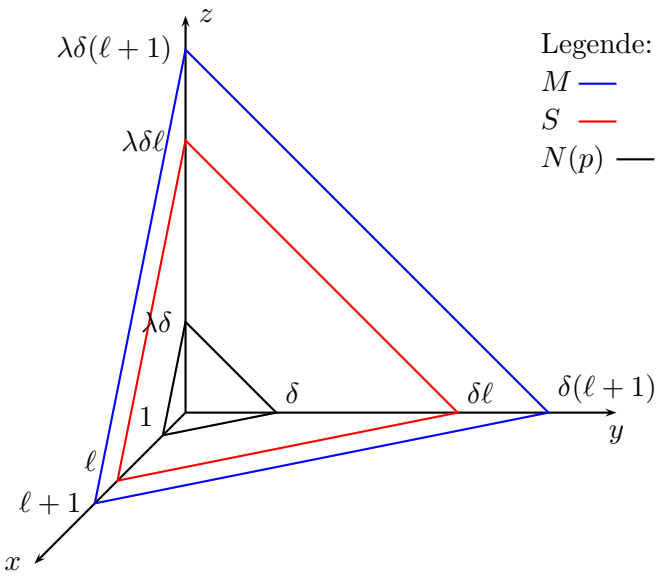

Abbildung 4.6: Modulare linke untere Dreiecksform

Lemma 4.13
Die Mengen S und M, welche mit Hilfe der modularen linken unteren Dreieckskonstruktion bestimmt werden, sind zulässig für ein Polynom $p(x,y,z) = f_N(y,z) - Nx$, wenn das Newton-Polygon $N(f_N)$ linke untere Dreiecksform hat.

Beweis: Da M als Minkowski-Summe von S und $N(p)$ definiert ist, ist die erste Bedingung der Definition für zulässige Mengen erfüllt.

Um zu zeigen, dass die Mengen S und M auch die zweite Bedingung erfüllen, wird ein Polynom $g(x,y,z) = \sum g_{ijk} x^i y^j z^k$ betrachtet, welches nicht über S definiert ist. Es wird gezeigt, dass $g(x,y,z) \cdot p(x,y,z)$ nicht über M definiert ist.

Da $g(x,y,z)$ nicht über der Menge S definiert ist, gibt es mindestens ein Monom $x^i y^j z^k$ mit $\lambda\delta i + \lambda j + k > \lambda\delta l$. Es sei $l_{xyz} = \max\{\lambda\delta i + \lambda j + k \mid \lambda\delta i + \lambda j + k > \lambda\delta\ell \wedge g_{ijk} \neq 0\}$. Wir wählen nun unter allen Tripeln (i,j,k), die $\lambda\delta i + \lambda j + k = l_{xyz}$ und $g_{ijk} \neq 0$ erfüllen, den Exponenten aus, mit maximalen j aus. Existieren mehrere Exponente, die dieser Bedingung genügen, wählen wir unter ihnen den lexikographisch größten. Wir bezeichnen diesen Exponenten mit (i_0, j_0, k_0). Der Koeffizient von $x^{i_0} y^{j_0+\delta} z^{k_0}$ in $f(x,y,z) \cdot p(x,y,z)$ ist von 0 verschieden. Nach Wahl des Tripels (i_0, j_0, k_0) gilt $\lambda\delta i_0 + \lambda j_0 + k_0 > \lambda\delta l$, daher ist $\lambda\delta i_0 + \lambda(j_0 + \delta) + k_0 + > \lambda\delta\ell + \lambda\delta = \lambda\delta(\ell + 1)$. Das bedeutet, dass $f(x,y,z) \cdot p(x,y,z)$ nicht über M definiert ist.

□

Konstruktion 4.14 (Modulare rechte untere Dreiecksform)
Das Newton-Polygon $N(f)$ des Polynoms $f(y,z)$ sei das rechte untere Dreieck $RD(0,\delta,\lambda)$ mit $\lambda > 0$. Dann ist das Newton-Polytop $N(p)$ von $p(x,y,z) = f_N(y,z) - Nx$, wobei $f_N(y,z) := f(y,z) \mod N$ ist, von der Form

$$N(p) := \operatorname{conv}\left\{(i,j,k) \in \mathbb{N}^3 \mid 0 \le i \le 1, 0 \le j \le \delta(1-i), 0 \le k \le \lambda\delta j\right\}.$$

Dann definieren wir die Menge S wie folgt

$$S := \left\{x^i y^j z^k \mid 0 \le i \le \ell, 0 \le j \le \delta(\ell - i), 0 \le k \le \lambda j + \eta\ell\right\}.$$

Dabei ist $\ell \in \mathbb{N}$ und $\eta > 0$ mit $\ell\eta \in \mathbb{N}$. Entsprechend ist dann die Menge M definiert durch

$$M := \left\{x^i y^j z^k \mid 0 \le i \le \ell + 1, 0 \le j \le \delta((\ell+1) - i), 0 \le k \le \lambda j + \eta\ell\right\}.$$

Die Parameter ℓ und η werden später zur Optimierung der Schranken verwendet.

Lemma 4.15
Die Mengen S und M, die mit der modularen rechten unteren Dreieckskonstruktion bestimmt werden, sind zulässig für ein Polynom $p(x,y,z) = f_N(y,z) - Nx$, wenn das Newton-Polygon $N(f_N)$ rechte untere Dreiecksform hat.

Beweis: Die erste Bedingung für zulässige Mengen ist erfüllt, da M als Minkowski-Summe von S und $N(p)$ definiert ist. Um die zweite Bedingung zu zeigen, betrachten wir ein Polynom $g(x,y,z)$, welches nicht über S definiert ist, und zeigen, dass $g(x,y,z) \cdot p(x,y,z)$ nicht über M definiert ist.

Da $g(x,y,z)$ nicht über S definiert ist, gibt es mindestens ein Tripel (i,j,k) mit $g_{ijk} \neq 0$ und $\delta i + j > \delta\ell$ oder $k > \lambda j + \eta\ell$.

Der Fall $\delta i + j > \delta\ell$ verläuft analog zum modularen Rechteckfall.

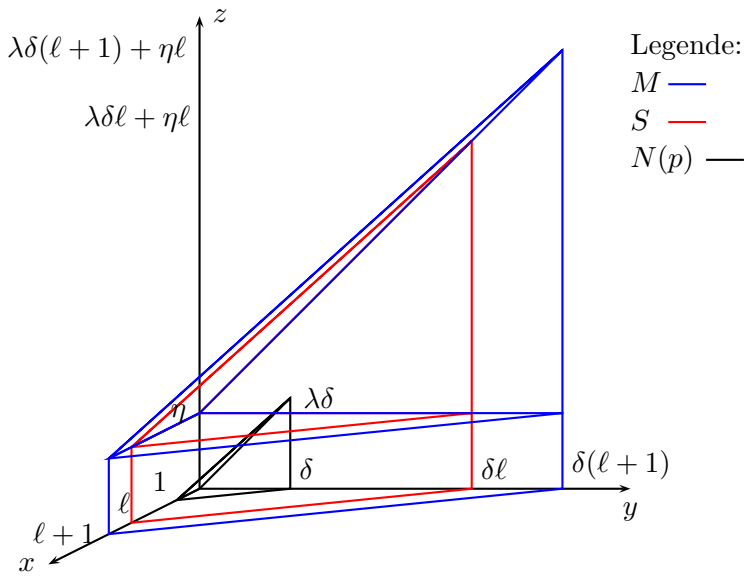

Abbildung 4.7: Modulare rechte untere Dreiecksform

Es sei also $k > \lambda j + \eta\ell$.

Bei der nun verwendeten lexikographischen Ordnung nehmen wir an, dass $j \leq k \leq i$ gilt. Dies bedeutet, dass (i, j, k) lexikographisch größer ist als (i', j', k'), wenn das erste von 0 verschiedene Element in $(j, k, i) - (j', k', i')$ negativ ist.

Wir wählen das bezüglich der lexikographischen Ordnung größte Tripel (i, j, k), das $g_{ijk} \neq 0$ und $k > \lambda j + \eta\ell$ erfüllt, und bezeichnen es mit (i_0, j_0, k_0). Dann ist der Koeffizient von $x^{i_0}y^{j_0+\delta}z^{k_0+\lambda\delta}$ in $p(x, y, z)\cdot g(x, y, z)$ von 0 verschieden. Da $k_0 > \lambda j_0+\eta\ell$ ist, ist auch $k_0 + \lambda\delta > \lambda j_0 + \lambda\delta + \eta\ell$. Also ist $x^{i_0}y^{j_0+\delta}z^{k_0+\lambda\delta} \notin M$ und somit ist $p(x, y, z) \cdot g(x, y, z)$ nicht über M definiert. □

Ähnlich wie im Lemma 4.9 lässt sich für eine allgemeinere Klasse von bivariaten modularen Polynomen ein Konstruktion für zulässige Mengen S und M angeben. Diese Klasse beinhaltet die modulare Rechteckkonstruktion und die modulare linke untere Dreieckskonstruktion, jedoch nicht die modulare rechte untere Dreieckskonstruktion. Da der Beweis jedoch sehr technisch ist, möchten wir an dieser Stelle darauf verzichten.

Wir haben in diesem Abschnitt mögliche Konstruktionen für die Mengen S und M für bestimmte Formen des Newton-Polygons eines bivariaten modularen Polynoms angegeben, wobei wir das bivariate modulare Polynom als trivariates ganzzahliges Polynom betrachten. Für diese Konstruktionen haben wir gezeigt, dass sie zulässige Mengen liefern. Mit Hilfe dieser Konstruktionen können wir nun im folgenden Kapitel die Schranken für die Nullstellen bivariater modularer Polynomen maximieren.

5 Der bivariate modulare Fall als Spezialfall des trivariaten ganzzahligen Falls

In diesem Abschnitt wird untersucht, ob sich der bivariate modulare Fall mit den Methoden von Blömer und May [1] als Spezialfall auf den trivariaten ganzzahligen Fall zurückführen lässt. Zur genaueren Analyse der Schranken für Polynome einer bestimmten Form ist keine Gittertheorie mehr notwendig. Wir benutzen den trivariaten Fall des Satzes von Coron (Satz 3.4) als Blackbox und beschränken uns auf die Optimierung der Monom-Mengen S und M.

Wie bereits in Kapitel 4 erwähnt, betrachten wir parametrisierte Mengen S und M. Mit Hilfe der Bedingung für die Schranken der Nullstellen ganzzahliger trivariater Polynome (3.7) ermitteln wir die optimalen Werte für diese Parameter. Diese Optimierung werden wir in diesem Kapitel nicht explizit ausführen, sondern wir zeigen lediglich, welche Schranken wir mit den optimalen Parameterwerten erhalten.

5.1 Die linke untere Dreiecksform

Zunächst werden bivariate Polynome vom totalen Grad δ betrachtet. Das heißt, wir betrachten Polynome, deren Newton-Polygon ein linkes unteres Dreieck bildet.

Satz 5.1
Es sei $f(y,z) \in \mathbb{Z}[y,z]$ ein irreduzibles Polynom vom totalen Grad δ. Ferner seien Y und Z natürliche Zahlen, welche der Bedingung

$$YZ < 2^{-\left(\frac{25\,\delta}{24\,\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right)} \cdot N^{\frac{1}{\delta}} - \mathcal{O}(\varepsilon)$$

für ein $\varepsilon \in (0,1]$ genügen. Dann können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$, die

$$f(y_0, z_0) \equiv 0 \mod N \quad \textit{mit } |y_0| \leq Y,\ |z_0| \leq Z$$

erfüllen, in Zeit polynomiell in $\log N$ und δ gefunden werden.

Beweis: Wir betrachten den bivariaten modularen Fall

$$f(y,z) \equiv 0 \mod N$$

als trivariaten Fall

$$p(x,y,z) := f_N(y,z) - N\,x = 0$$

über $\mathbb{Z}$, wobei $f_N(y,z) := f(y,z) \mod N$.

Da das Newton-Polygon des Polynoms $f_N(y,z)$ ein linkes unteres Dreieck ist, wenden wir die Konstruktion 4.12 mit $\lambda = 1$ an und erhalten die Mengen

$$S := \left\{ x^i y^j z^k \mid 0 \le i \le \ell, 0 \le j \le \delta\,(\ell - i), 0 \le k \le \delta\,(\ell - i) - j \right\}$$

und

$$M := \left\{ x^i y^j z^k \mid 0 \le i \le \ell + 1, 0 \le j \le \delta\,(\ell + 1 - i), 0 \le k \le \delta\,(\ell + 1 - i) - j \right\}.$$

Der Parameter ℓ wird später in Abhängigkeit von ε gewählt und beeinflusst so die Güte der Schranken. Die Mengen S und M sind nach Lemma 4.13 zulässig für $p(x,y,z)$ und der Satz 3.4 ist anwendbar.

