Zur algebraischen Komplexität von Polynomen und ihren Vielfachen

Dissertation
zur Erlangung des akademischen Grades
des Doktors der Naturwissenschaften
an der Universität Konstanz
Fachbereich Mathematik und Statistik
vorgelegt von

Karin Halupczok

Konstanz,
den 19. März 2001

Zusammenfassung

Wir untersuchen konkrete Polynome $f \in \mathbb{C}[X]$, so daß alle Polynome $\neq 0$ aus dem Hauptideal $\mathbb{C}[X] \cdot f$ schwerberechenbar sind.

Polynome $f \in \mathbb{C}[X]$, die durch ihre Nullstellen gegeben sind, lassen sich dabei besonders gut behandeln. Unsere Methoden liefern aber auch sämtliche uns bekannten Beispiele schwerberechenbarer Polynome mit speziellen Koeffizienten. Wir geben auch konkrete Polynome durch ihre Koeffizienten an, so daß alle Vielfachen $\neq 0$ schwerberechenbar sind.

Wir zeigen ferner, daß es ein Polynom mit vergleichsweise kleinen ganzzahligen Koeffizienten bzw. Nullstellen gibt, dessen Vielfache $\neq 0$ alle schwerberechenbar sind. Der Beweis dazu ist nicht konstruktiv.

Danksagung

An dieser Stelle möchte ich mich bei Herrn Prof. Dr. W. Baur für seine sehr gute Betreuung und Unterstützung während der Entwicklung und Erstellung dieser Arbeit herzlich bedanken.

Im besonderen danke ich auch meinem Freund Immanuel Herrmann für das Korrekturlesen und für gute Vorschläge.

Hiermit möchte ich auch allen weiteren Personen danken, die mich in meinem „Dasein“ als Doktorandin unterstützt haben, vor allem dem Fachbereich Mathematik und Statistik der Universität Konstanz, insbesondere Herrn Prof. Dr. H.-J. Stoß und Herrn Prof. Dr. V. Strassen, und außerdem sämtlichen Freunden und Bekannten aus Konstanz, Freiburg, Karlsruhe, Tübingen, usw., darunter meinen Freunden aus Grips e. V.

Inhaltsverzeichnis

Notationen

$\mathbb{N}$	natürliche Zahlen inklusive 0
$\mathbb{N}_{\geq 1}$	natürliche Zahlen größer gleich 1
$\mathbb{Z}$	ganze Zahlen
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	Körper der rationalen, reellen bzw. komplexen Zahlen
log	Logarithmus zur Basis 2
$k[Y_1, \ldots, Y_n]$	Polynomring in den Unbestimmten $Y_1, \ldots, Y_n$ über dem Körper k
$\deg f$	(Total-)Grad des Polynoms $f \in k[Y_1, \ldots, Y_n]$
$\deg_{Y_i} f$	Grad des Polynoms $f \in k[Y_1, \ldots, Y_n]$ in Y_i
$\operatorname{wt} f$	Gewicht des Polynoms $f \in k[Y_1, \ldots, Y_n]$, definiert als Summe der Absolutbeträge der Koeffizienten von f
$L(f)$	Komplexität von $f \in k[X]$
$\operatorname{ggT}(f, g)$	größter gemeinsamer Teiler $\in k[X]$ der Polynome $f, g \in k[X]$
Mipo_x	Minimalpolynom $\in \mathbb{Q}[X]$ der über $\mathbb{Q}$ algebraischen Zahl $x \in \mathbb{C}$
$\det A$	Determinante der Matrix $A \in \mathbb{C}^{n \times n}$
$\lfloor x \rfloor$	größte ganze Zahl kleiner gleich x
$\lceil x \rceil$	kleinste ganze Zahl größer gleich x

1 Einleitung

Sei k ein unendlicher Körper. Wir behandeln die Berechnung rationaler Funktionen in $k(X)$ und benutzen dafür durchgängig das nichtskalare Berechnungsmodell, siehe Bürgisser et al. [4] und Strassen [15]; bei diesem Modell sind Multiplikationen und Divisionen mit Elementen des Körpers k kostenlos, ebenso beliebige Additionen und Subtraktionen. Was kostet, sind nichtskalare Multiplikationen und Divisionen.

Wir formalisieren dieses Berechnungsmodell mit Hilfe des Begriffs einer Berechnungsfolge folgendermaßen:

Ist X eine Unbestimmte, so ist eine *Berechnungsfolge* eine Folge rationaler Funktionen $g_1, \ldots, g_r \in k(X)$ mit folgender Eigenschaft: Für jede natürliche Zahl $i \in \{1, \ldots, r\}$ gibt es

$$u_i, v_i \in \sum_{1 \le j < i} k g_j + kX + k,$$

so daß $g_i = u_i \cdot v_i$ oder $g_i = \frac{u_i}{v_i}$ und $v_i \neq 0$ gilt. Die natürliche Zahl r heißt *Länge* der Berechnungsfolge und gibt den Kostenaufwand der Berechnung wieder.

Wir sagen, eine Berechnungsfolge $g_1, \ldots, g_r$ *berechnet* eine rationale Funktion $f \in k(X)$, falls

$$f \in \sum_{i=1}^{r} k g_i + kX + k$$

gilt. Die *Komplexität* von $f \in k(X)$ ist die kleinste Zahl $r \in \mathbb{N}$, für die es eine Berechnungsfolge der Länge r gibt, die f berechnet. Wir bezeichnen die Komplexität von f mit $L(f)$.

Wir behandeln in dieser Arbeit nur Polynome $f \in k[X]$ und deren Komplexität in diesem Modell.

Das Polynom X^n mit $n \geq 1$ hat beispielsweise die Komplexität $L(X^n) \leq 2 \log n$, und ein weiteres Beispiel ist das Polynom $f = \sum_{i=0}^{n} X^i$ für $n \geq 1$, es

hat die Komplexität $L(f) \leq 2 \log n + 2$. Denn es ist

$$\sum_{i=0}^{n} X^i = \frac{X^n \cdot X - 1}{X - 1},$$

und X^n läßt sich in höchstens $2 \log n$ Operationen berechnen, dazu kommt noch eine Multiplikation und eine Division.

Auch ohne Divisionen erhalten wir für dieses Polynom eine obere Komplexitätsschranke derselben Größenordnung: Unter Verwendung von

$$\sum_{i=0}^{2n} X^i = \sum_{i=0}^{n} X^i + X^n \cdot \left(\sum_{i=0}^{n} X^i - 1 \right)$$

erhält man rekursiv $L_{\text{divisionsfrei}}(f) \leq 3 \log n$.

Ist allgemein $n \geq 1$ der Grad eines Polynoms f, so gilt stets die untere Abschätzung

$$L(f) \geq \log n,$$

die wir die *Gradschranke* nennen, vgl. Bürgisser et al. [4].

Eine allgemeingültige obere Abschätzung für die Komplexität eines Polynoms f vom Grad $n \geq 1$ ist

$$L(f) \leq 2\sqrt{n},$$

vgl. ebenso Bürgisser et al. [4]. Dieses von Paterson und Stockmeyer stammende Resultat (die Autoren zeigen in [11] sogar $L(f) \leq \sqrt{2n} + C \log n$ für eine Konstante $C > 0$) werden wir in dieser Arbeit öfters benutzen.

Wir beschäftigen uns im weiteren nur mit unteren Komplexitätsschranken für Polynome.

Ein nützliches Hilfsmittel, das untere Schranken liefert, ist der sogenannte *Darstellungssatz*, den wir in Kapitel 2 beweisen. Dieser Satz taucht zuerst

bei STRASSEN [14] auf und wurde später von SCHNORR [12] verbessert. Die hier vorgestellte Version hat eine leicht verbesserte Gewichtsabschätzung gegenüber der im Buch von BÜRGISSER ET AL. [4].

Eine bekannte und leicht zu zeigende Folgerung des Darstellungssatzes ist, daß Zariski fastalle Polynome $f \in k[X]$ vom Grad n die Komplexität $L(f) > \sqrt{n} - 2$ haben. Das bedeutet, daß es ein Polynom $H \in k[Y_1, \ldots, Y_n]\backslash 0$ über k gibt, so daß $L(f) > \sqrt{n} - 2$ für alle $f = \sum_{i=0}^{n} a_i X^i$ mit $H(a_1, \ldots, a_n) \neq 0$ gilt.

Ziel ist es, konkrete Familien von Polynomen $(f_n)_{n\in\mathbb{N}}$, $\deg f = n$, anzugeben, so daß $L(f_n)$ nach unten in der Größenordnung besser als durch $\log n$, nämlich etwa durch $C\sqrt{n}$, $C\sqrt[3]{n}$ oder auch $C\sqrt{\frac{n}{\log n}}$ für eine Konstante $C > 0$ abgeschätzt werden kann. Solche Familien nennen wir *schwerberechenbar*, im Gegensatz zu den *leichtberechenbaren*. Ist klar, welche Familien von Polynomen gemeint sind, sprechen wir einfacher von Polynomen, die schwer- oder leichtberechenbar sind. Die beiden obigen Polynome X^n und $\sum_{i=0}^{n} X^i$ sind beispielsweise leichtberechenbar.

Nach dem Erwähnten sind Zariski fastalle Polynome schwerberechenbar, mit unterer Komplexitätsschranke $\sqrt{n} - 2$ von optimaler Größenordnung (wegen der oberen Schranke $2\sqrt{n}$ von PATERSON und STOCKMEYER). Jedoch bereitet es große Schwierigkeiten, spezielle schwerberechenbare Polynome explizit anzugeben. Die ersten Beispiele nannte STRASSEN 1974 in [14]. Seine Methoden liefern schwerberechenbare Polynome mit gewissen algebraischen Koeffizienten wie etwa $f = \sum_{i=1}^{n} \sqrt{p_i} X^i$, wobei p_i die i-te Primzahl bezeichnet, oder schwerberechenbare Polynome mit schnellwachsenden rationalen Koeffizienten wie etwa $f = \sum_{i=1}^{n} 2^{2^i} X^i$. Deren Komplexität ist in beiden Fällen nach unten beschränkt durch $C\sqrt{\frac{n}{\log n}}$ für eine Konstante $C > 0$.

Ein bislang ungelöstes Problem ist es, ein spezielles schwerberechenbares Polynom mit vergleichsweise kleinen ganzzahligen Koeffizienten anzugeben, obwohl sich zeigen läßt, daß die meisten Polynome vom Grad n mit Koeffizienten $\in \{0, 1\}$ schwerberechenbar sind (man vergleiche dazu STOSS [13]). Leichtberechenbare hingegen kann man unter diesen 0-1-Polynomen konkret angeben, wie etwa die obigen Polynome X^n und $\sum_{i=0}^{n} X^i$.

HEINTZ und MORGENSTERN beweisen in [7] einen Satz über die Komplexität von Polynomen, die durch ihre Nullstellen gegeben sind. Sie verwenden dazu Methoden aus der algebraischen Geometrie. Für $f = \prod_{i=1}^{n}(X - \sqrt{p_i})$, wobei p_i wie oben die i-te Primzahl bezeichnet, erhalten sie $L(f) \geq C\sqrt{\frac{n}{\log n}}$ mit einer Konstanten $C > 0$. Dieses spezielle Polynom behandelt auch BAUR in [2] mit einem Satz, der auf elementaren Methoden beruht. Für das Polynom $\prod_{i=1}^{n}(X - 2^{2^i})$ zeigen ALDAZ ET AL. in [1] ein ähnliches Ergebnis.

In dieser Arbeit interessieren wir uns für spezielle schwerberechenbare Polynome $f \in \mathbb{C}[X]$ derart, daß wir für die Komplexität aller Vielfachen $\neq 0$ von f, genauer für $\min\{L(fg)\,;\, 0 \neq g \in \mathbb{C}[X]\}$, eine untere Schranke beweisen können, normalerweise in Abhängigkeit des Grades von f. Wir behandeln also Polynome $\neq 0$ des von f erzeugten Hauptideals in $\mathbb{C}[X]$. In diesem Zusammenhang nennen wir den Grad von f stets s. Beispielsweise zeigen wir für hinreichend großes s und $f = \prod_{i=1}^{s}(X - 2^{2^i})$, daß $L(fg) \geq \frac{1}{16}\sqrt[3]{s}$ für alle $0 \neq g \in \mathbb{C}[X]$ gilt. Der genaue Wert der Konstanten $\frac{1}{16}$ spielt natürlich keine Rolle.

Es ist zu bemerken, daß bei genügend hohem Grad von g die Gradschranke, auf fg angewendet, eine solche untere Schranke für $L(fg)$, die nur von f abhängt, sicher übersteigt; für solche g ist diese untere Schranke für $L(fg)$ dann trivial. Interessant sind daher beispielsweise die Vielfachen fg, bei denen der Grad von g polynomial im Grad von f ist. Hier beweisen wir stets eine untere Schranke für $\min\{L(fg)\,;\, 0 \neq g \in \mathbb{C}[X]\}$, die insbesondere für $L(f)$ nichttrivial ist, und nennen diese eine nichttriviale untere Komplexitätsschranke für alle Vielfachen $\neq 0$ von f. Wir sprechen dann auch von schwerberechenbaren Vielfachen $\neq 0$.

Ergebnisse zu diesem Vielfachenproblem liefert auch MALAJOVICH in [10]. Er gibt dort Polynome an, die durch schnell wachsende Nullstellen gegeben sind, mit der Eigenschaft, daß in diesem Sinne auch alle Vielfachen $\neq 0$ schwerberechenbar sind. Er behandelt beispielsweise das Polynom $f = \prod_{i=1}^{s}(X - 2^{2^{si}})$ und erhält für jedes $g \in \mathbb{C}[X]\backslash 0$ die Abschätzung $L(fg) \geq C\sqrt{\frac{s}{\log D}}$ mit $D = \deg fg$ und einer Konstanten $C > 0$, also unter Berücksichtigung der Gradschranke $L(fg) \geq \max\left\{\log D, C\sqrt{\frac{s}{\log D}}\right\}$. Elimination von D lie-

fert leicht die Abschätzung $L(fg) \geq C' \sqrt[3]{s}$ für eine Konstante $C' > 0$. Dies ist die zugehörige untere Schranke des Problems in unserem Sinn, die nur von s abhängt.

Die Existenz schwerberechenbarer Polynome f mit der Eigenschaft, daß kein Vielfaches $fg \neq 0$ wesentlich schneller berechnet werden kann, ist nicht selbstverständlich. Man kann schwerberechenbare Polynome mit einem leicht zu berechnenden Vielfachen $\neq 0$ angeben: Beispielsweise sind die meisten Faktoren vom Grad d mit $\frac{1}{3}n \leq d \leq \frac{2}{3}n$ des Polynoms $X^n - 1$ schwerberechenbar, man vergleiche wiederum STOSS [13]. Ein gewisses Vielfaches $\neq 0$ eines solchen Faktors, nämlich das Vielfache $X^n - 1$, ist leichtberechenbar. Ein weiteres Beispiel: Es gibt Polynome mit symmetrischer Galoisgruppe, die leichtberechenbar sind, andererseits sind die meisten normierten Faktoren solcher Polynome schwerberechenbar. Dies ist ein Ergebnis von HEINTZ in [6], man vergleiche dazu auch LÖH [9].

Will man Vielfache von Polynomen betrachten, bietet sich die Untersuchung von Polynomen, die durch Nullstellen gegeben sind, an. Denn betrachten wir ein Polynom $\prod_{i=1}^{s}(X - x_i) \in \mathbb{C}[X]$ mit s (nicht notwendig verschiedenen) Nullstellen $x_1, \ldots, x_s \in \mathbb{C}$, so besitzt auch jedes Vielfache fg für $g \in \mathbb{C}[X]$ (mindestens) diese Nullstellen.

In Kapitel 3 zeigen wir den für diese Arbeit zentralen Satz 1, der besonders gut auf derartige Polynome beliebigen Grades mit gewissen s Nullstellen anwendbar ist, aber auch allerlei andere Anwendungen ermöglicht. Wir verwenden zum Beweis von Satz 1 nur elementare Methoden, das Siegelsche Lemma und den Darstellungssatz aus Kapitel 2.

Satz 1 ist dem Satz aus BAUR und HALUPCZOK [3] sehr ähnlich und nur geringfügig allgemeiner. Wie dort verwenden wir auch hier Satz 1 zur Konstruktion schwerberechenbarer Polynome, deren Vielfache $\neq 0$ ebenfalls schwerberechenbar sind. Diese Anwendungen behandeln wir in Kapitel 4. Die leichte Verallgemeinerung des Satzes 1 gegenüber der Version in [3] erlaubt verschiedenartige Anwendungen.

Wir fassen die Ergebnisse dieser Anwendungen im folgenden zusammen.

In Abschnitt 4.1 betrachten wir Polynome $f \neq 0$, die an gewissen algebraischen Stellen $x_1, \ldots, x_s \in \mathbb{C}$ hohen Grades rationale Werte, z. B. 0, annehmen. Dazu gehören insbesondere Polynome mit gewissen paarweise verschiedenen Nullstellen $x_1, \ldots, x_s$; diese sind von der Form $g \cdot \prod_{i=1}^{s}(X - x_i)$ mit $0 \neq g \in \mathbb{C}[X]$ beliebig. Deren Komplexität ist nach unten beschränkt durch $\frac{1}{8}\sqrt{s}$.

Schwerberechenbare Polynome, die an (genügend vielen) schnellwachsenden Stellen ganzzahlige Werte, z. B. 0, annehmen, untersuchen wir in Abschnitt 4.2. Dort erhalten wir speziell für $f = g \cdot \prod_{i=1}^{s}(X - 2^{2^{\lceil\sqrt{s}\rceil i}})$, wobei $0 \neq g \in \mathbb{C}[X]$ beliebig, die Komplexität $L(f) \geq \frac{1}{8}\sqrt{s}$, ebenso für $f = g \cdot \prod_{i=1}^{s}(X - 2^{2^{si}})$. Für diese Polynome erhalten wir also eine verbesserte untere Komplexitätsschranke gegenüber der von Malajovich in [10]. Für $f = g \cdot \prod_{i=1}^{s}(X - 2^{2^i})$ erhalten wir $L(f) \geq \frac{1}{16}\sqrt[3]{s}$, und für ein Polynom f mit $f(2^{2^i}) = 2^i$ für $i \in \{1, \ldots, s\}$, das also den Logarithmus an den Stellen $2^{2^1}, \ldots, 2^{2^s}$ interpoliert, die Abschätzung $L(f) \geq \frac{1}{32}\sqrt[3]{s}$.

Daß man auch die Komplexität von Polynomen mit gewissen Nullstellen $x_1, \ldots, x_s$ beliebigen Grades und deren Vielfache behandeln kann, zeigen wir in Abschnitt 4.3. Für das Polynom $f = \prod_{i=1}^{s}(X - \sqrt{p_i})$ beispielsweise, wobei p_i wiederum die i-te Primzahl bezeichnet, zeigen wir, daß $L(fg) \geq \frac{1}{5}\sqrt[3]{s}$ für alle $g \in \mathbb{C}[X]$ mit $g(-\sqrt{p_1}) \cdots g(-\sqrt{p_s}) \neq 0$ gilt. Für das Polynom $f \cdot \prod_{i=1}^{s}(X + \sqrt{p_i}) = \prod_{i=1}^{s}(X^2 - p_i)$ mit vergleichsweise kleinen ganzzahligen Koeffizienten läßt sich mit unserer Methode jedoch keine nichttriviale untere Komplexitätsschranke beweisen.

In Abschnitt 4.4 behandeln wir Polynome f, die an (genügend vielen) rationalen Stellen $y_1, \ldots, y_s$ algebraische Werte in linear disjunkten Körpern annehmen. Für diese gilt $L(f) \geq \frac{1}{5}\sqrt[3]{s}$. Für algebraische Werte hohen Grades erhalten wir sogar $L(f) \geq \frac{1}{8}\sqrt{s}$.

Für Polynome f, die an (genügend vielen) ganzzahligen Stellen $y_1, \ldots, y_s$ schnell wachsende Werte annehmen, erhalten wir in 4.5 nichttriviale untere Komplexitätsschranken. Beispiele dafür sind alle Polynome $f \in \mathbb{C}[X]$ mit $f(2^i) = 2^{2^i}$ für $i \in \{1, \ldots, s\}$, welche die Exponentialfunktion an den Stellen $2^1, 2^2, \ldots, 2^s$ interpolieren; für diese gilt $L(f) \geq \frac{1}{10}\sqrt[3]{s}$. Solche Schranken können wir auch für gewisse Vielfache fg oder Verkettungen $g \circ f$ dieser

Polynome f beweisen.

In 4.6 zeigen wir, daß unsere Methode auch wieder die bisher bekannten Beispiele für schwerberechenbare Polynome mit algebraischen oder schnell wachsenden Koeffizienten liefert.

Daß es auch möglich ist, nichttriviale Komplexitätsschranken für Vielfache $\neq 0$ von Polynomen mit konkreten Koeffizienten zu erhalten, zeigen wir in Kapitel 5. Dort stellen wir eine Variante von Satz 1 vor, die speziell für diesen Fall anwendbar ist. Ist f ein Polynom vom (hinreichend großen) Grad s mit gewissen algebraischen Koeffizienten hohen Grades, so gilt $L(fg) \geq \frac{1}{8}\sqrt{s}$ für $g \in \mathbb{C}[X]\backslash 0$ beliebig.

In Kapitel 6 zeigen wir für alle hinreichend großen s die Existenz eines Polynoms f vom Grad s mit vergleichsweisen kleinen ganzzahligen Koeffizienten und der Eigenschaft, daß jedes Vielfache $fg \neq 0$ eine nichtriviale untere Komplexitätsschranke besitzt. „Vergleichsweise klein“ bedeutet hier, daß die Koeffizienten des Polynoms f im Betrag durch $2^{\sqrt[3]{s}}$ beschränkt sind. Dieser Beweis ist nicht konstruktiv. Analog können wir für alle hinreichend großen s zeigen, daß es ein Polynom f vom Grad s mit s derart kleinen ganzzahligen Nullstellen und dieser Eigenschaft gibt, ebenfalls nicht konstruktiv. (Mehrfache Nullstellen sind dabei möglich.)