Wir setzen $\tau = \gamma = \delta$. Dann liefern die Formeln für $s_x,\ s_y,\ s_z,\ s,\ m$ und ω:

$$\begin{aligned} s_x &= \frac{(\ell+1)(2\,\delta^2\,\ell^2 + \delta^2\,\ell + 9\,\delta\,\ell + 12)}{12} \\ &= \frac{\delta^2\,\ell^3}{6}\left(1 + \mathcal{O}\left(\frac{1}{\ell}\right)\right), \\ s_y &= s_z \\ &= \frac{\delta(\ell+1)(\delta\,\ell + \delta + 2)(\delta\,\ell + \delta + 1)}{6} \\ &= \frac{\delta^3\,\ell^3}{6}\left(1 + \mathcal{O}\left(\frac{1}{\ell}\right)\right) \end{aligned}$$

und

$$\begin{aligned} s &= \frac{(\ell+1)(2\,\delta^2\,\ell^2 + \delta^2\,\ell + 9\,\delta\,\ell + 12)}{12}, \\ m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2 + 5\,\delta^2\ell + 9\,\delta\,\ell + 12 + 3\,\delta^2 + 9\,\delta)}{12}, \\ \omega &= (\ell+2)(\delta + \delta\,\ell + 1)^2. \end{aligned}$$

Außerdem gilt $s - 1 \ge \frac{\delta^2\,\ell^3}{6}$. Die Anwendung des Satzes 3.4 mit den oben genannten Abschätzungen für s_x, s_y, s_z, s, m und ω liefert die folgende Bedingung:

$$X^{\frac{\delta^2\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} (YZ)^{\frac{\delta^3\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} \;<\; 2^{-\frac{m\,(4\,\omega+m+3)}{4}}\, W^{\frac{\delta^2\,\ell^3}{6}}.$$

Dies impliziert die Schranke

$$X(YZ)^{\delta} \;<\; 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3\,(1+\mathcal{O}(1/\ell))}}\, W^{\frac{1}{1+\mathcal{O}(1/\ell)}}.$$

Wir beobachten, dass für $x > 0$ gilt: $\frac{1}{1+x} \geq 1 - x$. Daher kann der Exponent von W durch $1 - \mathcal{O}\left(\frac{1}{\ell}\right)$ abgeschätzt werden. Dies führt zu der Bedingung

$$X(YZ)^{\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{l}\right)\right)} W^{1-\mathcal{O}\left(\frac{1}{\ell}\right)}.$$

Da wir $f(y, z)$ modulo N reduzieren, können wir x_0 folgendermaßen abschätzen:

$$\begin{aligned} |x_0| &\leq \frac{|f_N(y_0, z_0)|}{N} \\ &\leq \sum_{j=0}^{\delta} \sum_{k=0}^{\delta-j} Y^j Z^k \\ &< \frac{(\delta+1)(\delta+2)}{2} Y^{\delta}\, Z^{\delta}. \end{aligned}$$

Setzen wir nun $X = \frac{(\delta+1)(\delta+2)}{2} Y^{\delta}\, Z^{\delta}$, dann gilt $W = \|p(xX, yY, zY)\|_{\infty} = NX$. Diese Beobachtungen führen auf die folgende Schranke:

$$(YZ)^{\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{l}\right)\right)}\, N^{1-\mathcal{O}\left(\frac{1}{l}\right)}\, X^{-\mathcal{O}\left(\frac{1}{l}\right)}. \tag{5.1}$$

Nun setzen wir $X = \frac{(\delta+1)(\delta+2)}{2} Y^{\delta}\, Z^{\delta}$ in (5.1) ein und erhalten so die Bedingung

$$(YZ)^{\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{l}\right)\right)}\, N^{1-\mathcal{O}\left(\frac{1}{l}\right)} \left(\frac{(\delta+1)(\delta+2)}{2} (Y\,Z)^{\delta}\right)^{-\mathcal{O}\left(\frac{1}{l}\right)}.$$

Weiterhin gilt $Y \leq N$ und $Z \leq N$, da es sich hierbei um Schranken für die Nullstellen eines modularen Polynoms handelt. Damit ergibt sich die Bedingung:

$$(YZ)^{\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{l}\right)\right)} \left(\frac{(\delta+1)(\delta+2)}{2}\right)^{-\mathcal{O}\left(\frac{1}{l}\right)}\, N\, N^{-\mathcal{O}\left(\frac{\delta}{l}\right)}. \tag{5.2}$$

Indem wir die Terme $2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{l}\right)\right)}$ und $\left(\frac{(\delta+1)(\delta+2)}{2}\right)^{-\mathcal{O}\left(\frac{1}{l}\right)}$ zusammenfassen und beide Seiten der Ungleichung (5.2) mit $1/\delta$ potenzieren, erhalten wir

$$YZ < 2^{-\left(\frac{25\,\delta\,\ell^3}{24} + \mathcal{O}\left(\delta\,\ell^2\right)\right)}\, N^{\frac{1}{\delta}} - \mathcal{O}\left(\frac{1}{\ell}\right). \tag{5.3}$$

Die ausführliche Abschätzung des Exponenten von 2 wird im Anhang B.1 angegeben. Wird $\ell = \lfloor 1/\varepsilon \rfloor$ gesetzt, liefert (5.3) die gewünschte Abschätzung

$$YZ < 2^{-\left(\frac{25\,\delta}{24\,\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right)} N^{\frac{1}{\delta}} - \mathcal{O}(\varepsilon). \tag{5.4}$$

Für die Schranken Y und Z, die (5.4) erfüllen, erhalten wir laut Satz 3.4 einen Algorithmus zur Bestimmung der Nullstellen ganzzahliger modularer Polynomialgleichungen mit Laufzeit polynomiell in $(\log W, m)$. Da m als Polynom in δ und $1/\varepsilon$ aufgefasst werden kann, hat der Algorithmus polynomielle Laufzeit in $(\log W, \delta, 1/\varepsilon)$.

Es bleibt zu zeigen, dass $\log W$ polynomiell in $\log N$ ist. Da Y und Z Schranken für die Nullstellen eines bivariaten Polynoms modulo N sind, gilt $Y, Z \leq N$. Außerdem gilt, wie bereits beobachtet, $X = \frac{(\delta+1)(\delta+2)}{2} Y^\delta Z^\delta$ und

$$W = X N = \frac{(\delta+1)(\delta+2)}{2} Y^\delta Z^\delta \leq \frac{(\delta+1)(\delta+2)}{2} N^2.$$

Somit ist W polynomiell in N. Für ein festes $\varepsilon > 0$ ist die Laufzeit daher polynomiell in $(\log N, \delta)$. □

5.2 Die Rechteckform

Im Folgenden richtet sich das Augenmerk auf bivariate Polynome vom Grad δ in den Variablen y und z. Das sind Polynome, deren Newton-Polygon Rechteckform besitzt.

Die Maximierung der Schranken Y und Z für die Nullstellen eines bivariaten ganzzahligen Polynoms, welche in Polynomialzeit berechnet werden können, verläuft analog zu Satz 5.1.

Satz 5.2
Es sei $f(y,z) \in \mathbb{Z}[y,z]$ ein Polynom vom Grad δ in y und z. Ferner seien Y und Z natürliche Zahlen, welche für ein $\varepsilon \in (0,1]$

$$YZ < 2^{-\left(\frac{\delta}{\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right)} N^{\frac{2}{3\delta}} - \mathcal{O}(\varepsilon)$$

füllen. Dann können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$, für die

$$f(x_0, y_0) \equiv 0 \quad \textit{mit } |y_0| \leq Y,\ |z_0| \leq Z$$

gilt, in Zeit polynomiell in $\log N$ und δ gefunden werden.

Beweis: Die bivariate modulare Gleichung

$$f(y,z) \equiv 0 \mod N$$

wird als trivariate Polynomialgleichung

$$p(x,y,z) := f_N(y,z) - Nx = 0$$

über $\mathbb{Z}$ aufgefasst, wobei $f_N(y,z) := f(y,z) \mod N$. Das Newton-Polygon von $f(y,z)$ ist ein Rechteck. Somit kann Konstruktion 4.10 mit $\lambda = 1$ und $\eta = 0$ angewendet werden und wir erhalten die Mengen

$$S := \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell, 0 \leq j \leq \delta(\ell - i), 0 \leq k \leq \delta(\ell - i) \right\}$$

und

$$M := \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell + 1, 0 \leq j \leq \delta(\ell + 1 - i), 0 \leq k \leq \delta(\ell + 1 - i) \right\}.$$

Der Parameter ℓ wird später in Abhängigkeit von ε gewählt und die Wahl des Parameters $\eta = 0$ vereinfacht die folgenden Abschätzungen. Laut Lemma 4.11 sind S und M zulässig für $p(x, y, z)$. Damit ist Satz 3.4 anwendbar mit $\tau = \gamma = \delta$. Dies liefert mit den Formeln für s_x, s_y, s_z, s, m und ω:

$$\begin{aligned} s_x &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+6\,\delta\,\ell+6)}{6} \\ &= \frac{\delta^2\,\ell^3}{3}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right), \\ s_y &= s_z \\ &= \frac{\delta\,(\ell+1)(\delta\,\ell+\delta+1)^2}{2} \\ &= \frac{\delta^3\,\ell^3}{2}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right) \end{aligned}$$

sowie

$$\begin{aligned} s &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+6\,\delta\,\ell+6)}{6}, \\ m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2+5\,\delta^2\,\ell+6\,\delta\,\ell+6+2\,\delta^2+6\,\delta)}{6} \\ \omega &= (\ell+2)(\delta+\delta\,\ell+1)^2. \end{aligned}$$

Außerdem gilt $s-1 \geq \frac{\delta^2\,\ell^3}{3}$. Nun wenden wir Satz 3.4 mit den oben genannten Abschätzungen für s_x, s_y, s_z, s, m und ω an. Somit erhalten wir die folgende Bedingung:

$$X^{\frac{\delta^2\,\ell^3}{3}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)}(YZ)^{\frac{\delta^3\,\ell^3}{2}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} < 2^{-\frac{m\,(4\,\omega+m+3)}{4}}\,W^{\frac{\delta^2\,\ell^3}{3}}.$$

Dies führt auf die Schranke

$$X^2(YZ)^{3\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3(1+\mathcal{O}(1/\ell))}}\,W^{\frac{2}{1+\mathcal{O}(1/\ell)}}.$$

Wie im Beweis von Satz 5.1 kann der Exponent von W durch $2-\mathcal{O}\left(\frac{1}{\ell}\right)$ abgeschätzt werden, was die folgende Bedingung liefert:

$$X^2(YZ)^{3\delta} < 2^{-\frac{6\,m(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\,W^{2-\mathcal{O}\left(\frac{1}{\ell}\right)}.$$

Da wir das Polynom $f(y, z)$ modulo N reduzieren, können wir x_0 folgendermaßen abschätzen:

$$\begin{aligned} |x_0| &\leq \frac{|f_N(y_0, z_0)|}{N} \\ &\leq \sum_{j=0}^{\delta}\sum_{k=0}^{\delta} Y^j Z^k \\ &\leq (\delta+1)^2 \cdot Y^\delta\,Z^\delta. \end{aligned}$$

Wir setzen $X = (\delta+1)^2 \cdot Y^\delta\, Z^\delta$, dann gilt $W = NX$. Damit ergibt sich die Schranke:

$$(YZ)^{3\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)} N^{2-\mathcal{O}\left(\frac{1}{l}\right)} X^{-\mathcal{O}\left(\frac{1}{l}\right)}. \tag{5.5}$$

Mit $X = (\delta+1)^2 \cdot Y^\delta\, Z^\delta$ erhalten wir aus (5.5) die Bedingung

$$(YZ)^{3\delta} < 2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, N^{2-\mathcal{O}\left(\frac{1}{l}\right)} \left((\delta+1)^2 \cdot Y^\delta Z^\delta\right)^{-\mathcal{O}\left(\frac{1}{l}\right)}.$$

Weiterhin gilt $Y, Z \leq N$, da es Schranken für die Nullstellen eines modularen Polynoms sind. Das impliziert die Schranke

$$(YZ)^{3\delta} < 2^{-\left(3\,\delta^2\,\ell^3+\mathcal{O}\left(\delta^2\,\ell^2\right)\right)}\, N^{2-\mathcal{O}\left(\frac{\delta}{\ell}\right)},$$

woraus sich

$$YZ < 2^{-\left(\delta\,\ell^3+\mathcal{O}\left(\delta\,\ell^2\right)\right)}\, N^{\frac{2}{3\,\delta}-\mathcal{O}\left(\frac{1}{\ell}\right)} \tag{5.6}$$

ergibt. Die Abschätzung für den Exponenten von 2 kann im Anhang B.2 nachgelesen werden. Wir setzen nun in (5.6) $\ell = \lfloor 1/\varepsilon \rfloor$. Dann erhalten wir die gewünschte Abschätzung

$$YZ < 2^{-\left(\frac{\delta}{\varepsilon^3}+\mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right)}\, N^{\frac{2}{3\,\delta}-\mathcal{O}(\varepsilon)}. \tag{5.7}$$

Für Schranken Y und Z, die (5.7) erfüllen, liefert dies einen Algorithmus zur Bestimmung von Nullstellen ganzzahliger modularer Polynome mit Laufzeit polynomiell in $(\log W, \delta, 1/\varepsilon)$, da m als Polynom in δ und $1/\varepsilon$ aufgefasst werden kann. Es gilt

$$W = \|p(x,y,z)\|_\infty = NX = N(\delta+1)^2(YZ)^\delta \leq (\delta+1)^2 N^{2\,\delta+1},$$

somit ist

$$\log W \leq 2\,\log(\delta+1) + (2\,\delta+1)\log N.$$

Da $\log W$ also polynomiell in $\log N$ ist, ist die Laufzeit des Algorithmus für ein festes $\varepsilon > 0$ polynomiell in $(\log N, \delta)$. □

Diese Ergebnis lässt sich noch verbessern, wenn wir nähere Informationen über die Größenordnung der Schranken Y und Z der Nullstellen besitzen. Da Y und Z Schranken für die Nullstellen eines modularen Polynoms sind, wissen wir, dass $Y = N^\alpha$ und $Z = N^\beta$ für $\alpha, \beta \in (0,1)$ gilt. Stehen nun α und β und somit Y und Z im Verhältnis $\alpha + 2\,\beta \leq \frac{1}{\delta}$ zueinander, vergrößern wir die Menge S und somit das Gitter L durch zusätzliche z-Shifts. Wir erzielen bessere Schranken, da die Determinante der Basismatrix verhältnismäßig klein bleibt, während s vergrößert wird. Durch die Bedingung $\alpha + 2\beta \leq \frac{1}{\delta}$ stellen wir sicher, dass wir bei der Optimierung einen positiven Parameterwert erhalten. Dies wird im Beweis an der entsprechenden Stelle erwähnt werden. Für einen negativen Parameterwert erhalten wir ein Ergebnis, welches analog zur Vergrößerung der Menge S durch zusätzliche y-Shifts ist (vgl. Satz 5.4).

Satz 5.3
Es sei $f(y,z)$ ein irreduzibles bivariates ganzzahliges Polynom vom Grad δ in y und z. Weiter seien Y, Z ganze Zahlen, wobei $Y = N^\alpha, Z = N^\beta$ für $\alpha, \beta \in (0,1)$ und

$$\alpha + 2\,\beta \leq \frac{1}{\delta} \tag{5.8}$$

gilt. Falls Y und Z für ein $\varepsilon \in (0,1]$ die Bedingung

$$N^{\alpha\,(6-3\,\alpha\,\delta)+4\,\beta} < 2^{-\left(\frac{13\,(\alpha\,\delta-1)^2}{6\,\beta\,\varepsilon^3} + \mathcal{O}\left(\frac{(\alpha^2+\beta)\,\delta^2+1}{\beta\,\varepsilon^2}\right)\right) N^{\frac{3}{\delta}-\mathcal{O}(-\alpha\,\delta-2\beta\,\delta+1)\varepsilon)}}$$

erfüllen, können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$ mit

$$f(y_0, z_0) \equiv 0 \mod N \quad \textit{für } |y_0| \leq Y,\ |z_0| \leq Z$$

in Zeit polynomiell in $\log N$ und δ gefunden werden.

Beweis: Erneut wird der bivariate modulare Fall

$$f(y,z) \equiv 0 \mod N$$

als trivariater ganzzahliger Fall

$$p(x,y,z) := f_N(y,z) - Nx = 0$$

mit $f_N(y,z) := f(y,z) \mod N$ aufgefasst. Für die Schranken $Y = N^\alpha$ und $Z = N^\beta$ gilt $\alpha + 2\,\beta \leq \frac{1}{\delta}$. Daher wird die ursprüngliche Menge der Shiftpolynome durch zusätzliche z-Shifts vergrößert. Durch Anwendung der Konstruktion 4.10 mit $\lambda = 1$ erhalten wir die Mengen

$$S := \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell, 0 \leq j \leq \delta(\ell - i), 0 \leq k \leq \delta(\ell - i) + \eta\ell \right\}$$

für $\eta > 0$ und

$$M := \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell + 1, 0 \leq j \leq \delta(\ell + 1 - i), 0 \leq k \leq \delta(\ell + 1 - i) + \eta\ell \right\}.$$

Der Parameter η wird später zur Maximierung der Schranken benötigt. Da wir wissen, dass $Y = N^\alpha$ und $Z = N^\beta$ gilt, können wir diesen Parameter optimieren und später den optimalen Wert für η in unsere Schranken einsetzen.

Die Mengen S und M sind zulässig für $p(x,y,z)$. Damit ist der Satz 3.4 mit $\tau = \delta$ und

$\gamma = \delta + \eta$ anwendbar und liefert die folgenden Formeln für s_x, s_y, s_z, s, m und ω:

$$\begin{aligned}
s_x &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+6\,\delta\,\ell+6+6\,\eta\,\ell+3\,\delta\,\eta\,\ell^2)}{6} \\
&= \frac{(3\,\eta+2\,\delta)\,\delta\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right), \\
s_y &= \frac{\delta\,(\ell+1)(\delta\,\ell+\delta+1)(\delta\,\ell+\delta+\eta\,\ell+1)}{2} \\
&= \frac{(\delta+\eta)\,\delta^2\,\ell^3}{2}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right), \\
s_z &= \frac{(\delta+\eta\,\ell+\delta\,\ell)(\delta\,\ell+\delta+1)(\delta\,\ell+\delta+\eta\,\ell+1)}{2} \\
&= \frac{(\delta^2+\eta^2+2\,\delta\,\eta)\,\delta\,\ell^3}{2}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)
\end{aligned}$$

und

$$\begin{aligned}
s &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+6\,\delta\,\ell+6+6\,\eta\,\ell+3\,\delta\,\eta\,\ell^2)}{6}, \\
m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2+5\,\delta^2\,\ell+3\,\delta\,\eta\,\ell^2+6\,\delta\,\ell+6+3\,\delta^2+6\,\delta+3\,\delta\,\eta\,\ell+6\,\eta\,\ell)}{6}, \\
\omega &= (\ell+2)(\delta+\delta\,\ell+1)(\delta+(\delta+\eta)\,\ell+1).
\end{aligned}$$

Weiterhin gilt $s-1 \geq \frac{(3\,\eta+2\,\delta)\,\delta\,l^3}{6}$. Satz 3.4 liefert dann mit den obigen Abschätzungen die Bedingung:

$$\begin{aligned}
X^{\frac{(3\,\eta+2\,\delta)\,\delta\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} Y^{\frac{(\delta+\eta)\,\delta^2\,\ell^3}{2}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} Z^{\frac{(\delta^2+\eta^2+2\delta\,\eta)\,\delta\,\ell^3}{2}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} \\
< 2^{-\frac{m\,(4\,\omega+m+3)}{4}}\, W^{\frac{(3\,\eta+2\,\delta)\,\delta\,\ell^3}{6}}.
\end{aligned}$$

Dies impliziert die Schranke

$$X^{(3\,\eta+2\,\delta)} Y^{3\,(\delta+\eta)\,\delta} Z^{3\,(\delta^2+\eta^2+2\,\delta\,\eta)} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3(1+\mathcal{O}(1/\ell))}}\, W^{\frac{(3\,\eta+2\,\delta)}{1+\mathcal{O}(1/\ell)}}.$$

Auch hier kann der Exponent von W wieder wie im Beweis von Satz 5.1 durch $(3\,\eta+2\,\delta)(1-\mathcal{O}(1/\ell))$ abgeschätzt werden, was auf die Bedingung

$$X^{(3\,\eta+2\,\delta)} Y^{3\,(\delta+\eta)\,\delta} Z^{3\,(\delta^2+\eta^2+2\,\delta\,\eta)} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, W^{(3\,\eta+2\,\delta)\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}$$

führt. Wie in Satz 5.2 gilt auch hier $X = (\delta+1)^2 \cdot Y^\delta\, Z^\delta$ und $W = NX$, da die Form des Newton-Polytops des betrachteten Polynoms sich nicht verändert hat. Mit diesen Schranken erhalten wir analog zu Satz 5.2 die Bedingung

$$\begin{aligned}
Y^{3\,(\delta+\eta)\,\delta} Z^{3\,(\delta^2+\eta^2+2\,\delta\,\eta)} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, N^{(3\,\eta+2\,\delta)\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)} \\
\cdot\, X^{-(3\,\eta+2\,\delta)\mathcal{O}\left(\frac{1}{\ell}\right)}.
\end{aligned}$$

Da $X = (\delta+1)^2 (YZ)^\delta$ und $Y, Z \leq N$ gilt, ergibt sich die Schranke

$$Y^{3\,(\delta+\eta)\,\delta} Z^{3\,(\delta^2+\eta^2+2\,\delta\,\eta)} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)-(2\,\delta+3\,\eta)\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right)} N^{(3\,\eta+2\,\delta)\left(1-\mathcal{O}\left(\frac{\delta}{\ell}\right)\right)}.$$

Wir setzen $Y = N^\alpha, Z = N^\beta$ und $\eta = -\frac{\alpha\,\delta+2\,\beta\,\delta-1}{2\,\beta}$. Wegen (5.8) ist $\eta \geq 0$. So erhalten wir die Bedingung

$$\begin{aligned} N^{\frac{-3\,\alpha^2\,\delta^2+6\,\alpha\,\delta-3+4\,\beta\,\delta}{4\,\beta}} \quad &< \quad 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)-\mathcal{O}\left(-\frac{(\alpha\,\delta+2\,\beta\,\delta+1)\log(\delta)}{\beta\,\ell}\right)} \\ &\quad \cdot N^{-\mathcal{O}\left(-\frac{(\alpha\,\delta+2\,\beta\,\delta-1)\,\delta}{\beta\,\ell}\right)}. \end{aligned}$$

Diese Bedingung impliziert die Schranke

$$\begin{aligned} N^{3\,\alpha\,(2\,\delta-\alpha\,\delta)+4\,\beta} \quad &< \quad 2^{-\frac{6\,\beta\,m\,(4\,\omega+m+3)}{\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)-\mathcal{O}\left(-\frac{(\alpha\,\delta+2\,\beta\,\delta+1)\log(\delta)}{\ell}\right)} \\ &\quad \cdot N^{\frac{3}{\delta}}\, N^{-\mathcal{O}\left(\frac{-\alpha\,\delta-2\,\beta\,\delta+1}{\ell}\right)}. \end{aligned} \tag{5.9}$$

Hierbei kann der Exponent von 2 folgendermaßen abgeschätzt werden:

$$\frac{6\,\beta\,m\,(4\,\omega+m+3)}{\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)+\mathcal{O}\left(\frac{\log(\delta)\alpha\,\delta+2\,\beta\,\delta+1)}{\ell}\right) \leq \frac{13\,(\alpha\,\delta-1)^2}{6\,\beta}\ell^3+\mathcal{O}\left(\frac{(\alpha^2+\beta)\,\delta^2+1}{\beta}\ell^2\right).$$

Setzen wir in (5.9) $\ell := \lfloor 1/\varepsilon \rfloor$, so erhalten wir die gewünschte Abschätzung

$$N^{3\,\alpha(2\,\delta-\alpha\,\delta)+4\,\beta} < 2^{-\frac{13\,(\alpha\,\delta-1)^2}{6\beta\,\varepsilon^3}-\mathcal{O}\left(\frac{(\alpha^2+\beta)\,\delta^2+1}{\beta\,\varepsilon^2}\right)} N^{\frac{3}{\delta}}\, N^{-\mathcal{O}((-\alpha\,\delta-2\,\beta\,\delta+1)\,\varepsilon)}. \tag{5.10}$$

Für α und β, die (5.10) erfüllen, erhalten wir einen Algorithmus zur Bestimmung von Nullstellen bivariater modularer Polynome mit Laufzeit polynomiell in $(\log W, \delta, 1/\varepsilon)$. Analog zum Beweis von Satz 5.2 kann gezeigt werden, dass $\log W$ polynomiell in $\log N$ ist. Für ein festes $\varepsilon > 0$ ist die Laufzeit dann polynomiell in $(\log N, \delta)$. □

Gilt $2\,\alpha + \beta \leq \frac{1}{\delta}$ lässt sich durch zusätzlich y-Shifts ein analoges Ergebnis erzielen, indem wir Y und Z vertauschen.

Satz 5.4
Es sei $f(y,z) \in \mathbb{Z}[y,z]$ ein Polynom vom Grad δ in y, z. Es seien $Y, Z \in \mathbb{N}$, wobei $Y = N^\alpha, Z = N^\beta$ für $\alpha, \beta \in (0,1)$ und

$$2\,\alpha + \beta \leq \frac{1}{\delta}$$

gilt. Dann können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$, die

$$f(y_0, z_0) = 0 \mod N \text{ mit } |y_0| \leq Y,\ |z_0| \leq Z$$

erfüllen, in Zeit polynomiell in $\log N$ und δ gefunden werden unter der Voraussetzung, dass für ein $\varepsilon \in (0,1]$

$$N^{\beta\,(6-3\,\beta\,\delta)+4\,\alpha} < 2^{-\frac{13(\beta\,\delta-1)^2}{6\,\alpha}-\mathcal{O}\left(\frac{(\alpha+\beta^2)\,\delta^2+1}{\alpha\,\varepsilon^2}\right)} N^{\frac{3}{\delta}-\mathcal{O}((-2\,\alpha\,\delta-\beta\,\delta+1)\,\varepsilon)}$$

gilt.

5.3 Die rechte untere Dreiecksform

In diesem Abschnitt befassen wir uns mit bivariaten Polynomen modulo N, deren Newton-Polygon ein rechtes unteres Dreieck bildet. Einen Spezialfall dieser Polynome betrachten wir im Abschnitt 6.2. Dort werden wir zeigen, wie sich mit dem Polynom von Boneh und Durfee [2] der geheime Schlüssel d im RSA-Verschlüsselungsschema in Polynomialzeit berechnen lässt, wenn dieser hinreichend klein ist.