2 Der Darstellungssatz

Der Darstellungssatz ist ein wichtiges Hilfsmittel, um untere Schranken für die Komplexität von Polynomen in einer Variablen zu beweisen. Er wurde zuerst von STRASSEN [14] formuliert und später von SCHNORR [12] verbessert. Wir zeigen hier eine Version, die auf die von SCHNORR zurückgeht. Dabei halten wir uns im wesentlichen an den Beweis aus BÜRGISSER ET AL. [4], erhalten jedoch eine leicht verbesserte Gewichtsabschätzung.

Man untersucht eine generische Berechnungsfolge, bei der jeder möglicherweise vorkommene Skalar durch eine Unbestimmte Z_μ ersetzt wird. Es zeigt sich, daß sich alle in maximal r Schritten berechenbare Polynome durch Polynome beschreiben lassen, deren Koeffizienten feste Polynome Q_ν in den Unbestimmten Z_μ sind. Man nennt die Polynome Q_ν die *Darstellungspolynome* zu r. Ihre Koeffizienten sind ganzzahlig. Der Darstellungssatz formuliert die Existenz solcher Darstellungspolynome Q_ν, die gewissen Grad- und Gewichtsabschätzungen genügen.

Das *Gewicht* $\operatorname{wt} g$ eines Polynoms $g \in \mathbb{Q}[Y_1, \ldots, Y_m]$ ist definiert als die Summe der Absolutbeträge aller Koeffizienten von g. Das Gewicht wt ist subadditiv und submultiplikativ, d. h. für $g, h \in \mathbb{Q}[Y_1, \ldots, Y_m]$ gilt $\operatorname{wt}(g+h) \leq \operatorname{wt} g + \operatorname{wt} h$ und $\operatorname{wt}(g \cdot h) \leq (\operatorname{wt} g) \cdot (\operatorname{wt} h)$, wie man leicht mit Hilfe der Dreiecksungleichung des Absolutbetrages überprüfen kann. Der *Grad* $\deg g$ bezeichnet den Totalgrad des Polynoms $g \in \mathbb{Q}[Y_1, \ldots, Y_m]$.

Darstellungssatz. *Für jede ganze Zahl $r \geq 1$ gibt es Polynome $Q_0, Q_1, \cdots \in \mathbb{Z}[Z_1, \ldots, Z_{(r+2)^2}]$ mit:*

(i) $\deg Q_\nu \leq 2rn$ *für* $0 \leq \nu \leq n$ *und* $n \geq 2$.

(ii) $\operatorname{wt} Q_\nu \leq 4^{n^r}$ *für* $0 \leq \nu \leq n$ *und* $n \geq 6$.

(iii) Für alle Polynome $f \in k[X]$ vom Grad $\leq n \in \mathbb{N}_{\geq 1}$ über einem unendlichen Körper k mit $L(f) \leq r$ gilt: Für fast alle $\xi \in k$ (d. h. bis auf endlich viele Ausnahmen) gibt es $\eta_1, \ldots, \eta_{(r+2)^2} \in k$ mit

$$f(X + \xi) = \sum_{\nu=0}^{n} Q_\nu(\underline{\eta}) X^\nu.$$

In dem Buch von BÜRGISSER ET AL. [4] wird als obere Gewichtsschranke nur $2^{n^{2r}}$ statt 4^{n^r} bewiesen.

Wir zeigen zunächst ein Lemma, aus dem wir den Darstellungssatz dann leicht folgern können.

Lemma 1. *Für alle $i \in \mathbb{N}$ und alle $\nu \in \mathbb{N}_{\geq 1}$ gibt es Polynome $Q_{i,\nu} \in \mathbb{Z}[Z_1, Z_2, \ldots, Z_{i^2+2i}]$ mit folgenden Eigenschaften:*

(i) $\deg Q_{i,\nu} \leq (2i-1)\nu + 1$ *für* $i \geq 1$,

(ii) $1 + \sum_{j=0}^{i} \sum_{\mu=1}^{\nu} \operatorname{wt} Q_{j,\mu} \leq 4^{\nu^i}$ *für* $\nu \geq 4$,

(iii) Zu jeder Berechnungsfolge $g_1, \ldots, g_r$ über einem unendlichen Körper k gibt es zu fast allen $\xi \in k$ Elemente $\zeta_1, \ldots, \zeta_r, \eta_1, \ldots, \eta_{r^2+2r} \in k$ so, daß

$$g_i(X + \xi) = \zeta_i \left(1 + \sum_{\nu \geq 1} Q_{i,\nu}(\eta_1, \eta_2, \ldots, \eta_{i^2+2i}) X^\nu \right)$$

für $1 \leq i \leq r$ gilt.

Beweis: Wir definieren die $Q_{i,\nu}$ rekursiv bezüglich i durch

$$Q_{0,1} := 1, \qquad Q_{0,\nu} := 0 \text{ für } \nu > 1$$

und für festes $i \geq 1$ durch Koeffizientenvergleich in der Gleichung

$$\begin{aligned} 1 + \sum_{\nu \geq 1} Q_{i,\nu} X^\nu = & \left(1 + \sum_{0 \leq j < i} A_j \sum_{\nu \geq 1} Q_{j,\nu} X^\nu \right) \\ \cdot & \left(C \left(1 + \sum_{0 \leq j < i} B_j \sum_{\nu \geq 1} Q_{j,\nu} X^\nu \right) + (1 - C) \left(1 + \sum_{0 \leq j < i} B_j \sum_{\nu \geq 1} Q_{j,\nu} X^\nu \right)^{-1} \right) \end{aligned} \tag{2.1}$$

mit den Unbestimmten

$$C = Z_{i^2}, \qquad A_j = Z_{i^2+j+1}, \qquad B_j = Z_{i^2+i+j+1}, \qquad \text{für } 0 \leq j < i.$$

Die rechte Seite der Gleichung (2.1) ist eine Potenzreihe in X mit konstantem Term 1 und Koeffizienten in $\mathbb{Z}[Z_1, \ldots, Z_{i^2+2i}]$. Man beachte dabei, daß $(i-1)^2 + 2(i-1) = i^2 - 1$ ist.

Wir zeigen zunächst (iii) durch vollständige Induktion nach r.

Für $r = 0$ ist nichts zu zeigen, sei also $r > 0$. Gilt $g_r = 0$, so sei $\zeta_r := 0$, und die Induktionsvoraussetzung liefert die Behauptung.

Sei also $g_r \neq 0$, und $g_r = u_r \cdot v_r$ oder $g_r = \frac{u_r}{v_r}$ mit

$$u_r = \sum_{1 \leq j < r} \alpha_j g_j + \alpha_0 X + \alpha', \qquad v_r = \sum_{1 \leq j < r} \beta_j g_j + \beta_0 X + \beta'.$$

Nach Induktionsvoraussetzung gibt es für fast alle $\xi \in k$ Elemente $\zeta_1, \ldots, \zeta_{r-1}, \eta_1, \ldots, \eta_{(r-1)^2+2(r-1)} = \eta_{r^2-1} \in k$ mit

$$g_j(X + \xi) = \zeta_j \left(1 + \sum_{\nu \geq 1} Q_{j,\nu}(\underline{\eta}) X^\nu \right) \text{ für } 1 \leq j < r.$$

Fall 1: Sei $g_r = u_r \cdot v_r$. Gilt für $\xi \in k$ zusätzlich $g_r(\xi) \neq 0$ (dies ist für fast alle $\xi \in k$ der Fall), so folgt

$$\begin{aligned} g_r(X + \xi) &= u_r(X + \xi) \cdot v_r(X + \xi) \\ &= \left(u_r(\xi) + \sum_{0 \leq j < r} \alpha_j \zeta_j \sum_{\nu \geq 1} Q_{j,\nu}(\underline{\eta}) X^\nu \right) \cdot \left(v_r(\xi) + \sum_{0 \leq j < r} \beta_j \zeta_j \sum_{\nu \geq 1} Q_{j,\nu}(\underline{\eta}) X^\nu \right) \\ &= g_r(\xi) \left(1 + \sum_{0 \leq j < r} \frac{\alpha_j \zeta_j}{u_r(\xi)} \sum_{\nu \geq 1} Q_{j,\nu}(\underline{\eta}) X^\nu \right) \cdot \left(1 + \sum_{0 \leq j < r} \frac{\beta_j \zeta_j}{v_r(\xi)} \sum_{\nu \geq 1} Q_{j,\nu}(\underline{\eta}) X^\nu \right), \end{aligned}$$

wobei $\zeta_0 := 1$ sei.

Wir setzen $\zeta_r := g_r(\xi)$, $\eta_{r^2} := 1$, und

$$\eta_{r^2+j+1} := \frac{\alpha_j \zeta_j}{u_r(\xi)}, \qquad \eta_{r^2+r+j+1} := \frac{\beta_j \zeta_j}{v_r(\xi)} \qquad \text{für alle } 0 \leq j < r.$$

Es folgt wegen (2.1)

$$g_r(X + \xi) = \zeta_r \left(1 + \sum_{\nu \geq 1} Q_{r,\nu}(\underline{\eta}) X^\nu \right).$$

Fall 2: Sei $g_r = \frac{u_r}{v_r}$. Hier verfahren wir analog, setzen aber $\eta_{r^2} := 0$.

Nun zum Beweis von (i), der Gradabschätzung der $Q_{i,\nu}$.

Für formale Potenzreihen in X über einem Ring R gilt die Gleichung

$$\begin{aligned}\Big(1 - \sum_{\nu\geq 1} R_\nu X^\nu\Big)^{-1} &= 1 + \sum_{\rho\geq 1}\Big(\sum_{\nu\geq 1} R_\nu X^\nu\Big)^\rho \\ &= 1 + \sum_{\nu\geq 1}\Bigg(\sum_{\substack{\rho\geq 1\\ \nu_1+\cdots+\nu_\rho=\nu}} R_{\nu_1}R_{\nu_2}\cdots R_{\nu_\rho}\Bigg)X^\nu,\end{aligned}$$

wobei die $\nu_1, \ldots, \nu_\rho \in \mathbb{N}_{\geq 1}$ und die $R_\nu \in R$ sind.

Mit dieser Formel liefert ein Koeffizientenvergleich für festes $i \geq 1$ in (2.1) die Gleichung

$$Q_{i,\nu} = \sum_{\kappa+\mu=\nu} E_\kappa F_\mu \text{ für alle } \nu \geq 1,$$

wobei $E_0 = 1$ und $E_\kappa = \sum_{0\leq j<i} A_j Q_{j,\kappa}$ für $\kappa \geq 1$, sowie $F_0 = 1$ und

$$\begin{aligned}F_\mu =& C\sum_{0\leq j<i} B_j Q_{j,\mu} \\ &+(1-C)\sum_{\substack{\rho\geq 1\\ \mu_1+\cdots+\mu_\rho=\mu}}\Bigg(\Big(-\sum_{0\leq j<i} B_j Q_{j,\mu_1}\Big)\cdots\Big(-\sum_{0\leq j<i} B_j Q_{j,\mu_\rho}\Big)\Bigg)\end{aligned}$$

für $\mu \geq 1$.

Wir zeigen damit die Behauptung (i) mit vollständiger Induktion nach $i \geq 1$.

Für $i = 1$ ist $E_0 = 1$, $E_1 = A_0$, $E_\kappa = 0$ für $\kappa > 1$, da $Q_{0,1} = 1$ und $Q_{0,\nu} = 0$ für $\nu > 1$. Es folgt

$$Q_{1,\nu} = F_\nu + A_0 F_{\nu-1} \text{ für } \nu \geq 1.$$

Für $\mu \geq 1$ ist

$$\deg F_\mu \leq \max\{2, 1+\mu\} = 1+\mu,$$

und es folgt

$$\deg Q_{1,\nu} \leq \nu + 1 \text{ für } \nu \geq 1.$$

Für $i > 1$ und $\kappa \geq 1$ ist nach Induktionsvoraussetzung

$$\deg E_\kappa \leq 1 + (2(i-1)-1)\kappa + 1 = 2 - 2\kappa + (2i-1)\kappa \leq (2i-1)\kappa$$

und für $\mu \geq 1$ ebenso

$$\begin{aligned}\deg F_\mu &\leq \max\{1 + (2i-1)\mu + 2 - 2\mu, 1 + \mu + (2(i-1)-1)\mu + \mu\} \\ &\leq (2i-1)\mu + 1.\end{aligned}$$

Es folgt

$$\begin{aligned}\deg E_0 F_\nu &\leq (2i-1)\nu + 1, \\ \deg E_\nu F_0 &\leq (2i-1)\nu + 1,\end{aligned}$$

und für κ, μ mit $\kappa\mu \neq 0$, $\kappa + \mu = \nu$, folgt

$$\deg E_\kappa F_\mu \leq (2i-1)\nu + 1.$$

Nun zum Beweis von (ii), der Gewichtsabschätzung.

Mit der Abkürzung

$$G_{j,\nu} := \sum_{\mu=1}^{\nu} Q_{j,\mu} X^\mu$$

schreiben wir Gleichung (2.1) für ein festes $\nu \geq 2$ folgendermaßen:

$$\begin{aligned}1 + \sum_{\mu \geq 1} Q_{i,\mu} X^\mu = \Bigg(1 + \underbrace{\sum_{0 \leq j < i} A_j G_{j,\nu}}_{(*)}\Bigg) \cdot \Bigg(C\Bigg(1 + \sum_{0 \leq j < i} B_j G_{j,\nu}\Bigg) \\ + (1-C) \sum_{\sigma=0}^{\nu-1} (-1)^\sigma \Bigg(\sum_{0 \leq j < i} B_j G_{j,\nu} \Bigg)^\sigma \Bigg) \\ + (1-C)(-1)^\nu \Bigg(\sum_{0 \leq j < i} B_j G_{j,\nu} \Bigg)^\nu + P \cdot X^{\nu+1},\end{aligned} \tag{2.2}$$

wobei P eine geeignete formale Potenzreihen in X mit Koeffizienten aus $\mathbb{Z}[Z_1, \ldots, Z_{i^2+2i}]$ ist.

Zur Erklärung: Ausgehend von der Gleichung (2.1) wurde eine Umformung der Gestalt

$$\left(1 - \sum_{\nu \geq 1} R_\nu X^\nu\right)^{-1} = \sum_{\sigma \geq 0} \left(\sum_{\nu \geq 1} R_\nu X^\nu\right)^\sigma$$

durchgeführt. Der erste Summand in der dritten Zeile von (2.2) müßte zunächst innerhalb der großen Klammer der zweiten Zeile stehen. Bei Multiplikation dieses Summands mit dem Term (*) der ersten Zeile ist der resultierende Grad in X mindestens $\nu + 1$ (für $\nu \geq 2$), und daher „absorbieren“ wir dieses Ergebnis im Term $P \cdot X^{\nu+1}$. Bei Multiplikation des Summands mit der zweiten 1 der ersten Zeile erhalten wir ihn nocheinmal außerhalb der großen Klammer.

Wir setzen

$$S_{i,\nu} := 1 + \sum_{j=0}^{i} \sum_{\mu=1}^{\nu} \operatorname{wt} Q_{j,\mu}.$$

Es ist also $S_{0,\nu} = 1 + 1 = 2$ und

$$\operatorname{wt}\left(1 + \sum_{j=0}^{i-1} A_j \sum_{\mu=1}^{\nu} Q_{j,\mu} X^\mu\right) = S_{i-1,\nu}.$$

Letzteres gilt natürlich ebenso mit den Unbestimmten B_j anstelle von A_j.

Zu zeigen ist $S_{i,\nu} \leq 4^{\nu^i}$ für $\nu \geq 4$.

Wegen Subadditivität und Submultiplikativität von wt folgt aus (2.2) die Ungleichung

$$\begin{aligned} 1 + \operatorname{wt}\left(\sum_{\mu=1}^{\nu} Q_{i,\mu} X^\mu\right) &\leq S_{i-1,\nu}\left(S_{i-1,\nu} + 2\sum_{\sigma=0}^{\nu-1} S_{i-1,\nu}^\sigma\right) + 2S_{i-1,\nu}^\nu \\ &\leq S_{i-1,\nu}^2 + 2S_{i-1,\nu} \sum_{\sigma=0}^{\nu-2} S_{i-1,\nu}^\sigma + 2S_{i-1,\nu}^\nu + 2S_{i-1,\nu}^\nu \leq 7S_{i-1,\nu}^\nu, \end{aligned}$$

da $S_{i-1,\nu} \geq S_{0,\nu} = 2$ für $\nu \geq 2$.

Dies zeigt

$$S_{i,\nu} = 1 + \sum_{j=0}^{i} \sum_{\mu=1}^{\nu} \operatorname{wt} Q_{j,\mu} = 1 + \sum_{j=0}^{i-1} \sum_{\mu=1}^{\nu} \operatorname{wt} Q_{j,\mu} + \sum_{\mu=1}^{\nu} \operatorname{wt} Q_{i,\mu}$$

$$< S_{i-1,\nu} + 7S_{i-1,\nu}^{\nu} \leq 8S_{i-1,\nu}^{\nu}. \quad (2.3)$$

Setzen wir $\lambda_{i,\nu} := \log S_{i,\nu}$, so gilt $\lambda_{i,\nu} \leq 3 + \nu\lambda_{i-1,\nu}$, und $\lambda_{0,\nu} = \log S_{0,\nu} = 1$.

Wir bekommen induktiv $\lambda_{i,\nu} \leq 2\nu^i - 1$ für $\nu \geq 4$. Denn für $i = 0$ ist $\lambda_{0,\nu} = 1 \leq 2\nu^0 - 1$, und für $i > 0$ ist

$$\lambda_{i,\nu} \leq 3 + \nu\lambda_{i-1,\nu} \leq 3 + 2\nu^{i+1} - \nu \leq 2\nu^{i+1} - 1,$$

wobei in der letzten Ungleichung $\nu \geq 4$ benutzt wurde.

Es folgt $S_{i,\nu} = 2^{\lambda_{i,\nu}} \leq 2^{2\nu^i - 1} \leq 2^{2\nu^i} = 4^{\nu^i}$. □

Mit Hilfe des eben bewiesenen Lemmas zeigen wir nun den anfangs formulierten Darstellungssatz.

Beweis des Darstellungssatzes:
Wir setzen

$$Q_\nu(Z_1, \ldots, Z_{r^2+3r+2}) := \begin{cases} \sum_{j=1}^{r} Z_{r^2+2r+j} Q_{j,\nu}(Z_1, \ldots, Z_{j^2+2j}), & \text{für } \nu > 1, \\ \sum_{j=1}^{r} Z_{r^2+2r+j} Q_{j,\nu}(Z_1, \ldots, Z_{j^2+2j}) + Z_{r^2+3r+1}, & \text{für } \nu = 1, \\ Z_{r^2+3r+2}, & \text{für } \nu = 0. \end{cases}$$

Daraus folgt nach dem Lemma, Teil (i),

$$\deg Q_\nu \leq (2r-1)\nu + 2 \leq 2r\nu \leq 2rn$$

für $n \geq \nu \geq 2$. Ferner ist $\deg Q_0 = 1$ und $\deg Q_1 \leq 2r + 1 \leq 2rn$ für $n \geq 2$.

Ebenso folgt nach dem Lemma, Teil (ii), daß

$$\operatorname{wt} Q_\nu \leq 1 + \sum_{j=1}^{r} \operatorname{wt} Q_{j,\nu} \leq 4^{\nu^r} \leq 4^{n^r},$$

für $n \geq \nu \geq 4$. Für $\nu \in \{0, 1, 2, 3\}$ ist dies noch zu zeigen. Klar ist $\operatorname{wt} Q_0 = 1 \leq 4^{n^r}$.

Es gilt für $\nu \in \{1, 2, 3\}$ die Abschätzung

$$\operatorname{wt} Q_\nu \leq 1 + \sum_{j=1}^{r} \operatorname{wt} Q_{j,\nu} \leq S_{r,\nu} \leq 2^{\nu^r + 3\nu^{r-1} + \cdots + 3\nu + 3}$$

nach der Ungleichung (2.3) im Beweis des Lemmas.

Also ist $\operatorname{wt} Q_1 \leq 2^{1+3r} \leq 4^{n^r}$ und

$$\operatorname{wt} Q_\nu \leq 2^{\nu^r + 3\nu^r} = 2^{4\nu^r} \leq 4^{2 \cdot 3^r} \leq 4^{n^r}$$

für $\nu = 2, 3$ und $n \geq 6$.

Es sei nun $f \in k[X]$ mit $L(f) \leq r$, und sei $n \geq \deg f$. Sei $g_1, \ldots, g_r$ eine Berechnungsfolge für f, und sei

$$f = \sum_{i=1}^{r} \alpha_i g_i + \alpha X + \beta.$$

Dann gilt nach dem Teil (iii) des Lemmas für fast alle $\xi \in k$ die Gleichung

$$\begin{aligned} f(X + \xi) &= f(\xi) + \left(\sum_{j=1}^{r} (\alpha_j \zeta_j) Q_{j,1}(\underline{\eta}) + \alpha \right) X \\ &\quad + \sum_{\nu \geq 2} \left(\sum_{j=1}^{r} (\alpha_j \zeta_j) Q_{j,\nu}(\underline{\eta}) \right) X^\nu \\ &= \sum_{\nu=0}^{n} Q_\nu(\underline{\eta}) X^\nu, \end{aligned}$$

wobei

$$\begin{aligned}\eta_{r^2+2r+j} &:= \alpha_j \zeta_j, \text{ für } j = 1, \ldots, r,\\ \eta_{r^2+3r+1} &:= \alpha,\\ \eta_{r^2+3r+2} &:= f(\xi).\end{aligned}$$

Man beachte noch, daß die Anzahl der Unbestimmten eines Polynoms Q_ν gleich $r^2 + 3r + 2 < (r + 2)^2$ ist. Wir verwenden aber den einfacheren Term $(r + 2)^2$. □

3 Ein Satz über nullstellenrelevante Polynome

Auf der Grundlage des Darstellungssatzes beweisen wir in diesem Kapitel einen Satz, der im nächsten Kapitel die Konstruktion schwerberechenbarer Polynome zuläßt.

Die Idee dabei ist, wie folgt mit einer Nullstellenmethode zu arbeiten. Sind s nicht notwendig verschiedene, geeignete Nullstellen $x_1, \ldots, x_s$ eines Polynoms $f \neq 0$ bekannt, so können wir eine Aussage über die Komplexität von f machen. Diese betrifft also *alle* Polynome $\neq 0$, die mindestens $x_1, \ldots, x_s$ (eventuell auch mehrfach gezählt) als Nullstellen haben. Das sind alle Polynome der Form $g \cdot \prod_{i=1}^{s}(X - x_i)$ mit $g \neq 0$.

Für die Arbeit mit einer solchen Nullstellenmethode ist hier der folgende Begriff der Nullstellenrelevanz nützlich.

Konvention: Sei k ein unendlicher Körper. Für $n \in \mathbb{N}$ und $s \in \mathbb{N}_{\geq 1}$ bezeichnen $U_0, \ldots, U_n, X_1, \ldots, X_s, X$ unabhängige Unbestimmte.

Definition. Ein Polynom $q \in \mathbb{Q}[X_1, \ldots, X_s]\backslash 0$ heißt *nullstellenrelevant* bezüglich $P_1, \ldots, P_s \in \mathbb{Q}[U_0, \ldots, U_n, X]$ und $r \geq 1$, falls gilt:

Für alle Polynome $f = \sum_{j=0}^{n} a_j X^j \in k[X]\backslash 0$ mit $L(f) \leq r$ und so, daß $P_i(a_0, \ldots, a_n, X) \neq 0$ für alle $i \in \{1, \ldots, s\}$ ist, gilt: Ist für jedes $i \in \{1, \ldots, s\}$ $x_i \in k$ irgendeine Nullstelle von $P_i(a_0, \ldots, a_n, X)$, so ist $q(x_1, \ldots, x_s) = 0$.

Wir erläutern diese Definition an einer typischen Situation. Sind die Polynome $P_1, \ldots, P_s$ alle gleich dem „generischen Polynom“ $F := U_0 + U_1 X + \cdots + U_n X^n$ vom Grad n, so ist q nullstellenrelevant bezüglich $F, \ldots, F$ (s mal) und r, falls für alle Polynome $f \neq 0$ vom Grad $\leq n$ mit $L(f) \leq r$ und mit Nullstellen $x_1, \ldots, x_s$ gilt: $q(x_1, \ldots, x_s) = 0$.

Daraus folgt: Besitzt ein spezielles Polynom f Nullstellen $x_1, \ldots, x_s$ so, daß $q(x_1, \ldots, x_s) = 0$ nicht erfüllt ist (das hängt dann ab von der Beschaffenheit von q), so ist $L(f) > r$. Dies werden wir ausnutzen, um in den Anwendungen schwerberechenbare Polynome zu konstruieren. Die Polynome P_i sind als

eine Verallgemeinerung des generischen Polynoms F zu betrachten. Diese ist hilfreich, um verschiedenartige Anwendungen zu untersuchen, auch solche, in denen f nicht durch Nullstellen vorgegeben ist.

Der Satz 1, den wir nun formulieren und beweisen werden, liefert Bedingungen für die Existenz solcher nullstellenrelevanter Polynome q und gibt Abschätzungen für Grad- und Koeffizientengrößen von q an.

Satz 1. *Seien* $r, s, n \in \mathbb{N}_{\geq 1}$ *mit* $r \leq 2\sqrt{n}$, $s \leq 2n$ *und* $n \geq 24^2$.
Seien $P_1, \ldots, P_s \in \mathbb{Q}[U_0, \ldots, U_n, X]$ *Polynome mit* $\deg_{U_j} P_i \leq 3n$ *für alle* $i \in \{1, \ldots, s\}$ *und alle* $j \in \{0, \ldots, n\}$. *Sei* $\gamma \in \mathbb{R}$ *mit* $1 < \gamma \leq n$ *und*

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s > n^{7(r+2)^2}. \tag{3.1}$$

(a) Dann gibt es ein bzgl. $P_1, \ldots, P_s$ *und* r *nullstellenrelevantes Polynom* $q \in \mathbb{Q}[X_1, \ldots, X_s]$ *mit*

$$\deg_{X_i} q < \gamma \deg_X P_i \text{ für alle } i \in \{1, \ldots, s\}.$$

(b) Haben die Polynome $P_1, \ldots, P_s$ *außerdem ganzzahlige Koeffizienten, und gilt* $\operatorname{wt} P_i \leq 4^{n^{r+2}}$ *und* $\deg_X P_i \leq 4^{n^r}$ *für alle* $i \in \{1, \ldots, s\}$, *so gibt es ein Polynom* q *gemäß (a) derart, daß alle seine Koeffizienten gleich* -1, 0 *oder* 1 *sind.*

Wir zeigen diesen Satz schrittweise in mehreren Teilen.

Notationen:
Wir bezeichnen im folgenden mit d_i den Grad von P_i in X, d. h. $d_i := \deg_X P_i$ für alle $i \in \{1, \ldots, s\}$.

Sind $Q_0(\underline{Z}), \ldots, Q_n(\underline{Z})$ die Polynome des Darstellungssatzes für n und r in den Unbestimmten $Z_1, \ldots, Z_{(r+2)^2}$, so schreiben wir

$$P_i(\underline{Q}(\underline{Z}), X_i) := P_i(Q_0(\underline{Z}), \ldots, Q_n(\underline{Z}), X_i)$$

für alle $i \in \{1, \ldots, s\}$.

Lemma 2. *Ist*

$$Q = \sum_{0 \le j_1, \ldots, j_s < n} q_{\underline{j}}(X_1, \ldots, X_s) Y_1^{j_1} \cdots Y_s^{j_s} \in \mathbb{Q}[\underline{X}, \underline{Y}] \backslash 0$$

ein Polynom in Unbestimmten $\underline{X}, \underline{Y}$ *mit*

$$Q(\underline{X}, P_1(\underline{Q}(\underline{Z}), X_1), \ldots, P_s(\underline{Q}(\underline{Z}), X_s)) = 0,$$

so gilt:

(i) Für alle $f = \sum_{j=0}^{n} a_j X^j \in k[X]$ *vom Grad* $\le n$ *mit* $L(f) \le r$ *ist*

$$Q(\underline{X}, P_1(\underline{a}, X_1), \ldots, P_s(\underline{a}, X_s)) = 0.$$

(ii) Für das lexikographisch erste $\underline{j}$ *mit* $q_{\underline{j}} \neq 0$ *ist das Polynom* $q_{\underline{j}}$ *nullstellenrelevant bzgl.* $P_1, \ldots, P_s$ *und* r.

Beweis. Zu (i):
Sei $f = \sum_{j=0}^{n} a_j X^j \in k[X]$ ein Polynom vom Grad $\le n$ mit $L(f) \le r$. Sei Z eine neue Unbestimmte, und $f(X+Z) = \sum_{j=0}^{n} f_j(Z) X^j$. Wegen dem Darstellungssatz, Teil (iii), gibt es für fast alle $\xi \in k$ gewisse $\eta_1, \ldots, \eta_{(r+2)^2} \in k$ mit $f_j(\xi) = Q_j(\underline{\eta})$ für alle $j \in \{0, \ldots, n\}$. Also gilt

$$Q(\underline{X}, P_1(f_0(\xi), \ldots, f_n(\xi), X_1), \ldots, P_s(f_0(\xi), \ldots, f_n(\xi), X_s)) = 0$$

für fast alle $\xi \in k$. Da k unendlich ist, folgt

$$Q(\underline{X}, P_1(f_0(Z), \ldots, f_n(Z), X_1), \ldots, P_s(f_0(Z), \ldots, f_n(Z), X_s)) = 0.$$

Mit $a_j = f_j(0)$ für alle $j \in \{0, \ldots, n\}$ erhalten wir

$$Q(\underline{X}, P_1(\underline{a}, X_1), \ldots, P_s(\underline{a}, X_s)) = 0.$$

Zu (ii):
Wir ordnen die s-Tupel $\underline{j} = (j_1, \ldots, j_s) \in \{0, \ldots, n-1\}^s$ lexikographisch an, d. h. $\underline{j}$ ist lexikographisch kleiner als $\underline{j'}$, falls

$$\exists\, r \in \{1, \ldots, s\} \;:\; j_1 = j_1', \ldots, j_{r-1} = j_{r-1}',\; j_r < j_r'.$$

Sei nun $\underline{k} = (k_1, \ldots, k_s)$ das lexikographisch erste s-Tupel $\underline{k}$ mit $q_{\underline{k}} \neq 0$.

Wir zeigen, daß $q_{\underline{k}}$ nullstellenrelevant bezüglich $P_1, \ldots, P_s$ und r ist.

Sei dazu $f = \sum_{j=0}^{n} a_j X^j \in k[X] \backslash 0$ vom Grad $\leq n$ mit $L(f) \leq r$ mit $P_i(a_0, \ldots, a_n, X) \neq 0$, und x_i eine Nullstelle von $P_i(a_0, \ldots, a_n, X)$ der Multiplizität $e_i \geq 1$ für alle $i \in \{1, \ldots, s\}$. Dann ist

$$P_i(a_0, \ldots, a_n, X) = (X - x_i)^{e_i} \cdot h_i(X)$$

mit $h_i(X) \in k[X]$, $h_i(x_i) \neq 0$, für alle $i \in \{1, \ldots, s\}$.

Wir entwickeln die Polynome $h_i(X_i)$ um x_i und die $q_{\underline{j}}$ um $x_1, \ldots, x_s$, d. h. wir schreiben für alle $\underline{j} \in \{0, \ldots, n-1\}^s$ und $i \in \{1, \ldots, s\}$

$$\begin{aligned} q_{\underline{j}}(\underline{X}) &= q_{\underline{j}}(\underline{x}) + R_{\underline{j}}(X_1 - x_1, \ldots, X_s - x_s) \\ \text{und } h_i(X_i) &= h_i(x_i) + H_i(X_i - x_i) \end{aligned}$$

mit Polynomen $R_{\underline{j}} \in \mathbb{Q}[Y_1, \ldots, Y_s]$ und $H_i \in \mathbb{Q}[X]$. Dann ist

$$\begin{aligned} &Q(X_1, \ldots, X_s, P_1(\underline{a}, X_1), \ldots, P_s(\underline{a}, X_s)) \\ &\quad = \sum_{0 \leq j_1, \ldots, j_s < n} q_{\underline{j}}(X_1, \ldots, X_s)(X_1 - x_1)^{e_1 j_1} h_1^{j_1}(X_1) \cdots (X_s - x_s)^{e_s j_s} h_s^{j_s}(X_s) \\ &\quad = \sum_{0 \leq j_1, \ldots, j_s < n} (q_{\underline{j}}(\underline{x}) + R_{\underline{j}}(X_1 - x_1, \ldots, X_s - x_s)) \\ &\qquad\qquad \cdot (h_1(x_1) + H_1(X_1 - x_1))^{j_1} \cdots (h_s(x_s) + H_s(X_s - x_s))^{j_s} \\ &\qquad\qquad \cdot (X_1 - x_1)^{e_1 j_1} \cdots (X_s - x_s)^{e_s j_s}. \end{aligned} \tag{3.2}$$

Wir schreiben dies als Linearkombination von Potenzprodukten der Form

$$(X_1 - x_1)^{l_1} \cdots (X_s - x_s)^{l_s}$$

mit gewissen Exponententupeln $(l_1, \ldots, l_s) \in \mathbb{N}^s$. Dazu multiplizieren wir die Summanden in (3.2) dementsprechend aus. Der Term mit lexikographisch kleinstem Exponententupel in $X_1 - x_1, \ldots, X_s - x_s$ ist dann

$$q_{\underline{k}}(x_1, \ldots, x_s) h_1^{k_1}(x_1) \cdots h_s^{k_s}(x_s)(X_1 - x_1)^{e_1 k_1} \cdots (X_s - x_s)^{e_s k_s}, \tag{3.3}$$

da kein anderer Summand außer der für $\underline{j} = \underline{k}$ zum Potenzprodukt mit dem Exponententupel $(e_1k_1, \ldots, e_sk_s)$ beiträgt.

Nach Teil (i) ist das Polynom $Q(X_1, \ldots, X_s, P_1(\underline{a}, X_1), \ldots, P_s(\underline{a}, X_s))$ gleich 0, also ist der Term (3.3) gleich 0, und es folgt $q_{\underline{k}}(x_1, \ldots, x_s) = 0$. □

Lemma 3. *Unter den Voraussetzungen von Satz 1 gibt es ein Polynom Q wie in Lemma 2 mit $\deg_{X_i} q_{\underline{j}} < \gamma d_i$ für alle $i, \underline{j}$.*

Beweis. Wir betrachten die Gleichung

$$Q(\underline{X}, P_1(\underline{Q}(\underline{Z}), X_1), \ldots, P_s(\underline{Q}(\underline{Z}), X_s)) = 0,$$

also die Gleichung

$$\sum_{0 \le j_1, \ldots, j_s < n} q_{\underline{j}}(\underline{X}) P_1^{j_1}(\underline{Q}(\underline{Z}), X_1) \cdots P_s^{j_s}(\underline{Q}(\underline{Z}), X_s) = 0 \tag{3.4}$$

als homogenes lineares Gleichungssystem für die unbekannten Koeffizienten der $q_{\underline{j}}$ mit $\deg_{X_i} q_{\underline{j}} < \gamma d_i$ für alle $i, \underline{j}$.

Man erhält es, wenn man die linke Seite von (3.4) als Linearkombination von Monomen in $\underline{X}, \underline{Z}$ schreibt und einen Koeffizientenvergleich vornimmt. Das System hat rationale Koeffizienten, und gesucht ist eine nichttriviale Lösung.

Die Anzahl N der Unbekannten des Gleichungssystems ist

$$N = n^s \cdot \lceil \gamma d_1 \rceil \cdots \lceil \gamma d_s \rceil,$$

und die Anzahl M seiner Gleichungen ist gleich der Anzahl der in (3.4) vorkommenden Monome in $\underline{X}, \underline{Z}$. Wir bestimmen dazu für jede Unbestimmte X_i bzw. Z_j den höchsten Grad, mit der sie in (3.4) vorkommen kann.

Für X_i ist dieser Grad $\lceil \gamma d_i \rceil - 1 + d_i(n-1)$.
Für Z_j ist er

$$\begin{aligned} 2rn \cdot 3n \cdot (n+1) \cdot (n-1)s &\le 2 \cdot 2\sqrt{n} \cdot n \cdot 3n(n^2-1) \cdot 2n \\ &< 24n^{\frac{1}{2}+5} \le n^6 \end{aligned}$$

für $n \geq 24^2$; diese Abschätzung gilt wegen der Gradabschätzung im Darstellungssatz, und wegen $r \leq 2\sqrt{n}$, $\deg_{U_i} P_j \leq 3n$ und $s \leq 2n$. Es folgt

$$M \leq n^{6(r+2)^2} \prod_{i=1}^{s} (\lceil \gamma d_i \rceil + d_i(n-1)).$$

Wir erhalten

$$\begin{aligned} \frac{N}{M} &\geq \frac{n^s \prod_{i=1}^{s} (\lceil \gamma d_i \rceil)}{n^{6(r+2)^2} \prod_{i=1}^{s} (\lceil \gamma d_i \rceil + d_i(n-1))} \\ &\geq \frac{n^s}{n^{6(r+2)^2}} \prod_{i=1}^{s} \left(\frac{\gamma d_i}{\gamma d_i + d_i(n-1)} \right) = \frac{1}{n^{6(r+2)^2}} \left(\frac{n\gamma}{\gamma + n - 1} \right)^s. \end{aligned}$$

Da

$$\frac{n\gamma}{\gamma + n - 1} = \frac{\gamma}{1 + \frac{\gamma - 1}{n}} \geq \frac{\gamma}{1 + \frac{\gamma - 1}{\gamma}} = \frac{\gamma^2}{2\gamma - 1}$$

wegen $1 < \gamma \leq n$ gilt, folgt

$$\frac{N}{M} \geq \frac{1}{n^{6(r+2)^2}} \left(\frac{\gamma^2}{2\gamma - 1} \right)^s > n^{(r+2)^2} \geq 2 > 1, \tag{3.5}$$

unter Verwendung von (3.1). Also ist $M < N$, und das Gleichungssystem hat eine nichttriviale rationale Lösung. Daher gibt es Polynome $q_{\underline{j}}$ mit (i), die nicht alle gleich 0 sind, so daß (3.4) gilt. □

Für das nächste Lemma benötigen wir als Hilfsmittel zunächst das Siegelsche Lemma. Es liefert eine Abschätzung der Komponenten einer nichttrivialen ganzzahligen Lösung eines homogenen linearen Gleichungssystems mit beschränkten ganzzahligen Koeffizienten.

Siegelsches Lemma. *Seien $l_1, \ldots, l_M \in \mathbb{Z}[X_1, \ldots, X_N]$ Linearfomen vom Gewicht $\leq w$ für eine positive ganze Zahl w. Falls $N > M$, existiert ein nichttrivialer Vektor $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$ mit $l_1(\underline{x}) = \cdots = l_M(\underline{x}) = 0$ und*

$$|x_i| \leq w^{\frac{M}{N-M}} \text{ für alle } i \in \{1, \ldots, N\}.$$

Beweis. Sei $z := \lfloor w^{\frac{M}{N-M}} \rfloor$. Dann ist $w < (z+1)^{\frac{N-M}{M}}$ und somit

$$wz + 1 \leq w(z+1) < (z+1)^{\frac{N}{M}}.$$

Für jedes $\underline{x} \in \{0, \ldots, z\}^N$ gilt $-S_j z \leq l_j(\underline{x}) \leq T_j z$, wobei $-S_j$ die Summe der negativen Koeffizienten von l_j, und T_j die Summe der positiven Koeffizienten von l_j sei, für alle $j \in \{1, \ldots, M\}$.

Es gilt $S_j + T_j \leq w$. Sei $\underline{l} : \mathbb{Z}^N \to \mathbb{Z}^M$ die Abbildung, die ein $\underline{x} = (x_1, \ldots, x_N)$ $\in \mathbb{Z}^N$ abbildet auf $(l_1(\underline{x}), \ldots, l_M(\underline{x})) \in \mathbb{Z}^M$. Diese bildet also den Würfel $\{0, \ldots, z\}^N$ ab auf eine Teilmenge des Würfels $\{-S_j z, \ldots, T_j z\}^M$.

Der letztere hat $(S_j z + T_j z + 1)^M \leq (wz+1)^M$ viele Elemente. Wegen $(wz+1)^M < (z+1)^N$ gibt es also zwei verschiedene Vektoren $\underline{x}^{(1)}, \underline{x}^{(2)} \in \{0, \ldots, z\}^N$ mit $\underline{l}(\underline{x}^{(1)}) = \underline{l}(\underline{x}^{(2)})$. Der Vektor $\underline{x} := \underline{x}^{(1)} - \underline{x}^{(2)}$ erfüllt dann die Behauptung. □

Lemma 4. *Unter den Voraussetzungen von Satz 1 inklusive Teil (b) gibt es ein Polynom Q gemäß Lemma 3 so, daß die Koeffizienten der $q_{\underline{j}}$ gleich -1, 0 oder 1 sind.*

Beweis. Wir wenden das Siegelsche Lemma auf das homogene lineare Gleichungssystem aus (3.4) an. Dieses hat ganzzahlige Koeffizienten, wenn die Polynome $P_1, \ldots, P_s$ ganzzahlige Koeffizienten haben.

Die Gewichte der Linearformen der linearen Gleichungen des Systems schätzen wir nach oben ab durch das Gewicht des Polynoms auf der linken Seite von (3.4), wobei wir die Koeffizienten von $q_{\underline{j}}$ als zusätzliche Unbestimmte betrachten.

Wir erhalten unter Verwendung der Subadditivität und Submultiplikativität des Gewichts für das Gewicht einer Linearform des Gleichungssystems die obere Abschätzung

$$n^s \cdot \lceil \gamma d_1 \rceil \cdots \lceil \gamma d_s \rceil \cdot \left(4^{n^{r+2}} \cdot \left(4^{n^r}\right)^{3n\cdot(n+1)} \right)^{(n-1)s},$$

wobei wir die Abschätzungen $\operatorname{wt} P_i \leq 4^{n^{r+2}}$, $\deg Q_j \leq 4^{n^r}$ und $\deg_{U_j} P_i \leq 3n$ benutzt haben.

Wegen $s \leq 2n$, $\gamma \leq n$ und $d_i \leq 4^{n^r}$ läßt sich dieser Ausdruck wiederum nach oben abschätzen durch

$$\begin{aligned} & n^{2n} \cdot \left(n \cdot 4^{n^r}\right)^{2n} \cdot \left(4^{n^{r+2}} \cdot 4^{6n^{r+2}}\right)^{(n-1)\cdot 2n} \\ & \leq n^{4n} \cdot 4^{2n^{r+1}} \cdot 4^{7n^{r+2}\cdot 2n^2} \\ & \leq 4^{4n^2+2n^{r+1}+14n^{r+4}} \leq 4^{20n^{r+4}} =: w. \end{aligned}$$

Wegen Ungleichung (3.5) gilt $\frac{M}{N-M} \leq 2\frac{M}{N} \leq 2n^{-(r+2)^2}$, und daraus folgt

$$w^{\frac{M}{N-M}} \leq \left(4^{20n^{r+4}}\right)^{2n^{-(r+2)^2}} = 4^{40n^{-r^2-3r}}.$$

Dies ist kleiner als 2, d. h. es ist $\frac{40}{n^{r^2+3r}} < \frac{1}{2}$, da $n > 80$.