Satz 5.5
Es sei $f(y,z) = \sum_{j=0}^{\delta} \sum_{k=0}^{j} f_{jk} y^j z^k \in \mathbb{Z}[y,z]$ *ein irreduzibles Polynom. Ferner seien* Y *und* Z *natürliche Zahlen, welche für ein* $\varepsilon \in (0,1]$ *die Bedingung*

$$Y^2 Z < 2^{-\left(\frac{25\,\delta}{24\,\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right)} N^{\frac{1}{\delta}} N^{-\mathcal{O}(\varepsilon)}$$

erfüllen. Dann können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$*, die*

$$f(y_0, z_0) \equiv 0 \mod N \quad \textit{mit } |y_0| \leq Y, |z_0| \leq Z$$

erfüllen, in Zeit polynomiell in $\log N$ *und* δ *gefunden werden.*

Beweis: Wir fassen den bivariaten modularen Fall

$$f(y,z) \equiv 0 \mod N$$

als trivariaten ganzzahligen Fall

$$p(x,y,z) := f_N(y,z) - Nx = 0$$

mit $f_N(y,z) = f(y,z) \mod N$ auf. Das Newton-Polytop von $f(y,z)$ bildet ein rechtes unteres Dreieck. Aus Konstruktion 4.14 erhalten wir die Mengen

$$S = \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell, 0 \leq j \leq \delta\,(\ell - i), 0 \leq k \leq j \right\}$$

und

$$M = \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell + 1, 0 \leq j \leq \delta\,(\ell + 1 - i), 0 \leq k \leq j \right\}.$$

Diese Mengen sind laut Lemma 4.15 zulässig für $p(x,y,z) = f_N(y,z) - Nx$. Mit dem Satz 3.4 für $\tau = \gamma = \delta$ erhalten wir folgende Formeln für s_x, s_y, s_z, s, m und ω:

$$\begin{aligned}
s_x &= \frac{(\ell+1)(2\,\delta^2\,\ell^2 + \delta^2\,\ell + 9\,\delta\,\ell + 12)}{12} \\
&= \frac{\delta^2\,\ell^3}{6}\left(1 + \mathcal{O}\left(\frac{1}{\ell}\right)\right), \\
s_y &= \frac{\delta(\ell+1)(\delta\,\ell + \delta + 1)(\delta\,\ell + \delta + 2)}{3} \\
&= \frac{\delta^3\,\ell^3}{3}\left(1 + \mathcal{O}\left(\frac{1}{\ell}\right)\right), \\
s_z &= \frac{\delta(\ell+1)(\delta\,\ell + \delta + 1)(\delta\,\ell + \delta + 2)}{6} \\
&= \frac{\delta^3\,\ell^3}{6}\left(1 + \mathcal{O}\left(\frac{1}{\ell}\right)\right)
\end{aligned}$$

sowie

$$\begin{aligned} s &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+9\delta\,\ell+12)}{12}, \\ m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2+5\,\delta^2\,\ell+9\,\delta\,\ell+12+3\,\delta^2+9\,\delta)}{12}, \\ \omega &= (\ell+2)(\delta+\delta\,\ell+1)^2. \end{aligned}$$

Außerdem gilt $s-1 \geq \frac{\delta^2\,\ell^3}{6}$. Mit diesen Formeln liefert Satz 3.4 die Bedingung

$$X^{\frac{\delta^2\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} Y^{\frac{\delta^3\,\ell^3}{3}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} Z^{\frac{\delta^3\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} < 2^{-\frac{m\,(4\,\omega+m+3)}{4}}\, W^{\frac{\delta^2\,\ell^3}{6}}.$$

Hieraus erhalten wir die Schranke

$$XY^{2\,\delta}Z^{\delta} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta^2\,\ell^3(1+\mathcal{O}(1/\ell))}}\, W^{\frac{1}{1+\mathcal{O}(1/\ell)}}.$$

Der Exponent von W lässt sich analog zum Beweis von Satz 5.1 durch $1-\mathcal{O}\left(\frac{1}{\ell}\right)$ abschätzen, was folgende Bedingung liefert:

$$XY^{2\,\delta}Z^{\delta} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, W^{1-\mathcal{O}\left(\frac{1}{\ell}\right)}. \tag{5.11}$$

Wir können eine obere Schranke für x_0 angeben, da wir $f(y,z)$ modulo N reduzieren:

$$\begin{aligned} |x_0| &\leq \frac{|f_N(y_0,z_0)|}{N} \\ &\leq \sum_{j=0}^{\delta}\sum_{k=0}^{j} Y^j Z^k \\ &\leq \frac{(\delta+1)(\delta+2)}{2} Y^{\delta}\,Z^{\delta}. \end{aligned}$$

Setzen wir nun $X = \frac{(\delta+1)(\delta+2)}{2} Y^{\delta}\,Z^{\delta}$, dann gilt $W = \|p(xX,yY,zY)\|_{\infty} = NX$. Damit ergibt sich aus (5.11) die Bedingung

$$Y^{2\,\delta}Z^{\delta} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta^2\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, N^{1-\mathcal{O}\left(\frac{1}{\ell}\right)}\, X^{-\mathcal{O}\left(\frac{1}{\ell}\right)}.$$

Weiterhin gilt $Y, Z \leq N$, da es sich hierbei um Schranken für die Nullstellen eines modularen Polynoms handelt. Dann erhalten wir mit $X = \frac{(\delta+1)(\delta+2)}{2} Y^{\delta}\,Z^{\delta} \leq \frac{(\delta+1)(\delta+2)}{2} N^{2\delta}$ wir die folgende Schranke

$$Y^{2\,\delta}Z^{\delta} < 2^{-\left(\frac{25}{24}\delta^2\,\ell^3+\mathcal{O}(\delta^2\,\ell^2)\right)}\, N^{1-\mathcal{O}\left(\frac{\delta}{\ell}\right)}.$$

Aus der vorherigen Bedingung ergibt sich

$$Y^2 Z < 2^{-\left(\frac{25}{24}\delta\,\ell^3+\mathcal{O}(\delta\,\ell^2)\right)\, N^{\frac{1}{\delta}} - \mathcal{O}\left(\frac{1}{\ell}\right)}. \tag{5.12}$$

Wenn wir $\varepsilon = \lfloor 1/\ell \rfloor$ setzen, liefert (5.12) die gewünschte Schranke

$$Y^2 Z < 2^{-\left(\frac{25\,\delta}{24\,\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right) N^{\frac{1}{\delta}}} N^{-\mathcal{O}(\varepsilon)}. \tag{5.13}$$

Somit erhalten wir einen Algorithmus zur Nullstellensuche. Mit diesem Algorithmus können nun alle Nullstellen (y_0, z_0) mit $|y_0| < Y$ und $|z_0| < Z$ in Laufzeit polynomiell in $(\log W, \delta, \frac{1}{\varepsilon})$ gefunden werden, sofern die Schranken Y und Z der Bedingung (5.13) genügen. Analog zum Beweis von Satz 5.1 kann gezeigt werden, dass $\log W$ polynomiell in $\log N$ ist. Für ein festes $\varepsilon > 0$ ist die Laufzeit somit polynomiell in $(\log N, \delta)$. □

Auch hier lässt sich ähnlich wie im Satz 5.3 das Ergebnis verbessern, indem wir durch zusätzliche z-Shifts die Menge S und somit das Gitter L vergrößern, während die Determinate des Gitters L verhältnismäßig klein bleibt. Wiederum stellen wir eine Bedingung an α und β, die sicherstellt, dass unser Parameterwert bei der Konstruktion der zulässigen Mengen S und M nicht negativ ist.

Satz 5.6
Es sei $f(y,z) = \sum_{j=0}^{\delta} \sum_{k=0}^{j} f_{jk} y^j z^k \in \mathbb{Z}[y,z]$ *ein irreduzibles Polynom. Es seien* $Y = N^\alpha$, $Z = N^\beta \in \mathbb{N}$ *mit* $\alpha, \beta \in (0,1)$ *und*

$$\alpha + \beta \leq \frac{1}{\delta}. \tag{5.14}$$

Dann können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$, *die*

$$f(y_0, z_0) \equiv 0 \mod N \quad \textit{mit } |y_0| \leq Y, |z_0| \leq Z$$

erfüllen, in Zeit polynomiell in $\log N$ *und* δ *gefunden werden unter der Voraussetzung, dass für ein* $\varepsilon \in (0,1]$

$$N^{(3\,\alpha+\beta)(\delta\,\beta+2-\delta\,\alpha)} < 2^{-\left(\frac{(4\,\alpha^2\,\delta+2\,\beta)\,\delta+4}{\beta\,\varepsilon^3} + \mathcal{O}\left(\frac{(\alpha+\beta)\,\delta^2+\delta}{\beta\,\varepsilon^2}\right)\right) N^{\frac{3}{\delta}} N^{-\mathcal{O}\left(-\frac{\delta\,\alpha+\delta\,\beta-1}{\delta}\varepsilon\right)}}$$

gilt.

Beweis: Erneut betrachten wir den bivariaten modularen Fall $f(y,z) \equiv 0 \mod N$ als trivariaten Fall über $\mathbb{Z}$. Es sei

$$p(x,y,z) := f_N(y,z) - Nx = 0$$

über $\mathbb{Z}$, wobei $f_N(y,z) = f(y,z) \mod N$. Das bessere Ergebnis im Vergleich zu Satz 5.5 erzielen wir, indem wir die ursprüngliche Shift-Menge S und dementsprechend auch M durch zusätzliche z-Shift erweitern. Aus Konstruktion 4.14 erhalten wir mit $\lambda = 1$ die Mengen

$$S \;=\; \left\{ x^i y^j z^k \mid 0 \leq i \leq \ell, 0 \leq j \leq \delta\,(\ell - i), 0 \leq k \leq j + \eta\ell \right\}$$

und

$$M \;=\; \Big\{x^i y^j z^k \mid 0 \le i \le \ell+1, 0 \le j \le \delta\,(\ell+1-i), 0 \le k \le j+\eta\ell\Big\}.$$

Die Definitionen aus Satz 3.4 mit $\tau = \delta$ sowie $\gamma = \delta + \eta$ liefern uns

$$\begin{aligned}
s_x &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+9\,\delta\,\ell+12+6\,\eta\,\delta\,\ell^2+12\,\eta\,\ell)}{12}\\
&= \frac{(\delta^2+3\,\eta\,\delta)\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right),\\
s_y &= \frac{\delta(\ell+1)(\delta\,\ell+\delta+1)(2\,\delta\,\ell+2\,\delta+4+3\,\eta\,\ell)}{6}\\
&= \frac{(2\,\delta^3+3\,\delta^2\,\eta)\,\ell^3}{3}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right),\\
s_z &= \frac{\delta\,(\ell+1)(\delta^2\,\ell^2+3\,\eta\,\delta\,\ell^2+2\,\delta^2\,\ell+3\,\delta\,\ell+\delta^2+3\,\eta\,\ell\,\delta+6\,\eta\,\ell+3\,\eta^2\,\ell^2+3\,\delta+2)}{6}\\
&= \frac{(\delta^3+3\,\delta^2\,\eta+3\,\delta\,\eta^2)\,\ell^3}{6}\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)
\end{aligned}$$

sowie

$$\begin{aligned}
s &= \frac{(\ell+1)(2\,\delta^2\,\ell^2+\delta^2\,\ell+12\,\eta\,\ell+6\,\eta\,\delta\,\ell^2+9\,\delta\,\ell+12)}{12},\\
m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2+5\,\delta^2\,\ell+9\,\delta\,\ell+6\,\delta\,\eta\,\ell^2+12\,\eta\,\ell+6\,\eta\,\delta\,\ell+12+3\,\delta^2+9\,\delta)}{12},\\
\omega &= (\ell+2)(\delta+\delta\,\ell+1)(\delta+(\delta+\eta)\,\ell+1).
\end{aligned}$$

Weiterhin gilt $s-1 \ge \frac{(\delta^2+3\,\eta\,\delta)\,\ell^3}{6}$. Mit diesen Formeln für s_x, s_y, s_z, s, m und ω erhalten wir aus Satz 3.4 folgende Bedingung

$$\begin{aligned}
X^{\frac{\delta^2+3\,\eta\,\delta}{6}\ell^3\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} Y^{\frac{3\,\delta^2\,\eta+2\,\delta^3}{6}\ell^3\left(1+\mathcal{O}\left(\frac{1}{\ell}\right)\right)} Z^{\frac{3\,\delta^2\,\eta+3\,\delta\,\eta^2+\delta^3}{6}\ell^3(1+\mathcal{O}(1/\ell))}&\\
< 2^{-\frac{m\,(4\,\omega+m+3)}{4}}\, W^{\frac{\delta^2+3\,\eta\,\delta}{6}\ell^3}&.
\end{aligned}$$

Daraus folgt mit der Abschätzung $\frac{1}{1+x} \ge 1-x$ für $x > 0$:

$$X^{\delta+3\,\eta} Y^{3\,\delta\,\eta+2\,\delta^2} Z^{3\,\delta\,\eta+3\,\eta^2+\delta^2} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, W^{(\delta+3\,\eta)\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}. \qquad (5.15)$$

Da wir Polynome der gleichen Form wie in Satz 5.5 betrachten, ist $X = \frac{(\delta+1)(\delta+2)}{2} Y^\delta\, Z^\delta$ eine obere Schranke für die Größe von x_0. Dann gilt $W = \|p(xX, yY, zY)\|_\infty = NX$. Somit erhalten wir aus (5.15) die Bedingung

$$\begin{aligned}
Y^{3\,\delta\,\eta+2\,\delta^2} Z^{3\,\delta\,\eta+3\,\eta^2+\delta^2} &< 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\, N^{(\delta+3\,\eta)\left(1-\mathcal{O}\left(\frac{1}{\ell}\right)\right)}\\
&\quad\cdot\left(\frac{(\delta+1)(\delta+2)}{2}(YZ)^\delta\right)^{-(\delta+3\,\eta)\mathcal{O}\left(\frac{1}{\ell}\right)}
\end{aligned}$$

Weiterhin gilt $Y, Z \le N$. Dies liefert die Schranke:

$$Y^{3\,\delta\,\eta+2\,\delta^2} Z^{3\,\delta\,\eta+3\,\eta^2+\delta^2} \;<\; 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}-(\delta+3\,\eta)\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right)} N^{(\delta+3\,\eta)\left(1-\mathcal{O}\left(\frac{\delta}{\ell}\right)\right)}.$$

Mit $Y = N^{\alpha}$ und $Z = N^{\beta}$ erhalten wir die Bedingung

$$N^{\alpha\,(3\,\delta\,\eta+2\,\delta^2)+\beta\,(3\,\delta\,\eta+3\,\eta^2+\delta^2)} < 2^{-\frac{3\,m\,(4\,\omega+m+3)}{2\,\delta\,\ell^3}-(\delta+3\,\eta)\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right)} N^{(\delta+3\,\eta)\left(1+\mathcal{O}\left(\frac{\delta}{\ell}\right)\right)}.$$

Wir setzen nun $\eta = -\frac{\delta\,\alpha+\delta\,\beta-1}{2\,\beta}$. Es gilt dann $\eta \geq 0$, da $\alpha + \beta \leq \frac{1}{\delta}$ und wir erhalten die Schranke

$$N^{(3\,\alpha+\beta)(\delta\,\beta+2-\delta\,\alpha)} < 2^{-\frac{4\,\alpha^2\,\delta^2+2\,\beta\,\delta+4}{\beta}\ell^3 - \mathcal{O}\left(\frac{(\alpha+\beta)\,\delta^2+\delta)}{\beta}\ell^2\right)} N^{\frac{3}{\delta}}\, N^{-\mathcal{O}\left(-\frac{\delta\,\alpha+\delta\,\beta-1}{\delta\,\ell}\right)}. \tag{5.16}$$

Wir setzen nun $\ell = \lfloor 1/\varepsilon \rfloor$ in (5.16). Dies liefert die gewünschte Abschätzung

$$N^{(3\,\alpha+\beta)(\delta\,\beta+2-\delta\,\alpha)} < 2^{-\left(\frac{(4\,\alpha^2\,\delta+2\,\beta)\,\delta+4}{\beta\,\varepsilon^3} + \mathcal{O}\left(\frac{(\alpha+\beta)\,\delta^2+\delta}{\beta\,\varepsilon^2}\right)\right)} N^{\frac{3}{\delta}}\, N^{-\mathcal{O}\left(-\frac{\delta\,\alpha+\delta\,\beta-1}{\delta}\varepsilon\right)}. \tag{5.17}$$

Wir erhalten somit für α und β, welche die vorhergehende Bedingung (5.17) erfüllen, einen Algorithmus zur Nullstellensuche bei bivariaten modularen Polynomen mit Laufzeit polynomiell in $(\log W, \delta, \frac{1}{\varepsilon})$. Analog zu Satz 5.1 können wir zeigen, dass W polynomiell in N und somit $\log W$ polynomiell in $\log N$ ist. Da $\log W$ polynomiell in $\log N$ ist, ist für ein festes $\varepsilon > 0$ die Laufzeit also polynomiell in $(\log N, \delta)$. □

Nun haben wir für drei Formen gezeigt, dass sich der bivariate modulare Fall auf den trivariaten ganzzahligen Fall zurückführen lässt.