Somit liefert das Siegelsche Lemma eine nichttriviale Lösung für (3.4) mit Komponenten -1, 0 oder 1. Also besitzen die Polynome q_j nur die Koeffizienten -1, 0 oder 1. □

Beweis von Satz 1. Der Beweis von Teil (a) des Satzes 1 besteht aus Lemma 2 und Lemma 3. Der Teil (b) folgt zusätzlich aus Lemma 4. □

Für die Anwendungen müssen $x_1, \ldots, x_s \in k$ bekannt sein, welche $q(x_1, \ldots, x_s) \neq 0$ erfüllen. Dafür stellen wir die beiden nächsten Lemmata als Hilfsmittel bereit.

Lemma 5. *Seien $d_1, \ldots, d_s \in \mathbb{N}$ natürliche Zahlen ≥ 2. Seien $x_1, \ldots, x_s \in \mathbb{C}$ über $\mathbb{Q}$ entweder algebraisch unabhängig oder algebraisch mit $[\mathbb{Q}(x_i) : \mathbb{Q}] \geq d_i$ für alle $i \in \{1, \ldots, s\}$ und*

$$[\mathbb{Q}(x_1, \ldots, x_s) : \mathbb{Q}] = \prod_{i=1}^{s} [\mathbb{Q}(x_i) : \mathbb{Q}].$$

Sei $q \in \mathbb{Q}[X_1, \ldots, X_s] \backslash 0$ vom Grad $< d_i$ in X_i für jedes $i \in \{1, \ldots, s\}$. Dann ist $q(x_1, \ldots, x_s) \neq 0$.

Beweis. Aufgrund der Voraussetzungen sind die Monome $x_1^{i_1} \cdots x_s^{i_s} \in \mathbb{Q}(x_1, \ldots, x_s)$ mit $0 \leq i_\nu < d_\nu$ für alle $\nu \in \{1, \ldots, s\}$ linear unabhängig über $\mathbb{Q}$. Daher ist $q(x_1, \ldots, x_s) \neq 0$. □

Um auch rationale $x_1, \ldots, x_s$ zu erhalten, die das Gewünschte leisten, benötigen wir das nächste Lemma.

Lemma 6. *Seien B, d, s positive ganze Zahlen und $x_1, \ldots, x_s \in \mathbb{C}$ mit $|x_1| \geq B + 1$ und $|x_i|^d \leq |x_{i+1}|$ für alle $i \in \{1, \ldots, s-1\}$.*
Sei $q \in \mathbb{Z}[X_1, \ldots, X_s] \backslash 0$ vom Grad $< d$ in jeder Unbestimmten und mit ganzzahligen Koeffizienten $\xi_{\underline{\nu}}$, so daß $-B \leq \xi_{\underline{\nu}} \leq B$ für alle $\underline{\nu} \in \{0, \ldots, d-1\}^s$ gilt. Dann ist $q(x_1, \ldots, x_s) \neq 0$.

Beweis. Seien die $\underline{\nu} \in \{0, \ldots, d-1\}^s$ antilexikographisch angeordnet, d. h. $\underline{\nu}$ ist antilexikographisch kleiner als $\underline{\nu'}$, falls

$$\exists\, r \in \{1, \ldots, s\} \;:\; \nu_r < \nu'_r, \nu_{r+1} = \nu'_{r+1}, \ldots, \nu_{s-1} = \nu'_{s-1}, \nu_s = \nu'_s.$$

Diese Anordnung sei mit $<$ bezeichnet.

Wir zeigen zunächst durch vollständige Induktion nach dieser Ordnung, daß

$$|x_1^{\nu_1} \cdots x_s^{\nu_s}| > B \sum_{\substack{\underline{\mu} < \underline{\nu} \\ \underline{\mu} \neq \underline{\nu}}} |x_1^{\mu_1} \cdots x_s^{\mu_s}| \tag{3.6}$$

für jedes $\underline{\nu} \in \{0, \ldots, d-1\}^s$ gilt.

Es genügt, dies zu zeigen. Denn ist $\underline{\nu} \in \{0, \ldots, d-1\}^s$ das größte Element bezüglich der antilexikographischen Ordnung mit $\xi_{\underline{\nu}} \neq 0$, so ist

$$\begin{aligned} q(x_1, \ldots, x_s) &= \left| \sum_{\underline{\mu} \in \{0, \ldots, d-1\}^s} \xi_{\underline{\mu}}\; x_1^{\mu_1} \cdots x_s^{\mu_s} \right| \\ &\geq |x_1^{\nu_1} \ldots x_s^{\nu_s}| \;\; - B \sum_{\substack{\underline{\mu} < \underline{\nu} \\ \underline{\mu} \neq \underline{\nu}}} |x_1^{\mu_1} \ldots x_s^{\mu_s}| > 0. \end{aligned}$$

Nun zum Beweis von (3.6).

Induktionsanfang: Sei $\underline{\nu} = (0, \ldots, 0)$. Dann ist $|x_1^0 \cdots x_s^0| = 1 > 0$.

Induktionsschritt: Sei $\underline{\nu} > (0, \ldots, 0)$. Dann ist

$$\begin{aligned} B \sum_{\substack{\underline{\mu} < \underline{\nu} \\ \underline{\mu} \neq \underline{\nu}}} |x_1^{\mu_1} \cdots x_s^{\mu_s}| &= B \sum_{\substack{\underline{\mu} < \underline{\nu}' \\ \underline{\mu} \neq \underline{\nu}'}} |x_1^{\mu_1} \cdots x_s^{\mu_s}| + B \left| x_1^{\nu_1'} \cdots x_s^{\nu_s'} \right| \\ &< (B+1) \left| x_1^{\nu_1'} \cdots x_s^{\nu_s'} \right| \end{aligned}$$

nach Induktionsvoraussetzung. $\underline{\nu'}$ bezeichnet dabei den Vorgänger von $\underline{\nu}$ bezüglich der antilexikographischen Ordnung.

Es ist nun zu zeigen, daß dieser Ausdruck $\leq |x_1^{\nu_1} \cdots x_s^{\nu_s}|$ ist. Dafür ist eine Fallunterscheidung durchzuführen.

1. Fall: Es ist $\nu_1' = A$, $\nu_1 = A + 1$ für ein $A \in \{0, \ldots, d-2\}$, und $\nu_l' = \nu_l$ für alle $l \in \{2, \ldots, s\}$. Dann ist auch

$$\begin{aligned} (B+1) \left| x_1^{\nu_1'} \cdots x_s^{\nu_s'} \right| &= (B+1)|x_1|^A \cdot |x_2^{\nu_2} \cdots x_s^{\nu_s}| \\ &\leq |x_1|^{A+1} \cdot |x_2^{\nu_2} \cdots x_s^{\nu_s}| = |x_1^{\nu_1} \cdots x_s^{\nu_s}| \end{aligned}$$

wegen $B + 1 \leq |x_1|$.

2. Fall: Es existiert ein $m \in \{1, \ldots, s-1\}$, mit $\nu_1' = \cdots = \nu_m' = d - 1$, $\nu_{m+1}' = A$,
$\nu_1 = \cdots = \nu_m = 0$, $\nu_{m+1} = A + 1$, für ein $A \in \{0, \ldots, d-2\}$, und $\nu_l = \nu_l'$ für alle $l \in \{m+2, \ldots, s\}$. Dann gilt

$$\begin{aligned} (B+1) \left| x_1^{d-1} \cdots x_m^{d-1} \right| &\leq (B+1) \cdot |x_{m+1}|^{(d-1)\left(\frac{1}{d^m} + \frac{1}{d^{m-1}} + \cdots + \frac{1}{d}\right)} \\ &= (B+1) \cdot |x_{m+1}|^{1 - \frac{1}{d^m}} \leq |x_{m+1}| \cdot \frac{B+1}{|x_1|} \leq |x_{m+1}| \end{aligned}$$

wegen $B + 1 \leq |x_1|$.

Also ist

$$\begin{aligned} (B+1) \left| x_1^{\nu_1'} \cdots x_s^{\nu_s'} \right| &= (B+1) \left| x_1^{d-1} \cdots x_m^{d-1} \cdot x_{m+1}^A \cdot x_{m+2}^{\nu_{m+2}'} \cdots x_s^{\nu_s'} \right| \\ \leq \left| x_{m+1}^{A+1} \cdot x_{m+2}^{\nu_{m+2}'} \cdots x_s^{\nu_s'} \right| &= \left| x_1^{\nu_1} \cdots x_s^{\nu_s} \right|. \end{aligned}$$

□

Eine Voraussetzung von Satz 1 ist $s \leq 2n$. Um diese Abschätzung zu erhalten, benutzen wir in manchen Anwendungen das nächste Lemma.

Lemma 7. *Sei $s \in \mathbb{N}$ mit $s \geq 3$, seien $x_1, \ldots, x_s \in \mathbb{C}$ paarweise verschieden und sei $f \in \mathbb{C}[X]$ vom Grad $\leq s-2$ und nicht konstant. Dann gilt:*

(a) Es existiert ein $p \in \mathbb{C}[X_1, \ldots, X_s] \backslash 0$ mit $\deg_{X_i} p \leq s-2$ für alle $i \in \{1, \ldots, s\}$ und mit Koeffizienten der Form $\pm(f(x_i) - f(x_j))$ für $i, j \in \{1, \ldots, s\}$, so daß $p(x_1, \ldots, x_s) = 0$ ist.

(b) Es existiert eine nichttriviale Linearkombination der $f(x_1), \ldots, f(x_s)$ mit Koeffizienten aus $\mathbb{Z}[x_1, \ldots, x_s]$, die gleich 0 ist. Gilt außerdem $|x_1|, \ldots, |x_s| \leq B$ für eine positive ganze Zahl B, so sind diese Koeffizienten betraglich kleiner als $(2B)^{\frac{s^2}{2}}$.

Beweis. Wir setzen $y_i := f(x_i)$ für alle $i \in \{1, \ldots, s\}$ und schreiben $f = \sum_{j=0}^{s-2} a_j X^j$.

Die $y_1, \ldots, y_s$ sind nicht alle gleich: Seien sie sonst etwa alle gleich y. Dann hat das Polynom $f(X) - y$ vom Grad $\leq s-2$ die s verschiedenen Nullstellen $x_1, \ldots, x_s$ und ist daher gleich 0, d. h. f ist konstant im Widerspruch zur Voraussetzung.

Für Unbestimmte $X_1, \ldots, X_s, Y_1, \ldots, Y_s$ sei

$$V(\underline{X}, \underline{Y}) := \begin{pmatrix} 1 & X_1 & \ldots & X_1^{s-2} & Y_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & X_s & \ldots & X_s^{s-2} & Y_s \end{pmatrix} \in (\mathbb{C}[\underline{X}, \underline{Y}])^{s \times s}.$$

Sei nun $P(\underline{X}, \underline{Y}) := \det V(\underline{X}, \underline{Y}) \in \mathbb{C}[\underline{X}, \underline{Y}]$.

Wegen

$$V(\underline{x}, \underline{y}) \cdot (a_0, a_1, \cdots, a_{s-2}, -1)^{\mathrm{T}} = (f(x_1) - y_1, \ldots, f(x_s) - y_s)^{\mathrm{T}} = 0$$

ist die Matrix $V(\underline{x}, \underline{y})$ singulär, deswegen gilt $P(\underline{x}, \underline{y}) = 0$.

Zu (a): Es gilt

$$\begin{aligned} P(\underline{X},\underline{Y}) &= \sum_{\pi\in\mathfrak{S}_s} \operatorname{sign}(\pi)\; X_{\pi(2)}X_{\pi(3)}^2\cdots X_{\pi(s-1)}^{s-2}Y_{\pi(s)} \\ &= \sum_{\substack{\pi\in\mathfrak{S}_s \\ \pi(s)>\pi(1)}} \operatorname{sign}(\pi)\; (Y_{\pi(s)}-Y_{\pi(1)})\, X_{\pi(2)}X_{\pi(3)}^2\cdots X_{\pi(s-1)}^{s-2}, \end{aligned}$$

wobei $\mathfrak{S}_s$ die Menge aller Permutationen von $\{1,\ldots,s\}$ bezeichnet. Somit erfüllt $p(\underline{X}) := P(\underline{X},\underline{y}) \in \mathbb{C}[\underline{X}]$ wegen $P(\underline{x},\underline{y}) = 0$ die Behauptung von Teil (a). Dabei ist $p \neq 0$, da die $y_1,\ldots,y_s$ nicht alle gleich sind.

Zu (b): Wir entwickeln die Determinante von $V(\underline{X})$ nach der letzten Spalte. Demnach ist

$$P(\underline{X},\underline{Y}) = (-1)^{s+1}Y_1 \det V_1 + (-1)^{s+2}Y_2 \det V_2 + \cdots + (-1)^{s+s}Y_s \det V_s,$$

wobei die VANDERMONDEmatrix V_i aus $V(\underline{X},\underline{Y})$ durch Streichen der letzten Spalte und i-ten Zeile entsteht, für alle $i \in \{1,\ldots,s\}$. Somit ist $P(\underline{x},\underline{y})$ eine Linearkombination von $y_1,\ldots,y_s$, die gleich 0 ist. Die Koeffizienten dieser Linearkombination sind bis auf das Vorzeichen VANDERMONDEdeterminanten, für $i \in \{1,\ldots,s\}$ nämlich

$$\det V_i = \prod_{\substack{k>l \\ k\neq i, l\neq i}} (x_k - x_l) \neq 0,$$

wobei

$$|\det V_i| = \prod_{\substack{k>l \\ k\neq i, l\neq i}} |x_k - x_l| \leq \prod_{\substack{k>l \\ k\neq i, l\neq i}} (2B) < (2B)^{\frac{s^2}{2}}$$

gilt. Dies zeigt Teil (b). □

4 Anwendungen des Satzes auf schwerberechenbare Polynome

Für unsere Anwendungen ist der unendliche Körper k stets der Körper $\mathbb{C}$ der komplexen Zahlen.

4.1 Algebraische Stützstellen hohen Grades

Das erste Korollar beschreibt schwerberechenbare Interpolationspolynome mit algebraisch unabhängigen Stützstellen oder algebraischen Stützstellen genügend hohen Grades. Für die rationalen Werte an diesen Stützstellen ist insbesondere der Wert 0 möglich, in diesem Fall handelt es sich um Polynome $\neq 0$ eines Ideals $\mathbb{C}[X] \cdot f$, also um alle Vielfachen $\neq 0$ eines Polynoms f.

Korollar 1. *Sei $s \in \mathbb{N}$ hinreichend groß, und seien $x_1, \ldots, x_s \in \mathbb{C}$ über $\mathbb{Q}$ entweder algebraisch unabhängig oder algebraisch mit $[\mathbb{Q}(x_i) : \mathbb{Q}] \geq 2^{\sqrt{s}}$ für alle $i \in \{1, \ldots, s\}$ und*

$$[\mathbb{Q}(x_1, \ldots, x_s) : \mathbb{Q}] = \prod_{i=1}^{s} [\mathbb{Q}(x_i) : \mathbb{Q}].$$

Sei $f \in \mathbb{C}[X]$ nicht konstant mit $f(x_i) \in \mathbb{Q}$ für alle $i \in \{1, \ldots, s\}$.
Dann ist $L(f) \geq \frac{1}{8}\sqrt{s}$.

Bemerkungen.

(i) Der genaue Wert der Konstanten $\frac{1}{8}$ ist hier, wie in den weiteren Korollaren, nicht wichtig. Es kommt auf die Größenordnung der unteren Schranke an.

(ii) Die Bedingung $f(x_i) \in \mathbb{Q}$ trifft insbesondere auf diejenigen Polynome f zu, unter deren Nullstellen $x_1, \ldots, x_s$ sind. Das Korollar besagt daher auch, daß alle Vielfachen $\neq 0$ des Polynoms $\prod_{i=1}^{s}(X - x_i)$ schwerberechenbar sind.

Beispiel. (Vergleiche auch BAUR und HALUPCZOK [3].) Sei $a \in \mathbb{Z}\backslash\{0, \pm 1\}$ quadratfrei. Ist s hinreichend groß, sind $p_1, \ldots, p_s$ paarweise verschiedene positive Primzahlen $\geq 2^{\sqrt{s}}$, und ist $f \in \mathbb{C}[X]$ mit $f(a^{\frac{1}{p_i}}) \in \mathbb{Q}$ für alle $i \in \{1, \ldots, s\}$, so ist $L(f) \geq \frac{1}{8}\sqrt{s}$.

Beweis. Sei $x_i := a^{\frac{1}{p_i}}$ für alle $i \in \{1, \ldots, s\}$. Dann ist $[\mathbb{Q}(x_i) : \mathbb{Q}] = p_i$ und $[\mathbb{Q}(x_1, \ldots, x_s) : \mathbb{Q}] = p_1 \cdots p_s$. Korollar 1 läßt sich also anwenden. □

Ein solches Polynom f ist beispielsweise $f = \prod_{i=1}^{s}(X - a^{\frac{1}{p_i}}) \cdot g$ mit $g \in \mathbb{C}[X]\backslash 0$ beliebig.

Beweis des Korollars. Sei im folgenden $n := \deg f$. Die $x_1, \ldots, x_s$ sind nach Voraussetzung paarweise verschieden.

Es gilt $n \geq s - 1$. Denn sonst sei $n \leq s - 2$, und da f nicht konstant ist, folgt aus Lemma 7, Teil (a), die Existenz eines Polynoms $p \in \mathbb{C}[X_1, \ldots, X_s]\backslash 0$ vom Grad $\leq s - 2 < 2^{\sqrt{s}}$ in jedem X_i und mit Koeffizienten $\pm(f(x_i) - f(x_j)) \in \mathbb{Q}$, so daß $p(x_1, \ldots, x_s) = 0$ gilt, im Widerspruch zu Lemma 5. Somit ist für hinreichend großes s auch n groß, und auch die Voraussetzung $s \leq 2n$ von Satz 1 ist erfüllt.

Sei $P_i(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n - f(x_i) \in \mathbb{Q}[\underline{U}, X]$ für alle $i \in \{1, \ldots, s\}$, und $\gamma := n$. Wir zeigen, daß damit alle weiteren Voraussetzungen von Satz 1 erfüllt sind. Die Voraussetzung $\deg_{U_j} P_i \leq 3n$ gilt offensichtlich. Sei $f = \sum_{j=0}^{n} a_j X^j$ und $r := L(f) \geq \log n \geq 1$ für $n \geq 2$. Es gilt weiter nach PATERSON und STOCKMEYER [11] die Abschätzung $r \leq 2\sqrt{n}$, eine weitere Voraussetzung von Satz 1.

Wir gehen indirekt vor und nehmen an, daß $14(r+2)^2 < s$ sei. Dann ist $2r \leq \sqrt{s}$, und für algebraische x_i ist $[\mathbb{Q}(x_i) : \mathbb{Q}] \geq 2^{\sqrt{s}} \geq 2^{2r} \geq n^2$, da wegen der Gradschranke $2^r \geq n$ gilt. Weiter gilt, da n groß ist,

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s = \left(\frac{n^2}{2n-1}\right)^s > \left(\frac{n}{2}\right)^s > \left(\frac{n}{2}\right)^{14(r+2)^2} \geq n^{7(r+2)^2}.$$

Nach Satz 1 existiert dann ein bezüglich $P_1, \ldots, P_s$ und r nullstellenrelevantes Polynom $q \in \mathbb{Q}[X_1, \ldots, X_s]$ mit $\deg_{X_i} q < \gamma n = n^2$ für alle $i \in \{1, \ldots, s\}$. Da

$P_i(\underline{a}, X) = f(X) - f(x_i) \neq 0$ und $P_i(\underline{a}, x_i) = f(x_i) - f(x_i) = 0$ für alle i ist, gilt $q(x_1, \ldots, x_s) = 0$. Dies ist jedoch nach Lemma 5 nicht möglich.

Dieser Widerspruch zeigt, daß $14(r+2)^2 \geq s$ ist. Wegen $2r \geq r + 2 \geq \sqrt{\frac{s}{14}}$ für $n \geq 4$ (da $r \geq \log n \geq 2$) folgt $r \geq \frac{1}{2}\sqrt{\frac{1}{14}}\sqrt{s} \geq \frac{1}{8}\sqrt{s}$. □

4.2 Schnell wachsende Stützstellen bzw. Nullstellen

Auch bestimmte Interpolationspolynome mit schnell wachsenden Stützstellen sind schwerberechenbar. Die ganzzahligen Werte an diesen Stellen sollen im Betrag nach oben beschränkt sein, und wie in Korollar 1 ist auch hier der Wert 0 möglich.

Korollar 2. *Sei s hinreichend groß, sei $B \in \mathbb{N}$ mit $1 \leq B \leq 2^{s^2}$, und seien $x_1, \ldots, x_s \in \mathbb{C}$ mit $|x_1| \geq B+1$ und $|x_{i+1}| \geq |x_i|^{2^{\sqrt{s}}}$ für alle $i \in \{1, \ldots, s-1\}$. Sei $f \in \mathbb{C}[X]$ nicht konstant mit $f(x_i) \in \mathbb{Z}$ und $|f(x_i)| \leq \frac{B}{2}$ für alle $i \in \{1, \ldots, s\}$. Dann ist $L(f) \geq \frac{1}{8}\sqrt{s}$.*

Beispiel. Jedes Polynom f mit $f(2^{2^{i\lceil\sqrt{s}\rceil}}) = 2^{i\lceil\sqrt{s}\rceil}$ für alle $i \in \{1, \ldots, s\}$ erfüllt diese Bedingungen mit $B = 2^{s\lceil\sqrt{s}\rceil+1} \leq 2^{s^2}$, denn für hinreichend großes s ist

$$|x_1| = 2^{2^{\lceil\sqrt{s}\rceil}} \geq 2^{s\lceil\sqrt{s}\rceil+1} + 1.$$

Also gilt $L(f) \geq \frac{1}{8}\sqrt{s}$. Ein solches Polynom f interpoliert den Logarithmus an den schnell wachsenden Stellen $2^{2^{i\lceil\sqrt{s}\rceil}}$ für alle $i \in \{1, \ldots, s\}$.

Polynome f, die an diesen Stellen den Wert 0 haben, erfüllen ebenso die Bedingungen des Korollars 2, und zwar mit $B = 1$. Also gilt für jedes $g \in \mathbb{C}[X]\backslash 0$ und $f = \prod_{i=1}^{s}(X - 2^{2^{i\lceil\sqrt{s}\rceil}}) \cdot g$ die Abschätzung $L(f) \geq \frac{1}{8}\sqrt{s}$. Dies gilt ebenso für Polynome f, die an den Stellen $2^{2^{si}}$ für $i \in \{1, \ldots, s\}$ den Wert 0 haben. Diese Polynome hat auch Malajovich in [10] untersucht, seine Ergebnisse führen auf die untere Schranke $L(f) \geq C\sqrt[3]{s}$ für eine Konstante $C > 0$.

Beweis des Korollars. Wir gehen wie im Beweis von Korollar 1 vor. Sei wieder $n := \deg f$ und $r := L(f)$, also ist $r \leq 2\sqrt{n}$. Nach Voraussetzung sind die $x_1, \ldots, x_s$ paarweise verschieden.

Es gilt $n \geq s-1$. Denn sonst sei $n \leq s-2$, und da f nicht konstant ist, folgt aus Lemma 7, Teil (a), die Existenz eines Polynoms $p \in \mathbb{C}[X_1, \ldots, X_s]\backslash 0$ vom Grad $\leq s-2 < 2^{\sqrt{s}}$ in jedem X_i und mit Koeffizienten $\pm(f(x_i) - f(x_j)) \in \mathbb{Z}$ vom Betrag $\leq B$, so daß $p(x_1, \ldots, x_s) = 0$ gilt, im Widerspruch zu Lemma 6. Somit gilt die Voraussetzung $s \leq 2n$ von Satz 1, und für hinreichend großes s ist auch n groß.

Wir setzen wie im Beweis von Korollar 1 wieder

$$P_i(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n - f(x_i) \in \mathbb{Z}[\underline{U}, X]$$

für alle $i \in \{1, \ldots, s\}$, und $\gamma := n$. Wie dort gilt $\deg_{U_j} P_i \leq 3n$. Wir nehmen an, daß $14(r+2)^2 < s$ sei; dann gilt $2^{\sqrt{s}} \geq n^2$ und

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s > n^{7(r+2)^2},$$

genau wie im Beweis von Korollar 1. Zu überprüfen sind nur noch die Voraussetzungen in Teil (b) von Satz 1.

Zum einen hat $P_i(\underline{U}, X)$ ganzzahlige Koeffizienten, und es gilt $\deg_X P_i = n \leq 4^{n^r}$ sowie

$$\operatorname{wt} P_i \leq n + 1 + |f(x_i)| \leq n + 1 + 2^{s^2} \leq n + 1 + 2^{4n^2} \leq 4^{n^{r+2}}, \quad \text{für jedes } i \in \{1, \ldots, s\}.$$

Teil (b) von Satz 1 zeigt somit, daß es ein nullstellenrelevantes Polynom q mit $\deg_{X_i} q < \gamma n = n^2$ für alle $i \in \{1, \ldots, s\}$ gibt, das sogar die Koeffizienten -1, 0 oder 1 hat.

Es gilt $q(x_1, \ldots, x_s) = 0$, da q nullstellenrelevant bezüglich $P_1, \ldots, P_s$ und r ist. Dies ist nach Lemma 6 aber nicht möglich, da $|x_1| \geq B + 1 \geq 2$ und $|x_{i+1}| \geq |x_i|^{2^{\sqrt{s}}} \geq |x_i|^{n^2}$ ist für alle $i \in \{1, \ldots, s-1\}$.

Es folgt $14(r+2)^2 \geq s$, und wie im Beweis von Korollar 1 folgt $r \geq \frac{1}{8}\sqrt{s}$. □

Wachsen die Stellen $x_1, \ldots, x_s$ nicht so schnell wie in Korollar 2, so erhalten wir die etwas schwächere untere Schranke $\frac{1}{16}\sqrt[3]{s}$:

Korollar 3. *Sei s hinreichend groß, sei $B \in \mathbb{N}$ mit $1 \leq B \leq 2^{s^2}$ und seien $x_1, \ldots, x_s \in \mathbb{C}$ mit $|x_1| \geq B + 1$ und $|x_{i+1}| \geq |x_i|^2$ für alle $i \in \{1, \ldots, s-1\}$. Sei $f \in \mathbb{C}[X]$ nicht konstant mit $f(x_i) \in \mathbb{Z}$ und $|f(x_i)| \leq \frac{B}{2}$ für alle $i \in \{1, \ldots, s\}$. Dann ist $L(f) \geq \frac{1}{16}\sqrt[3]{s}$.*

Beispiel. Ein Polynom f mit $f(2^{2^i}) = 2^i$ für alle $i \in \mathbb{N}$ mit $1 + \log s \le i \le s$ erfüllt diese Bedingungen mit $B = 2^{s+1}$. (Insbesondere gilt $|x_1| = 2^{2^{\lceil 1+\log s \rceil}} \ge B + 1$.) Es interpoliert den Logarithmus an den schnell wachsenden Stellen 2^{2^i} für $i \in \mathbb{N}$ mit $1 + \log s \le i \le s$. Es folgt $L(f) \ge \frac{1}{16}\sqrt[3]{s - \lceil \log s \rceil} \ge \frac{1}{32}\sqrt[3]{s}$ für alle hinreichend großen s.

Ein Polynom f, das an den Stellen 2^{2^i} für alle $i \in \{1, \dots, s\}$ den Wert 0 hat, erfüllt mit $B = 1$ ebenso die Bedingungen in Korollar 3. Also ist $f = \prod_{i=1}^{s}(X - 2^{2^i}) \cdot g$ mit beliebigem $g \in \mathbb{C}[X]\backslash 0$ schwerberechenbar, d. h. hier, daß $L(f) \ge \frac{1}{16}\sqrt[3]{s}$ gilt. Das Polynom $\prod_{i=1}^{s}(X - 2^{2^i})$ selbst wurde bereits von Aldaz et al. in [1] behandelt. Dort wird $L(\prod_{i=1}^{s}(X - 2^{2^i})) \ge C\sqrt{\frac{s}{\log s}}$ für eine Konstante $C > 0$ gezeigt.

Beweis des Korollars. Wir setzen $t := \lfloor \sqrt[3]{s} \rfloor$ und $y_i := x_{it}$ für alle $i \in \mathbb{N}$ mit $1 \le i \le \lfloor \frac{s}{t} \rfloor$. Dann gilt

$$|y_i|^{2^t} = |x_{it}|^{2^t} \le |x_{it+1}|^{2^{t-1}} \le \cdots \le |x_{(i+1)t}| = |y_{i+1}|.$$

Wir nehmen an, daß $14(r+2)^2 < \lfloor \frac{s}{t} \rfloor$ für $r := L(f)$ gelte. Dann ist $2r < \sqrt[3]{s}$ und somit $2^t \ge 2^{\sqrt[3]{s}} \ge 2^{2r} \ge n^2$ laut Gradschranke, wobei $n := \deg f$.

Wir gehen nun genau so vor wie in Korollar 1 bzw. 2, allerdings mit den Stellen $y_1, \dots, y_{\lfloor \frac{s}{t} \rfloor}$ statt $x_1, \dots, x_s$.

Es gilt $n \ge \lfloor \frac{s}{t} \rfloor - 1$. Denn sonst sei $n \le \lfloor \frac{s}{t} \rfloor - 2$, und da f nicht konstant ist, folgt aus Lemma 7, Teil (a), die Existenz eines Polynoms $p \in \mathbb{C}[X_1, \dots, X_{\lfloor \frac{s}{t} \rfloor}]\backslash 0$ vom Grad $\le \lfloor \frac{s}{t} \rfloor - 2 < 2^t$ in jedem X_i (wegen $s < t \cdot 2^t = \lfloor \sqrt[3]{s} \rfloor \cdot 2^{\lfloor \sqrt[3]{s} \rfloor}$ für großes s), und mit Koeffizienten $\pm(f(y_i) - f(y_j)) \in \mathbb{Z}$ vom Betrag $\le B$, wobei $i, j \in \mathbb{N}$ mit $1 \le i, j \le \lfloor \frac{s}{t} \rfloor$, so daß $p(y_1, \dots, y_{\lfloor \frac{s}{t} \rfloor}) = 0$ gilt, im Widerspruch zu Lemma 6.

Wir setzen nun

$$P_i(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n - f(y_i) \in \mathbb{Z}[\underline{U}, X]$$

für $i \in \mathbb{N}$ mit $1 \le i \le \lfloor \frac{s}{t} \rfloor$, und $\gamma := n$.

Die Voraussetzungen von Satz 1 inklusive Teil (b) sind erfüllt, genau wie in Korollar 1 und 2, allerdings mit $\lfloor \frac{s}{t} \rfloor$ statt s. Daher existiert ein bezüglich $P_1, \ldots, P_{\lfloor \frac{s}{t} \rfloor}$ und r nullstellenrelevantes Polynom q mit Koeffizienten -1, 0 oder 1, so daß $\deg_{X_i} q < \gamma n = n^2$ für alle $i \in \mathbb{N}$ mit $1 \leq i \leq \lfloor \frac{s}{t} \rfloor$ gilt. Da somit $q(y_1, \ldots, y_{\lfloor \frac{s}{t} \rfloor}) = 0$ ist, erhalten wir einen Widerspruch zu Lemma 6.

Dies zeigt $14(r+2)^2 \geq \lfloor \frac{s}{t} \rfloor$, also ist $r \geq \frac{1}{8}\sqrt{\lfloor \frac{s}{t} \rfloor} \geq \frac{1}{8}\sqrt{\frac{s}{\sqrt[3]{s}} - 1} \geq \frac{1}{16}\sqrt[3]{s}$ für hinreichend großes s. □

4.3 Algebraische Nullstellen beliebigen Grades ≥ 2

Korollar 1 gilt insbesondere für Polynome f mit Nullstellen $x_1, \ldots, x_s$, die algebraisch von genügend hohem Grad sind. Wir formulieren nun die entsprechende Aussage mit algebraischen Nullstellen $x_1, \ldots, x_s$ beliebigen Grades ≥ 2 über $\mathbb{Q}$. Man muß dabei zusätzlich voraussetzen, daß für jede Nullstelle x_i nur begrenzt viele Konjugierte von x_i ebenfalls Nullstellen von f sind.

Ein Beispiel dafür ist das Polynom $f = \prod_{i=1}^{s}(X - \sqrt{p_i})$ mit paarweise verschiedenen positiven Primzahlen $p_1, \ldots, p_s$. Das Polynom f ist schwerberechenbar, siehe auch Baur [2]. Korollar 4 zeigt, daß jedes Polynom $f \cdot g$ schwerberechenbar ist (d. h. $L(fg) \geq \frac{1}{5}\sqrt[3]{s}$ für hinreichend großes s), sofern jede der Zahlen $-\sqrt{p_1}, \ldots, -\sqrt{p_s}$ *nicht* Nullstelle von $g \in \mathbb{C}[X]$ ist. Über die Komplexität des Polynoms $f \cdot \prod_{i=1}^{s}(X + \sqrt{p_i}) = \prod_{i=1}^{s}(X^2 - p_i)$, bei dem die rationalen Koeffizienten vergleichsweise klein sind, können wir mit unseren Mitteln keine Aussage machen.

Korollar 4. *Sei s hinreichend groß und seien $x_1, \ldots, x_s \in \mathbb{C}$ algebraisch über $\mathbb{Q}$ mit $[\mathbb{Q}(x_i) : \mathbb{Q}] = m_i \geq 2$ für alle $i \in \{1, \ldots, s\}$ und mit*

$$[\mathbb{Q}(x_1, \ldots, x_s) : \mathbb{Q}] = m_1 \cdots m_s.$$

Dann hat jedes Polynom $f \in \mathbb{C}[X]\backslash 0$ mit $f(x_1) = \cdots = f(x_s) = 0$ und so, daß

$$\deg \mathrm{ggT}(f, \mathrm{Mipo}_{x_i}) \leq \frac{m_i}{2} \text{ für alle } i \in \{1, \ldots, s\} \text{ ist,}$$

Komplexität $L(f) \geq \frac{1}{5}\sqrt[3]{s}$.

Bemerkung. Mit $\mathrm{Mipo}_{x_i} \in \mathbb{Q}[X]$ bezeichnen wir das Minimalpolynom von x_i über $\mathbb{Q}$. Es ist das eindeutig bestimmte normierte Polynom $\neq 0$ minimalen Grades m_i, so daß $\mathrm{Mipo}_{x_i}(x_i) = 0$ gilt. Die Bedingung

$$\deg \mathrm{ggT}(f, \mathrm{Mipo}_{x_i}) \leq \frac{m_i}{2}$$

bedeutet, daß für jedes $i \in \{1, \ldots, s\}$ mindestens $\lceil \frac{m_i}{2} \rceil$ viele Konjugierte von x_i, also die Nullstellen von Mipo_{x_i}, *nicht* Nullstellen von f sind.

Beweis des Korollars. Es gilt für $n := \deg f$, daß $n \geq s$ ist, da $\prod_{i=1}^{s}(X - x_i)$ Teiler von f ist. (Die Nullstellen $x_1, \ldots, x_s$ sind nach Voraussetzung paarweise verschieden.) Sei $f = \sum_{j=0}^{n} a_j X^j$.

Sei $i \in \{1, \ldots, s\}$ fest.

(i) Falls $m_i > 2n$, setzen wir

$$P_i(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n$$

für die Unbestimmten $U_0, \ldots, U_n$. Dann ist $P_i(\underline{a}, X) = f(X) \neq 0$ und $P_i(\underline{a}, x_i) = f(x_i) = 0$.

(ii) Falls $m_i \leq 2n$, bestimmen wir P_i wie folgt:

Sei $\pi_i := \mathrm{Mipo}_{x_i} \in \mathbb{Q}[X]$, also $m_i = \deg \pi_i$.

Sei $g_i := \mathrm{ggT}(f, \pi_i)$ und $t_i := \deg g_i \leq \frac{m_i}{2}$.

Gesucht sind nun $v, w \in \mathbb{C}[X]$ mit $\deg v < m_i - t_i$ und $\deg w < n - t_i$, die die Polynomgleichung

$$vf + w\pi_i = g_i$$

lösen.

Wir vergleichen die Koeffizienten der Monome $X^{n+m_i-t_i-1}, \ldots, X^{t_i+1}, X^{t_i}$ auf beiden Seiten dieser Polynomgleichung und erhalten ein lineares Gleichungssystem

$$Ax = e \tag{4.1}$$

für die unbekannten Koeffizienten von v bzw. w, und zwar mit einer quadratischen Koeffizientenmatrix $A \in \mathbb{C}^{(n+m_i-2t_i)\times(n+m_i-2t_i)}$ und der rechten Seite $e := (0, \ldots, 0, 1)^{\mathrm{T}} \in \mathbb{Q}^{n+m_i-2t_i}$.

Wir zeigen nun, daß es genau eine Lösung des Gleichungssystems (4.1) gibt.

Zur Existenz: Seien Polynome $V, W \in \mathbb{C}[X]$ gegeben mit

$$V\frac{f}{g_i} + W\frac{\pi_i}{g_i} = 1.$$

Solche Polynome V, W existieren, da die Polynome $\frac{f}{g_i}$ und $\frac{\pi_i}{g_i}$ teilerfremd sind.

Durch Division von V durch $\frac{\pi_i}{g_i}$ mit Rest erhält man $V = v + R\frac{\pi_i}{g_i}$ mit Polynomen v und R, wobei $\deg v < m_i - t_i$ ist. Es folgt

$$v\frac{f}{g_i} + \left(R\frac{f}{g_i} + W\right)\frac{\pi_i}{g_i} = 1$$

mit $\deg\left(R\frac{f}{g_i} + W\right) \leq \deg v + (n - t_i) - (m_i - t_i) < n - t_i$. Wir setzen also $w := R\frac{f}{g_i} + W$. Die Koeffizienten von v und w lösen (4.1).

Zur Eindeutigkeit: Sind v, w und $\bar{v}, \bar{w}$ die zugehörigen Polynome zweier Lösungen von (4.1), so ist

$$(v - \bar{v})f + (w - \bar{w})\pi_i = h$$

mit einem $h \in \mathbb{C}[X]$ und $\deg h < \deg g_i = t_i$, also $h = 0$, da g_i das eindeutig bestimmte normierte Polynom $\neq 0$ minimalen Grades in $\mathbb{C}[X]f + \mathbb{C}[X]\pi_i$ ist. Aus $h = 0$ folgt, daß $\frac{\pi_i}{g_i}$ Teiler von $v - \bar{v}$ ist; somit gilt aus Gradgründen $v - \bar{v} = 0$. Damit ist auch $w - \bar{w} = 0$.

Die Matrix A in (4.1) ist also regulär, und nach der Cramerschen Regel ist die eindeutige Lösung von (4.1) gegeben durch

$$x_j := \frac{\det A_j}{\det A}, \quad j = 1, \ldots, n + m_i - 2t_i,$$

wobei A_j aus A durch Ersetzen der j-ten Spalte durch e entsteht.

Für Unbestimme $U_0, \ldots, U_n$ sei $F := U_0 + U_1X + \cdots + U_nX^n$. Wie oben vergleichen wir auf beiden Seiten der Polynomgleichung

$$\begin{gathered}\tilde{v}F + \tilde{w}\pi_i = X^{t_i} + \text{ Terme niedrigeren Grades in } X, \\ \text{wobei } \tilde{v}, \tilde{w} \in \mathbb{Q}(\underline{U})[X],\ \deg_X \tilde{v} < m_i - t_i,\ \deg_X \tilde{w} < n - t_i,\end{gathered} \tag{4.2}$$

die Koeffizienten der Monome $X^{n+m_i-t_i-1}, \ldots, X^{t_i+1}, X^{t_i}$ und erhalten ein lineares Gleichungssystem

$$By = e \tag{4.3}$$

mit $B \in \mathbb{Q}[\underline{U}]^{(n+m_i-2t_i)\times(n+m_i-2t_i)}$, e wie oben, für die unbekannten Koeffizienten der Polynome $\tilde{v}, \tilde{w}$. Die Einträge der Matrix B sind dabei polynomial in jeder Unbestimmten U_ν, für $\nu \in \{0, \ldots, n\}$, und zwar höchstens vom Grad 1 in U_ν, wie man aus (4.2) ablesen kann.

Es ist $\det B \neq 0$, da man durch Einsetzen von $a_0 \ldots, a_n$ für $U_0, \ldots, U_n$ in der Matrix B die Matrix A erhält und $\det A \neq 0$ ist.

Wir setzen

$$y_j := \frac{\det B_j}{\det B}, \quad j = 1, \ldots, n + m_i - 2t_i,$$

wobei B_j aus B durch Ersetzen der j-ten Spalte durch e entsteht.

Der Vektor $y := (y_1, \ldots, y_{n+m-2t_i})^{\mathrm{T}}$ ist dann eine Lösung von $By = e$, bzw. das zugehörige Paar $\tilde{v}, \tilde{w}$ Lösung von (4.2). Durch Einsetzen von $\underline{a}$ in $\underline{U}$ in diese Lösung erhalten wir die Lösung v, w gemäß (4.1), denn aus den Matrizen B_j bzw. B erhält man so A_j bzw. A.

Es sei $P_i(\underline{U}, X) := (\det B)(\tilde{v}F + \tilde{w}\pi_i) \in \mathbb{Q}[\underline{U}][X]$.

Dann ist $\deg_X P_i = t_i \leq \frac{m_i}{2}$, und für jedes $\nu \in \{0, \ldots, n\}$ ist

$$\begin{aligned} \deg_{U_\nu} P_i &\leq \max\{\deg_{U_\nu} \det B_j \mid 1 \leq j \leq n + m_i - 2t_i\} + 1 \\ &\leq (n + m_i - 2t_i - 1) + 1 \leq 3n \end{aligned}$$

wegen $m_i \leq 2n$, und da die Einträge der Matrizen B_j höchstens vom Grad 1 in U_ν sind. (Wir entwickeln $\det B_j$ nach der Spalte e.)

Ferner ist $P_i(\underline{a}, X) = (\det A)(vf + w\pi_i) \neq 0$ und $P_i(\underline{a}, x_i) = 0$, da $x_i \in \mathbb{C}$ gemeinsame Nullstelle von f und π_i ist.