6 Angriff auf RSA

Die Methode von Coppersmith spielt in der Kryptanalyse des Kryptosystems RSA eine bedeutende Rolle. In diesem Kapitel stellen wir einige Angriffe auf das RSA-Verfahren mittels Nullstellenberechnung trivariater ganzzahliger Polynome vor. Dabei werden wir zeigen, dass es möglich ist, den geheimen Schlüssel d effizient zu berechnen, wenn bestimmte Kriterien erfüllt sind.

6.1 Eine kleine Einführung in RSA

Das asymmetrische Verschlüsselungsverfahren RSA wurde 1978 von Rivest, Shamir und Adleman entwickelt. Es ist das erste veröffentlichte asymmetrische Kryptosystem. RSA wird heute noch zur Verschlüsselung von Daten, welche über das Internet ausgetauscht werden, und zum Austausch von Codeschlüsseln für symmetrische Kryptosysteme verwendet.

Definition 6.1 (Kryptosystem)
Ein Kryptosystem ist ein 5*-Tupel* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, welcher die folgenden Bedingungen erfüllt:*

- $\mathcal{P}$ *ist eine endliche Menge von Klartexten.*
- $\mathcal{C}$ *ist eine endliche Menge von Chiffretexten.*
- $\mathcal{K}$ *ist eine endliche Menge von Schlüsseln.*
- *Zu jedem* $k \in \mathcal{K}$ *existiert eine Verschlüsselungsfunktion* $e_k \in \mathcal{E}$ *mit*

  $$e_k : \mathcal{P} \to \mathcal{C}$$

  und eine Entschlüsselungsfunktion $d_k \in \mathcal{D}$ *mit*

  $$d_k : \mathcal{C} \to \mathcal{P},$$

  sodass für alle $x \in \mathcal{P}$ *gilt:*

  $$d_k(e_k(x)) = x.$$

Bei einem asymmetrischen oder public-key Verschlüsselungsverfahren ist die Verschlüsselungsfunktion e_k bekannt. Sie ist der sogenannte öffentliche Schlüssel. Die Entschlüsselungsfunktion ist geheim. Dies hat den Vorteil, dass jeder eine beliebige Nachricht mit dem öffentlichen Schlüssel verschlüsseln und versenden kann. Jedoch nur der Empfänger, der in Besitz des geheimen Schlüssels ist und für den die Nachricht dementsprechend

bestimmt ist, kann sie entschlüsseln. Dabei sollen sowohl die Schlüssel als auch die Ver- und Entschlüsselungsfunktion effizient zu berechnen sein. Ein solches Verfahren ist RSA.

Das RSA-Verfahren operiert auf einem Ring $\mathbb{Z}_N$. Dabei ist $N \in \mathbb{N}$ ein ganze Zahl, welche aus zwei Primzahlen p und q zusammengesetzt ist, und $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ der Ring der ganzen Zahlen modulo N. Die Menge $\mathbb{Z}_N^* \subset \mathbb{Z}_N$ bezeichnet die Einheitengruppe des Rings $\mathbb{Z}_N$. Sie enthält alle Element aus $\mathbb{Z}_N$, die zu N teilerfremd sind. Das bedeutet, dass $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N \mid \mathrm{ggT}(N, x) = 1\}$ ist.

Die Eulersche φ-Funktion $\varphi(N)$ gibt die Anzahl der zu N teilerfremden Elemente in $\mathbb{Z}_N$, also die Anzahl der Elemente in $\mathbb{Z}_N^*$, an. Es gelten die folgenden Eigenschaften:

- $\varphi(p) = p - 1$ für eine Primzahl p.
- $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ für teilerfremde Zahlen $m, n \in \mathbb{N}$.

Nun können wir das RSA-Kryptosystem angeben.

Kryptosystem 6.2 (RSA-Verschlüsselungsverfahren)
Es sei $N = pq$, wobei p und q Primzahlen sind. Ferner seien $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$ und

$$\mathcal{K} = \{(N, p, q, e, d) \mid e, d \in \mathbb{Z}_{\varphi(N)}^* \text{ mit } ed \equiv 1 \mod \varphi(N)\}.$$

Dabei ist (N, e) der öffentliche Schlüssel und (p, q, d) der geheime Schlüssel.

Für die Nachricht $m \in \mathbb{Z}_N$ ist

$$c = m^e \mod N$$

die Verschlüsselung mit dem öffentlichen Schlüssel (e, N). Die Entschlüsselung von c mit dem geheimen Schlüssel d ist

$$c^d \mod N.$$

Der Korrektheit des RSA-Verschlüsselungssystems ergibt sich für $m \in \mathbb{Z}_N^*$ aus dem Satz von Euler. Mit dem Chinesischen Restsatz kann leicht gezeigt werden, dass für alle $m \in \mathbb{Z}_N$ die Entschlüsselung $c^d = m^{e\,d} \equiv m \mod N$ korrekt ist.

6.2 Angriff auf RSA bei kleinem geheimen Schlüssel

Im Jahr 1990 stellte Wiener [15] einen Angriff mittels Kettenbrüchen vor, bei dem der geheime Schlüssel d in polynomieller Zeit aus (N, e) berechnet werden kann, wenn $d < N^{1/4}$ gilt.

Satz 6.3 (Wiener)
Es sei (e, N) ein öffentlicher RSA-Schlüssel mit $N = pq$, wobei $q < p < 2q$ gilt. Außerdem gelte für $d \in \mathbb{Z}_{\varphi(N)}^*$ mit $ed = 1 \mod \varphi(N)$, dass $d < \frac{1}{3}N^{\frac{1}{4}}$. Dann kann d aus (e, N) in Zeit $\mathcal{O}((\log N)^2)$ berechnet werden.

Dieses Ergebnis verbessern Boneh und Durfee in [2]. Sie betrachten dazu ein Polynom $y(A+z)-1 \mod e$. Der geheime Schlüssel d kann aus den Nullstellen dieses Polynoms berechnet werden. Sie zeigen, dass mittels dieser Methode für $d < N^{0.284}$ der geheime Schlüssel d in Polynomialzeit ermittelt werden kann.

Wir betrachten nun diesen bivariaten modularen Fall als trivariaten ganzzahligen Fall und erhalten dasselbe Ergebnis wie Boneh und Durfee. Zunächst jedoch beschreiben wir, wie wir dieses Polynom aus der RSA-Schlüsselgleichung erhalten.

Im Folgenden betrachten wir ein RSA-Verschlüsselungsschema mit dem RSA-Modul N, wobei die Primzahlen p und q mit $N = pq$ von der gleichen Größenordnung sind. Das bedeutet, dass $q < p < 2q$ gilt.

Es sei (N, e) der öffentliche Schlüssel. Dann erfüllt der zugehörige geheime Schlüssel d die Äquivalenz $ed \equiv 1 \mod \varphi(N)$, wobei $\varphi(N) = (p-1)(q-1) = N - p - q + 1$ ist. Hierbei sind e und d im Allgemeinen beide kleiner als $\varphi(N)$. Aufgrund der Äquivalenz $ed \equiv 1 \mod \varphi(N)$ existiert eine ganze Zahl $y \in \mathbb{Z}$, sodass

$$ed + y(N + 1 - (p + q)) = 1 \tag{6.1}$$

gilt. Wir setzen nun $A = N + 1$ und $z = -(p + q)$, da uns p und q nicht bekannt sind. Dann gilt

$$y\,(A + z) \equiv 1 \mod e \tag{6.2}$$

Wir setzen $e = N^{\alpha}$ für ein $\alpha \in (0, 1)$. Da e und N von der gleichen Größenordnung sind, ist α eine Zahl nahe 1. Weiterhin nehmen wir an, dass der geheime Schlüssel $d < N^{\delta_0}$ mit $\delta_0 \in (0, 1)$ erfüllt.

Aus Gleichung (6.1) folgern wir:

$$|y| \leq \frac{|1 - ed|}{N + 1 - p - q} < \frac{e\,d}{\varphi(N)} \leq \frac{2\,e\,d}{N} < 2\,N^{\alpha+\delta_0-1} = 2e^{1+\frac{\delta_0-1}{\alpha}}$$

Da $q < p$ ist, gilt $q < \sqrt{N}$. Weiter folgt $p < 2\sqrt{N}$ aus $p < 2q$. Hieraus erhalten wir insgesamt die folgende Abschätzung für z:

$$|z| < 3N^{0,5} = 3e^{\frac{1}{2\,\alpha}}.$$

Da e und N von der gleichen Größenordnung sind, setzen wir $\alpha = 1$. Dann gilt

$$y\,(A + z) - 1 \equiv 0 \mod e \quad \text{mit } |y| < e_0^{\delta} \text{ und } |z| < e^{1/2}.$$

Daraus folgern wir das trivariate ganzzahlige Polynom:

$$p(x, y, z) = y(\,A + z) - 1 - ex.$$

Eine Nullstelle (x_0, y_0, z_0) des Polynoms $p(x, y, z)$ ist das Tripel $(d, k, -(p + q))$, wobei $ed + k\varphi(N) = 1$ gilt.

Das Newton-Polytop von $p(x, y, z)$ hat rechte untere Dreiecksform, deshalb wenden wir Satz 5.6 an. Wir beachten, dass in diesem Fall $e = N$ gilt, da wir $\alpha = 1$ gesetzt

haben. Dabei ist der Grad δ des Polynoms $p(x, y, z)$ gleich 1, $Y = e^{\delta_0} = N^{\delta_0}$ und $Z = e^{1/2} = N^{1/2}$. Damit erhalten wir die Bedingung:

$$N^{(3\,\delta_0+1/2)(2,5-\delta_0)} < N^3 2^{-\frac{25}{24\,\varepsilon^3}} - \mathcal{O}\left(\tfrac{1}{\varepsilon^2}\right) N^{\mathcal{O}(\delta_0\,\varepsilon)}.$$

Vernachlässigung der Terme niederer Ordnung sowie des Terms $2^{-\frac{25}{24\,\varepsilon^3}-\mathcal{O}\left(\frac{1}{\varepsilon^2}\right)} N^{\mathcal{O}(\delta_0\,\varepsilon)}$ liefert uns die Bedingung:

$$(3\,\delta_0 + \frac{1}{2})(\frac{5}{2} - \delta_0) < 3.$$

Daraus folgt direkt

$$\delta_0 < \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.284.$$

Wenn für den geheimen Schlüssel $d < N^{\delta_0}$ gilt, kann d aus dem öffentlichen Schlüssel (e, N) in Polynomialzeit berechnet werden. Da wir bei der Herleitung Terme niederer Ordnung vernächlässigt haben, muss nun $\delta_0 < 0.284 - \varepsilon$ gelten.

Satz 6.4
Es sei $N = pq$ ein RSA-Modul. Dabei seien p und q Primzahlen mit $q < p < 2p$. Außerdem gelte für einen geheimen Schlüssel d mit $ed \equiv 1 \mod \varphi(N)$, dass $d < N^{\delta_0}$ ist. Dann kann d in Polynomialzeit aus dem öffentlichen Schlüssel (e, N) berechnet werden, wenn für ein $\varepsilon > 0$

$$\delta_0 < \frac{7}{6} - \frac{\sqrt{7}}{3} - \varepsilon$$

gilt.

6.3 Angriffe auf RSA bei kleinem, teilweise bekannten geheimen Schlüssel

In diesem Abschnitt befassen wir uns mit zwei der in Arbeit von Ernst, Jochemsz, May und de Weger [8] vorgestellten Angriffe auf RSA. Hierbei betrachten wir zwei verschiedenen trivariate ganzzahlige Polynome f_{MSB1} und f_{MSB2}, die sich aus verschiedenen Darstellungen der RSA-Schlüsselgleichung ergeben. Der geheime Schlüssel d lässt sich jeweils effizient als Nullstelle dieser Polynome aus e und N berechnen, wenn d klein und teilweise bekannt ist.