(iii) Wir setzen

$$\gamma := \min\left(\left\{\frac{m_k}{n} \;\middle|\; m_k > 2n,\ 1 \leq k \leq s\right\} \cup \left\{\frac{m_j}{t_j} \;\middle|\; m_j \leq 2n,\ 1 \leq j \leq s\right\}\right).$$

Damit ist $\gamma \geq 2$, da $t_j \leq \frac{m_j}{2}$, und somit gilt

$$\frac{\gamma^2}{2\gamma - 1} \geq \frac{4}{3}.$$

Nach Konstruktion gilt $\gamma \deg_X P_i \leq m_i$ für alle $i \in \{1, \ldots, s\}$. Denn ist $\gamma = \frac{m_k}{n}$ für ein $m_k > 2n$, so ist

$$\gamma \deg_X P_i = \begin{cases} \frac{m_k}{n} \cdot n \leq \frac{m_i}{n} \cdot n = m_i, & \text{falls } m_i > 2n, \\ \frac{m_k}{n} \cdot t_i \leq \frac{m_i}{t_i} \cdot t_i = m_i, & \text{falls } m_i \leq 2n, \end{cases}$$

und ist $\gamma = \frac{m_j}{t_j}$ für ein $m_j \leq 2n$, so ist

$$\gamma \deg_X P_i = \begin{cases} \frac{m_j}{t_j} \cdot n \leq \frac{m_i}{n} \cdot n = m_i, & \text{falls } m_i > 2n, \\ \frac{m_j}{t_j} \cdot t_i \leq \frac{m_i}{t_i} \cdot t_i = m_i, & \text{falls } m_i \leq 2n. \end{cases}$$

Wir können Satz 1 mit diesen Polynomen P_i für $i \in \{1, \ldots, s\}$ und diesem γ anwenden. Sei dazu $r := L(f)$; dann gilt $r \leq 2\sqrt{n}$.

Unter der Annahme, daß $\left(\frac{4}{3}\right)^s > n^{7(r+2)^2}$ sei, gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s \geq \left(\frac{4}{3}\right)^s > n^{7(r+2)^2}.$$

Dann existiert nach Satz 1 ein bezüglich $P_1, \ldots, P_s$ und r nullstellenrelevantes Polynom $q \in \mathbb{Q}[X_1, \ldots, X_s]$ mit $\deg_{X_i} q < \gamma \deg_X P_i \leq m_i$ für $1 \leq i \leq s$. Da $P_i(\underline{a}, X) \neq 0$ und $P_i(\underline{a}, x_i) = 0$ nach Konstruktion der P_i gilt, ist also $q(x_1, \ldots, x_s) = 0$, im Widerspruch zur Voraussetzung an die $x_1, \ldots, x_s$ wegen Lemma 5.

Dies zeigt, daß $\left(\frac{4}{3}\right)^s \leq n^{7(r+2)^2}$ gilt, also ist (für $r \geq \log n \geq 2$)

$$2r \geq r + 2 \geq \sqrt{\frac{1}{7} \log \frac{4}{3}} \sqrt{\frac{s}{\log n}} \geq \frac{1}{5} \sqrt{\frac{s}{\log n}},$$

und somit

$$r \geq \frac{1}{10}\sqrt{\frac{s}{\log n}}. \tag{4.4}$$

Der Vergleich mit der Gradschranke, nämlich $r \geq \max\left\{\log n, \frac{1}{10}\sqrt{\frac{s}{\log n}}\right\}$, zeigt $r \geq \frac{1}{5}\sqrt[3]{s}$ (durch Elimination von n in $\log n = \frac{1}{10}\sqrt{\frac{s}{\log n}}$). □

Wir geben nun einige Folgerungen dieses Korollars an.

Folgerungen

1. Es ist $L(g\cdot\prod_{i=1}^{s}(X-x_i)) \geq \frac{1}{5}\sqrt[3]{s}$ für alle hinreichend großen s, wobei für die algebraischen Erweiterungen $\mathbb{Q}(x_1), \ldots, \mathbb{Q}(x_s)$, jeweils vom Grad ≥ 2 über $\mathbb{Q}$, wieder

   $$[\mathbb{Q}(x_1, \ldots, x_s) : \mathbb{Q}] = \prod_{i=1}^{s}[\mathbb{Q}(x_i) : \mathbb{Q}]$$

   gilt, und für jedes i ist kein Konjugiertes von x_i Nullstelle von $g \in \mathbb{C}[X]$.

   Beispiel: Es ist $L(g\cdot\prod_{i=1}^{s}(X-\sqrt{p_i})) \geq \frac{1}{5}\sqrt[3]{s}$ für alle hinreichend großen s, wobei $p_1, \ldots, p_s$ paarweise verschiedene positive Primzahlen sind, und $g \in \mathbb{C}[X]$ mit $g(-\sqrt{p_i}) \neq 0$ für alle $i \in \{1, \ldots, s\}$.

2. Die Formel (4.4) im Beweis zeigt $L(\prod_{i=1}^{s}(X - x_i)) \geq \frac{1}{10}\sqrt{\frac{s}{\log s}}$ für alle hinreichend großen s, wobei für die algebraischen Erweiterungen $\mathbb{Q}(x_1), \ldots, \mathbb{Q}(x_s)$, jeweils vom Grad ≥ 2 über $\mathbb{Q}$, wieder

   $$[\mathbb{Q}(x_1, \ldots, x_s) : \mathbb{Q}] = \prod_{i=1}^{s}[\mathbb{Q}(x_i) : \mathbb{Q}]$$

   gilt.

   Beispiel: Es ist $L(\prod_{j=1}^{s}(X - \sqrt{p_j})) \geq \frac{1}{10}\sqrt{\frac{s}{\log s}}$ für alle hinreichend großen s, wobei wie oben $p_1, \ldots, p_s$ paarweise verschiedene positive Primzahlen sind. Dies ist das in der Einleitung erwähnte Resultat von Heintz und Morgenstern in [7].

4.4 Algebraische Werte an rationalen Stützstellen

Das nächste Korollar beschreibt schwerberechenbare Interpolationspolynome mit rationalen Stützstellen und gewissen Werten an diesen Stellen, die über $\mathbb{Q}$ algebraisch unabhängig oder algebraisch vom Grad ≥ 2 sind.

Korollar 5. *Sei s hinreichend groß, seien $y_1, \ldots, y_s \in \mathbb{Q}$ und sei $f \in \mathbb{C}[X]$, wobei $f(y_1), \ldots, f(y_s)$ über $\mathbb{Q}$ entweder algebraisch unabhängig seien, oder algebraisch mit $[\mathbb{Q}(f(y_i)) : \mathbb{Q}] \geq 2$ für alle $i \in \{1, \ldots, s\}$ und*

$$[\mathbb{Q}(f(y_1), \ldots, f(y_s)) : \mathbb{Q}] = \prod_{i=1}^{s} [\mathbb{Q}(f(y_i)) : \mathbb{Q}].$$

Dann ist $L(f) \geq \frac{1}{5}\sqrt[3]{s}$.

Beispiel. Ist s hinreichend groß, sind $p_1, \ldots, p_s$ paarweise verschiedene positive Primzahlen und ist $f \in \mathbb{C}[X]$ mit $f(i) = \sqrt{p_i}$ für alle $i \in \{1 \ldots, s\}$, so ist $L(f) \geq \frac{1}{5}\sqrt[3]{s}$.

Beweis des Korollars. Zunächst sind laut Voraussetzung die $y_1, \ldots, y_s$ paarweise verschieden und f nicht konstant.

Für $n := \deg f$ gilt $n \geq s - 1$. Denn sonst zeigt Lemma 7, Teil (b), daß eine nichttriviale Linearkombination der $f(y_1), \ldots, f(y_s)$ mit Koeffizienten aus $\mathbb{Z}[y_1, \ldots, y_s] \subseteq \mathbb{Q}$ existiert, die gleich 0 ist, im Widerspruch zu Lemma 5.

Sei $P_i(\underline{U}, X) := U_0 + U_1 y_i + U_2 y_i^2 + \cdots + U_n y_i^n - X \in \mathbb{Q}[\underline{U}, X]$ für alle $i \in \{1, \ldots, s\}$, und $\gamma := 2$.

Sei $f = \sum_{j=0}^{n} a_j X^j$. Dann ist $P_i(\underline{a}, X) = f(y_i) - X \neq 0$, und $P_i(\underline{a}, f(y_i)) = f(y_i) - f(y_i) = 0$ für alle $i \in \{1, \ldots, s\}$. Sei $r := L(f)$; also gilt $r \leq 2\sqrt{n}$.

Es gelte $(\frac{4}{3})^s > n^{7(r+2)^2}$, dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s = \left(\frac{4}{3}\right)^s > n^{7(r+2)^2},$$

und es existiert nach Satz 1 ein bezüglich $P_1, \ldots, P_s$ und r nullstellenrelevantes $q \in \mathbb{Q}[X_1, \ldots, X_s]$ mit $\deg_{X_i} q < 2$ für $1 \leq i \leq s$. Es gilt dann also

$q(f(y_1),\ldots,f(y_s))=0$. Dies ist nach Lemma 5 aufgrund der Voraussetzungen an die $f(y_1),\ldots,f(y_s)$ nicht möglich, und es folgt $(\frac{4}{3})^s \leq n^{7(r+2)^2}$, also $r \geq \frac{1}{5}\sqrt[3]{s}$ wie im Beweis von Korollar 4. □

Bemerkung. Gilt neben den anderen Voraussetzungen in Korollar 5 sogar $[\mathbb{Q}(f(y_i)):\mathbb{Q}] \geq 2^{\sqrt{s}}$ für alle $i \in \{1,\ldots,s\}$, so gilt $L(f) \geq \frac{1}{8}\sqrt{s}$.

Beweis: Wir benutzen dieselben Polynome P_i wie in Korollar 5, und für $\gamma := n$ ist

$$\frac{\gamma^2}{2\gamma-1} = \frac{n^2}{2n-1} > \frac{n^2}{2n} = \frac{n}{2}.$$

Es gelte $14(r+2)^2 < s$, dann gilt $r \leq \sqrt{s}$ und

$$\left(\frac{n}{2}\right)^s > \left(\frac{n}{2}\right)^{14(r+2)^2} \geq n^{7(r+2)^2}, \text{ letzteres für großes } n.$$

Aus Satz 1 folgt $q(f(y_1),\ldots,f(y_s))=0$ mit $\deg_{X_i} q < n$ für alle $i \in \{1,\ldots,s\}$, und dies ist wegen $[\mathbb{Q}(f(y_i)):\mathbb{Q}] \geq 2^{\sqrt{s}} \geq 2^r \geq n$ (Gradschranke) ein Widerspruch zu Lemma 5. Es folgt $14(r+2)^2 \geq s$, also $r \geq \frac{1}{8}\sqrt{s}$ für hinreichend großes s, wie im Beweis von Korollar 1. □

Beispiel. Sei $a \in \mathbb{Z}\backslash\{0,\pm 1\}$ quadratfrei. Ist s hinreichend groß, sind $p_1,\ldots,p_s \geq 2^{\sqrt{s}}$ paarweise verschiedene positive Primzahlen und ist $f \in \mathbb{C}[X]$ mit $f(i) = a^{\frac{1}{p_i}}$ für alle $i \in \{1,\ldots,s\}$, so ist $L(f) \geq \frac{1}{8}\sqrt{s}$.

4.5 Schnell wachsende Werte an ganzzahligen Stützstellen

Das nächste Korollar beschreibt schwerberechenbare Interpolationspolynome mit ganzzahligen, im Betrag nach oben beschränkten Stützstellen, aber schnell wachsenden Werten an diesen Stellen.

Korollar 6. *Sei s hinreichend groß, sei $B \in \mathbb{N}$ mit $1 \le B \le 2^{s^2}$, seien $y_1, \ldots, y_s \in \mathbb{Z}$ mit $|y_i| \le B$ für alle $i \in \{1, \ldots, s\}$, und sei $f \in \mathbb{C}[X]$ mit $|f(y_1)| \ge (2B)^{\frac{s^2}{2}}$ und $|f(y_{i+1})| \ge |f(y_i)|^2$ für alle $i \in \{1, \ldots, s-1\}$. Dann ist $L(f) \ge \frac{1}{5}\sqrt[3]{s}$.*

Beispiel. Ein Polynom f mit $f(2^i) = 2^{2^i}$ für alle $i \in \mathbb{N}$ mit $1 + 3\log s \le i \le s$ erfüllt diese Bedingungen mit $B = 2^{4s-1}$; denn wir haben $s - \lceil 3\log s \rceil$ viele Stellen, und es gilt

$$|f(y_1)| = |f(2^{\lceil 1+3\log s \rceil})| \ge 2^{2s^3} = (2B)^{\frac{s^2}{2}} \ge (2B)^{\frac{1}{2}(s-\lceil 3\log s \rceil)^2}.$$

Es interpoliert die Exponentialfunktion an den Stellen 2^i für $1 + 3\log s \le i \le s$. Es folgt $L(f) \ge \frac{1}{5}\sqrt[3]{s - \lceil 3\log s \rceil} \ge \frac{1}{10}\sqrt[3]{s}$ für alle hinreichend großen s.

Beweis des Korollars. Zunächst sind laut Voraussetzung die $y_1, \ldots, y_s$ paarweise verschieden und f nicht konstant. Wir gehen wie in Korollar 5 vor. Sei dazu wieder $n := \deg f$ und $r := L(f)$.

Es gilt $n \ge s-1$. Denn sonst gibt es nach Lemma 7, Teil (b), eine nichttriviale Linearkombination der $f(y_1), \ldots, f(y_s)$ mit Koeffizienten aus $\mathbb{Z}[y_1, \ldots, y_s] \subseteq \mathbb{Z}$ vom Betrag $< (2B)^{\frac{s^2}{2}}$, die gleich 0 ist, im Widerspruch zu Lemma 6.

Wir setzen wie im Beweis von Korollar 5

$$P_i(\underline{U}, X) := U_0 + U_1 y_i + U_2 y_i^2 + \cdots + U_n y_i^n - X \in \mathbb{Z}[\underline{U}, X]$$

für alle $i \in \{1, \ldots, s\}$ und $\gamma := 2$. Wir nehmen an, daß $(\frac{4}{3})^s > n^{7(r+2)^2}$ sei. Dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s = \left(\frac{4}{3}\right)^s > n^{7(r+2)^2}.$$

Wir prüfen nun die Voraussetzungen für Teil (b) von Satz 1.

Zum einen hat jedes $P_i(\underline{U}, X)$ ganzzahlige Koeffizienten, und es gilt $\deg_X P_i = 1 \leq 4^{n^r}$ sowie

$$\begin{aligned} \operatorname{wt} P_i \leq 1 + B + B^2 + \cdots + B^n + 1 &\leq \max\{n+2, B^{n+1}\} \\ &\leq 2^{s^2 \cdot 2n} \leq 2^{4n^2 \cdot 2n} = 2^{8n^3} \leq 4^{n^{r+2}} \end{aligned}$$

für große s und n, da ohne Einschränkung $r \geq 2$ wegen der Gradschranke $r \geq \log n$ gilt.

Satz 1 mit Teil (b) zeigt somit, daß es ein nullstellenrelevantes Polynom q mit $\deg_{X_i} q < 2$ für alle $i \in \{1, \ldots, s\}$ gibt, das sogar die Koeffizienten -1, 0 oder 1 hat.

Es folgt $q(f(y_1), \ldots, f(y_s)) = 0$, was nach dem Lemma 6 nicht möglich ist, da $|f(y_1)| \geq 2$ und $|f(y_{i+1})| \geq |f(y_i)|^2$ für alle $i \in \{1, \ldots, s-1\}$ gilt.

Es folgt also $(\frac{4}{3})^s \leq n^{7(r+2)^2}$, und somit $r \geq \frac{1}{5}\sqrt[3]{s}$ für alle hinreichend großen s, wie im Beweis von Korollar 4. □

Bemerkung. Gilt neben den anderen Voraussetzungen in Korollar 6 sogar $|f(y_{i+1})| \geq |f(y_i)|^{2^{\sqrt{s}}}$ für alle $i \in \{1, \ldots, s-1\}$, so gilt $L(f) \geq \frac{1}{8}\sqrt{s}$.

Beweis: Wir benutzen dieselben Polynome P_i wie im Beweis von Korollar 6, und $\gamma := n$ liefert

$$\frac{\gamma^2}{2\gamma - 1} = \frac{n^2}{2n-1} > \frac{n^2}{2n} = \frac{n}{2}.$$

Es gelte $14(r+2)^2 < s$, dann gilt $r \leq \sqrt{s}$ und

$$\left(\frac{n}{2}\right)^s > \left(\frac{n}{2}\right)^{14(r+2)^2} \geq n^{7(r+2)^2}, \text{ letzteres für } n \geq 4.$$

Satz 1 zeigt $q(f(y_1), \ldots, f(y_s)) = 0$ für ein $q \neq 0$ mit $\deg_{X_i} q < n$ für alle $i \in \{1, \ldots, s\}$, wobei die Koeffizienten des nichttrivialen Polynoms q alle 0, 1 oder -1 sind. Dies ist ein Widerspruch zu Lemma 6 wegen $2^{\sqrt{s}} \geq 2^r \geq n$ (Gradschranke). Wir erhalten $14(r+2)^2 \geq s$, also $r \geq \frac{1}{8}\sqrt{s}$ für alle hinreichend großen s, wie im Beweis von Korollar 1. □

Beispiel. Ein Polynom f mit $f(2^{i\lceil\sqrt{s}\rceil}) = 2^{2^{i\lceil\sqrt{s}\rceil}}$ für alle $i \in \{1,\dots,s\}$ erfüllt diese Bedingung mit $B = 2^{s\lceil\sqrt{s}\rceil}$; denn es gilt $|f(y_1)| = |f(2^{\lceil\sqrt{s}\rceil})| \geq 2^{2^{\sqrt{s}}} \geq (2B)^{\frac{s^2}{2}}$ für alle hinreichend großen s. Es interpoliert die Exponentialfunktion an den Stellen $2^{i\lceil\sqrt{s}\rceil}$ für alle $i \in \{1,\dots,s\}$. Es gilt also $L(f) \geq \frac{1}{8}\sqrt{s}$.

Auch gewisse Vielfache der Polynome aus Korollar 6 sind schwerberechenbar:

Korollar 7. *Sei s hinreichend groß, sei $B \in \mathbb{N}$ mit $1 \leq B \leq 2^{s^2}$, seien $y_1,\dots,y_s \in \mathbb{Z}$ mit $|y_i| \leq B$ für alle $i \in \{1,\dots,s\}$, und sei $f \in \mathbb{C}[X]$ mit $|f(y_1)| \geq (2B)^{\frac{s^2}{2}}$ und $|f(y_{i+1})| \geq |f(y_i)|^2$ für alle $i \in \{1,\dots,s-1\}$. Sei $g \in \mathbb{C}[X]\backslash 0$ mit $|g(y_i)| \leq 2^{s^3}$ für alle $i \in \{1,\dots,s\}$. Dann ist $L(fg) \geq \frac{1}{5}\sqrt[3]{s}$.*

Beweis des Korollars. Sei $n := \deg fg$. Dann ist $n \geq \deg f \geq s-1$; man vergleiche dazu den Beweis von Korollar 6. Sei $r := L(fg)$.

Wir setzen $P_i(\underline{U}, X) := \sum_{j=0}^{n} U_j y_i^j - g(y_i) \cdot X \in \mathbb{Z}[\underline{U}, X]$ für $i \in \{1,\dots,s\}$. Dann ist $\deg_X P_i = 1 \leq 4^{n^r}$ und

$$\begin{aligned}\operatorname{wt} P_i &\leq 1 + B + B^2 + \cdots + B^n + 2^{s^3} \leq \max\{n+1, B^{n+1}\} + 2^{s^3} \\ &\leq 2^{1+s^2\cdot 2n} \leq 2^{4n^2\cdot 4n} = 2^{16n^3} \leq 4^{n^{r+2}}\end{aligned}$$

für große s und n, da wegen der Gradschranke $r \geq \log n \geq 2$ gilt.

Sei $fg = \sum_{j=0}^{n} a_j X^j$. Dann ist $P_i(\underline{a}, X) = (fg)(y_i) - g(y_i) \cdot X \neq 0$ und $P_i(\underline{a}, f(y_i)) = 0$.

Sei $\gamma := 2$. Es gelte $\left(\frac{4}{3}\right)^s > n^{7(r+2)^2}$, dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s = \left(\frac{4}{3}\right)^s > n^{7(r+2)^2}.$$

Satz 1 mit seinem Teil (b) zeigt dann die Existenz eines nullstellenrelevanten Polynoms q mit $\deg_{X_i} q < 2$ für alle $i \in \{1,\dots,s\}$ und mit Koeffizienten 0, 1 oder -1. Es gilt somit $q(f(y_1,\dots,f(y_s))) = 0$, im Widerspruch zu Lemma 6.

Dies zeigt, daß doch $\left(\frac{4}{3}\right)^s \leq n^{7(r+2)^2}$ ist, also folgt wieder $r \geq \frac{1}{5}\sqrt[3]{s}$, wie im Beweis von Korollar 4. □

Schwerberechenbare Polynome erhält man auch durch Verketten eines Polynoms f aus Korollar 6 mit einem Polynom g, das ganzzahlige Koeffizienten und beschränktes Gewicht besitzt:

Korollar 8. *Sei s hinreichend groß, sei $B \in \mathbb{N}$ mit $1 \leq B \leq 2^{s^2}$, seien $y_1, \ldots, y_s \in \mathbb{Z}$ mit $|y_i| \leq B$ für alle $i \in \{1, \ldots, s\}$, und sei $f \in \mathbb{C}[X]$ mit $|f(y_1)| \geq (2B)^{\frac{s^2}{2}}$ und $|f(y_{i+1})| \geq |f(y_i)|^2$ für alle $i \in \{1, \ldots, s-1\}$. Sei $g \in \mathbb{Z}[X]\backslash 0$ mit $\operatorname{wt} g \leq 2^{s^3}$ für alle $i \in \{1, \ldots, s\}$. Dann ist $L(g \circ f) \geq \frac{1}{16}\sqrt[3]{s}$.*

Beweis des Korollars. Sei $n := \deg(g \circ f)$. Dann ist $n \geq \deg f \geq s - 1$; man vergleiche dazu den Beweis von Korollar 6.