Wir nehmen wie im Abschnitt 6.2 an, dass der RSA-Modul N aus zwei verschiedenen Primzahl p und q der gleichen Eingabegröße zusammen gesetzt ist. Die Eingabegröße von N sei gleich n, das heißt $n = \lceil \log N \rceil$. Da p und q von der gleichen Eingabegröße sind, gilt

$$p + q < 3N^{1/2}.$$

Ferner seien $e, d < \varphi(N)$, wobei e von der gleichen Eingabegröße wie N ist. Weiterhin ist βn die Eingabegröße von d für $\beta \in (0, 1)$. Außerdem sei k eine ganze Zahl, für welche

$$e\,d - 1 = k\,\varphi(N)$$

gilt. Dann können wir k folgendermaßen abschätzen

$$k = \frac{e\,d-1}{\varphi(N)} \leq \frac{e\,d}{\varphi(N)} \leq d \leq N^{\beta}.$$

Mit MSB (most significant bits) bezeichnen wir die führenden Bits der Binärdarstellung einer Zahl, also die höchstwertigen Bits einer Zahl.

Es seien nun die $(\beta-\alpha)\,n$ MSB von d dem Angreifer bekannt, wobei $0 < \alpha < \beta$ gilt. Dann lässt sich d darstellen als $d = \tilde{d} + d_0$, wobei

- $\tilde{d}$ die MSB von d bezeichnet, also die $(\beta-\alpha)\,n$ führenden Bits der Binärdarstellung von d, welche dem Angreifer bekannt sind, und
- d_0 die letzten α Bits der Binärdarstellung, also die nicht-signifikanten Bits von d bezeichnet, welche der Angreifer nicht kennt.

Dies bedeutet explizit, dass

$$d < N^{\beta} \text{ und } |d_0| = |d - \tilde{d}| < N^{\alpha}$$

gilt.

Angriff mit dem Polynom f_{MSB1}

Ziel dieses Angriffs ist es, den geheimen Schlüssel d effizient zu berechnen, während uns möglichst wenige der MSB bekannt sein müssen. Das heißt, wir wollen β maximieren, welches die Eingabegröße von d ist, und $(\beta-\alpha)\,n$, als Anzahl der bekannten MSB, minimieren. Die RSA-Schlüsselgleichung $e\,d-1 = k\,\varphi(N)$ lässt sich mittels des Wissens über die MSB von d nun folgendermaßen darstellen:

$$e\,(\tilde{d} - d_0) - 1 = k\,(N - (p+q-1)). \tag{6.3}$$

Dabei sind $d_0,\ k$ und $p+q-1$ nicht bekannt. Somit können wir aus (6.3) das Polynom

$$\begin{aligned} f_{MSB1}(x,y,z) &:= e\,(x+\tilde{d}) - 1 - y(-z+N) \\ &= e\,x - N\,y + y\,z + R \text{ mit } R = e\tilde{d} - 1 \end{aligned} \tag{6.4}$$

herleiten, welches die Nullstelle $(x_0, y_0, z_0) = (d_0, k, p+q-1)$ besitzt. Wir setzen nun $X = N^{\alpha}$, $Y = N^{\beta}$ und $Z = 3\,N^{1/2}$. Dann gilt $|x_0| < X$, $|y_0| < Y$ und $|z_0| < Z$.

Das Polynom $f_{MSB1}(x,y,z)$ ist trivariat, ganzzahlig und irreduzibel. Somit kann Satz 3.4 angewandt werden mit den Mengen

$$S = \left\{ x^i y^j z^k | 0 \leq i \leq \ell, 0 \leq j \leq \ell - i, 0 \leq k \leq j + \eta\ell \right\}$$

und

$$M = \left\{ x^i y^j z^k | 0 \leq i \leq \ell + 1, 0 \leq j \leq \ell + 1 - i, 0 \leq k \leq j + \eta\ell \right\},$$

wobei $\eta \in \mathbb{R}$ der zu optimierende Parameter ist. Die Wahl des Parameter $\ell \in \mathbb{N}$ hängt ähnlich wie im Beweis des Satzes 5.1 mit der gewünschten Güte der Schranken zusammen.

Diese Mengen erfüllen die im Satz 3.4 geforderte Eigenschaft. Weiterhin können wir zeigen, dass die Mengen S und M zulässig sind für $f_{MSB1}(x, y, z)$. Der Beweis erfolgt analog zum Beweis von Lemma 4.15 und wird hier nicht explizit aufgeführt.

Es ist jedoch zu beachten, dass das Polynom $f_{MSB1}(x, y, z)$ nicht aus einem bivariaten modularen Polynom, welches als trivariates ganzzahliges Polynom aufgefasst wird, hervorgeht und somit der Satz 5.6 nicht angewendet werden kann.

Wenden wir nun Satz 3.4 auf das Polynom $f_{MSB1}(x, y, z)$ und die Mengen S und M an. Dabei gilt $d_x = d_y = d_z = 1$, $\tau = 1$ und $\gamma = 1 + \eta$. Somit erhalten wir als Exponenten von X, Y und Z:

$$\begin{aligned} s_x &= \frac{(\ell+1)(2\,\ell^2+\ell+9\,\ell+12+6\,\eta\,\ell^2+12\,\eta\,\ell)}{12} \\ &= \frac{1+3\,\eta}{6}\ell^3+\frac{3\,\eta+2}{2}\ell^2+\frac{11+6\,\eta}{6}\ell+1, \\ s_y &= \frac{(\ell+1)(\ell+2)(2\,\ell+6+3\,\eta\,\ell)}{6} \\ &= \frac{2+3\,\eta}{6}\ell^3+\frac{3\,\eta+4}{2}\ell^2+\frac{3\,\eta+11}{3}\ell+3 \end{aligned}$$

und

$$\begin{aligned} s_z &= \frac{(\ell+1)(\ell^2+5\,\ell+3\,\eta\,\ell^2+9\,\eta\,\ell+3\,\eta\,\ell^2+6)}{6} \\ &= \frac{1+3\,\eta+3\,\eta^2}{6}\ell^3+\frac{4\,\eta+2+\eta^2}{2}\ell^2+\frac{9\,\eta+11}{6}\ell+1. \end{aligned}$$

Die Menge S enthält

$$\begin{aligned} s &= \frac{(2+\ell)\,(\ell+1)\,(\ell+3\,\eta\,\ell+3)}{6} \\ &\geq \frac{3\,\eta+1}{6}\ell^3+1 \end{aligned}$$

Elemente. Weiterhin gilt

$$m = \frac{(\,l+3)\,(2+\ell)\,(\ell+3\,\eta\,\ell+4)}{6}$$

und

$$\omega = (\ell+2)^2(\ell+\eta\,\ell+2).$$

Satz 3.4 besagt nun, dass alle Nullstellen (x_0, y_0, z_0) des Polynoms $f_{MSB1}(x, y, z)$, welche $|x_0| \leq X$, $|y_0| \leq Y$ und $|z_0| \leq Z$ erfüllen, in Polynomialzeit gefunden werden können unter der Voraussetzung, dass

$$X^{s_x+\ell}Y^{s_y+\tau\ell}Z^{s_z+\gamma\ell} < 2^{-\frac{m(4\omega+m+3)}{4}}W^{s-1}$$

gilt. Ignorieren wir nun alle Terme der Ordung $o(\ell^3)$ und den Term $2^{-\frac{m(4\omega+m+3)}{4}}$, so erhalten wir folgende Bedingung:

$$X^{\frac{1+3\,\eta}{6}\ell^3} Y^{\frac{2+3\,\eta}{6}\ell^3} Z^{\frac{1+3\,\eta+3\,\eta^2}{6}\ell^3} < W^{\frac{1+3\,\eta}{6}\ell^3}.$$

Daraus ergibt sich die Schranke

$$X^{1+3\,\eta} Y^{2+3\,\eta} Z^{1+3\,\eta+3\,\eta^2} < W^{1+3\,\eta}.$$

Nun setzen wir die Darstellung von $X,\ Y,\ Z$ in Abhängigkeit von N in die Ungleichung ein, dabei ignorieren wir die konstanten Faktoren. Es gilt außerdem

$$W = \|f_{MSB1}(xX, yY, zY)\| \geq NY = N^{1+\beta}.$$

Dies liefert die Bedingung

$$N^{\alpha(1+3\,\eta)} N^{\beta\,(2+3\,\eta)} N^{\frac{1}{2}(1+3\,\eta+3\,\eta^2)} < N^{(1+\beta)(1+3\,\eta)}.$$

Somit muss

$$\alpha + 3\,\alpha\,\eta + \beta - \frac{1}{2} - \frac{3}{2}\eta + \frac{3}{2}\eta^2 < 0$$

gelten. Die linke Seite der Ungleichung ist minimal für $\eta = \frac{1}{2} - \alpha$. Mit diesem Wert für η erhalten wir

$$\alpha < \frac{5}{6} - \frac{\sqrt{1+6\beta}}{3}.$$

Dies gibt uns in Abhängigkeit der Eingabegröße $\beta\,n$ des geheimen Schlüssels d eine obere Schranke an, wie viele der MSB der Angreifer kennen muss, um den geheimen Schlüssel d in Polynomialzeit berechnen zu können. Umgekehrt bedeutet das, wenn mindestens $\alpha\,n$ für $\alpha \geq \frac{5}{6} - \frac{\sqrt{1+6\beta}}{3}$ der nicht-signifikanten Bits unbekannt sind, lässt sich der geheime Schlüssel mit dieser Methode nicht in Polynomialzeit berechnen.

Der Angriff von Boneh und Durfee im Abschnitt 6.2 kann als Spezialfall dieses Angriffs gesehen werden. Dabei wird angenommen, dass die bekannten höchstwertigen Bits alle 0 sind.

Angriff mit dem Polynom f_{MSB2}

Kennt ein Angreifer $\tilde{d}$, die $(\beta-\alpha)n$ höchstwertigen Bits der Binärdarstellung von d, so kann er eine Approximation $\tilde{k}$ von $k \in \mathbb{Z}$ mit $ed - 1 = k\varphi(N)$ berechnen:

$$\tilde{k} = \frac{e\,\tilde{d} - 1}{N}.$$

Bezeichnen wir nun mit $k_0 = k - \tilde{k}$ den unbekannten Teil von k. Somit erhalten wir für k_0 diese Abschätzung:

$$\begin{aligned}
|k_0| &= |k - \tilde{k}| \\
&= \left| \frac{e\,d - 1}{\varphi N} - \frac{e\,\tilde{d} - 1}{N} \right| \\
&= \left| \frac{(e\,d - 1)N - (e\,\tilde{d} - 1)N - (e\,\tilde{d} - 1) + (e\,\tilde{d} - 1)(p+q)}{\varphi(N)\,N} \right| \\
&\leq \left| \frac{e\,(d - \tilde{d})}{\varphi N} \right| + \left| \frac{(p+q-1)(e\,\tilde{d} - 1)}{\varphi(N)\,N} \right| \\
&\leq \frac{e}{\varphi(N)} \left(|d - \tilde{d}| + \frac{|p+q-1||\tilde{d}|}{N} \right) \\
&\leq \underbrace{\frac{e}{\varphi(N)}}_{\leq 1} \left(N^{\alpha} + 3\,N^{\beta - \frac{1}{2}} \right) \\
&\leq 4\,N^{\gamma} \quad \text{mit } \gamma = \max\{\alpha, \beta - \frac{1}{2}\}
\end{aligned}$$

Mit diesem Wissen über die MSB von k können wir die RSA-Schlüsselgleichung folgendermaßen darstellen:

$$e\,(\tilde{d} + d_0) - 1 = (\tilde{k} + k_0)(N - (p + q - 1))$$

Somit hat das Polynom

$$f_{MSB2} := e\,x - N\,y + y\,z + \tilde{k}\,z + R \quad \text{mit } R := e\,\tilde{d} - 1 - \tilde{k}\,N$$

die Nullstelle $(x_0, y_0, z_0) = (d_0, k_0, p + q - 1)$. Dabei gilt in diesem Fall $|x_0| \leq X = N^{\alpha}$, $|y_0| \leq Y = 4\,N^{\gamma}$ und $|z_0| \leq Z = 3\,N^{\frac{1}{2}}$.

Das Polynom $f_{MSB2}(x, y, z)$ ist ein irreduzibles trivariates ganzzahliges Polynom, daher können wir Satz 3.4 anwenden.