Sei $r := L(g \circ f)$. Wir setzen $P_i(\underline{U}, X) := \sum_{j=0}^{n} U_j y_i^j - g(X) \in \mathbb{Z}[\underline{U}, X]$ für alle $i \in \{1, \ldots, s\}$. Dann ist $\deg_X P_i \leq n \leq 4^{n^r}$ und

$$\begin{aligned}\operatorname{wt} P_i &\leq 1 + B + B^2 + \cdots + B^n + 2^{s^3} \leq \max\{n+1, B^{n+1}\} + 2^{s^3} \\ &\leq 2^{1+s^2 \cdot 2n} \leq 2^{4n^2 \cdot 4n} = 2^{16n^3} \leq 4^{n^{r+2}}\end{aligned}$$

für große s und n, da ohne Einschränkung $r \geq 2$ wegen der Gradschranke $r \geq \log n$ gilt.

Sei $g \circ f = \sum_{j=0}^{n} a_j X^j$. Dann ist $P_i(\underline{a}, X) = g(f(y_i)) - g(X) \neq 0$ und $P_i(\underline{a}, f(y_i)) = 0$. Sei $\gamma := n$ und ohne Einschränkung $2r \leq \sqrt[3]{s} - 1$.

Wir setzen nun $t := \lfloor \sqrt[3]{s} \rfloor$ und $x_i := f(y_{it})$ für alle $i \in \mathbb{N}$ mit $1 \leq i \leq \lfloor \frac{s}{t} \rfloor$. Dann ist

$$|x_i|^{2^t} = |f(y_{it})|^{2^t} \leq |f(y_{it+1})|^{2^{t-1}} \leq \cdots \leq |f(y_{(i+1)t})| = |x_{i+1}|$$

und $2^t \geq 2^{\sqrt[3]{s}-1} \geq 2^{2r} \geq n^2$ laut Gradschranke.

Es gelte $14(r+2)^2 < \lfloor \frac{s}{t} \rfloor$, dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^{\lfloor \frac{s}{t} \rfloor} = \left(\frac{n^2}{2n-1}\right)^{\lfloor \frac{s}{t} \rfloor} > \left(\frac{n}{2}\right)^{\lfloor \frac{s}{t} \rfloor} > \left(\frac{n}{2}\right)^{14(r+2)^2} \geq n^{7(r+2)^2}$$

für alle hinreichend großen n.

Satz 1, angewendet auf die $x_1, \ldots, x_{\lfloor \frac{s}{t} \rfloor}$, zeigt nun die Existenz eines nullstellenrelevanten Polynoms q mit $\deg_{X_i} q < n^2 \leq 2^t$ für alle $i \in \mathbb{N}$ mit

$1 \leq i \leq \lfloor \frac{s}{t} \rfloor$ und mit Koeffizienten 0, 1 oder -1. Es gilt $q(x_1, \ldots, x_{\lfloor \frac{s}{t} \rfloor}) = 0$, im Widerspruch zu Lemma 6.

Dies zeigt, daß doch $14(r+2)^2 \geq \lfloor \frac{s}{t} \rfloor$ ist. Es folgt $r \geq \frac{1}{16}\sqrt[3]{s}$ für alle hinreichend großen s, wie im Beweis von Korollar 3. □

4.6 Algebraische oder schnell wachsende Koeffizienten

In diesem Abschnitt wollen wir zeigen, daß Satz 1 auch bisher bekannte schwerberechenbare Polynome mit algebraischen oder schnell wachsenden Koeffizienten liefert, die bereits STRASSEN [14] angegeben hat. Weitere Beispiele für schwerberechenbare Polynome mit gewissen Koeffizienten sind bei VON ZUR GATHEN und STRASSEN [5] oder bei HEINTZ und SIEVEKING [8] zu finden.

Korollar 9. *Sei n hinreichend groß und seien $a_1, \ldots, a_n \in \mathbb{C}$ algebraisch über $\mathbb{Q}$ mit $[\mathbb{Q}(a_i) : \mathbb{Q}] \geq 2$ für alle $i \in \{1, \ldots, n\}$ und*

$$[\mathbb{Q}(a_1, \ldots, a_n) : \mathbb{Q}] = \prod_{i=1}^{n} [\mathbb{Q}(a_i) : \mathbb{Q}].$$

Sei $f = \sum_{i=1}^{n} a_i X^i \in \mathbb{C}[X]$. Dann ist $L(f) \geq \frac{1}{10}\sqrt{\frac{n}{\log n}}$.

Beispiel. Ist n hinreichend groß, sind $p_1, \ldots, p_n$ paarweise verschiedene positive Primzahlen und ist $f = \sum_{i=1}^{n} \sqrt{p_i} X^i \in \mathbb{C}[X]$, so ist $L(f) \geq \frac{1}{10}\sqrt{\frac{n}{\log n}}$.

Beweis. Wegen $[\mathbb{Q}(\sqrt{p_i}) : \mathbb{Q}] = 2$ für alle $i \in \{1, \ldots, n\}$, und $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$ läßt sich Korollar 9 anwenden. □

Beweis des Korollars. Wir setzen $s := n$ und $P_i(\underline{U}, X) := X - U_i$ für alle $i \in \{1, \ldots, s\}$. Sei $\gamma := 2$ und $r := L(f)$. Die Polynome $P_i(\underline{a}, X) = X - a_i$ sind $\neq 0$, und es gilt $P_i(\underline{a}, a_i) = a_i - a_i = 0$ für alle $i \in \{1, \ldots, s\}$.

Es gelte $(\frac{4}{3})^n > n^{7(r+2)^2}$, dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s = \left(\frac{4}{3}\right)^s > n^{7(r+2)^2},$$

und die Voraussetzung (3.1) von Satz 1 ist erfüllt.

Nach Satz 1 gibt es somit ein Polynom $q \in \mathbb{Q}[X_1, \ldots, X_s] \backslash 0$ mit $\deg_{X_i} q < 2$ für alle $i \in \{1, \ldots, s\}$ und mit $q(a_1, \ldots, a_s) = 0$. Wegen Lemma 5 ist das nicht möglich.

Dies zeigt $(\frac{4}{3})^n \leq n^{7(r+2)^2}$, also $r \geq \frac{1}{10}\sqrt{\frac{n}{\log n}}$ für alle hinreichend großen n. □

Sind die Koeffizienten eines Polynoms algebraisch unabhängig oder algebraisch von genügend hohem Grad, erhalten wir eine optimale untere Komplexitätsschranke $\frac{1}{8}\sqrt{n}$ für den Grad n des Polynoms.

Korollar 10. *Sei n hinreichend groß, seien $a_1, \ldots, a_n \in \mathbb{C}$ über $\mathbb{Q}$ entweder algebraisch unabhängig oder algebraisch mit $[\mathbb{Q}(a_i) : \mathbb{Q}] \geq n$ für alle $i \in \{1, \ldots, n\}$ und*

$$[\mathbb{Q}(a_1, \ldots, a_n) : \mathbb{Q}] = \prod_{i=1}^{n} [\mathbb{Q}(a_i) : \mathbb{Q}].$$

Sei $f = \sum_{i=1}^{n} a_i X^i \in \mathbb{C}[X]$. Dann ist $L(f) \geq \frac{1}{8}\sqrt{n}$.

Beispiel. Ist n hinreichend groß, sind $p_1, \ldots, p_n > n$ paarweise verschiedene positive Primzahlen und ist $f = \sum_{j=1}^{n} e^{\frac{2\pi i}{p_j}} X^j \in \mathbb{C}[X]$, so ist $L(f) \geq \frac{1}{8}\sqrt{n}$.

Beweis. Wegen $[\mathbb{Q}(e^{\frac{2\pi i}{p_j}}) : \mathbb{Q}] = p_j - 1$ für alle $j \in \{1, \ldots, n\}$, und $[\mathbb{Q}(e^{\frac{2\pi i}{p_1}}, \ldots, e^{\frac{2\pi i}{p_n}}) : \mathbb{Q}] = (p_1 - 1) \cdots (p_n - 1)$ läßt sich Korollar 10 anwenden. □

Beweis des Korollars. Sei $s := n$ und $P_i(\underline{U}, X) := X - U_i$ für alle $i \in \{1, \ldots, s\}$. Sei $\gamma := n$ und $r := L(f)$.

Es gelte $n^{7(r+2)^2} < (\frac{n}{2})^n$, dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^n = \left(\frac{n^2}{2n-1}\right)^n > \left(\frac{n^2}{2n}\right)^n = \left(\frac{n}{2}\right)^n > n^{7(r+2)^2}.$$

Satz 1 zeigt dann die Existenz eines Polynoms $q \in \mathbb{Q}[X_1, \ldots, X_s] \backslash 0$ mit $\deg_{X_i} q < n$ für alle $i \in \{1, \ldots, s\}$ und $q(a_1, \ldots, a_n) = 0$, was Lemma 5 widerspricht. Es folgt $n^{7(r+2)^2} \geq (\frac{n}{2})^n$ und somit $2r \geq r + 2 \geq \sqrt{\frac{1}{14}}\sqrt{n}$ für alle hinreichend großen n, also ist $r \geq \frac{1}{8}\sqrt{n}$. □

Auch Polynome mit schnell wachsenden Koeffizienten können mit unserer Methode behandelt werden:

Korollar 11. *Sei n hinreichend groß, und seien $a_1, \ldots, a_n \in \mathbb{C}$ mit $|a_1| \geq 2$ und $|a_{i+1}| \geq |a_i|^2$ für alle $i \in \{1, \ldots, n-1\}$. Sei $f = \sum_{i=1}^{n} a_i X^i \in \mathbb{C}[X]$. Dann ist $L(f) \geq \frac{1}{10}\sqrt{\frac{n}{\log n}}$.*

Beispiel. Ist n hinreichend groß, und ist $f = \sum_{i=1}^{n} 2^{2^i} X^i \in \mathbb{C}[X]$, so ist $L(f) \geq \frac{1}{10}\sqrt{\frac{n}{\log n}}$.

Beweis. Wegen $|2^{2^0}| = 2$ und $|2^{2^{i+1}}| = |2^{2^i}|^2$ für $i \in \{1, \ldots, n-1\}$ läßt sich Korollar 11 anwenden. □

Beweis des Korollars. Wir gehen so vor wie im Beweis von Korollar 9. Sei $s := n$, $r := L(f)$ und $\gamma := 2$.

Die Polynome $P_i(\underline{U}, X) = X - U_i$ haben ganzzahlige Koeffizienten, und es gilt $\deg_X P_i = 1 \leq 4^{n^r}$ sowie $\operatorname{wt} P_i = 2 \leq 4^{n^{r+2}}$ für alle $i \in \{1, \ldots, n\}$. Die Voraussetzungen von Teil (b) in Satz 1 sind also erfüllt.

Es gelte $(\frac{4}{3})^n > n^{7(r+2)^2}$, dann gilt

$$\left(\frac{\gamma^2}{2\gamma - 1}\right)^s = \left(\frac{4}{3}\right)^s > n^{7(r+2)^2},$$

und die Voraussetzung (3.1) von Satz 1 ist erfüllt.

Nach Satz 1, Teil (b), gibt es somit ein Polynom $q \in \mathbb{Q}[X_1, \ldots, X_s] \backslash 0$ mit Koeffizienten 0, 1 oder -1, so daß $q(a_1, \ldots, a_s) = 0$ gilt. Wegen Lemma 6 ist das aber nicht möglich.

Dies zeigt $(\frac{4}{3})^n \leq n^{7(r+2)^2}$, also $r \geq \frac{1}{10}\sqrt{\frac{n}{\log n}}$. □

5 Vielfache von Polynomen mit speziellen Koeffizienten

In Abschnitt 4.6 konnten wir Polynome f mit algebraischen oder schnell wachsenden Koeffizienten behandeln. Um auch schwerberechenbare Vielfache $f \cdot g$ solcher Polynome f zu erhalten, benutzen wir eine Methode, die wieder mit den Nullstellen von f arbeitet. Dafür verwenden wir eine modifizierte Version von Satz 1, die dies zuläßt. Wir zeigen die Existenz eines nullstellenrelevanten Polynoms q, das die spezielle Form eines Polynoms in $\sigma_1(\underline{X}), \ldots, \sigma_s(\underline{X})$ hat. Die Polynome $\sigma_1, \ldots, \sigma_s$ bezeichnen die elementarsymmetrischen Funktionen in den s Unbestimmten $X_1, \ldots, X_s$, also

$$\sigma_i(\underline{X}) := \sum_{1 \le j_1 < \cdots < j_i \le s} X_{j_1} \cdots X_{j_i} \in \mathbb{Z}[X_1, \ldots, X_s]$$

für alle $i \in \{1, \ldots, s\}$.

Gilt somit für $x_1, \ldots, x_s$ bzw. für $\sigma_1(\underline{x}), \ldots, \sigma_s(\underline{x})$, daß $p(\sigma_1(\underline{x}), \ldots, \sigma_s(\underline{x})) = 0$ nicht erfüllt ist, so sind alle Polynome, die mindestens die Nullstellen $x_1, \ldots, x_s$ besitzen, schwerberechenbar. Dies sind alle Polynome der Form fg mit $f = \prod_{i=1}^{s}(X - x_i) = X^s + \sum_{i=0}^{s-1}(-1)^{s-i}\sigma_{s-i}(\underline{x})X^i$ und $g \in \mathbb{C}[X]\backslash 0$. Es genügt dann, nur die Koeffizienten von f zu kennen, nicht die Nullstellen.

Wir werden in diesem Kapitel diese Idee durchführen. Wir zeigen zunächst die Modifikation von Satz 1.

Satz 2. *Seien $r, s, n \in \mathbb{N}_{\ge 1}$ mit $r \le 2\sqrt{n}$, $s \le 2n$ und $n \ge 48^2$.*
Seien $P_1, \ldots, P_s \in \mathbb{Q}[U_0, \ldots, U_n, X]$ Polynome mit $\deg_X P_1 = \cdots = \deg_X P_s$ und $\deg_{U_j} P_i \le 3n$ für alle $i \in \{1, \ldots, s\}$ und alle $j \in \{0, \ldots, n\}$. Sei $\gamma \in \mathbb{R}$ mit $1 < \gamma \le n$ und

$$\left(\frac{\gamma^2}{s+\gamma}\right)^s > n^{8(r+2)^2}. \tag{5.1}$$

(a) Dann gibt es ein bzgl. $P_1, \ldots, P_s$ und r nullstellenrelevantes Polynom $q \in \mathbb{Q}[X_1, \ldots, X_s]$ der Form

$$q(X_1, \ldots, X_s) = p(\sigma_1(\underline{X}), \ldots, \sigma_s(\underline{X}))$$

mit $p \in \mathbb{Q}[Y_1, \ldots, Y_s]$ *und* $\deg_{Y_i} p < \gamma \deg_X P_1$ *für alle* $i \in \{1, \ldots, s\}$.

(b) Haben die Polynome $P_1, \ldots, P_s$ *außerdem ganzzahlige Koeffizienten, und gilt* $\operatorname{wt} P_i \le 4^{n^{r+2}}$ *für alle* $i \in \{1, \ldots, s\}$ *und* $\deg_X P_1 \le 4^{n^r}$*, so gibt es ein Polynom* p *gemäß Teil (a) derart, daß alle seine Koeffizienten gleich* -1, 0 *oder* 1 *sind.*

Beweisidee: Wir gehen so vor wie im Beweis von Satz 1, setzen aber die dort auftauchenden $q_{\underline{j}}$ an als

$$q_{\underline{j}}(X_1, \ldots, X_s) = p_{\underline{j}}(\sigma_1(\underline{X}), \ldots, \sigma_s(\underline{X})).$$

Die $p_{\underline{j}} \in \mathbb{Q}[Y_1, \ldots, Y_s]$ wählen wir so, daß $\deg_{Y_i} p_{\underline{j}} < \gamma d$ für alle $i, \underline{j}$ gilt, wobei $d := \deg_X P_1 = \cdots = \deg_X P_s$ ist.

Wieder gilt Lemma 2. Zu zeigen sind noch die Analoga zu Lemma 3 und Lemma 4.

Lemma 8. *Unter den Voraussetzungen von Satz 2 gibt es ein Polynom*

$$Q = \sum_{0 \le j_1, \ldots, j_s < n^2} q_{\underline{j}}(X_1, \ldots, X_s) Y_1^{j_1} \cdots Y_s^{j_s} \in \mathbb{Q}[\underline{X}, \underline{Y}] \backslash 0$$

wie in Lemma 2, so daß gilt: $q_{\underline{j}}(X_1, \ldots, X_s) = p_{\underline{j}}(\sigma_1(\underline{X}), \ldots, \sigma_s(\underline{X}))$ *mit* $p_{\underline{j}} \in \mathbb{Q}[Y_1, \ldots, Y_s]$ *und* $\deg_{X_i} p_{\underline{j}} < \gamma d$ *für alle* $i, \underline{j}$.

Beweis. Wir betrachten die Gleichung

$$Q(\underline{X}, P_1(\underline{Q}(\underline{Z}), X_1), \ldots, P_s(\underline{Q}(\underline{Z}), X_s)) = 0,$$

also

$$\sum_{0 \le j_1, \ldots, j_s < n^2} p_{\underline{j}}(\sigma_1(\underline{X}), \ldots, \sigma_s(\underline{X})) P_1(\underline{Q}(\underline{Z}), X_1)^{j_1} \cdots P_s(\underline{Q}(\underline{Z}), X_s)^{j_s} = 0 \tag{5.2}$$

mit $\deg_{X_i} p_{\underline{j}} < \gamma d$ für alle $i, \underline{j}$. Wir fassen diese auf als homogenes lineares Gleichungssystem für die Koeffizienten der $p_{\underline{j}}$ als Unbekannten; dies sind $N := (n^2 \cdot \lceil \gamma d \rceil)^s$ viele.

Der höchste Grad, in dem ein X_i vorkommen kann, ist nun $s(\lceil \gamma d \rceil - 1) + d(n^2 - 1)$.

Bei der Abschätzung für den höchsten Grad in einem Z_j bekommen wir

$$\begin{aligned} &2rn \cdot 3n \cdot (n+1) \cdot (n^2-1)s \\ &\qquad < 2 \cdot 2\sqrt{n} \cdot n \cdot 3n \cdot 2n \cdot n^2 \cdot 2n = 48n^{\frac{1}{2}+6} \leq n^7 \text{ für } n \geq 48^2. \end{aligned}$$

Die Anzahl M der Gleichungen ist somit

$$M \leq n^{7(r+2)^2}(1 + s\gamma d + d(n^2-1))^s.$$

Es ist nun

$$\begin{aligned} \frac{\gamma d n^2}{1 + s\gamma d + d(n^2-1)} &\geq \frac{\gamma d n^2}{d + s\gamma d + d(n^2-1)} = \frac{\gamma n^2}{s\gamma + n^2} \\ &= \frac{\gamma}{s\frac{\gamma}{n^2} + 1} \geq \frac{\gamma}{s\frac{\gamma}{\gamma^2} + 1} = \frac{\gamma^3}{s\gamma + \gamma^2} = \frac{\gamma^2}{s + \gamma}, \end{aligned}$$

da $d \geq 1$ und $\gamma \leq n$. Ungleichung (5.1) liefert also

$$\begin{aligned} \frac{N}{M} &\geq \frac{1}{n^{7(r+2)^2}} \left(\frac{\gamma d n^2}{1 + s\gamma d + d(n^2-1)} \right)^s \\ &\geq \frac{1}{n^{7(r+2)^2}} \left(\frac{\gamma^2}{s+\gamma} \right)^s > n^{(r+2)^2} \geq 2 > 1, \end{aligned} \tag{5.3}$$

d. h. $N > M$, und es existiert somit eine nichttriviale Lösung für das Gleichungssystem. □

Lemma 4 hat folgendes Analogon.

Lemma 9. *Unter den Voraussetzungen von Satz 2 inklusive Teil (b) ist das Polynom Q aus Lemma 8 so wählbar, daß die Koeffizienten der $p_{\underline{j}}$ gleich -1, 0 oder 1 sind.*

Beweis. Wir wenden das Siegelsche Lemma auf das nun abgeänderte Gleichungssystem aus (5.2) an. Die Gewichte der Linearformen der linearen Gleichungen des Systems schätzen wir nach oben ab durch das Gewicht des Polynoms auf der linken Seite von (5.2), wobei wir nun die Koeffizienten von

$p_{\underline{j}}$ als zusätzliche Unbestimmte betrachten. Als obere Abschätzung für dieses Gewicht erhalten wir

$$n^{2s} \cdot (\lceil \gamma d \rceil)^s \cdot \left(4^{n^{r+2}} \cdot \left(4^{n^r}\right)^{(n+1)\cdot 3n}\right)^{(n^2-1)s},$$

wobei $\operatorname{wt} P_i \leq 4^{n^{r+2}}$, $\deg Q_j \leq 4^{n^r}$ und $\deg_{U_j} P_i \leq 3n$ verwendet wurde.

Wegen $s \leq 2n$, $\gamma \leq n$ und $d \leq 4^{n^r}$ läßt sich dies weiter nach oben abschätzen durch

$$\begin{aligned} & n^{4n} \cdot \left(n \cdot 4^{n^r}\right)^{2n} \cdot \left(4^{n^{r+2}} \cdot 4^{6n^{r+2}}\right)^{(n^2-1)\cdot 2n} \\ & \leq n^{6n} \cdot 4^{2n^{r+1}} \cdot 4^{7n^{r+2}\cdot 2n^3} \\ & \leq 4^{6n^2+2n^{r+1}+14n^{r+5}} \leq 4^{20n^{r+5}} =: w. \end{aligned}$$

Wegen Ungleichung (5.3) gilt $\frac{M}{N-M} \leq 2\frac{M}{N} \leq 2n^{-(r+2)^2}$, und daraus folgt

$$w^{\frac{M}{N-M}} \leq \left(4^{20n^{r+5}}\right)^{2n^{-(r+2)^2}} = 4^{40n^{-r^2-3r+1}}.$$

Dies ist kleiner als 2, d. h. es ist $\frac{40}{n^{r^2+3r-1}} < \frac{1}{2}$, da $n > 80$.