Wir wählen die Mengen

$$S := \{x^i y^j z^k | 0 \leq i \leq \ell, 0 \leq j \leq \ell + \eta\ell - i, 0 \leq k \leq \ell - i\}$$

und

$$M := \{x^i y^j z^k | 0 \leq i \leq \ell + 1, 0 \leq j \leq \ell + 1 + \eta\ell - i, 0 \leq k \leq \ell + 1 - i\}.$$

Dann erhalten wir als Exponenten für X, Y und Z:

$$\begin{aligned}
s_x &= \frac{(\ell+1)(\ell+2)(2\,\ell + 3\,\eta\,\ell + 3)}{6} \\
&= \frac{1}{6}\left((2 + 3\,\eta)\,\ell^3 + (9 + 9\,\eta)\,\ell^2 + (13 + 6\,\eta)\,\ell + 6 \right), \\
s_y &= \frac{(\ell+2)(\ell + \eta\,\ell + 2)(\ell + \eta\,\ell + 1)}{2} \\
&= \frac{1}{6}\left(3\,(1+\eta)^2\,\ell^3 + (15 + 21\,\eta + 6\,\eta^2)\,\ell^2 + (24 + 18\,\eta)\,\ell + 12 \right)
\end{aligned}$$

und

$$\begin{aligned} s_z &= \frac{(\ell+1)(\ell+2)(\ell+\eta\,\ell+2)}{2} \\ &= \frac{1}{6}\left((3+3\,\eta)\,\ell^3+(15+9\,\eta)\,\ell^2+(24+6\,\eta)\,\ell+12\right). \end{aligned}$$

Die Menge S enthält

$$\begin{aligned} s &= \frac{(\ell+1)(\ell+2)(2\,\ell+3\,\eta\,\ell+3)}{6} \\ &= \frac{1}{6}\left((2+3\,\eta)\,\ell^3+(9+9\,\eta)\,\ell^2+(13+6\,\eta)\,\ell+6\right) \end{aligned}$$

Elemente und die Menge M enthält

$$m = \frac{(\ell+2)(\ell+3)(2\,\ell+3\,\eta\,\ell+5)}{6}$$

Elemente. Weiterhin gilt

$$\omega = (\ell+2)^2((1+\eta)\,\ell+2).$$

Nun können wir laut Satz 3.4 alle Nullstellen (x_0, y_0, z_0) des Polynoms f_{MSB2} mit $|x_0| \leq X$ $|y_0| \leq Y$ und $|z_0| \leq Z$ in polynomieller Zeit finden, wenn

$$X^{s_x+\ell}Y^{s_y+\tau\ell}Z^{s_z+\gamma\ell} < 2^{-\frac{m\,(4\,\omega+m+3)}{4}}W^{s-1}$$

gilt. Vernachlässigen der Termen der Ordnung $o(\ell^3)$ und des Terms $2^{-\frac{m\,(4\,\omega+m+3)}{4}}$ liefert die Ungleichung

$$X^{2+3\,\eta}Y^{3\,(1+\eta)^2}Z^{3+3\,\eta} < W^{2+3\,\eta}$$

Dabei gilt $X = N^{\alpha},\ Y = 4\,N^{\gamma}$ mit $\gamma = \max\{\alpha, \beta - \frac{1}{2}\},\ Z = 3\,N^{\frac{1}{2}}$ und

$$W = \max\{eX, NY, YZ, \tilde{k}Z, R\} \geq NY = 4\,N^{1+\gamma}.$$

Setzen wir diese Grenzen ein, wobei wir die konstanten Faktoren vernachlässigen, liefert dies:

$$N^{\alpha(2+3\,\eta)}N^{3\,\gamma\,(1+\eta)^2}N^{\frac{1}{2}(3+3\,\eta)} < N^{(1+\gamma)(2+3\,\eta)}.$$

Somit muss

$$3\,\gamma\,\eta^2 + (3\,\alpha+3\,\gamma-\frac{3}{2})\eta - \frac{1}{2} + 2\,\alpha + \gamma < 0$$

gelten. Für $\eta := \frac{1-2\,\gamma-2\,\alpha}{4\,\gamma}$ wird die linke Seite der Ungleichung minimal und wir erhalten:

$$\alpha < \frac{1}{2} + \frac{\gamma}{3} - \frac{\sqrt{6\,\gamma+4\,\gamma^2}}{3} \tag{6.5}$$

Gelte nun $\gamma = \alpha$. Das bedeutet, dass $\alpha \geq \beta - 1/2$ gilt. Dann liefert uns (6.5)

$$\begin{aligned} \alpha &< \frac{1}{2} + \frac{\alpha}{3} - \frac{\sqrt{6\,\alpha+4\,\alpha^2}}{3} \\ \Leftrightarrow \alpha &< \frac{3}{16} \end{aligned}$$

Dementsprechend gilt dann $\beta \leq \frac{11}{16}$.

Für $\gamma = \beta - \frac{1}{2}$ erhalten wir mit (6.5)

$$\alpha < \frac{1}{3} + \frac{\beta}{3} - \frac{\sqrt{4\,\beta^2 + 2\,\beta - 2}}{3}$$

In diesem Fall gilt $\beta > \frac{11}{16}$, da $\beta - \frac{1}{2} \geq \alpha$ gilt.

Fassen wir nun alle Ergebnisse diese Abschnitts zusammen.

Satz 6.5
Es sei $N = pq$ ein RSA-Modul der Eingabegröße n. Es seien p und q Primzahlen der gleichen Größenordnung. Es gelte $0 < \alpha < \beta < 1$. Weiterhin sei e der öffentliche Schlüssel und d der geheime Schlüssel im RSA-Verfahren. Dabei sei e von der gleichen Eingabegröße wie der RSA-Modul N und es sei $d < N^{\beta}$. Sind nun dem Angreifer die $(\beta - \alpha)\,n$ MSB des geheimen Schüssels d bekannt, kann er diesen in polynomieller Zeit berechnen, falls

- $\alpha < \frac{5}{6} - \frac{\sqrt{1+6\,\beta}}{3} - \varepsilon$,
- $\alpha < \frac{3}{16} - \varepsilon$ *und* $\beta \leq \frac{11}{16}$ *oder*
- $\alpha < \frac{1}{3} + \frac{\beta}{3} - \frac{\sqrt{4\,\beta^2+2\,\beta-2}}{3} - \varepsilon$ *und* $\beta > \frac{11}{16}$

gilt.

Die um ε schlechteren Schranken im Vergleich zu den angebenen Herleitungen ergeben aus der Vernachlässigung der Terme niederer Ordnung und des Terms $2^{-\frac{m\,(4\,\omega+m+3)}{4}}$.

Wir haben in diesem Kapitel drei Beispiele für Angriffe auf das RSA-Verfahren gesehen, bei denen die Methode von Coppersmith angewendet wird. Es gibt noch eine Vielzahl weiterer Angriffe dieser Form auf das Kryptosystem RSA. So können wir beispielsweise ein RSA-Schlüsselpaar (e, d) betrachten, bei dem dem Angreifer die niederwertigsten Bits bekannt sind [8].

Anhang A

Der Variablenwechsel

A.1 Der bivariate Fall

Der im Satz 3.2 beschrieben Algorithmus zur Suche kleiner Nullstellen setzt voraus, dass das konstante Glied p_{00} des Polynoms $p(x, y)$ von 0 verschieden ist. Im Fall $p_{00} = 0$ erhalten wir durch einen einfachen Wechsel der Variablen ein Polynom $p^*(x, y)$ mit $p^*_{00} \neq 0$. Dieser Variablenwechsel wird im Folgenden beschrieben.

Es sei $p(x, y)$ ein Polynom vom maximalen Grad d_x in x. Wir stellen $p(x, y)$ als

$$p(x, y) = a(x) \cdot x + b(x, y) \cdot y$$

dar, wobei $a(x)$ ein univariates Polynom vom Grad höchstens $d_x - 1$ ist. Da $p(x, y)$ irreduzibel ist, ist das Polynom $a(x)$ von 0 verschieden. Weiterhin existiert ein i mit $0 < i \leq d_x$, sodass $a(i) \neq 0$, da $\deg a \leq d_x - 1$. Dann ist $p^*(i, 0) \neq 0$. Wir setzen nun

$$p^*(x, y) := p(x + i, y).$$

Dann erhalten wir ein Polynom $p^*(x, y)$ mit $p^*_{00} \neq 0$. Falls (x_0, y_0) eine Nullstelle von $p^*(x, y)$ ist, so ist $(x_0 + i, y_0)$ eine Nullstelle von $p(x, y)$. Wir benutzen also $p^*(x, y)$ statt $p(x, y)$.

A.2 Der trivariate Fall

Wir betrachten nun ein trivariates irreduzibles ganzzahliges Polynom $p(x, y, z)$ mit $p_{000} = 0$. Da wir im Algorithmus, den uns Satz 3.4 liefert, benötigen, dass p_{000} invertierbar ist, nehmen wir ein Variablenwechsel vor, sodass wir ein Polynom $p^*(x, y, z)$ erhalten mit $p^*_{000} \neq 0$. Wir ersetzen dann im Beweis des Satzes 3.4 $p(x, y, z)$ durch $p^*(x, y, z)$. Der Variablenwechsel erfolgt im Wesentlichen ähnlich wie im bivariaten Fall.

Es sei $p(x, y, z)$ ein Polynom mit maximalem Grad d_x in x und d_y in y. Das Polynom $p(x, y, z)$ kann dargestellt werden als

$$p(x, y, z) = a(x) \cdot x + b_1(x, y) \cdot y + c(x, y, z) \cdot z,$$

wobei $\deg(a(x)) \leq d_x - 1$ und $\deg_y(b_1(x, y)) \leq d_y - 1$. Da $p(x, y, z)$ irreduzibel ist, ist das Polynom $a(x)$ oder das Polynom $b(x)$ von 0 verschieden. Wir unterscheiden nun diese beide Fälle.

1. Es sei $a(x) \neq 0$.

   Da $\deg(a(x)) \leq d_x - 1$, existiert ein $i, 0 < i \leq d_x$, mit $a(i) \neq 0$. Somit ist auch $p(i,0,0) \neq 0$. Wir setzen daher $p^*(x,y,z) := p(x+i,y,z)$, dann ist $p^*(0,0,0) \neq 0$.

2. Es sei $a(x) = 0$ und $b_1(x,y) \neq 0$.

   Schreibe
   $$b_1(x,y) = b_2'(x) \cdot x + b_2(x,y) \cdot y.$$
   Da $b_1(x,y) \neq 0$, ist $b_2'(x)$ oder $b_2(x,y)$ von 0 verschieden.

   (i) Es sei $b_2'(x) \neq 0$.

   Da $\deg b_2'(x) \leq d_x - 1$ ist, existiert ein i mit $0 < i \leq d_x$, sodass $b_2'(i) \neq 0$. Damit ist auch $p(i,1,0) \neq 0$. Wir setzen $p^*(x,y,z) := p(x+i,y+1,z)$, dann ist $p^*(0,0,0) \neq 0$.

   (ii) Es sei $b_2'(x) = 0$ und $b_2(x,y) \neq 0$.

   Dann können wir $b_2(x,y)$ erneut darstellen als $b_2(x,y) = b_3'(x) \cdot x + b_3(x,y) \cdot y$. Ist dann $b_3'(x) \neq 0$, verfahren wir wie im Fall (i). Gilt jedoch $b_3'(x) = 0$ und $b_3(x,y) \neq 0$, verfahren wir wie folgt.

   Wir beobachten, dass $\deg_y(b_1(x,y)) \leq d_y - 1$, $\deg_y(b_2(x,y)) \leq d_y - 2$ und $\deg_y(b_3(x,y)) \leq d_y - 3$ gilt. Wir können also sukzessiv $b_i(x,y)$ als
   $$b_i(x,y) = b_{i+1}'(x) \cdot x + b_{i+1}(x,y) \cdot y$$
   darstellen. Dabei gilt $b_{i+1}'(x) \neq 0$ oder $b_{i+1}(x,y) \neq 0$. Im Fall $b_{i+1}'(x) \neq 0$ können wir Fall (i) anwenden.

   Im Fall $b_{i+1}(x,y) \neq 0$ gilt nach höchstens d_y dieser Schritte, dass $\deg(b_{d_y}(x,y)) = 0$ ist. Also ist $b_{d_y}(x,y)$ ein Polynom in x vom Grad höchstens d_x. Dann existiert also ein i mit $0 \leq i \leq d_x$, sodass $b_{d_y}(i,y) = b_{d_y}(i) \neq 0$ gilt. Somit ist auch $p(i,1,0) \neq 0$. Wir setzen $p^*(x,y,z) := p(x+i,y+1,z)$, dann gilt $p^*(0,0,0) \neq 0$.

Anhang B

Abschätzung für den Exponenten von 2

B.1 Abschätzung für den Exponenten von 2 für die modulare linke untere Dreiecksform

In diesem Abschnitt wollen wir die Abschätzungen für den Exponenten von 2 im Satz 5.1 angeben. Zur Erinnerung:

Satz
Es sei $f(y,z) \in \mathbb{Z}[y,z]$ ein irreduzibles Polynom vom totalen Grad δ. Es seien Y und Z natürliche Zahlen, welche der Bedingung

$$YZ < 2^{-\left(\frac{25\delta}{24\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right) \cdot N^{\frac{1}{\delta}} - \mathcal{O}\left(\frac{\varepsilon}{\delta}\right)}$$

genügen für ein $\varepsilon \in (0,1]$. Dann können alle Paare $(y_0, z_0) \in \mathbb{Z}^2$, die

$$f(y_0, z_0) \equiv 0 \mod N \quad \textit{mit } |y_0| \leq Y,\ |z_0| \leq Z$$

erfüllen, in Zeit polynomiell in $\log N$ und δ gefunden werden.