Somit liefert das Siegelsche Lemma eine nichttriviale Lösung für (5.2) mit Komponenten -1, 0 oder 1. Also besitzen die zugehörigen Polynome $p_{\underline{j}}$ nur die Koeffizienten -1, 0 oder 1. □

Beweis von Satz 2. Der Beweis von Teil (a) in Satz 2 besteht aus Lemma 2 und Lemma 8. Der Teil (b) folgt zusätzlich aus Lemma 9. □

Das erste Korollar aus Satz 2 beschreibt die Komplexität von Polynomen $\neq 0$ eines Ideals $\mathbb{C}[X] \cdot f$, bei dem die Koeffizienten von f algebraisch unabhängig oder algebraisch von genügend hohem Grad sind.

Korollar 12. *Sei s hinreichend groß, und seien $\alpha_0, \ldots, \alpha_{s-1} \in \mathbb{C}$ über $\mathbb{Q}$ entweder algebraisch unabhängig oder algebraisch mit $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] > 2^{\sqrt{s}}$ für*

alle $i \in \{0, \dots, s-1\}$ *und*

$$[\mathbb{Q}(\alpha_0, \dots, \alpha_{s-1}) : \mathbb{Q}] = \prod_{i=0}^{s-1} [\mathbb{Q}(\alpha_i) : \mathbb{Q}].$$

Sei $f = \sum_{i=0}^{s} \alpha_i X^i \in \mathbb{C}[X]$ *mit* $\alpha_s = 1$, *und* $g \in \mathbb{C}[X] \backslash 0$. *Dann ist* $L(fg) \geq \frac{1}{8}\sqrt{s}$.

Beispiel. Ist s hinreichend groß, sind $p_1, \dots, p_s$ paarweise verschiedene Primzahlen mit $p_j - 1 \geq 2^{\sqrt{s}}$ für alle $j \in \{1, \dots, s\}$, und ist

$$f = X^s + \sum_{j=1}^{s} e^{\frac{2\pi i}{p_j}} X^{j-1} \in \mathbb{C}[X]$$

und $g \in \mathbb{C}[X] \backslash 0$, so ist $L(fg) \geq \frac{1}{8}\sqrt{s}$.

Beweis. Sei $\alpha_{j-1} := e^{\frac{2\pi i}{p_j}}$ für $j \in \{1, \dots, s\}$. Dann ist $[\mathbb{Q}(\alpha_{j-1}) : \mathbb{Q}] = \varphi(p_j) = p_j - 1$ und

$$[\mathbb{Q}(\alpha_0, \dots, \alpha_{s-1}) : \mathbb{Q}] = \varphi(p_1 \cdots p_s) = (p_1 - 1) \cdots (p_s - 1).$$

Korollar 12 zeigt die Behauptung. □

Beweis des Korollars. Sei $n := \deg(fg) \geq s$; für hinreichend großes s ist also auch n groß genug, um Satz 2 anzuwenden.

Sei $P_i(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n$ für alle $i \in \{1, \dots, s\}$. Sei $\gamma := n$ und $r := L(fg)$; insbesondere gilt $r \leq 2\sqrt{n}$.

Es gelte $16(r+2)^2 < s$, dann ist $2r \leq \sqrt{s}$ und $2^{\sqrt{s}} \geq 2^{2r} \geq n^2$. Weiter ist

$$\begin{aligned} \left(\frac{\gamma^2}{s+\gamma}\right)^s = \left(\frac{n^2}{s+n}\right)^s &\geq \left(\frac{n^2}{n+n}\right)^s \\ = \left(\frac{n}{2}\right)^s > \left(\frac{n}{2}\right)^{16(r+2)^2} &\geq n^{8(r+2)^2}, \end{aligned}$$

wobei $s \leq n$ und $n \geq 4$ verwendet wurde; also gilt (5.1).

Seien nun $x_1, \ldots, x_s \in \mathbb{C}$ die komplexen Nullstellen von f, und sei $fg(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$.

Dann ist $P_i(\underline{a}, X) = fg(X) \neq 0$ und $P_i(\underline{a}, x_i) = fg(x_i) = 0$ für alle $i \in \{1, \ldots, s\}$.

Nach Satz 2 existiert dann ein Polynom $p \in \mathbb{Q}[Y_1, \ldots, Y_s]\backslash 0$ mit $\deg_{Y_i} p < \gamma n = n^2$, so daß

$$\begin{aligned} 0 &= p(\sigma_1(x_1, \ldots, x_s), \ldots, \sigma_s(x_1, \ldots, x_s)) \\ &= p(-\alpha_{s-1}, \alpha_{s-2}, \ldots, (-1)^s \alpha_0), \end{aligned}$$

im Widerspruch zu Lemma 5, da $2^{\sqrt{s}} \geq n^2$.

Es folgt $16(r+2)^2 \geq s$, also $2r \geq r + 2 \geq \frac{1}{4}\sqrt{s}$ (da $r \geq \log n \geq 2$ für $n \geq 4$), also ist $r \geq \frac{1}{8}\sqrt{s}$. □

Bemerkung. In Korollar 12 spielen die Nullstellen von f nur beweistechnisch eine Rolle, sie müssen nicht bekannt sein.

Zum Abschluß dieses Kapitels beschreiben wir die Komplexität von Polynomen $\neq 0$ eines Ideals $\mathbb{C}[X] \cdot f$, bei dem die Koeffizienten von f schnell wachsend sind.

Korollar 13. *Sei s hinreichend groß, und seien $\alpha_0, \ldots, \alpha_{s-1} \in \mathbb{C}$ mit $|\alpha_0| \geq 2$ und $|\alpha_{i+1}| \geq |\alpha_i|^{2^{\sqrt{s}}}$ für alle $i \in \{0, \ldots, s-2\}$. Sei $f = \sum_{i=0}^{s} \alpha_i X^i \in \mathbb{C}[X]$ mit $\alpha_s = 1$, und $g \in \mathbb{C}[X]\backslash 0$. Dann ist $L(fg) \geq \frac{1}{8}\sqrt{s}$.*

Beispiel. Ist s hinreichend groß, und ist

$$f = X^s + \sum_{j=1}^{s} 2^{2^{j\lceil\sqrt{s}\rceil}} X^{j-1} \in \mathbb{C}[X]$$

und $g \in \mathbb{C}[X]\backslash 0$, so ist $L(fg) \geq \frac{1}{8}\sqrt{s}$.

Beweis des Korollars. Wir gehen genauso vor wie im Beweis von Korollar 12. Sei wieder $n := L(fg) \geq s$ und $r := L(fg)$. Sei $P_i(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n$ und $\gamma := n$.

Es gelte $16(r+2)^2 < s$, dann gilt wieder $2^{\sqrt{s}} \geq n^2$ und

$$\left(\frac{\gamma^2}{s+\gamma}\right)^s > n^{8(r+2)^2}.$$

Zu überprüfen sind noch die Voraussetzungen von Teil (b) in Satz 2. Sie gelten, da $P_i \in \mathbb{Z}[\underline{U}, X]$, $\deg_X P_i = n \leq 4^{n^r}$ und $\operatorname{wt} P_i = n + 1 \leq 4^{n^{r+2}}$ gilt.

Demnach gibt es nach Satz 2 ein Polynom $p \neq 0$ mit Koeffizienten -1, 0 oder 1 und $p(-\alpha_{s-1}, \alpha_{s-2}, \ldots, (-1)^s \alpha_0) = 0$. Wegen $\deg_{Y_i} p < n^2 \leq 2^{\sqrt{s}}$ haben wir einen Widerspruch zu Lemma 6.

Es folgt $16(r+2)^2 \geq s$, also $L(fg) \geq \frac{1}{8}\sqrt{s}$. □

Bemerkung. Sei f ein Polynom mit weniger schnell wachsenden Koeffizienten, und zwar mit Koeffizienten $\alpha_0, \ldots, \alpha_{s-1} \in \mathbb{C}$ so, daß $|\alpha_0| \geq 2$ und $|\alpha_{i+1}| \geq |\alpha_i|^2$ für alle $i \in \{0, \ldots, s-2\}$ gilt. So ein Polynom ist beispielsweise $f = X^s + \sum_{i=0}^{s-1} 2^{2^i} X^i$.

Man erwartet, daß f ebenfalls derart ist, daß alle seine Vielfachen $\neq 0$ schwerberechenbar sind, vermutlich mit unterer Komplexitätsschranke $C\sqrt[3]{s}$ für jedes Vielfache $\neq 0$, mit einer Konstanten $C > 0$.

Tatsächlich läßt sich dies mit unseren Methoden nicht zeigen.

Diese laufen nämlich darauf hinaus, ein nullstellenrelevantes Polynom der Form $p(\sigma_t(\underline{X}), \sigma_{2t}(\underline{X}), \ldots, \sigma_{\lfloor \frac{s}{t} \rfloor t}(\underline{X}))$ mit $t := \lfloor \sqrt[3]{s} \rfloor$ zu benutzen, ähnlich wie es im Beweis von Korollar 3 benutzt wurde.

Um zu zeigen, daß ein solches Polynom existiert, wäre eine Modifikation von Satz 2 nötig, die nicht möglich ist. Denn im modifizierten linearen Gleichungssystem, das dem in (5.2) entspricht, bleibt die Abschätzung für die Anzahl M der Gleichungen zwar gleich, aber die Anzahl N der Unbestimmten ist dann zu klein. Die Bedingung $N > M$ läßt sich so nicht mehr erfüllen.

6 Vergleichsweise kleine ganzzahlige Koeffizienten

Es gibt ein Polynom mit vergleichsweise kleinen ganzzahligen Koeffizienten, so daß alle Vielfachen $\neq 0$ schwerberechenbar sind. Gemeint ist ein Polynom, dessen Koeffizienten nicht schnell wachsen, wie das sonst bisher der Fall war (z. B. in Korollar 13). Genauer gesagt, diese lassen sich im Betrag nach oben durch $2^{\sqrt[3]{s}}$ abschätzen, wenn s den Grad bezeichnet. Leider läßt sich ein solches Polynom nicht explizit angeben.

Wir erhalten *nicht*, daß die meisten Polynome mit derart kleinen ganzzahligen Koeffizienten diese Eigenschaft besitzen. Dies wäre in dem Sinne des in der Einleitung erwähnten bekannten Satzes, nach dem die meisten Polynome mit $\{0,1\}$-Koeffizienten schwerberechenbar sind.

Satz 3. *Für alle hinreichend großen s gibt es ein Polynom $f \in \mathbb{Z}[X]$ vom Grad s und mit Koeffizienten vom Betrag $\leq 2^{\sqrt[3]{s}}$ so, daß für alle $g \in \mathbb{C}[X]\backslash 0$ die Abschätzung $L(fg) \geq \frac{1}{12}\sqrt[3]{s}$ gilt.*

Beweis. Sei s hinreichend groß mit $r := \lfloor \frac{1}{6}\sqrt[3]{s} \rfloor \geq 1$. Dann gilt

$$\left(\frac{5}{4}\right)^s > 2^{6r(r+2)^2}, \tag{6.1}$$

da $6r(r+2)^2 \leq 6r(3r)^2 = 54r^3 \leq \frac{54}{6^3}s = \frac{1}{4}s < s\log\left(\frac{5}{4}\right)$ gilt. Sei $n := 2^r = 2^{\lfloor \frac{1}{6}\sqrt[3]{s} \rfloor}$. Für hinreichend großes s ist also auch n groß, und es gilt $s \leq n$.

Seien $Q_0(\underline{Z}), \ldots, Q_n(\underline{Z})$ die Polynome des Darstellungssatzes für n und r in den Unbestimmten $Z_1, \ldots, Z_{(r+2)^2}$. Sei für Unbestimmte $U_0, \ldots, U_n$

$$P(\underline{U}, X) := U_0 + U_1 X + \cdots + U_n X^n$$

und

$$F(\underline{Z}, X) := P(Q_0(\underline{Z}), \ldots, Q_n(\underline{Z}), X) \in \mathbb{Z}[\underline{Z}, X].$$

Wir betrachten für weitere Unbestimmte $X_1, \ldots, X_s$ die Gleichung

$$\sum_{0 \leq j_1, \ldots, j_s < n^2} q_{\underline{j}}(\underline{X}) F^{j_1}(\underline{Z}, X_1) \cdots F^{j_s}(\underline{Z}, X_s) = 0 \tag{6.2}$$

mit

$$q_{\underline{j}}(\underline{X}) = \sum_{-n\le k_1,\ldots,k_s\le n} \beta_{\underline{j},\underline{k}} \prod_{i=1}^{s} \prod_{\substack{-n\le l\le n\\ l\neq k_i}} (\sigma_i(\underline{X}) - l) \in \mathbb{Q}[\underline{X}] \qquad (6.3)$$

als homogenes lineares Gleichungssystem in den Unbekannten $\beta_{\underline{j},\underline{k}}$. Man erhält es (wie im Beweis von Lemma 3), wenn man die linke Seite von (6.2) als Linearkombination von Monomen in $\underline{X}, \underline{Z}$ schreibt und einen Koeffizientenvergleich vornimmt. Es hat ganzzahlige Koeffizienten, und gesucht ist eine nichttriviale rationale Lösung.

Die Anzahl N der Unbekannten $\beta_{\underline{j},\underline{k}}$ des Gleichungssystems ist

$$N = n^{2s} \cdot (2n+1)^s,$$

und die Anzahl M seiner Gleichungen ist gleich der Anzahl der in (6.2) vorkommenden Monome in $\underline{X}, \underline{Z}$. Wir bestimmen dazu für jede Unbestimmte X_i bzw. Z_j den höchsten Grad, mit der sie in (6.2) vorkommen kann.

Für X_i ist dieser Grad $2ns + n(n^2-1)$.
Für Z_j ist er $2rn(n+1)(n^2-1)s \le n^6 - 1$. Diese Abschätzung gilt wegen der Gradabschätzung im Darstellungssatz, $r \le \sqrt{s} \le \sqrt{n}$ und $s \le n$. Es folgt

$$M \le n^{6(r+2)^2}(2ns + n(n^2-1) + 1)^s.$$

Wir erhalten

$$\begin{aligned}
\frac{N}{M} &\ge \frac{1}{n^{6(r+2)^2}} \left(\frac{n^2(2n+1)}{2ns + n(n^2-1) + 1}\right)^s \\
&\ge \frac{1}{n^{6(r+2)^2}} \left(\frac{n^2(2n+1)}{2n^2 + n^3}\right)^s = \frac{1}{n^{6(r+2)^2}} \left(\frac{2n+1}{2+n}\right)^s \\
&\ge \frac{1}{n^{6(r+2)^2}} \left(\frac{5}{4}\right)^s > \frac{1}{n^{6(r+2)^2}} 2^{6r(r+2)^2} = \left(\frac{2^r}{n}\right)^{6(r+2)^2} = 1,
\end{aligned}$$

wegen Ungleichung (6.1). Also ist $M < N$, und das Gleichungssystem hat eine nichttriviale rationale Lösung für die Unbekannten $\beta_{\underline{j},\underline{k}}$. Die zugehörigen Polynome $q_{\underline{j}}$ der Form (6.3) erfüllen also (6.2) und sind nicht alle gleich 0: Ist etwa $\beta_{\underline{j}',\underline{k}'} \neq 0$, und sind $x_1, \ldots, x_s$ die komplexen Nullstellen des Polynoms

$$X^s + \sum_{i=0}^{s-1} (-1)^{s-i} k'_{s-i} X^i \in \mathbb{Z}[X],$$

so gilt

$$q_{\underline{j'}}(x_1,\ldots,x_s) = \sum_{-n\le k_1,\ldots,k_s\le n} \beta_{\underline{j'},\underline{k}} \prod_{i=1}^{s} \prod_{\substack{-n\le l\le n\\ l\neq k_i}} (\sigma_i(\underline{x}) - l)$$

$$= \sum_{-n\le k_1,\ldots,k_s\le n} \beta_{\underline{j'},\underline{k}} \prod_{i=1}^{s} \prod_{\substack{-n\le l\le n\\ l\neq k_i}} (k'_i - l) = \beta_{\underline{j'},\underline{k'}} \prod_{i=1}^{s} \prod_{\substack{-n\le l\le n\\ l\neq k'_i}} (k'_i - l) \neq 0, \quad (6.4)$$

also ist $q_{\underline{j'}} \neq 0$.

Sei nun $\underline{j'} = (j'_1,\ldots,j'_s)$ das lexikographisch erste s-Tupel $\underline{j}$ mit $q_{\underline{j}} \neq 0$, und dazu ein $\underline{k'}$ mit $\beta_{\underline{j'},\underline{k'}} \neq 0$ gegeben. Sei

$$f := X^s + \sum_{i=0}^{s-1} (-1)^{s-i} k'_{s-i} X^i \in \mathbb{Z}[X].$$

Dann ist $|k'_i| \le n = 2^r \le 2^{\frac{1}{6}\sqrt[3]{s}} \le 2^{\sqrt[3]{s}}$ für alle $i \in \{1,\ldots,s\}$. Wir zeigen, daß dieses Polynom f die Behauptung erfüllt.

Sei dazu $g \in \mathbb{C}[X]\backslash 0$. Wir nehmen an, daß $L(fg) \le r$ sei.

Da dann wegen der Gradabschätzung $\deg(fg) \le 2^{L(fg)} \le 2^r = n$ gilt, schreiben wir $fg = \sum_{j=0}^{n} b_j X^j \in \mathbb{C}[X]$.

Nun gilt Lemma 2 für das Polynom

$$Q := \sum_{\underline{j}} q_{\underline{j}}(\underline{X}) Y_1^{j_1} \cdots Y_s^{j_s} \in \mathbb{Z}[\underline{X},\underline{Y}]$$

mit $P_i := P$ für alle $i \in \{1,\ldots,s\}$. Somit ist $q_{\underline{j'}}$ nullstellenrelevant bzgl. $\underbrace{P,\ldots,P}_{s\text{-mal}}$ und r.

Es folgt: Sind $x_1,\ldots,x_s$ die komplexen Nullstellen von f, so sind $x_1,\ldots,x_s$ Nullstellen von $P(\underline{b},X) = fg(X) \neq 0$, und somit ist $q_{\underline{j'}}(x_1,\ldots,x_s) = 0$.

Wie in (6.4) können wir aber auch $q_{\underline{j'}}(x_1, \ldots, x_s) \neq 0$ zeigen, und dies ist ein Widerspruch zur Annahme $L(fg) \leq r = \lfloor \frac{1}{6}\sqrt[3]{s} \rfloor$. Es folgt $L(fg) > r \geq \frac{1}{12}\sqrt[3]{s}$ für hinreichend großes s. □

Ebenso können wir auch den folgenden Satz zeigen:

Satz 4. *Für alle hinreichend großen s gibt es ein Polynom $f \in \mathbb{Z}[X]$ vom Grad s und mit s ganzzahligen Nullstellen vom Betrag $\leq 2^{\sqrt[3]{s}}$ so, daß für alle $g \in \mathbb{C}[X]\backslash 0$ die Abschätzung $L(fg) \geq \frac{1}{12}\sqrt[3]{s}$ gilt. (Mehrfache Nullstellen sind dabei möglich.)*

Der Beweis verläuft analog zu dem von Satz 3, wobei die $\sigma_i(\underline{X})$ in dem Ansatz (6.3) für die $q_{\underline{j}}$ jeweils durch X_i zu ersetzen sind. Die Abschätzungen für N und M bleiben gleich. Zu beachten ist noch, daß die komplexen Nullstellen $x_1, \ldots, x_s$ von f, nämlich $k'_1, \ldots, k'_s$, in der erforderlichen Reihenfolge gewählt werden können.

Literaturverzeichnis

[1] M. Aldaz, J. Heintz, G. Matera, J. L. Montaña and L. M. Pardo (2000), Timespace tradeoffs in algebraic complexity theory. *J. of Complexity* **16**, 2-49.

[2] W. Baur (1997), Simplified Lower Bounds for Polynomials with Algebraic Coefficients. *J. of Complexity* **13**, 38-41.

[3] W. Baur and K. Halupczok (1999), On lower bounds for the complexity of polynomials and their multiples. *Comp. Compl.* **8**, 309-315.

[4] P. Bürgisser, M. Clausen and A. Shokrollahi (1997). Algebraic Complexity Theory, *A Series of comprehensive studies in mathematics* **315**, *Springer*.

[5] J. von zur Gathen and V. Strassen (1980), Some polynomials that are hard to compute. *Theoret. Comp. Sc.* **11**, 331-336.

[6] J. Heintz (1986), On polynomials with symmetric Galois group which are easy to compute. *Theoret. Comp. Sc.* **47**, 99-105.

[7] J. Heintz and J. Morgenstern (1993), On the intrinsic complexity of elimination theory. *J. of Complexity* **9**, 471-498.

[8] J. Heintz and M. Sieveking (1980), Lower bounds for polynomials with algebraic coefficients. *Theoret. Comp. Sc.* **11**, 321-330.

[9] A. Löh (2000), Komplexitätsschranken für Polynome mit algebraischen Koeffizienten. Diplomarbeit, Konstanz.

[10] G. Malajovich (1999), Lower bounds for some decision problems over $\mathbb{C}$. Eingereicht bei *Theoret. Comp. Sc.*

[11] M. S. Paterson and L. J. Stockmeyer (1973), On the number of nonscalar multiplications necessary to evaluate polynomials. *SIAM J. Comput.* **2**, 60-66.

[12] C. P. Schnorr (1978), Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials. *Theoret. Comp. Sc.* **7**, 251-261.

[13] H.-J. Stoss (1989), Lower Bounds for the complexity of polynomials. *Theoret. Comp. Sc.* **64**, 15-23.

[14] V. Strassen (1974), Polynomials with rational coefficients which are hard to compute. *SIAM J. Comput.* **3**, 128-149.

[15] V. Strassen (1984), Algebraische Berechnungskomplexität. *Perspectives in Mathematics, Anniversary of Oberwolfach 1984. Birkhäuser.*