Es gilt:

$$\begin{aligned} m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2 + 5\,\delta^2\,\ell + 9\,\delta\,\ell + 12 + 3\,\delta^2 + 9\,\delta)}{12} \\ &= \frac{2\,\delta^2\,\ell^3 + 9\,\delta^2\,\ell^2 + 9\,\delta\,\ell^2 + 12\,\ell + 13\,\delta\,\ell + 27\,\delta\,\ell + 24 + 6\,\delta^2 + 18\,\delta}{12}, \\ \omega &= (\ell+2)(\delta + \delta\,\ell + 1)^2 \\ &= 5\,\delta^2\,\ell + 4\,\delta^2\,\ell^2 + 6\,\delta\,\ell + \delta^2\,\ell^3 + 2\,\delta\,\ell^2 + \ell + 2\,\delta + 2\,\delta^2 + 4\,\delta + 2. \end{aligned}$$

Satz 3.4 liefert uns die Bedingung

$$X^{s_x+\ell} Y^{s_y+\tau\ell} Z^{s_z+\gamma\ell} < 2^{-\frac{m(4\omega+m+3)}{4}} W^{s-1}$$

Wir können nun den Exponenten von 2 folgendermaßen abschätzen:

$$\begin{aligned}\frac{m\,(4\,\omega+m+3)}{4} &= \frac{25}{144}\delta^4\,\ell^6+\left(\frac{55}{48}\delta^3+\frac{71}{48}\delta^4\right)\ell^5+\left(\frac{29655}{576}\delta^4+\frac{263}{32}\delta^3+\frac{185}{64}\delta^2\right)\ell^4\\ &\quad+\left(\frac{25}{8}\delta+\frac{563}{32}\delta^2+\frac{551}{24}\delta^3+\frac{899}{96}\delta^4\right)\ell^3\\ &\quad+\left(\frac{259}{16}\delta+\frac{999}{32}\delta^3+\frac{5413}{576}\delta^4+\frac{2481}{64}\delta^2+\frac{5}{4}\right)\ell^2\\ &\quad+\left(\frac{427}{16}\delta+\frac{73}{2}\delta^2+\frac{497}{24}\delta^3+\frac{79}{16}\delta^4+\frac{23}{4}\right)\ell\\ &\quad+\frac{199}{16}\delta^2+\frac{109}{8}\delta+\frac{43}{8}\delta^3+\frac{13}{2}+\frac{17}{16}\delta^4\end{aligned}$$

Im Beweis von Satz 5.1 potenzieren wir nun beide Seiten der Bedingung mit $\frac{6}{\delta^2\ell^3}(1+\mathcal{O}(1/\ell))$. Somit ergibt sich für den Exponenten von 2

$$\begin{aligned}\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3(1+\mathcal{O}(1/\ell))} &\leq \left(\frac{25}{24}\delta^2\,\ell^3+\left(\frac{71}{8}\delta^2+\frac{55}{8}\delta\right)\ell^2+\left(\frac{789}{16}\delta+\frac{2965}{96}\delta^2+\frac{555}{32}\right)\ell\right.\\ &\quad\left.+\frac{1689}{16}+\frac{75}{4\delta}+\frac{899}{16}\delta^2+\frac{551}{4}\delta+\mathcal{O}(\delta^2/\ell)\right)(1-\mathcal{O}(1/\ell))\\ &\leq \frac{25}{24}\delta^2\ell^3+16\delta^2\ell^2+98\delta^2\ell+319\delta^2+\mathcal{O}(\delta^2/\ell)\end{aligned}$$

Dann werden die Terme $2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\,\delta^2\,\ell^3}(1-\mathcal{O}(1/\ell))}$ und $\left(\frac{(\delta+1)(\delta+2)}{2}\right)^{-\mathcal{O}(1/\ell)}$ zusammengefasst. Es gilt

$$\left(\frac{(\delta+1)(\delta+2)}{2}\right)^{-\mathcal{O}(1/\ell)}=2^{-(\log((\delta+1)(\delta+2))-1)\mathcal{O}\left(\frac{1}{\ell}\right)}=2^{-\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right)}$$

Um die Abschätzung (5.3) zu erhalten wird nun mit $1/\delta$ potenziert. Dies liefert

$$\frac{25}{24}\delta\,\ell^3+16\,\delta\,\ell^2+98\,\delta\,\ell+319\,\delta+\mathcal{O}(\delta/\ell)+\mathcal{O}\left(\frac{\log(\delta)}{\delta\,\ell}\right)$$

als Exponenten von 2. Wird nun $\ell=\lfloor 1/\varepsilon\rfloor$ gesetzt erhalten wir den gewünschten Exponent

$$\frac{25\,\delta}{24\,\varepsilon^3}+\frac{16\,\delta}{\varepsilon^2}+\frac{98\,\delta}{\varepsilon}+319\,\delta+\mathcal{O}\left(\delta\,\varepsilon\right)+\mathcal{O}\left(\frac{\log(\delta)\,\varepsilon}{\delta}\right)=\frac{25\,\delta}{24\,\varepsilon^3}+\mathcal{O}\left(\frac{\delta^2}{\varepsilon^2}\right)$$

von 2.

Hierzu analog verläuft auch die Abschätzung des Exponenten von 2 für die modulare rechte untere Dreiecksform ohne zusätzliche Shifts (Satz 5.5). Daher wird diese Abschätzung nicht mehr explizit aufgeführt.

B.2 Abschätzung für den Exponenten von 2 für die modulare Rechtecksform ohne zusätzliche Shifts

Nun werden wir die Abschätzung des Exponenten von 2 im Satz 5.2 angeben. Zur Erinnerung:

Satz
Es sei $f(y,z) \in \mathbb{Z}[y,z]$ ein Polynom vom Grad δ in y und z. Es seien Y und Z natürliche Zahlen, welche für ein $\varepsilon \in (0,1]$

$$YZ < 2^{-\left(\frac{\delta}{\varepsilon^3} + \mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right)\right) N^{\frac{2}{3\delta}} - \mathcal{O}\left(\frac{\varepsilon}{\delta}\right)}$$

erfüllen. Dann können alle Nullstellen (y_0, z_0) modulo N des Polynoms $f(x,y)$ mit $|y_0| \leq Y,\ |z_0| \leq Z$ in Zeit polynomiell in $\log N$ und δ gefunden werden.

Der Exponent von 2 ist nach der Bedingung aus Satz 3.4 $-\frac{m\,(4\,\omega+m+3)}{4}$, wobei

$$\begin{aligned} m &= \frac{(\ell+2)(2\,\delta^2\,\ell^2+5\,\delta^2\,\ell+6\,\delta\,\ell+6+2\,\delta^2+6\,\delta)}{6} \\ &= \frac{2\,\delta^2\,\ell^3+9\,\delta^2\,\ell^2+6\,\delta\,\ell+6\,\ell+20\,\delta\,\ell+10\,\delta^2\,\ell+12+16\,\delta}{6} \end{aligned}$$

und

$$\begin{aligned} \omega &= (\ell+2)(\delta+\delta\,\ell+1)^2 \\ &= 5\,\delta^2\,\ell+4\,\delta^2\ell^2+6\,\delta\,\ell+\delta^2\,\ell^3+2\,\delta\,\ell^2+\ell+2\,\delta+4\,\delta+2 \end{aligned}$$

ist. Es gilt also

$$\begin{aligned} \frac{m\,(4\,\omega+m+3)}{4} &= \frac{13}{36}\delta^4\,\ell^6+\left(\frac{11}{6}\delta^3+\frac{37}{12}\delta^4\right)\ell^5+\left(\frac{491}{36}\delta^3+\frac{1465}{144}\delta^4+\frac{15}{4}\delta^2\right)\ell^4 \\ &\quad+\left(\frac{143}{6}\delta^2+\frac{7}{2}\delta+\frac{193}{12}\delta^4+\frac{346}{9}\delta^3\right)\ell^3 \\ &\quad+\left(\frac{451}{9}\delta^3+\frac{75}{4}\delta+\frac{5}{4}+\frac{433}{36}\delta^4+\frac{3929}{72}\delta^2\right)\ell^2 \\ &\quad+\left(\frac{65}{2}\delta+\frac{10}{3}\delta^4+\frac{260}{9}\delta^3+\frac{1873}{36}\delta^2+\frac{23}{4}\right)\ell \\ &\quad+\frac{148}{9}\delta+18\,\delta+\frac{16}{3}\delta^3+\frac{13}{2} \end{aligned}$$

Nun werden beide Seiten der Bedingung

$$X^{\frac{\delta^2\,\ell^3}{3}(1+\mathcal{O}(1/\ell))}(YZ)^{\frac{\delta^3\,\ell^3}{2}(1+\mathcal{O}(1/\ell))} < 2^{-\frac{m\,(4\,\omega+m+3}{4}} W^{\frac{\delta^2\,\ell^3}{3}}$$

mit $\frac{6}{\delta^2\,\ell^3(1+\mathcal{O}(1/\ell)}$ potenziert. Dies liefert den folgenden Exponenten von 2:

$$\begin{aligned}
\frac{6\,m\,(4\,\omega+m+3)}{4\delta^2\ell^3(1+\mathcal{O}(1/\ell))} &\leq \frac{6\,m\,(4\,\omega+m+3)}{4\delta^2\ell^3}(1-\mathcal{O}(1/\ell)) \\
&= \left(\frac{13}{6}\delta^2\,\ell^3+\left(11\,\delta+\frac{37}{2}\delta^2\right)\ell^2+\left(\frac{491}{6}\delta+\frac{1465}{24}\delta^2+\frac{45}{2}\right)\ell\right. \\
&\quad \left.+\,143+\frac{21}{\delta}+\frac{193}{2}\delta^2+\frac{692}{3}\delta+\mathcal{O}(\delta^2/\ell)\right)(1-\mathcal{O}(1/\ell)) \\
&\leq \frac{13}{6}\delta^2\,\ell^3+\left(11\delta+\frac{37}{2}\delta^2\right)\ell^2+\left(\frac{491}{6}\delta+\frac{1465}{24}\delta^2+\frac{45}{2}\right)\ell \\
&\quad +143+\frac{21}{\delta}+\frac{193}{2}\delta^2+\frac{692}{3}\delta+\mathcal{O}(\delta^2/\ell)
\end{aligned}$$

Dann fassen wir die Terme $2^{-\frac{6\,m\,(4\,\omega+m+3)}{4\delta^2\ell^3}(1-\mathcal{O}(1/\ell))}$ und $((\delta+1)^2)^{-\mathcal{O}(1/\ell)}$ zusammen. Da

$$((\delta+1)^2)^{-\mathcal{O}(1/\ell)} = 2^{-2\,\log(\delta+1)\cdot\mathcal{O}\left(\frac{1}{\ell}\right)} = 2^{-\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right)}$$

gilt, erhalten wir als Exponenten von 2:

$$\begin{aligned}
&-\left(\frac{13}{6}\delta^2\,\ell^3+\left(11\,\delta+\frac{37}{2}\delta^2\right)\ell^2+\left(\frac{491}{6}\delta+\frac{1465}{24}\delta^2+\frac{45}{2}\right)\ell\right. \\
&\left.+143+\frac{21}{\delta}+\frac{193}{2}\delta^2+\frac{692}{3}\delta+\mathcal{O}\left(\frac{\delta^2}{\ell}\right)+\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right)\right) \\
&\geq -\left(3\,\delta^2\,\ell^3+\mathcal{O}(\delta^2\,\ell^2)\right)
\end{aligned}$$

Um nun Abschätzung (5.6) zu erhalten wird in Beweis von Satz 5.2 mit $\frac{1}{3\,\delta}$ potenziert. Damit erhalten wir folgenden Exponenten für 2, welche wir weiter abschätzen.

$$\begin{aligned}
\frac{m(4\omega+m+3)}{2\delta^3\ell^3}+\mathcal{O}\left(\frac{\log(\delta)}{\ell}\right) &\leq \frac{13}{18}\delta\ell^3+\left(\frac{11}{3}+\frac{37}{6}\delta\right)\ell^2+\left(\frac{491}{18}+\frac{1465}{72}\delta+\frac{15}{2\delta}\right)\ell \\
&\quad +\frac{143}{3\delta}+\frac{7}{\delta}^2+\frac{193}{6}\delta+\frac{692}{9}+\mathcal{O}\left(\frac{\delta}{\ell}\right)+\mathcal{O}\left(\frac{\log(\delta)}{\delta\,\ell}\right) \\
&\leq \delta\ell^3+10\delta\ell^2+56\delta\ell+164\delta+\mathcal{O}\left(\frac{\delta}{\ell}\right)
\end{aligned}$$

Setzen wir nun $\ell=\lfloor 1/\varepsilon\rfloor$ liefert uns dies den gewünschten Exponenten von 2:

$$\frac{\delta}{\varepsilon^3}+\frac{10\delta}{\varepsilon^2}+\frac{56\delta}{\varepsilon}+164\delta+\mathcal{O}(\delta\varepsilon)=\frac{\delta}{\varepsilon^3}+\mathcal{O}\left(\frac{\delta}{\varepsilon^2}\right).$$

Anhang C

Literaturverzeichnis

[1] Blömer, J., and May, A. A tool kit for finding small roots of bivariate polynomials over the integers. In *Advances in Cryptology (Eurocrypt 2005)* (2005), vol. 3494 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 251–267.

[2] Boneh, D., and Durfee, G. Cryptanalysis of RSA with private key d less than $n^{0.292}$. *IEEE transactions on Information Theory 46* (2000), 1339–1349.

[3] Coppersmith, D. Finding a small root of a bivariate integer equation; factoring high bits known. In *Advances in Cryptology (Eurocrypt 1996)* (1996), vol. 1070 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 178–189.

[4] Coppersmith, D. Finding a small root of a univariate modular equation. In *Advances in Cryptology (Eurocrypt 1996)* (1996), vol. 1070 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 155–165.

[5] Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology 10* (1997), 223–260.

[6] Coppersmith, D. Finding small solutions to small degree polynomials. In *Cryptography and Lattice Conference (CaLC 2001)* (2001), vol. 2146 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 20–31.

[7] Coron, J.-S. Finding small roots of bivariate integer polynomial equations revisited. In *Advances in Cryptology (Eurocrypt 2004)* (2004), vol. 3027 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 492–505.

[8] Ernst, M., Jochemsz, E., May, A., and de Weger, B. Partial key exposure attacks on RSA up to full size exponents. In *Advances in Cryptology (Eurocrypt 2005)* (2005), vol. 3494 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 371–386.

[9] Gathen, J. v. z., and Gerhard, J. *Modern Computer Algebra*, 2nd ed. Cambridge University Press, 2003.

[10] Howgrave-Graham, N. Finding small roots of univariate modular equations revisited. In *Cryptography an Coding, (CaLC 2001)* (1997), vol. 2146 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 131–142.

[11] Lenstra, A., Lenstra, H. J., and Lovász, L. Factoring polynomials with rational coefficients. *Mathematische Annalen 261* (1982), 513–534.

[12] May, A. New RSA vulnerabilities using lattice reduction methods. Dissertation, Universität Paderborn, 2003.

[13] Mignotte, M. *Mathematics for Computer Algebra*. Springer-Verlag, 1992.

[14] Stinson, D. *Cryptography - Theory and Practice*. Chapman & Hall/CRC, 2002.

[15] Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory 36*, 3 (1990), 553–558.

[16] Yap, C. K. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, 2000.